# Oracle® Enterprise Manager

Cloud Control Advanced Installation and Configuration Guide

12*c* Release 5 (12.1.0.5)

**E24089-47**

February 2016

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide, 12*c* Release 5 (12.1.0.5)

E24089-47

Primary Author: Aravind Jayaraaman

Contributing Author: Dennis Lee, Pradeep Gopal, Genevieve D'Souza, Namrata Bhakthavatsalam, Leo Cloutier, Thom Chumley

Contributor: Enterprise Manager Cloud Control Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams.

# Contents

## Part II Installing Enterprise Manager System

## 3 Installing Enterprise Manager in Silent Mode

## 4 Installing Enterprise Manager Using the Software-Only Method

## Part III Installing Additional Oracle Management Service

## 5 Installing Additional Oracle Management Services in Silent Mode

## Part IV Installing Oracle Management Agent

## 6 Installing Oracle Management Agent in Silent Mode

## 7 Cloning Oracle Management Agents

## 8 Installing Shared Agents

## 9 Installing the Oracle Management Agent Software Now and Configuring It Later

## Part V Advanced Installation and Configuration

## 10 Configuring Enterprise Manager for Firewalls

## 11 Sizing Your Enterprise Manager Deployment

## 12 Installing ADP with Advanced Installation Options

## 13 Installing JVMD with Advanced Install Options

## 14 Configuring BI Publisher with Enterprise Manager

## 15 Running the OMS in Console-Only Mode

## Part VI Configuring Enterprise Manager for High Availability

## 16 High Availability Solutions

## 17 Enterprise Manager High Availability

## 18 Enterprise Manager Disaster Recovery

## 19 Backing Up and Recovering Enterprise Manager

## 20 Running Multiple BI Publisher Servers

## Part VII Deinstallation

## 21 Deinstalling Enterprise Manager (Single and Multi-OMS Environments)

## 22 Deinstalling Oracle Management Agents

## 23 Deinstalling ADP and JVMD

## 24 Removing Standby Oracle Management Services

# Part VIII Appendixes

## A Understanding the Enterprise Manager Directory Structure

## B Overview of the Installation and Configuration Log Files

## C Redirecting Oracle Management Agent to Another Oracle Management Service

## D Applying Patches to Oracle Management Agents While Deploying or Upgrading Them

## E Using the RepManager Utility

## F Collecting OCM Data Using Oracle Harvester

## G Enabling the Enterprise Manager Accessibility Features

## H Configuring Targets for Failover in Active/Passive Environments

## I Standby OMSs Using Standby WebLogic Domain

## J Troubleshooting

# Preface

*Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* is an extension to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

While the *Oracle Enterprise Manager Cloud Control Basic Installation Guide* covers basic installation procedures that help you get started with Enterprise Manager Cloud Control, the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* covers advanced installation procedures that help you install and configure the Enterprise Manager Cloud Control components in more complex environments.

This preface contains the following topics:

- Intended Audience
- Purpose of the Document
- Documentation Accessibility
- Related Documents
- Conventions

## Intended Audience

*Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* is meant for system administrators who want to install Enterprise Manager Cloud Control components in complex environments.

## Purpose of the Document

*Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* covers the following:

- Installing the following in graphical mode:
  - Enterprise Manager Cloud Control software only so that you can configure it later
  - Oracle Management Agent using a shared Oracle home
  - Application Dependency and Performance (ADP) with advanced installation options
  - JVM Diagnostics (JVMD) with advanced installation options
- Installing the following in silent mode:
  - Enterprise Manager Cloud Control

  - Enterprise Manager Cloud Control software only so that you can configure it later
  - Additional Oracle Management Service
  - Oracle Management Agent
  - Oracle Management Agent software only so that you can configure it later
  - Oracle Management Agent using a shared Oracle home
- Cloning Oracle Management Agent in graphical and silent mode
- Configuring advanced installation tasks such as configuring firewalls, sizing the Enterprise Manager deployment, and integrating BI publisher.
- Deinstalling Enterprise Manager Cloud Control and Oracle Management Agent in graphical and silent mode

*Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* does NOT cover the following procedures. These procedures are documented in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- Installing Enterprise Manager Cloud Control in graphical mode
- Installing an additional Oracle Management Service in graphical mode
- Installing Oracle Management Agent in graphical mode
- Installing JVM Diagnostics and Application Dependency and Performance with default installation options

Also, *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* does NOT cover the procedure for upgrading your existing Enterprise Manager system. The upgrade procedure is documented in the *Oracle Enterprise Manager Cloud Control Upgrade Guide.*

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

For 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 Upgrade Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*

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

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

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. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `monospace` | Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

# What’s New in This Book Revision

In addition updating the books for an incremental software release or a patch set release, Oracle revises its books regularly to incorporate bug fixes and value-added feedback from customers, product managers, support teams, and other key stakeholders. Every time a book is revised, the revision number of the book is increased by one and then published on Oracle Technology Network (OTN).

This chapter lists the changes incorporated in the latest revision (E24089-47) and all the previous revisions of *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* (this book). Note that the latest revision (E24089-47) is the current revision published on OTN, and the latest revision always contains all the changes incorporated in its previous revisions.

In particular, this chapter covers the following:

- Changes Incorporated in the Latest Revision (Published)
- Changes Incorporated in the Previous Revisions (Archived)

## Changes Incorporated in the Latest Revision (Published)

The following are the changes incorporated in the latest revision (E24089-47) that is published on OTN.

| Part, Chapter, or Section Number | Change Description |
|---|---|
| Chapter J | Added a reference note to My Oracle Support note 1495519.1.at section J.1.7.2. |

## Changes Incorporated in the Previous Revisions (Archived)

The following sections describe the changes incorporated in the previous revisions. These revisions have been archived, and therefore are not currently available on OTN.

### Changes Incorporated in E24089-46

| Part, Chapter, or Section Number | Change Description |
|---|---|
| Chapter 11 | Removed references to 13c. |

## Changes Incorporated in E24089-45

| Part, Chapter, or Section Number | Change Description |
|---|---|
| Section 7.2 | Added a point about `emd.properties` file changes not being carried over after cloning. |

## Changes Incorporated in E24089-44

| Part, Chapter, or Section Number | Change Description |
|---|---|
| Chapter 18 | Update chapter reference in the introductory paragraph. |
| Chapter 14 | Remove release 5 references. Correct *configureBIP* script reference. |

# Part I

## Getting Started

This part describes how you can procure the Enterprise Manager Cloud Control software and the Oracle Management Agent software, and explains some key concepts you must know before you start using Enterprise Manager Cloud Control. In particular, this part contains the following chapters:

- Chapter 1, "Procuring the Software"
- Chapter 2, "Understanding the Basics"

1

# Procuring the Software

This chapter describes how you can procure the Enterprise Manager Cloud Control software and the Oracle Management Agent software. In particular, this chapter covers the following:

- Releases Available for Enterprise Manager Cloud Control
- Procuring the Enterprise Manager Cloud Control Software
- Procuring the Oracle Management Agent Software

## 1.1 Releases Available for Enterprise Manager Cloud Control

Table 1–1 describes the releases Enterprise Manager Cloud Control has had so far.

*Table 1–1 Enterprise Manager Cloud Control Releases*

| Release Numbers | Release Type | Release Date | Implementation Method | Description |
|---|---|---|---|---|
| *(Recommended)*<br>Oracle Enterprise Manager Cloud Control 12*c* Release 5 (12.1.0.5) | Patch Set 4 | June 2015 | ■ New installation of 12*c* Release 5 (12.1.0.5)<br>■ Upgrade from 12*c* Release 4 (12.1.0.4)<br>■ Upgrade from 12*c* Release 3 (12.1.0.3) *[either (12.1.0.3) or (12.1.0.3) Plug-in Update 1]*<br>■ Upgrade from 12*c* Release 2 (12.1.0.2) *[either (12.1.0.2) or (12.1.0.2) Plug-in Update 1]*<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Patch set containing several bug fixes, enhancements, and new features. |
| Oracle Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4) | Patch Set 3 | May 2014 | ■ New installation of 12*c* Release 4 (12.1.0.4)<br>■ Upgrade from 12*c* Release 3 (12.1.0.3) *[either (12.1.0.3) or (12.1.0.3) Plug-in Update 1]*<br>■ Upgrade from 12*c* Release 2 (12.1.0.2) *[either (12.1.0.2) or (12.1.0.2) Plug-in Update 1]*<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Patch set containing several bug fixes, enhancements, and new features. |

*Table 1–1 (Cont.) Enterprise Manager Cloud Control Releases*

| Release Numbers | Release Type | Release Date | Implementation Method | Description |
|---|---|---|---|---|
| Oracle Enterprise Manager Cloud Control 12*c* Release 3 Plug-in Update 1 (12.1.0.3) | Plug-In Update 1<br>*(Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3) software with plug-ins released in October 2013)* | October 2013 | ■ New installation of 12*c* Release 3 (12.1.0.3)<br>■ Upgrade from 12*c* Release 2 (12.1.0.2), which is (12.1.0.2) Patch Set 1 or (12.1.0.2) Plug-in Update 1<br>■ Upgrade from 12*c* Release 1 (12.1.0.1), only with Bundle Patch 1<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Contains the 12*c* Release 3 (12.1.0.3) software binaries updated with new plug-ins and updated plug-in versions released in October 2013.<br>However, the 12c Release 3 (12.1.0.3) software binaries have not been changed; they have only been integrated with new plug-ins and updated plug-in versions released in October 2013. Even the Management Agent software binaries have not been changed. This is essentially a release, and not a patch set or a patch.<br>To view a list of plug-ins integrated with this release, see the *List of Plug-ins Integrated with this Release* section in the *Getting Started* chapter of the *Oracle Enterprise Manager Cloud Control Basic Installation Guide 12c Release 3 (12.1.0.3)*. The guide is available in the Enterprise Manager documentation library at the following URL:<br>`http://www.oracle.com/technetwork/indexes/documentation/index.html` |
| Oracle Enterprise Manager Cloud Control 12*c* Release 3 (12.1.0.3) | Patch Set 2 | June 2013 | ■ New installation of 12*c* Release 3 (12.1.0.3)<br>■ Upgrade from 12*c* Release 2 (12.1.0.2) *[either (12.1.0.2) or (12.1.0.2) Plug-in Update 1]*<br>■ Upgrade from 12*c* Release 1 (12.1.0.1), only with Bundle Patch 1<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Patch set containing several bug fixes, enhancements, and new features. |

*Table 1–1 (Cont.) Enterprise Manager Cloud Control Releases*

| Release Numbers | Release Type | Release Date | Implementation Method | Description |
|---|---|---|---|---|
| Oracle Enterprise Manager Cloud Control 12c Release 2 Plug-in Update 1 (12.1.0.2) | Plug-In Update 1<br>*(Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) software with plug-ins released in February 2013)* | February 2013 | ▪ New installation of 12*c* Release 2 (12.1.0.2)<br>▪ Upgrade from 12*c* Release 1 (12.1.0.1), with or without Bundle Patch 1<br>▪ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Contains the 12*c* Release 2 (12.1.0.2) software binaries updated with new plug-ins and updated plug-in versions released in February 2013.<br>However, the 12c Release 2 (12.1.0.2) software binaries have not been changed; they have only been integrated with new plug-ins and updated plug-in versions released in February 2013. Even the Management Agent software binaries have not been changed. This is essentially a release, and not a patch set or a patch.<br>To view a list of plug-ins integrated with this release, see the *List of Plug-ins Integrated with this Release* section in the *Getting Started* chapter of the *Oracle Enterprise Manager Cloud Control Basic Installation Guide 12c Release 2 (12.1.0.2)*. The guide is available in the Enterprise Manager documentation library at the following URL:<br>`http://www.oracle.com/technetwork/indexes/documentation/index.html` |

*Table 1–1 (Cont.) Enterprise Manager Cloud Control Releases*

| Release Numbers | Release Type | Release Date | Implementation Method | Description |
|---|---|---|---|---|
| Enterprise Manager Cloud Control 12*c* Release 2 (12.1.0.2) | Patch Set 1 | August 2012 | ■ New installation of 12*c* Release 2 (12.1.0.2)<br>■ Upgrade from 12*c* Release 1 (12.1.0.1), with or without Bundle Patch 1<br>■ Upgrade from 10g Release 5 (10.2.0.5), 11g Release 1 (11.1.0.1) | Patch set containing several bug fixes, enhancements, and new features. |
| Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.1) | Bundle Patch 1 | January 2012 | ■ New installation of 12c Release 1 (12.1.0.1) containing Bundle Patch 1.<br>■ Patching of the base release, that is, 12*c* Release 1 (12.1.0.1)<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | Bundle patch containing several bug fixes and support for ported platforms. |
| Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.1) | Base Release | October 2011 | ■ New installation of 12*c* Release 1 (12.1.0.1)<br>■ Upgrade from 10*g* Release 5 (10.2.0.5), 11*g* Release 1 (11.1.0.1) | First ever 12*c* release. |

**Note:** For more information on these releases and the platforms they support, access the Enterprise Manager Cloud Control Certification Matrix. For instructions to access this matrix, refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 1.2 Procuring the Enterprise Manager Cloud Control Software

You can procure the Enterprise Manager Cloud Control software from either the product DVD or the Oracle Technology Network (OTN) Web site. This section describes these sources and covers the following:

- How Do You Access the Enterprise Manager Cloud Control Software from a DVD?
- How Do You Procure the Software from Oracle Technology Network?

### 1.2.1 How Do You Access the Enterprise Manager Cloud Control Software from a DVD?

You can obtain the Enterprise Manager Cloud Control software from the product DVD that is available through Oracle Service Delivery Managers or Oracle Sales Representatives. The software may be available either on a single DVD or on DVDs depending on the operating system.

This section covers the following:

- Accessing the Software from a DVD
- Setting Mount Points for a DVD

#### 1.2.1.1 Accessing the Software from a DVD

If the software is available on a single DVD, then insert the DVD into the DVD drive, and manually run the Enterprise Manager Cloud Control Installation Wizard.

If the software is available on multiple DVDs, then copy the archived software from each of the DVDs to a location on your local disk. Extract the contents of each of the archived files to the same location. Then, invoke the Enterprise Manager Cloud Control Installation Wizard.

For example, for 12*c* Release 5 (12.1.0.5), Oracle delivers three DVDs for Linux x86 and x86_64, mainly these:

- DVD1, containing a ZIP file with the name `em12105_linux_disk1of3.zip`
- DVD2, containing a ZIP file with the name `em12105_linux_disk2of3.zip`
- DVD3, containing a ZIP file with the name `em12105_linux_disk3of3.zip`

In this case, copy the three ZIP files to a location on your disk, for example, `/temp,` and then extract their contents in the same location. Extracting the contents to different locations will cause the installation to fail.

```
$ cp -r em12105_linux_disk1of3.zip /temp

$ cp -r em12105_linux_disk2of3.zip /temp

$ cp -r em12105_linux_disk3of3.zip /temp

$ cd /temp

$ unzip em12105_linux_disk1of3.zip

$ unzip em12105_linux_disk2of3.zip

$ unzip em12105_linux_disk3of3.zip
```

> **Note:** For information about the Enterprise Manager Cloud Control Installation Wizard, see Section 2.1.2.

#### 1.2.1.2 Setting Mount Points for a DVD

If you want to access the DVD from a shared DVD drive, then set a mount point for the DVD drive.

On most Linux operating systems, the disk mounts automatically when you insert the DVD into the DVD drive. However, for some Linux operating systems, you might have to manually mount the disk. To verify whether the disk mounts automatically and to manually mount the disk if it does not mount itself automatically, follow these steps:

1. Insert the DVD into the disk drive.
2. To verify if the disk is automatically mounted, run the following command:
   - On Red Hat Enterprise Linux:

     ```
     # ls /mnt/cdrom
     ```

   - On SUSE Linux Enterprise Server:

     ```
     # ls /media/cdrom
     ```

3. If the command in Step (2) fails to display the contents of the disk, then run the following command:

   - On Red Hat Enterprise Linux:

     ```
     # mount -t nfs <host name>:/mnt/<full path to the dvdrom>
     ```

   - On SUSE Linux Enterprise Server:

     ```
     # mount -t nfs <host name>:/media/<full path to the dvdrom>
     ```

On most AIX operating systems, the disk mounts automatically when you insert the DVD into the DVD drive. However, for some AIX operating systems, you might have to manually mount the disk. To manually mount the disk if it does not mount itself automatically, follow these steps:

1. Switch the user to *root* user by running the following command:

   ```
   $ su -root
   ```

2. Insert the disk into the drive.

   > **Note:** If required, enter the following command to eject the currently mounted disk and to remove it from the drive:
   >
   > ```
   > # /usr/sbin/umount /<SD_DVD>
   > ```

3. Enter the following command:

   ```
   # /usr/sbin/mount -rv cdrfs /dev/cd0 /SD_DVD
   ```

   In this example command, /SD_DVD is the disk mount point directory and /dev/cd0 is the device name for the disk device.

4. If you are prompted to specify the disk location, then specify the disk mount point directory path. For example, /SD_DVD

## 1.2.2 How Do You Procure the Software from Oracle Technology Network?

You can procure the Enterprise Manager Cloud Control software from OTN. The software available on OTN is archived using Info-ZIP's highly portable ZIP utility. The software is available in  ZIP files. After downloading the software, you will need the UNZIP utility to extract the files.

This section covers the following:

- Downloading the Enterprise Manager Cloud Control Software
- Verifying the File Size of Enterprise Manager Zip Files
- Extracting the Contents of the Enterprise Manager Zip File
- Verifying the Enterprise Manager Cloud Control Software Release Description
- Verifying the Platform Information

### 1.2.2.1 Downloading the Enterprise Manager Cloud Control Software

To download the Enterprise Manager Cloud Control software from OTN, access the following URL:

http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html

The software is available in ZIP files. Download the ZIP files to a common location on your local disk.

#### 1.2.2.2 Verifying the File Size of Enterprise Manager Zip Files

After downloading the ZIP files, do the following:

1. Run the `cksum` command against the ZIP files and check if the file checksum of the downloaded software is the same as the file checksum displayed on OTN.

   For example, the following is the format of the ZIP files released for 12*c* Release 5 (12.1.0.5):

   *em12105_<platform>_diskNofM.zip (<value> bytes) (cksum - <value>)*

   Here, *<platform>* refers to the operating system, *N* refers to the ZIP file number, and *M* refers to the total number of ZIP files available for download. For example, em12105_linux_disk1of3.zip, em12105_linux_disk2of3.zip, em12105_linux_disk3of3.zip.

   The value *(cksum - <value>)* is the file checksum that you need to check. To check the file checksum of the first ZIP file, run the following command:

   ```
   $ cksum em12105_<platform>_diskNofM.zip
   ```

   For example,

   ```
   $ cksum em12105_linux_disk1of3.zip
   ```

2. Extract the contents of the ZIP files to a single directory. Navigate to the directory and verify if you see the following files:

   ```
   [a@adcxxxxxxx Disk1]$ ls
   install  libskgxn  plugins           response      stage   WT.zip
   jdk      oms       runInstaller      wls           bipruntime
   ```

#### 1.2.2.3 Extracting the Contents of the Enterprise Manager Zip File

You must unzip the archive on the platform for which it was intended. For example, if you download the software for the Linux x86 operating system, then you must unzip the file on a Linux x86 operating system only. If you unzip the file on a Microsoft Windows computer and then move the stage area to a Linux computer, then the staged area files will get corrupted. This is because Microsoft Windows does not preserve the case sensitivity or the permission bits of Linux file names.

If you have downloaded a single ZIP file, then extract the contents of it and manually run the Enterprise Manager Cloud Control Installation Wizard.

> **Note:** For information about the Enterprise Manager Cloud Control Installation Wizard, see Section 2.1.2.

If you have downloaded multiple ZIP files to a common location, then extract the contents of all the ZIP files in the same location, and then manually run the Enterprise Manager Cloud Control Installation Wizard.

> **WARNING: Extracting the contents to different locations will cause the installation to fail.**

> **Tip:** If you plan to store the files on a DVD, then first extract the contents of the ZIP files, and then copy those extracted files to the DVD. Do NOT copy the ZIP files; you need the unzipped contents of the ZIP files to install the product.

### 1.2.2.4 Verifying the Enterprise Manager Cloud Control Software Release Description

Verify the software release details to ensure that you have downloaded the latest version.

1. After extracting the contents of the software ZIP files, navigate to the following location and access the properties file that contains the software release description:

   ```
   Disk1/install/em/release.properties
   ```

2. Make sure you see the following description that confirms that it is the latest software:

   **Release:Oracle Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5)**

### 1.2.2.5 Verifying the Platform Information

After extracting the contents of the ZIP file, access the following file to verify the platform information. Here, `<Software_Location>` can be either the DVD mount point or the location on your local disk where you have extracted the contents of the ZIP files.

```
<Software_Location>/stage/shiphomeproperties.xml
```

Note that a 32-bit Enterprise Manager Cloud Control software (both Enterprise Manager Cloud Control and Oracle Management Agent) can be installed only on a 32-bit operating system that is running on a 32-bit hardware. Similarly, a 64-bit Enterprise Manager software can be installed only on a 64-bit operating system that is running on a 64-bit hardware.

Do NOT try to install a 32-bit software on a 64-bit platform or vice versa; the installation may proceed, but will fail eventually. Therefore, ensure that you use the right software download for the right platform.

The `shiphomeproperties.xml` file provides the platform information as shown here:

```
<?xml version="1.0" standalone="yes" ?>
<ORACLEHOME_INFO>
<ARU_PLATFORM_INFO>
<ARU_ID>46</ARU_ID>
<ARU_ID_DESCRIPTION>Linux x86</ARU_ID_DESCRIPTION>
</ARU_PLATFORM_INFO>
</ORACLEHOME_INFO>
```

You can see the platform information in the `<ARU_ID_DESCRIPTION>` syntax. Table 1–2 lists the platform names that may be enclosed in this syntax, and describes whether the names represent a 32-bit or 64-bit software.

*Table 1–2 Verifying Platform Information*

| Platform Name | Platform Specified in ARU_ID_ DESCRIPTION | 32-bit / 64-bit |
|---|---|---|
| Linux x86 | Linux x86 | 32-bit |
| Microsoft Windows (32-bit) | Win 32 | 32-bit |

*Table 1–2 (Cont.) Verifying Platform Information*

| Platform Name | Platform Specified in ARU_ID_ DESCRIPTION | 32-bit / 64-bit |
|---|---|---|
| Microsoft Windows (64-bit AMD64) | win 64 | 64-bit |
| Microsoft Windows (64-bit IA) | Windows Itanium | 64-bit |
| Solaris Operating System (SPARC 64-bit) | Solaris | 64-bit |
| HPUX PA-RISC(64-bit) | HPUNIX | 64-Bit |
| AIX | AIX | 64-bit |
| HP_IA64 | HPI | 64-bit |
| Linux x86-64 | Linux AMD | 64-bit |
| linux_ia64 | Linux Itanium | 64-bit |
| IBM Power Based Linux | Linux PPC | 64-bit |
| linux_zseries64 | zLinux | 64-bit |
| HP Tru64 UNIX | Decunix | 64-bit |
| Solaris Operating System (x86-64) | Solaris AMD64 | 64-bit |
| Solaris Operating System (x86) | Solaris AMD32 | 32-bit |

## 1.3 Procuring the Oracle Management Agent Software

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control, and therefore, its software is part of the Enterprise Manager Cloud Control software. When you install Enterprise Manager Cloud Control, the installation wizard automatically installs a Management Agent.

You can install additional Management Agents using the Add Host Targets Wizard built into the Enterprise Manager Cloud Control console (Cloud Control console). The wizard uses the Management Agent software that is already present in the OMS home.

However, note that the Management Agent software present in the OMS home is always for the version and platform on which that OMS is running. For example, if the OMS is Oracle Management Service 12*c* and it is running on Linux platform, then the Management Agent software available there is also for Linux platform.

If you want to install a Management Agent for a platform that is different from the one on which the OMS is running, then ensure that you download that software using the Self Update Console, which is built into the Cloud Control console.

For information on Self Update, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to download the software, see the chapter on updating Cloud Control in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

**Note:** The Management Agent software for 12*c* Release X (12.1.0.X) is not available on OTN, so the only way you can download the software is using the Self Update Console.

# 2

# Understanding the Basics

This chapter introduces you to some key concepts of Enterprise Manager Cloud Control, and describes some important aspects of installation that you must know before you proceed any further.

In particular, this chapter covers the following:

- Understanding the Basics of Enterprise Manager Cloud Control Installation
- Understanding the Oracle WebLogic Server Requirement for an Enterprise Manager Installation
- Understanding the Installation Directories
- Understanding the Configuration Assistants
- Understanding the Prerequisite Checks before Installing Enterprise Manager Cloud Control
- Understanding the Limitations of Enterprise Manager Cloud Control
- Understanding the Startup Scripts
- Understanding Other Miscellaneous Concepts

## 2.1 Understanding the Basics of Enterprise Manager Cloud Control Installation

This section describes the fundamental aspects of the installation process. In particular, this section covers the following:

- What are the Different Installation Modes Offered by Enterprise Manager Cloud Control?
- What Is an Enterprise Manager Cloud Control Installation Wizard?
- What Installation Types Are Offered by the Enterprise Manager Cloud Control Installation Wizard?
- What Is Oracle Configuration Manager?
- What Are the Enterprise Manager Cloud Control Software Updates?
- What is a Deployment Size for Enterprise Manager Cloud Control in an Advanced Configuration?
- What Is an Add Host Target Wizard?
- What Is a Plug-in?
- What Is an Add Management Service Deployment Procedure?

- What Ports Are Used for Installation?
- What Data Files Are Created While Configuring Oracle Management Repository?
- How Do You Delete the Data Files Created While Configuring Oracle Management Repository?
- Globalization Support for Enterprise Manager

### 2.1.1 What are the Different Installation Modes Offered by Enterprise Manager Cloud Control?

You can install Enterprise Manager Cloud Control or any of its core components either in an interactive, graphical mode or in a silent mode.

| | |
|---|---|
| **Graphical Mode** | Graphical mode is the Graphical User Interface (GUI) method that involves usage of a Java-based installation wizard or a browser-based application that is built into and accessed from the Enterprise Manager Cloud Control console. This method is best suited for first-time installations because you are guided through the entire installation process and your installation details are captured using the interview screens. |
| **Silent Mode** | Silent method involves usage of Oracle-supplied response files or scripts that capture all the information required for installation. This method is simpler and faster, but requires you to have some knowledge on the installation process so that you can provide your installation details in the response files without having to see the interview screens of the installation wizard. |

In both these modes, you can perform a *software-only* installation. A *Software-Only* installation is an approach that enables you to install only the software binaries of Enterprise Manager Cloud Control or a Management Agent, that is, without any configuration to the installation. This is best suited when you want to install the software at one point and configure it later.

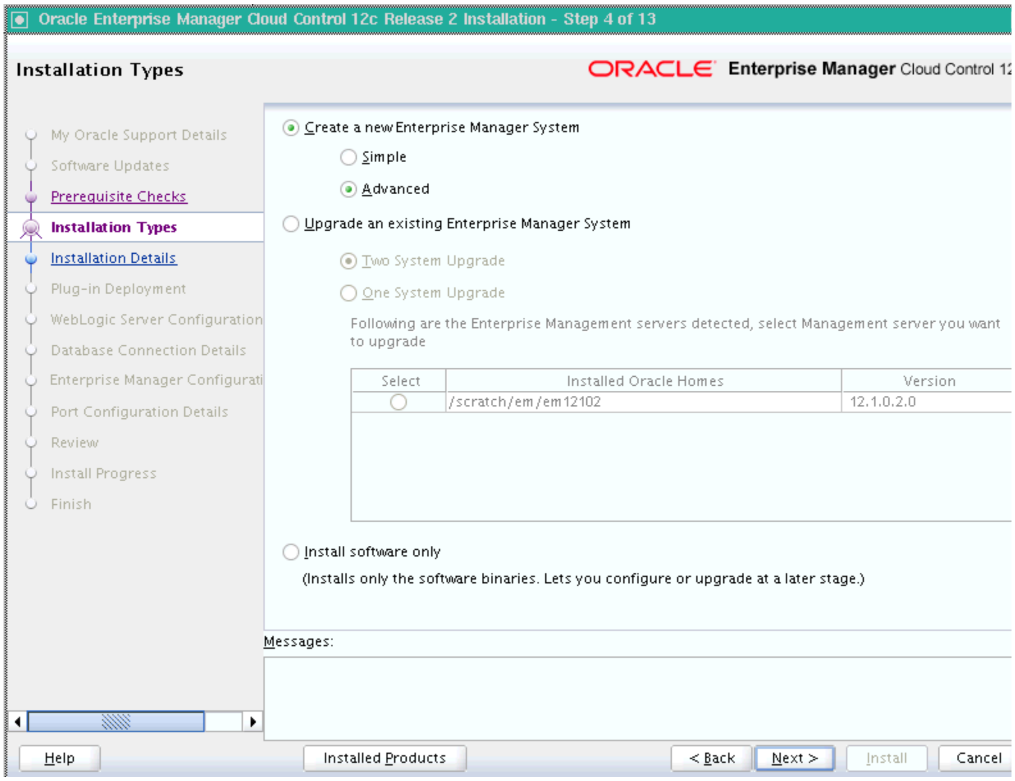
### 2.1.2 What Is an Enterprise Manager Cloud Control Installation Wizard?

Enterprise Manager Cloud Control Installation Wizard is a Java-based wizard that helps you install or upgrade to Enterprise Manager Cloud Control in graphical mode. If you are installing Enterprise Manager Cloud Control or any of its core components for the first time, then Oracle strongly recommends you to use this installation wizard.

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

Figure 2–1 describes the key elements of the installation wizard.

*Figure 2–1 Enterprise Manager Cloud Control Installation Wizard*



Oracle Enterprise Manager Cloud Control 12c Release 2 Installation - Step 4 of 13

Installation Types

ORACLE Enterprise Manager Cloud Control 12
My Oracle Support Details
Software Updates
Prerequisite Checks
Installation Types
Installation Details
Plug-in Deployment
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configurati
Port Configuration Details
Review
Install Progress
Finish

● Create a new Enterprise Manager System

○ Simple

● Advanced

○ Upgrade an existing Enterprise Manager System

● Two System Upgrade

○ One System Upgrade

Following are the Enterprise Management servers detected, select Management server you want to upgrade

| Select | Installed Oracle Homes | Version |
|---|---|---|
| ○ | /scratch/em/em12102 | 12.1.0.2.0 |

○ Install software only

(Installs only the software binaries. Lets you configure or upgrade at a later stage.)

Messages:

## 2.1.3 What Installation Types Are Offered by the Enterprise Manager Cloud Control Installation Wizard?

The Enterprise Manager Cloud Control Installation Wizard offers the following installation types:

- Create a New Enterprise Manager System
- Upgrade an Existing Enterprise Manager System
- Install Only the Software

### 2.1.3.1 Create a New Enterprise Manager System

This installation type enables you to install a new Enterprise Manager Cloud Control system with either simple or advanced configuration settings. For information about simple and advanced installation types, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

For information about what is installed for both simple and advanced installation types, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

> **Note:** If you want to install Enterprise Manager Cloud Control for evaluation or demo purposes, then use the *Simple* installation type.

### 2.1.3.2 Upgrade an Existing Enterprise Manager System

This installation type enables you to upgrade the following to Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5):

- Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4)]
- Enterprise Manager Cloud Control 12*c* Release 3 (12.1.0.3) [(12.1.0.3) or (12.1.0.3) Plug-in Update 1]
- Enterprise Manager Cloud Control 12*c* Release 2 (12.1.0.2) [(12.1.0.2) or (12.1.0.2) Plug-in Update 1]
- Enterprise Manager 11*g* Grid Control Release 1 (11.1.0.1)
- Enterprise Manager 10*g* Grid Control Release 5 (10.2.0.5)

For upgrading Enterprise Manager 10*g* Grid Control Release 5 (10.2.0.5) and Enterprise Manager 11*g* Grid Control Release 1 (11.1.0.1), you can select one of the following approaches. However, for upgrading Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4), 12*c* Release 3 (12.1.0.3), or 12*c* Release 2 (12.1.0.2), you can select only *One System Upgrade* approach.

- **One System Upgrade,** 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 Management Repository in the existing Oracle Database itself. Since the upgrade happens on the same host, there is a reasonable downtime involved.
- **Two System Upgrade,** 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 Oracle Database, but upgrades the one in the backed up database, thus offering the scope for 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.

> **Note:** For more information on these upgrade options, see the *Oracle Enterprise Manager Cloud Control Upgrade Guide.*

#### 2.1.3.3 Install Only the Software

This installation type enables you to install only the software binaries of Enterprise Manager Cloud Control at one point, and configure it at a later point.

This approach helps you divide the installation process into two phases, mainly the installation phase and the configuration phase. Understandably, the installation phase takes less time compared to the configuration phase because the installation phase involves only copying of binaries.

For information about what is installed during the installation phase and what is configured during the configuration phase, refer to Section 4.1.

### 2.1.4 What Is Oracle Configuration Manager?

With Enterprise Manager Cloud Control, you can choose to enable Oracle Configuration Manager. Alternatively, you can enable it after installing Enterprise Manager Cloud Control.

Oracle Configuration Manager automatically collects configuration information from your environment at regular intervals and uploads it to Oracle repository. This helps Oracle maintain up-to-date information about your environment, identify security vulnerabilities, quickly diagnose support issues, and offer better solutions consistently.

**However, no business or personal information is collected and uploaded, except for local contact name in the event of transmission problems. Oracle guarantees that all the information collected will be kept strictly confidential and under no circumstances will this information be shared with any other party**.

Oracle recommends that the host from where you are running the installation wizard have a connection to the Internet so that the configuration information can be automatically collected and uploaded to My Oracle Support.

If the host from where you are running the installation wizard has a connection to the Internet, then on the My Oracle Support Details screen of the installation wizard, enter the My Oracle Support user name (or e-mail address) and password.

Otherwise, 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. To understand how the configuration information can be manually collected and uploaded, see the steps outlined in Section 2.1.4.1.

If you want to enable it after installing Enterprise Manager Cloud Control, then see Section 2.1.4.2.

#### 2.1.4.1 Manually Collecting and Uploading the Configuration Information

To manually collect the configuration information, follow these steps:

1. Navigate to the OMS home and run the following command:

   ```
   $<OMS_HOME>/ccr/bin/emCCR collect
   ```

   For Oracle Configuration Manager 10.2.7 and higher, the collected configuration information is stored in the `/ccr/hosts/state/upload/ocmconfig.jar` file. For lower versions of Oracle Configuration Manager, the collected configuration information is stored in the `/ccr/state/upload/ocmconfig.jar` file. When you run the same command next time, the ocmconfig.jar file gets overwritten with fresh data. Therefore, at any point, you will see only one ocmconfig.jar file.

2. Upload the `ocmconfig.jar` file to a Service Request on My Oracle Support.

3. Repeat Step (1) and Step (2) from the Management Agent home.

#### 2.1.4.2 Enabling Oracle Configuration Manager After Installing Enterprise Manager Cloud Control

To enable Oracle Configuration Manager at a later point, do the following:

1. Set the environment variable `ORACLE_CONFIG_HOME` to the Oracle Management Service instance base directory. Oracle Management Service instance base is the directory where the configuration files of the OMS are created.

   – 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>
     ```

   **Note:** For information about Oracle Management Service instance base directory, refer to Section 2.3.3.

2. From the OMS home, run the following command:

```
$<OMS_HOME>/ccr/bin/setupCCR
```

## 2.1.5 What Are the Enterprise Manager Cloud Control Software Updates?

This section describes the following:

- What Is a Software Update?
- How Does the Software Update Feature Work?
- What Types of Software Updates Are Downloaded and Applied?
- How Can I Find Out What Bugs Have Been Fixed by the Software Updates?
- Are the Software Updates Applied Automatically Even for Databases That Have Oracle Management Repository Preconfigured?
- How Can You Download the Software Updates?
- Can I Download and Apply These Patches After Installation or Upgrade?
- How Can You Identify What Patches Have Been Applied?

### 2.1.5.1 What Is a Software Update?

Software Update is a feature built in to the Enterprise Manager Cloud Control Installation Wizard. The feature appears as the Software Updates screen in the installer, and enables you to automatically download and deploy the latest recommended patches while installing or upgrading Enterprise Manager Cloud Control.

This way, you do not have to keep a manual check on the patches released by Oracle. All patches required by the installer for successful installation and upgrade are automatically detected and downloaded from My Oracle Support, and applied during the installation or upgrade, thus reducing the known issues and potential failures.

> **Note:** The patches available via the Software Updates screen must be downloaded only via the Software Updates screen, and not from My Oracle Support.

### 2.1.5.2 How Does the Software Update Feature Work?

The Software Update feature connects to My Oracle Support and first downloads a patch, that consists of a file called `patch.xml`. The installer parses the `patch.xml file`, and creates a directory titled `updates` to download all the required updates. The `updates` directory has the following subdirectories:

- `updates/agent`

  Contains patches related only to the central agent (Management Agent installed with the OMS).

- `updates/oms`

  Contains patches related to the OMS.

- `updates/metadata`

  Contains a subdirectory, inside which you will find the `patch.xml` that determines what all updates must be downloaded and on which Oracle home they must be applied.

> **Note:** All software updates must be downloaded and applied only via the Software Updates screen in the Installer , and not from My Oracle Support.

#### 2.1.5.3 What Types of Software Updates Are Downloaded and Applied?

The following are the different types of updates that can be applied using this feature:

- OUI/Opatch Updates

  Includes the latest OUI/Opatch versions or their updates. If a new version of the installer is downloaded, then OUI is restarted and launched from the location where the latest version is downloaded.

- Prerequisite Updates

  Includes new prerequisite check-related updates released in response to issues reported after a release of Enterprise Manager Cloud Control. This enables OUI to always run the latests set of prerequisite checks, thus resulting in a smoother installation or upgrade experience.

- EM installer Updates

  Includes updates that fix OUI issues—essentially, Java code changes that most likely results in automatic restart of OUI after their application.

- Interim Patch Updates

  Includes patches such as DST patches, performance-related patches, and so on. They are automatically detected, downloaded, and applied.

- Patch Set Updates

  Includes multiple patch updates that fix bugs, enhance existing features, and also sometimes introduce new features.

#### 2.1.5.4 How Can I Find Out What Bugs Have Been Fixed by the Software Updates?

To know what bugs or issues have been fixed by the software updates downloaded via the Software Updates screen, refer to My Oracle Support note 1099123.1.

#### 2.1.5.5 Are the Software Updates Applied Automatically Even for Databases That Have Oracle Management Repository Preconfigured?

During installation, you are prompted for the details of a database where Oracle Management Repository can be configured. If you plan to provide the details of a database that already has an Oracle Management Repository preconfigured using the database templates offered by Oracle, then the selected software updates are not automatically applied. In such a case, you must manually download and apply the software updates on the database after the installation.

#### 2.1.5.6 How Can You Download the Software Updates?

You can download the software updates in one of the following ways:

- **Download by User (Offline Mode):** Use this option when you do not have Internet connectivity on the host where you are installing Enterprise Manager, to connect to My Oracle Support.

  To download the software updates, follow these steps:

**Caution:** **Make sure you download and apply the software updates only using the installer. DO NOT directly download them from My Oracle Support.**

1. On a host that has Internet connectivity, invoke the Enterprise Manager Cloud Control Installation Wizard with the `-downloadUpdates` argument in the following way. This argument ensures that the installation wizard is invoked only for downloading the software updates. **Make sure you run this command only from the downloaded Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) software location, and NOT from the existing OMS home or database home.**

   ```
   <EM_12.1.0.5_Software_Extracted_Location/Disk1>./runInstaller
   -downloadUpdates
   ```

   **Note:**

   - On Microsoft Windows, run `setup.exe -downloadUpdates.`
   - Make sure you download these updates on another host (with Internet connectivity) that runs on the same operating system as the host on which you want to invoke the installer and install the product. For example, if you want to install on Linux, them make sure the host with Internet connectivity on which you are downloading these updates also runs on Linux. Similarly, if you want to install on Microsoft Windows, make sure you download the patches on another host that runs on Microsoft Windows.

   Enterprise Manager Cloud Control Installation Wizard appears with only two screens, the titles of which appear on the left menu.

2. On the Software Updates screen, enter the *My Oracle Support* account user name and password, and click **Search for Updates**. The installation wizard displays the *Downloading Updates* dialog, and downloads the software updates to `/tmp/OraInstall<timestamp>/updates.` Click **Next.**

   The installation wizard restarts itself, and this time, displays all the screens, the titles of which appear on the left menu. Exit the installation wizard because you have invoked it on this host only to download the software updates, and not install the OMS.

3. Copy the entire `updates` directory to the host where you want to install the OMS.

   **Note:** Make sure the host from where you are copying the directory and the host on which you are copying the directory run on the same operating system. For example, if you downloaded the updates to the directory on Linux host, then make sure you copy it to another Linux host where want to install the product. Copying the directory across operating systems is not recommended for the installation.

4. On the host where you want to install the OMS, invoke the installation wizard.

   – **In Graphical Mode:** On the Software Updates screen of the installation wizard, select **Search for Updates**, and then, select **Local Directory**. Enter the location where you copied the updates, and click **Search for Updates**. To search the computer and select the location, click **Browse**.

For example, if you copied the entire `updates` directory to `/u01/home/em/`, then select or enter `/u01/home/em/updates`.

Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch. Otherwise, click **Next.** The installer automatically applies all the patches while installing or upgrading the Enterprise Manager system.

– **In Silent Mode:** Invoke the installer passing the response file with the `INSTALL_UPDATES_SELECTION` parameter set to `"staged"`, and the `STAGE_LOCATION` parameter set to the absolute path of the location where the updates are available.

> **Note:** If you have a proxy server set up, then invoke the installation wizard passing the `-showProxy` argument. For example, if you are invoking in graphical mode, then invoke in the following way:
>
> ```
> <Software_Location>/runInstaller -showProxy
> ```

- **Automatic Download by Installation Wizard (Online Mode):** Use this option when you have Internet connectivity to connect to My Oracle Support automatically using the Enterprise Manager Cloud Control Installation Wizard.

  On a host that has Internet connectivity, invoke the Enterprise Manager Cloud Control Installation Wizard.

  - **In Graphical Mode:** On the Software Updates screen of the installation wizard, select **Search for Updates**, then select **My Oracle Support**. 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. Otherwise, click **Next.** The installer automatically applies all the patches while installing or upgrading the Enterprise Manager system.

  - **In Silent Mode:** Invoke the installer passing the response file with the `INSTALL_UPDATES_SELECTION` parameter set to `"download"`, and the `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and the `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES` parameters set to your *My Oracle Support* credentials.

#### 2.1.5.7 Can I Download and Apply These Patches After Installation or Upgrade?

Ideally, you must download and apply the software updates only at the time of installing or upgrading the Enterprise Manager system. The software updates fix issues with the installation or upgrade process, and therefore, they are necessary at the time of installing or upgrading the Enterprise Manager system.

The only exception is when you provide the details of a database that already has an Oracle Management Repository preconfiguring using the database templates offered by Oracle. In such a case, you must manually download and apply the updates on the database after the installation.

#### 2.1.5.8 How Can You Identify What Patches Have Been Applied?

To identify what patches have been applied, run the following command from the OMS home or the Management Agent home. The output of this command lists all the applied patches.

```
<ORACLE_HOME>/OPatch/opatch lsinventory
```

### 2.1.6 What is a Deployment Size for Enterprise Manager Cloud Control in an Advanced Configuration?

When you install Enterprise Manager Cloud Control with advanced configuration settings (*Advanced* installation type), you have an option of selecting the deployment size of your choice. This option is available in both graphical mode (Enterprise Manager Cloud Control Installation Wizard) and silent mode (response file).

The deployment size essentially indicates the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.

Table 2–1 describes each deployment size.

***Table 2–1 Deployment Size***

| Deployment Size | Targets Count | Management Agents Count | Concurrent User Session Count |
|---|---|---|---|
| Small | Up to 999 | Up to 99 | Up to 10 |
| Medium | Between 1000 and 9999 | Between 100 and 999 | Between 10 and 24 |
| Large | 10,000 or more | 1000 or more | Between 25 and 50 |

**Note:** If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you select on this screen matches with the deployment size for which you ran the SQL script as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. Otherwise, you will see errors.

If you want to select a deployment size different from the deployment size for which you ran the SQL script earlier, then do one of the following:

- Minimize the installer, run the SQL script intended for the deployment size you want to select, then return to this screen and select the desired deployment size. To understand the SQL script to be run for each deployment size, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- Select the deployment size of your choice on this screen, and click **Next.** When you see errors, manually fix the parameters in the database, then return to this screen to continue with the installation.

The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make. For more information about these deployment sizes, and the database parameters set for each of them, refer to Chapter 11.

After installing Enterprise Manager Cloud Control with a particular deployment size, you can choose to increase or decrease the count of targets, Management Agents, or concurrent user sessions. However, if you do increase the count to a level that is not appropriate for the selected deployment size, then the performance might suffer. Under such circumstances, Oracle recommends you to modify the database parameters according to the desired deployment size, as described in Chapter 11.

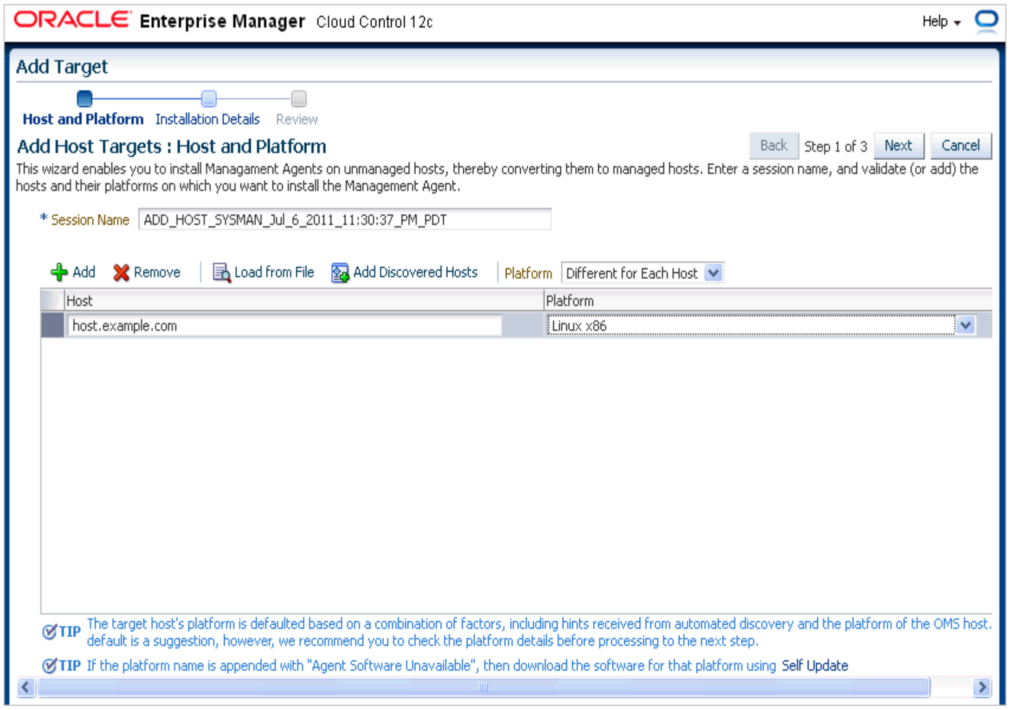
### 2.1.7 What Is an Add Host Target Wizard?

The Add Host Targets Wizard (Figure 2–2) is a GUI-rich application accessible from within the Cloud Control console, and used for installing Management Agents on unmanaged hosts and converting them to managed hosts in the Enterprise Manager system.

Using the Add Host Targets Wizard, you can do the following:

- Install a fresh Management Agent
- Clone an existing well-tested, pre-patched, and running Management Agent
- Install a Management Agent from an existing, centrally shared Management Agent

*Figure 2–2 Add Host Target Wizard*



Add Host Targets : Host and Platform

This wizard enables you to install Managament Agents on unmanaged hosts, thereby converting them to managed hosts. Enter a session name, and validate (or add) the hosts and their platforms on which you want to install the Management Agent.

* Session Name: ADD_HOST_SYSMAN_Jul_6_2011_11:30:37_PM_PDT

Platform: Different for Each Host

| Host | Platform |
|---|---|
| host.example.com | Linux x86 |

TIP The target host's platform is defaulted based on a combination of factors, including hints received from automated discovery and the platform of the OMS host. default is a suggestion, however, we recommend you to check the platform details before processing to the next step.

TIP If the platform name is appended with "Agent Software Unavailable", then download the software for that platform using Self Update

Although the Add Host Targets Wizard can be used for remotely installing one Management Agent, the wizard is best suited for mass-deployment of Management Agents, particularly while mass-deploying Management Agents of different releases on hosts of different platforms. The wizard gives you the flexibility to select hosts on which you want to install a Management Agent. This helps you when you want to install the Management Agent on several hosts, in one attempt.

### 2.1.8 What Is a Plug-in?

Plug-ins are modules that can be plugged into an existing Enterprise Manager Cloud Control deployment to extend target management or other vertical functionality in Enterprise Manager.

At a high level, plug-ins contain archives for monitoring and discovering OMS instances and Management Agents. The archives contain Java and SQL codes, and metadata.

For more information, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

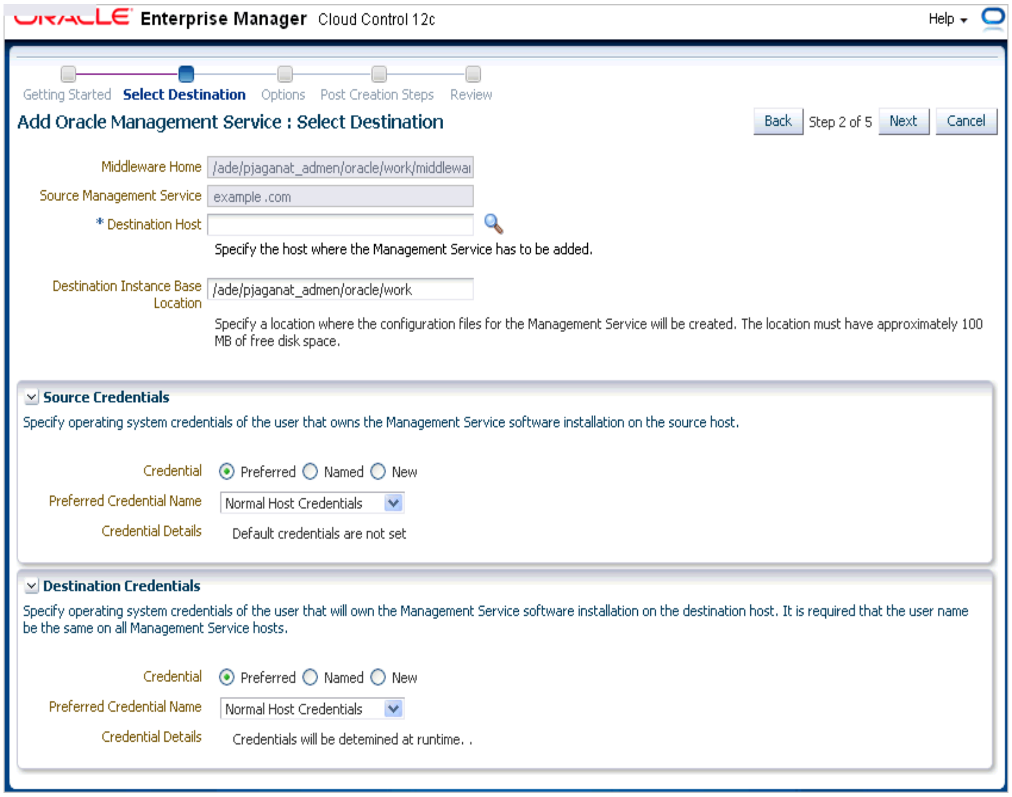
### 2.1.9 What Is an Add Management Service Deployment Procedure?

A deployment procedure is a procedure that contains a hierarchal sequence of provisioning or patching steps, where each step may contain a sequence of other steps. In other words, the workflow of all tasks that need to be performed for a particular life cycle management activity is encapsulated in a deployment procedure.

Enterprise Manager Cloud Control offers deployment procedures, and all of these can be accessed from within the Cloud Control console. One of the deployment procedures that falls within the context of Enterprise Manager Cloud Control installation is the Add Management Service deployment procedure.

The Add Management Service deployment procedure (Figure 2–3) helps you meet high-availability requirements by enabling you to install an additional OMS using an existing OMS that is running on an AdminServer host.

***Figure 2–3 Add Management Service Deployment Procedure***



Add Oracle Management Service : Select Destination

Middleware Home: /ade/pjaganat_admen/oracle/work/middlewai

Source Management Service: example .com

* Destination Host:

Specify the host where the Management Service has to be added.

Destination Instance Base Location: /ade/pjaganat_admen/oracle/work

Specify a location where the configuration files for the Management Service will be created. The location must have approximately 100 MB of free disk space.

**Source Credentials**

Specify operating system credentials of the user that owns the Management Service software installation on the source host.

Credential: ● Preferred ○ Named ○ New

Preferred Credential Name: Normal Host Credentials

Credential Details: Default credentials are not set

**Destination Credentials**

Specify operating system credentials of the user that will own the Management Service software installation on the destination host. It is required that the user name be the same on all Management Service hosts.

Credential: ● Preferred ○ Named ○ New

Preferred Credential Name: Normal Host Credentials

Credential Details: Credentials will be detemined at runtime. .

In simple words, the Add Management Service deployment procedure enables you to install additional OMS instances in your environment. The deployment procedure clones an existing OMS and replicates its configuration to the destination host.

The earlier releases of Enterprise Manager offered this installation type from the Enterprise Manager Installation Wizard. However, for the Enterprise Manager Cloud Control release, this installation type is offered as a deployment procedure.

For more information about the deployment procedure, see the chapter on adding additional management service in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 2.1.10 What Ports Are Used for Installation?

This section describes the default ports that are honored while installing Enterprise Manager Cloud Control. In particular, this section covers the following:

- What Default Ports Are Used for Enterprise Manager Cloud Control Installation?
- How Can You Check Whether a Port Is Free?
- How Can You Customize the Ports During and After Installing Enterprise Manager Cloud Control?
- What Precautions You Must Take While Customizing the Enterprise Manager Cloud Control Ports?

### 2.1.10.1 What Default Ports Are Used for Enterprise Manager Cloud Control Installation?

The following are the default ports used for installation:

- **Enterprise Manager Cloud Control**

| | Upload Port | Console Port |
|---|---|---|
| **HTTP Port** | 4889<br>If 4889 is not available, then the first available free port from the range 4889 to 4898 is selected. | The first available free port from the range 7788 - 7798 is selected. |
| **HTTPS Port** | 1159<br>If 1159 is not available, then the first available free port from the range 4899 to 4908 is selected. | The first available free port from the range 7799 - 7809 is selected. |

- **Oracle Management Agent**

  The default upload port for Management Agent is 3872. The same port is used for both HTTP and HTTPS. If 3872 is not available, then the first available free port from the range 1830 to 1849 is selected.

- **Administration Server**

  The default HTTP port for Administration Server is 7001.

  The default HTTPS port for Admin Server is 7101. If 7101 is not available, then the first available free port from the range 7101 to 7200 is selected.

- **Node Manager**

  The default HTTPS port for Node Manager is 7401. If 7401 is not available, then the first available free port from the range 7401 to 7500 is selected.

- **Managed Server**

  The default HTTP port for Managed Server is 7201. If 7201 is not available, then the first available free port from the range 7201 to 7300 is selected.

  The default HTTPS port for Managed Server is 7301. If 7301 is not available, then the first available free port from the range 7301 to 7400 is selected.

- **Oracle Management Repository**

  The default port for Oracle Management Repository is 1521.

- **JVM Diagnostics Managed Server**

  The default HTTP port for JVM Diagnostics Managed Server is 3800.

  The default HTTPS port for JVM Diagnostics Managed Server is 3801.

- **Application Dependency and Performance RMI Registry**

  The default port for Application Dependency and Performance RMI Registry is 51099.

- **Application Dependency and Performance Java Provider**

  The default port for Application Dependency and Performance Java Provider is 5503.

- **Application Dependency and Performance Remote Service Controller**

  The default port for Application Dependency and Performance Remote Service Controller is 55000.

- **Real User Experience Insight**

  The default HTTPS port for Real User Experience Insight is 443.

- **Oracle BI Publisher**

  The default HTTP port for Oracle BI Publisher is 9701. If 9701 is not available, then the first available free port from the range 9701 to 9800 is selected.

  The default HTTPS port for Oracle BI Publisher is 9801. If 9801 is not available, then the first available free port from the range 9701 to 9900 is selected.

  > **Note:** Although Oracle BI Publisher 11g (11.1.1.7) is installed by default, it is not configured. To configure it post installation, follow the instructions in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

#### 2.1.10.2 How Can You Check Whether a Port Is Free?

To check whether a port is free, run the following command:

- On Unix:

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

- On Microsoft Windows:

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

#### 2.1.10.3 How Can You Customize the Ports During and After Installing Enterprise Manager Cloud Control?

Enterprise Manager Cloud Control offers you the flexibility to use custom ports instead of default ports.

**Customizing the Ports While Installing Enterprise Manager Cloud Control**

> **WARNING: Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.**

- If you are installing Enterprise Manager Cloud Control (advanced installation) in graphical mode, that is, using the Enterprise Manager Cloud Control Installation Wizard, then you can use the Port Configuration Details screen to enter custom ports. You can also import a `staticports.ini` file that already captures the custom ports.t
- If you are installing Enterprise Manager Cloud Control in silent mode, that is, using the installation procedures described in Part II, then update the `staticports.ini` file with suitable custom ports.

  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
  ```

**Customizing the HTTP/HTTPS Console and the Upload Ports After Installing Enterprise Manager Cloud Control**

> **WARNING: Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.**

If you want to change the HTTP/HTTPS console ports and upload ports after installing Enterprise Manager Cloud Control, then follow these steps:

1. Stop the OMS:

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

2. Update the emoms properties with HTTP and HTTPS ports as described in Table 2–2. Specify the values for parameters `<http_upload_new>, <https_upload_new>, <http_console_new>`, and `<https_console_new>`):

*Table 2–2 Updating EMOMS Properties with HTTP and HTTPS Ports*

| Port/Property Type | Command to Run |
|---|---|
| HTTP Upload Port | `<OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerPort -value <http_upload_new>` |
| HTTPS Upload Port | `<OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort -value <https_upload_new>` |

*Table 2–2 (Cont.) Updating EMOMS Properties with HTTP and HTTPS Ports*

| Port/Property Type | Command to Run |
|---|---|
| HTTP Console Port | `<OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerPort -value <http_console_new>` |
| HTTPS Console Port | `<OMS_Home>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerHTTPSPort -value <https_console_new>` |

3. Back up the following file:

   ```
   $<OMS_INSTANCE_HOME>/emgc.properties
   ```

   After backing up the file, open the original `emgc.properties` file, and specify the new port numbers for the following parameters:

   ```
   EM_UPLOAD_HTTP_PORT=<http_upload_new>
   EM_UPLOAD_HTTPS_PORT=<https_upload_new>
   EM_CONSOLE_HTTP_PORT=<http_console_new>
   EM_CONSOLE_HTTPS_PORT=<https_console_new>
   ```

4. Back up the files `httpd.conf`, `ssl.conf`, and `httpd_em.conf` from the following location:

   ```
   $<WEBTIER_INSTANCE_HOME>/config/OHS/ohs#/
   ```

   After backing up the files, open the original files, and specify the new port numbers:

   - In `httpd.conf` file, in the **Listen** directive section, replace `<http_console_orig>` with `<http_console_new>`.
   - In `ssl.conf` file, in the **Listen** and **Virtual Host** directive sections, replace `<https_console_orig>` with `<https_console_new>`.
   - In `httpd_em.conf` file, in the **Listen and VirtualHost** directive section, replace `<http_upload_orig>` with `<http_upload_new>`, and `<https_upload_orig>` with `<https_upload_new>`, respectively.

5. Start the OMS, and verify its status:

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

   ```
   $<OMS_HOME>/bin/emctl status oms -details
   ```

6. If the OMS is configured with any Server Load Balance (SLB), then update the ports in the SLB pools, monitors, and so on.

7. If the OMS is configured for SSO or OAM, then re-run the SSO or OAM configuration.

8. Back up the following file:

   ```
   $<AGENT_INSTANCE_HOME>/sysman/config/emd.properties
   ```

   > **Note:** Back up the `emd.properties` file from all Management Agents that are communicating with the OMS.

   After backing up the file, open the original `emd.properties` file, and verify the URL mentioned in `REPOSITORY_URL`. If the URL is an HTTPS URL, then change the port number to `<https_upload_new>`. If the URL is an HTTP URL, then change the port number to `<http_upload_new>`.

9. If there are any EM CLI instances set up on the ports you have changed, then set up those instances again. To do so, from each EM CLI instance, run the command `emcli setup` or `emcli status,` and note the EM URL that appears.

   If you have changed that port number, run the following command:

   ```
   emcli setup -url=http(s)://<host>:<new_port#>/em -dir=<dir>....
   ```

10. After changing the console port, you must update the URL for the EM Console Service with the new port number. However, you can skip this step if the URL is that of an SLB and not of an OMS.

    a. From the **Targets** menu, select **All Targets.**

    b. In the **Search Target Name** text box, enter **EM Console Service,** and click the search icon.

    c. In the search results table, click **EM Console Service.**

    d. On the EM Console Service page, from the **EM Service** menu, select **Administration,** then select **Service Tests and Beacons.**

    e. On the Service Tests and Beacons page, in the Service Tests table, select **EM Console Service Test,** and click **Edit.**

    f. On the Edit Service Test: EM Console Service Test page, in the Transaction section, in the Steps table, select **Access Login Page.**

    g. On the Edit Step: Access Login page, in the Request section, in the **URL** text box, change the port in the URL.

    h. Click **Continue.**

    i. Click **OK.**

    j. On the Security Configuration page, click **Yes.**

#### 2.1.10.4 What Precautions You Must Take While Customizing the Enterprise Manager Cloud Control Ports?

While updating the `staticports.ini` file, you must be extremely careful because an error in the file can cause the installation wizard to use default ports without displaying any warning. Therefore, before updating the `staticports.ini` file, check for these points:

- Do NOT set any port to a value lower than or equal to 1024. Ports up to 1024 are typically reserved for root users (super users). Therefore, make sure the port you customize is always set to a value greater than 1024.

- If a port is already being used by a component or any other application, do not enter that port (used port) in the `staticports.ini` file. If you do, then the related configuration assistant also fails.

- If you have entered the same port for more than one component, then the installation displays an error after the prerequisite checks phase. You must rectify this error before proceeding with the installation.

- If you have syntax errors in the `staticports.ini` file (for example, if you omitted the equal (=) character for a line), then the installation wizard ignores the line. For the components specified on such lines, the installation wizard assigns the default ports. The installation wizard does not display a warning for lines with syntax errors.

- If you misspell a component name, then the installation wizard assigns the default port for the component. Names of components in the file are case-sensitive. The installation wizard does not display a warning for lines with unrecognized names.
- If you enter a nonnumeric value for the port number, then the installation wizard ignores the line and assigns the default port number for the component. It does this without displaying any warning.
- If you misspell the parameter on the command line, then the installation wizard does not display a warning. It continues and assigns default ports to all components.
- If you enter a relative path to the `staticports.ini` file (for example, `./staticports.ini`) in the command line, then the installation wizard does not find the file. It continues without displaying a warning and it assigns default ports to all components. You must enter a full path to the `staticports.ini` file.

### 2.1.11 What Data Files Are Created While Configuring Oracle Management Repository?

The following are the data files created while configuring Oracle Management Repository:

| | |
|---|---|
| `mgmt.dbf` | Stores information about the monitored targets, their metrics, and so on. |
| `mgmt_ecm_depot1.dbf` | Stores configuration information collected from the monitored targets. |
| `mgmt_deepdive.dbf` | Stores monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP). |

### 2.1.12 How Do You Delete the Data Files Created While Configuring Oracle Management Repository?

To delete the data files, you must drop the SYSMAN/MDS schema. To do so, run the following command from the OMS home.

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host>
<repository_database_port> <repository_database_sid> -action drop -dbUser
<repository_database_user> -dbPassword <repository_database_password>
-dbRole <repository_database_user_role> -mwHome <middleware_home>
-mwOraHome <oms_home> -oracleHome <oms_home>
```

**Note:**

- For Microsoft Windows, invoke `RepManager.bat`.
- If you are dropping the schemas that belong to a 10*g* Release 2 (10.2.x.x) Management Repository, then run the command without these arguments:

  ```
  -mwHome <middleware_home> -mwOraHome <middleware_ora_
  home> -oracleHome <OMS_HOME>
  ```

After dropping the schema, manually delete the database files `mgmt.dbf` and `mgmt_ecm_depot1.dbf`.

You can find these files by running the following command as SYS:

```
SELECT FILE_NAME FROM DBA_DATA_FILES WHERE UPPER (TABLESPACE_NAME) LIKE
'MGMT%';
```

Table 2–3 describes the `-action` options that are supported by the different versions of RepManager.

***Table 2–3 RepManager Support for -action dropall and -action drop Commands***

| RepManager Version | Command Supported |
|---|---|
| 12*c* Release 5 (12.1.0.5), 12*c* Release 4 (12.1.0.4) | `-action drop`<br>The command drops SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, SYSMAN_RO, and SYSMAN_BIPLATFORM. |
| 12*c* Release 1 (12.1.0.1) , 12*c* Release 2 (12.1.0.2), and 12*c* Release 3 (12.1.0.3) | ■ `-action dropall`<br>■ `-action drop`<br>The commands drop SYSMAN, SYSMAN_MDS, SYSMAN_APM, SYSMAN_OPSS, and SYSMAN_RO. |
| 11*g* Release 1 (11.1.0.1) | ■ `-action dropall`<br>The command drops only SYSMAN and SYSMAN_MDS.<br>■ `-action drop`<br>The command drops only SYSMAN. |
| 10g Release 5(10.2.0.5) | `-action drop`<br>The command drops only SYSMAN. |

### 2.1.13 Globalization Support for Enterprise Manager

Enterprise Manager Cloud Control is translated to the following languages:

- Brazilian Portuguese
- Chinese (Simplified and Traditional)
- French
- German
- Italian
- Japanese
- Korean
- Spanish

The preferred language set in your Web browser is the language that is used in the Enterprise Manager Cloud Control Console.

The language or the locale set on the operating system is the language used in the Enterprise Manager Cloud Control Installation Wizard.

## 2.2 Understanding the Oracle WebLogic Server Requirement for an Enterprise Manager Installation

Enterprise Manager Cloud Control requires Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.

If Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing a new Enterprise Manager Cloud Control.

This section describes some important aspects related to Oracle WebLogic Server that you must know before you install Enterprise Manager Cloud Control.

In particular, this section covers the following:

- How Do I Verify Whether Oracle WebLogic Server Is Installed?
- Is Oracle WebLogic Server Cluster Supported?
- If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?
- When and Why Do You Need the Oracle WebLogic Server Credentials?
- When and Why Do You Need the Node Manager Credentials?
- How Do You Find Admin Server Port After Installing Enterprise Manager?
- How Do You Verify Whether Admin Server Is Running?
- How Do You Start the Admin Server?

## 2.2.1 How Do I Verify Whether Oracle WebLogic Server Is Installed?

To verify whether Oracle WebLogic Server is installed, check the following file in the Oracle Middleware home:

```
$<MW_HOME>/logs/log.txt
```

The following is the sample output of the `log.txt` file:

```
release 10.3.6.0 [Added]
    |_____Common Infrastructure Engineering 7.1.0.0 [Added]
    |     |_____Uninstall [Added]
    |     |_____Patch Client [Added]
    |     |_____Patch Attachment Facility [Added]
    |     |_____Clone Facility [Added]
    |_____WebLogic Server 10.3.6.0 [Added]
    |     |_____Core Application Server [Added]
    |     |_____Administration Console [Added]
    |     |_____Configuration Wizard and Upgrade Framework [Added]
    |     |_____Web 2.0 HTTP Pub-Sub Server [Added]
    |     |_____WebLogic SCA [Added]
    |     |_____WebLogic JDBC Drivers [Added]
    |     |_____Third Party JDBC Drivers [Added]
    |     |_____WebLogic Server Clients [Added]
    |     |_____WebLogic Web Server Plugins [Added]
    |     |_____UDDI and Xquery Support [Added]
    |     |_____Server Examples [Added]
    |     |_____Evaluation Database [Added]
    |     |_____Workshop Code Completion Support [Added]
    |_____Oracle Configuration Manager 10.3.3.1 [Added]
    |     |_____Data Collector [Added]
    |_____Oracle Coherence 3.6.0.3 [Not Installed]
          |_____Coherence Product Files [Not Installed]
          |_____Coherence Examples [Not Installed]
```

## 2.2.2 Is Oracle WebLogic Server Cluster Supported?

Oracle WebLogic Server cluster consists of Oracle WebLogic Servers running simultaneously and working together to provide increased scalability and reliability. A cluster appears to be a single Oracle WebLogic Server instance. The server instances that constitute a cluster can run on the same host, or be located on different hosts.

You can install Enterprise Manager Cloud Control on an Oracle WebLogic Server Cluster, however, you cannot take advantage of the cluster configurations.

### 2.2.3 If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?

If Oracle WebLogic Server already exists, then the existing domain is NOT used. Instead, the Enterprise Manager Cloud Control Installation Wizard creates a new domain and deploys the Enterprise Manager Cloud Control software to it.

### 2.2.4 When and Why Do You Need the Oracle WebLogic Server Credentials?

While installing or upgrading to Enterprise Manager Cloud Control, you are prompted to enter the Oracle WebLogic Server credentials (user name and password). The credentials are used for creating the WebLogic domain and other associated components such as the Admin Server, the managed server, and the node manager.

The WebLogic user name is the default user name that will be used as the administrative user for the WebLogic Domain. By default, the user name is `weblogic`. And the WebLogic password is the password for this default administrative user account.

### 2.2.5 When and Why Do You Need the Node Manager Credentials?

While installing or upgrading to Enterprise Manager Cloud Control, you are prompted to enter the Node Manager password for the default Node Manager user account, which is `nodemanager`. The password is used for configuring 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.

**Note:** On Microsoft Windows, a Node Manager service is NOT created. This is an expected behavior.

### 2.2.6 How Do You Find Admin Server Port After Installing Enterprise Manager?

To find the Admin Server port, view the value set for the `AS_HTTPS_PORT` parameter in the `emgc.properties` file. This file is available in the Oracle Management Service Instance Base location.

For example,

```
/DATA/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

### 2.2.7 How Do You Verify Whether Admin Server Is Running?

To install an additional OMS, the Admin Server that is used by the first OMS must be up and running. To verify whether the Admin Server is running, access the Admin Server console using the following URL:

```
https://host:port/console
```

Here, host and port are values specified in the `EM_INSTANCE_HOST` and `AS_HTTPS_PORT` parameters, respectively, in the `emgc.properties` file. This properties file is available in the Oracle Management Service Instance Base location of the first OMS.

For example,

```
/DATA/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

### 2.2.8 How Do You Start the Admin Server?

You can start the Admin Server by running the following command. Although the command is used essentially to start the OMS, the command in turn starts the Admin Server on which that OMS is running. So run this command even if you know that the OMS is already running.

```
emctl start oms
```

## 2.3 Understanding the Installation Directories

This section describes the installation directories that need to be entered while installing Enterprise Manager Cloud Control or any of its core components. In particular, this section covers the following:

- What Is an Oracle Inventory Directory?
- What Is an Oracle Middleware Home?
- What Is an Oracle Management Service Instance Base Location?
- What Is an Oracle Home?
- What Is an Agent Base Directory?
- What is an Agent Instance Directory?
- What Is a /TMP or C:\Temp Directory Used For?

### 2.3.1 What Is an Oracle Inventory Directory?

If Enterprise Manager Cloud Control is the first Oracle product that you are installing, then the Enterprise Manager Cloud Control Installation Wizard prompts you to enter an inventory directory (also called the *oraInventory* directory).

This inventory directory is used by the installation wizard to place all the installer files and directories on the host. The installation wizard automatically sets up subdirectories for each Oracle product to contain the inventory data.

You can enter the *oraInventory* directory in two ways:

- While installing Enterprise Manager Cloud Control using the installation wizard, you can enter the *oraInventory* directory in the Oracle Inventory screen. When you enter it in this screen, you must also select the appropriate operating system group name that will own the *oraInventory* directories. The group you select must have write permission on the *oraInventory* directories.

- While installing Enterprise Manager Cloud Control in silent mode, that is, without using the installation wizard, you can enter the *oraInventory* directory using the `-invPtrLoc` parameter. This parameter considers the path to a location where the inventory pointer file (`oraInst.loc`) is available. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

  For example

  ```
  ./runInstaller -invPtrLoc /scratch/OracleHomes/oraInst.loc
  ```

**Note:**

- For a typical non-HA environment, the Central Inventory (oraInventory) can be in a shared or non-shared location. If you use a shared location, then ensure that only one shared location is maintained per host, and no two hosts update the same shared location. One inventory file is meant only for one host, so it must not be shared and edited by other hosts. When you use the /etc/oraInst.loc file, ensure that the inventory location specified there is not pointing to such a location. If you have configured a shared location that is common for two or more hosts, then switch over to a non-shared location.
- For a typical HA environment with primary and standby disaster recovery sites using storage replication and virtual host names, the Central Inventory (oraInventory) for software installed on the shared storage using the virtual host name should be located in a shared location that is common between the OMS host in the primary site and the OMS host in the standby site. This shared location should be located on the replicated storage so that the oraInventory can be accessed from the active site for software maintenance activities.

If you already have an Oracle product installed on the host, then the installation wizard uses the existing *oraInventory* directory that was created while installing that Oracle product. Ensure that you have *write* permission on that directory. To do so, run the installer as the same operating system user as the one who installed the other Oracle product.

**Note:** The *oraInventory* directory is different from *Installation Directory*. For information about *Installation Directory*, see Section 2.3.2.

### 2.3.2 What Is an Oracle Middleware Home?

While installing or upgrading to Enterprise Manager Cloud Control, you are required to enter the Oracle Middleware home.

*Oracle Middleware home* (Middleware home) is the parent directory that has the Oracle WebLogic Server home, the Java Development Kit, the Web tier instance files, one or more Oracle homes, the OMS instance base directory, and other relevant files. This is where the OMS and the plug-ins are deployed.

For example,

```
/u01/app/Oracle/Middleware
```

If you are installing or upgrading to Enterprise Manager Cloud Control, then:

- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are already installed in your environment, then the installation wizard automatically detects them and displays the absolute path to the Middleware home where they are installed.

  In this case, validate the Middleware home that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location.

Ensure that the path you enter does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms. Also ensure that the directory you provide has write permission, and does not contain any files or subdirectories.

For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing Enterprise Manager Cloud Control.

  In this case, enter the absolute path to a new middleware home directory where you want to have them installed.

  Ensure that the path you enter does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms. Also ensure that the directory you enter has write permission, and does not contain any files or subdirectories. Even in the case of two system upgrade, enter a new middleware home location, and not the old middleware home directory that you used for the earlier release of the Enterprise Manager system.

  For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

**Note:** *Oracle Middleware home* is different from *Oracle Home* of OMS or Management Agent. For information about *Oracle Home*, see Section 2.3.4, "What Is an Oracle Home?".

### 2.3.3 What Is an Oracle Management Service Instance Base Location?

While installing Enterprise Manager Cloud Control, you are required to enter the Oracle Management Service Instance Base Location.

*Oracle Management Service Instance Base Location* is a directory (`gc_inst`) outside the Middleware home where the configuration files of the OMS are stored.

The installation wizard uses its built-in algorithm to identify this location, and displays it for you to validate. If the Middleware home is `/u01/app/Oracle/Middleware/`, then by default, the following is the Oracle Management Service Instance Base Location:

```
/u01/app/Oracle/gc_inst
```

You can either accept the default location or specify another location that has *write* permission.

**Note:** For information about *Oracle Middleware home*, see Section 2.3.2.

### 2.3.4 What Is an Oracle Home?

*Oracle Home* or *Oracle home* is the directory where the OMS, the Management Agent, and the plug-ins are installed. Table 2–4 lists the default *Oracle homes* are created.

***Table 2–4 Oracle Homes of OMS, Management Plug-Ins***

| Component | Default Oracle Home | Sample Location |
|---|---|---|
| Oracle Management Service | `$<MIDDLEWARE_HOME>/oms` | `/u01/app/Oracle/Middleware/oms` |
| Oracle Management Agent | `$<AGENT_BASE_DIR>/core/12.1.0.5.0` | `/u01/app/Oracle/agent/core/12.1.0.5.0` |
| Plug-In (OMS-specific plug-ins) | `$<MIDDLEWARE_HOME>/plugins/<pluginID_Version>` | `/u01/app/Oracle/software/plugins/oracle.sysman.db.agent.plugin_12.1.0.5.0` |
| Plug-In (agent-specific plug-ins) | `$<AGENT_BASE_DIR>/plugins` | `/u01/app/Oracle/agent/plugins` |

**Note:** *Oracle Home* is different from *OraInventory*. For information about *OraInventory* directory, see Section 2.3.1.

### 2.3.5 What Is an Agent Base Directory?

While installing Enterprise Manager Cloud Control and a standalone Management Agent using the Add Host Targets Wizard, you are required to enter an installation base directory, which is essentially the agent base directory.

Agent Base Directory is a directory outside the Oracle Middleware Home, where the Management Agent home is created.

For example, if the agent base directory is `/u01/app/Oracle/agent`, then the Management Agent home is created as `/u01/app/Oracle/agent/core/12.1.0.5.0`.

### 2.3.6 What is an Agent Instance Directory?

*Agent Instance Directory* is a directory (`agent_inst`) created for storing all Management Agent-related configuration files.

Agent Instance Directory is created inside the agent base directory.

For example, if the agent base directory is `/u01/app/Oracle/agent`, then by default, the following is the agent instance directory:

```
/u01/app/Oracle/agent/agent_inst
```

### 2.3.7 What Is a /TMP or C:\Temp Directory Used For?

When you invoke the Enterprise Manager Cloud Control Installation Wizard, it automatically copies some executable files and link files to a temporary directory on the host.

For example, the default `/tmp` directory on UNIX hosts, and `C:\Temp` on Microsoft Windows hosts.

If the host is set to run `cron` jobs along with many other processes that may be running periodically, then these jobs attempt to clean up the default temporary directory, thereby deleting some files and causing the installation wizard to fail.

If there are any `cron` jobs or processes that are automatically run on the hosts to clean up the temporary directories, then ensure that you set the `TMP` or `TEMP` environment variable to a location that is different from the default location. Ensure that the non-default location you set is secure on the hard drive, that is, the non-default location is a location where cleanup jobs are not run. Also ensure that you have *write* permissions on this alternative directory.

This must be done before you run the installer to invoke the Enterprise Manager Cloud Control Installation Wizard. (For UNIX operating systems, you invoke `runInstaller`, and for Microsoft Windows, you invoke `setup.exe`).

**Note:** Specifying an alternative temporary directory location is not mandatory, and is required `only` if any `cron` jobs are set on the computers to clean up the `/tmp` directory.

## 2.4 Understanding the Configuration Assistants

This section describes the postinstallation activities that are performed by the installation wizard. In particular, this section covers the following:

- What Are Configuration Assistants?
- What Configuration Assistants Are Run by the Installation Wizard?
- What Do You Do When Configuration Assistants Fail?

### 2.4.1 What Are Configuration Assistants?

While installing or upgrading to Enterprise Manager Cloud Control in either GUI mode (using the installation wizard) or silent mode (using a response file), a set of configuration assistants are run at the end of the installation process to configure the installed or upgraded components. Your installation or upgrade process is complete only after all the components are configured using these configuration assistants.

**Note:** Even when you perform a software-only installation of Enterprise Manager, when you run the `ConfigureGC.sh` script to configure the installation, the configuration assistants are internally run. (On Microsoft Windows, run the `ConfigureGC.bat` script.)

### 2.4.2 What Configuration Assistants Are Run by the Installation Wizard?

This section lists the configuration assistants run by the installation wizard for the different installation types.

- Configuration Assistants Run While Installing a New Enterprise Manager
- Configuration Assistants Run While Upgrading an Existing Enterprise Manager
- Configuration Assistants Run While Upgrading an Additional Oracle Management Service

#### 2.4.2.1 Configuration Assistants Run While Installing a New Enterprise Manager

The following are the configuration assistants that are run while installing a new Enterprise Manager, that is, when you select *Create a new Enterprise Manager System* in the installation wizard.

- Plugins Prerequisites Check

- Repository Configuration

> **Note:** If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *Repository Out-of-Box Configuration* is run instead of *Repository Configuration*.

- MDS Schema Configuration

> **Note:** If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *MDA Schema Configuration* is not run.

- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

#### 2.4.2.2 Configuration Assistants Run While Upgrading an Existing Enterprise Manager

The following are the configuration assistants that are run while upgrading an existing Enterprise Manager, that is, when you select *Upgrade an existing Enterprise Manager System* in the installation wizard.

**1-System Upgrade Approach**

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Plugins Inventory Migration *(does not run if you are upgrading from 12c Release X (12.1.0.X) to 12c Release X (12.1.0.X))*.

In addition, while upgrading 12*c* Release 4 (12.1.0.4), 12*c* Release 3 (12.1.0.3), or 12*c* Release 2 (12.1.0.2), the following are run:

- Stopping APM Engines
- Stop Admin Server *(does not run if you are upgrading from 10g Release 5 (10.2.0.5) to 12c Release X (12.1.0.X))*

> **Note:** Agent Configuration Assistant is not run because the Management Agent is not upgraded as it is either predeployed by the *Preupgrade Console* (for 10.2.0.5 or 11.1 Management Agents) or upgraded using the *Agent Upgrade Console* (for 12.1.0.4, 12.1.0.3, and 12.1.0.2 Management Agents).

**2-System Upgrade Approach**

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

**1-System Upgrade Approach on a Different Host**

- Plugins Prerequisite Check
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plugins Deployment and Configuration
- Plugins Inventory Migration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration
- Agent Configuration Assistant

#### 2.4.2.3 Configuration Assistants Run While Upgrading an Additional Oracle Management Service

Additional OMS instances are upgraded only using the 1-system upgrade approach. The following are the configuration assistants that are run while upgrading an additional OMS, that is, when you select *Upgrade an existing Enterprise Manager System*, then select an additional OMS in the installation wizard.

- Plugins Prerequisite Check
- OMS Configuration
- Plugins Deployment and Configuration
- Start Oracle Management Service
- Oracle Configuration Manager Repeater Configuration

In addition, while upgrading 12*c* Release 4 (12.1.0.4), 12*c* Release 3 (12.1.0.3), or 12*c* Release 2 (12.1.0.2), the following are run:

- Stopping APM Engines

- Stop Admin Server *(does not run if you are upgrading from 10g Release 5 (10.2.0.5) to 12c Release X (12.1.0.X))*

> **Note:** The Agent Configuration Assistant is not run because the Management Agent is not upgraded as it is either predeployed by the *Preupgrade Console* (for 10.2.0.5 or 11.1 Management Agents) or upgraded using the *Agent Upgrade Console* (for 12.1.0.4, 12.1.0.3, and 12.1.0.2 Management Agents).

### 2.4.3 What Do You Do When Configuration Assistants Fail?

If an optional configuration assistant fails, then the installation wizard ignores the failure and runs to the next configuration assistant automatically. However, if a mandatory configuration assistant fails, then the installation wizard stops the installation process. In this case, you are expected to resolve the issue and rerun the configuration assistant.

For information about the log files to review when a configuration assistant fails, and the actions to be taken to resolve the issue, see Appendix J.

## 2.5 Understanding the Prerequisite Checks before Installing Enterprise Manager Cloud Control

Every time you install Enterprise Manager Cloud Control using the installation wizard, a set of prerequisite checks are run to verify if the environment meets the minimum requirements for a successful installation. The installation wizard checks for a variety of things including required operating system patches, operating system packages, kernel parameters, and so on.

The following sections describe these prerequisite checks. In particular, this section covers the following:

- What Prerequisite Checks Are Run by Default?
- How Do You Run the Prerequisite Checks in a Standalone Mode?

### 2.5.1 What Prerequisite Checks Are Run by Default?

The following are the default prerequisite checks that are run for different installation types—*Creating a New Enterprise Manager System* and *Upgrading an Existing Enterprise Manager System:*

- Prerequisite check for verifying whether the installation is being done on a certified operating system.
- Prerequisite check for verifying whether all the certified packages and libraries have been installed.
- Prerequisite check for verifying whether the glibc package has been installed. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether there is sufficient disk space in the `temp` directory. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether there is sufficient disk space in the inventory directory.
- Prerequisite check for verifying whether there is *write* permission in the inventory directory. *(Not applicable for OMS installation)*

- Prerequisite check for verifying whether the software is compatible with the current operating system.
- Prerequisite check for verifying whether there is sufficient physical memory.
- Prerequisite check for verifying the required `ulimit` value. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying the host name.
- Prerequisite check for verifying whether the `LD_ASSUME_KERNEL` environment variable is set. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether proper timezone is set.
- Prerequisite check for verifying whether there is 4 GB of swap space. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether the `http_proxy` environment variable is set. Ideally, it must not be set.

## 2.5.2 How Do You Run the Prerequisite Checks in a Standalone Mode?

You can run the prerequisite checks in standalone mode before invoking the installation wizard. This helps you identify and resolve issues that might otherwise cause the installation to fail.

**WARNING: When you run the prerequisite checks in standalone mode on a host where there are no Oracle products installed, the prerequisite check that checks for the central inventory hard disk space fails. This failure is expected because there are no Oracle products installed on the host. You can safely ignore this failure, and proceed with the actual installation.**

Table 2–5 shows the commands you need to run to run the prerequisite checks in standalone mode:

***Table 2–5 Running Prerequisite Checks in Standalone Mode***

| Installation Type | Command |
|---|---|
| ■ Create a New Enterprise Manager System<br>■ Upgrade an Existing Enterprise Manager System<br>■ Install Software Only | `<Software_Location>/install/runInstaller -prereqchecker PREREQ_CONFIG_LOCATION=<Software_Location>/stage/prereq -entryPoint "oracle.sysman.top.oms_Core" -prereqLogLoc <absolute_path_to_log_location> -silent  -waitForCompletion` |

**Note:** On Microsoft Windows, replace `/runInstaller` with `setup.exe`. Also, `<Software_Location>` mentioned in the commands in Table 2–5 refer to the location where the Enterprise Manager software is available. For example, DVD. If you have downloaded the software from Oracle Technology Network (OTN), then enter the absolute path to that downloaded location.

## 2.6 Understanding the Limitations of Enterprise Manager Cloud Control

This section describes the limitations you might face while using Enterprise Manager Cloud Control. In particular, this section covers the following:

- Can You Access Unlicensed Components?
- What Are the Limitations with DHCP-Enabled Machines?

### 2.6.1 Can You Access Unlicensed Components?

Although the installation media in your media pack contain many Oracle components, you are permitted to use only those components for which you have purchased licenses. Oracle Support Service does not provide support for components for which licenses have not been purchased.

For more information, access the Enterprise Manager documentation library at the following URL and view the *Oracle Enterprise Manager Licensing Information Guide*:

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

### 2.6.2 What Are the Limitations with DHCP-Enabled Machines?

Do NOT run the OMS on a computer that is DHCP enabled. Oracle strongly suggests that you use a static host name or IP address assigned on the network for Enterprise Manager Cloud Control components to function properly.

For more information, refer to *My Oracle Support* Note 428665.1 at:

https://support.oracle.com/

## 2.7 Understanding the Startup Scripts

By default, Enterprise Manager Cloud Control offers a startup script called `gcstartup` with every installation of OMS and Management Agent. The startup script ensures that the OMS and the Management Agent are started automatically every time their hosts are rebooted, thereby relieving you of the manual effort.

### 2.7.1 Where is the Startup Script Stored?

The startup script is present in the following location of the OMS host and the Management Agent host:

```
/etc/init.d/gcstartup
```

### 2.7.2 What does the Startup Script Invoke?

On the OMS host, the startup script invokes the following file to start up the OMS when its host is rebooted:

```
$<OMS_HOME>/install/unix/scripts/omsstup
```

Similarly, on the Management Agent host, the startup script invokes the following file to start up the Management Agent when its host is rebooted:

```
$<AGENT_HOME>/install/unix/scripts/agentstup
```

### 2.7.3 How Do I Stop the Startup Script from Starting the OMS or the Management Agent?

If you do not want the startup script to start the OMS and the Management Agent when their hosts are rebooted, then remove the `omsstup` file and the `agentstup` file from the respective hosts.

Alternatively, you can rename the file `/etc/oragchomelist` to `/etc/oragchomelist_bak`.

### 2.7.4 Can the Startup Script Start an OMS or a Management Agent on a Remote Host?

The startup script is specific to the host on which an OMS or a Management Agent is installed. Therefore, the startup script cannot start an OMS or a Management Agent on a remote host.

### 2.7.5 How Do I Change the Management Agent Service Priority Level that the Startup Script Follows While Starting Up or Shutting Down the Management Agent?

You can change the Management Agent service priority level either while installing the Management Agent, or after installing the Management Agent.

To change the Management Agent service priority level while installing Management Agents using the Add Host Targets Wizard, use the `START_PRIORITY_LEVEL` and `SHUT_PRIORITY_LEVEL` additional parameters that are described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To change the Management Agent service priority level while installing a Management Agent using the `agentDeploy` script, use the `START_PRIORITY_LEVEL` and `SHUT_PRIORITY_LEVEL` response file parameters that are described in Table 6–3.

To change the Management Agent service priority level after installing the Management Agent, follow these steps:

1. Navigate to the `/etc/rc.d` directory. If the `rc.d` directory is not present within `/etc`, navigate to `/sbin/rc.d`.
2. Delete all the `gcstartup` files present in the `/etc/rc.d` or `/sbin/rc.d` directory. To search for these files, run the following command:

   ```
   find . -name "*gcstartup"
   ```

3. Edit the `START_PRIORITY_LEVEL` and `SHUT_PRIORITY_LEVEL` parameters in the `$<ORACLE_HOME>/install/unix/scripts/gcroot.sh` file.

   For more information about these parameters, see Table 6–3.

4. Run the `root.sh` script from the Management Agent home:

   ```
   $<ORACLE_HOME>/root.sh
   ```

For example, the output of the `find . -name "*gcstartup"` command that you run after navigating to `/etc/rc.d` may be the following:

```
./rc5.d/K19gcstartup
./rc5.d/S98gcstartup
./rc5.d/S98lockgcstartup
./rc5.d/K19unlockgcstartup
./rc3.d/K19gcstartup
./rc3.d/S98gcstartup
./rc3.d/S98lockgcstartup
./rc3.d/K19unlockgcstartup
./rc2.d/K19gcstartup
```

```
./rc2.d/S98gcstartup
./rc2.d/S98lockgcstartup
./rc2.d/K19unlockgcstartup
./init.d/unlockgcstartup
./init.d/gcstartup
./init.d/lockgcstartup
```

If this is the output, delete all the `gcstartup` files present in the `./rc5.d, ./rc3.d, ./rc2.d` and `./init.d` directories, edit the `START_PRIORITY_LEVEL` and `SHUT_PRIORITY_LEVEL` parameters in the `/tmp/agent/core/12.1.0.5.0/install/unix/scripts/gcroot.sh` file (if `ORACLE_HOME` is `/tmp/agent/core/12.1.0.5.0/`), then run `root.sh`.

## 2.8 Understanding Other Miscellaneous Concepts

This section covers miscellaneous concepts related to the installation of Enterprise Manager Cloud Control. In particular, this section covers the following:

- What Is a Host List File?
- What Scripts Are Run During the Installation Process?

### 2.8.1 What Is a Host List File?

While using the Add Host Targets Wizard, you can enter the hosts on which you want to install Oracle Management Agent, in two ways — you can either enter the host name or the IP address, or select an external file that contains a list of hosts mentioned.

If you choose to select an external file, then ensure that the file contains only the host name or the host name followed by the platform name.

The following is an example of the external file with only the host names.

```
host1.example.com
host2.example.com
```

The following is an example of the external file with the host names and the platform names.

```
host1.example.com linux
host2.example.com aix
```

### 2.8.2 What Scripts Are Run During the Installation Process?

At least once during or after the installation of Enterprise Manager Cloud Control or Management Agent, you are prompted to log in as a *root* user and run `oraInstRoot.sh`, `allroot.sh`, or `root.sh`. You must log in as a *root* user because the scripts edit files in the `/etc` directory and create files in the local bin directory (`/usr/local/bin`, by default).

After every installation, a check is performed to identify the Central Inventory (`oraInventory`) directory. The Central Inventory directory is a directory that is automatically created by the installation wizard when an Oracle product is installed on a host for the very first time.

**Note:**

- For a typical non-HA environment, the Central Inventory (oraInventory) can be in a shared or non-shared location. If you use a shared location, then ensure that only one shared location is maintained per host, and no two hosts update the same shared location. One inventory file is meant only for one host, so it must not be shared and edited by other hosts. When you use the /etc/oraInst.loc file, ensure that the inventory location specified there is not pointing to such a location. If you have configured a shared location that is common for two or more hosts, then switch over to a non-shared location.
- For a typical HA environment with primary and standby disaster recovery sites using storage replication and virtual host names, the Central Inventory (oraInventory) for software installed on the shared storage using the virtual host name should be located in a shared location that is common between the OMS host in the primary site and the OMS host in the standby site. This shared location should be located on the replicated storage so that the oraInventory can be accessed from the active site for software maintenance activities.

- If you have NOT installed an Oracle product before on the host, then run the `oraInstRoot.sh` script from the Central Inventory:

  ```
  $Home/oraInventory/oraInstRoot.sh
  ```

  The `oraInstRoot.sh` script is run to create the `oraInst.loc` file. The `oraInst.loc` file contains the Central Inventory location.

- However, if you already have an Oracle product on the host, then run `allroot.sh` script from the OMS home:

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

# Part II

## Installing Enterprise Manager System

This part describes the different ways of installing Enterprise Manager Cloud Control. In particular, this part contains the following chapters:

- Chapter 3, "Installing Enterprise Manager in Silent Mode"
- Chapter 4, "Installing Enterprise Manager Using the Software-Only Method"

# 3

# Installing Enterprise Manager in Silent Mode

This chapter describes how you can install Enterprise Manager Cloud Control while utilizing an existing, certified Oracle Database, in silent mode. In particular, this section covers the following:

- Introduction to Installing Enterprise Manager in Silent Mode
- Before You Begin Installing Enterprise Manager in Silent Mode
- Prerequisites for Installing Enterprise Manager in Silent Mode
- Installing Enterprise Manager in Silent Mode
- Performing Postinstallation Tasks After Installing an Enterprise Manager System in Silent Mode

**Note:** All general purpose file systems, including OCFS2 and ACFS, are acceptable for storing Enterprise Manager Cloud Control 12*c* software binaries and OMS instance home files (configuration files in `gc_inst`). However, OCFS is not considered a general purpose file system, and therefore is not considered acceptable for this use.

**WARNING: Do not install Enterprise Manager Cloud Control 12c on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.**

## 3.1 Introduction to Installing Enterprise Manager in Silent Mode

If you are familiar with the way Enterprise Manager is installed, and if you want to install it without facing any interview screens of the installation wizard, then the best option is to install it in silent mode.

In silent mode, you use a response file that captures all the information you need to successfully complete an installation. This saves time and effort in one way because the installation details are captured just once, and in a single file that can be circulated and reused for installation on other hosts.

However, whether you install Enterprise Manager in graphical mode or silent mode, the installation process, the installed components, and the configuration process remain the same. Therefore, silent mode of installing Enterprise Manager is only an option offered to you.

To understand what components are installed, what configuration assistants are run, and how the directory structure will look after installation, see the chapter on installing Enterprise Manager system in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 3.2 Before You Begin Installing Enterprise Manager in Silent Mode

Before you begin, keep these points in mind:

- You must ensure that you have the latest Enterprise Manager Cloud Control software.

  To download the latest software, access the following URL:

  `http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html`

  For information about downloading the latest software, refer to Section 1.2.2.

- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.

- You can install Enterprise Manager Cloud Control only on a single host—locally on the server where you invoke the installation wizard with a response file. You cannot install on remote hosts.

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

- Oracle Management Service 12*c* can communicate only with the following versions of Oracle Management Agent 12*c:*

***Table 3–1 Compatibility Between OMS and Management Agents Across 12c Releases***

| | **Oracle Management Agent 12c Release 1 (12.1.0.1) + Bundle Patch 1**<br>*(Refers to agents and their plug-ins patched or upgraded to, or installed with Bundle Patch 1)* | **Oracle Management Agent 12c Release 2 (12.1.0.2)** | **Oracle Management Agent 12c Release 3 (12.1.0.3)** | **Oracle Management Agent 12c Release 4 (12.1.0.4)** | **Oracle Management Agent 12c Release 5 (12.1.0.5)** |
|---|---|---|---|---|---|
| **Oracle Management Service 12c Release 1 (12.1.0.1) + Bundle Patch 1** | Yes<br>*(includes Management Agents with and without Bundle Patch 1)* | No | No | No | No |
| **Oracle Management Service 12c Release 2 (12.1.0.2)** | Yes<br>*(includes Management Agents with and without Bundle Patch 1)* | Yes | No | No | No |

*Table 3–1 (Cont.) Compatibility Between OMS and Management Agents Across 12c Releases*

| | | | | | |
|---|---|---|---|---|---|
| **Oracle Management Service 12c Release 3 (12.1.0.3)** | Yes<br>*(Only Management Agents released in January 2012 [with Bundle Patch 1])* | Yes | Yes | No | No |
| **Oracle Management Service 12c Release 4 (12.1.0.4)** | No | Yes | Yes | Yes | No |
| **Oracle Management Service 12c Release 5 (12.1.0.5)** | No | Yes | Yes | Yes | Yes |

- You must not set the `ORACLE_HOME` and `ORACLE_SID` environment variables. You must ensure that the Oracle directories do NOT appear in the PATH.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11*g* Release 1 (10.3.6), but only if you do not specify the use of existing installations. Oracle strongly recommends using the 12*c* installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12*c*.
- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6.0.43.0 (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).
  - Download JDK 1.6.0.43.0 for your platform from the platform vendor's Web site.

    For example, download SUN JDK 1.6.0.43.0 for Linux platforms from the following Oracle Web site URL:

    http://www.oracle.com/technetwork/java/javase/downloads/index.html
  - 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 11*g* Release 1 (10.3.6) on Linux 64-bit platforms, first install the 64-bit JDK for your platform, and then download and use the `wls1036_generic.jar` file to install Oracle WebLogic Server.

    For example,

    ```
    <JDK home>/bin/java -d64 -jar <absolute_path _to_wls1036_
    generic.jar>
    ```
  - If you want to manually install Oracle WebLogic Server 11*g* Release 1 (10.3.6) on Linux 32-bit platforms, then download and use either the `wls1036_linux32.bin` file or the `wls1036_generic.jar` file.

    For example,

```
<JDK home>/bin/java  -jar <absolute_path _to_wls1036_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.

- After installing Oracle WebLogic Server, make sure you apply the patches 14482558, 13349651, 16080294, and 16888501 on it. Without these patches, the additional OMS installation will fail.

  For instructions to apply these patches, see the following URL:

  `http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC`

- You must ensure that the Oracle WebLogic Server 11*g* Release 1 (10.3.6) 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.

- Do not install on a symlink. Installing in such a location may impact life cycle operations such as patching and scaling out.

- You can optionally use the database templates offered by Oracle to create a database instance with a preconfigured Management Repository. To do so, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. You can use such a database instance for simple as well as advanced installation.

  However, note that the database templates are essentially designed for simple installation, although they can be used for advanced installation. Therefore, while performing an advanced installation (possibly with small, medium, or large deployment size selection), when you provide the details of such a database, you will be prompted that the database parameters need to be modified to suit the deployment size you selected. You can confirm the message to proceed further. The installation wizard will automatically set the database parameters to the required values.

- If you are installing on an NFS-mounted drive and creating the OMS instance base directory (gc_inst) on that NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. Modify the lock file location in the `httpd.conf` file to map to a location on a local file system. For instructions, refer to Section 3.5.

- Enterprise Manager is not affected when you enable or disable features such as XML DB on the Oracle Database in which you plan to configure the Management

Repository. Therefore, you can enable or disable any feature in the database because Enterprise Manager does not rely on them

- If you want to optionally follow the configuration guidelines for deploying the Management Repository so that your management data is secure, reliable, and always available, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to `"skip"`. However, if you want to apply them during installation, then you can modify this variable as described in Table 3–3.
- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

  `http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf`

  When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.
- 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`.
- As a prerequisite, you must have an existing Oracle Database to configure the Management Repository. This database can also have the Automatic Memory Management (AMM) feature enabled.
- If you are installing in, or will be converting in the future to, a high-availability or a disaster-recovery configuration, then review and become familiar with the contents in Chapter 16, Chapter 17, Chapter 18 before continuing with this installation.

  Once you have reviewed the information in the aforementioned chapters, follow the best practices referenced in Chapter 17, specifically the information in Section 17.3.1 in order to best prepare your installation for high availability or disaster recovery.
- The locale-specific data is stored in the `<OMS_Oracle_Home>/nls/data` directory. Oracle strongly recommends that you either set the environment variable `ORA_NLS10` to `<OMS_Oracle_Home>/nls/data` or do not set at all.
- If you install the OMS and the Oracle Database, which houses the Management Repository, on the same host, then when you reboot the host, the OMS and the Management Agent installed with it will not automatically start up. You will have to manually start them.
- Enforcing option is supported for Security-Enhanced Linux (SELinux).

## 3.3 Prerequisites for Installing Enterprise Manager in Silent Mode

Meet the prerequisites described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 3.4 Installing Enterprise Manager in Silent Mode

This section covers the following:

- Installing Enterprise Manager in Silent Mode
- Advanced Installer Options Supported for Installing an Enterprise Manager System in Silent Mode
- Limitations with the Advanced Options Supported for Installing an Enterprise Manager System in Silent Mode
- Editing the new_install.rsp Response File for Installing an Enterprise Manager in Silent Mode

### 3.4.1 Installing Enterprise Manager in Silent Mode

To install a complete Enterprise Manager system in silent mode, follow these steps:

> **Note:** Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
>
> **However, if you plan to use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure you pass the following parameter while invoking the EM Prerequisite Kit.**
>
> ```
> -componentVariables repository:EXECUTE_CHECKS_NOSEED_DB_
> FOUND:false
> ```

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

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

   In this command, `<Software_Location>` is either the DVD location or the location where you have downloaded the software kit.

2. Edit the response file and enter appropriate values for the variables described in Table 3–3.

3. Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

- If this is the first Oracle product you are installing on the host, then run the following command:

  ```
  ./runInstaller -silent -responseFile <absolute_path>/new_
  install.rsp [-invPtrLoc <absolute_path_to_oraInst.loc>]
  ```

- Otherwise, run the following command:

  ```
  ./runInstaller -silent -responseFile <absolute_path>/new_
  install.rsp
  ```

---

**Note:**

- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.
- When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which a subdirectory in the `Disk1` directory of the Enterprise Manager software.

  There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/`, and when the TEMP variable is set to `/tmp`, the installation wizard tries to look for the opatch JAR file in the `/tmp/../stage` directory, which is equivalent to `/stage`. However, if you do not have read and write permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the TEMP variable to a location where the install user has access to, and then relaunch the installation wizard.
- If you connect to a database instance that was created using the database template offered by Oracle, then you will be prompted that the database parameters need to be modified to suit the deployment size you selected. This is because the templates are essentially designed for simple installation, and the database parameters are set as required for simple installation. Since it is used for advanced installation, the parameters must be set to different values. You can confirm the message to proceed further. The installation wizard will automatically set the parameters to the required values.
- For information about the additional, advanced options you can pass while invoking the installer, refer to Section 3.4.2.

---

**Note:**

- If a prerequisite check fails reporting a missing package, then make sure you install the required package, and retry the installation. The installer validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installer uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and retry the configuration assistant. For more information, see Appendix J.

### 3.4.2 Advanced Installer Options Supported for Installing an Enterprise Manager System in Silent Mode

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

- 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 -silent
  -responseFile <absolute_path>/new_install.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>/new_install.rsp
  ```

  To understand the limitations involved with this advanced option, see Section 3.4.3.

### 3.4.3 Limitations with the Advanced Options Supported for Installing an Enterprise Manager System in Silent Mode

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 3–2 lists the different combinations of these advanced options, and describes the workaround to be followed for each combination:

***Table 3–2 Advanced Options and Workarounds***

| Advanced Option | Workaround |
|---|---|
| `START_OMS=false`<br>`b_startAgent=false` | **1.** Start the OMS:<br>`$<OMS_HOME>/bin/emctl start oms`<br>**2.** Secure the Management Agent:<br>`$<AGENT_HOME>/bin/emctl secure agent`<br>**3.** Start the Management Agent:<br>`$<AGENT_HOME>/bin/emctl start agent`<br>**4.** Add the targets:<br>`$<AGENT_HOME>/bin/emctl config agent addinternaltargets`<br>**5.** Upload the targets:<br>`$<AGENT_HOME>/bin/emctl upload agent` |
| `START_OMS=true`<br>`b_startAgent=false` | Start the Management Agent:<br>`$<AGENT_HOME>/bin/emctl start agent` |
| `START_OMS=false`<br>`b_startAgent=true` | **1.** Start the OMS:<br>`$<OMS_HOME>/bin/emctl start oms`<br>**2.** Secure the Management Agent:<br>`$<AGENT_HOME>/bin/emctl secure agent`<br>**3.** Add the targets:<br>`$<AGENT_HOME>/bin/emctl config agent addinternaltargets`<br>**4.** Upload the targets:<br>`$<AGENT_HOME>/bin/emctl upload agent` |

### 3.4.4 Editing the new_install.rsp Response File for Installing an Enterprise Manager in Silent Mode

Table 3–3 describes what variables you must edit and how you must edit them in the `new_install.rsp` response file for installing Enterprise Manager Cloud Control in silent mode.

*Table 3–3 Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| UNIX_ GROUP_ NAME | String | Yes | *(Required only when central inventory does not exist)* Enter the name of the UNIX group you belong to.<br>For example, `"dba"`<br>**Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms. |
| INVENTOR Y_ LOCATION | String | Yes | *(Required only when central inventory does not exist)* Enter the absolute path to the Central Inventory. Ensure that you have *read, write,* and *execute* permissions on the default inventory directory.<br>For example, `"/scratch/oracle/oraInventory"`.<br>**Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms. |
| SECURITY_ UPDATES_ VIA_ MYORACLE SUPPORT | Boolean | No | ■ Enter `TRUE` if you want to download and install security updates. Then, enter the credentials for the following variables in double quotes:<br>`MYORACLESUPPORT_USERNAME`<br>`MYORACLESUPPORT_PASSWORD`<br>■ Enter `FALSE` if you do not want to download and install security updates: |
| DECLINE_ SECURITY_ UPDATES | Boolean | No | ■ Enter `TRUE` if you want to decline the security updates. In this case, you should have entered `False` for `SECURITY_UPDATES_VIA_ MYORACLESUPPORT`.<br>■ 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 | String | Yes | By default, this variable is set to `"skip"` indicating that the software updates will not be installed during installation.<br>■ 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 in double quotes:<br>`MYORACLESUPPORT_USERNAME_FOR_ SOFTWAREUPDATES`<br>`MYORACLESUPPORT_PASSWORD_FOR_ SOFTWAREUPDATES`<br>■ 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, in double quotes. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| PROXY_ USER | String | Yes | Enter the user name that can be used to access the proxy server.<br>**Note:** Applies only if you have set the SECURITY_ UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION variable to "download", and only if your connection to the Internet requires you to connect through a proxy. |
| PROXY_ PWD | String | Yes | Enter the password that can be used to access the proxy server.<br>**Note:** Applies only if you have set the SECURITY_ UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy. |
| PROXY_ HOST | String | Yes | Enter the name of the proxy host.<br>**Note:** Applies only if you have set the SECURITY_ UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy. |
| PROXY_ PORT | String | Yes | Enter the port used by the proxy server.<br>**Note:** Applies only if you have set the SECURITY_ UPDATES_VIA_MYORACLESUPPORT variable to TRUE and/or the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| ORACLE_MIDDLEWARE_HOME_LOCATION | String | Yes | Enter the location where you want the installer to install Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.<br>For example, `"/u01/app/Oracle/Middleware"`.<br>Ensure that the middleware location has *write* permission.<br>If you have already installed them manually, then enter the location where you have installed them. Also, make sure you have applied the patches 14482558, 13349651, 16080294, and 16888501 on the Oracle WebLogic Server. Without these patches, the additional OMS installation will fail.<br>For instruction to apply these patches, see the following URL:<br>`http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC`<br>For more information about Oracle Middleware home, see Section 2.3.2.<br>**Note:** Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.<br>For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms. |
| ORACLE_HOSTNAME | String | Yes | Enter a fully qualified domain name that is registered in the DNS and is accessible from other network hosts, or enter an alias host name that is defined in the `/etc/hosts` file on all the OMS instances at this site.<br>The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.<br>If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host. |

**Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System**

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| AGENT_ BASE_DIR | String | Yes | Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed.<br>For example, `"/oracle/agent"`.<br>Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home.<br>**Note:** *(Only for Microsoft Windows)* Ensure that the number of characters in the agent base directory path does not exceed 25 characters.<br>For example, the agent base directory path `C:\Oracle\Agent\` containing only 16 characters is acceptable. However, `C:\Oracle\ManagementAgent\12c\new` containing more than 25 characters is not acceptable. |
| WLS_ ADMIN_ SERVER_ USERNAME | String | Yes | By default, `weblogic` 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 skip this variable. However, if you want to have a custom name, then enter the name of your choice. |
| WLS_ ADMIN_ SERVER_ PASSWORD | String | Yes | Enter a password for the WebLogic user account.<br>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 | String | Yes | Confirm the password for the WebLogic user account. |
| NODE_ MANAGER _ PASSWORD | String | Yes | 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.<br>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 | String | Yes | Confirm the password for the node manager user account. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| ORACLE_INSTANCE_HOME_LOCATION | String | Yes | By default, `gc_inst` is considered as the OMS Instance Base directory for storing all OMS-related configuration files. Enter the absolute path to a location outside the middleware home leading up to the directory name.<br>For more information about this location, see Section 2.3.3.<br>**Note:** If you are installing on an NFS-mounted drive and creating the OMS instance base directory (gc_inst) on that NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. For instructions, refer to Section 3.5. |
| CONFIGURE_ORACLE_SOFTWARE_LIBRARY | Boolean | No | If you want to configure the Software Library at the time of installation, set this parameter to `TRUE`. Otherwise, set it to `FALSE`.<br>Even if you do not configure it at the time of installation, your installation will succeed, and you can always configure it later from the Enterprise Manager Cloud Control Console. However, Oracle recommends that you configure it at the time of installation so that it is automatically configured by the installer, thus saving your time and effort. |
| SOFTWARE_LIBRARY_LOCATION | String | Yes | If you have set `CONFIGURE_ORACLE_SOFTWARE_LIBRARY` to `TRUE,` then enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured. Ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same *OMS Shared File System* storage location. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| DATABASE_HOSTNAME | String | Yes | Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores.<br>For example, `"example.com"`.<br>If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.<br>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.<br>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.<br>However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command:<br>`$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conndesc "(DESCRIPTION=(ADDRESS_LIST=(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=EMREP)))" -repos_user sysman`<br>If your Oracle RAC database 11.2 or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.<br>**Note:** If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for the `SYSMAN_PASSWORD` parameter. |
| LISTENER_PORT | String | Yes | Enter the listener port to connect to the existing database.<br>For example, "`1521"`. |
| SERVICENAME_OR_SID | String | Yes | Enter the service name or the system ID (SID) of the existing database.<br>For example, `"orcl"`. |
| SYS_PASSWORD | String | Yes | Enter the SYS user account's password. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| SYSMAN_ PASSWORD | String | Yes | Enter a password for creating a SYSMAN user account. This password is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.<br>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.<br>If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_ OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for this parameter. |
| SYSMAN_ CONFIRM_ PASSWORD | String | Yes | Confirm the SYSMAN user account's password. |

***Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System***

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| DEPLOYMENT_SIZE | String | Yes | Set one of the following values to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.<br>- **SMALL,** to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions<br>- **MEDIUM,** to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions<br>- **LARGE,** to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions<br>For example, `"MEDIUM"`.<br>The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make.<br>You can also modify the deployment size after the installation. For more information on deployment sizes, the prerequisite checks that are run, the database parameters that are set, and how you can modify the deployment size after installation, refer to Section 2.1.6.<br>**Note:**<br>If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you set here matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.<br>If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:<br>- Create another database instance with a template for the desired deployment size, then return to this response file and set the same deployment size to this parameter. For instructions to create a database instance with an Oracle-supplied template, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>- In the database instance you have created, fix the parameters to support the deployment size you want to set here in the response file. To automatically fix the database parameters using Oracle-supplied SQL scripts, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| MANAGEMENT_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to the location where the data file (`mgmt.dbf`) for management tablespace can be stored. Ensure that the specified path leads up to the file name.<br>For example:<br>■ If the database is on a file system, then the path must look like "`/u01/oracle/prod/oradata/mgmt.dbf`".<br>■ If the database is on Automatic Storage Management (ASM), then the path must look like `"+DATA/oemrsp01d/datafile/mgmt.dbf"`, where `disk_group1` is a diskgroup created on ASM and prod is the Service ID (SID).<br>■ If the database is on a raw device, then the path must look like "`</dev/raw1>/prod/oradata/mgmt.dbf`", where `/dev/raw1` is the raw device and prod is the SID.<br>Enterprise Manager Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data. |
| CONFIGURATION_DATA_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to the location where the data file (`mgmt_ecm_depot1.dbf`) for configuration data tablespace can be stored. Ensure that the specified path leads up to the file name.<br>For example, `"/home/john/oradata/mgmt_ecm_depot1.dbf"`.<br>Enterprise Manager Cloud Control requires this data file to store configuration information collected from the monitored targets. |
| JVM_DIAGNOSTICS_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to a location where the data file (`mgmt_deepdive.dbf`) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name.<br>For example, `"/home/john/oradata/mgmt_deepdive.dbf"`.<br>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP). |
| AGENT_REGISTRATION_PASSWORD | String | Yes | Enter a password to secure the communication between the OMS and the Management Agents. Note that you have to provide the same registration password for securing your Management Agents. |
| AGENT_REGISTRATION_CONFIRM_PASSWORD | String | Yes | Confirm the agent registration password. |

*Table 3–3 (Cont.) Editing Response File for Installing Enterprise Manager System*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| STATIC_PORTS_FILE | String | Yes | By default, ports described in Section 2.1.10 are honored. If you want to accept the default ports, then leave this field blank.<br>If you want to use custom ports, then enter the absolute path to the `staticports.ini` file that lists the custom ports to be used for the installation. |
| PLUGIN_SELECTION | String List | Yes<br>*(A comma-separated list of plug-in names, where the plug-in names must be in double quotes)* | 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.<br>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 plug-in IDs for this variable.<br>For example,<br>`PLUGIN_SELECTION={"oracle.sysman.empa","oracle.sysman.vt"}`<br>If you want to install any plug-in that is not available in the software kit, then do the following:<br>**1.** Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location:<br>`http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html`<br>**2.** Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded.<br>**3.** Invoke the installer with the following option, and pass the location where you downloaded the plug-ins:<br>`./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>` |

## 3.5 Performing Postinstallation Tasks After Installing an Enterprise Manager System in Silent Mode

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

# 4

# Installing Enterprise Manager Using the Software-Only Method

This chapter explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point, and configure the installation at a later point. In particular, this chapter covers the following:

- Introduction to Installing Enterprise Manager Using the Software-Only Method
- Before You Begin Installing Enterprise Manager Using the Software-Only Method
- Prerequisites for Installing Enterprise Manager Using the Software-Only Method
- Installing Enterprise Manager Using the Software-Only Method

> **Note:** All general purpose file systems, including OCFS2 and ACFS, are acceptable for storing Enterprise Manager Cloud Control 12c software binaries and OMS instance home files (configuration files in `gc_inst`). However, OCFS is not considered a general purpose file system, and therefore is not considered acceptable for this use.

> **WARNING: Do not install Enterprise Manager Cloud Control 12c on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.**

## 4.1 Introduction to Installing Enterprise Manager Using the Software-Only Method

You can choose to install only the software binaries of Enterprise Manager Cloud Control at one point and configure it at a later point in time to work with an existing, certified Oracle Database. This approach enables you to divide the installation process into two phases, mainly the installation phase and the configuration phase. Understandably, the installation phase takes less time compared to the configuration phase because the installation phase involves only copying of binaries. This approach helps you plan your installation according to the time and priorities you have.

During the installation phase, you invoke the installer to create Oracle homes and install the following components in the Middleware home:

- Java Development Kit (JDK) 1.6.0.43.0
- Oracle WebLogic Server 11*g* Release 1 (10.3.6)
- Oracle Management Service 12*c*

- Oracle Management Agent 12*c*
- Oracle BI Publisher 11*g* (11.1.1.7), which includes `Oracle_BI1` directory.

> **Note:** Although Oracle BI Publisher 11g (11.1.1.7) is installed by default, it is not configured. To configure it post installation, follow the instructions in *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

- Oracle JRF 11*g* Release (11.1.1.7.0), which includes `oracle_common` directory
- Oracle Web Tier 11*g* Release (11.1.1.7.0), which includes `Oracle_WT` directory

> **Note:**
>
> - Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11*g* Release 1 (10.3.6) are installed only if you do not specify the use of existing installations. Oracle strongly recommends using the 12*c* installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12*c*.
> - If you want to manually install Oracle WebLogic Server 11*g* Release 1 (10.3.6), then follow the guidelines outlined in Section 4.2.

During the configuration phase, you invoke a configuration script to 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.

> **Note:** On Microsoft Windows, a Node Manager service is NOT created. This is an expected behavior.

- Configure an Oracle Management Service Instance Base location (`gc_inst`) outside the Middleware home, for storing all configuration details related to Oracle Management Service 12*c*.

  For example, if the Middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/gc_inst`.
- Configure Oracle Management Repository in the existing, certified Oracle Database.
- Deploy and configure 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

  - Oracle Cloud Framework Plug-In

    **Note:** In addition to the mandatory plug-ins listed above, you can optionally install other plug-ins available in the software kit. The installer offers a screen where you can select the optional plug-ins and install them. However, if you want to install some plug-ins that are not available in the software kit, then refer to the point about installing additional plug-ins in Section 4.4.1.3.1.

- Run the following configuration assistants to configure the installed or upgraded components:
  - Plugins Prerequisite Check
  - Repository Configuration

    **Note:** If you use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then *Repository Out-of-Box Configuration Assistant* is run instead of *Repository Configuration Assistant*.

  - MDS Schema Configuration
  - OMS Configuration
  - Plugins Deployment and Configuration
  - Start Oracle Management Service
  - Oracle Configuration Manager Repeater Configuration
  - Agent Configuration Assistant

## 4.2 Before You Begin Installing Enterprise Manager Using the Software-Only Method

Before you begin, keep these points in mind:

- You must ensure that you have the latest Enterprise Manager Cloud Control software.

  To download the latest software, access the following URL:

  `http://www.oracle.com/technetwork/oem/enterprise-manager/downloads/index.html`

  For information about downloading the latest software, refer to Section 1.2.2.

- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager Cloud Control software from. For example, do not download and run the software from a directory titled `EM Software` because there is a white space between the two words of the directory name.

- You can install Enterprise Manager Cloud Control using the installation wizard only on a single host, that is, locally on the server where the wizard is invoked. You cannot install on remote hosts.

- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Oracle Management Service 12*c* can communicate only with the versions of Oracle Management Agent 12*c* described in Table 3–1.
- You must not set the `ORACLE_HOME` and `ORACLE_SID` environment variables. You must ensure that the Oracle directories do NOT appear in the PATH.
- Do not install on a symlink. Installing in such a location may impact life cycle operations such as patching and scaling out.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6.0.43.0 and Oracle WebLogic Server 11*g* Release 1 (10.3.6), but only if you do not specify the use of existing installations. Oracle strongly recommends using the 12*c* installation process to install the JDK and Oracle WebLogic Server for use with Enterprise Manager 12*c*.
- *(Only for Graphical Mode)* You must set the `DISPLAY` environment variable.
  - In bash terminal, run the following command:

    ```
    export DISPLAY=<hostname>:<vnc port>.0
    ```

    For example, `export DISPLAY=example.com:1.0`
  - In other terminals, run the following command:

    ```
    setenv DISPLAY <hostname>:1.0
    ```

    For example, `setenv DISPLAY example.com:1.0`
- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6.0.43.0 (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).
  - Download JDK 1.6.0.43.0 for your platform from the platform vendor's Web site.

    For example, download SUN JDK 1.6.0.43.0 for Linux platforms from the following Oracle Web site URL:

    http://www.oracle.com/technetwork/java/javase/downloads/index.html
  - 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 11*g* Release 1 (10.3.6) on Linux 64-bit platforms, first install the 64-bit JDK for your platform, and then download and use the `wls1036_generic.jar` file to install Oracle WebLogic Server.

    For example,

    ```
    <JDK home>/bin/java -d64 -jar <absolute_path _to_wls1036_
    generic.jar>
    ```

  - If you want to manually install Oracle WebLogic Server 11*g* Release 1 (10.3.6) on Linux 32-bit platforms, then download and use either the `wls1036_linux32.bin` file or the `wls1036_generic.jar` file.

    For example,

    ```
    <JDK home>/bin/java  -jar <absolute_path _to_wls1036_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.

  - After installing Oracle WebLogic Server, make sure you apply the patches 14482558, 13349651, 16080294, and 16888501 on it. Without these patches, the additional OMS installation will fail.

    For instructions to apply these patches, see the following URL:

    `http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC`

- You must ensure that the Oracle WebLogic Server 11*g* Release 1 (10.3.6) 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.

- You can optionally use the database templates offered by Oracle to create a database instance with a preconfigured Management Repository. To do so, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

  However, note that the database templates are essentially designed for simple installation, although they can be used for advanced installation. Therefore, while performing an advanced installation (possibly with small, medium, or large deployment size selection), when you provide the details of such a database, you will be prompted that the database parameters need to be modified to suit the deployment size you selected. You can confirm the message to proceed further. The installation wizard will automatically set the database parameters to the required values.

- If you are installing in, or will be converting in the future to, a high-availability or a disaster-recovery configuration, then review and become familiar with the contents in Chapter 16, Chapter 17, Chapter 18 before continuing with this installation.

  Once you have reviewed the information in the aforementioned chapters, follow the best practices referenced in Chapter 17, specifically the information in

Section 17.3.1 in order to best prepare your installation for high availability or disaster recovery.

- Enterprise Manager is not affected when you enable or disable features such as XML DB on the Oracle Database in which you plan to configure the Management Repository. Therefore, you can enable or disable any feature in the database because Enterprise Manager does not rely on them.
- If you want to optionally follow the configuration guidelines for deploying the Management Repository so that your management data is secure, reliable, and always available, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- *(Only for Silent Mode)* By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to `"skip"`. However, if you want to apply them during installation, then you can modify this variable as described in Section 4.4.2.1.1.
- If you are installing on an NFS-mounted drive and creating the OMS instance base directory (gc_inst) on that NFS-mounted drive, then after you install, move the lock files from the NFS-mounted drive to a local file system location. Modify the lock file location in the `httpd.conf` file to map to a location on a local file system. For instructions, refer to Section 4.4.1.4 or Section 4.4.2.4 depending on the approach you adopt.
- By default, the upload ports and console ports as described in Section 2.1.10 are used.
- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

  `http://www.oracle.com/support/library/brochure/lifetime-support-technology.pdf`

  When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.
- 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`.
- As a prerequisite, you must have an existing Oracle Database to configure the Management Repository. This database can also have the Automatic Memory Management (AMM) feature enabled.
- The locale-specific data is stored in the `<OMS_Oracle_Home>/nls/data` directory. Oracle strongly recommends that you either set the environment variable `ORA_NLS10` to `<OMS_Oracle_Home>/nls/data` or do not set at all.
- If you install the OMS and the Oracle Database, which houses the Management Repository, on the same host, then when you reboot the host, the OMS and the Management Agent installed with it will not automatically start up. You will have to manually start them.

## 4.3 Prerequisites for Installing Enterprise Manager Using the Software-Only Method

Meet the prerequisites described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 4.4 Installing Enterprise Manager Using the Software-Only Method

This section describes the following:

- Installing Enterprise Manager Using the Software-Only Method in Graphical Mode
- Installing Enterprise Manager Using the Software-Only Method in Silent Mode

### 4.4.1 Installing Enterprise Manager Using the Software-Only Method in Graphical Mode

This section explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point in graphical mode, and configure the installation at a later point. In particular, this section covers the following:

- Installing the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode
- Running the Root Script
- Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode
- Performing Postconfiguration Tasks After Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode

#### 4.4.1.1 Installing the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode

To install only the software binaries of Enterprise Manager Cloud Control in graphical mode, follow these steps:

**Note:** Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Basic Installation Guide*.

**However, if you plan to use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure you pass the following parameter while invoking the EM Prerequisite Kit.**

```
-componentVariables repository:EXECUTE_CHECKS_NOSEED_DB_
FOUND:false
```

1. **Invoke the Enterprise Manager Cloud Control Installation Wizard**

Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

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

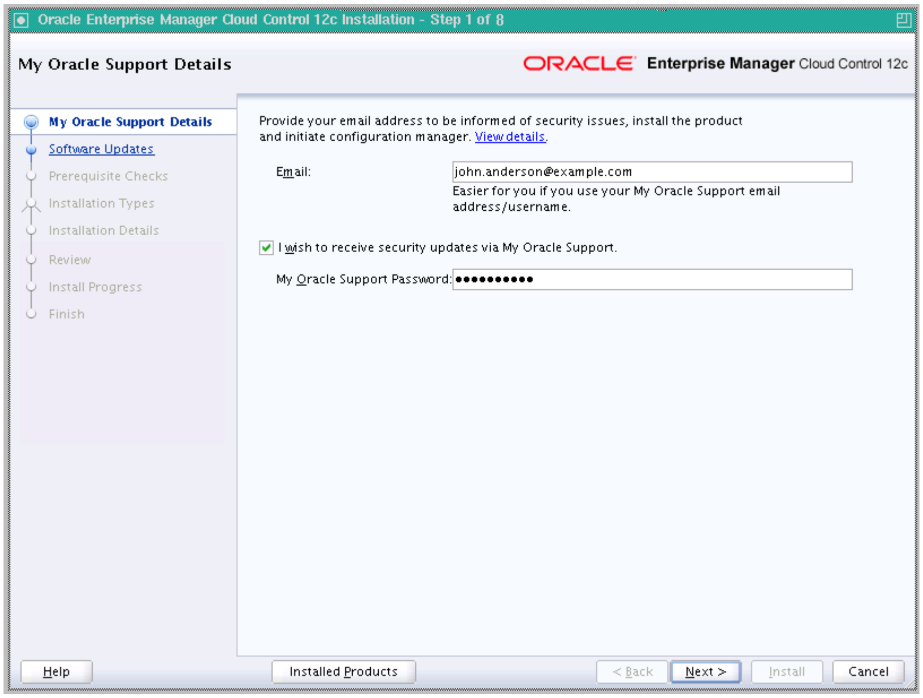
**Note:**

- In this command, `<Software_Location>` refers to either the DVD or 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.`
- The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
- For information about the additional, advanced options you can pass while invoking the installer, refer to Section 4.4.1.1.1.

**Note:** When you invoke `runInstaller` or `setup.exe,` if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which a subdirectory in the `Disk1` directory of the Enterprise Manager software.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/,` and when the TEMP variable is set to `/tmp,` the installation wizard tries to look for the opatch JAR file in the `/tmp/../stage` directory, which is equivalent to `/stage.` However, if you do not have read and write permission on `/stage,` then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the TEMP variable to a location where the install user has access to, and then relaunch the installation wizard.

2. **(Optional) Enter My Oracle Support Details**


Oracle Enterprise Manager Cloud Control 12c Installation - Step 1 of 8
My Oracle Support Details
ORACLE Enterprise Manager Cloud Control 12c
My Oracle Support Details
Software Updates
Prerequisite Checks
Installation Types
Installation Details
Review
Install Progress
Finish
Help
Installed Products
< Back
Next >
Install
Cancel

Provide your email address to be informed of security issues, install the product and initiate configuration manager. View details.

Email: john.anderson@example.com

Easier for you if you use your My Oracle Support email address/username.

☑ I wish to receive security updates via My Oracle Support.

My Oracle Support Password: ●●●●●●●●●●

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*.

---

**Note:** For information about manually collecting the configuration information and uploading it to *My Oracle Support*, see Section 2.1.4.1.

---

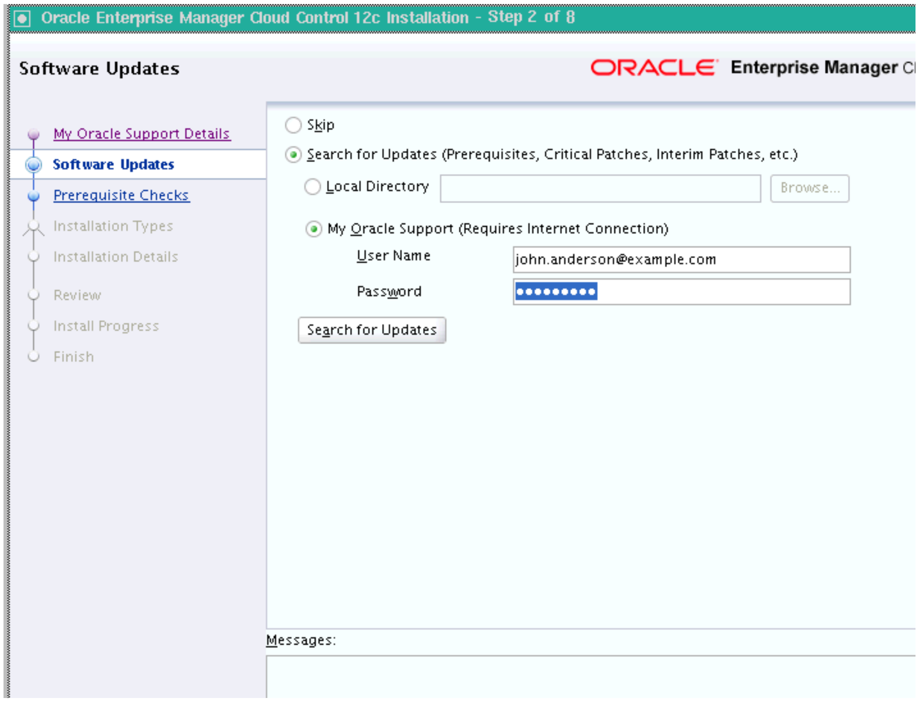
---

**Note:** Beginning with Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3), My Oracle Support accesses support.oracle.com directly. This means that you must provide network access to this URL, or grant proxy access to it from any client that will access My Oracle Support.

---

3. Click **Next**.

4. **(Recommended) Install Software Updates**



○ Skip

● Search for Updates (Prerequisites, Critical Patches, Interim Patches, etc.)

○ Local Directory

● My Oracle Support (Requires Internet Connection)

User Name: john.anderson@example.com

Password: ●●●●●●●●●

On the Software Updates screen, select **Search for Updates,** and then select one of the following options to apply the latest software updates:

- **Local Directory,** if you do not have Internet connectivity on your host, and want to download the updates in offline mode and apply them while performing the installation.
- **My Oracle Support,** if you have Internet connectivity on your host, and want to connect to My Oracle Support directly via the installer to download the updates in online mode and apply them while performing the installation.

For more information on these options, and for instructions to download and apply the software updates using these options, see Section 2.1.5.6.

> **Note:** The Software Updates screen uses the built-in feature *Software Update* to automatically download and deploy the latest recommended patches while installing or upgrading Enterprise Manager Cloud Control. This way, you do not have to keep a manual check on the patches released by Oracle. All patches required by the installer for successful installation and upgrade are automatically detected and downloaded from My Oracle Support, and applied during the installation or upgrade, thus reducing the known issues and potential failures. Oracle strongly recommends using this feature, and applying the software updates while the installation is in progress. For more information, see Section 2.1.5.1.

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. **Enter Oracle Inventory Details**

   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:**

   - 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.
   - Ensure that you have *read, write,* and *execute* permissions on the default inventory directory. If you do not have the required permissions, then exit the installer, invoke the installer again with the `INVENTORY_LOCATION` parameter, and pass the absolute path to the alternative inventory location.

     For example,

     ```
     <Software_Location>/runInstaller INVENTORY_
     LOCATION=<absolute_path_to_inventory_directory>
     ```

     Alternatively, invoke the installer with the `-invPtrLoc` parameter, and pass the absolute path to the oraInst.loc file that contains the alternative inventory location.

     For example,

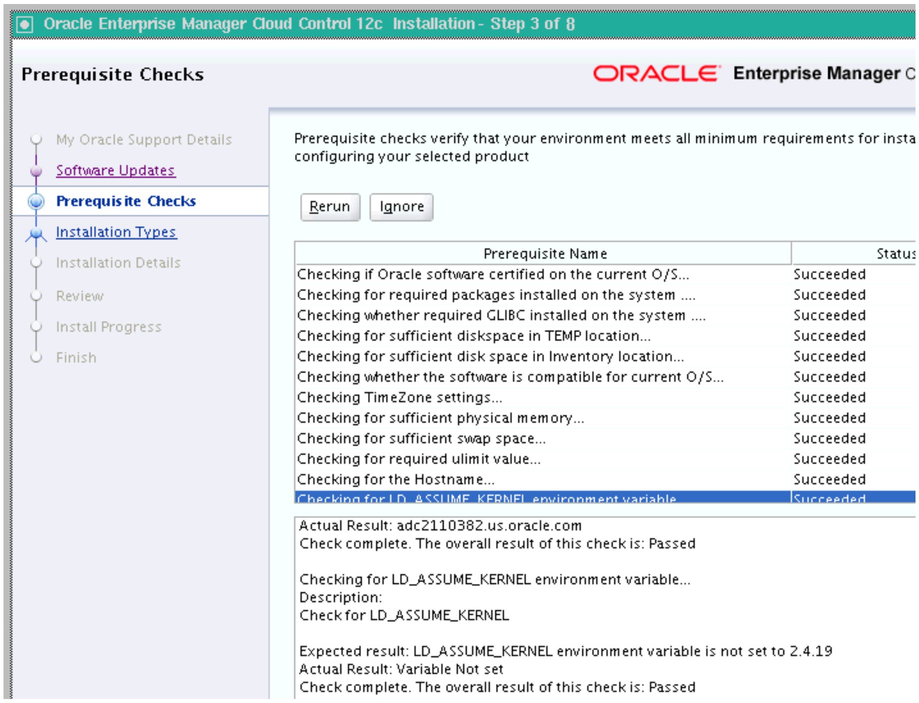
     ```
     <Software_Location>/runInstaller -invPtrLoc <absolute_
     path_to_oraInst.loc>
     ```

     **However, note that these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms.**

   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. **Check Prerequisites**



Prerequisite checks verify that your environment meets all minimum requirements for insta
configuring your selected product

| Prerequisite Name | Status |
|---|---|
| Checking if Oracle software certified on the current O/S... | Succeeded |
| Checking for required packages installed on the system .... | Succeeded |
| Checking whether required GLIBC installed on the system .... | Succeeded |
| Checking for sufficient diskspace in TEMP location... | Succeeded |
| Checking for sufficient disk space in Inventory location... | Succeeded |
| Checking whether the software is compatible for current O/S... | Succeeded |
| Checking TimeZone settings... | Succeeded |
| Checking for sufficient physical memory... | Succeeded |
| Checking for sufficient swap space... | Succeeded |
| Checking for required ulimit value... | Succeeded |
| Checking for the Hostname... | Succeeded |
| Checking for LD_ASSUME_KERNEL environment variable | Succeeded |

```
Actual Result: adc2110382.us.oracle.com
Check complete. The overall result of this check is: Passed

Checking for LD_ASSUME_KERNEL environment variable...
Description:
Check for LD_ASSUME_KERNEL

Expected result: LD_ASSUME_KERNEL environment variable is not set to 2.4.19
Actual Result: Variable Not set
Check complete. The overall result of this check is: Passed
```

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 installation.

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.

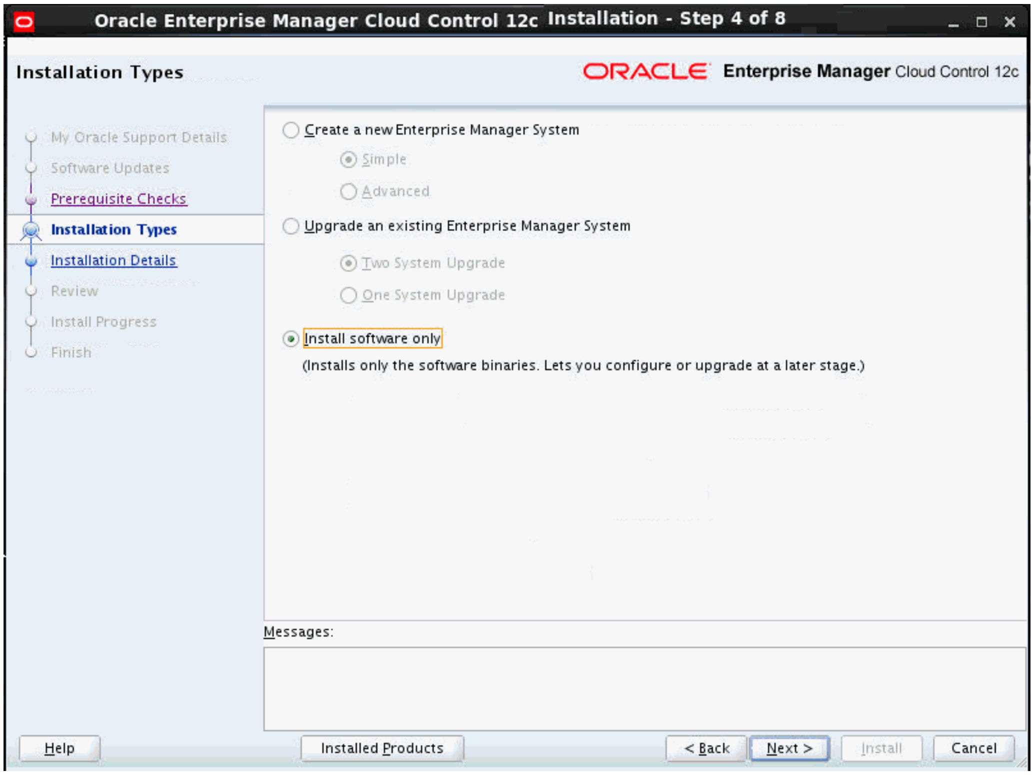
The status of the prerequisite check can be either **Warning**, **Failed**, or **Succeeded**.

- If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the installation. 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.
- However, all package requirements must be met or fixed before proceeding any further. Otherwise, the installation might fail.

9. Click **Next**.

**Note:** If a prerequisite check fails reporting a missing package, then make sure you install the required package, and click **Rerun.** The installation wizard validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installation wizard uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

10. **Select Installation Type**



Oracle Enterprise Manager Cloud Control 12c Installation - Step 4 of 8

Installation Types

○ Create a new Enterprise Manager System

● Simple

○ Advanced

○ Upgrade an existing Enterprise Manager System

● Two System Upgrade

○ One System Upgrade

● Install software only

(Installs only the software binaries. Lets you configure or upgrade at a later stage.)

Messages:

On the Installation Types screen, select **Install software only**.

11. Click **Next**.

12. **Enter Installation Details**

    On the Installation Details screen, do the following:

    a. Enter or validate or enter the Middleware home where you want to install the OMS and other core components.

**Note:**

- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are already installed in your environment, then the installer automatically detects them and displays the absolute path to the Middleware home where they are installed. In this case, validate the Middleware home location that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location. Ensure that the Middleware home location you select or enter is a Middleware home location that does not have any Oracle homes.

  Also make sure you have applied the patches 14482558, 13349651, 16080294, and 16888501 on the Oracle WebLogic Server. Without these patches, the additional OMS installation will fail.

  For instructions to apply these patches, see the following URL:

  `http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC`

  For more information on Oracle WebLogic Server downloads and demos, access the following URL:

  `http://www.oracle.com/technology/products/weblogic/index.html`

- If Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0 are NOT already installed in your environment, then the installer automatically installs them for you while installing the Enterprise Manager system. In this case, enter the absolute path to a directory where you want to have them installed. For example, `/oracle/software/`. Ensure that the directory you enter does not contain any files or subdirectories.

- Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.

  For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

**b.** Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed. For example, if the middleware home is `/u01/app/Oracle/Middleware/`, then you can specify the agent base directory as `/u01/app/Oracle/agent12c`.

Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the middleware home.

**Note:** Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.

For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

c. Validate the name of the host where you want to configure the OMS.

The host name appears as a fully qualified name, or as a virtual host name if your host is configured with virtual machine. If the installation wizard was invoked with a value for ORACLE_HOSTNAME, then this field is prepopulated with that name.

Accept the default host name, or enter a fully qualified domain name that is registered in the DNS and is accessible from other network hosts, or enter an alias host name that is defined in the `/etc/hosts` file on all the OMS instances at this site.

**Note:** The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.

13. Click **Next**.

14. **Review and Install**

    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.

15. **Track the Progress**

    On the Install Progress screen, view the overall progress (in percentage) of the installation.

16. **End the Installation**

    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.

**4.4.1.1.1 Using Advanced Installer Options While Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Graphical Mode** The following are some additional, advanced options you can pass while invoking the installer:

- 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 installation wizard with the WLS_DOMAIN_NAME option, and enter a unique custom name.

  > **Note:** Ensure that the WLS_DOMAIN_NAME option is used even when the ConfigureGC.sh is invoked to configure the software binaries as described in Section 4.4.1.3.

  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
  ```

- If you want to set the Central Inventory, then pass the -invPtrLoc parameter. This parameter considers the path to a location where the inventory pointer file (oraInst.loc) is available. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

  For example,

  ```
  ./runInstaller -invPtrLoc /scratch/OracleHomes/oraInst.loc -silent
  -responseFile <absolute_path_response_file>
  ```

- After you install the software binaries, you will configure the binaries. And after the configuration ends successfully, by default, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the installation wizard with START_OMS and b_startAgent options, and set them to true or false depending on what you want to control.

  > **Note:** Ensure that the START_OMS and b_startAgent options are used even when the ConfigureGC.sh is invoked to configure the software binaries as described in Section 4.4.1.3.

  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 3.4.3.

#### 4.4.1.2 Running the Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager Cloud Control, log in as a *root* user in a new terminal and run the following scripts:

- If this is the first Oracle product you just installed on the host, then run the oraInstroot.sh script from the inventory location specified in the oraInst.loc file that is available in the Management Agent home.

  For example, if the inventory location specified in the oraInst.loc file is $HOME/oraInventory, then run the following command:

  ```
  $HOME/oraInventory/oraInstRoot.sh
  ```

**Note:** If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $HOME/oraInventory/oraInstRoot.sh
```

- Run the `allroot.sh` script from the OMS home:

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

**Note:** If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo $<OMS_HOME>/allroot.sh
```

#### 4.4.1.3 Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode

To configure Enterprise Manager Cloud Control, follow these steps:

1. **Invoke the Enterprise Manager Cloud Control Installation Wizard**

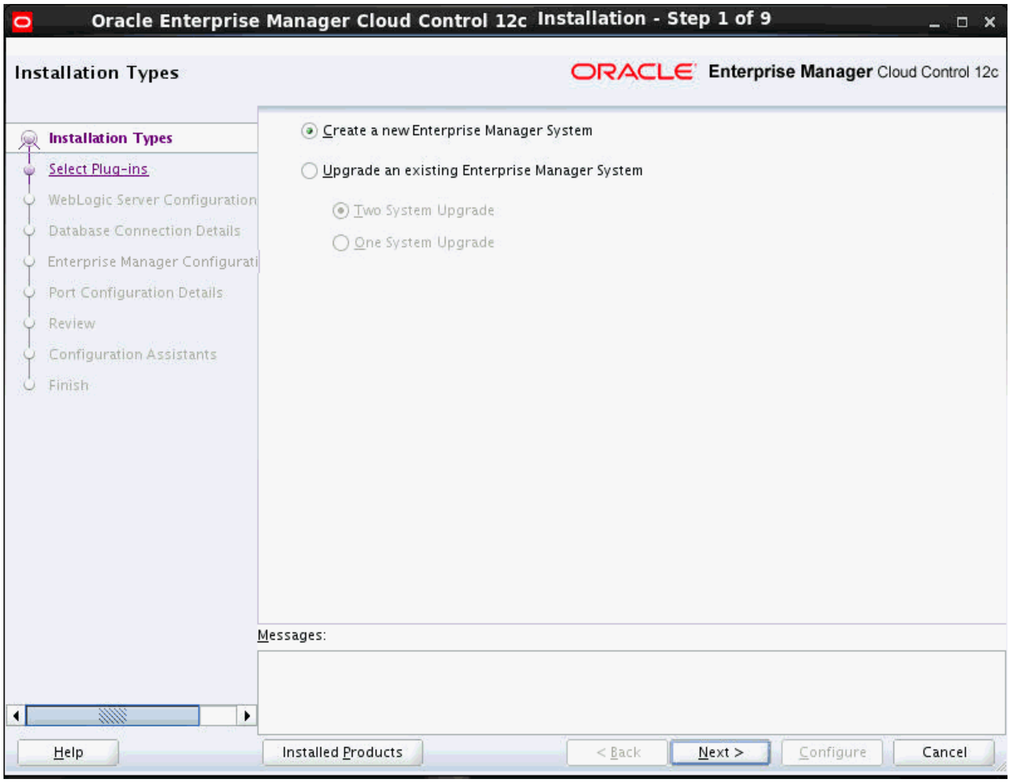
   Invoke the installation wizard. (On Unix, make sure you invoke the installation wizard as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

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

   **Note:**

   - While installing the software binaries as described in Section 4.4.1.1, if you had passed the argument `-invPtrLoc,` then pass the same argument here as well.
   - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
   - For information about the additional, advanced options you can pass while invoking the script, refer to Section 4.4.1.3.1.
   - The only way to configure a software-only installation is to run the `ConfigureGC.sh` (or `ConfigureGC.bat` on Microsoft Windows) script. DO NOT run the individual configuration assistants to configure a software-only installation. If you want to run the individual configuration assistants to configure the installation for some reason, then contact Oracle Support.
   - If you have already configured a software-only installation (the Oracle home) using the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows, then DO NOT try to reconfigure it—either using the script or using the individual configuration assistants.

2. **Select Installation Type**


Oracle Enterprise Manager Cloud Control 12c Installation - Step 1 of 9
Installation Types
ORACLE Enterprise Manager Cloud Control 12c
Installation Types
Select Plug-ins
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configurati
Port Configuration Details
Review
Configuration Assistants
Finish
Help
Installed Products
< Back
Next >
Configure
Cancel

● Create a new Enterprise Manager System

○ Upgrade an existing Enterprise Manager System

● Two System Upgrade

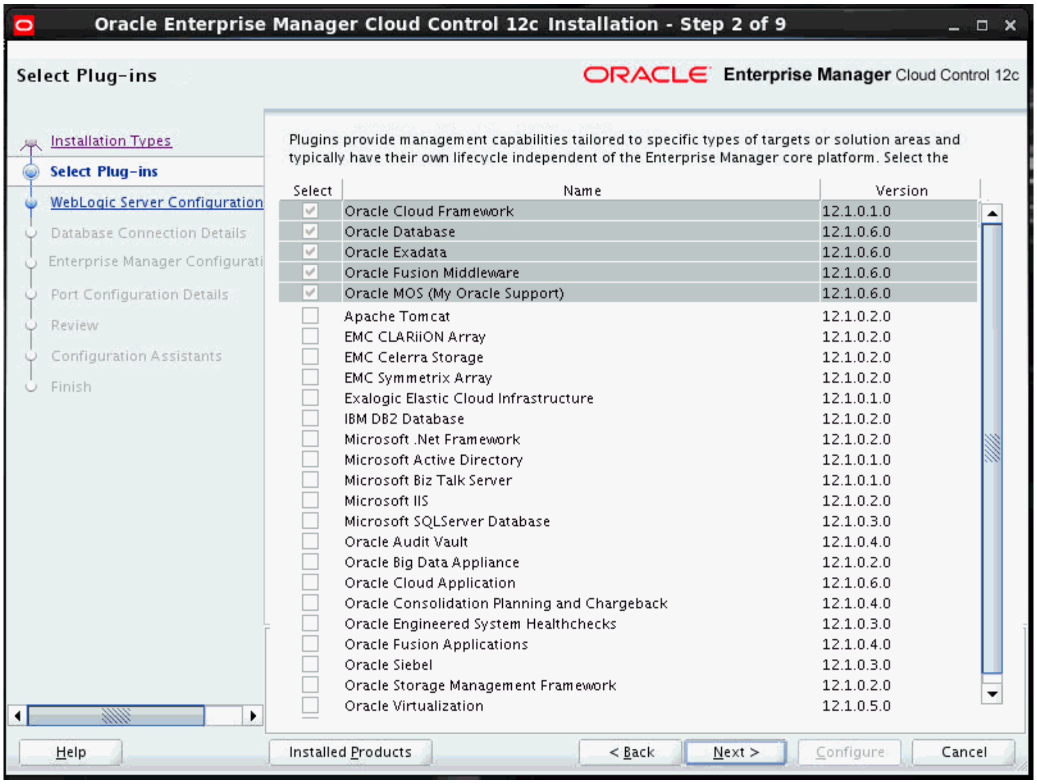
○ One System Upgrade

Messages:

In the installation wizard, on the Installation Types screen, select **Create a New Enterprise Manager System**.

3. Click **Next**.

4. **Deploy Plug-Ins**



Oracle Enterprise Manager Cloud Control 12c Installation - Step 2 of 9

Select Plug-ins

ORACLE Enterprise Manager Cloud Control 12c
Installation Types
Select Plug-ins
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configurati
Port Configuration Details
Review
Configuration Assistants
Finish

Plugins provide management capabilities tailored to specific types of targets or solution areas and typically have their own lifecycle independent of the Enterprise Manager core platform. Select the

| Select | Name | Version |
|---|---|---|
| ☑ | Oracle Cloud Framework | 12.1.0.1.0 |
| ☑ | Oracle Database | 12.1.0.6.0 |
| ☑ | Oracle Exadata | 12.1.0.6.0 |
| ☑ | Oracle Fusion Middleware | 12.1.0.6.0 |
| ☑ | Oracle MOS (My Oracle Support) | 12.1.0.6.0 |
| ☐ | Apache Tomcat | 12.1.0.2.0 |
| ☐ | EMC CLARiiON Array | 12.1.0.2.0 |
| ☐ | EMC Celerra Storage | 12.1.0.2.0 |
| ☐ | EMC Symmetrix Array | 12.1.0.2.0 |
| ☐ | Exalogic Elastic Cloud Infrastructure | 12.1.0.1.0 |
| ☐ | IBM DB2 Database | 12.1.0.2.0 |
| ☐ | Microsoft .Net Framework | 12.1.0.2.0 |
| ☐ | Microsoft Active Directory | 12.1.0.1.0 |
| ☐ | Microsoft Biz Talk Server | 12.1.0.1.0 |
| ☐ | Microsoft IIS | 12.1.0.2.0 |
| ☐ | Microsoft SQLServer Database | 12.1.0.3.0 |
| ☐ | Oracle Audit Vault | 12.1.0.4.0 |
| ☐ | Oracle Big Data Appliance | 12.1.0.2.0 |
| ☐ | Oracle Cloud Application | 12.1.0.6.0 |
| ☐ | Oracle Consolidation Planning and Chargeback | 12.1.0.4.0 |
| ☐ | Oracle Engineered System Healthchecks | 12.1.0.3.0 |
| ☐ | Oracle Fusion Applications | 12.1.0.4.0 |
| ☐ | Oracle Siebel | 12.1.0.3.0 |
| ☐ | Oracle Storage Management Framework | 12.1.0.2.0 |
| ☐ | Oracle Virtualization | 12.1.0.5.0 |

On the Plug-In Deployment screen, select the optional plug-ins you want to install from the software kit (DVD, downloaded software) while installing the Enterprise Manager system.

The pre-selected rows are mandatory plug-ins that will be installed by default. Select the optional ones you want to install.

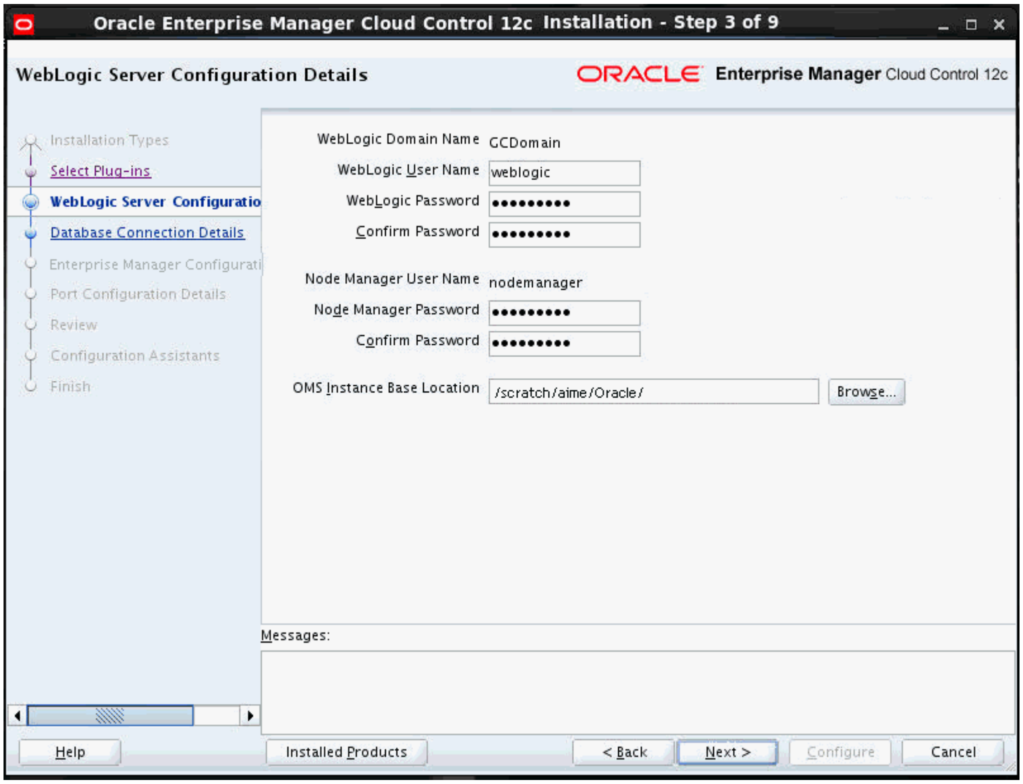
---

**Note:** During installation, 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 4.4.1.1.1.

---

5. Click **Next**.

6. **Enter WebLogic Server Configuration Details**


Oracle Enterprise Manager Cloud Control 12c Installation - Step 3 of 9
WebLogic Server Configuration Details
ORACLE Enterprise Manager Cloud Control 12c
Installation Types
Select Plug-ins
WebLogic Server Configuratio
Database Connection Details
Enterprise Manager Configurati
Port Configuration Details
Review
Configuration Assistants
Finish
Messages:
Browse...
Help
Installed Products
< Back
Next >
Configure
Cancel

WebLogic Domain Name GCDomain

WebLogic User Name weblogic

WebLogic Password ●●●●●●●●●

Confirm Password ●●●●●●●●●

Node Manager User Name nodemanager

Node Manager Password ●●●●●●●●●

Confirm Password ●●●●●●●●●

OMS Instance Base Location /scratch/aime/Oracle/

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. Ensure that the Oracle Management Service instance base location is outside the middleware home

---

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

---

---

**Note:** Ensure that the Oracle Management Service instance base location is outside the middleware home.

---

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.

---

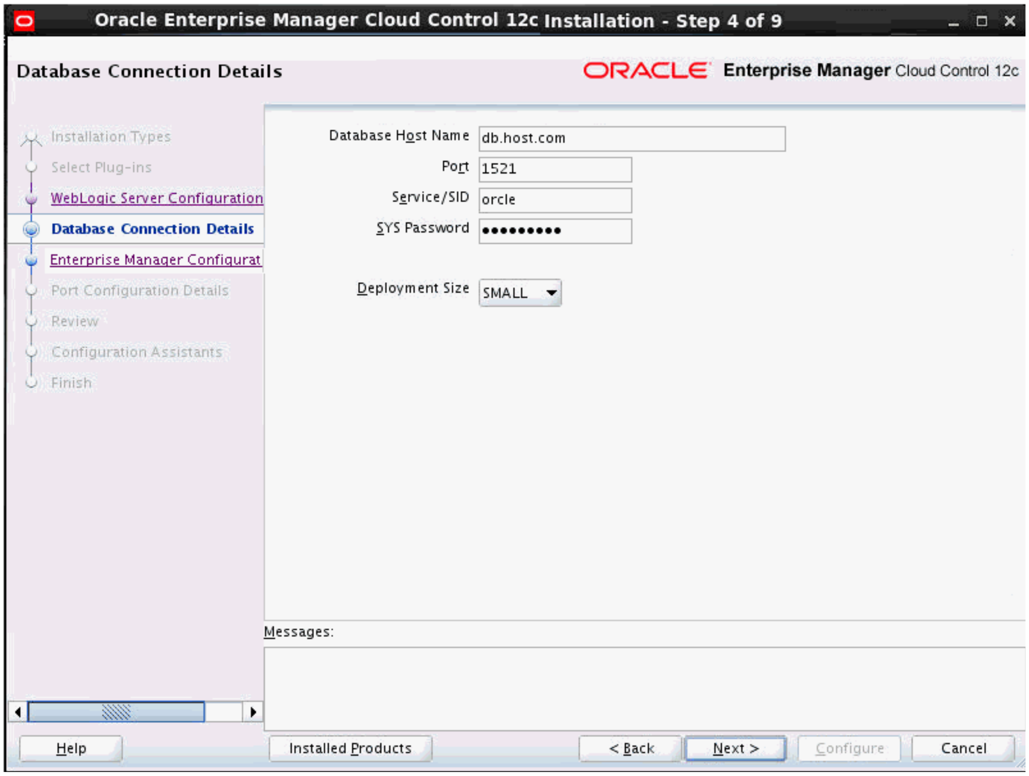
**Note:** On Microsoft Windows, a Node Manager service is NOT created. This is an expected behavior.

---

By default, the Oracle Management Service instance base location is `gc_inst`, which is created outside the Middleware home for storing all configuration details related to the OMS.

7. Click **Next**.

8. **Enter Database Connection Details**


Oracle Enterprise Manager Cloud Control 12c Installation - Step 4 of 9
Database Connection Details
ORACLE Enterprise Manager Cloud Control 12c
Installation Types
Select Plug-ins
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configurat
Port Configuration Details
Review
Configuration Assistants
Finish
Messages:
Help
Installed Products
< Back
Next >
Configure
Cancel

Database Host Name: db.host.com
Port: 1521
Service/SID: orcle
SYS Password: ●●●●●●●●●
Deployment Size: SMALL

On the Database Connection Details screen, do the following:

a. Provide details of the existing, certified database where the Management Repository needs to be created. If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.

   The installer uses this information to connect to the existing database for creating the SYSMAN schema and plug-in schemas. If you provide details of a database that already has a preconfigured Management Repository, then the installer only creates plug-in schemas.

**Note:**

- For information about creating a database instance with a preconfigured Management Repository using the database templates offered by Oracle, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on the Repository Configuration Details screen (as described in Step (10)).
- To identify whether your database is a certified database listed in the certification matrix, access the certification matrix as described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If you see a warning stating that the database you have provided already has Enterprise Manager schemas configured, then make sure you drop those schemas first, then deinstall the Enterprise Manager software that had created those schemas, and then return to the installer to proceed with the new installation. For instructions to drop the schemas and deinstall the software, see Chapter 21.
- For information on all the database initialization parameters that are set, and all the prerequisite checks that are run, and for instructions to run the prerequisite checks manually if they fail, the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- 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*.

**b.** Select the deployment size from the **Deployment Size** list to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.

The prerequisite checks are run regardless of the selection you make, but the values to be set for the various parameters checked depend on the selection you make.

For more information on deployment sizes, the prerequisite checks that are run, the database parameters that are set, and how you can modify the deployment size after installation, refer to Section 2.1.6.

Table 4–1 describes each deployment size.

***Table 4–1 Deployment Size***

| Deployment Size | Targets Count | Management Agents Count | Concurrent User Session Count |
|---|---|---|---|
| Small | Up to 999 | Up to 99 | Up to 10 |
| Medium | Between 1000 and 9999 | Between 100 and 999 | Between 10 and 24 |
| Large | 10,000 or more | 1000 or more | Between 25 and 50 |

9. Click **Next**.

> **Note:** If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you select on this screen matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.
>
> If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:
>
> - Select the deployment size of your choice on this screen, and click **Next.** When you see errors, fix the parameters in the database, then return to this screen to continue with the installation. To automatically fix the parameters using Oracle-supplied SQL scripts, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
> - Minimize the installer, create another database instance with a template for the desired deployment size, then return to this screen and select the matching deployment size. For instructions, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

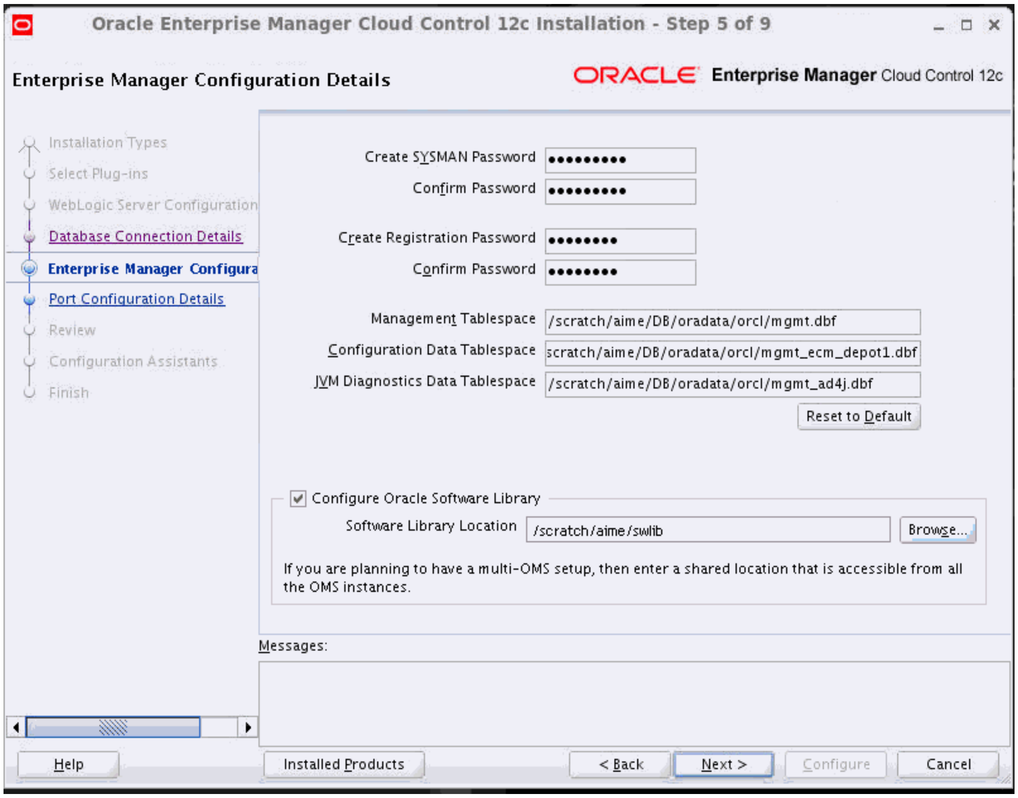
> **Note:**
>
> If you are connecting to an Oracle RAC database, and if you have entered the virtual host name of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connect string with information about the other nodes that are part of the cluster. Update the connect string and click **OK**. If you want to test the connection, click **Test Connection**.
>
> If your Oracle RAC database 11.2. or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.
>
> 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.*

---

**Note:** If you are connecting to an Oracle Database that already has a Database Control configured, then you will see an error message prompting you to deconfigure it. Make sure you deconfigure the database control repository, the database control application, and the database control's central agent. For instructions, see Section A.5 of My Oracle Support note 278100.1.

---

**10. Enter Enterprise Manager Configuration Details**



Oracle Enterprise Manager Cloud Control 12c Installation - Step 5 of 9

Enterprise Manager Configuration Details

ORACLE Enterprise Manager Cloud Control 12c

Installation Types
Select Plug-ins
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configura
Port Configuration Details
Review
Configuration Assistants
Finish

Create SYSMAN Password ●●●●●●●●●

Confirm Password ●●●●●●●●●

Create Registration Password ●●●●●●●●

Confirm Password ●●●●●●●●

Management Tablespace /scratch/aime/DB/oradata/orcl/mgmt.dbf

Configuration Data Tablespace scratch/aime/DB/oradata/orcl/mgmt_ecm_depot1.dbf

JVM Diagnostics Data Tablespace /scratch/aime/DB/oradata/orcl/mgmt_ad4j.dbf

☑ Configure Oracle Software Library

Software Library Location /scratch/aime/swlib

If you are planning to have a multi-OMS setup, then enter a shared location that is accessible from all the OMS instances.

Messages:

On the Repository Configuration Details screen, do the following:

a. For **SYSMAN Password**, enter a password for creating the SYSMAN user account. The SYSMAN user account is used for creating the SYSMAN schema, which holds most of the relational data used in managing Enterprise Manager Cloud Control. SYSMAN is also the super administrator for Enterprise Manager Cloud Control.

**Note:**

- Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
- If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on this screen.

**b.** For **Registration Password**, enter a password for registering the new Management Agents that join the Enterprise Manager system.

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

**c.** For **Management Tablespace**, enter the absolute path to the location where the data file for management tablespace (`mgmt.dbf`) can be stored. The installer uses this information for storing data about the monitored targets, their metrics, and so on. Ensure that the specified path leads up to the file name.

For example, `/u01/oracle/prod/oradata/mgmt.dbf`

If the database is on Oracle Automatic Storage Management (Oracle ASM), then the path must look like: `+<disk_group>/<sid>/<subdir_path_if_any>/<datafilename>.dbf`

For example, `+DATA/oemrsp01d/datafile/mgmt.dbf`

**d.** For **Configuration Data Tablespace**, enter the absolute path to the location where the data file for configuration data tablespace (`mgmt_ecm_depot1.dbf`) can be stored. This is required for storing configuration information collected from the monitored targets. Ensure that the specified path leads up to the file name.

For example, `/u01/oracle/prod/oradata/mgmt_ecm_depot1.dbf`

If the database is on Oracle Automatic Storage Management (Oracle ASM), then the path must look like: `+<disk_group>/<sid>/<subdir_path_if_any>/<datafilename>.dbf`

For example, `+DATA/oemrsp01d/datafile/mgmt_ecm_depot1.dbf`

**e.** For **JVM Diagnostics Data Tablespace**, enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (`mgmt_deepdive.dbf`) can be stored. Ensure that the specified 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).

For example, `/u01/oracle/prod/oradata/mgmt_deepdive.dbf`

If the database is on Oracle Automatic Storage Management (Oracle ASM), then the path must look like: `+<disk_group>/<sid>/<subdir_path_if_any>/<datafilename>.dbf`

For example, `+DATA/oemrsp01d/datafile/mgmt_deepdive.dbf`

f. If you want to configure Oracle Software Library (Software Library), select **Configure Oracle Software Library.** Enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured.

By default, an *OMS Shared File System* storage location is configured, so ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same *OMS Shared File System* storage location.

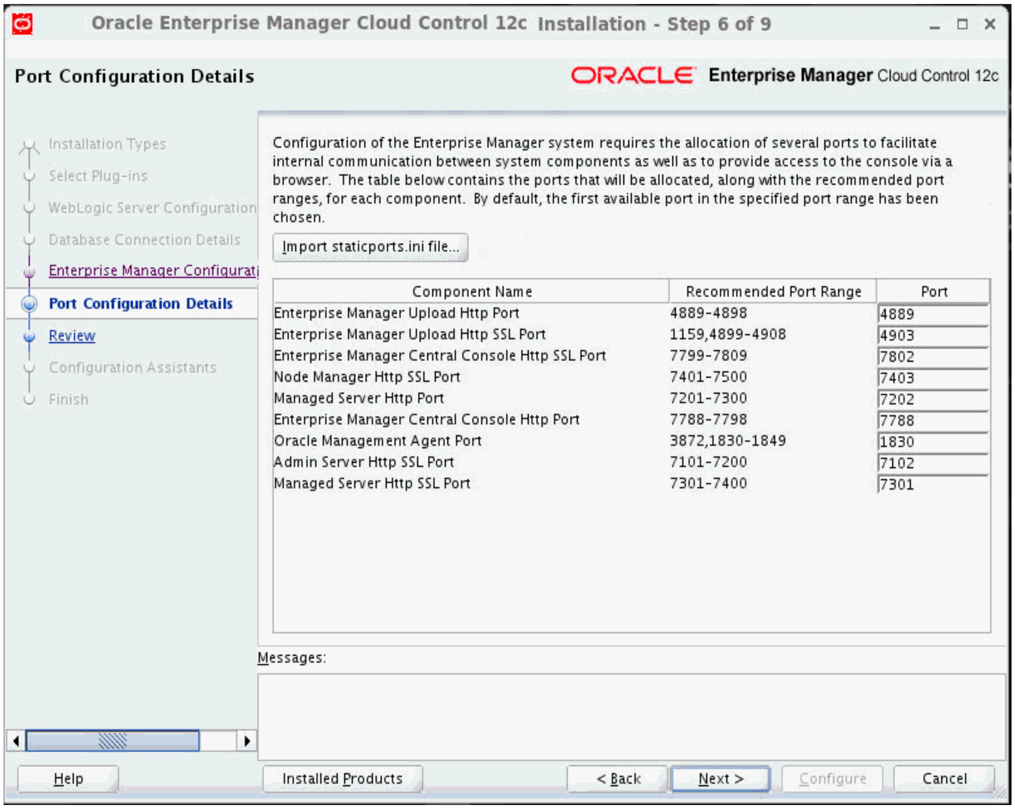
**Note:**

- Oracle recommends that you maintain the Software Library outside the Middleware Home. For example, if the middleware home is `/u01/software/oracle/middleware`, then you can maintain the Software Library in `/u01/software/oracle`.
- Oracle strongly recommends that you enter a mounted location on the OMS host so that the same location can be used when you install additional OMS instances. However, if you are unable to provide a mounted location or if you are testing the installation in a test environment and do not want to provide a mounted location, then you can provide a local file system location. In this case, after the installation, make sure you migrate to a mounted location.

  For information about the Software Library storage locations, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to migrate to an *OMS Agent File System* storage location, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- On Microsoft Windows, if you are unable to provide a mounted location, then enter a local file system location at the time of installing the product, and migrate to an *OMS Agent File System* storage location later. The *OMS Agent File System* storage location is the recommend storage type on Microsoft Windows.

  For information about the Software Library storage locations, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*. For instructions to migrate to an *OMS Agent File System* storage location, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- Configuring the Software Library at the time of installation is optional. Even if you do not select this option and configure it now, your installation will succeed. You always have the option of configuring the Software Library later from the Enterprise Manager Cloud Control Console. However, Oracle strongly recommends that you select this option and configure it at the time of installation so that the installer can automatically configure it for you, thus saving your time and effort.
- Once the Software Library is configured, you can view the location details in the Software Library Console. To access the Software Library Console, in Cloud Control, from the **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**

11. Click **Next**.
12. **Customize Ports**


Oracle Enterprise Manager Cloud Control 12c Installation - Step 6 of 9
Port Configuration Details
ORACLE Enterprise Manager Cloud Control 12c
Installation Types
Select Plug-ins
WebLogic Server Configuration
Database Connection Details
Enterprise Manager Configurati
Port Configuration Details
Review
Configuration Assistants
Finish
Import staticports.ini file...
Messages:
Help
Installed Products
< Back
Next >
Configure
Cancel

Configuration of the Enterprise Manager system requires the allocation of several ports to facilitate internal communication between system components as well as to provide access to the console via a browser. The table below contains the ports that will be allocated, along with the recommended port ranges, for each component. By default, the first available port in the specified port range has been chosen.

| Component Name | Recommended Port Range | Port |
|---|---|---|
| Enterprise Manager Upload Http Port | 4889-4898 | 4889 |
| Enterprise Manager Upload Http SSL Port | 1159,4899-4908 | 4903 |
| Enterprise Manager Central Console Http SSL Port | 7799-7809 | 7802 |
| Node Manager Http SSL Port | 7401-7500 | 7403 |
| Managed Server Http Port | 7201-7300 | 7202 |
| Enterprise Manager Central Console Http Port | 7788-7798 | 7788 |
| Oracle Management Agent Port | 3872,1830-1849 | 1830 |
| Admin Server Http SSL Port | 7101-7200 | 7102 |
| Managed Server Http SSL Port | 7301-7400 | 7301 |

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

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.
>
> The `staticports.ini` file is available in the following location:
>
> ```
> <Software_Extracted_Location>/response
> ```

13. Click **Next**.
14. **Review and Configure**

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. **Track the Progress**

    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. Resolve the issue and retry the configuration assistant. For more information, see Appendix J.
    > - If you accidently 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. For Microsoft Windows platforms, invoke runConfig.bat script.
    >
    >   ```
    >   $<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}
    >   ```
    >
    >   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

16. **End the Installation**

    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.

#### 4.4.1.3.1 Using Advanced Script Options While Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Graphical Mode

The following are some additional, advanced options you can pass while invoking the `configureGC.sh` script (or `configureGC.bat` on Microsoft Windows):

- 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.

  > **Note:** Ensure that the `WLS_DOMAIN_NAME` option was used even when the installation wizard was invoked to install the software binaries as described in Section 4.4.1.1.

  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
  ```

- If you want to install some plug-ins that are not in the software kit, then follow these steps:

  1. Manually download the plug-ins from the Enterprise Manager Download page on OTN, and store them in an accessible location.

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

  2. Invoke the `ConfigureGC.sh` script (or `ConfigureGC`.bat on Microsoft Windows) with the following option, and pass the location where the plug-ins you want to install are available:

     ```
     ./ConfigureGC.sh -pluginLocation <absolute_path_to_plugin_software_
     location>
     ```

     The Plug-In Deployment screen of the installation wizard displays a list of plug-ins available in the software kit as well as the plug-ins available in this custom location. You can choose the ones you want to install.

- 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.

  **Note:** Ensure that the `START_OMS` and `b_startAgent` options are used even when the installation wizard was invoked to install the software binaries as described in Section 4.4.1.1.

  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 3.4.3.

#### 4.4.1.4 Performing Postconfiguration Tasks After Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Graphical Mode

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

### 4.4.2 Installing Enterprise Manager Using the Software-Only Method in Silent Mode

This section explains how you can install only the software binaries of Enterprise Manager Cloud Control at one point in silent mode, and configure the installation at a later point. In particular, this section covers the following:

- Installing the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode
- Running the Root Script
- Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode

- Performing Postconfiguration Tasks After Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode

#### 4.4.2.1 Installing the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode

To install only the software binaries of Enterprise Manager Cloud Control in silent mode, follow these steps:

> **Note:** Oracle recommends you to run the EM Prerequisite Kit before invoking the installer to ensure that you meet all the repository requirements beforehand. Even if you do not run it manually, the installer anyway runs it in the background while installing the product. However, running it manually beforehand sets up your Management Repository even before you can start the installation or upgrade process. For information on the kit, to understand how to run it, and to know about the prerequisite checks it runs, see *Oracle Enterprise Manager Basic Installation Guide*.
>
> **However, if you plan to use a database instance that was created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure you pass the following parameter while invoking the EM Prerequisite Kit.**
>
> ```
> -componentVariables repository:EXECUTE_CHECKS_NOSEED_DB_
> FOUND:false
> ```

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 either the DVD or the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in Table 4–2.

3. Invoke the installer. (On Unix, make sure you invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.)

   - If this is the first Oracle product you are installing on the host, then run the following command:

     ```
     ./runInstaller -silent -responseFile <absolute_path>/software_
     only.rsp [-invPtrLoc <absolute_path_to_oraInst.loc>]
     ```

   - Otherwise, run the following command:

     ```
     ./runInstaller -silent -responseFile <absolute_path>/software_
     only.rsp
     ```

**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 3.4.2.

**Note:** When you invoke `runInstaller` or `setup.exe`, if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have read and write access to `/stage`, which a subdirectory in the `Disk1` directory of the Enterprise Manager software.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/`, and when the TEMP variable is set to `/tmp`, the installation wizard tries to look for the opatch JAR file in the `/tmp/../stage` directory, which is equivalent to `/stage`. However, if you do not have read and write permission on `/stage`, then the installation wizard can hang. Under such circumstances, verify if you have read and write access to the `/stage` directory. If you do not have, then set the TEMP variable to a location where the install user has access to, and then relaunch the installation wizard.

#### 4.4.2.1.1 Editing the software_only.rsp Response File for Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode i

Table 4–2 describes what variables you must edit and how you must edit them in the `software_only.rsp` response file for installing the software binaries.

***Table 4–2 Editing the software_only.rsp Response File for Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quote Required for Values? | Description |
|---|---|---|---|
| UNIX_GROUP_NAME | String | Yes | (Required only when central inventory does not exist) Enter the name of the UNIX group you belong to.<br>For example, `"dba"`.<br>**Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms. |

***Table 4–2 (Cont.) Editing the software_only.rsp Response File for Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quote Required for Values? | Description |
|---|---|---|---|
| INVENTORY_ LOCATION | String | Yes | (Required only when central inventory does not exist) Enter the absolute path to the Central Inventory. Ensure that you have *read*, *write*, and *execute* permissions on the default inventory directory.<br>For example, `"/scratch/oracle/oraInventory"`.<br>**Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms. |
| SECURITY_ UPDATES_ VIA_ MYORACLES UPPORT | Boolean | No | ■ Enter `TRUE` if you want to download and install security updates. Then, enter the credentials for the following variables in double quotes:<br>`MYORACLESUPPORT_USERNAME`<br>`MYORACLESUPPORT_PASSWORD`<br>■ Enter `FALSE` if you do not want to download and install security updates: |
| DECLINE_ SECURITY_ UPDATES | Boolean | No | ■ Enter `TRUE` if you want to decline the security updates. In this case, you should have entered `False` for `SECURITY_UPDATES_ VIA_MYORACLESUPPORT`.<br>■ 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 | String | Yes | By default, this variable is set to `"skip"` indicating that the software updates will not be installed during installation.<br>■ 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 in double quotes.<br>`MYORACLESUPPORT_USERNAME_FOR_ SOFTWAREUPDATES`<br>`MYORACLESUPPORT_PASSWORD_FOR_ SOFTWAREUPDATES`<br>■ 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, in double quotes. |

*Table 4–2 (Cont.) Editing the software_only.rsp Response File for Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quote Required for Values? | Description |
|---|---|---|---|
| ORACLE_MIDDLEWARE_HOME_LOCATION | String | Yes | Enter the location where you want the installer to install Oracle WebLogic Server 11*g* Release 1 (10.3.6) and Java Development Kit 1.6.0.43.0.<br>For example, `"/u01/app/Oracle/Middleware"`.<br>Ensure that the middleware location has *write* permission to create the OMS home.<br>If you have already installed them manually, then enter the location where you have installed them. Also make sure you have applied the patches 14482558, 13349651, 16080294, and 16888501 on it. Without these patches, the additional OMS installation will fail.<br>For instructions to apply these patches, see the following URL:<br>`http://docs.oracle.com/cd/E14759_01/doc.32/e14143/intro.htm#CHDCAJFC`<br>For more information about Oracle Middleware home, see Section 2.3.2.<br>**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.<br>**Note:** Ensure that the number of characters in the middleware home path does not exceed 70 characters for Unix platforms and 25 characters for Microsoft Windows platforms.<br>For example, the middleware home path `C:\Oracle\MW\EM` containing only 15 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms. |

*Table 4–2 (Cont.) Editing the software_only.rsp Response File for Installing the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quote Required for Values? | Description |
|---|---|---|---|
| AGENT_ BASE_DIR | String | Yes | Enter the absolute path to the agent base directory, a location outside the Oracle Middleware home where the Management Agent can be installed.<br>For example, `"/oracle/agent"`.<br>Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home.<br>**Note:** *(Only for Microsoft Windows)* Ensure that the number of characters in the agent base directory path does not exceed 25 characters.<br>For example, the agent base directory path `C:\Oracle\Agent\` containing only 16 characters is acceptable. However, `C:\Oracle\ManagementAgent\12c\new` containing more than 25 characters is not acceptable. |
| ORACLE_ HOSTNAME | String | Yes | Enter a fully qualified domain name that is registered in the DNS and is accessible from other network hosts, or enter an alias host name that is defined in the `/etc/hosts` file on all the OMS instances at this site.<br>The host name must resolve to the local host because the host name is used for the local Oracle WebLogic Server as well as the Oracle Management Service. Do not provide a remote host or a load balancer virtual host in this field. Do not enter an IP address. Do not use underscores in the name. Short names are allowed, but you will see a warning, so Oracle recommends that you enter a fully qualified domain name instead.<br>If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host. |

#### 4.4.2.2 Running the Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager Cloud Control, log in as a *root* user in a new terminal and run the following scripts:

- If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the Management Agent home.

  For example, if the inventory location specified in the `oraInst.loc` file is `$HOME/oraInventory`, then run the following command:

  ```
  $HOME/oraInventory/oraInstRoot.sh
  ```

> **Note:** If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:
>
> ```
> /usr/local/bin/sudo $HOME/oraInventory/oraInstRoot.sh
> ```

- Run the `allroot.sh` script from the OMS home:

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

> **Note:** If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:
>
> ```
> /usr/local/bin/sudo $<OMS_HOME>/allroot.sh
> ```

#### 4.4.2.3 Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode

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/new_install.rsp
   ```

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

2. Edit the response file and enter appropriate values for the variables described in Table 4–3.

3. Configure the software binaries by invoking the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows) passing the response you edited in the previous step:

   ```
   $<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh -silent
   -responseFile <absolute_path>/new_install.rsp [-invPtrLoc <absolute_
   path_to_inventory_directory>]
   ```

**Note:**

- While installing the software binaries as described in Section 4.4.2.1, if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
- The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
- For information about the additional, advanced options you can pass while invoking the script, refer to Section 4.4.1.3.1.
- The only way to configure a software-only installation is to run the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows). DO NOT run the individual configuration assistants to configure a software-only installation. If you want to run the individual configuration assistants to configure the installation for some reason, then contact Oracle Support.
- If you have already configured a software-only installation (the Oracle home) using the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows), then DO NOT try to reconfigure it—either using the script or using the individual configuration assistants.
- If you connect to a database instance that was created using the database template offered by Oracle, then you will be prompted that the database parameters need to be modified to suit the deployment size you selected. This is because the templates are essentially designed for simple installation, and the database parameters are set as required for simple installation. Since it is used for advanced installation, the parameters must be set to different values. You can confirm the message to proceed further. The installation wizard will automatically set the parameters to the required values.

**Note:**

- If a prerequisite check fails reporting a missing package, then make sure you install the required package, and retry the installation. The installer validates the package name as well as the version, so make sure you install the packages of the minimum versions mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. To understand the logic the installer uses to verify these packages, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and rerun the configuration assistant. For more information, see Appendix J.

#### 4.4.2.3.1 Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode

Table 4–3 describes what variables you must edit and how you must edit them in the `new_install.rsp` file for configuring the software binaries.

*Table 4–3 Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| WLS_ADMIN_SERVER_USERNAME | String | Yes | By default, `weblogic` 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 | String | Yes | Enter a password for the WebLogic user account.<br>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 | String | Yes | Confirm the password for the WebLogic user account. |
| NODE_MANAGER_PASSWORD | String | Yes | 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.<br>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 | String | Yes | Confirm the password for the node manager user account. |
| ORACLE_INSTANCE_HOME_LOCATION | String | Yes | By default, `gc_inst` is considered as the OMS Instance Base directory for storing all OMS-related configuration files. Enter the absolute path to a location outside the middleware home leading up to the directory name.<br>For more information about this location, see Section 2.3.3. |

*Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| CONFIGURE_ORACLE_SOFTWARE_LIBRARY | Boolean | No | If you want to configure the Software Library at the time of installation, set this parameter to `TRUE`. Otherwise, set it to `FALSE`.<br>Even if you do not configure it at the time of installation, your installation will succeed, and you can always configure it later from the Enterprise Manager Cloud Control Console. However, Oracle recommends that you configure it at the time of installation so that it is automatically configured by the installer, thus saving your time and effort. |
| SOFTWARE_LIBRARY_LOCATION | String | Yes | If you have set `CONFIGURE_ORACLE_SOFTWARE_LIBRARY` to `TRUE`, then enter the absolute path leading up to a unique directory name on the OMS host where the Software Library can be configured. Ensure that the location you enter is a mounted location on the OMS host, and is placed outside the Middleware Home. Also ensure that the OMS process owner has read/write access to that location. Configuring on a mounted location helps when you install additional OMS instances as they will require read/write access to the same *OMS Shared File System* storage location. |

***Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| DATABASE_HOSTNAME | String | Yes | Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores.<br>For example, `"example.com"`.<br>If you have already created a database instance with a preconfigured Management Repository using the database templates offered by Oracle, then provide details about that database instance.<br>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.<br>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.<br>However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command:<br>`$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conndesc "(DESCRIPTION= (ADDRESS_LIST=(FAILOVER=ON) (ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521)) (ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=EMREP)))" -repos_user sysman`<br>If your Oracle RAC database 11.2 or higher is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.<br>**Note:** If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for the `SYSMAN_PASSWORD` parameter. |
| LISTENER_PORT | String | Yes | Enter the listener port to connect to the existing database.<br>For example, `"1521"`. |

*Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| SERVICENAME_ OR_SID | String | Yes | Enter the service name or the system ID (SID) of the existing database.<br>For example, "orcl". |
| SYS_PASSWORD | String | Yes | Enter the SYS user account's password. |
| SYSMAN_ PASSWORD | String | Yes | Enter a password for creating a SYSMAN user account. This password is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.<br>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.<br>**Note:** If you connect to a database instance that was created using the database template offered by Oracle, then note that the password assigned to the user accounts SYSMAN_MDS, SYSMAN_APM, and SYSMAN_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter for this parameter. |
| SYSMAN_ CONFIRM_ PASSWORD | String | Yes | Confirm the SYSMAN user account's password. |

***Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| DEPLOYMENT_SIZE | String | Yes | Set one of the following values to indicate the number of targets you plan to monitor, the number of Management Agents you plan to have, and the number of concurrent user sessions you plan to have.<br>■ **SMALL,** to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions<br>■ **MEDIUM,** to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions<br>■ **LARGE,** to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions.<br>For example, `"MEDIUM"`.<br>If the database you are connecting to is a database instance created with a preconfigured Management Repository using the database templates offered by Oracle, then make sure the deployment size you set here matches with the deployment size you selected on the Step 2 of 12: Database Templates screen of Oracle Database Configuration Assistant (DBCA) while creating the database instance.<br>If you want to select a deployment size different from the deployment size you had selected while creating the database instance using DBCA, then do one of the following:<br>■ Create another database instance with a template for the desired deployment size, then return to this response file and set the same deployment size to this parameter. For instructions to create a database instance with an Oracle-supplied template, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>■ In the database instance you have created, fix the parameters to support the deployment size you want to set here in the response file. To automatically fix the database parameters using Oracle-supplied SQL scripts, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |

*Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode*

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| MANAGEMENT_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to the location where the data file for management tablespace (`mgmt.dbf`) can be stored. Ensure that the specified path leads up to the file name.<br>For example:<br>- If the database is on a file system, then the path must look like `"/u01/oracle/prod/oradata/mgmt.dbf"`.<br>- If the database is on Automatic Storage Management (ASM), then the path must look like `"+<disk_group1>/prod/oradata/mgmt.dbf"`, where `disk_group1` is a diskgroup created on ASM and prod is the Service ID (SID).<br>- If the database is on a raw device, then the path must look like `"</dev/raw1>/prod/oradata/mgmt.dbf"`, where `/dev/raw1` is the raw device and prod is the SID.<br>Enterprise Manager Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data. |
| CONFIGURATION_DATA_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to the location where the data file for configuration data tablespace (`mgmt_ecm_depot1.dbf`) can be stored. Ensure that the specified path leads up to the file name.<br>For example, `"/home/john/oradata/mgmt_ecm_depot1.dbf"`.<br>Enterprise Manager Cloud Control requires this data file to store configuration information collected from the monitored targets. |

***Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| JVM_DIAGNOSTICS_TABLESPACE_LOCATION | String | Yes | Enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (`mgmt_deepdive.dbf`) can be stored. Ensure that the specified path leads up to the file name.<br>For example, `"/home/john/oradata/mgmt_deepdive.dbf"`.<br>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP). |
| AGENT_REGISTRATION_PASSWORD | String | Yes | Enter a password to secure the communication between the OMS and the Management Agents. Note that you have to provide the same registration password for securing your Management Agents. |
| AGENT_REGISTRATION_CONFIRM_PASSWORD | String | Yes | Confirm the agent registration password. |
| STATIC_PORTS_FILE | String | Yes | By default, ports described in Section 2.1.10 are honored. If you want to accept the default ports, then leave this field blank.<br>If you want to use custom ports, then enter the absolute path to the `staticports.ini` file that lists the custom ports to be used for the installation. |

***Table 4–3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager 12c Release 5 (12.1.0.5) Software Using the Software-Only Method in Silent Mode***

| Parameter | Data Type | Double Quotes Required for Value? | Description |
|---|---|---|---|
| PLUGIN_SELECTION | | | 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.<br>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 plug-in IDs for this variable.<br>For example,<br>`PLUGIN_SELECTION={"oracle.sysman.empa","oracle.sysman.vt"}`<br>If you want to install any plug-in that is not available in the software kit, then do the following:<br>1. Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location:<br>`http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html`<br>2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded.<br>3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins:<br>`./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>` |

#### 4.4.2.4 Performing Postconfiguration Tasks After Configuring the Enterprise Manager Cloud Control 12c Release 5 (12.1.0.5) Software Binaries in Silent Mode

Perform the post-install steps as described in the chapter on installing Enterprise Manager system that is available in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

# Part III

# Installing Additional Oracle Management Service

This part contains the following chapters:

# 5

# Installing Additional Oracle Management Services in Silent Mode

Oracle recommends you to use the Add Management Service deployment procedure to install an additional Oracle Management Service (OMS). The Add Management Service deployment procedure offers a GUI-rich, interactive way of installing an additional OMS. For instructions, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

However, if you have any security restrictions or audit demands in your environment, or if you are not permitted to use Oracle credentials to log in over the network for installation, then follow these steps to manually install an additional OMS in silent, non-interactive mode.

> **WARNING: Do not install Enterprise Manager Cloud Control 12c on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.**

1. If Oracle Software Library (Software Library) is configured on the main OMS, which comes with Enterprise Manager Cloud Control, then do the following:

   - **On Unix Platforms:** Ensure that Software Library is read-write accessible from the remote host where you plan to install the additional OMS.

   - **On Microsoft Windows Platforms:** If you do not have an option to share or mount the Software Library, then copy the Software library from the main, source OMS host to the destination host where you plan to install the additional OMS.

   In this procedure, for easy understanding, the OMS that comes with Enterprise Manager Cloud Control is referred to as the *first OMS*, and the additional OMS you install is referred to as the *additional OMS*.

2. On the remote host, perform a software-only installation of the additional OMS as described in Section 4.4.1.

**Note:**

- Ensure that you install the software binaries as the same user as the one used for installing the first OMS. You must be able to access the Software Library files.
- Ensure that you install the software binaries in the same middleware location as that of the first OMS.
- At the end of the software-only installation, do NOT run the `ConfigureGC.sh` (for Unix platforms) or `ConfigureGC.bat` script (for Microsoft Windows) as prompted by the installer. That file must be run only when you are performing a fresh installation.

3. Deploy the plug-ins:

   - **In GUI Mode (using the installer screen)**

     Invoke the `PluginInstall.sh` script from the following location:

     ```
     $<OMS_HOME>/sysman/install/PluginInstall.sh
     ```

     On the Plug-In Deployment screen, select the optional plug-ins you want to install.

     The screen displays only those plug-ins that were available in the software kit (DVD, downloaded software) you used in the previous step for installing the software binaries.

     The pre-selected rows on this screen are mandatory plug-ins that will be installed by default. Select the optional ones you want to install.

   - **In Silent Mode (command line):**

     Invoke the `PluginInstall.sh` script from the following location:

     ```
     $<OMS_HOME>/sysman/install/PluginInstall.sh -silent PLUGIN_
     SELECTION="{PLUGIN_ID1,PLUGIN_ID2}"
     ```

     For example,

     ```
     $<OMS_HOME>/sysman/install/PluginInstall.sh -silent PLUGIN_
     SELECTION="{oracle.sysman.emfa,oracle.sysman.vt}"
     ```

**Note:**

- On Microsoft Windows, run `PluginInstall.bat.`
- Ensure that you select the same set of plug-ins as the ones on the source OMS (or first OMS).

  To identify the plug-ins installed on the source OMS (or first OMS), follow these steps:

  1. Connect to the Management Repository and run the following SQL query to retrieve a list of plug-ins installed:

     ```
     SELECT epv.plugin_id, epv.version, epv.rev_
     version FROM em_plugin_version epv, em_
     current_deployed_plugin ecp WHERE epv.plugin_
     type NOT IN ('BUILT_IN_TARGET_TYPE',
     'INSTALL_HOME') AND ecp.dest_type='2' AND
     epv.plugin_version_id = ecp.plugin_version_id
     ```

  2. Make a note of the additional plug-ins you installed.

- To install the additional plug-ins that are installed on the source OMS (or first OMS), or to install any additional plug-ins that are not in the software kit you used for installing the binaries, follow these steps:

  1. Manually download the plug-ins from the Enterprise Manager Download page on OTN, and store them in an accessible location.

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

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

     **In GUI Mode (using the installer screen):**

     ```
     $<OMS_HOME>/sysman/install/PluginInstall.sh
     -pluginLocation <absolute_path_to_plugin_
     software_location>
     ```

     The Plug-In Deployment screen displays a list of plug-ins that were available in the software kit as well as the downloaded plug-ins available in this custom location. You can choose the ones you want to install.

     **In Silent Mode (command line):**

     ```
     $<OMS_HOME>/sysman/install/PluginInstall.sh
     -silent PLUGIN_SELECTION="{PLUGIN_ID1,PLUGIN_
     ID2}"-pluginLocation <absolute_path_to_
     plugin_software_location>
     ```

4. On the additional OMS, apply all the patches you applied on the first OMS so that both OMS instances are identical and are in sync. Patches include patches that

modified the Enterprise Manager system, the Software Library, the OMS files, the Management Repository, and so on.

To identify the patches you applied on the first OMS, run the following commands from the platform home:

```
$<Platform Home>/OPatch/opatchauto lspatches
```

This command displays the installed patches and Oracle home relationships. Map the installed patches to the patch `.zip` files on My Oracle Support site (`https://support.oracle.com/`). Download the files and unzip the archives on the additional OMSs. If patches are already available in the file system or a shared area, reuse those patches to apply it on other OMSs.

> **Note:** For more details on installed patches in the platform, and Plug-in homes, run the command `$ORACLE_HOME/OPatch/opatch lsinventory -details -oh <desired home path>`.

To apply the patches, run the following commands:

- For each system patch:

  ```
  <Platform Home>/OPatch/opatchauto apply <patch location> -bitonly
  -oh <Platform Home> -invPtrLoc <Platform Home>/oraInst.loc
  ```

  ```
  <Platform Home>/OPatch/opatchauto commit -id 17513525 -oh <Platform
  Home> -invPtrLoc <Platform Home>/oraInst.loc
  ```

  > **Note:** A patch is a system patch if it has a `<system patch location>/bundle.xml` file. The system patch ID is the top level directory patch ID number. This ID is also available in the `<System patch location>/bundle.xml` file. For example, `<system_patch_bundle_xml type_version="2.0" bundle_type="ENGSYSTEM" patch_abstract="sample System Patch description" patch_id="1111115">` clearly indicates the patch ID as 1111115.

- For each one-off patch specifically for the platform homes:

  ```
  <Platform Home>/OPatch/opatch  napply <one-off location>  -oh
  <Platform Home> -invPtrLoc <Platform Home>/oraInst.loc
  ```

5. Export the configuration details from the first OMS. To do so, run the following command from the Oracle home of the first OMS, and pass the location where the configuration details can be exported as a file.

   ```
   $<OMS_HOME>/bin/emctl exportconfig oms -dir <absolute_path_to_
   directory>
   ```

6. Copy the exported configuration details file from the first OMS host to the additional OMS host.

7. If the additional OMS is being installed using an alias host name, then set the `ORACLE_HOSTNAME` environment variable to the alias host name.

8. Recover the configuration details onto the additional OMS. To do so, run the following command from the Oracle home of the additional OMS:

   ```
   $<OMS_HOME>/bin/omsca recover -ms -backup_file <absolute_path_to_the_
   file_copied_in_step4> [-AS_HTTPS_PORT <port> -MSPORT <port> -MS_HTTPS_
   ```

```
PORT <port> -EM_NODEMGR_PORT <port> -EM_UPLOAD_PORT <port> -EM_UPLOAD_
HTTPS_PORT <port> -EM_CONSOLE_PORT <port> -EM_CONSOLE_HTTPS_PORT <port>
-config_home <absolute_path_to_instance_dir> -EM_INSTANCE_HOST <second_
oms_host_name>] -EM_BIP_PORT <port> -EM_BIP_HTTPS_PORT <port>
```

For example,

```
$<OMS_HOME>/bin/omsca recover -ms -backup_file
/opt/oracle/product/backup/opf_ADMIN_20120504_031016.bka -AS_HTTPS_PORT
7101 -MSPORT 7202 -MS_HTTPS_PORT 7301 -EM_NODEMGR_PORT 7403 -EM_UPLOAD_
PORT 4889 -EM_UPLOAD_HTTPS_PORT 4900 -EM_CONSOLE_PORT 7788 -EM_CONSOLE_
HTTPS_PORT 7799 -config_home /opt/oracle/product/omsmdw/gc_inst -EM_
BIP_PORT 9701 -EM_BIP_HTTPS_PORT 9702 -EM_INSTANCE_HOST example.com
```

> **Note:** If the additional OMS is being installed using an alias host name, then set the `EM_INSTANCE_HOST` parameter to the alias host name that is defined in the `/etc/hosts` file on all the OMS instances at this site.

9. *(Applicable only if you do not already have a Management Agent on the host)* Configure the Management Agent on the additional OMS host by running the following command from the OMS home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<middleware_
home>/agent OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_port> AGENT_
REGISTRATION_PASSWORD=<password> -configOnly
```

> **Note:**
>
> - If you have a Server Load Balancer (SLB) configured, then directly enter the host name and the port number of the SLB for the `OMS_HOST` and `EM_UPLOAD_PORT` parameters. If an SLB is not configured, then enter the host name and the secure upload port of the first OMS for the `OMS_HOST` and `EM_UPLOAD_PORT` parameters.
> - If the additional OMS is being installed using an alias host name, then add the `ORACLE_HOSTNAME=<alias host name>` parameter to the command and set the parameter to the alias host name that is defined in the `/etc/hosts` file on all the OMS instances at this site.

10. Deploy the required plug-ins on the Management Agent.

    For information about deploying plug-ins, refer to the section *Deploying Plug-Ins on Oracle Management Agent* in the chapter *Managing Plug-Ins,* in the *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

11. Import the trusted certificate on the additional OMS host, where you configured the Management Agent as described in Step (8). When prompted for a password, enter `welcome`.

```
$<AGENT_HOME>/bin/emctl secure add_trust_cert_to_jks
```

12. Review and perform the applicable steps outlined in the postinstallation tasks section of *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

13. Manually discover the Oracle WebLogic Server target.

a. Ensure that both the first and the additional OMS instances are up and running.

b. In the Cloud Control console, from the **Targets** menu, select **All Targets.**

c. On the All Targets page, search and click **/EMGC_GCDomain/GCDomain/.**

d. On the EMGC_GCDomain home page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain.**

e. On the Refresh WebLogic Domain page, click **Add / Update Targets,** and follow the steps guided by the wizard.

   Enterprise Manager Cloud Control refreshes the WebLogic Domain and discovers the second managed server on the additional OMS host.

For information about discovering the other targets, refer to the chapter *Adding Targets* in the *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

For configuring the shared Oracle Software Library location and the Server Load Balancer, refer to *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

# Part IV

# Installing Oracle Management Agent

This part describes the different ways of installing Oracle Management Agent. In particular, this part contains the following chapters:

# 6 Installing Oracle Management Agent in Silent Mode

This chapter describes how you can install Oracle Management Agent (Management Agent) in silent mode. In particular, this chapter covers the following:

## 6.1 Overview of Installing a Management Agent in Silent Mode

Installing a Management Agent in silent mode is only an alternative to installing it using the Add Host Targets Wizard. While the Add Host Targets Wizard requires you to use its GUI-rich interview screens for providing all installation details, the silent mode requires you to use a response file for providing installation details and deployment scripts to install Management Agents on hosts.

Installing in silent mode is useful when you want to install an additional Management Agent on a destination host from the destination host itself, without using the Add Host Targets Wizard.

You can install Management Agents in silent mode using the following methods:

**Using the AgentPull Script**

In this method, you do not have to use EM CLI to download the Management Agent software onto the remote destination host before executing the script to install the Management Agent. This method supports only a few additional parameters, and is ideal for a basic Management Agent install.

**Using the agentDeploy Script**

In this method, you must use EM CLI to download the Management Agent software onto the remote destination host before executing the script to install the Management Agent. You can either choose to use EM CLI from the OMS host, or from the remote destination host. If you choose to use EM CLI from the OMS host, you must transfer the downloaded Management Agent software to the remote destination host before executing the script to install the Management Agent. This method supports many additional parameters, and is ideal for a customized Management Agent install.

**Using the RPM File**

In this method, you obtain the `.rpm` file using EM CLI on the OMS host, then transfer the file to the remote destination host before running the file to install the Management Agent. Using the `.rpm` file, you can also choose to install a Management Agent while provisioning an operating system on a bare metal host. For more information, see the *Oracle Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching*. This guide is available in the Enterprise Manager documentation library at:

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

**Note:**

- The Management Agent `.rpm` file can be obtained using EM CLI only for Linux x86 and Linux x86-64 platforms.
- For Enterprise Manager 12*c* (12.1.0.x), installing a Management Agent by downloading the Management Agent `.rpm` file from Oracle Technology Network (OTN) is not supported.

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
    |_____core
         |_____12.1.0.5.0
    |_____plugins
    |_____plugins.txt
    |_____plugins.txt.status
    |_____agent_inst
    |_____sbin
    |_____agentimage.properties
```

**Note:**

- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide.*

  When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.
- *(For Microsoft Windows hosts)* If you upgrade a 12.1.0.x Management Agent and you want to install another Management Agent on the same host, which points to a different OMS, ensure that you specify the `s_agentSrvcName` parameter while installing the Management Agent, as described in Section 6.4.6.

## 6.2 Before You Begin Installing a Management Agent in Silent Mode

Before you begin installing a Management Agent in silent mode, keep these points in mind:

- You can install a Management Agent on only one host at a time by using the silent methods. Therefore, use this approach when you want to install a Management Agent on only a few hosts.

- The Management Agent software for the platform of the host on which you want to install a Management Agent must be downloaded and applied, using Self Update. Only the Management Agent software for the OMS host platform is downloaded and applied by default. The Management Agent software contains the core binaries required for installation, the response file to be edited and passed, and the `agentDeploy.sh` script (`agentDeploy.bat` for Microsoft Windows).

  For information on how to download and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

- In Enterprise Manager Cloud Control 12*c* Release 5 (12.1.0.5.0), you can save the Management Agent one-off patches that you want to apply on a particular version of the Management Agent software, such that these patches are automatically applied on the software whenever a new Management Agent of the same version is deployed, or an old Management Agent is upgraded to that version.

  For information on how to do this, see Appendix D.

  Also, you can apply one-off patches on a plug-in and create a custom patched plug-in, such that this custom patched plug-in is deployed on all the new Management Agents that you deploy, and all the old Management Agents that you upgrade.

  For information on how to do this, see *Oracle Enterprise Manager Cloud Control Administration Guide.*

- From Enterprise Manager Cloud Control 12*c* Release 5 (12.1.0.5), parallel deployment of Management Agents using the `AgentPull.sh` script (`AgentPull.bat` for Microsoft Windows) is supported. This enables you to deploy Management Agents on multiple hosts, at the same time (in a parallel manner), using the `AgentPull.sh` or `AgentPull.bat` script.

- If you want to install a Management Agent on a Microsoft Windows host in silent mode, ensure that you execute the `AgentPull.bat` or `agentDeploy.bat` script from the default command prompt, which is `cmd.exe,` and not from any other command prompt.

- You cannot run any preinstallation or postinstallation scripts as part of the installation process. You can run them manually before or after the installation.

- By default, installing a Management Agent in silent mode configures only the following types of plug-ins:

  - All discovery plug-ins that were configured with the OMS from where the Management Agent software is being deployed.
  - Oracle Home discovery plug-in
  - Oracle Home monitoring plug-in

- Upgrading a lower release of Solaris by applying a kernel patch or a patch bundle is not equivalent to installing the actual Solaris 5.10 Update 9 image. Oracle Management Agent 12c Release 5 (12.1.0.5) was built, tested, and certified on a minimum update version of Solaris 5.10 Update 9, so Oracle recommends that you install Oracle Management Agent only on Solaris 5.10 Update 9, and not on any release that was upgraded using patches.

## 6.3 Prerequisites for Installing a Management Agent in Silent Mode

Before installing a Management Agent in silent mode, ensure that you meet the following prerequisites:

***Table 6–1 Prerequisites for Installing Oracle Management Agent in Silent Mode***

| 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 *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| Operating System Requirements | Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on *My Oracle Support*.<br>To access the Enterprise Manager certification matrix, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>For information about platforms receiving future support, refer to *My Oracle Support* note 793512.1. |
| File System Requirements | Ensure that the file system mounted on the destination host does not permit buffered writes. |
| File Descriptor Requirements | ■ Ensure that the maximum user process limit is set to 13312 or greater.<br>To verify the current value set, run the following command:<br>`ulimit -u`<br>If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.<br>■ Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.<br>To verify the current value set, run the following commands:<br>**For Soft Limit:**<br>`/bin/sh -c "ulimit -n"`<br>**For Hard Limit:**<br>`/bin/sh -c "ulimit -Hn"`<br>If the current value is not 4096 or greater, then as a *root* user, update the `/etc/security/limits.conf` file with the following entries:<br>`<UID> soft nofile 4096`<br>`<UID> hard nofile 16384` |
| Package Requirements | Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>If you choose to install a Management Agent using a `.rpm` file, ensure that the `rpm-build` package is installed on the host. To verify this, run the following command:<br>`rpm -qa \| grep rpm-build` |
| cURL Utility Requirements<br>(For installing using the `AgentPull` script only) | Ensure that you install the cURL utility on the destination host.<br>You can download the cURL utility from the following URL:<br>`http://curl.haxx.se/dlwiz/?type=bin`<br>**Note:** For destination hosts running on Microsoft Windows, Oracle recommends that you install cURL in `c:\`. |

***Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode***

| Requirement | Description |
|---|---|
| ZIP and UNZIP Utility Requirements | Ensure that the ZIP and the UNZIP utilities are present on the destination host.<br>The ZIP utility must be of version 3.0 2008 build or higher.<br>The UNZIP utility must be of version 6.0 or higher. |
| 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.<br>For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>**Note:** If your enterprise has a policy against installing Management Agents using the OMS install operating system user account, you can use a different operating system user account to install Management Agents. However, ensure that the user account you use and the OMS install user account belong to the same primary group. |
| /etc/hosts File Requirements | Ensure that the `/etc/hosts` file on the host has the IP address, the fully qualified name, and the short name in the following format:<br>`172.16.0.0 example.com mypc` |
| Time Zone Requirements | Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:<br>`echo $TZ`<br>If the time zone displayed is incorrect, run the following commands, before running the `agentDeploy.sh` or `agentDeploy.bat` scripts, to set the correct time zone:<br>■ For Korn shell:<br>`TZ=<value>`<br>`export TZ`<br>■ For Bourne shell or Bash shell:<br>`export TZ=<value>`<br>■ For C shell:<br>`setenv TZ <value>`<br>For example, in the Bash shell, run the following command to set the time zone to America/New_York:<br>`export TZ='America/New_York'`<br>To set the time zone on a destination host that runs on Microsoft Windows, from the **Start** menu, select **Control Panel.** Click **Date and Time,** then select the **Time Zone** tab. Select your time zone from the displayed drop down list.<br>To view a list of the time zones you can use, access the `supportedtzs.lst` file present in the `<AGENT_HOME>/sysman/admin` directory of the central agent (that is, the Management Agent installed on the OMS host).<br>**Note:** If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the host after installing the Management Agent. For information on setting time zones post install, refer Section 6.5. |

*Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode*

| Requirement | Description |
|---|---|
| PATH Environment Variable Requirements<br>(For installing using the `AgentPull` script only) | Ensure that the location of `zip` and `unzip` is part of the `PATH` environment variable.<br>For example, if `zip` and `unzip` are present in `/usr/bin,` then `/usr/bin` must be part of the `PATH` environment variable. |
| Path Validation Requirements | Validate the path to all command locations. For more information, refer to the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| `CLASSPATH` Environment Variable Requirements | Unset the `CLASSPATH` environment variable. You can always reset the variable to the original value after the installation is complete. |
| Port Requirements | Ensure that the default ports described in Section 2.1.10.1 are free. |
| Temporary Directory Space Requirements | Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.<br>By default, the temporary directory location set to the environment variable `TMP` or `TEMP` is honored. If both are set, then TEMP is honored. If none of them are set, then the following default values are honored: `/tmp` on UNIX hosts and `c:\Temp` on Microsoft Windows hosts. |
| /var/tmp Requirements<br>(For installing using the `.rpm` file only) | Ensure that the `/var/tmp` directory has at least 700 MB of free space. |
| /usr/lib/oracle Requirements<br>(For installing using the `.rpm` file only) | Ensure that the `/usr/lib/oracle` directory exists and has at least 2 GB of free space. If it does not exist, create it, and ensure that the install user has write permissions on it. |
| Agent Base Directory Requirements | Ensure the following:<br>■ The agent base directory is empty and has at least 1 GB of free space.<br>■ The directory name does not contain any spaces.<br>■ The install user owns the agent base directory. The agent base directory and the parent directories of the agent base directory have read, write, and execute permissions for the install user. Ensure that the install user or the *root* user owns all the parent directories of the agent base directory, and that the parent directories have read and execute permissions for the install user group and all the other users. Also, ensure that the *root* user owns the root directory.<br>For example, if the agent base directory is `/scratch/OracleHomes/agent`, and *oracle* is the install user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or the *root* user, and the root directory (/) must be owned by the *root* user.<br>■ If the agent base directory is mounted, it is mounted with the `setuid` option turned on. |
| Agent Instance Home Requirements<br>(For installing using the `agentDeploy` script only) | Ensure that the agent instance home location you specify in the response file is empty. |

*Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode*

| Requirement | Description |
|---|---|
| Permission Requirements | - Ensure that you have *write* permission in the agent instance home.<br>- Ensure that you have *write* permission in the temporary directory. |
| Installing User Requirements | If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group, and have *read* and *write* permissions on the inventory directory.<br>For example, if the inventory owner is *abc* and the user installing the Management Agent is *xyz*, then ensure that *abc* and *xyz* belong to the same group, and they have read and write access to the inventory. |
| Central Inventory (oraInventory) Requirements | - Ensure that you allocate 100 MB of space on all destination hosts for the Central Inventory.<br>- Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all destination hosts.<br>If you do not have these permissions on the default inventory (typically in the location mentioned in the `/etc/oraInst.loc` file) on any destination host, then ensure that you enter the path to an alternative inventory location using the `INVENTORY_LOCATION` or `-invPtrLoc` arguments as described in Table 6–6. Note that these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms. |
| Agent User Account Permissions and Rights<br>(For installing using the `AgentPull` or `agentDeploy` scripts only) | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the agent user account has permissions and rights to perform the following:<br>- Act as part of the operating system.<br>- Adjust memory quotas for a process.<br>- Replace process level token.<br>- Log on as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>**1.** Launch the Local Security Policy.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Policy**.<br>**2.** In the Local Security Policy window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**. |
| Permissions for cmd.exe<br>(For installing using the `AgentPull` or `agentDeploy` scripts only) | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that you grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` |
| Runtime Library File Requirements | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the `Msvcp71.dll` and `Msvcr71.dll` runtime library files are present in `c:\windows\system32`. |

## 6.4 Installing a Management Agent in Silent Mode

This section describes the actions involved in installing a Management Agent in silent mode. It consists of the following:

- Installing a Management Agent Using the AgentPull Script
- Installing a Management Agent Using the agentDeploy Script
- Installing a Management Agent Using the RPM File
- Installing a Management Agent on a Virtual Host
- Response File Parameters for Installing a Management Agent in Silent Mode Using the AgentPull Script
- Response File Parameters for Installing a Management Agent in Silent Mode Using the agentDeploy Script
- Response File Parameters for Installing a Management Agent in Silent Mode Using an RPM File
- Options Supported by the AgentPull Script
- Options Supported by the agentDeploy Script
- About the Contents of the Downloaded Management Agent Software

---

**Important:** If the OMS host is running on Microsoft Windows, and the OMS software was installed in a drive other than `C:\`, then update the `SCRATCH_PATH` variable in `$OMS_HOME\oui\prov\resources\ssPaths_msplats.properties`.

For example, if the OMS software was installed in `D:\`, ensure that you update the `SCRATCH_PATH` variable to `D:\tmpada`

---

### 6.4.1 Installing a Management Agent Using the AgentPull Script

To install a Management Agent using the `AgentPull` script, follow these steps:

1. Acquiring the Management Agent Software.
2. Installing the Management Agent Using the AgentPull Script.

---

**Important: To install a Management Agent using the AgentPull script, you do not need to download the Management Agent software onto the destination host. The AgentPull script performs this action automatically.**

---

#### 6.4.1.1 Acquiring the Management Agent Software

1. If the destination host runs on UNIX, access the following URL from the host:

   ```
   https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage
   ```

   If the destination host runs on Microsoft Windows, access the following URL from the host:

   ```
   https://<OMS_HOST>:<OMS_PORT>/em/install/getAgentImage?script=bat
   ```

   Save the file as `AgentPull.sh` (`AgentPull.bat` for Microsoft Windows) to a temporary directory, say `/tmp` (`c:\temp` for Microsoft Windows).

> **Note:** You can also use the following command to obtain the `AgentPull.sh` script:
>
> ```
> curl "https://<OMS_HOST>:<OMS_
> PORT>/em/install/getAgentImage" --insecure -o AgentPull.sh
> ```
>
> To use this command, ensure that you have the cURL utility installed, as described in Table 6–1.

2. (Only for UNIX Operating Systems) Provide the execute permission to the `AgentPull.sh` script by running the following command:

   ```
   chmod +x <absolute_path_to_AgentPull.sh>
   ```

   For example, run the command `chmod +x /tmp/AgentPull.sh`.

3. Identify the platforms for which the Management Agent software is available on the OMS host. Run the `AgentPull.sh` script (`AgentPull.bat` for Microsoft Windows) specifying the `-showPlatforms` option to display the platforms for which the Management Agent software is available on the OMS host.

   ```
   <absolute_path_to_AgentPull.sh> -showPlatforms
   ```

   The following is a sample output of the command.

   ```
   Platforms Version
   Linux x86-64 12.1.0.5.0
   Microsoft Windows x64 (64-bit) 12.1.0.5.0
   IBM AIX on POWER Systems (64-bit) 12.1.0.5.0
   ```

   If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

   For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

   > **Note:** If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform,** Red Hat Enterprise Linux 4.x **64-bit platform,** or the SUSE Linux Enterprise 10 **64-bit platform,** ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

#### 6.4.1.2 Installing the Management Agent Using the AgentPull Script

1. If the destination host runs on UNIX, and the OMS host runs on Microsoft Windows, run the following command:

   ```
   dos2unix <absolute_path_to_AgentPull.sh>
   ```

   For example, run the command `dos2unix /tmp/AgentPull.sh`.

2. Create a response file (in any location on the destination host) specifying the parameters described in Table 6–2. Ensure that you do not name the response file `agent.rsp`.

   The following are the contents of a sample response file, `agent.properties`.

   ```
   LOGIN_USER=sysman
   LOGIN_PASSWORD=welcome
   ```

```
PLATFORM="Linux x86-64"
AGENT_REGISTRATION_PASSWORD=wel246come
```

If you want the script to ignore a particular response file parameter, specify a '#' before the parameter. For example, #VERSION.

3. Run the AgentPull.sh script (AgentPull.bat for Microsoft Windows) specifying the RSPFILE_LOC and AGENT_BASE_DIR parameters.

   ```
   <absolute_path_to_AgentPull.sh> RSPFILE_LOC=<absolute_path_to_
   responsefile> AGENT_BASE_DIR=<absolute_path_to_agentbasedir>
   ```

   For example, run the following command:

   ```
   /tmp/AgentPull.sh RSPFILE_LOC=/tmp/agent.properties AGENT_BASE_
   DIR=/scratch/agent
   ```

   The AgentPull.sh script (and AgentPull.bat) supports certain options, such as -download_only, which downloads the Management Agent software, but does not deploy the Management Agent. These supported options are described in Table 6–5.

   If you are installing a Management Agent on a Microsoft Windows host using AgentPull.bat, ensure that you execute AgentPull.bat from the default command prompt, which is cmd.exe, and not from any other command prompt.

   If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see Section B.3.

## 6.4.2 Installing a Management Agent Using the agentDeploy Script

You can install a Management Agent using the agentDeploy.sh or agentDeploy.bat script in the following ways:

- Using EM CLI from the Remote Destination Host
- Using EM CLI from the OMS Host

### 6.4.2.1 Using EM CLI from the Remote Destination Host

To install a Management Agent using the agentDeploy script, and EM CLI from the destination host, follow these steps:

1. **Acquiring the Management Agent Software and Downloading it onto the Destination Host Using EM CLI.**

   1. Set up EM CLI on the destination host.

      For information on how to set up EM CLI on a host that is not running the OMS, refer the Command Line Interface Concepts and Installation chapter of *Oracle Enterprise Manager Command Line Interface.*

   2. On the destination host, from the EM CLI install location, log in to EM CLI:

      ```
      <emcli_install_location>/emcli login -username=<username>
      ```

      For example,

      ```
      <emcli_install_location>/emcli login -username=sysman
      ```

      Specify the password when you are prompted for it.

**Note:** Ensure that the EM CLI log in user has the `ADD_TARGET` privilege.

3. Synchronize EM CLI:

   ```
   <emcli_install_location>/emcli sync
   ```

4. Identify the platforms for which the Management Agent software is available in Software Library:

   ```
   <emcli_install_location>/emcli get_supported_platforms
   ```

   This command lists all the platforms for which the Management Agent software is available in Software Library. The following is the sample output of the command.

   ```
   -----------------------------------------------
   Version = 12.1.0.5.0
   Platform Name = Linux x86-64
   -----------------------------------------------
   Version = 12.1.0.5.0
   Platform Name = Oracle Solaris on x86-64 (64-bit)
   -----------------------------------------------
   Version = 12.1.0.5.0
   Platform Name = HP-UX PA-RISC (64-bit)
   -----------------------------------------------
   ```

   If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

   For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

   **Note:** If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform,** Red Hat Enterprise Linux 4.x **64-bit platform,** or the SUSE Linux Enterprise 10 **64-bit platform,** ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

5. Download the Management Agent software from Software Library to a temporary directory on the destination host:

   ```
   <emcli_install_location>/emcli get_agentimage
   -destination=<download_directory> -platform="<platform>"
   -version=<version>
   ```

   For example,

   ```
   ./emcli get_agentimage -destination=/tmp/agentImage
   -platform="Linux x86-64" -version=12.1.0.5.0
   ```

---

**Important:** If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the destination host platform, then you must set the `ZIP_LOC` environment variable to the location of the ZIP utility. For example, if the ZIP utility is present in `/usr/bin/zip`, set `ZIP_LOC=usr/bin/zip`.

Also, ensure that the ZIP utility is of version 3.0 2008 build or higher.

If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the OMS host platform, then you must set the `ZIP_LOC` environment variable to `$OMS_HOME/bin/zip`, that is, the location of the ZIP utility on the OMS host.

---

**Note:** In the command, note the following:

- `-destination` is a directory on the destination host where you want the Management Agent software to be downloaded. Ensure that you have write permission on this location.
- `-platform` is the platform for which you want to download the software; this must match one of the platforms listed in the previous step for which the software is available in Software Library.
- `-version` is the version of the Management Agent software that you want to download; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.

---

The command downloads the core Management Agent software to the destination directory you entered. For example, for Linux x86-64, you will see the file `12.1.0.5.0_AgentCore_226.zip`. For information on the contents of this core software, see Section 6.4.10.

2. **Installing the Management Agent Using the agentDeploy Script.**

   1. On the destination host, extract the contents of the ZIP file using the unzip utility:

      ```
      unzip <software_zip_file_location> -d <software_extract_location>
      ```

      For example,

      ```
      unzip /tmp/agentImage/12.1.0.5.0_AgentCore_226.zip -d /tmp/agtImg
      ```

   2. Edit the response file `agent.rsp` as described in Table 6–3.

      ```
      <software_extract_location>/agent.rsp
      ```

      The following are the contents of a sample response file.

      ```
      OMS_HOST=example.com
      EM_UPLOAD_PORT=14511
      AGENT_REGISTRATION_PASSWORD=abc123
      AGENT_PORT=1832
      ```

      If you want the script to ignore a particular response file parameter, specify a '#' before the parameter. For example, `#AGENT_PORT`.

3. Invoke the deployment script and pass the response file:

   ```
   <software_extract_location>/agentDeploy.sh AGENT_BASE_
   DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<software_
   extract_location>/agent.rsp
   ```

   If a proxy is set up between the destination host and the OMS host, you must specify the `REPOSITORY_PROXYHOST` and `REPOSITORY_PROXYPORT` parameters in a properties file, then specify the `PROPERTIES_FILE` parameter while running `agentDeploy.sh` to install a Management Agent on the destination host:

   ```
   <software_extract_location>/agentDeploy.sh AGENT_BASE_
   DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_path_
   to_responsefile> PROPERTIES_FILE=<absolute_path_to_properties_file>
   ```

   For example, `/tmp/agtImg/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c RESPONSE_FILE=/tmp/agtImg/agent.rsp PROPERTIES_FILE=/tmp/agent.properties`

   The properties file you use must have the following format:

   ```
   REPOSITORY_PROXYHOST=<proxy_host_name>
   REPOSITORY_PROXYPORT=<proxy_port>
   ```

   **Note:**

   - Instead of passing a response file, you can choose to pass response file parameters explicitly while invoking the deployment script.

     The mandatory response file parameters are `OMS_HOST`, `EM_UPLOAD_PORT`, and `AGENT_REGISTRATION_PASSWORD`.

     For example,

     ```
     /tmp/agtImg/agentDeploy.sh AGENT_BASE_
     DIR=/scratch/agent12c OMS_HOST=example.com EM_UPLOAD_
     PORT=14511 AGENT_REGISTRATION_PASSWORD=2bornot2b
     ```

   - When you pass the arguments while invoking the deployment script, these values need not be given with double quotes. However, when you provide them in a response file, the values need to be in double quotes (except for the argument `b_startAgent`).

   - In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see Section 6.4.9.

   - If you are installing a Management Agent on a Microsoft Windows host using `agentDeploy.bat,` ensure that you execute `agentDeploy.bat` from the default command prompt, which is `cmd.exe,` and not from any other command prompt.

4. Run the root scripts after the install. For more information, see Section 6.5.

If you want to install a Management Agent on a physical host, and install another Management Agent on a virtual host that is installed on the physical host, ensuring that both the Management Agents use the same port for communication, follow these steps:

1. Install a Management Agent on the physical host. Stop the Management Agent.
2. Install a Management Agent on the virtual host. Stop the Management Agent.
3. Set `AgentListenOnAllNICs=false` in the `$<AGENT_HOME>/sysman/config/emd.properties` file. Ensure that you perform this step for both the Management Agents.
4. Start up both the Management Agents.

If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see Section B.3.

#### 6.4.2.2 Using EM CLI from the OMS Host

To install a Management Agent using the `agentDeploy` script, and EM CLI from the OMS host, follow these steps:

1. **Acquiring the Management Agent Software and Downloading it onto the OMS Host Using EM CLI.**

   1. On the OMS host, from the OMS home, log in to EM CLI. EM CLI is available by default with every OMS installation, so you need not install the client separately on the OMS host.

      ```
      $<OMS_HOME>/bin/emcli login -username=<username>
      ```

      For example,

      ```
      $<OMS_HOME>/bin/emcli login -username=sysman
      ```

      Specify the password when you are prompted for it.

      **Note:**

      - Ensure that the EM CLI log in user has the `ADD_TARGET` privilege.
      - If you have configured a load balancer for a multiple OMS setup, ensure that you run the EM CLI commands on one of the local OMS hosts, and not on the load balancer hosts.
      - If you have configured a load balancer for a multiple OMS setup, and you choose to use the EM CLI `setup` command, ensure that you pass the OMS host and port as parameters, and not the load balancer host and port.

        For example, `emcli setup -url=https://<OMS_HOST>:<OMS_PORT>/em -user=sysman -password=sysman`

   2. Synchronize EM CLI:

      ```
      $<OMS_HOME>/bin/emcli sync
      ```

   3. Identify the platforms for which the Management Agent software is available in Software Library:

      ```
      $<OMS_HOME>/bin/emcli get_supported_platforms
      ```

      This command lists all the platforms for which the Management Agent software is available in Software Library. The following shows the sample output of the command.

      ```
      -----------------------------------------------
      ```

```
Version = 12.1.0.5.0
Platform Name = Linux x86-64
---------------------------------------------------
Version = 12.1.0.5.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
---------------------------------------------------
Version = 12.1.0.5.0
Platform Name = HP-UX PA-RISC (64-bit)
---------------------------------------------------
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

**Note:** If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform,** Red Hat Enterprise Linux 4.x **64-bit platform,** or the SUSE Linux Enterprise 10 **64-bit platform,** ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

4. Download the Management Agent software from Software Library to a temporary directory on the OMS host:

```
$<OMS_HOME>/bin/emcli get_agentimage -destination=<download_
directory> -platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage -destination=/tmp -platform="Linux x86-64"
-version=12.1.0.5.0
```

**Important:** If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the OMS host platform, then you must set the `ZIP_LOC` environment variable to `$OMS_HOME/bin/zip`, which is the location of the ZIP utility on the OMS host.

If you use the `get_agentimage` EM CLI verb to download the Management Agent software for a platform different from the destination host platform, then you must set the `ZIP_LOC` environment variable to the location of the ZIP utility. For example, if the ZIP utility is present in `/usr/bin/zip`, set `ZIP_LOC=usr/bin/zip`.

Also, ensure that the ZIP utility is of version 3.0 2008 build or higher.

**Note:** In the command, note the following:

- `-destination` is a directory on the OMS host where you want the Management Agent software to be downloaded. Ensure that you have write permission on this location.

  If the destination directory is titled with two or more words separated by a space, then enclose the directory name with double quotes.

  For example, if the destination directory is titled `/tmp/linux agentimage`, then enter the value as `-destination="/tmp/linux agentimage"`
- `-platform` is the platform for which you want to download the software; this must match one of the platforms listed in the previous step for which the software is available in Software Library.
- `-version` is the version of the Management Agent software that you want to download; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.

The command downloads the core Management Agent software to the destination directory you entered. For example, for Linux x86-64, you will see the file `12.1.0.5.0_AgentCore_226.zip`. For information on the contents of this core software, see Section 6.4.10.

2. **Transferring the Management Agent Software to the Destination Host.**

   Transfer the downloaded ZIP file to a temporary directory (`/tmp`) on the destination host where you want to install the Management Agent. You can use any file transfer utility to transfer the file.

3. **Installing the Management Agent Using the agentDeploy Script.**

   Follow Step 2 mentioned in Section 6.4.2.1 to install the Management Agent.

## 6.4.3 Installing a Management Agent Using the RPM File

To install a Management Agent using a `.rpm` file, follow these steps:

1. Acquiring the Management Agent Software and Downloading the RPM File onto the OMS Host.
2. Transferring the RPM File to the Destination Host.
3. Installing the Management Agent Using the RPM File.

### 6.4.3.1 Acquiring the Management Agent Software and Downloading the RPM File onto the OMS Host

1. On the OMS host, from the OMS home, log in to EM CLI. EM CLI is available by default with every OMS installation, so you need not install the client separately on the OMS host.

   ```
   $<OMS_HOME>/bin/emcli login -username=<username>
   ```

   For example,

```
$<OMS_HOME>/bin/emcli login -username=sysman
```

Specify the password when you are prompted for it.

> **Note:** Ensure that the EM CLI log in user has the `ADD_TARGET` privilege.

2. Synchronize EM CLI:

```
$<OMS_HOME>/bin/emcli sync
```

3. Identify the platforms for which the Management Agent software is available in Software Library:

```
$<OMS_HOME>/bin/emcli get_supported_platforms
```

This command lists all the platforms for which the Management Agent software is available in Software Library. The following is the sample output of the command.

```
---------------------------------------------------
Version = 12.1.0.5.0
Platform Name = Linux x86-64
---------------------------------------------------
Version = 12.1.0.5.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
---------------------------------------------------
Version = 12.1.0.5.0
Platform Name = HP-UX PA-RISC (64-bit)
---------------------------------------------------
```

If the output lists the platform on which you want to install the Management Agent, then proceed to the next step. Otherwise, acquire and apply the Management Agent software for the required platform using Self Update.

For information on how to acquire and apply the Management Agent software for a platform using Self Update, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

> **Note:** If you want to install a Management Agent on a host that is running on the Oracle Enterprise Linux 4.x **64-bit platform,** Red Hat Enterprise Linux 4.x **64-bit platform,** or the SUSE Linux Enterprise 10 **64-bit platform,** ensure that the **32-bit version of the Management Agent software for the platform** is available in Software Library.

4. Download the `.rpm` file of the Management Agent from Software Library to a temporary directory on the OMS host:

```
$<OMS_HOME>/bin/emcli get_agentimage_rpm -destination=<download_
directory> -platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage_rpm -destination=/tmp/agentRPM -platform="Linux
x86-64" -version=12.1.0.5.0
```

In the command, note the following:

- `-destination` is a directory on the OMS host where you want the `.rpm` file to be downloaded. Ensure that you have write permission on this location.

- `-platform` is the platform for which you want to download the `.rpm` file; this must match one of the platforms listed in the previous step for which the software is available on the OMS host.
- `-version` is the version of the Management Agent for which you want to download the `.rpm` file; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.

The command downloads the `.rpm` file of the core Management Agent to the destination directory you entered. For example, `oracle-agt-12.1.0.5.0-1.0.i386.rpm`

Also, this command retrieves the Management Agent software, patches, and plug-ins present in the OMS home. For information on how to save Management Agent patches to the OMS home such that they are applied whenever a Management Agent is deployed, see Section D.1.

### 6.4.3.2 Transferring the RPM File to the Destination Host

1. Transfer the downloaded `.rpm` file to a temporary directory `(/tmp)` on the destination host where you want to install the Management Agent. You can use any file transfer utility to transfer the file.

### 6.4.3.3 Installing the Management Agent Using the RPM File

1. On the destination host, install the `.rpm` file as a *root* user to install the Management Agent:

```
rpm -ivh <download_directory>/<rpm_file>
```

For example,

```
rpm -ivh /tmp/oracle-agt-12.1.0.5.0-1.0.i386.rpm
```

**Note:** The following is the output of the command:

```
Preparing... ########################################### [100%]
Running the prereq
1:oracle-agt ########################################### [100%]
Follow the below steps to complete the agent rpm installation:
1. Edit the properties file: /usr/lib/oracle/agent/agent.properties
with the correct values
2. Execute the command /etc/init.d/oracle-agt RESPONSE_
FILE=<location_to_agent.properties>
```

When you use a `.rpm` file to install a Management Agent, the default agent base directory location is `/usr/lib/oracle/agent`. To install the Management Agent using a custom agent base directory location, run the following command as a *root* user:

```
rpm -ivh --relocate /usr/lib/oracle/agent=<custom_agent_base_directory_
location> <download_directory>/<rpm_file>
```

For example,

```
rpm -ivh --relocate /usr/lib/oracle/agent=/scratch/aime/agent
tmp/agent_rpm/oracle-agt-12.1.0.5.0-1.0.i386.rpm
```

When you use a `.rpm` file to install a Management Agent, the inventory location is always `<agent_base_directory>/oraInventory`. As the default agent base directory location is `/usr/lib/oracle/agent`, the default inventory location is

/usr/lib/oracle/agent/oraInventory. If you choose to install the Management Agent in a custom agent base directory location (using the --relocate option), say in /oem/agent, then the inventory location is /oem/agent/oraInventory.

2. Edit the agent.properties file as described in Table 6–4. The file is available in the following location:

```
/usr/lib/oracle/agent/agent.properties
```

3. Run the following command to complete the installation:

```
/etc/init.d/oracle-agt RESPONSE_FILE=<location_to_agent.properties>
```

   If the Management Agent install fails, diagnose the problem by viewing the Management Agent install logs. For information on the location of these logs, see Section B.3.

### 6.4.4 Installing a Management Agent on a Virtual Host

To install a Management Agent on a virtual host, follow these steps:

1. Follow the steps described in Section 6.4.2.1 or Section 6.4.2.2. While invoking the agentDeploy.sh or the agentDeploy.bat script, ensure that you specify the ORACLE_HOSTNAME parameter.

   For example, <software_extract_location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_path_to_response_file> ORACLE_HOSTNAME=<name_of_virtual_host>

   For more information about the ORACLE_HOSTNAME parameter, see Table 6–3.

2. If the virtual host is associated with a virtual Network Interface Controller (NIC), set AgentListenOnAllNICs=false in the $<AGENT_HOME>/sysman/config/emd.properties file, then run the following command:

```
$<AGENT_HOME>/bin/emctl reload
```

### 6.4.5 Response File Parameters for Installing a Management Agent in Silent Mode Using the AgentPull Script

Table 6–2 describes the mandatory parameters that you must include, and the optional parameters that you can include in the response file, while installing a Management Agent using the AgentPull script.

***Table 6–2 Creating a Response File for Installing Oracle Management Agent Using AgentPull Script***

| Parameter | Description |
|---|---|
| LOGIN_USER | *(Mandatory)* Enter the Enterprise Manager console login user name.<br>For example, LOGIN_USER=sysman |
| LOGIN_PASSWORD | *(Mandatory)* Enter the Enterprise Manager console login password.<br>For example, LOGIN_PASSWORD=welcome1 |
| PLATFORM | *(Mandatory)* Enter the platform for which you want to download the Management Agent software.<br>For example, PLATFORM="Linux x86-64"<br>**Note:** The value of this parameter must be in " ". |

***Table 6–2 (Cont.) Creating a Response File for Installing Oracle Management Agent Using AgentPull Script***

| Parameter | Description |
|---|---|
| AGENT_REGISTRATION_PASSWORD | *(Mandatory)* Enter a password for registering new Management Agents that join the Enterprise Manager system.<br>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.<br>For example, `AGENT_REGISTRATION_PASSWORD=Wel456come` |
| VERSION | *(Optional)* Enter the version of the Management Agent software you want to download.<br>For example, `VERSION=12.1.0.5.0`<br>If you do not specify this parameter, it is assigned the OMS version. |
| CURL_PATH<br>(For Microsoft Windows hosts only) | *(Optional)* Enter the absolute path of the installed cURL utility.<br>For example, `CURL_PATH=c:\Program Files\curl`<br>If you do not include this parameter, it is assigned the value `c:\`. |
| OMS_HOST | *(Optional)* Enter the OMS host name.<br>For example, `OMS_HOST=example.com` |
| EM_UPLOAD_PORT | *(Optional)* Enter the upload port (HTTP or HTTPS) for communicating with the OMS.<br>For example, `EM_UPLOAD_PORT=14511` |
| AGENT_INSTANCE_HOME | *(Optional)* Enter a directory location on the destination host where all Management Agent-related configuration files can be stored. For this parameter, you can do one of the following:<br>■ Leave it blank.<br>In this case, by default, an instance directory titled `agent_inst` is created in the agent installation base directory.<br>For example, if the installation base directory is `/john/oracle/`, then the instance directory is defaulted to `/john/oracle/agent_inst`<br>■ Enter the absolute path to a custom directory.<br>Although you can enter any location as a custom location, Oracle recommends you to maintain the instance directory inside the installation base directory.<br>For example, `AGENT_INSTANCE_HOME=/john/oracle/instance_dir/inst_mydir` |
| AGENT_PORT | *(Optional)* Enter a free port on which the Management Agent process should be started. The same port is used for both HTTP and HTTPS.<br>For example, `AGENT_PORT=1832`<br>If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored. |

*Table 6–2 (Cont.) Creating a Response File for Installing Oracle Management Agent Using AgentPull Script*

| Parameter | Description |
|---|---|
| b_startAgent | *(Optional)* Enter `TRUE` if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter `FALSE`.<br>For example, `b_startAgent=TRUE`<br>If you do not include this parameter, it defaults to `TRUE`. |
| ORACLE_HOSTNAME | *(Optional)* Enter the fully qualified domain name of the host where you want to install the Management Agent.<br>For example, `ORACLE_HOSTNAME=example.com`<br>If you do not include this parameter, it defaults to the physical host name. |
| ALLOW_IPADDRESS | *(Optional)* Enter `TRUE` if you want to specify an IP address for `ORACLE_HOSTNAME`. If `ALLOW_IPADDRESS` is set to `FALSE`, a prerequisite check fails when you specify an IP address for `ORACLE_HOSTNAME` while installing a Management Agent.<br>For example, `ALLOW_IPADDRESS=TRUE`<br>If you do not include this parameter, it defaults to `FALSE`. |
| START_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is started. This parameter accepts values between `0` and `99`. However, Oracle recommends that you provide a value between `91` and `99` for this parameter.<br>For example, `START_PRIORITY_LEVEL=95`<br>If you do not include this parameter, it defaults to `98`. |
| SHUT_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is shut down. This parameter accepts values between `0` and `99`.<br>For example, `SHUT_PRIORITY_LEVEL=25`<br>If you do not include this parameter, it defaults to `19`. |
| PROPERTIES_FILE | *(Optional)* Use this parameter to specify the absolute location of the properties file.<br>For example, `PROPERTIES_FILE=/tmp/agent.properties`<br>In the properties file, specify the parameters that you want to use for the Management Agent deployment. The list of parameters that you can specify in the properties file is present in `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:<br>`REPOSITORY_PROXYHOST=abc.example.com`<br>`REPOSITORY_PROXYPORT=1532`<br>The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:<br>`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>` |

***Table 6–2 (Cont.) Creating a Response File for Installing Oracle Management Agent Using AgentPull Script***

| Parameter | Description |
|---|---|
| s_agentHomeName | *(Optional)* Enter the name of the Oracle home you want to see created for the Management Agent.<br>For example, `s_agentHomeName=agent12cR2`<br>If you do not include this parameter, it defaults to `agent12cn`, where `n` is `1` for the first Management Agent installed on the host, `2` for the second Management Agent installed on the host, and so on.<br>**Note:** Ensure that the name you enter consists of only alphanumeric characters, and is not more than 128 characters long. |
| s_agentSrvcName<br>(Only for Microsoft Windows hosts) | *(Optional)* Enter the customized Management Agent service name.<br>For example, `s_agentSrvcName=agentsrvc1`<br>If you do not include this parameter, it defaults to *Oracle*+<oracle_home_name>+*Agent*.<br>**Note:** *(For Microsoft Windows hosts)* If you upgrade a 12.1.0.x Management Agent installed on a host and you want to install another Management Agent on the same host, which points to a different OMS, specify the `s_agentSrvcName` parameter while installing the Management Agent. |

## 6.4.6 Response File Parameters for Installing a Management Agent in Silent Mode Using the agentDeploy Script

Table 6–3 describes the mandatory parameters that you must include, and the optional parameters that you can include in the response file, while installing a Management Agent using the `agentDeploy` script.

***Table 6–3 Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script***

| Parameter | Description |
|---|---|
| OMS_HOST | *(Mandatory)* Enter the OMS host name.<br>For example, `OMS_HOST=example.com` |
| EM_UPLOAD_PORT | *(Mandatory)* Enter the upload port (HTTP or HTTPS) for communicating with the OMS.<br>For example, `EM_UPLOAD_PORT=14511` |
| AGENT_REGISTRATION_ PASSWORD | *(Mandatory)* Enter a password for registering new Management Agents that join the Enterprise Manager system.<br>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.<br>For example, `AGENT_REGISTRATION_PASSWORD=Wel456come` |

**Table 6–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script**

| Parameter | Description |
|---|---|
| AGENT_INSTANCE_HOME | *(Optional)* Enter a directory location on the destination host where all Management Agent-related configuration files can be stored. For this parameter, you can do one of the following:<br>- Leave it blank.<br>In this case, by default, an instance directory titled `agent_inst` is created in the agent installation base directory.<br>For example, if the installation base directory is `/john/oracle/`, then the instance directory is defaulted to `/john/oracle/agent_inst`<br>- Enter the absolute path to a custom directory.<br>Although you can enter any location as a custom location, Oracle recommends you to maintain the instance directory inside the installation base directory.<br>For example, `AGENT_INSTANCE_HOME=/john/oracle/instance_dir/inst_mydir` |
| AGENT_PORT | *(Optional)* Enter a free port on which the Management Agent process should be started. The same port is used for both HTTP and HTTPS.<br>For example, `AGENT_PORT=1832`<br>If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored. |
| b_startAgent | *(Optional)* Enter `TRUE` if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter `FALSE`.<br>For example, `b_startAgent=TRUE`<br>If you do not include this parameter, it defaults to `TRUE`. |
| ORACLE_HOSTNAME | *(Optional)* Enter the fully qualified domain name of the host where you want to install the Management Agent.<br>For example, `ORACLE_HOSTNAME=example.com`<br>If you do not include this parameter, it defaults to the physical host name. |
| ALLOW_IPADDRESS | *(Optional)* Enter `TRUE` if you want to specify an IP address for `ORACLE_HOSTNAME`. If `ALLOW_IPADDRESS` is set to `FALSE`, a prerequisite check fails when you specify an IP address for `ORACLE_HOSTNAME` while installing a Management Agent.<br>For example, `ALLOW_IPADDRESS=TRUE`<br>If you do not include this parameter, it defaults to `FALSE`. |
| START_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is started. This parameter accepts values between `0` and `99`. However, Oracle recommends that you provide a value between `91` and `99` for this parameter.<br>For example, `START_PRIORITY_LEVEL=95`<br>If you do not include this parameter, it defaults to `98`. |

*Table 6–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script*

| Parameter | Description |
|---|---|
| SHUT_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is shut down. This parameter accepts values between `0` and `99`.<br>For example, `SHUT_PRIORITY_LEVEL=25`<br>If you do not include this parameter, it defaults to `19`. |
| PROPERTIES_FILE | *(Optional)* Use this parameter to specify the absolute location of the properties file.<br>For example, `PROPERTIES_FILE=/tmp/agent.properties`<br>In the properties file, specify the parameters that you want to use for the Management Agent deployment. The list of parameters that you can specify in the properties file is present in `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:<br>`REPOSITORY_PROXYHOST=abc.example.com`<br>`REPOSITORY_PROXYPORT=1532`<br>The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:<br>`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>` |
| s_agentHomeName | *(Optional)* Enter the name of the Oracle home you want to see created for the Management Agent.<br>For example, `s_agentHomeName=agent12cR2`<br>If you do not include this parameter, it defaults to `agent12cn`, where `n` is `1` for the first Management Agent installed on the host, `2` for the second Management Agent installed on the host, and so on.<br>**Note:** Ensure that the name you enter consists of only alphanumeric characters, and is not more than 128 characters long. |
| s_agentSrvcName<br>(Only for Microsoft Windows hosts) | *(Optional)* Enter the customized Management Agent service name.<br>For example, `s_agentSrvcName=agentsrvc1`<br>If you do not include this parameter, it defaults to *Oracle*+<oracle_home_name>+*Agent*.<br>**Note:** *(For Microsoft Windows hosts)* If you upgrade a 12.1.0.x Management Agent installed on a host and you want to install another Management Agent on the same host, which points to a different OMS, specify the `s_agentSrvcName` parameter while installing the Management Agent. |

### 6.4.7 Response File Parameters for Installing a Management Agent in Silent Mode Using an RPM File

Table 6–4 describes the mandatory parameters that you must include, and the optional parameters that you can include in the response file, while installing a Management Agent using a `.rpm` file.

*Table 6–4 Creating a Response File for Installing Oracle Management Agent Using an RPM File*

| Parameter | Description |
|---|---|
| OMS_HOST | *(Mandatory)* Enter the host name of the OMS to which you want to connect.<br>For example, `OMS_HOST=example.com` |
| OMS_PORT | *(Mandatory)* Enter the upload port (HTTP or HTTPS) to communicate with the OMS.<br>For example, `OMS_PORT=1835` |
| AGENT_REGISTRATION_PASSWORD | *(Mandatory)* Enter a password for registering new Management Agents that join the Enterprise Manager system.<br>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.<br>For example, `AGENT_REGISTRATION_PASSWORD=Wel456come` |
| AGENT_USERNAME | *(Mandatory)* Enter the user name with which you want to install the Management Agent.<br>For example, `AGENT_USERNAME=oracle` |
| AGENT_GROUP | *(Mandatory)* Enter the group to which the Management Agent user should belong.<br>For example, `AGENT_GROUP=dba` |
| AGENT_PORT | *(Optional)* Enter the port used for the Management Agent process.<br>For example, `AGENT_PORT=1832`<br>If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored. |
| ORACLE_HOSTNAME | *(Only for Virtual Hosts)* Enter the virtual host name where you want to install the Management Agent.<br>For example, `ORACLE_HOSTNAME=example.com` |

## 6.4.8 Options Supported by the AgentPull Script

Table 6–5 lists the options supported by the `AgentPull.sh` script. On Microsoft Windows, these options apply to the `AgentPull.bat` file.

*Table 6–5 Understanding the Options Supported by AgentPull.sh/AgentPull.bat*

| Option | Description |
|---|---|
| -download_only | Only downloads the Management Agent software. Does not deploy the Management Agent. |
| -showPlatforms | Displays the platforms for which the Management Agent software is available on the OMS host. Does not install the Management Agent. |
| -help | Displays command line help and describes the usage of the `AgentPull.sh` script. |

### 6.4.9 Options Supported by the agentDeploy Script

Table 6–6 lists the options supported by the `agentDeploy.sh` script. On Microsoft Windows, these options apply to the `agentDeploy.bat` file.

*Table 6–6 Understanding the Options Supported by agentDeploy.sh/agentDeploy.bat*

| Option | Description |
|---|---|
| -prereqOnly | Runs only the prerequisite checks. Does NOT actually install the Management Agent.<br>This option is useful when you want to verify whether your environment meets all the prerequisites for a successful Management Agent installation. |
| -ignorePrereqs | Skips running the prerequisite checks. Use this when you have already used the `-prereqOnly` option and verified the prerequisites, and only want to install the software binaries. |
| INVENTORY_LOCATION | Enter the absolute path to the Central Inventory (oraInventory).<br>For example, `INVENTORY_LOCATION=$HOME/oraInventory`<br>**Important:**<br>■ This option is supported only on Unix platforms, and not on Microsoft Windows platforms.<br>■ Ensure that you use this option only when no other Oracle product is installed on the remote host, and the Central Inventory pointer `/var/opt/oracle/oraInst.loc` (for Solaris and HP-UX platforms) or `/etc/oraInst.loc` (for other Unix platforms) does not exist.<br>■ If you use this option, ensure that you do not use the `-invPtrLoc` option. |
| -invPtrLoc | Enter the absolute path to the inventory file that has the location of the Central Inventory (oraInventory).<br>For example, `-invPtrLoc /tmp/oraInst.loc`<br>**Important:**<br>■ This option is supported only on Unix platforms, and not on Microsoft Windows platforms.<br>■ You can use this option even when another Oracle product is already installed on the remote host, and the Central Inventory pointer `/var/opt/oracle/oraInst.loc` (for Solaris and HP-UX platforms) or `/etc/oraInst.loc` (for other Unix platforms) exists.<br>■ If you use this option, ensure that you do not use the `INVENTORY_LOCATION` option. |
| -help | Displays command line help and describes the usage of the deployment script. |
| -debug | Logs more debug messages useful for debugging and resolving errors. |
| -ignoreUnzip | Skips extracting the software binaries of the Management Agent software. Use this when you do not want to copy the binaries again, but only want to configure the available binaries. |

*Table 6–6 (Cont.) Understanding the Options Supported by*

| Option | Description |
|---|---|
| -softwareOnly | Installs only the software binaries, and does NOT configure the installation. Use this when you want to perform a software-only installation of the Management Agent. For more information, see Chapter 9.<br>**Note:** This option does not apply if you are cloning using a ZIP file. |
| -configOnly | Configures the software binaries, and does not install any software binaries. Use this when you have performed a software-only installation using the `-softwareOnly` option, so that only the configuration is done to the copied software binaries. For more information, see Chapter 9.<br>**Note:** This option does not apply if you are cloning using a ZIP file. |
| -forceConfigure | Forcefully configures the Management Agent even when the OMS is unreachable. Use this option only when you are installing the Management Agent before installing the OMS, and when you know for sure that you will install the OMS later on the same host and port mentioned for the parameters `OMS_HOST` and `EM_UPLOAD_PORT`, respectively, in the response file you pass.<br>If you pass this option, then do not pass -configOnly, -softwareOnly, and -prereqOnly.<br>Note: When you pass this option, the Management Agent is configured to use HTTP (non-secure) communication. To establish a secure HTTPS communication between the Management Agent and the OMS, you must manually secure the Management Agent after the OMS is available. |

### 6.4.10 About the Contents of the Downloaded Management Agent Software

Table 6–7 describes the contents of the core Management Agent software you download before installing the Management Agent using the `agentDeploy` script.

*Table 6–7 Contents of the Downloaded Management Agent Software*

| Files | Description |
|---|---|
| 12.1.0.5.0_PluginsOneoffs_<platform id>.zip | Plug-in ZIP file containing all the discovering plug-ins, which were installed with the OMS, Oracle Home discovery plug-in, and Oracle Home monitoring plug-in. |
| agentcoreimage.zip | Archived ZIP file containing the core agent bits and agent set-uid binaries. |
| agentDeploy.sh/agentDeploy.bat | Script used for deploying the Management Agent. |
| unzip | Utility used for unarchiving the ZIP files. |
| agentimage.properties | Properties file used for getting the version, platform ID, and so on. |
| agent.rsp | Response file to be edited and passed for installing the Management Agent. |

### 6.4.11 About the Contents of the Management Agent RPM File

If you choose to install a Management Agent using the `.rpm` file, the `.rpm` file you download contains an agent base directory. Table 6–8 describes the contents of this agent base directory:

*Table 6–8 Contents of the Agent Base Directory Present in RPM File*

| Element | Description |
|---|---|
| core/12.1.0.5.0 | Contains the Management Agent software. |
| sbin | Contains the Management Agent binaries. |
| plugins.txt | Response file specifying the plug-ins deployed on the Management Agent. |
| plugins | Contains the plug-in software. |
| agentimage.properties | Properties file used for getting the version, platform ID, and so on. |
| agent.properties | Response file to be edited and passed for installing the Management Agent. |
| oracle-agt | Management Agent configuration script. |

## 6.5 After Installing a Management Agent in Silent Mode

After you install the Management Agent, follow these steps:

1. (Only for UNIX Operating Systems) Manually run the following scripts as a *root* user:

   - If this is the first Oracle product you just installed on the host, then run the `orainstRoot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the Management Agent home. This location is also displayed when you run the `agentDeploy` script with the `-configOnly` option.

     For example, if the inventory location specified is `$HOME/oraInventory`, then run the following command:

     ```
     $HOME/oraInventory/orainstRoot.sh
     ```

   - Run the `root.sh` script from the Management Agent home:

     ```
     $<AGENT_HOME>/root.sh
     ```

   **Note:** You do not need to run the `orainstRoot.sh` and `root.sh` scripts if you are installing a Management Agent using a `.rpm` file.

2. Verify the installation:

   a. Navigate to the Management Agent home and run the following command to see a message that confirms that the Management Agent is up and running:

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

   b. Navigate to the Management Agent home and run the following command to see a message that confirms that EMD upload completed successfully:

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

3. Verify whether all the plug-ins listed in `$<AGENT_BASE_DIRECTORY>/plugins.txt` were installed successfully. To do so, run the following command:

   ```
   $<AGENT_INSTANCE_HOME>/bin/emctl listplugins agent -type all
   ```

4. If you had ignored a prerequisite check warning about wrong time zone settings, run the following command and follow the steps it displays:

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

5. By default, the host and the Management Agent get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

   To monitor the other targets, you must 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 chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

**Note:**

- If 12c (12.1.0.x) Management Agents hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.
- To know the location where a Management Agent is deployed on a Microsoft Windows host, that is, the Management Agent Oracle home, access `<INVENTORY_LOCATION>\inventory.xml`, then search for `HOME NAME="agent12c2"`. The value of the `LOC` parameter denotes the Management Agent Oracle home.

  For example, in the following line of `C:\Program Files\Oracle\inventory.xml`, `D:\agent12cr4\core\12.1.0.5.0` denotes the Management Agent Oracle home:

  ```
  <HOME NAME="agent12c2"
  LOC="D:\agent12cr4\core\12.1.0.5.0" TYPE="O" IDX="10">
  ```

- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide.*

  When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

# 7 Cloning Oracle Management Agents

This chapter explains how you can clone existing Oracle Management Agents (Management Agents) using the Cloud Control console, or in silent mode. In particular, this chapter covers the following:

- Overview of Cloning Management Agents
- Before You Begin Cloning a Management Agent
- Prerequisites for Cloning a Management Agent
- Cloning a Management Agent
- After Cloning a Management Agent

## 7.1 Overview of Cloning Management Agents

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to monitor the targets running on that managed host.

Therefore, if you want to monitor a target running on a host, you must first convert that unmanaged host to a managed host by installing an Oracle Management Agent, and then manually discover the targets running on it to start monitoring them.

However, the Management Agent you install using other installation types is always a fresh installation without any customized configuration that you had done or interim one-off patches that you had applied to other running Management Agents.

If you want to install an additional Management Agent that is identical to the existing well-tested, pre-patched, and running Management Agent, then a good option is to clone the existing instance. This saves time and effort in patching a fresh installation all over again and bringing it to the current state.

You can clone an existing Management Agent in graphical or silent mode.

- In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. The wizard enables you to select a source Management Agent, which you want to clone, and identify one or more remote hosts on which you want to clone it.

  The wizard first copies the source Management Agent image to the host on which Oracle Management Service (OMS) is running, and then, it transfers that copied image to the destination hosts. Although the wizard can be used for remotely cloning one, single Management Agent, it is best suited for mass-deployment of Management Agents, particularly while mass-deploying Management Agents of different releases on hosts of different platforms.

- In silent mode, you use a compressed file (ZIP), which you transfer. Understandably, this is a much easier method because you compress the Oracle home of an existing Management Agent and transfer it to the destination host without having to specify any parameters or values in an interview screen, but still retaining all its configuration settings and applied one-off patches.

  While cloning Management Agents in silent mode, you need to create a different compressed file for every platform on which you want to deploy the cloned Management Agent. Hence, this method is not ideal for the mass deployment of Management Agents on hosts of different platforms. This method is a quick and an effective one for deploying Management Agents on hosts that have the same platform.

After installing a Management Agent, to monitor a target, add the target 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 chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
    |_____core
         |_____12.1.0.5.0
    |_____plugins
    |_____plugins.txt
    |_____plugins.txt.status
    |_____agent_inst
    |_____sbin
    |_____agentimage.properties
```

> **Note:** You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide.*
>
> When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

## 7.2 Before You Begin Cloning a Management Agent

Before you begin cloning an Oracle Management Agent, keep these points in mind:

- *(Only for Graphical Mode)* The Add Host Targets Wizard converts an unmanaged host to a managed host in the Enterprise Manager system by cloning an existing Oracle Management Agent.

- Oracle Management Agent 12*c* communicates only with Oracle Management Service 12*c* and not with any earlier release of Enterprise Manager.

  For more information on the compatibility between a particular version of Oracle Management Agent 12*c* and a particular version of Oracle Management Service 12*c*, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

- *(Only for Graphical Mode)* Using the Add Host Targets Wizard, you can clone only when the source host (from where you are cloning the Management Agent) and the destination host are running on the same operating system. Therefore, if you have hosts running on different platforms, then you must have one deployment session per platform.
- Ensure that you do not use the central agent (that is, the Management Agent installed on the OMS host) as the source Management Agent.
- While cloning, the source Management Agent is not shut down.
- *(Only for Graphical Mode)* If you have multiple hosts, sharing a common mounted drive, then install the Management Agents in two different phases:

  1. First, clone the Management Agent to the host where the drive is shared by selecting the deployment type **Clone Existing Agent** in the Add Host Targets Wizard. Follow the instructions outlined in this chapter.
  2. Then, install a Management Agent on all other hosts that access the shared, mounted drive by selecting the deployment type **Add Host to Shared Agent** in the Add Host Targets Wizard. (Here, you will select the Management Agent you installed in the previous step.) For more information, follow the instructions outlined in Chapter 8.
- Cloning on shared clusters is NOT supported. If you have an Oracle RAC Cluster with multiple nodes, then you must clone the Management Agent on each of the nodes separately. In other words, in the Add Host Targets Wizard, you must add each node explicitly as a destination host.
- *(Only for Graphical Mode)* The Add Host Targets Wizard uses SSH to establish connectivity between Oracle Management Service (OMS) and the remote hosts where you want to install the Management Agents
- *(Only for Graphical Mode)* Only SSH1 (SSH version 1) and SSH2 (SSH version 2) protocols offered by OpenSSH are supported for deploying a Management Agent.
- *(Only for Graphical Mode)* The Add Host Targets Wizard supports Named Credentials that enable you to use a set of credentials registered with a particular name specifically for this operation, by your administrator. This ensures an additional layer of security for your passwords because as an operator, you can only select the named credential, which is saved and stored by an administrator, and not know the actual user name and password associated with it.

  In case the named credential you select does not have the privileges to clone, then you can set the named credential to run as another user (locked user account). In this case, the wizard logs in to the hosts using the named credential you select, but clones using the locked user account you set.

  For example, you can create a named credential titled User_A (the user account that has remote login access), and set it to run as User_X (the Management Agent install user account for which `no direct login` is set) that has the required privileges. In this case, the wizard logs in to the hosts as User_A, but installs as User_X, using the privilege delegation setting (sudo or PowerBroker) specified in the named credential.
- *(Only for Graphical Mode)* Named credentials support SSH public key authentication and password based authentication. So you can use an existing SSH public key authentication without exposing your passwords.

  To set up SSH public key authentication for a named credential, follow these steps:

---

**Note:** If you have already set up SSH public key authentication for a named credential and the SSH keys are already created, upload the SSH keys to Enterprise Manager, as mentioned in Step 3 of the following procedure.

---

1. Navigate to the following location in the OMS home:

   ```
   $<OMS_HOME>/oui/prov/resources/scripts
   ```

   For example,

   ```
   /home/software/em/middleware/oms/oui/prov/resources/scripts
   ```

2. If the OMS host runs on Oracle Solaris, edit the `sshUserSetup.sh` script to change the following:

   ```
   "SunOS")  SSH="/usr/local/bin/ssh"

             SSH_KEYGEN="/usr/local/bin/ssh-keygen"
   ```

   to

   ```
   "SunOS")  SSH="/usr/bin/ssh"

             SSH_KEYGEN="/usr/bin/ssh-keygen"
   ```

3. If the OMS host runs on any Unix based operating system, run the `sshUserSetup.sh` script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

   ```
   sshUserSetup.sh -setup -user <agent_install_user_name> -hosts
   <target_hosts>
   ```

   The following SSH keys are created:

   ```
   $HOME/.ssh/id_rsa
   $HOME/.ssh/id_rsa_pub
   ```

   Here, `$HOME` refers to the home directory of the OMS install user.

   If the OMS host runs on Microsoft Windows, install Cygwin on the OMS host (described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*), then run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

   ```
   sshUserSetupNT.sh -setup -user <agent_install_user_name> -hosts
   <target_hosts>
   ```

4. Upload the SSH keys to Enterprise Manager.

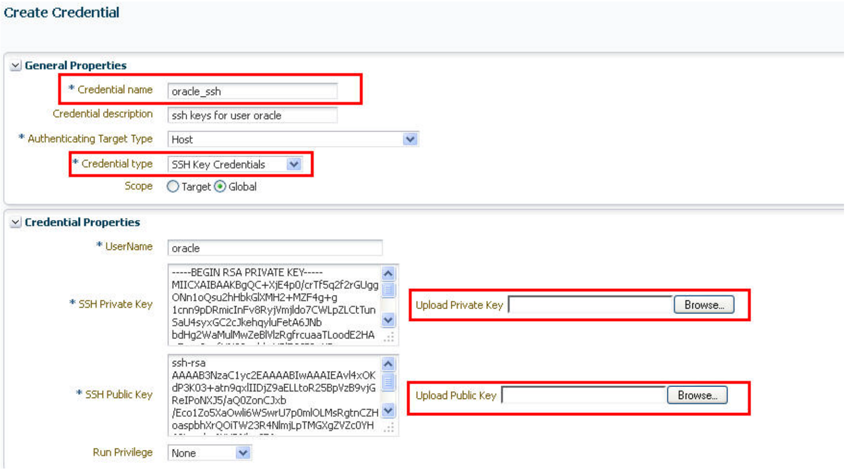
   From the **Setup** menu, select **Security,** then select **Named Credentials.** Click **Create.** For **Credential Name,** specify the name of the credential, for **Credential Type,** select **SSH Key Credentials,** and for **Scope,** select **Global.** If you do not select the **Global** option, you cannot use the SSH named credential to install Management Agents using the Add Host Targets Wizard.

   To upload one of the private SSH keys created in Step 3, in the Credential Properties section, specify the location of the private SSH key as a value for the **Upload Private Key** field. Click **Save.**

To upload one of the public SSH keys created in Step 3, in the Credential Properties section, specify the location of the public SSH key as a value for the **Upload Public Key** field. Click **Save.**

Figure 7–1 describes how to upload SSH keys to Enterprise Manager.

***Figure 7–1 Uploading SSH Keys to Enterprise Manager***



Create Credential

General Properties

* Credential name: oracle_ssh

Credential description: ssh keys for user oracle

* Authenticating Target Type: Host

* Credential type: SSH Key Credentials

Scope: ○ Target ● Global

Credential Properties

* UserName: oracle

* SSH Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC+XjE4p0/crTf5q2f2rGUgg
ONn1oQsu2hHbkGlXMH2+MZF4g+g
1cnn9pDRmicInFv8RyjVmjldo7CWLpZLCtTun
SaU4syxGC2cJkehqyluFetA6JNb
bdHg2WaMulMwZeBlVlzRgfrcuaaTLoodE2HA
```

Upload Private Key: Browse...

* SSH Public Key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvl4xOK
dP3K03+atn9qxlIIDjZ9aELLtoR25BpVzB9vjG
ReIPoNXJ5/aQ0ZonCJxb
/Eco1Zo5XaOwli6WSwrU7p0mlOLMsRgtnCZH
oaspbhXrQOiTW23R4NlmjLpTMGXgZVZc0YH
```

Upload Public Key: Browse...

Run Privilege: None

If you have already set up SSH public key authentication for a named credential, you can use the named credential while installing Management Agents using the Add Host Targets Wizard.

- By default, the Add Host Targets Wizard configures all the plug-ins that were configured with the Management Agent you are cloning.
- You must have *read* privileges on the Oracle WebLogic Server's alert log directories for the Support Workbench (Incident) metrics to work properly. You must also ensure that the Management Agent that is monitoring this Oracle WebLogic Server target is running on the same host as the Oracle WebLogic Server.
- Upgrading a lower release of Solaris by applying a kernel patch or a patch bundle is not equivalent to installing the actual Solaris 5.10 Update 9 image. Oracle Management Agent 12c Release 5 (12.1.0.5) was built, tested, and certified on a minimum update version of Solaris 5.10 Update 9, so Oracle recommends that you install Oracle Management Agent only on Solaris 5.10 Update 9, and not on any release that was upgraded using patches.
- Changes done to the `emd.properties` file on the source host before cloning are not carried over to the destination host after cloning.

## 7.3 Prerequisites for Cloning a Management Agent

Before cloning the Management Agent, ensure that you meet the following prerequisites.

***Table 7–1 Prerequisites for Cloning 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 *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| Software Requirements<br>*(Only for Graphical Mode)* | *(For Microsoft Windows)* Ensure that you have installed Cygwin 1.7 on the destination host. For more information, see the chapter on installing Cygwin in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*<br>**Note:** While running `cygwin.bat` in Microsoft Windows Server 2008 and Microsoft Windows Vista, ensure that you invoke it in administrator mode. To do this, right-click the `cygwin.bat` file and select **Run as administrator.** |
| Operating System Requirements | Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on *My Oracle Support*.<br>To access the Enterprise Manager certification matrix, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>For information about platforms receiving future support, refer to *My Oracle Support* note 793512.1.<br>**Note:** If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:<br>`cat /etc/release`<br>You should see the output similar to the following. Here, `s10s_u6` indicates that update 6, which is not a supported update level for installation, is installed.<br>`Solaris 10 10/08 s10s_u6wos_07b SPARC` |
| File System Requirements | Ensure that the file system mounted on the destination host does not permit buffered writes. |
| File Descriptor Requirements | ■ Ensure that the maximum user process limit is set to 13312 or greater.<br>To verify the current value set, run the following command:<br>`ulimit -u`<br>If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.<br>■ Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.<br>To verify the current value set, run the following commands:<br>**For Soft Limit:**<br>`/bin/sh -c "ulimit -n"`<br>**For Hard Limit:**<br>`/bin/sh -c "ulimit -Hn"`<br>If the current value is not 4096 or greater, then as a *root* user, update the `/etc/security/limits.conf` file with the following entries:<br>`<UID> soft nofile 4096`<br>`<UID> hard nofile 16384` |

*Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent*

| Requirement | Description |
|---|---|
| Package Requirements | Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| 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.<br>For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>**Note:** If your enterprise has a policy against installing Management Agents using the OMS install operating system user account, you can use a different operating system user account to install Management Agents. However, ensure that the user account you use and the OMS install user account belong to the same primary group. |
| /etc/hosts File Requirements | Ensure that the `/etc/hosts` file on the host has the IP address, the fully qualified name, and the short name in the following format:<br>`172.16.0.0  example.com  mypc` |
| Destination Host Requirements | Ensure that the destination hosts are accessible from the host where the OMS is running.<br>If the destination host and the host on which OMS is running belong to different network domains, then ensure that you update the `/etc/hosts` file on the destination host to add a line with the IP address of that host, the fully qualified name of that host, and the short name of the host.<br>For example, if the fully-qualified host name is `example.com` and the short name is `mypc`, then add the following line in the `/etc/hosts` file:<br>`172.16.0.0  example.com  mypc` |
| Destination Host Credential Requirements<br>*(Only for Graphical Mode)* | Ensure that all the destination hosts running on the same operating system have the same set of credentials. For example, all the destination hosts running on Linux operating system must have the same set of credentials.<br>The wizard installs the Management Agent using the same user account. If you have hosts running on the same operating system but with different credentials, then have two different deployment sessions. |

*Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent*

| Requirement | Description |
|---|---|
| Destination Host Time Zone Requirements<br>*(Only for Graphical Mode)* | Ensure that the time zones of the destination hosts have been set correctly. To verify the time zone of a destination host, log in to the OMS host, and run the following command:<br>`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ’`<br>If the time zone displayed is incorrect, log in to the destination host, and follow these steps:<br>**1.** Run the following commands to set the time zone on the destination host:<br>■ For Korn shell:<br>`TZ=<value>`<br>`export TZ`<br>■ For Bourne shell or Bash shell:<br>`export TZ=<value>`<br>■ For C shell:<br>`setenv TZ <value>`<br>For example, in the Bash shell, run the following command to set the time zone to America/New_York:<br>`export TZ=’America/New_York’`<br>To set the time zone on a destination host that runs on Microsoft Windows, from the **Start** menu, select **Control Panel.** Click **Date and Time,** then select the **Time Zone** tab. Select your time zone from the displayed drop down list.<br>To view a list of the time zones you can use, access the `supportedtzs.lst` file present in the `<AGENT_HOME>/sysman/admin` directory of the central agent (that is, the Management Agent installed on the OMS host).<br>**2.** Restart the SSH daemon.<br>If the destination host runs on a UNIX based operating system, run the following command:<br>`sudo /etc/init.d/sshd restart`<br>If the destination host runs on a Microsoft Windows operating system, run the following commands:<br>`cygrunsrv -E sshd`<br>`cygrunsrv -S sshd`<br>**3.** Verify whether the SSH server can access the `TZ` environment variable by logging in to the OMS host, and running the following command:<br>`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`<br>**Note:** If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the destination hosts after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5. |

***Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent***

| Requirement | Description |
|---|---|
| Time Zone Requirements<br>*(Only for Silent Mode)* | Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:<br>`echo $TZ`<br>If the time zone displayed is incorrect, run the following commands, before running the `agentDeploy.sh` or `agentDeploy.bat` scripts, to set the correct time zone:<br>■ For Korn shell:<br>`TZ=<value>`<br>`export TZ`<br>■ For Bourne shell or Bash shell:<br>`export TZ=<value>`<br>■ For C shell:<br>`setenv TZ <value>`<br>For example, in the Bash shell, run the following command to set the time zone to America/New_York:<br>`export TZ='America/New_York'`<br>To set the time zone on a destination host that runs on Microsoft Windows, from the **Start** menu, select **Control Panel.** Click **Date and Time,** then select the **Time Zone** tab. Select your time zone from the displayed drop down list.<br>To view a list of the time zones you can use, access the `supportedtzs.lst` file present in the `<AGENT_HOME>/sysman/admin` directory of the central agent (that is, the Management Agent installed on the OMS host).<br>**Note:**<br>■ If you are installing a Management Agent on a host that runs on Microsoft Windows Server 2003, and you encounter an error when you use the Asia/Kolkata time zone, see the My Oracle Support note 1530571.1.<br>■ If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the host after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5.<br>**Note:** If you had ignored a prerequisite check warning about wrong time zone settings during the cloning procedure, you must set the correct time zone on the host after cloning the Management Agent. For information on setting time zones post cloning, see Section 7.5. |

***Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent***

| Requirement | Description |
|---|---|
| sudo/pbrun/sesu/su SSH Requirements<br>*(Only for Graphical Mode)* | *(Only for UNIX)*<br>Ensure that you set the `oracle.sysman.prov.agentpush.enablePty` property to `true` in the `$<OMS_HOME>/sysman/prov/agentpush/agentpush.properties` file, if the privilege delegation tool you are using requires a pseudo terminal for remote command execution via SSH. Most privilege delegation tools such as pbrun, sesu, and su require a pseudo terminal for remote command execution, by default.<br>**Note:** If you are using sudo as your privilege delegation tool, and you do not want to set the `oracle.sysman.prov.agentpush.enablePty` property to `true,` do one of the following:<br>■ Include `Defaults visiblepw` in the `/etc/sudoers` file, or enter the `sudo` command with the `-S` option for **Privileged Delegation Setting** on the Installation Details page.<br>For information on how to access the Installation Details page, see Section 7.4.1.<br>■ Comment out `Defaults requiretty` in the `/etc/sudoers` file. |
| sudo/pbrun/sesu/su Requirements (for *Root* User)<br>*(Only for Graphical Mode)* | *(Only for UNIX)*<br>■ Ensure that the installing user has the privileges to invoke the `id` command and the `agentdeployroot.sh` script as *root.* Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`<install_user> ALL=(root) /usr/bin/id, <agent_home>/*/agentdeployroot.sh`<br>For example, `oracle ALL=(root) /usr/bin/id, /home/oracle/agentibd/*/agentdeployroot.sh`<br>Here, `oracle` is the installing user, and `/home/oracle/agentibd` is the Management Agent home, that is, the agent base directory.<br>■ You do not require the following entry in the `/etc/sudoers` file for installing a Management Agent. However, the entry is required for performing provisioning and patching operations in Enterprise Manager. Therefore, if you are removing this entry before installing a Management Agent, then ensure that you bring back the entry after installing the Management Agent.<br>**In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), Release 3 (12.1.0.3), Release 4 (12.1.0.4), or Release 5 (12.1.0.5):**<br>`(root) /<AGENT_BASE_DIRECTORY>/sbin/nmosudo`<br>**In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with Bundle Patch 1]:**<br>`(root) /<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo` |

***Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent***

| Requirement | Description |
|---|---|
| sudo/pbrun/sesu/su Requirements (for Locked Account User)<br>*(Only for Graphical Mode)* | *(Only for UNIX)*<br>Ensure that the installing user has the privileges to invoke `/bin/sh` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`login_user1 ALL=(oracle) /bin/sh`<br>Here, `login_user1` is the SSH log in user, and `oracle` is the locked account and install user.<br>If you do not want to grant privileges to the installing user to invoke `/bin/sh` as the locked account user, set the `oracle.sysman.prov.agentpush.pdpShellOutEnabled` property to `false`, and ensure that the installing user has the privileges to invoke `id, chmod, cp, mkdir, rm, tar, emctl, agentDeploy.sh, runInstaller,` and `unzip` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`login_user1 ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp, /bin/mkdir, /bin/rm, /bin/tar, /home/oracle/agentibd/agent_inst/bin/emctl, /home/oracle/agentibd/*/agentDeploy.sh, /home/oracle/agentibd/*/prereq_stage/core/12.1.0.5.0/oui/bin/runInstaller, /home/oracle/agentibd/*/unzip, /home/oracle/agentibd/*/unzipTmp/unzip`<br>Here, `login_user1` is the SSH log in user, `oracle` is the locked account and install user, and `/home/oracle/agentibd` is the agent base directory. |
| Permission Requirements | ■ Ensure that the agent base directory you specify is empty and has *write* permission.<br>■ Ensure that the instance directory is empty and has *write* permission. |
| PATH Environment Variable Requirements<br>*(Only for Graphical Mode)* | On the destination host, ensure the following:<br>■ *(For Microsoft Windows)* Ensure that the Cygwin software location appears before other software locations in the PATH environment variable. After making it the first entry, restart the SSH daemon (sshd).<br>■ (*For UNIX*) On the destination host, ensure that the SCP binaries (for example, /usr/bin/scp) are in the `PATH` environment variable: |
| Path Validation Requirements | Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| `CLASSPATH` Environment Variable Requirements | Unset the `CLASSPATH` environment variable. You can always reset the variable to the original value after the installation is complete. |

***Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent***

| Requirement | Description |
|---|---|
| Temporary Directory Space Requirements | Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.<br>By default, the temporary directory location set to the environment variable `TMP` or `TEMP` is honored. If both are set, then TEMP is honored. If none of them are set, then the following default values are honored: `/tmp` on UNIX hosts and `c:\Temp` on Microsoft Windows hosts. |
| Agent Base Directory Requirements | Ensure that the agent base directory is empty and has at least 1 GB of free space.<br>Ensure that the directory name does not contain any spaces.<br>The install user owns the agent base directory. The agent base directory and the parent directories of the agent base directory have read, write, and execute permissions for the install user. Ensure that the install user or the *root* user owns all the parent directories of the agent base directory, and that the parent directories have read and execute permissions for the install user group and all the other users. Also, ensure that the *root* user owns the root directory.<br>For example, if the agent base directory is `/scratch/OracleHomes/agent`, and *oracle* is the install user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or the *root* user, and the root directory (/) must be owned by the *root* user.<br>If the agent base directory is mounted, then ensure that it is mounted with the `setuid` turned on. |
| Default SSH Port Requirements<br>*(Only for Graphical Mode)* | Ensure that the SSH daemon is running on the default port (that is, 22) on all the destination hosts. To verify the SSH port on a Unix host, run the following command:<br>`netstat -anp \| grep -i sshd`<br>For example, the output of this command may be the following:<br>`tcp     0 0 0.0.0.0:22       0.0.0.0:*       LISTEN 3188/sshd`<br>The above output indicates that the SSH daemon is running on port 22.<br>Also, on a Unix host, you can run the following command to verify the SSH port:<br>`cat /etc/ssh/sshd_config`<br>For a Microsoft Windows host, the SSH port value is mentioned in the `C:\cygwin\etc\sshd_config` file.<br>If the SSH port is a non-default port, that is, any port other than 22, then update the `SSH_PORT` property in the following file:<br>`$<OMS_HOME>/oui/prov/resources/Paths.properties` |
| Software Availability Requirements<br>*(Only for Graphical Mode)* | **For Cloning an Existing Management Agent**<br>Ensure that you already have Oracle Management Agent 12*c* running in your environment. Ensure that the platform on which it is running is the same as the platform of the destination hosts on which you want to clone.<br>**For Installing a Management Agent Using Shared Oracle Home**<br>Ensure that you already have Oracle Management Agent 12*c* installed as a *Master Agent* in a shared, mounted location. |

*Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent*

| **Requirement** | **Description** |
|---|---|
| Installation Base Directory Requirements<br>*(Only for Graphical Mode)* | Ensure that the agent base directory you specify in the Installation Base Directory field is empty and has *write* permission. |
| Job System Requirements | Ensure that the job system is enabled on the source Management Agent you want to clone. |
| Installing User Requirements | If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group.<br>Also ensure that the inventory owner and the group to which the owner belongs have *read* and *write* permissions on the inventory directory.<br>For example, if the inventory owner is *abc* and the user installing the Management Agent is *xyz*, then ensure that *abc* and *xyz* belong to the same group, and they have read and write access to the inventory. |
| Central Inventory (oraInventory) Requirements | ■ Ensure that you allocate 100 MB of space on all destination hosts for the Central Inventory.<br>■ Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all destination hosts. If you do not have these permissions on the default inventory (typically at `/etc/oraInst.loc`) on any destination 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. However, these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms.<br>`INVENTORY_LOCATION=<absolute_path_to_inventory_directory>`<br>`-invPtrLoc <absolute_path_to_oraInst.loc>` |
| Port Requirements | Ensure that the default ports described in Section 2.1.10.1 are free. |
| Agent User Account Permissions and Rights<br>*(Only for Microsoft Windows)* | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Adjust memory quotas for a process.<br>■ Replace process level token.<br>■ Log on as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>**1.** Launch the Local Security Policy.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Policy**.<br>**2.** In the Local Security Policy window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**. |

*Table 7–1 (Cont.) Prerequisites for Cloning Oracle Management Agent*

| Requirement | Description |
|---|---|
| Permissions for cmd.exe | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that you grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` |
| Runtime Library File Requirements | *(For Microsoft Windows)* If you are installing the Management Agent on a Microsoft Windows-based operating system, then ensure that the `Msvcp71.dll` and `Msvcr71.dll` runtime library files are present in `c:\windows\system32`. |
| Preinstallation/Postinstallation Scripts Requirements<br>*(Only for Graphical Mode)* | Ensure that the preinstallation and postinstallation scripts that you want to run along with the installation are available either on the OMS host, destination hosts, or on a shared location accessible to the destination hosts. |
| Browser Requirements | ■ Ensure that you use a certified browser as mentioned in the Enterprise Manager certification matrix available on *My Oracle Support*.<br>To access the Enterprise Manager certification matrix, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>■ If you use Microsoft Internet Explorer 8 or 9, do the following:<br>■ Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the **Tools** menu, click **Compatibility View** to disable it if it is enabled. Also, click **Compatibility View Settings** and deregister the Enterprise Manager Cloud Control console URL.<br>■ Enable XMLHTTP. To do so, from the **Tools** menu, click **Internet Options**. Click the **Advanced** tab, and under the **Security** heading, select **Enable native XMLHTTP support** to enable it. |

## 7.4 Cloning a Management Agent

This section describes the following:

- Cloning a Management Agent in Graphical Mode
- Cloning a Management Agent in Silent Mode

> **Important:** If the OMS host is running on Microsoft Windows, and the OMS software was installed in a drive other than `C:\`, then update the `SCRATCH_PATH` variable in `$OMS_HOME\oui\prov\resources\ssPaths_msplats.properties`.
>
> For example, if the OMS software was installed in `D:\`, ensure that you update the `SCRATCH_PATH` variable to `D:\tmpada`

## 7.4.1 Cloning a Management Agent in Graphical Mode

This section describes how to clone a Management Agent using the Cloud Control console. It consists of the following:

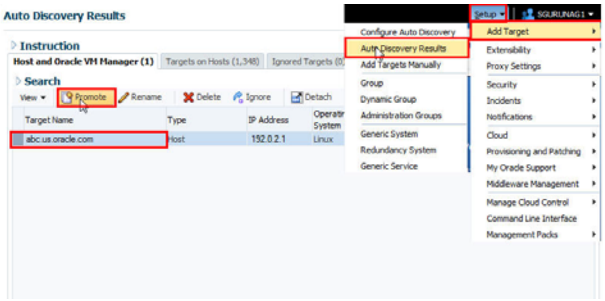
- Cloning a Management Agent Using Add Host Targets Wizard
- Format of Host List File
- Additional Parameters Supported for Cloning a Management Agent in Graphical Mode

### 7.4.1.1 Cloning a Management Agent Using Add Host Targets Wizard

To clone a Management Agent in graphical mode using Add Host Targets Wizard, follow these steps:

1. In Cloud Control, do one of the following:

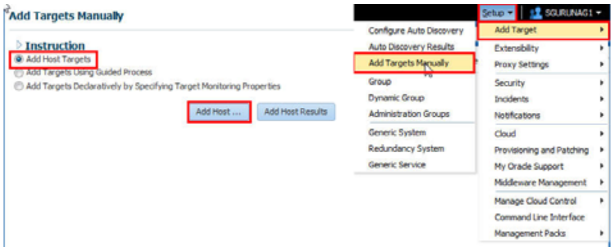
   - From the **Setup** menu, select **Add Target**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.



| Target Name | Type | IP Address | Operatir System |
|---|---|---|---|
| abc.us.oracle.com | Host | 192.0.2.1 | Linux |

   Enterprise Manager Cloud Control displays the Add Host Wizard, where you can select the option to clone an existing Management Agent.

   - From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.



● Add Host Targets
○ Add Targets Using Guided Process
○ Add Targets Declaratively by Specifying Target Monitoring Properties

   Enterprise Manager Cloud Control displays the Add Host Wizard, where you can select the option to clone an existing Management Agent.

2. On the Host and Platform page, do the following:

   a. Accept the default name assigned for this session or enter a unique name of your choice. 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, `add_host_operation_1`

      A unique deployment activity name enables you to save the cloning details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.

   b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to clone the Management Agent.

      **Note:**

      - Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
      - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
      - You must ensure that the host name you enter does not have underscores.

      Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager. For information on how the host name entries must appear in the host file, see Section 7.4.1.2.

      **Note:** When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

      As you can clone only if the source host and destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

**Note:** If you are cloning a Management Agent on a platform that is different from the platform on which the OMS host is running, then ensure that the Management Agent software for that platform is available in Oracle Software Library (Software Library). If the Management Agent software for the required platform is not available in Software Library, acquire and apply the software using the Self Update console.

To access the Self Update Console, from the **Setup** menu, select **Extensibility,** then select **Self Update.** To acquire the latest Management Agent software, click **Agent Software,** select the required software, then click **Download.**

For more information on how to acquire and apply the Management Agent software for a platform using the Self Update console, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

c. Click **Next**.

3. On the Installation Details page, do the following:

a. In the Deployment Type section, select **Clone Existing Agent**. Then, for **Select Target**, click the torch icon and select the Management Agent you want to clone.

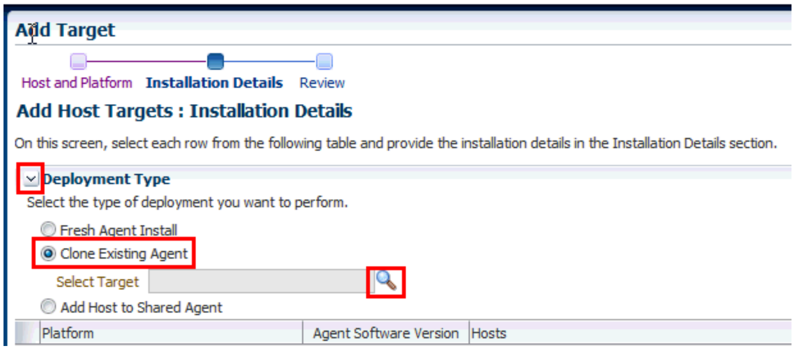
**Note:**

- Ensure that you do not use the central agent (that is, the Management Agent installed on the OMS host) as the source Management Agent.
- If you have multiple hosts sharing a common mounted drive, then install the Management Agents in two different phases:

  1. In the Add Host Targets Wizard, select the deployment type **Clone Existing Agent**, and clone the Management Agent to the host where the drive is shared.
  2. In the Add Host Targets Wizard, select the deployment type **Add Host to Shared Agent**, and install a Management Agent on all other hosts that access the shared, mounted drive. (Here, you will select the Management Agent you cloned in the previous step as the master agent or shared agent.)

Figure 7–2 describes this step.

*Figure 7–2 Cloning a Management Agent*



Add Host Targets : Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type

Select the type of deployment you want to perform.

○ Fresh Agent Install

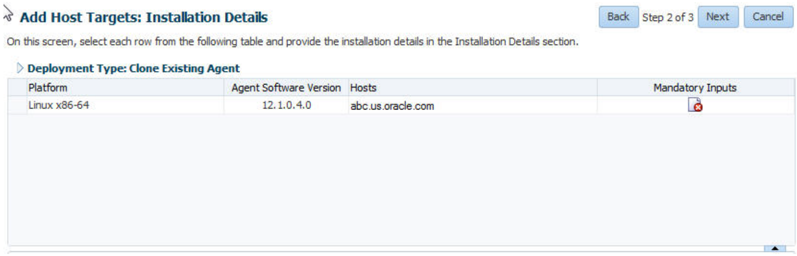
● Clone Existing Agent

Select Target

○ Add Host to Shared Agent

| Platform | Agent Software Version | Hosts |
|---|---|---|

b. From the table, select the first row that indicates the hosts grouped by their common platform name.



Add Host Targets: Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type: Clone Existing Agent

| Platform | Agent Software Version | Hosts | Mandatory Inputs |
|---|---|---|---|
| Linux x86-64 | 12.1.0.4.0 | abc.us.oracle.com | |

c. In the Installation Details section, provide the installation details common to the hosts selected in Step 3 (b). For **Installation Base Directory**, enter the absolute path to the agent base directory where you want the software binaries, security files, and inventory files of the Management Agent to be copied.

For example, `/usr/home/software/oracle/agentHome`

If the path you enter does not exist, the application creates a directory at the specified path, and copies the Management Agent software binaries, security files, and inventory files there.

---

**Note:** The Installation Base Directory is essentially the agent base directory. Ensure that the directory you provide is empty. If a previously run deployment session had failed for some reason, then you might see an ADATMP_<timestamp> subdirectory in the installation base directory. In this case, either delete the subdirectory and start a new deployment session, or retry the failed session from the Add Host Status page.

---

d. For **Instance Directory**, accept the default instance directory location or enter the absolute path to a directory of your choice where all Management Agent-related configuration files can be stored.

For example, `/usr/home/software/oracle/agentHome/agent_inst`

If you are entering a custom location, then ensure that the directory has write permission. Oracle recommends you to maintain the instance directory inside the installation base directory.

If the path you enter does not exist, the application creates a directory at the specified path, and stores all the Management Agent-related configuration files there.

e. From **Named Credential** list, select an appropriate profile whose credentials can be used for setting up the SSH connectivity between the OMS and the remote hosts, and for installing a Management Agent on each of the remote hosts.

**Note:**

- If you do not have a credential profile, or if you have one but do not see it in the **Named Credential** list, then click the plus icon against this list. In the Create New Named Credential window, enter the credentials and store them with an appropriate profile name so that it can be selected and used for installing the Management Agents. Also set the run privilege if you want to switch over from the Named Credential you are creating, to another user who has the privileges to perform the installation.
- If the plus icon is disabled against this list, then you do not have the privileges to create a profile with credentials. In this case, contact your administrator and either request him/her to grant you the privileges to create a new profile or request him/her to create a profile and grant you the access to view it in the **Named Credential** list.
- If you have manually set up SSH public key authentication between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.

f. For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

For example, you can specify one of the following for the **Privileged Delegation Setting** field:

```
/usr/bin/sudo -u %RUNAS% %COMMAND%
/usr/bin/sudo -u -S %RUNAS% %COMMAND% (if a pseudo terminal is required for
remote command execution via SSH)
/usr/bin/sesu - %RUNAS% -c "%COMMAND%"
/usr/bin/pbrun %PROFILE% -u %RUNAS% %COMMAND%
/usr/bin/su - %RUNAS% -c "%COMMAND%"
```

If you leave the **Privileged Delegation Setting** field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see Section 7.5.

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

> **Note:** In the Privilege Delegation setting, the `%RUNAS%` is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

   The custom port you enter must not be busy. If you are not sure, you can leave this field blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

   If you want to run the script as `root`, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see Table 7–2.

   For example, if you want to provide the inventory pointer location file, then enter `-invPtrLoc` followed by the absolute path to the file location. Note that this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

j. Repeat Step 3 (b) to Step 3 (i) for every other row you have in the table.

k. Click **Next**.

4. On the Review page, review the details you have provided and if you are satisfied with the details, then click **Deploy Agent** to clone the Management Agent.

   If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

   When you click **Deploy Agent** and submit the deployment session, you are automatically taken to the Add Host Status page that enables you to monitor the progress of the deployment session.

> **Note:** On the Add Host Status page, if you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:
>
> ```
> $<OMS_
> HOME>/sysman/prov/agentpush/<timestampdir>/applogs/deployfwk
> .log
> ```
>
> This error usually occurs when the job system is not enabled on the source Management Agent you are cloning. Ensure that the job system is enabled.

#### 7.4.1.2 Format of Host List File

In the Add Host Targets Wizard, you can click **Load from File** to add the hosts listed in a file. However, ensure that the file you select has one of the following formats:

- Only the host name.

  For Example,

  ```
  host1.example.com
  ```

  ```
  host2.example.com
  ```

- The host name followed by the platform name.

  For Example,

  ```
  host1.example.com linux_x64
  ```

  ```
  host2.example.com aix
  ```

  The supported platform names are linux_x64, linux, solaris, hpunix, hpi, linux64_zseries, aix, linux_ppc64, windows_x64, solaris_x64, win32.

#### 7.4.1.3 Additional Parameters Supported for Cloning a Management Agent in Graphical Mode

Table 7–2 lists the additional parameters supported for cloning a Management Agent in graphical mode.

*Table 7–2 Supported Additional Parameters*

| Parameter | Description |
|---|---|
| INVENTORY_LOCATION | Enter the absolute path to the Central Inventory (oraInventory).<br>For example, `INVENTORY_LOCATION=$HOME/oraInventory`<br>**Important:**<br>■ This parameter is supported only on Unix platforms, and not on Microsoft Windows platforms.<br>■ Ensure that you use this parameter only when no other Oracle product is installed on the remote host, and the Central Inventory pointer `/var/opt/oracle/oraInst.loc` (for Solaris and HP-UX platforms) or `/etc/oraInst.loc` (for other Unix platforms) does not exist.<br>■ If you use this parameter, ensure that you do not use the `-invPtrLoc` parameter. |
| -invPtrLoc | Enter the absolute path to the inventory file that has the location of the Central Inventory (oraInventory).<br>For example, `-invPtrLoc /tmp/oraInst.loc`<br>**Important:**<br>■ This parameter is supported only on Unix platforms, and not on Microsoft Windows platforms.<br>■ You can use this parameter even when another Oracle product is already installed on the remote host, and the Central Inventory pointer `/var/opt/oracle/oraInst.loc` (for Solaris and HP-UX platforms) or `/etc/oraInst.loc` (for other Unix platforms) exists.<br>■ If you use this parameter, ensure that you do not use the `INVENTORY_LOCATION` parameter. |

*Table 7–2 (Cont.) Supported Additional Parameters*

| Parameter | Description |
|---|---|
| s_agentSrvcName | *(Only for Microsoft Windows)* Enter a custom name for the Management Agent service.<br>Every Management Agent appears as a service in Microsoft Windows, and every Management Agent has a default service name. If you want to assign a custom name to identify it, then use this parameter.<br>For example, `s_agentSrvcName=agentsrvc1`<br>**Note:** If you upgrade a 12c Release 1 (12.1.0.1), Release 2 (12.1.0.2), Release 3 (12.1.0.3), or a Release 4 (12.1.0.4) Management Agent installed on a Microsoft Windows host to 12c Release 5 (12.1.0.5), and you want to install another Management Agent on the same host, reporting to a different OMS, ensure that you specify the `s_agentSrvcName` parameter. |
| EM_STAGE_DIR | Enter the absolute path to a custom location that can be created as a temporary Provisioning Advisor Framework (PAF) staging directory.<br>By default, every time you install a Management Agent, a 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.<br>If you want to override this location with a custom location, you can pass this option and enter a custom location.<br>For example,<br>`EM_STAGE_DIR=/home/john/software/oracle/pafdir` |
| b_startAgent=false | Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured.<br>If you do not specify this parameter, the Management Agent starts automatically once it is installed and configured. |
| b_secureAgent=false | Specify this parameter if you do not want the Management Agent to be secured after the install.<br>If you specify this parameter, ensure that you also specify the OMS HTTP port, using the `EM_UPLOAD_PORT` parameter.<br>For example, `b_secureAgent=false EM_UPLOAD_PORT=4899`<br>If you do not specify this parameter, the Management Agent is secured automatically after the install. |

## 7.4.2 Cloning a Management Agent in Silent Mode

To clone a Management Agent manually, follow these steps:

**Important:** Ensure that you do not use the central agent (that is, the Management Agent installed on the OMS host) as the source Management Agent.

1. Set the required environment variables as described in Table 7–3.

*Table 7–3 Setting Environment Variables for Cloning in Silent Mode*

| | | |
|---|---|---|
| AGENT_BASE_DIR | Set it to the installation base directory of the Management Agent you want to clone. | ■ In bash terminal, run the following command:<br>`export AGENT_BASE_DIR=<absolute_path_to_agent_install_base_dir>`<br>For example,<br>`export AGENT_BASE_DIR=/u01/app/Oracle/software/agent`<br>■ In other terminals, run the following command:<br>`setenv AGENT_BASE_DIR <absolute_path_to_agent_install_base_dir>`<br>For example,<br>`setenv AGENT_BASE_DIR /u01/app/Oracle/software/agent` |
| AGENT_HOME | Set it to the Oracle home of the Management Agent.<br>For example,<br>`/u01/app/Oracle/software/agent/core/12.1.0.5.0` | ■ In bash terminal, run the following command:<br>`export AGENT_HOME=<absolute_path_to_agent_home>`<br>For example,<br>`export AGENT_HOME=/u01/app/Oracle/software/agent/core/12.1.0.5.0`<br>■ In other terminals, run the following command:<br>`setenv AGENT_HOME <absolute_path_to_agent_home>`<br>For example,<br>`setenv AGENT_HOME /u01/app/Oracle/software/agent/core/12.1.0.5.0` |
| T_WORK | Set it to `/tmp/clone_work`. | ■ In bash terminal, run the following command:<br>`export T_WORK=/tmp/clone_work`<br>■ In other terminals, run the following command:<br>`setenv T_WORK /tmp/clone_work` |

2. Navigate to the agent base directory:

   ```
   cd $AGENT_BASE_DIR
   ```

3. Run the `create_plugin_list.pl` script from the Management Agent Oracle home:

   ```
   $AGENT_HOME/perl/bin/perl $AGENT_HOME/sysman/install/create_plugin_
   list.pl -instancehome <AGENT_INSTANCE_HOME>
   ```

4. Compress the directories and files present in the agent base directory, and create a ZIP file in the temporary directory (represented by the environment variable `T_WORK`):

   ```
   zip -r $T_WORK/agentcoreimage.zip core sbin plugins plugins.txt
   agentimage.properties
   ```

5. Navigate to the temporary directory (represented by the environment variable T_WORK):

   ```
   cd $T_WORK
   ```

6. Copy the agentDeploy.sh to the temporary directory:

   ```
   cp $AGENT_HOME/sysman/install/agentDeploy.sh .
   ```

7. Copy the UNZIP utility to the temporary directory:

   ```
   cp $AGENT_HOME/bin/unzip .
   ```

8. Copy the agentimage.properties to the temporary directory:

   ```
   cp $AGENT_BASE_DIR/agentimage.properties .
   ```

9. Create the final ZIP file with all the contents to be transferred, in the temporary directory:

   ```
   zip -r agent.zip $T_WORK/*
   ```

10. Transfer the ZIP file to the installation base directory of the destination host using a file transfer utility (for example, FTP).

11. Extract the contents of the ZIP file to a temporary directory on the destination host (the temporary directory is referred to as <extracted_location> in the steps that follow).

12. Create a response file titled agent.rsp (in the same directory) as described in Table 6–3.

    > **Note:** The response file you create can have any name, and not necessarily agent.rsp. For easy understanding, this chapter uses the name agent.rsp. Also, instead of creating a response file, you can choose to pass the values in separate arguments while invoking the deployment script. However, Oracle recommends that you create a response file and capture the information there.

13. Invoke the deployment script and pass the response file:

    ```
    <extracted_location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_to_
    clone_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile>
    ```

**Note:**

- Instead of creating a response file, if you choose to pass the values in separate arguments, then invoke the deployment script with some mandatory arguments in the following way:

  ```
   <extracted_location>/agentDeploy.sh AGENT_BASE_
  DIR=<absolute_path_to_agentbasedir> OMS_HOST=<oms_
  hostname> EM_UPLOAD_PORT=<em_upload_port> AGENT_
  REGISTRATION_PASSWORD=<password>
  ```

- In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see Section 6.4.9.
- If the source Management Agent was installed using the Add Host Targets Wizard, ensure that you specify the `b_startAgent=true` and the `b_secureAgent=true` parameters while invoking the deployment script.

## 7.5 After Cloning a Management Agent

After cloning a Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization**, **Remote Prerequisite Check**, and **Agent Deployment**.

   **Note:** In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.

   If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

   If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

   - Ignore the warning or failure, and continue with the session if you prefer.
     - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, Ignoring Failed Hosts.**
     - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, All Hosts**.
   - Fix the problem by reviewing the error description carefully, understanding its cause, and taking action as recommended by Oracle.

- You can choose to retry the deployment of Management Agents with the same installation details. To do so, click **Retry** and select **Retry Using Same Inputs.**
- You can retry the deployment of Management Agents with modified installation details. To do so, click **Retry** and select **Update Inputs and Retry.**

---

**Note:** If you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:

```
$<OMS_
HOME>/sysman/prov/agentpush/<timestampdir>/applogs/deployfwk
.log
```

This error usually occurs when the job system is not enabled on the source Management Agent you are cloning. Ensure that the job system is enabled.

---

2. Perform the post installation steps as described in Section 6.5.

---

**Note:**

- If Oracle Management Agents 12c (12.1.0.x) hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.
- You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For information on how to do this, see the Redirecting Oracle Management Agent to Another Oracle Management Service Appendix present in *Oracle Enterprise Manager Cloud Control Advanced Installation Guide.*

  When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

---

# 8 Installing Shared Agents

This chapter describes how you can install a *Shared Agent* with the help of a central, shared Oracle home location of an existing Oracle Management Agent (Management Agent) that is installed on an NFS-mounted drive.

## 8.1 Overview of Installing Shared Agents

*Shared Agent* is a Management Agent that is installed on a remote host, using the binaries of an existing Management Agent. The Management Agent that shares its software binaries, in this context, is called the *Master Agent*, and the one that is configured with an instance directory on the remote host is called a *Shared Agent* or an *NFS Agent*.

This feature facilitates the installation of multiple Management Agents by making use of very limited resources, and helps you carry out lifecycle operations with ease. For example, patching the *Master Agent* updates all its *Shared Agents.*

You can take advantage of this operation by installing additional Management Agents on hosts that share a mounted drive where a Management Agent is already installed. Such an operation makes use of the software binaries of the shared Oracle home present on the mounted drive, and configures the remote hosts such that they are managed by that Management Agent, thereby capitalizing on the NFS visibility and saving hard disk space on the remote hosts.

You can install a *Shared Agent* in graphical or silent mode. In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. In silent mode, you use the `AgentNFS.pl` script.

The wizard and the script use the software binaries from the shared Oracle home and configure an instance directory on each of the destination hosts for storing configuration files such as `emd.properties`, `targets.xml,` log files, and so on.

**Note:**

- *Shared Agents* can be installed on Exalogic systems.
- Installing a *Shared Agent* on a host running on Microsoft Windows is not supported.
- Unlike the Add Host Target Wizard, the `AgentNFS.pl` script must be run only from a destination host, and at a given time, only one Management Agent can be installed. Therefore, if you want to install only a few Management Agents, then use the `AgentNFS.pl` script.

## 8.2 Before You Begin Installing Shared Agents

Before you begin installing a *Shared Agent,* keep these points in mind:

- When you install a *Shared Agent*, you only configure an instance directory on the destination host to store configuration files; you do not actually install a Management Agent. However, a *Shared Agent* installed on a host behaves exactly like a Management Agent, and has all the features and capabilities of a Management Agent.
- Only the destination host and the *Shared Agent* installed on it get automatically discovered and monitored in the Enterprise Manager system. The targets running on that destination host do not get automatically discovered and added to the Enterprise Manager system.
- The source host (*where the Master Agent is running*) and the destination host must be running on the same operating system.
- The *Master Agent* and the *Shared Agent* must be installed with the same user account.
- *(Only for Graphical Mode)* The Add Host Targets Wizard uses SSH to establish connectivity between Oracle Management Service (OMS) and the remote hosts where you want to install the Management Agents.
- *(Only for Graphical Mode)* Only SSH1 (SSH version 1) and SSH2 (SSH version 2) protocols offered by OpenSSH are supported for deploying a Management Agent.
- *(Only for Graphical Mode)* The Add Host Targets Wizard supports Named Credentials that enable you to use a set of credentials registered with a particular name specifically for this operation, by your administrator. This ensures an additional layer of security for your passwords because as an operator, you can only select the named credential, which is saved and stored by an administrator, and not know the actual user name and password associated with it.

  In case the named credential you select does not have the privileges to perform the installation, then you can set the named credential to run as another user (locked user account). In this case, the wizard logs in to the hosts using the named credential you select, but performs the installation using the locked user account you set.

  For example, you can create a named credential titled User_A (the user account that has remote login access), and set it to run as User_X (the Management Agent install user account for which `no direct login` is set) that has the required privileges. In this case, the wizard logs in to the hosts as User_A, but installs as User_X, using the privilege delegation setting (sudo or PowerBroker) specified in the named credential.

- *(Only for Graphical Mode)* Named credentials support SSH public key authentication and password based authentication. So you can use an existing SSH public key authentication without exposing your passwords.

  To set up SSH public key authentication for a named credential, follow these steps:

  > **Note:** If you have already set up SSH public key authentication for a named credential and the SSH keys are already created, upload the SSH keys to Enterprise Manager, as mentioned in Step 3 of the following procedure.

  1. Navigate to the following location in the OMS home:

     ```
     $<OMS_HOME>/oui/prov/resources/scripts
     ```

     For example,

     ```
     /home/software/em/middleware/oms/oui/prov/resources/scripts
     ```

  2. If the OMS host runs on Oracle Solaris, edit the `sshUserSetup.sh` script to change the following:

     ```
     "SunOS")  SSH="/usr/local/bin/ssh"

               SSH_KEYGEN="/usr/local/bin/ssh-keygen"
     ```

     to

     ```
     "SunOS")  SSH="/usr/bin/ssh"

               SSH_KEYGEN="/usr/bin/ssh-keygen"
     ```

  3. If the OMS host runs on any Unix based operating system, run the `sshUserSetup.sh` script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

     ```
     sshUserSetup.sh -setup -user <agent_install_user_name> -hosts
     <target_hosts>
     ```

     The following SSH keys are created:

     ```
     $HOME/.ssh/id_rsa
     $HOME/.ssh/id_rsa_pub
     ```

     Here, `$HOME` refers to the home directory of the OMS install user.

     If the OMS host runs on Microsoft Windows, install Cygwin on the OMS host (described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*), then run the following script on the OMS host as the OMS user, and pass the Management Agent install user name and the fully qualified name of the target hosts:

     ```
     sshUserSetupNT.sh -setup -user <agent_install_user_name> -hosts
     <target_hosts>
     ```

  4. Upload the SSH keys to Enterprise Manager.

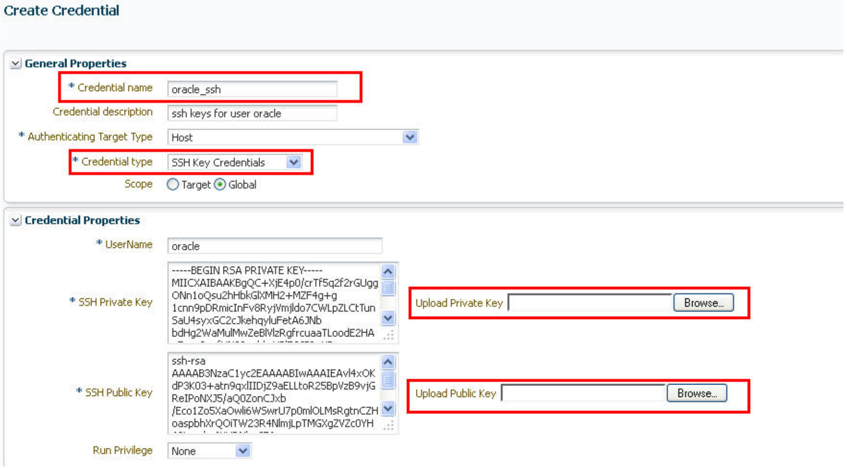
     From the **Setup** menu, select **Security,** then select **Named Credentials.** Click **Create.** For **Credential Name,** specify the name of the credential, for **Credential Type,** select **SSH Key Credentials,** and for **Scope,** select **Global.** If you do not select the **Global** option, you cannot use the SSH named credential to install Management Agents using the Add Host Targets Wizard.

To upload one of the private SSH keys created in Step 3, in the Credential Properties section, specify the location of the private SSH key as a value for the **Upload Private Key** field. Click **Save.**

To upload one of the public SSH keys created in Step 3, in the Credential Properties section, specify the location of the public SSH key as a value for the **Upload Public Key** field. Click **Save.**

Figure 8–1 describes how to upload SSH keys to Enterprise Manager.

***Figure 8–1 Uploading SSH Keys to Enterprise Manager***



Create Credential

General Properties

* Credential name: oracle_ssh

Credential description: ssh keys for user oracle

* Authenticating Target Type: Host

* Credential type: SSH Key Credentials

Scope: ○ Target ● Global

Credential Properties

* UserName: oracle

* SSH Private Key:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQC+XjE4p0/crTf5q2f2rGUgg
ONn1oQsu2hHbkGlXMH2+MZF4g+g
1cnn9pDRmicInFv8RyjVmjldo7CWLpZLCtTun
SaU4syxGC2cJkehqyluFetA6JNb
bdHg2WaMulMwZeBlVlzRgfrcuaaTLoodE2HA
```

Upload Private Key: Browse...

* SSH Public Key:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvl4xOK
dP3K03+atn9qxlIIDjZ9aELLtoR25BpVzB9vjG
ReIPoNXJ5/aQ0ZonCJxb
/Eco1Zo5XaOwli6WSwrU7p0mlOLMsRgtnCZH
oaspbhXrQOiTW23R4NlmjLpTMGXgZVZc0YH
```

Upload Public Key: Browse...

Run Privilege: None

If you have already set up SSH public key authentication for a named credential, you can use the named credential while installing Management Agents using the Add Host Targets Wizard.

- By default, the following types of plug-ins are configured on the *Shared Agent:*
  - All discovery plug-ins that were configured with the OMS from where the Management Agent software is being deployed.
  - Oracle Home discovery plug-in
  - Oracle Home monitoring plug-in
  - All the additional plug-ins deployed on the *Master Agent*
- Upgrading a lower release of Solaris by applying a kernel patch or a patch bundle is not equivalent to installing the actual Solaris 5.10 Update 9 image. Oracle Management Agent 12c Release 5 (12.1.0.5) was built, tested, and certified on a minimum update version of Solaris 5.10 Update 9, so Oracle recommends that you install Oracle Management Agent only on Solaris 5.10 Update 9, and not on any release that was upgraded using patches.

## 8.3 Prerequisites for Installing Shared Agents

Before installing a *Shared Agent*, ensure that you meet the following prerequisites:

***Table 8–1 Prerequisites for Installing Shared 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 *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| Destination Host Disk Space Requirements | Ensure that the *Master Agent* host has a minimum of 1 GB free hard disk space, and the *Shared Agent* host has a minimum of 2 MB free hard disk space. |
| Operating System Requirements | Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager certification matrix available on *My Oracle Support*.<br>You cannot install a *Shared Agent* using a *Master Agent* that runs on a Microsoft Windows platform. *Shared Agents* are not supported on Microsoft Windows platforms.<br>To access the Enterprise Manager certification matrix, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>For information about platforms receiving future support, refer to *My Oracle Support* note 793512.1.<br>**Note:** If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:<br>`cat /etc/release`<br>You should see the output similar to the following. Here, `s10s_u6` indicates that update 6, which is not a supported update level for installation, is installed.<br>`Solaris 10 10/08 s10s_u6wos_07b SPARC` |
| File System Requirements | Ensure that the file system mounted on the destination host does not permit buffered writes. |
| File Descriptor Requirements | ■ Ensure that the maximum user process limit is set to 13312 or greater.<br>To verify the current value set, run the following command:<br>`ulimit -u`<br>If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.<br>■ Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.<br>To verify the current value set, run the following commands:<br>**For Soft Limit:**<br>`/bin/sh -c "ulimit -n"`<br>**For Hard Limit:**<br>`/bin/sh -c "ulimit -Hn"`<br>If the current value is not 4096 or greater, then as a *root* user, update the `/etc/security/limits.conf` file with the following entries:<br>`<UID> soft nofile 4096`<br>`<UID> hard nofile 16384` |
| Package Requirements | Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |

***Table 8–1 (Cont.) Prerequisites for Installing Shared Agent***

| Requirement | Description |
|---|---|
| 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.<br>For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>**Note:** If your enterprise has a policy against installing Management Agents using the OMS install operating system user account, you can use a different operating system user account to install Management Agents. However, ensure that the user account you use and the OMS install user account belong to the same primary group. |
| Software Availability Requirements | Ensure that you already have Oracle Management Agent 12*c* installed as a *Master Agent* in a shared, mounted location.<br>For information on how to install a Management Agent, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.* |
| Software Mount Requirements | Ensure that at least one *Shared Agent* host has read write permissions on the mount location. To mount the Management Agent software on the *Shared Agent* host with read write permissions, run the following command:<br>`mount -t nfs -o rw <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent>`<br>For example, run the following command:<br>`mount -t nfs -o rw abc.oracle.com:/scratch/agent /scratch/agent`<br>To mount the Management Agent software on the *Shared Agent* host with read only permissions, run the following command:<br>`mount -t nfs -o ro <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent>`<br>For example, run the following command:<br>`mount -t nfs -o ro abc.oracle.com:/scratch/agent /scratch/agent`<br>**Note:** Before mounting the Management Agent software on the *Shared Agent* host, ensure that you have created the agent base directory on the *Shared Agent* host, such that the directory has the same path as the agent base directory on the *Master Agent* host. |
| /etc/hosts File Requirements | Ensure that the `/etc/hosts` file on the host has the IP address, the fully qualified name, and the short name in the following format:<br>`172.16.0.0 example.com mypc` |
| Destination Host Access Requirements | Ensure that the destination hosts are accessible from the host where the OMS is running.<br>If the destination host and the host on which OMS is running belong to different network domains, then ensure that you update the `/etc/hosts` file on the destination host to add a line with the IP address of that host, the fully qualified name of that host, and the short name of the host.<br>For example, if the fully-qualified host name is `example.com` and the short name is `mypc`, then add the following line in the `/etc/hosts` file:<br>`172.16.0.0 example.com mypc` |

***Table 8–1 (Cont.) Prerequisites for Installing Shared Agent***

| Requirement | Description |
|---|---|
| Destination Host Credential Requirements<br>*(Only for Graphical Mode)* | Ensure that all the destination hosts running on the same operating system have the same set of credentials. For example, all the destination hosts running on Linux operating system must have the same set of credentials.<br>The wizard installs the Management Agent using the same user account. If you have hosts running on the same operating system but with different credentials, then have two different deployment sessions. |

*Table 8–1 (Cont.) Prerequisites for Installing Shared Agent*

| Requirement | Description |
|---|---|
| Destination Host Time Zone Requirements<br>*(Only for Graphical Mode)* | Ensure that the time zones of the destination hosts have been set correctly. To verify the time zone of a destination host, log in to the OMS host, and run the following command:<br>`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`<br>If the time zone displayed is incorrect, log in to the destination host, and follow these steps:<br>**1.** Run the following commands to set the time zone on the destination host:<br>■ For Korn shell:<br>`TZ=<value>`<br>`export TZ`<br>■ For Bourne shell or Bash shell:<br>`export TZ=<value>`<br>■ For C shell:<br>`setenv TZ <value>`<br>For example, in the Bash shell, run the following command to set the time zone to America/New_York:<br>`export TZ='America/New_York'`<br>To view a list of the time zones you can use, access the supportedtzs.lst file present in the <AGENT_HOME>/sysman/admin directory of the central agent (that is, the Management Agent installed on the OMS host).<br>**2.** Restart the SSH daemon.<br>If the destination host runs on a UNIX based operating system, run the following command:<br>`sudo /etc/init.d/sshd restart`<br>If the destination host runs on a Microsoft Windows operating system, run the following commands:<br>`cygrunsrv -E sshd`<br>`cygrunsrv -S sshd`<br>**3.** Verify whether the SSH server can access the TZ environment variable by logging in to the OMS host, and running the following command:<br>`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`<br>**Note:** If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the destination hosts after installing the Management Agents. For information on setting time zones post install, refer Section 8.5. |

*Table 8–1 (Cont.) Prerequisites for Installing Shared Agent*

| Requirement | Description |
|---|---|
| Time Zone Requirements<br>*(Only for Silent Mode)* | Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:<br>`echo $TZ`<br>If the time zone displayed is incorrect, run the following commands, before running the `agentDeploy.sh` or `agentDeploy.bat` scripts, to set the correct time zone:<br>■ For Korn shell:<br>`TZ=<value>`<br>`export TZ`<br>■ For Bourne shell or Bash shell:<br>`export TZ=<value>`<br>■ For C shell:<br>`setenv TZ <value>`<br>For example, in the Bash shell, run the following command to set the time zone to America/New_York:<br>`export TZ='America/New_York'`<br>To view a list of the time zones you can use, access the `supportedtzs.lst` file present in the `<AGENT_HOME>/sysman/admin` directory of the central agent (that is, the Management Agent installed on the OMS host).<br>**Note:** If you had ignored a prerequisite check warning about wrong time zone settings during the Management Agent install, you must set the correct time zone on the host after installing the Management Agent. For information on setting time zones post install, refer Section 8.5. |
| sudo/pbrun/sesu/su SSH Requirements<br>*(Only for Graphical Mode)* | Ensure that you set the `oracle.sysman.prov.agentpush.enablePty` property to `true` in the `$<OMS_HOME>/sysman/prov/agentpush/agentpush.properties` file, if the privilege delegation tool you are using requires a pseudo terminal for remote command execution via SSH. Most privilege delegation tools such as pbrun, sesu, and su require a pseudo terminal for remote command execution, by default.<br>**Note:** If you are using sudo as your privilege delegation tool, and you do not want to set the `oracle.sysman.prov.agentpush.enablePty` property to `true,` do one of the following:<br>■ Include `Defaults visiblepw` in the `/etc/sudoers` file, or enter the `sudo` command with the `-S` option for **Privileged Delegation Setting** on the Installation Details page.<br>For information on how to access the Installation Details page, see Section 8.4.1.<br>■ Comment out `Defaults requiretty` in the `/etc/sudoers` file. |

*Table 8–1 (Cont.) Prerequisites for Installing Shared Agent*

| Requirement | Description |
|---|---|
| sudo/pbrun/sesu/su Requirements (for *Root* User)<br>*(Only for Graphical Mode)* | ■ Ensure that the installing user has the privileges to invoke the `id` command and the `agentdeployroot.sh` script as *root.* Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`<install_user> ALL=(root) /usr/bin/id, <agent_home>/*/agentdeployroot.sh`<br>For example, `oracle ALL=(root) /usr/bin/id, /u01/app/oracle/admin/shared/agent_home/*/agentdeployroot.sh`<br>Here, `oracle` is the installing user, and `/u01/app/oracle/admin/shared/agent_home` is the *Shared Agent* home.<br>■ You do not require the following entry in the `/etc/sudoers` file for installing a Management Agent. However, the entry is required for performing provisioning and patching operations in Enterprise Manager. Therefore, if you are removing this entry before installing a Management Agent, then ensure that you bring back the entry after installing the Management Agent.<br>**In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), Release 3 (12.1.0.3), Release 4 (12.1.0.4), and Release 5 (12.1.0.5):**<br>`(root) /<AGENT_BASE_DIRECTORY>/sbin/nmosudo`<br>**In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with Bundle Patch 1]:**<br>`(root) /<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo` |

***Table 8–1 (Cont.) Prerequisites for Installing Shared Agent***

| Requirement | Description |
|---|---|
| sudo/pbrun/sesu/su Requirements (for Locked Account User)<br>*(Only for Graphical Mode)* | Ensure that the installing user has the privileges to invoke `/bin/sh` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`login_user1 ALL=(oracle) /bin/sh`<br>Here, `login_user1` is the SSH log in user, and `oracle` is the locked account and install user.<br>If you do not want to grant privileges to the installing user to invoke `/bin/sh` as the locked account user, set the `oracle.sysman.prov.agentpush.pdpShellOutEnabled` property to `false`, and ensure that the installing user has the privileges to invoke `id, chmod, cp, mkdir, rm, tar, emctl, perl, runInstaller,` and `unzip` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool.<br>For example, if you are using sudo as your privilege delegation tool, include the following in the `/etc/sudoers` file to grant the required privileges:<br>`login_user1 ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp,`<br>`/bin/mkdir, /bin/rm, /bin/tar,`<br>`/home/oracle/agentinst/bin/emctl,`<br>`/home/oracle/agentibd/core/12.1.0.5.0/perl/bin/perl,`<br>`/home/oracle/agentibd/core/12.1.0.5.0/oui/bin/runInstaller,`<br>`/home/oracle/agentibd/core/12.1.0.5.0/bin/unzip`<br>Here, `login_user1` is the SSH log in user, `oracle` is the locked account and install user, `/home/oracle/agentinst` is the agent instance directory of the *Shared Agent*, and `/home/oracle/agentibd` is the agent base directory. |
| Temporary Directory Space Requirements | Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.<br>By default, the temporary directory location set to the environment variable `TMP` or `TEMP` is honored. If both are set, then TEMP is honored. If none of them are set, then the following default values are honored: `/tmp` on UNIX hosts and `c:\Temp` on Microsoft Windows hosts. |
| Instance Directory Requirements | Ensure that the *Shared Agent* instance directory (the directory where you want to save the *Shared Agent* configuration files) you specify is empty and has write permissions for the install user. Also, ensure that the parent directory has write permissions for the install user. |
| Shared Oracle Home Requirements | Ensure that the *Master Agent* home is accessible from the destination host where you want to install the *Shared Agent*. Ensure that the *Master Agent* home is mounted with the `setuid` turned on. |
| Path Validation Requirements<br>*(Only for Graphical Mode)* | Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. |
| `CLASSPATH` Environment Variable Requirements | If the value assigned to the CLASSPATH environment variable has white spaces in it, then ensure that you unset it. You can always reset the environment variable to the original value after the installation is complete. |

***Table 8–1 (Cont.) Prerequisites for Installing Shared Agent***

| Requirement | Description |
|---|---|
| Default SSH Port Requirements<br>*(Only for Graphical Mode)* | Ensure that the SSH daemon is running on the default port (that is, 22) on all the destination hosts. To verify the SSH port on a Unix host, run the following command:<br>`netstat -anp \| grep -i sshd`<br>For example, the output of this command may be the following:<br>`tcp      0 0 0.0.0.0:22        0.0.0.0:*         LISTEN 3188/sshd`<br>The above output indicates that the SSH daemon is running on port 22.<br>Also, on a Unix host, you can run the following command to verify the SSH port:<br>`cat /etc/ssh/sshd_config`<br>For a Microsoft Windows host, the SSH port value is mentioned in the `C:\cygwin\etc\sshd_config` file.<br>If the SSH port is a non-default port, that is, any port other than 22, then update the `SSH_PORT` property in the following file:<br>`$<OMS_HOME>/oui/prov/resources/Paths.properties` |
| Port Requirements | Ensure that the default ports described in Section 2.1.10.1 are free. |
| Installing User Requirements | ■ The *Master Agent* and the *Shared Agent* must be installed with the same user account.<br>■ If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group.<br>■ Ensure that the inventory owner and the group to which the owner belongs have *read* and *write* permissions on the inventory directory.<br>For example, if the inventory owner is *abc* and the user installing the Management Agent is *xyz*, then ensure that *abc* and *xyz* belong to the same group, and they have read and write access to the inventory. |
| Central Inventory (oraInventory) Requirements | ■ Ensure that you allocate 100 MB of space on all destination hosts for the Central Inventory.<br>■ The *Shared Agent* uses the inventory location mentioned in the `oraInst.loc` file, which is present in the `<MASTER_AGENT_BASE DIR>/core/12.1.0.5.0/` directory. Ensure that the *Shared Agent* user has read and write permissions on this directory. |
| Preinstallation/Postinstallation Scripts Requirements<br>*(Only for Graphical Mode)* | Ensure that the preinstallation and postinstallation scripts that you want to run along with the installation are available either on the OMS host, destination hosts, or on a shared location accessible to the destination hosts. |

*Table 8–1 (Cont.) Prerequisites for Installing Shared Agent*

| Requirement | Description |
|---|---|
| Browser Requirements<br>*(Only for Graphical Mode)* | ■ Ensure that you use a certified browser as mentioned in the Enterprise Manager certification matrix available on *My Oracle Support*.<br>To access the Enterprise Manager certification matrix, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.<br>■ If you use Microsoft Internet Explorer 8 or 9, do the following:<br>■ Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the **Tools** menu, click **Compatibility View** to disable it if it is enabled. Also, click **Compatibility View Settings** and deregister the Enterprise Manager Cloud Control console URL.<br>■ Enable XMLHTTP. To do so, from the **Tools** menu, click **Internet Options**. Click the **Advanced** tab, and under the **Security** heading, select **Enable native XMLHTTP support** to enable it. |

## 8.4 Installing Shared Agents

This section describes how to install *Shared Agents* using the Add Host Targets Wizard, as well as in silent mode. This section consists of the following:

- Installing Shared Agents Using Add Host Targets Wizard
- Additional Parameters Supported for Installing Shared Agents Using Add Host Targets Wizard
- Installing Shared Agents in Silent Mode
- Response File Parameters for Installing Shared Agents in Silent Mode

> **Important:** If the OMS host is running on Microsoft Windows, and the OMS software was installed in a drive other than `C:\`, then update the `SCRATCH_PATH` variable in `$OMS_HOME\oui\prov\resources\ssPaths_msplats.properties`.
>
> For example, if the OMS software was installed in `D:\`, ensure that you update the `SCRATCH_PATH` variable to `D:\tmpada`

### 8.4.1 Installing Shared Agents Using Add Host Targets Wizard

To install a *Shared Agent* in graphical mode, using Add Host Targets Wizard, follow these steps:

1. In Cloud Control, do one of the following:

   - From the **Setup** menu, select **Add Targets**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.

- From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.

2. On the Host and Platform page, do the following:

   a. Accept the default name assigned for this session or enter a unique name of your choice. 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, `add_host_operation_1`

   A unique deployment activity name enables you to save the installation details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.

   b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to install the Management Agent.

   **Note:**

   - Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
   - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
   - You must ensure that the host name you enter does not have underscores.

   Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager. For information on how the host name entries must appear in the host file, see Section 7.4.1.2

   **Note:** When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

   As the *Shared Agent* can be installed only if the source host and the destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

**Note:** If you are installing a Management Agent on a host that is running on a platform different from the OMS host platform, then ensure that the Management Agent software for that platform is available in Oracle Software Library (Software Library). If the Management Agent software for the required platform is not available in Software Library, acquire and apply the software using the Self Update console.

To access the Self Update Console, from the **Setup** menu, select **Extensibility,** then select **Self Update.** To acquire the latest Management Agent software, click **Agent Software,** select the required software, then click **Download.**

For more information on how to acquire and apply the Management Agent software for a platform using the Self Update console, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

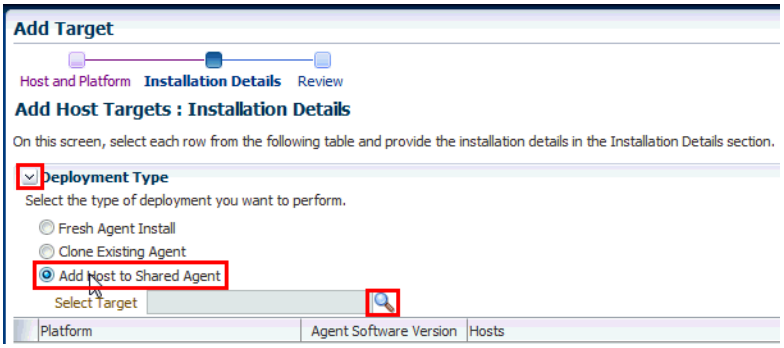
c. Click **Next**.

3. On the Installation Details page, do the following:

   a. In the Deployment Type section, select **Add Host to Shared Agent**. Then, for **Select Target**, click the torch icon and select the Management Agent that is shared and mounted. This location must be visible on all remote hosts.

   Figure 8–2 describes this step.

*Figure 8–2 Installing a Shared Agent*



Add Target

Host and Platform · Installation Details · Review

Add Host Targets : Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type

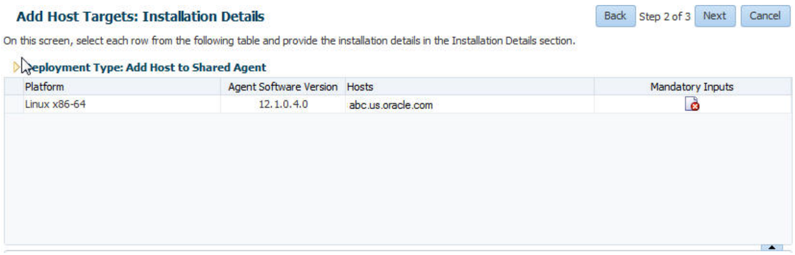
Select the type of deployment you want to perform.

○ Fresh Agent Install
○ Clone Existing Agent
● Add Host to Shared Agent

Select Target

| | Platform | Agent Software Version | Hosts |
|---|---|---|---|

   b. From the table, select the first row that indicates the hosts grouped by their common platform name.



Add Host Targets: Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type: Add Host to Shared Agent

| Platform | Agent Software Version | Hosts | Mandatory Inputs |
|---|---|---|---|
| Linux x86-64 | 12.1.0.4.0 | abc.us.oracle.com | |

   c. In the Installation Details section, provide the installation details common to the hosts selected in Step 3 (b). For **Oracle Home**, validate or enter the location of the shared Management Agent home. Ensure that the Management Agent home is on a shared location, and is accessible from all the destination hosts.

**d.** For **Instance Directory**, enter the absolute path to a directory, on the *Shared Agent* host, where all Management Agent-related configuration files can be stored. Ensure that the directory has write permission.

For example, `/usr/home/software/oracle/agentHome/agent_inst`

If the path you enter does not exist, the application creates a directory at the specified path, and stores all the Management Agent-related configuration files there.

**e.** From **Named Credential** list, select an appropriate profile whose credentials can be used for setting up the SSH connectivity between the OMS and the remote hosts, and for installing a Management Agent on each of the remote hosts.

---

**Note:**

- If you do not have a credential profile, or if you have one but do not see it in the **Named Credential** list, then click the plus icon against this list. In the Create New Named Credential window, enter the credentials and store them with an appropriate profile name so that it can be selected and used for installing the Management Agents. Also set the run privilege if you want to switch over from the Named Credential you are creating, to another user who has the privileges to perform the installation.
- If the plus icon is disabled against this list, then you do not have the privileges to create a profile with credentials. In this case, contact your administrator and either request him/her to grant you the privileges to create a new profile or request him/her to create a profile and grant you the access to view it in the **Named Credential** list.
- If you have manually set up SSH public key authentication between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.

---

**f.** For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

For example, you can specify one of the following for the **Privileged Delegation Setting** field:

```
/usr/bin/sudo -u %RUNAS% %COMMAND%
/usr/bin/sudo -u -S %RUNAS% %COMMAND% (if a pseudo terminal is required for
remote command execution via SSH)
/usr/bin/sesu - %RUNAS% -c "%COMMAND%"
/usr/bin/pbrun %PROFILE% -u %RUNAS% %COMMAND%
/usr/bin/su - %RUNAS% -c "%COMMAND%"
```

If you leave the **Privileged Delegation Setting** field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see Section 8.5.

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

---

**Note:** In the Privilege Delegation setting, the `%RUNAS%` is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

---

g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

   The custom port you enter must not be busy. If you are not sure, you can leave it blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

   If you want to run the script as `root`, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see Table 8–2.

   For example, if you want to provide the inventory pointer location file, then enter `-invPtrLoc` followed by the absolute path to the file location. However, this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

j. Repeat Step 3 (b) to Step 3 (h) for every other row you have in the table.

k. Click **Next**.

4. On the Review page, review the details you have provided and if you are satisfied with the details, then click **Deploy Agent** to install the Management Agent.

   If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

   When you click **Deploy Agent** and submit the deployment session, you are automatically taken to the Add Host Status page that enables you to monitor the progress of the deployment session.

---

**Note:** If you restart the destination host after installing a *Shared Agent,* and the *Shared Agent* does not start up automatically, restore the mount with the original permissions, then start the *Shared Agent* manually.

---

### 8.4.2 Additional Parameters Supported for Installing Shared Agents Using Add Host Targets Wizard

Table 8–2 lists the additional parameters supported for installing a *Shared Agent* in graphical mode.

***Table 8–2 Supported Additional Parameters***

| Parameter | Description |
|---|---|
| EM_STAGE_DIR | Enter the absolute path to a custom location that can be created as a temporary Provisioning Advisor Framework (PAF) staging directory.<br>By default, every time you install a Management Agent, a 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.<br>If you want to override this location with a custom location, you can pass this option and enter a custom location.<br>For example,<br>`EM_STAGE_DIR=/home/john/software/oracle/pafdir` |
| b_startAgent=false | Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured.<br>If you do not specify this parameter, the Management Agent starts automatically once it is installed and configured. |
| b_secureAgent=false | Specify this parameter if you do not want the Management Agent to be secured after the install.<br>If you specify this parameter, ensure that you also specify the OMS HTTP port, using the `EM_UPLOAD_PORT` parameter.<br>For example, `b_secureAgent=false EM_UPLOAD_PORT=4899`<br>If you do not specify this parameter, the Management Agent is secured automatically after the install. |

### 8.4.3 Installing Shared Agents in Silent Mode

To install a *Shared Agent* in silent mode, follow these steps:

**On the Master Agent Host:**

1. Run the `create_plugin_list.pl` script from the *Master Agent* host:

```
$AGENT_HOME/perl/bin/perl $AGENT_HOME/sysman/install/create_plugin_
list.pl -instancehome <AGENT_INSTANCE_HOME>
```

**On the Shared Agent Host:**

1. Create a response file titled `AgentNFS.rsp` as described in Table 8–3.

> **Note:** The response file you create can have any name, and not necessarily `AgentNFS.rsp`. For easy understanding, this chapter uses the name `AgentNFS.rsp`. Also, instead of creating a response file, you can choose to pass the arguments explicitly while invoking the script. However, Oracle recommends that you create a response file and capture the information there.

2. Invoke the script from the *Shared Agent* host, and pass the response file.

```
$<AGENT_HOME>/perl/bin/perl <AGENT_HOME>/sysman/install/AgentNFS.pl
-responseFile <absolute_path_to_response_file>
```

For example,

```
/scratch/agent_base_dir/core/12.1.0.5.0/perl/bin/perl /scratch/agent_
base_dir/core/12.1.0.5.0/sysman/install/AgentNFS.pl -responseFile
/home/john/AgentNFS.rsp
```

Ensure that `<AGENT_HOME>` is a shared location, and is accessible from all the destination hosts.

---

**Note:**

- Instead of creating a response file, you can choose to pass all the arguments explicitly while invoking the script. In this case, invoke the script in the following way:

  ```
  $<AGENT_HOME>/perl/bin/perl <AGENT_
  HOME>/sysman/install/AgentNFS.pl AGENT_INSTANCE_
  HOME=<absolute_path_to_instance_dir> ORACLE_
  HOME=<absolute_path_to_master_agent_oracle_home>
  <parameter1>=<value1> <parameter2>=<value2>
  <parameter3>=<value3>...
  ```

  For example,

  ```
  /scratch/agent_base_dir/core/12.1.0.5.0/perl/bin/perl
  /scratch/agent_base_
  dir/core/12.1.0.5.0/sysman/install/AgentNFS.pl AGENT_
  INSTANCE_HOME=/<local_location>/agent_inst ORACLE_
  HOME=/scratch/agent_base_dir/core/12.1.0.5.0 AGENT_
  PORT=1832 AGENT_REGISTRATION_PASSWORD=welcome b_
  startAgent=TRUE
  ```

  While specifying `AGENT_INSTANCE_HOME,` ensure that the location you specify is local to the host and is not reused by any other host.

- If the *Master Agent* was installed using the Add Host Targets Wizard, then ensure that you pass the following arguments with these values:

  ```
  AGENT_REGISTRATION_PASSWORD=<password>
  ```

  ```
  b_startAgent=TRUE
  ```

- Do NOT pass the `-invPtrLoc` argument because, by default, the location `<AGENT_HOME>/oraInst.loc` is honored, where `<AGENT_HOME>` is the *Master Agent*. Also ensure that the Oracle Inventory directory, to which the inventory file points, is not in a shared location.

- If you restart the destination host after installing a *Shared Agent,* and the *Shared Agent* does not start up automatically, restore the mount with the original permissions, then start the *Shared Agent* manually.

---

3. When prompted to run the `root.sh` script, run it from the instance directory of the *Shared Agent:*

   ```
   <AGENT_INSTANCE_HOME>/root.sh
   ```

If you are not a *root* user, then use SUDO to change to a *root* user. For example, run the following command:

```
/usr/local/bin/sudo /scratch/OracleHomes/agent_inst/root.sh
```

4. Repeat Step (2) to Step (4) on the remaining hosts where you want to install the *Shared Agent*.

### 8.4.4 Response File Parameters for Installing Shared Agents in Silent Mode

To install a *Shared Agent* in silent mode, you must invoke the `AgentNFS.pl` script and pass a response file that captures all the required information. Table 8–3 describes the various parameters you must include in the response file.

***Table 8–3 Creating a Response File for Installing Oracle Management Agent Using the AgentNFS.pl Script***

| Parameter | Description |
|---|---|
| ORACLE_HOME | Specify the absolute path to the *Master Agent* home, which is shared and visible on the destination host.<br>For example, `/scratch/agent_base_dir/core/12.1.0.5.0` |
| AGENT_PORT | *(Optional)* Enter the port on which the *Shared Agent* process should be started. You can enter any free port between 1830 and 1849. The same port is used for both HTTP and HTTPS.<br>For example, `1832` |
| AGENT_INSTANCE_HOME | Specify the absolute path to a location on the destination host where you want to store all Management Agent-related configuration files.<br>For example, `/<local_location>/agent_inst`<br>Ensure that this location is local to the host and is not reused by any other host. |
| AGENT_REGISTRATION_PASSWORD | Enter a password for registering new Management Agents that join the Enterprise Manager system.<br>By default, the communication between the OMS and the Management Agents is secured and locked. Any new Management Agents that join the Enterprise Manager system must be authenticated before they become part of the system. The password you enter here will be used for authenticating those new Management Agents.<br>For example, `Wel456come`<br>**Note:** If the *Master Agent* was installed using the Add Host Targets Wizard, then you must pass this parameter. |
| b_startAgent | Set it to `TRUE` so that the *Shared Agent* is started automatically once it is installed and configured.<br>**Note:** If the *Master Agent* was installed using the Add Host Targets Wizard, then you must pass this parameter. |
| ORACLE_HOSTNAME | *(Optional) (Only for Installation on Virtual Hosts)* Specify the virtual host name where you are installing the *Shared Agent*. |
| ALLOW_IPADDRESS | *(Optional)* Enter `TRUE` if you want to specify an IP address for `ORACLE_HOSTNAME`. If `ALLOW_IPADDRESS` is set to `FALSE`, a prerequisite check fails when you specify an IP address for `ORACLE_HOSTNAME` while installing a Management Agent.<br>For example, `ALLOW_IPADDRESS=TRUE`<br>If you do not include this parameter, it defaults to `FALSE`. |

*Table 8–3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using the AgentNFS.pl Script*

| Parameter | Description |
|---|---|
| START_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is started. This parameter accepts values between `0` and `99`. However, Oracle recommends that you provide a value between `91` and `99` for this parameter.<br>For example, `START_PRIORITY_LEVEL=95`<br>If you do not include this parameter, it defaults to `98`. |
| SHUT_PRIORITY_LEVEL<br>(For Unix based hosts only) | *(Optional)* Use this parameter to specify the priority level of the Management Agent service when the host is shut down. This parameter accepts values between `0` and `99`.<br>For example, `SHUT_PRIORITY_LEVEL=25`<br>If you do not include this parameter, it defaults to `19`. |
| PROPERTIES_FILE | *(Optional)* Use this parameter to specify the absolute location of the properties file.<br>For example, `PROPERTIES_FILE=/tmp/agent.properties`<br>In the properties file, specify the parameters that you want to use for the Management Agent deployment. The list of parameters that you can specify in the properties file is present in `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:<br>`REPOSITORY_PROXYHOST=abc.example.com`<br>`REPOSITORY_PROXYPORT=1532`<br>The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:<br>`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>` |

## 8.5 After Installing Shared Agents

After you install a *Shared Agent*, follow these steps:

1. *(Only for Graphical Mode)* Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization**, **Remote Prerequisite Check**, and **Agent Deployment**.

   > **Note:** In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.
   >
   > If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

   If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

- Ignore the warning or failure, and continue with the session if you prefer.
    - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, Ignoring Failed Hosts.**
    - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do so, click **Continue** and select **Continue, All Hosts**.
- Fix the problem by reviewing the error description carefully, understanding its cause, and taking action as recommended by Oracle.
    - You can choose to retry the deployment of Management Agents with the same installation details. To do so, click **Retry** and select **Retry Using Same Inputs.**
    - You can retry the deployment of Management Agents with modified installation details. To do so, click **Retry** and select **Update Inputs and Retry.**

2. Verify the installation:

    a. Navigate to the *Shared Agent* instance home and run the following command to see a message that confirms that the Management Agent is up and running:

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

    b. Navigate to the *Shared Agent* home and run the following command to see a message that confirms that EMD upload completed successfully:

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

3. *(Only for Graphical Mode)* If you have restrictive Privilege Delegation Provider (PDP) configuration settings, enter the location of `nmosudo` in your PDP configuration file.

    Enterprise Manager supports PDPs such as SUDO and PowerBroker that enable administrators to restrict certain users from running certain commands.

    In Enterprise Manager Cloud Control 12*c* Release 2 (12.1.0.2), Release 3 (12.1.0.3), Release 4 (12.1.0.4), and Release 5 (12.1.0.5), `nmosudo` is located in the `sbin` directory, which is in the agent base directory. For example, `<AGENT_BASE_DIRECTORY>/sbin/nmosudo`. In Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.1) [with or without Bundle Patch 1], `nmosudo` is located in the agent instance directory. For example, `<AGENT_INSTANCE_DIRECTORY>/bin/nmosudo`.

    Therefore, when you install a 12.1.0.5 Management Agent, you must modify your PDP configuration file to update the new location of `nmosudo`.

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

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

4. (Only for UNIX Operating Systems) Manually run the following scripts as a *root* user:

    - If this is the first Oracle product you installed on the host, then run the `orainstRoot.sh` script from the inventory location specified in the `oraInst.loc` file that is available in the *Shared Agent* home.

For example, if the inventory location specified in the `oraInst.loc` file is `$HOME/oraInventory`, then run the following command:

```
$HOME/oraInventory/orainstRoot.sh
```

- Run the `root.sh` script from the *Shared Agent* home:

  ```
  $<AGENT_HOME>/root.sh
  ```

5. If you had ignored a prerequisite check warning about wrong time zone settings, run the following command and follow the steps it displays:

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

6. By default, the host and the *Shared Agent* get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host 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.

   To add the host targets and the `oracle_emd` targets to the *Shared Agent,* run the following command:

   ```
   $<SHARED_AGENT_HOME>/bin/emctl config agent addinternaltargets
   ```

   For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

   > **Note:** If Oracle Management Agents 12c (12.1.0.x) hang frequently or do not respond on Solaris 9ux and 10ux operating systems, then refer to document ID 1427773.1 on My Oracle Support.

# 9

# Installing the Oracle Management Agent Software Now and Configuring It Later

This chapter explains how you can install only the software binaries of Oracle Management Agent (Management Agent) at one point and configure the installation at a later stage. In particular, this chapter covers the following:

## 9.1 Overview of Installing a Management Agent and Configuring It Later

You can choose to install only the software binaries of the Management Agent at one point and configure it at a later stage to work with the associated Oracle Management Service (OMS). This approach enables you to divide the installation process into two phases, mainly the installation phase and the configuration phase.

During the installation phase, you invoke the `agentDeploy.sh` script passing the `-softwareOnly` argument to copy the software binaries and create an Oracle home for the Management Agent. During the configuration phase, you invoke the same script passing `-configOnly` to configure the software binaries.

Understandably, the installation phase takes much lesser time compared to the configuration phase because the installation phase involves only copying of binaries. This helps you plan your installation according to the time and priorities you have.

**Note: This installation type is available only in silent mode.**

**Note:** If you want to repoint your existing Management Agents to a new Oracle Management Service (OMS), then you must first deinstall those Management Agents and plug-ins, and then redeploy those Management Agents and plug-ins using the new OMS. This is typically done when you want to move from an Enterprise Manager Cloud Control system in a test environment to an Enterprise Manager Cloud Control system in a production environment.

When you repoint your existing Management Agents to a new OMS, you cannot move the targets monitored by the Management Agents, the target history, and the Management Agent history. The monitored targets and the history data is lost.

## 9.2 Before You Begin Installing a Management Agent

Before you begin installing a Management Agent, review the points outlined in Section 6.2.

## 9.3 Prerequisites for Installing a Management Agent

Before installing the Management Agent, ensure that you meet the prerequisites described in Section 6.3.

## 9.4 Installing Only the Management Agent Software Binaries

To install only the software binaries of a Management Agent in silent mode, follow one of the procedures mentioned in Section 6.4.2. While invoking the deployment script, ensure that you pass the `-softwareOnly` option:

```
<Software_Extracted_Location>/agentDeploy.sh AGENT_BASE_DIR=<absolute_
path_to_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile>
-softwareOnly
```

For example, `/tmp/agtImg/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c RESPONSE_FILE=/tmp/agtImg/agent.rsp -softwareOnly`

If the Management Agent is installed successfully, a message mentioning so is displayed on the command line.

**Note:** Do not pass the option `-forceConfigure`.

## 9.5 Configuring the Management Agent Software Binaries

To configure the software binaries of a Management Agent in silent mode, invoke the deployment script with the following options from the Management Agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<absolute_path_
to_agentbasedir> RESPONSE_FILE=<absolute_path_to_responsefile> -configOnly
```

For example, `$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=/scratch/agent12c RESPONSE_FILE=/tmp/agtImg/agent.rsp -configOnly`

If the Management Agent is installed successfully, a message mentioning so is displayed on the command line.

**Note:**

- The response file you pass here is the same response file you passed in Section 9.4.
- Do not pass the option `-forceConfigure`.

## 9.6 After Installing a Management Agent

After you install the Management Agent, follow the steps outlined in Section 6.5.

# Part V

# Advanced Installation and Configuration

This part describes the advanced installation and configuration tasks you can perform after you have installed Enterprise Manager Cloud Control and have started using the product.

In particular, this part contains the following chapters:

# 10

# Configuring Enterprise Manager for Firewalls

Firewalls protect a company's Information Technology (IT) infrastructure by providing the ability to restrict network traffic by examining each network packet and determining the appropriate course of action.

Firewall configuration typically involves restricting the ports that are available to one side of the firewall, for example the Internet. It can also be set up to restrict the type of traffic that can pass through a particular port such as HTTP. If a client attempts to connect to a restricted port (a port not covered by a security "rule") or uses a protocol that is incorrect, then the client will be disconnected immediately by the firewall. Firewalls can also be used within a company Intranet to restrict user access to specific servers.

You can deploy the components of Oracle Enterprise Manager on different hosts throughout your enterprise. These hosts can be separated by firewalls. This chapter describes how firewalls can be configured to allow communication between the Enterprise Manager components.

This chapter contains the following sections:

- About Configuring Firewalls to Allow ICMP and UDP Traffic for Oracle Beacons
- About Enabling ICMP Echo Requests on Firewalls

## 10.1 About Considering Firewall Configurations While Using Enterprise Manager

Firewall configuration should be the last phase of Enterprise Manager deployment. Before you configure your firewalls, make sure you are able to log in to the Enterprise Manager console and that your Oracle Management Agents (Management Agent) are up and are monitoring targets.

If you are deploying Enterprise Manager in an environment where firewalls are already installed, open the default Enterprise Manager communication ports for all traffic until you have completed the installation and configuration processes and are certain that you are able to log in to Enterprise Manager and that your Management Agents are up and monitoring targets.

The default communication ports for Enterprise Manager are assigned during the installation. If you modify the default ports, be sure to use the new port assignments when you configure the firewalls.

If you are enabling Enterprise Manager Framework Security for the Oracle Management Service (OMS), the final step in that configuration process is to restrict uploads from the Management Agents to secure channels only. Before completing that step, configure your firewalls to allow both HTTP and HTTPS traffic between the Management Agent and Management Repository and test to be sure that you can log in to Enterprise Manager and that data is being uploaded to the Management Repository.

After you have confirmed that the OMS and Management Agents can communicate with both protocols enabled, complete the transition to secure mode and change your firewall configuration as necessary. If you incrementally configure your firewalls, it will be easier to troubleshoot any configuration problems.

## 10.2 Default Ports Used by Enterprise Manager Components

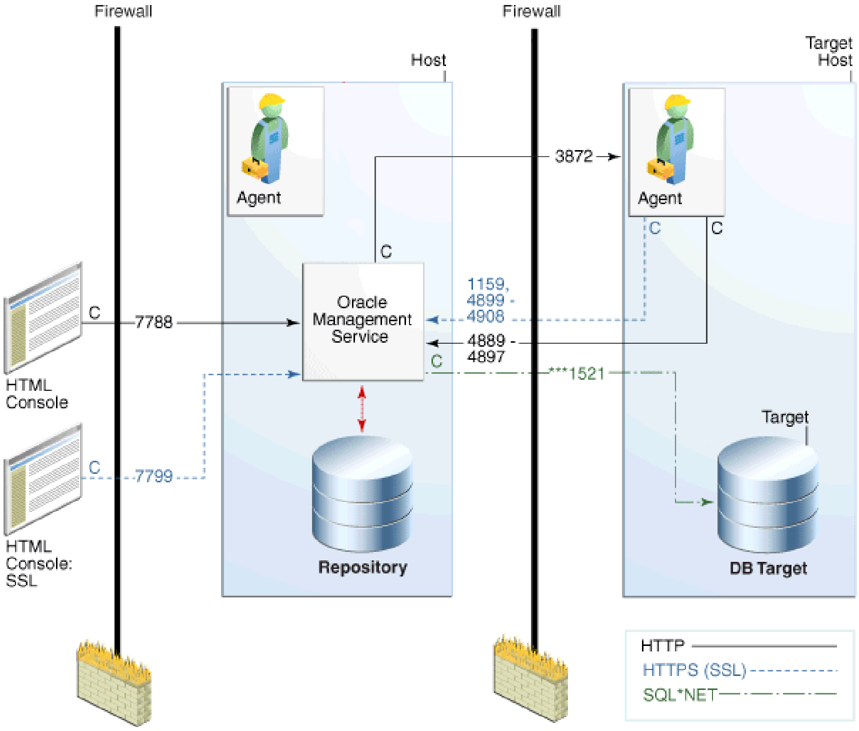
To learn about the ports used by the Enterprise Manager components, see Section 2.1.10.

## 10.3 About Firewall Configurations for Enterprise Manager

Your main task in enabling Enterprise Manager to work in a firewall-protected environment is to take advantage of proxy servers whenever possible, to make sure only the necessary ports are open for secure communications, and to make sure that only data necessary for running your business is allowed to pass through the firewall.

Figure 10–1 provides a topology of an Enterprise Manager environment that is using a firewall, and also illustrates the default ports that can be used.

***Figure 10–1 Firewall Port Requirements (Default)***



The conventions used in the preceding illustration are as follows:

***Table 10–1 Conventions Used In Illustration***

| Convention | Description |
|---|---|
| C | Is the entity that is making the call. |
| * | Enterprise Manager will default to the first available port within an Enterprise Manager set range. |
| ** | Enterprise Manager will default to the first available port. |
| *** | Database listener ports. |

**Notes:**

- The direction of the arrows specify the direction of ports.
- Port 1159, 4898-4989 indicates that 1159 is the default. If this port is not available, the Oracle Management Service will search in the specified range (4889 - 4897).
- To clone between two target hosts separated by a firewall, the agents will need to communicate to each other on the agent ports. The initiating Management Agent will make the call.
- Allow ICMP (0) Echo Reply and ICMP (8) Echo Request in the firewall.

## 10.4 About Firewalls Between Your Web Browser and the Enterprise Manager Console

Connections from your web browser to the Enterprise Manager console are performed over the default port used for your Oracle HTTP Server.

For example, the default, non-secure port for the Oracle HTTP Server is usually port 7788. If you are accessing the Enterprise Manager console using the following URL and port, then you must configure the firewall to allow the Enterprise Manager console to receive HTTP traffic over port 7788:

```
http://omshost.example.com:7788/em
```

On the other hand, if you have enabled security for your Oracle HTTP Server, you are likely using the default secure port for the server, which is usually port 7799. If you are accessing the Enterprise Manager console using the following URL and port, then you must configure the firewall to allow the Enterprise Manager console to receive HTTPS traffic over port 7799:

```
https://omshost.example.com:7799/em
```

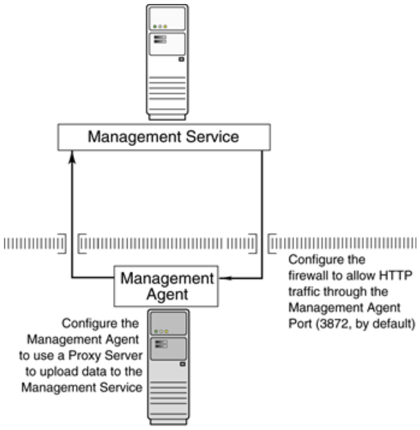
## 10.5 About Configuring a Management Agent on a Host Protected by a Firewall

If a Management Agent is installed on a host that is protected by a firewall and the OMS is on the other side of the firewall, you must perform the following tasks:

- Configure the Management Agent to use a proxy server for its uploads to the OMS, as described in Section 10.6.
- Configure the firewall to allow incoming HTTP traffic from the OMS on the Management Agent port. Regardless of whether or not Enterprise Manager Framework Security has been enabled, the default port is 3872. Incoming traffic can be received only if the port corresponding to the Management Agent is open in the firewall.

Figure 10–2 illustrates the connections the Management Agent must make when it is protected by a firewall.

***Figure 10–2 Configuration Tasks When the Management Agent Is Behind a Firewall***


Management Service
Management Agent
Configure the firewall to allow HTTP traffic through the Management Agent Port (3872, by default)
Configure the Management Agent to use a Proxy Server to upload data to the Management Service

The illustration shows a diagram of the Management Agent and the Management Service. A line representing the firewall appears between the Management Agent and the Management Service.

Two additional lines represent data being uploaded to the Management Service and the Management Service contacting the Management Agent, respectively. Text in the diagram explains how you need to:

- Configure the Management Agent to use a proxy server to upload data to the Management Service
- Open the Management Agent port (usually 1830) in the firewall so the Management Service can communicate with the Management Agent.

***********************************************************************************************

## 10.6 Configuring a Management Agent to Use a Proxy Server

You can configure a Management Agent to use a proxy server for its communications with an OMS outside the firewall, or to manage a target outside the firewall. To do so, follow these steps:

1. From the **Setup** menu, select **Agents**.
2. Click the Agent you want to configure in the Name column in the Management Agents table. The target home page for the Management Agent opens.
3. Select **Properties** from the **Agent** menu.
4. Select **Advanced Properties** from the pull down menu.
5. Supply the correct values for the `REPOSITORY_PROXYHOST` and `REPOSITORY_PROXYPORT` properties.
6. Click **Apply** to save your changes, which will be saved to the *AGENT_HOME*`/sysman/config/emd.properties` file.

> **Note:** The proxy password will be obfuscated when you restart the Management Agent.

## 10.7 About Configuring a Firewall to Allow the OMS to Communicate With the Management Agents

While the Management Agents in your environment must upload data from your managed hosts to the OMS, the OMS must also communicate with the Management Agents. As a result, if the Management Agent is protected by a firewall, the OMS must be able to contact the Management Agent through the firewall on the Management Agent port.

By default, the Enterprise Manager installation procedure assigns port 3872 to the Management Agent. However, if that port is occupied, the installation may assign an alternate port number.

After you determine the port number assigned to the Management Agent, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

## 10.8 About Configuring the OMS on a Host Protected by a Firewall

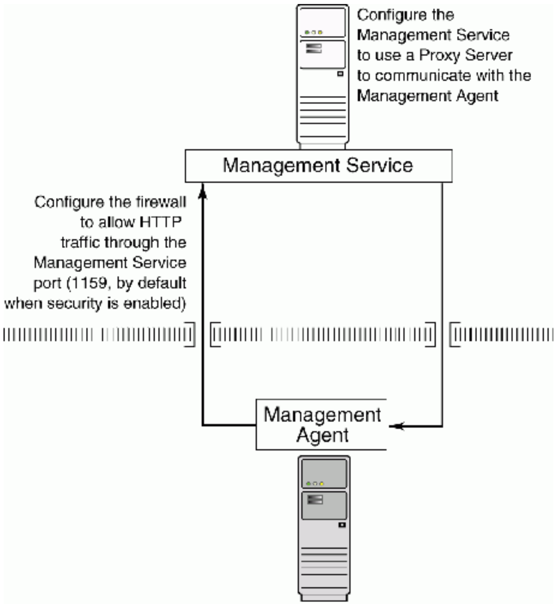
If your OMS is installed on a host that is protected by a firewall and the Management Agents that provide management data are on the other side of the firewall, you must perform the following tasks:

- Configure the OMS to use a proxy server for its communication with the Management Agents, as described in Section 10.9.
- Configure the firewall to allow incoming HTTP traffic from the Management Agents on the Management Repository upload port.

  If you have enabled Enterprise Manager Framework Security, the upload URL uses port 1159 by default. If this port is not available, Enterprise Manager will default to first available port in the range 4899-4908. If you have *not* enabled Enterprise Manager Framework Security, the upload port is the first available port in the range 4889 - 4897.

Figure 10–3 illustrates the connections the Management Agent must make when it is protected by a firewall.

*Figure 10–3    Configuration Tasks When the Management Service Is Behind a Firewall*


Configure the Management Service to use a Proxy Server to communicate with the Management Agent
Management Service
Configure the firewall to allow HTTP traffic through the Management Service port (1159, by default when security is enabled)
Management Agent

The illustration shows a diagram of the Management Agent and the Oracle Management Service. A line representing the firewall appears between them. The diagram includes text that explains how you must:

- Configure the Management Service to use a proxy server for connections to the Management Agent
- Open the upload URL port in the firewall so that data can be uploaded from the Management Agent to the Management Service.

*******************************************************************************************************************

## 10.9 Configuring the OMS to Use a Proxy Server to Communicate with Management Agents

This section describes how to configure the OMS to use a proxy server for its communication with Management Agents outside the firewall.

To configure the OMS to use a proxy server, do the following:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**

   > **Note:** The Proxy Settings for Agents page enables you to configure a proxy server that can be used for communication only from the OMS to the Management Agent, and not from the Management Agent to the OMS. Any proxy server you configure will be used for the communication between the OMS and all the Management Agents.

2. Select **Manual proxy configuration.**

3. Specify values for **Protocol, Proxy Server Host, Port,** and **No Proxy for.** If the specified proxy server has been configured using a security realm, login credentials, or both, then specify values for **Realm, User Name,** and **Password.**
4. Under the Test URL section, specify a Management Agent URL for **URL,** then click **Test** to test if the OMS can communicate with the specified Management Agent using the specified proxy server.
5. If the connection is successful, click **Apply** to save the proxy settings to the repository.
6. Restart the OMS. If you are using a multi-OMS setup, restart all the OMSes.

   To restart an OMS that runs on a Unix based platform, run the following commands:

   ```
   <OMS_HOME>/bin/emctl stop oms
   <OMS_HOME>/bin/emctl start oms
   ```

   To restart an OMS that runs on a Microsoft Windows platform, follow these steps:

   1. Right-click **My Computer,** then select **Manage.**
   2. In the Computer Management window, in the left pane, expand **Services and Applications,** then select **Services.**
   3. Select the `OracleManagementServer_EMGC_OMS*` service, then click the restart button.

## 10.10 About Configuring a Firewall to Allow Management Agents to Upload Data to the OMS

While the Management Agents in your environment must contact the Management Agents on your managed hosts, the OMS must also be able to receive the uploaded data from the Management Agents. If the OMS is behind a firewall, you must configure the firewall to allow the Management Agents to upload data on the upload port.

By default, the Enterprise Manager installation procedure assigns port 4889 as the Repository upload port. However, if that port is occupied, the installation will assign an alternate port number.

In addition, when you enable Enterprise Manager Framework Security, the upload port is automatically changed to the secure 1159 HTTPS port.

Administrators can also change the upload port after the installation.

After you determine the port number assigned to the OMS upload port, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

## 10.11 About Enabling the OMS to Access My Oracle Support

Unless online access to the Internet is strictly forbidden in your environment, OMS should be enabled to access My Oracle Support. This access is necessary to enable updates and patches to be downloaded, for example.

At minimum, the following URLs should be made available through the firewall:

- `aru-akam.oracle.com`

- `ccr.oracle.com`
- `login.oracle.com`
- `support.oracle.com`
- `updates.oracle.com`

Ensure that the default ports, that is, port 80 for HTTP connectivity and port 443 for HTTPS connectivity, are used to connect to the mentioned URLs.

## 10.12 About the dontProxyfor Property

When you configure the OMS or a Management Agent to use a proxy server, it is important to understand the purpose of the `dontProxyFor` property, which identifies specific URL domains for which the proxy will not be used.

For example, suppose the following were true:

- You have installed the OMS and several Management Agents on hosts that are inside the company firewall. These hosts are in the internal `.example.com` and `.example.us.com` domains.
- You have installed several additional Management Agents on hosts that are outside the firewall. These hosts are installed in the `.example.uk` domain.
- You have configured Enterprise Manager to automatically check for critical software patches on My Oracle Support.

In this scenario, you want the OMS to connect directly to the Management Agents inside the firewall without using the proxy server. On the other hand, you want the OMS to use the proxy server to contact the Management Agents outside the firewall, as well as the My Oracle Support site, which resides at the following URL:

```
http://support.oracle.com
```

The following properties will prevent the OMS from using the proxy server for connections to the Management Agents inside the firewall. Connections to My Oracle Support and to Management Agents outside the firewall will be routed through the proxy server:

```
proxyHost=proxy42.example.com
proxyHost=80
dontProxyFor=.example.com, .example.us.com
```

## 10.13 About Firewalls Between the OMS and the Management Repository

Secure connections between the OMS and the Management Repository are performed using features of Oracle Advanced Security. As a result, if the OMS and the Management Repository are separated by a firewall, you must configure the Oracle Net firewall proxy to allow the OMS to access the repository. Also, if you have configured a timeout for this firewall, ensure that you tune the `SQLNET.EXPIRE_TIME` parameter for Dead Connection Detection (DCD) at the database side, and set this parameter (in `$ORACLE_HOME/network/admin/sqlnet.ora`) to a value smaller than the value of the timeout configured for the firewall.

## 10.14 About Firewalls Between Enterprise Manager and a Managed Database Target

When you are using the Enterprise Manager console to manage a database, you must log in to the database from the Enterprise Manager console in order to perform certain monitoring and administration tasks. If you are logging in to a database on the other side of a firewall, you will need to configure the firewall to allow Oracle Net firewall proxy access.

Specifically, to perform any administrative activities on the managed database, you must be sure that the firewall is configured to allow the OMS to communicate with the database through the Oracle Listener port.

You can obtain the Listener port by reviewing the Listener home page in the Enterprise Manager console.

## 10.15 About Using Firewalls with Multiple OMS Instances

Enterprise Manager supports the use of multiple OMS instances that communicate with a common Management Repository. For example, using more than one OMS can be helpful for load balancing as you expand your central management capabilities across a growing e-business enterprise.

When you deploy multiple OMS instances in an environment protected by firewalls, be sure to consider the following:

- Each Management Agent is configured to upload data to one OMS. As a result, if there is a firewall between the Management Agent and its OMS, you must configure the firewall to allow the Management Agent to upload data to the OMS using the upload URL.

  **See Also:** Section 10.5, "About Configuring a Management Agent on a Host Protected by a Firewall"

  Section 10.8, "About Configuring the OMS on a Host Protected by a Firewall"

- In addition, each OMS must be able to contact any Management Agent in your enterprise so it can check for the availability of the Management Agent. As a result, you must be sure that your firewall is configured so that each OMS you deploy can communicate over HTTP or HTTPS with any Management Agent in your enterprise.

  Otherwise, an OMS without access to a particular Management Agent may report incorrect information about whether or not the Management Agent is up and running.

  **See Also:** "About Availability" in the Enterprise Manager online help for information about how Enterprise Manager determines host and Management Agent availability.

## 10.16 About Configuring Firewalls to Allow ICMP and UDP Traffic for Oracle Beacons

Oracle Beacons provide application performance availability and performance monitoring. They are part of the Application Service Level Management features of Enterprise Manager.

**See Also:** "About Application Service Level Management" in the Enterprise Manager Online Help

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) to transfer data between Oracle Beacons and the network components you are monitoring. There may be situations where your Web application components and the Beacons you use to monitor those components are separated by a firewall. In those cases, you must configure your firewall to allow ICMP, UDP and HTTP traffic.

## 10.17 About Enabling ICMP Echo Requests on Firewalls

OMS uses the Internet Control Message Protocol (ICMP) Echo Request to check the status target host machines. If the ICMP Echo Request is blocked by the firewall, a host machine will appear to be down.

To determine the status of any machine in the environment, ICMP Echo Requests must be enabled on the firewall. If the ICMP Echo Request is enabled, the `ping` command can be issued by the OMS to check the status of the machine.

Ensure that you allow ICMP (0) Echo Reply and ICMP (8) Echo Request in the firewall.

# 11

# Sizing Your Enterprise Manager Deployment

Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.5 has the ability to scale for hundreds of users and thousands of systems and services on a single Enterprise Manager implementation.

This chapter describes techniques for achieving optimal performance using the Oracle Enterprise Manager application. It can also help you with capacity planning, sizing and maximizing Enterprise Manager performance in a large scale environment. By maintaining routine housekeeping and monitoring performance regularly, you insure that you will have the required data to make accurate forecasts of future sizing requirements. Receiving good baseline values for the Enterprise Manager Cloud Control vital signs and setting reasonable warning and critical thresholds on baselines allows Enterprise Manager to monitor itself for you.

Sizing is a critical factor in Enterprise Manager performance. Inadequately-sized Enterprise Manager deployments may result in the overall benefits of Enterprise Manager being compromised. The resources required for the Enterprise Manager Oracle Management (OMS) Service and Management Repository tiers will vary significantly based on the number of monitored targets. While there are many additional aspects to be considered when sizing Enterprise Manager infrastructure, these guidelines provide a simple methodology that can be followed to determine the minimum required hardware resources and initial configuration settings for the OMS and Management Repository tiers.

This chapter contains the following sections:

- Enterprise Manager Cloud Control Sizing
- Enterprise Manager Cloud Control Performance Methodology
- Overview of Repository and Sizing Requirements for Fusion Middleware Monitoring

## 11.1 Enterprise Manager Cloud Control Sizing

Oracle Enterprise Manager provides a highly available and scalable deployment topology. This chapter lays out the basic minimum sizing and tuning recommendations for initial capacity planning for your Oracle Enterprise Manager deployment. This chapter assumes a basic understanding of Oracle Enterprise Manager components and systems. A complete description of Oracle Enterprise Manager can be obtained from `http://docs.oracle.com/cd/E24628_01/doc.121/e25353/overview.htm`. This information is a starting point for site sizing. Every site has its own characteristics and should be monitored and tuned as needed.

Sizing is a critical factor for Enterprise Manager performance. Inadequately sized Enterprise Manager deployments will result in frustrated users and the overall benefits of Enterprise Manager may be compromised. The resources required for Enterprise Manager OMS and Repository tiers will vary significantly based on the number of monitored targets. While there are many additional aspects to be considered when sizing Enterprise Manager infrastructure, the following guidelines provide a simple methodology that can be followed to determine the minimum required hardware resources and initial configuration settings for the OMS and Repository tiers.

## 11.1.1 Overview of Sizing Guidelines

The following sections provide an overview of the sizing guidelines.

### 11.1.1.1 Hardware Information

The sizing guidelines outlined in this chapter were obtained by running a virtual environment on the following hardware and operating system combination.

- Hardware -- Oracle's Sun Fire X4170 M2
- Hypervisor -- 64 bit Linux Oracle Virtual Server
- Operating System of Virtual Machines -- 64 bit Oracle Enterprise Linux

The virtual environment setup had a one to one mapping of CPUs between the Oracle Virtual Server (OVS) host and the virtual machines running on it. The OVS servers had enough RAM to support all virtual machines without memory swapping.

This information is based on a 64-bit Oracle Enterprise Linux environment. If you are running on other platforms, you will need to convert the sizing information based on similar hardware performance. This conversion should be based on single-thread performance. Running on a machine with 24 slow cores is not equivalent to running on a machine with 12 fast cores even though the total machine performance might be the same on a throughput benchmark. Single thread performance is critical for good Enterprises Manager user interface response times.

### 11.1.1.2 Sizing Specifications

The sizing guidelines for Oracle Enterprise Manager are divided into four sizes: Eval, Small, Medium and Large. The definitions of each size are shown in Table 11–1.

*Table 11–1 Oracle Enterprise Manager Site Sizes*

| Size | Agent Count | Target Count | Concurrent User Sessions |
|---|---|---|---|
| Eval | < 10 | < 100 | <3 |
| Small | < 100 | < 1000 | <10 |
| Medium | >= 100, < 1000 | >= 1000, < 10,000 | >= 10, < 25 |
| Large | >= 1000 | >= 10,000 | >= 25, <= 50* |

For larger user loads see Section 11.1.3.1, "Large Concurrent UI Load".

The Eval configuration is not meant for production environments. It is only to be used for trial and testing environments.

#### 11.1.1.3 Sizing for Upgraded Installs

If upgrading from a previous release of Enterprise Manager to Enterprise Manager 12*c*, the following queries can be run as the sysman user to obtain the Management Agent and target counts for use in Table 1.

- Agent count - select count(*) from mgmt_targets where target_type = 'oracle_emd'
- Target count – select count(*) from mgmt_targets where target_type != 'oracle_emd'

#### 11.1.1.4 Minimum Hardware Requirements

Table 11–2 lists the minimum hardware requirements for the four configurations.

***Table 11–2 Oracle Enterprise Manager Minimum Hardware Requirements***

| Size | OMS Machine Count* | Cores per OMS | Memory per OMS (GB) | Storage per OMS (GB) | Database Machine Count* | Cores per Database Machine | Memory per Database Machine (GB) |
|---|---|---|---|---|---|---|---|
| Eval | 1 | 2 | 4 | 18 | - | - | - |
| Small | 1 | 2 | 6 | 18 | 1 | 2 | 6 |
| Medium | 2 | 4 | 8 | 18 | 2 (Oracle RAC) | 4 | 8 |
| Large | 2<br>4 | 8<br>4 | 16<br>8 | 18<br>18 | 2 (Oracle RAC)<br>2 (Oracle RAC) | 8<br>8 | 16<br>16 |
| *The OMS and database instances are not co-located except for the Eval size. | | | | | | | |

***Table 11–3 Oracle Enterprise Manager Minimum Storage Requirements***

| Size | MGMT_ TABLESPACE (GB) | MGMT_ECM_ DEPOT_TS (GB) | TEMP | ARCHIVE LOG AREA (GB |
|---|---|---|---|---|
| Eval | 15 | 1 | 3 | Archive log off |
| Small | 50 | 1 | 10 | 25 |
| Medium | 200 | 4 | 20 | 100 |
| Large | 300 | 8 | 40 | 150 |

#### 11.1.1.5 Network Topology Considerations

A critical consideration when deploying Enterprise Manager Cloud Control is network performance between tiers. Enterprise Manager Cloud Control ensures tolerance of network glitches, failures, and outages between application tiers through error tolerance and recovery. The Management Agent in particular is able to handle a less performant or reliable network link to the Management Service without severe impact to the performance of Enterprise Manager as a whole. The scope of the impact, as far as a single Management Agent's data being delayed due to network issues, is not likely to be noticed at the Enterprise Manager Cloud Control system wide level.

The impact of slightly higher network latencies between the Management Service and Management Repository will be substantial, however. Implementations of Enterprise Manager Cloud Control have experienced significant performance issues when the network link between the Management Service and Management Repository is not of sufficient quality.

The Management Service host and Repository host should be located in close proximity to each other. Ideally, the round trip network latency between the two should be less than 1 millisecond.

## 11.1.2 Software Configurations

The following sections provide information about Eval, small, medium and large configurations.

### 11.1.2.1 Eval Configuration

The Eval configuration must be installed by selecting the Simple installation option. The installation then must be configured with the appropriate values.

**Minimum OMS Settings**

The Oracle Management Service (OMS) heap size should be set to 800 MB.

**Minimum Repository Database Settings**

Table 11–4 below lists the minimum repository database settings that are recommended for an Eval configuration.

*Table 11–4 Eval Configuration Minimum Database Settings*

| Parameter | Minimum Value |
|---|---|
| Processes | 300 |
| memory_target | 700 MB |
| redo log file size | 50 MB |
| shared_pool_size | 450 MB |
| session_cached_cursors | remove |

### 11.1.2.2 Small Configuration

The Small configuration is based on the minimum requirements that are required by the Oracle Enterprise Manager installer.

**Minimum OMS Settings**

No additional settings are required.

**Minimum Database Settings**

Table 11–5 lists the minimum recommended database settings.

*Table 11–5 Small Site Minimum Database Settings*

| Parameter | Minimum Value |
|---|---|
| processes | 300 |
| pga_aggregate_target* | 1024 MB |
| sga_target* | 2 GB |
| redo log file size | 300 MB |
| shared_pool_size | 600 MB |
| db_securefile | PERMITTED |
| *memory_target of 3 GB can be used in place of sga_target and pga_aggregate_target | |

#### 11.1.2.3 Medium Configuration

The Medium configuration modifies several out-of-box Oracle Enterprise Manager settings.

**Minimum OMS Settings**

The Oracle Management Service (OMS) heap size should be set to 4096 MB.

**Minimum Repository Database Settings**

Table 11–6 lists the minimum repository database settings that are recommended for a Medium configuration.

*Table 11–6 Medium Site Minimum Database Settings*

| Parameter | Minimum Value |
|---|---|
| processes | 600 |
| pga_aggregate_target* | 1280 MB |
| sga_target* | 4 GB |
| redo log file size | 600 MB |
| shared_pool_size | 600 MB |
| db_securefile | PERMITTED |

*memory_target of 5.25 GB can be used in place of sga_target and pga_aggregate_target

#### 11.1.2.4 Large Configuration

The Large configuration modifies several out-of-box Oracle Enterprise Manager settings.

**Minimum OMS Settings**

Table 11–7 lists the minimum OMS settings that are recommended for Large configurations.

*Table 11–7 Large Site Minimum OMS Settings*

| OMS Count | Heap Size Minimum Value |
|---|---|
| 2 | 8192 MB |
| 4 | 4096 MB |

**Minimum Repository Database Settings**

Table 11–8 lists the minimum repository database settings that are recommended for a Large configuration.

*Table 11–8 Large Site Minimum Database Settings*

| Parameter | Minimum Value |
|---|---|
| processes | 1000 |
| pga_aggregate_target* | 1536 MB |
| sga_target* | 6 GB |
| redo log file size | 1000 MB |
| shared_pool_size | 600 MB |

*memory_target of 7.5 GB can be used in place of sga_target and pga_aggregate_target

*Table 11–8 (Cont.) Large Site Minimum Database Settings*

| Parameter | Minimum Value |
|---|---|
| db_securefile | PERMITTED |
| *memory_target of 7.5 GB can be used in place of sga_target and pga_aggregate_target | |

#### 11.1.2.5 Repository Tablespace Sizing

Table 11–9 lists the required minimum storage requirements for the Management Repository.

*Table 11–9 Total Management Repository Storage*

| Deployment Size | Minimum Tablespace Sizes* | | | | |
|---|---|---|---|---|---|
| | SYSTEM** | MGMT_ TABLESPACE | MGMT_ECM_ DEPOT_TS | MGMT_AD4J_ TS | TEMP |
| Small | 600 MB | 50 GB | 1 GB | 100 MB | 10 GB |
| Medium | 600 MB | 200 GB | 4 GB | 200 MB | 20 GB |
| Large | 600 MB | 300 GB | Greater than 4 GB | 400 MB | 40 GB |

*These are strictly minimum values and are intended as rough guidelines only. The actual size of the MGMT_TABLESPACE could vary widely from deployment to deployment due to variations in target type distribution, user customization, and several other factors. These tablespaces are defined with AUTOEXTEND set to ON by default to help mitigate space constraint issues. On raw file systems Oracle recommends using more than the minimum size to help prevent space constraint issues.

**The SYSTEM and TEMP tablespace sizes are minimums for Enterprise Manager only repositories. If Enterprise Manager is sharing the repository database with other application(s), these minimums may be too low.

**Note**: You can either set up TABLESPACE FULL alerts if you want to have greater control over the management of your tablespaces, or you can allow Oracle to grow your database and not alert you through the AUTOEXTEND feature. Therefore to exercise greater control of the TABLESPACE FULL alerts, you can turn off autoextend.

### 11.1.3 Additional Configurations

Some Enterprise Manager installations may need additional tuning settings based on larger individual system loads. Additional settings are listed below.

#### 11.1.3.1 Large Concurrent UI Load

If more than 50 concurrent users are expected per OMS, the following settings should be altered as seen in Table 11–10.

*Table 11–10 Large Concurrent UI Load Additional Settings*

| Process | Parameter | Value | Where To Set |
|---|---|---|---|
| OMS | -Djbo.recyclethreshold | Number of concurrent users / number of OMS | Per OMS |
| OMS | -Djbo.ampool.maxavailablesize | Number of concurrent users / number of OMS | Per OMS |
| OMS | Heap Size | Additional 4GB for every increment of 50 users | Per OMS |
| Database | sga_target | Additional 1GB for every increment of 50 users | Per Instance |

Higher user loads will require more hardware capacity. An additional 2 cores for both the database and OMS hosts for every 50 concurrent users.

Example: A site with 1500 agents and 15,000 targets with 150 concurrent users would require at a minimum the setting modifications listed in Table 11–11 (based on a LARGE 2 OMS configuration).

***Table 11–11 Large Concurrent UI Load Additional Settings Example for 2 OMS Configurations***

| Process | Parameter | Value | Calculation |
|---|---|---|---|
| OMS | -Djbo.recyclethreshold | 75 (set on each OMS) | 150 users / 2 OMS |
| OMS | -Djbo.ampool.maxavailablesize | 75 (set on each OMS) | 150 users / 2 OMS |
| OMS | Heap Size | 12 GB (set on each OMS) | 8GB (standard large setting) + ((150 users – 50 default large user load) / 2 OMS)* (4GB / 50 users) |
| Database | sga_target | 8 GB | 6GB (standard large setting) + (150 users - 50 default large user load) * (1GB / 50 users) |

Minimum Additional Hardware required is listed in Table 11–12.

***Table 11–12 Large Concurrent UI Load Minimum Additional Hardware Example For 2 OMS Configuration***

| Tier | Parameter | Value | Calculation |
|---|---|---|---|
| OMS | CPU cores | 24 (total between all OMS hosts) | 8 cores * 2 OMS (default large core count) + (150 users - 50 default large user load) *(2 cores * 2 OMS)/ 50 users) |
| Database | CPU cores | 24 (total between all Database hosts) | 8 cores * 2 OMS (default large core count) + (150 users - 50 default large user load) *(2 cores * 2 OMS / 50 users) |

The physical memory of each machine would have to be increased to support running this configuration as well.

You can alter the value of the following parameters: *-Djbo.recyclethreshold*, *-Djbo.ampool.maxavailablesize*, and *Heap Size*. By default these values are set as follows:

- Djbo.recyclethreshold is set to 50
- Djbo.ampool.maxavailablesize is set to 50
- Heap Size is set to -Xms1024m -Xmx1740m

You can set the values for these memory parameters by making changes in the *startEMServer.sh* file, which can be found in the following location:

*gc_inst/user_projects/domains/GCDomain/bin*

For the -Djbo.recyclethreshold and -Djbo.ampool.maxavailablesize parameters, you can add the first section below to the second section.

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.security.egd=file:///dev/./urandom
-Dweblogic.debug.DebugSecurityAtn=true -Dweblogic.debug.DebugWebAppSecurity=true
-Dweblogic.SSL.LoginTimeoutMillis=300000 -Dj
ps.auth.debug=true -Xbootclasspath/p:/u01/EM12/oms/sysman/jlib/diagpatch_
bug11725986.jar -Djdkpatchlog=/u01/EM12/oms/sysman/log/diagpatch_bug11725986.log
-Doracle.apm.home=/u01/EM12/oms/apm/ -DAPM_
HELP_FILENAME=oesohwconfig.xml -Djava.util.logging.config.file=/tmp/logging.txt"

JAVA_OPTIONS="${JAVA_OPTIONS} -Djbo.recyclethreshold=100
-Djbo.ampool.maxavailablesize=5 -Djava.security.egd=file:///dev/./urandom
-Dweblogic.debug.DebugSecurityAtn=true -Dweblogic.debug.DebugWebAppSecurity=true
-Dweblogic.SSL.LoginTimeoutMillis=300000 -Djps.auth.debug=true
-Xbootclasspath/p:/u01/EM12/oms/sysman/jlib/diagpatch_bug11725986.jar
-Djdkpatchlog=/u01/EM12/oms/sysman/log/diagpatch_bug11725986.log
-Doracle.apm.home=/u01/EM12/oms/apm/ -DAPM_HELP_FILENAME=oesohwconfig.xml
-Djava.util.logging.config.file=/tmp/logging.txt"
```

For release 12.1.0.3 and later, see the point on *Changing Djbo.ampool.maxavailablesize and Djbo.recyclethreshold (JAVA_EM_ARGS)* in Section 11.1.3.5.

In the same file, you may change the heap size settings for the following section:

```
USER_MEM_ARGS="-Xms1024m -Xmx1740m -XX:MaxPermSize=1024M -XX:-DoEscapeAnalysis
-XX:+UseCodeCacheFlushing -XX:CompileThreshold=8000 -XX:PermSize=128m"
```

**Note:** Oracle does not recommend changing the Xms value.

### 11.1.3.2 Large Job System Load

If the jobs system has a backlog for long periods of time or if you would like the backlog processed faster, set the following parameters with the *emctl set property* command.

***Table 11–13 Large Job System Backlog Settings***

| Parameter | Value |
|---|---|
| oracle.sysman.core.jobs.shortPoolSize | 50 |
| oracle.sysman.core.jobs.longPoolSize | 24 |
| oracle.sysman.core.jobs.longSystemPoolSize | 20 |
| oracle.sysman.core.jobs.systemPoolSize | 50 |
| oracle.sysman.core.conn.maxConnForJobWorkers | 144* |

*This setting may require an increase in the processes setting in the database of 144 number of OMS servers.

These settings assume that there are sufficient database resources available to support more load. These parameters are likely to be required in a Large configuration with 2 OMS nodes.

### 11.1.3.3 Large Repository Side Available Load (Release 12.1.0.3 and above)

Many targets have repository side availability in Enterprise Manager: Services, Clusters, and so on. By default Enterprise Manger computes these availabilities with two processes. This should be adequate for most installations. If the availability calculation is taking more than 2 minutes on average, more processes can be added. To track the performance of this calculation, the following SQL statement should be run:

```
select status, actual_start_date, run_duration
  from dba_scheduler_job_run_details
 where owner='SYSMAN'
   and job_name='EM_REPOS_SEV_EVAL'
   and job_subname IS NULL
   and actual_start_date > sysdate-1/24
 order by actual_start_date;
```

This will track the run time of the job for the last hour. If your database has adequate free resources and the calculation is consistently taking more that 2 minutes you can add more processes by running the following commands as SYSMAN:

```
begin
 em_severity_repos.set_parallel_parametrization(1, <total number of processes>);
commit;
end;
/
```

The change is dynamic and the next iteration of the job uses the new process count. To determine the current setting, run the following SQL statement:

```
select parameter_value from em_sysavail_parameters  where parameter_name = 'NUM_
CHUNKS'
```

The total number of process should be incremented by 1 until the calculation takes, on average, less than 2 minutes. After each increase, repository resource consumption should be reevaluated before increasing further.

### 11.1.3.4 Large Number of Agents (Release 12.1.0.3)

The default out-of-box settings for Enterprise Manager has 2 ping recorder threads per OMS. This setting can handle 2000 agents per OMS. If your site needs to handle more agents than the number of OMSes * 2000, or your database per thread CPU performance is slow, then you can increase the number of ping recorder threads per OMS. The following parameter can be used:

*oracle.sysman.core.omsAgentComm.ping.heartbeatPingRecorderThreads*

This value defaults to 2 per OMS. Internal testing has shown that 1 ping thread per 1000 agents is sufficient under well-tuned situations. Each OMS requires a restart to use the new value.

### 11.1.3.5 Changing OMS Properties

The following section provides examples of changing the OMS settings recommended in this chapter. You may need to change OMS property settings, for example, when increasing the Job Backlog. The values in the examples should be substituted with the appropriate value for your configuration. Use the following instructions to change OMS properties.

**Changing the Heap Size**

Values of the following property names for Memory Args can be set in order to override their default values:

OMS_HEAP_MIN
OMS_HEAP_MAX
OMS_PERMGEN_MIN
OMS_PERMGEN_MAX

The following table describes the above parameters and provides a description, default values, recommendations for their use, and any notes, warnings or issues of which to be aware.

| Name | Description | Default | Recommendation | Notes, Warnings or Issues |
|---|---|---|---|---|
| OMS_HEAP_MIN (-Xms) | Change of –Xms is not really required. Should maintain post-installation default value. If a large setup becomes a 'very large setup' over a period of time, then user/sysadmin may choose to increase the value at the time of increasing the value of –Xmx. | 32/64 bit -<br>Small: 256M<br>Medium: 256M<br>Large: 256M<br>For IBM JVM, irrespective of the app size, use the following settings:<br>32-bit: 1024M<br>64-bit: 1740M | Same as mentioned in the Default section.<br>These are post installation defaults, thus the recommended setup. | N/A |
| OMS_HEAP_MAX (-Xmx) | As targets are added after the initial installation/setup of Enterprise Manager, increasing the HEAP size is recommended to avoid any unforeseen Out Of Memory Error of Tenured/Old Gen. | 32 bit –<br>Small/Medium/ Large: 1524M<br>64 bit -<br>Small: 1740M<br>Medium: 4096M<br>Large: 8192M<br>For IBM JVM, irrespective of the app size, there are no limits on the heap size. | Same as mentioned in the Default section.<br>These are post installation defaults, thus the recommended setup. | All these parameters should be changed, once users experience a lower throughput over a period of time, due to consistently high memory usage. The person (preferably *sysadmin*) manipulating the parameters must be aware of the limits/warnings. |
| OMS_PERMGEN_MIN (-XX:PermSize) | Change of –XX: PermSize is not required. Should maintain post-installation default value. | 32/64 bit -<br>Small: 128M<br>Medium: 128M<br>Large: 128M<br>For IBM JVM, irrespective of the app size, use the following settings:<br>32-bit: 128M<br>64-bit: 128M | Same as mentioned in the Default section.<br>These are post installation defaults, thus the recommended setup. | N/A |

| Name | Description | Default | Recommendation | Notes, Warnings or Issues |
|---|---|---|---|---|
| OMS_PERMGEN_MAX (-XX:MaxPermSize) | In Large configurations, where too many activities in the OMS container result in a large number of classloaders and 'Class' objects being created, the perm gen may become full, resulting in an Out Of Memory Error. | 32 bit –<br>Small/Medium/ Large: 612M<br>64 bit -<br>Small: 612M<br>Medium: 768M<br>Large: 768M<br>For IBM JVM, irrespective of the app size, use the following settings:<br>32-bit: 612M<br>64-bit: 612M | Same as mentioned in the Default section.<br>These are post installation defaults, thus the recommended setup. | N/A |

You can use either of the following two commands to set the value for any of the above properties:

*emctl set property –name EM_JAVA_MEM_ARGS –value <complete memory parameter>*

Or you can use:

*emctl set property –name <property_name> -value <number_followed_by_G_or_M>*

For example:

```
emctl set property -name OMS_PERMGEN_MAX -value 1024M
```

Use the following command to get the property name:

*emctl get property –name <property_name>*

Values of the following property names for JBO Args can be set in order to override their default values:

- JBO_MIN_POOL_SIZE - After this limit is exceeded, the application pool will time out application modules inactive longer than jbo.ampool.maxinactiveage. The default value is 1.
- JBO_POOL_TTL - Specifies the application module pool time to live for application module instances. The default value is -1.
- JBO_LAZY_LOAD - Determines whether to load components lazily. The default value is TRUE.
- JBO_MAX_CURSORS - The maximum number of cursors the business components may have open. The framework will clean up free JDBC statements as the number of cursors approaches this number. The default value is 5.
- JBO_RECYC_THRESHOLD - The recycle threshold, used in application module pooling. The default value is 50.
- JBO_MAX_POOL_SIZE - After this limit is exceeded, the application pool will time out application modules inactive for the longest time, even if that is less time than the jbo.ampool.maxinactiveage. The default value is 50.

Use either of the following commands to set the value for any of the above properties:

*emctl set property –name EM_JAVA_MEM_ARGS –value <complete memory parameter>*

Or you can use:

*emctl set property –name <property_name> -value <property_value>*

For example:

```
emctl set property -name JBO_MAX_POOL_SIZE -value 5
```

Use the following command to get the property name:

*emctl get property –name <property_name>*

An OMS restart using the below commands is required on each OMS after changing the property value:

```
emctl stop oms -all
emctl start oms
```

**Changing shortPoolSize**

To change the OMS property, oracle.sysman.core.jobs.shortPoolSize, follow these recommendations:

To set the property, enter the following command:

```
$ emctl set property -name oracle.sysman.core.jobs.shortPoolSize -value
200
```

To get the property (after changing from the default), enter the following command:

```
$ emctl get property -name “oracle.sysman.core.jobs.shortPoolSize”
```

To delete the property (revert to original setting), enter the following command:

```
$ emctl delete property -name “oracle.sysman.core.jobs.shortPoolSize”
```

An OMS and Node Manager restart using ‘emctl stop oms -all; emctl start oms’ is required on each OMS after changing the property value. The default value is 25.

**Changing longPoolSize**

To change the OMS property, oracle.sysman.core.jobs.longPoolSize, follow these recommendations:

To set the property, enter the following command:

```
$ emctl set property -name oracle.sysman.core.jobs.longPoolSize -value 200
```

To get the property (after changing from the default), enter the following command:

```
$ emctl get property -name “oracle.sysman.core.jobs.longPoolSize”
```

To delete the property (revert to original setting), enter the following command:

```
$ emctl delete property -name “oracle.sysman.core.jobs.longPoolSize”
```

An OMS restart using ‘emctl stop oms; emctl start oms’ is required on each OMS after changing the property value. The default value is 12.

**Changing longSystemPoolSize**

To change the OMS property, oracle.sysman.core.jobs.longSystemPoolSize, follow these recommendations:

To set the property, enter the following command:

```
$ emctl set property -name oracle.sysman.core.jobs.longSystemPoolSize
-value 200
```

To get the property (after changing from the default), enter the following command:

```
$ emctl get property -name "oracle.sysman.core.jobs.longSystemPoolSize"
```

To delete the property (revert to original setting), enter the following command:

```
$ emctl delete property -name "oracle.sysman.core.jobs.longSystemPoolSize"
```

An OMS restart using 'emctl stop oms; emctl start oms' is required on each OMS after changing the property value. The default value is 10.

**Changing systemPoolSize**

To change the OMS property, oracle.sysman.core.jobs.systemPoolSize, follow these recommendations:

To set the property, enter the following command:

```
$ emctl set property -name oracle.sysman.core.jobs.systemPoolSize -value
200
```

To get the property (after changing from the default), enter the following command:

```
$ emctl get property -name "oracle.sysman.core.jobs.systemPoolSize"
```

To delete the property (revert to original setting), enter the following command:

```
$ emctl delete property -name "oracle.sysman.core.jobs.systemPoolSize"
```

An OMS restart using 'emctl stop oms; emctl start oms' is required on each OMS after changing the property value. The default value is 25.

**Changing maxConnForJobWorkers**

To change the OMS property, oracle.sysman.core.conn.maxConnForJobWorkers, follow these recommendations:

To set the property, enter the following command:

```
$ emctl set property -name oracle.sysman.core.conn.maxConnForJobWorkers
-value 200
```

To get the property (after changing from the default), enter the following command:

```
$ emctl get property -name "oracle.sysman.core.conn.maxConnForJobWorkers"
```

To delete the property (revert to original setting), enter the following command:

```
$ emctl delete property -name
"oracle.sysman.core.conn.maxConnForJobWorkers"
```

An OMS restart using 'emctl stop oms; emctl start oms' is required on each OMS after changing the property value. The default value is 25.

**Changing Djbo.ampool.maxavailablesize and Djbo.recyclethreshold (JAVA_EM_ARGS)**

To change the OMS properties, *Djbo.ampool.maxavailablesize* and *Djbo.recyclethreshold*, follow these recommendations:

To set the properties, enter the following command:

```
$ emctl set property -name JAVA_EM_ARGS -value
"-Djbo.ampool.maxavailablesize=500 -Djbo.recyclethreshold=500"
```

To get the properties (after changing from the default), enter the following command:

```
$ emctl get property -name "JAVA_EM_ARGS"
```

To delete the properties (revert to original setting), enter the following command:

```
$ emctl delete property -name "JAVA_EM_ARGS"
```

An OMS restart using ‘emctl stop oms -all; emctl start oms’ is required on each OMS after changing the property value.

**Changing omsAgentComm.ping.heartbeatPingRecorderThreads**

To change the OMS property, oracle.sysman.core.omsAgentComm.ping.heartbeatPingRecorderThreads, follow these recommendations:

To set the property, enter the following command:

```
emctl set property -name
oracle.sysman.core.omsAgentComm.ping.heartbeatPingRecorderThreads -value 5
```

To get the property (after changing from the default), enter the following command:

```
emctl get property -name
oracle.sysman.core.omsAgentComm.ping.heartbeatPingRecorderThreads
```

To delete the properties (revert to original setting), enter the following command:

```
emctl delete property -name
oracle.sysman.core.omsAgentComm.ping.heartbeatPingRecorderThreads
```

An OMS restart using ‘emctl stop oms; emctl start oms’ is required on each OMS after changing the property value.

### 11.1.3.6 Modifying Database Settings

If you have downloaded the Database Templates for a Preconfigured Repository, you can run the appropriate SQL script to adjust the database parameters to the recommended settings. The scripts that you should run are listed in the following table:

| Size | Script |
|---|---|
| Small | set_repo_param_11.2.0.3_Database_SQL_for_EM12_1_0_4_Small_deployment.sql |
| Medium | set_repo_param_11.2.0.3_Database_SQL_for_EM12_1_0_4_Medium_deployment.sql |
| Large | set_repo_param_11.2.0.3_Database_SQL_for_EM12_1_0_4_Large_deployment.sql |

Note that the above scripts do not adjust MEMORY_TARGET/ SGA_TARGET/ PGA_AGGREGATE_TARGET so these parameters must be modified manually.

### 11.1.3.7 BI Publisher Configuration

If you plan to configure the installed BI Publisher (11.1.1.7.0) with Enterprise Manager Release 12*c* Cloud Control, which is required for BI Publisher reports to function, add 1.5 GB to the host memory requirements stated above.

## 11.2 Enterprise Manager Cloud Control Performance Methodology

An accurate predictor of capacity at scale is the actual metric trend information from each individual Enterprise Manager Cloud Control deployment. This information, combined with an established, rough, starting host system size and iterative tuning and maintenance, produces the most effective means of predicting capacity for your

Enterprise Manager Cloud Control deployment. It also assists in keeping your deployment performing at an optimal level.

Here are the steps to follow to enact the Enterprise Manager Cloud Control sizing methodology:

1. If you have not already installed Enterprise Manager Cloud Control, choose a rough starting host configuration as listed in Table 11–1.
2. Periodically evaluate your site's vital signs (detailed later).
3. Eliminate bottlenecks using routine DBA/Enterprise Manager administration housekeeping.
4. Eliminate bottlenecks using tuning.
5. Extrapolate linearly into the future to plan for future sizing requirements.

Step one need only be done once for a given deployment. Steps two, three, and four must be done, regardless of whether you plan to grow your Enterprise Manager Cloud Control site, for the life of the deployment on a regular basis. These steps are essential to an efficient Enterprise Manager Cloud Control site regardless of its size or workload. You must complete steps two, three, and four before you continue on to step five. This is critical. Step five is only required if you intend to grow the deployment size in terms of monitored targets. However, evaluating these trends regularly can be helpful in evaluating any other changes to the deployment.

### 11.2.1 Step 1: Choosing a Starting Platform Cloud Control Deployment

For information about choosing a starting platform Cloud Control deployment, see Section 11.1.1, "Overview of Sizing Guidelines".

### 11.2.2 Step 2: Periodically Evaluating the Vital Signs of Your Site

This is the most important step of the five. Without some degree of monitoring and understanding of trends or dramatic changes in the vital signs of your Enterprise Manager Cloud Control site, you are placing site performance at serious risk. Every monitored target sends data to the Management Repository for loading and aggregation through its associated Management Agent. This adds up to a considerable volume of activity that requires the same level of management and maintenance as any other enterprise application.

Enterprise Manager has "vital signs" that reflect its health. These vital signs should be monitored for trends over time as well as against established baseline thresholds. You must establish realistic baselines for the vital signs when performance is acceptable. Once baselines are established, you can use built-in Oracle Enterprise Manager Cloud Control functionality to set baseline warning and critical thresholds. This allows you to be notified automatically when something significant changes on your Enterprise Manager site. The following table is a point-in-time snapshot of the Enterprise Manager Cloud Control vital signs for two sites:

| Module | Metrics | EM Site 1 | EM Site 2 |
|---|---|---|---|
| Site | | emsite1 | emsite2 |
| | | | |
| Target Counts | Database Targets | 192 (45 not up) | 1218 (634 not up) |
| | Host Targets | 833 (12 not up) | 1042 (236 not up) |
| | | | |

| Module | Metrics | EM Site 1 | EM Site 2 |
|---|---|---|---|
| | Total Targets | 2580 (306 not up) | 12293 (6668 not up) |
| | | | |
| Overall Status | Overall Backoff Requests in the Last 10 Mins | 0 | 500 |
| | | | |
| Job Statistics | Estimated time for clearing current Job steps backlogJob | 0.1 | 7804 |
| | | | |
| Event Statistics | Pending Events Count | 2 | 4000 |
| | | | |
| Management Service Host Statistics | Average % CPU (Host 1) | 9 (emhost01) | 13 (emhost01) |
| | Average % CPU (Host 2) | 6 (emhost02) | 17 (emhost02) |
| | Average % CPU (Host 3) | N/A | 38 (em6003) |
| | Average % CPU (Host 4) | N/A | 12 (em6004) |
| | Number of cores per host | 2 X 2.8 (Xeon) | 4 X 2.4 (Xeon) |
| | Memory per Host (GB) | 8 | 8 |
| | | | |
| Management Repository Host Statistics | Average % CPU (Host 1) | 12 (db01rac) | 64 (em6001rac) |
| | Average % CPU (Host 2) | 14 (db02rac) | 78 (em6002rac) |
| | Number of CPU cores per host | 4 | 8 |
| | Memory target (GB) | 5.25 | 7.5 |
| | Memory per Host (GB) | 8 | 16 |
| | Total Management Repository Size (GB) | 56 | 98 |
| | Oracle RAC Interconnect Traffic (MB/s) | 1 | 4 |
| | Management Server Traffic (MB/s) | 4 | 4 |
| | Total Management Repository I/O (MB/s) | 6 | 27 |
| | | | |
| Enterprise Manager UI Page Response/Sec | Home Page | 3 | 6 |
| | All Host Page | 3 | 30+ |
| | All Database Page | 6 | 30+ |
| | Database Home Page | 2 | 2 |
| | Host Home Page | 2 | 2 |

The two Enterprise Manager sites are at the opposite ends of the scale for performance.

EM Site 1 is performing very well with very few backoff requests. It also has a very low job and event backlogs. The CPU utilization on both the OMS and Management Repository Server hosts are low. Most importantly, the UI Page Response times are excellent. To summarize, Site 1 is doing substantial work with minimal effort. This is how a well configured, tuned and maintained Oracle Enterprise Manager Cloud Control site should look.

Conversely, EM Site 2 is having difficulty. The site has substantial amounts of backoffs and sizable job and event backlogs. Worst of all are the user interface page response times. There is clearly a bottleneck on Site 2, possibly more than one.

These vital signs are all available from within the Enterprise Manager interface. Most values can be found on the All Metrics page for each host, or the All Metrics page for the OMS. Keeping an eye on the trends over time for these vital signs, in addition to assigning thresholds for warning and critical alerts, allows you to maintain good performance and anticipate future resource needs. You should plan to monitor these vital signs as follows:

- Take a baseline measurement of the vital sign values seen in the previous table when the Enterprise Manager Cloud Control site is running well.
- Set reasonable thresholds and notifications based on these baseline values so you can be notified automatically if they deviate substantially. This may require some iteration to fine-tune the thresholds for your site. Receiving too many notifications is not useful.
- On a daily (or weekly at a minimum) basis, watch for trends in the 7-day graphs for these values. This will not only help you spot impending trouble, but it will also allow you to plan for future resource needs.

The next step provides some guidance of what to do when the vital sign values are not within established thresholds. Also, it explains how to maintain your site's performance through routine housekeeping.

### 11.2.3 Step 3: Using DBA and Enterprise Manager Tasks To Eliminate Bottlenecks

It is critical to note that routine housekeeping helps keep your Enterprise Manager Cloud Control site running well. The following are lists of housekeeping tasks and the interval on which they should be done.

#### 11.2.3.1 Offline Monthly Tasks

Enterprise Manager Administrators should monitor the database built-in Segment Advisor for recommendations on Enterprise Manager Repository segment health. The Segment Advisor advises administrators which segments need to be rebuilt/reorganized and provides the commands to do so.

For more information about Segment Advisor and issues related to system health, refer to notes 242736.1 and 314112.1 in the My Oracle Support Knowledge Base.

### 11.2.4 Step 4: Eliminating Bottlenecks Through Tuning

The most common causes of performance bottlenecks in the Enterprise Manager Cloud Control application are listed below (in order of most to least common):

1. Housekeeping that is not being done (far and away the biggest source of performance problems)
2. Hardware or software that is incorrectly configured
3. Hardware resource exhaustion

When the vital signs are routinely outside of an established threshold, or are trending that way over time, you must address two areas. First, you must ensure that all previously listed housekeeping is up to date. Secondly, you must address resource utilization of the Enterprise Manager Cloud Control application. The vital signs listed in the previous table reflect key points of resource utilization and throughput in Enterprise Manager Cloud Control. The following sections cover some of the key vital signs along with possible options for dealing with vital signs that have crossed thresholds established from baseline values.

#### 11.2.4.1 High CPU Utilization

When you are asked to evaluate a site for performance and notice high CPU utilization, there are a few common steps you should follow to determine what resources are being used and where.

1. Use the Processes display on the Enterprise Manager Host home page to determine which processes are consuming the most CPU on any Management Service or Management Repository host that has crossed a CPU threshold.
2. Once you have established that Enterprise Manager is consuming the most CPU, use Enterprise Manager to identify what activity is the highest CPU consumer. Typically this manifests itself on a Management Repository host where most of the Management Service's work is performed. Here are a few typical spots to investigate when the Management Repository appears to be using too many resources.
   a. Click the CPU Used database resource listed on the Management Repository's Database Performance page to examine the SQL that is using the most CPU at the Management Repository.
   b. Check the Database Locks on the Management Repository's Database Performance page looking for any contention issues.
   c. Check the SQL Monitoring on the Management Repository's Database for any resource intensive SQL.

High CPU utilization is probably the most common symptom of any performance bottleneck. Typically, the Management Repository is the biggest consumer of CPU, which is where you should focus. A properly configured and maintained Management Repository host system that is not otherwise hardware resource constrained should average roughly 40 percent or less total CPU utilization. An OMS host system should average roughly 20 percent or less total CPU utilization. These relatively low average values should allow sufficient headroom for spikes in activity. Allowing for activity spikes helps keep your page performance more consistent over time. If your Enterprise Manager Cloud Control site interface pages happen to be responding well (approximately 3 seconds) while there are no significant backlogs, and it is using more CPU than recommended, you may not have to address it unless you are concerned it is part of a larger upward trend.

The recommended path for tracking down the root cause of high Management Repository CPU utilization is captured under step 3.b and 3.c listed above. This allows you to start at the Management Repository Performance page and work your way down to the SQL that is consuming the most CPU in its processing. This approach has been used very successfully on several real world sites.

If you are running Enterprise Manager on Intel based hosts, the Enterprise Manager Cloud Control Management Service and Management Repository will both benefit from Hyper-Threading (HT) being enabled on the host or hosts on which they are deployed. HT is a function of certain late models of Intel processors, which allows the execution of some amount of CPU instructions in parallel. This gives the appearance of double the number of CPUs physically available on the system. Testing has proven that HT provides approximately 1.5 times the CPU processing power as the same system without HT enabled. This can significantly improve system performance. The Management Service and Management Repository both frequently have more than one process executing simultaneously, so they can benefit greatly from HT.

#### 11.2.4.2 Loader Vital Signs

The vital signs for the loader indicate exactly how much data is continuously coming into the system from all the Enterprise Manager Agents. The most important item here is the “Number of Agents Sent Back in the Last Hour” metric. The metric can be found in the All Metrics page of each management service. This is the number of agents instructed to defer loading of data in the last hour. Ideally no agent should be instructed to defer loading, but some level of deferred loading is normal. If this value is above 2 percent of your deployed agent count and it is growing continuously, then action should be taken.

The number of Loader Threads is always set to 20 per OMS by default. Adding loader threads to an OMS increases the overall host CPU utilization. Customers can change this value as their site requires.

There are diminishing returns when adding loader threads if your repository does not have sufficient resources available. If you have available repository resources, as you add loader threads, you should see the “Number of Agents Sent Back in the Last Hour” metric decrease. If you are not seeing improvement you should explore other tuning or housekeeping opportunities.

To add more loader threads, you can change the following configuration parameter:

*oracle.sysman.core.gcloader.max_recv_thread*

The default value is 20. This is a per OMS setting.

You can access the Loader report by selecting Reports from the Enterprise menu and then choosing Information Publisher Reports. The title of the report is *Loader Statistics*. When you click on the report name, Enterprise Manager will execute the pre-defined report which will show the loader performance details.

#### 11.2.4.3 Rollup Vital Signs

The rollup process is the aggregation mechanism for Enterprise Manager Cloud Control. The two vital signs for the rollup are the rows/second and % of hour run. Due to the large volume of data rows processed by the rollup, it tends to be the largest consumer of Management Repository buffer cache space. Because of this, the rollup vital signs can be great indicators of the benefit of increasing buffer cache size.

Rollup rows/second shows exactly how many rows are being processed, or aggregated and stored, every second. This value is usually around 2,000 (+/- 500) rows per second on a site with a decent size buffer cache and reasonable speedy I/O. A downward trend over time for this value may indicate a future problem, but as long as % of hour run is under 100 your site is probably fine.

If rollup % of hour run is trending up (or is higher than your baseline), and you have not yet set the Management Repository buffer cache to its maximum, it may be advantageous to increase the buffer cache setting. Usually, if there is going to be a benefit from increasing buffer cache, you will see an overall improvement in resource utilization and throughput on the Management Repository host. The loader statistics will appear a little better. CPU utilization on the host will be reduced and I/O will decrease. The most telling improvement will be in the rollup statistics. There should be a noticeable improvement in both rollup rows/second and % of hour run. If you do not see any improvement in any of these vital signs, you can revert the buffer cache to its previous size. The old Buffer Cache Hit Ratio metric can be misleading. It has been observed in testing that Buffer Cache Hit Ratio will appear high when the buffer cache is significantly undersized and Enterprise Manager Cloud Control performance is struggling because of it. There will be times when increasing buffer cache will not help improve performance for Cloud Control. This is typically due to resource constraints or contention elsewhere in the application. Consider using the steps listed in the High CPU Utilization section to identify the point of contention. Cloud Control also provides advice on buffer cache sizing from the database itself. This is available on the database Memory Parameters page.

One important thing to note when considering increasing buffer cache is that there may be operating system mechanisms that can help improve Enterprise Manager Cloud Control performance. One example of this is the "large memory" option available on Red Hat Linux. The Linux OS Red Hat Advanced Server™ 2.1 (RHAS) has a feature called big pages. In RHAS 2.1, bigpages is a boot up parameter that can be used to pre-allocate large shared memory segments. Use of this feature, in conjunction with a large Management Repository SGA, can significantly improve overall Cloud Control application performance. Starting in Red Hat Enterprise Linux™ 3, big pages functionality is replaced with a new feature called huge pages, which no longer requires a boot-up parameter.

#### 11.2.4.4 Rollup Process

The Rollup process introduces the concept of rollup participating instance; where rollup processing will be distributed among all participating instances. To add a candidate instance to the participating EMROLLUP group, the parameter instance_groups should be set on the instance level as follows:

- Add *EMROLLUP_1* to the *instance_group* parameter for node 1

  Add *EMROLLUP_2* to the *instance_group* parameter for node 2

- Introduce the *PQ* and *PW* parallel processing modes where:
  - PQ is the parallel query/parallel dml mode. In this mode, each participating instance will have one worker utilizing the parallel degree specified.
  - PW is the parallel worker mode. In this mode, each participating instance will have a number of worker jobs equal to the parallel level specified
- Distribute the work load for all participating Oracle RAC instances as follows:
  - Each participating instance will be allocated equal number of targets. So for (n) number of participating instances with total workload (tl), each instance will be allocated *(tl/n).*
  - Each worker on any participating instance will be allocated equal number of targets of that instance workload. So for (il) number of targets per instance with (w) number of workers, each worker will be allocated *(il/w)*.
  - For each worker, the load is further divided into batches to control the number of times the rollup SQL is executed. The number of rows per batch will be the total number of rows allocated for the worker divided by the number of batches.

Use the following recommendations as guidelines during the Rollup process:

- Use the parallel worker (PW) mode, and utilize the participating EMROLLUP_xx instance group.
- The recommendation is to use the parallel worker mode.
- Splitting the work among more workers will improve the performance and scalability until a certain point where the diminishing returns rule will apply. This is dependent on the number of CPUs available on each Oracle RAC node. In this test case, running with 10 workers was the optimal configuration, balancing the response time, machine CPU and IO utilization.

- It is important to set a proper batch size (10 recommended). The optimal run was the one with 10 batches, attributed to balancing the number of executions of the main SQL (calling EMD_1HOUR_ROLLUP) and the sort space needed for each individual execution.
- Start by setting the number of batches to 10 bearing in mind the number of batches can be changed based on the data distribution.

The recommendations above will yield the following results. Using the multi-instance parallel worker (8 PW) mode (with the redesigned code described earlier) improves the performance by a factor of 9-13 when utilizing two participating Oracle RAC instances.

| Rollup row count (in millions) in MGMT_METRICS_1HOUR | Time (min) | Workers | Batch Size |
|---|---|---|---|
| 29.5 | 30 | 8 | 1 |
| 9.4 | 5 | 8 | 10 |

** For the entire test there were 15779 distinct TARGET_GUID

** The test produced “29.5 Million” new rollup rows in MGMT_METRICS_1HOUR

| Run ** | Rows/Workers | Batches/Workers | Rows/Batch | Time (min) |
|---|---|---|---|---|
| 8 PW /1 instance | 3945 | 3945 | 1 | 40 |
| 8 PW /2 instances | 1973 | 1973 | 1 | 30 |

### 11.2.4.5 Job, Notification, and Alert Vital Signs

Jobs, notifications, and alerts are indicators of the processing efficiency of the Management Service(s) on your Enterprise Manager Cloud Control site. Any negative trends in these values are usually a symptom of contention elsewhere in the application. The best use of these values is to measure the benefit of running with more than one OMS. There is one job dispatcher in each OMS. Adding OMS instances will not always improve these values. In general, adding OMS instances will improve overall throughput for Cloud Control when the application is not otherwise experiencing resource contention issues. Job, Notification, and Alert vital signs can help measure that improvement.

### 11.2.4.6 I/O Vital Signs

Monitoring the I/O throughput of the different channels in your Enterprise Manager Cloud Control deployment is essential to ensuring good performance. At minimum, there are three different I/O channels on which you should have a baseline and alert thresholds defined:

- Disk I/O from the Management Repository instance to its data files
- Network I/O between the OMS and Management Repository
- Oracle RAC interconnect (network) I/O (on Oracle RAC systems only)

You should understand the potential peak and sustained throughput I/O capabilities for each of these channels. Based on these and the baseline values you establish, you can derive reasonable thresholds for warning and critical alerts on them in Cloud Control. You will then be notified automatically if you approach these thresholds on your site. Some Cloud Control site administrators can be unaware or mistaken about what these I/O channels can handle on their sites. This can lead to Enterprise Manager Cloud Control saturating these channels, which in turn cripples performance on the site. In such an unfortunate situation, you would see that many vital signs would be impacted negatively.

To discover whether the Management Repository is involved, you can use Cloud Control to check the Database Performance page. On the Performance page for the Management Repository, click the wait graph showing the largest amount of time spent. From this you can continue to drill down into the actual SQL code or sessions that are waiting. This should help you to understand where the bottleneck is originating.

Another area to check is unexpected I/O load from non-Enterprise Manager Cloud Control sources like backups, another application, or a possible data-mining co-worker who engages in complex SQL queries, multiple Cartesian products, and so on.

Total Repository I/O trouble can be caused by two factors. The first is a lack of regular housekeeping. Some of the Cloud Control segments can be very badly fragmented causing a severe I/O drain. Second, there can be some poorly tuned SQL statements consuming much of the site I/O bandwidth. These two main contributors can cause most of the Cloud Control vital signs to plummet. In addition, the lax housekeeping can cause the Management Repository's allocated size to increase dramatically.

One important feature of which to take advantage is asynchronous I/O. Enabling asynchronous I/O can dramatically improve overall performance of the Cloud Control application. The Sun Solaris™ and Linux operating systems have this capability, but may be disabled by default. The Microsoft Windows™ operating system uses asynchronous I/O by default. Oracle strongly recommends enabling of this operating system feature on the Management Repository hosts and on Management Service hosts as well.

Automatic Storage Management (ASM) is recommended for Enterprise Manager Cloud Control repository database storage.

#### 11.2.4.7 About the Oracle Enterprise Manager Performance Page

There may be occasions when Enterprise Manager user interface pages are slow in the absence of any other performance degradation. The typical cause for these slow downs will be an area of Enterprise Manager housekeeping that has been overlooked. The first line of monitoring for Enterprise Manger page performance is the use of Enterprise Manager beacons. These functionalities are also useful for web applications other than Enterprise Manager.

Beacons are designed to be lightweight page performance monitoring targets. After defining a beacon target on an Management Agent, you can then define UI performance transactions using the beacon. These transactions are a series of UI page hits that you will manually walk through once. Thereafter, the beacon will automatically repeat your UI transaction on a specified interval. Each time the beacon transaction is run, Enterprise Manager will calculate its performance and store it for historical purposes. In addition, alerts can be generated when page performance degrades below thresholds you specify.

When you configure the Enterprise Manager beacon, you begin with a single predefined transaction that monitors the home page you specify during this process. You can then add as many transactions as are appropriate. You can also set up additional beacons from different points on your network against the same web application to measure the impact of WAN latency on application performance. This same functionality is available for all Web applications monitored by Enterprise Manager Cloud Control.

After you are alerted to a UI page that is performing poorly, you can then use the second line of page performance monitoring in Enterprise Manager Cloud Control. This  end-to-end (or E2E) monitoring functionality in Cloud Control is designed to allow you to break down processing time of a page into its basic parts. This will allow you to pinpoint when maintenance may be required to enhance page performance. E2E monitoring in Cloud Control lets you break down both the client side processing and the server side processing of a single page hit.

The next page down in the Middle Tier Performance section will break out the processing time by tier for the page. By clicking the largest slice of the Processing Time Breakdown pie chart, which is JDBC time above, you can get the SQL details. By clicking the SQL statement, you break out the performance of its execution over time.

The JDBC page displays the SQL calls the system is spending most of its page time executing. This SQL call could be an individual DML statement or a PL/SQL procedure call. In the case of an individual SQL statement, you should examine the segments (tables and their indexes) accessed by the statement to determine their housekeeping (rebuild and reorganization) needs. The PL/SQL procedure case is slightly more involved because you must look at the procedure's source code in the Management Repository to identify the tables and associated indexes accessed by the call.

Once you have identified the segments, you can then run the necessary rebuild and reorganization statements for them with the OMS down. This should dramatically improve page performance. There are cases where page performance will not be helped by rebuild and reorganization alone, such as when excessive numbers of open alerts, system errors, and metric errors exist. The only way to improve these calls is to address (for example, clean up or remove) the numbers of these issues. After these numbers are reduced, then the segment rebuild and reorganization should be completed to optimize performance. These scenarios are covered in Section 11.2.3. If you stay current, you should not need to analyze UI page performance as often, if at all.

For more information about new features for monitoring the performance of SQL procedures from the Enterprise Manager console, see the chapter, "Maintaining Enterprise Manager" in the *Enterprise Manager Administration* book.

#### 11.2.4.8 Determining the Optimum Number of Middle Tier OMS Servers

Determining the optimum number of middle tier OMS servers is not a trivial task. A number of data points must be considered for an informed, justified and acceptable decision for introducing additional OMS instances. The number of monitored targets is one of the first considerations, but its weight in decision making is normally not substantial.

The following items should be considered and examined as part of this exercise:

- The volume of job automation and scheduling used
- The number of administrators working simultaneously in the console
- Network bandwidth and data channel robustness from agents to the OMS servers
- Number of triggered violations and notifications
- Speed and stability of the IO system the OMS servers use

Careful investigation of each category is essential to making an informed decision. In some cases, just adding an OMS server or providing more CPU or memory to the same host may not make any difference in performance enhancement. You can use the current running OMS instances to collect accurate statistics on current OMS performance to calculate the number of required OMS servers for current or future deployments. Enterprise Manager has vital signs that reflect its health. These vital signs should be monitored for trends over time as well as against established baseline thresholds.

### 11.2.5 Step 5: Extrapolating Linearly Into the Future for Sizing Requirements

Determining future storage requirements is an excellent example of effectively using vital sign trends. You can use two built-in Cloud Control charts to forecast this: the total number of targets over time and the Management Repository size over time.

Both of the graphs are available on the All Metrics page for the Management Service. It should be obvious that there is a correlation between the two graphs. A straight line applied to both curves would reveal a fairly similar growth rate. After a target is added to Enterprise Manager Cloud Control for monitoring, there is a 31-day period where Management Repository growth will be seen because most of the data that will consume Management Repository space for a target requires approximately 31 days to be fully represented in the Management Repository. A small amount of growth will continue for that target for the next year because that is the longest default data retention time at the highest level of data aggregation. This should be negligible compared with the growth over the first 31 days.

When you stop adding targets, the graphs will level off in about 31 days. When the graphs level off, you should see a correlation between the number of targets added and the amount of additional space used in the Management Repository. Tracking these values from early on in your Enterprise Manager Cloud Control deployment process helps you to manage your site's storage capacity pro-actively. This history is an invaluable tool.

The same type of correlation can be made between CPU utilization and total targets to determine those requirements. There is a more immediate leveling off of CPU utilization as targets are added. There should be no significant increase in CPU cost over time after adding the targets beyond the relatively immediate increase. Introducing new monitoring to existing targets, whether new metrics or increased collections, would most likely lead to increased CPU utilization.

### 11.2.6 Using Returning Query Safeguards to Improve Performance

On the All Targets page, Enterprise Manager uses a safeguard that prevents a flood of data from slowing performance and consuming excessive resources within the OMS by limiting the number of rows that can be returned from a query. By default, the limit is set to 2000, but an Enterprise Manager administrator can modify the limit with the following command:

```
emctl set property -name oracle.sysman.core.uifwk.maxRows -value 2000
```

Providing a value equal to 0 will turn off the safeguard and fetch all rows. The new value takes immediate effect; no OMS restart is required. If the value is less than 0, the default value (2000) will be used instead. The only way to indicate that no limiting should be performed is to set the value to exactly 0.

When there are too many results returned from a query and this limit comes into effect, the following message appears under the results table:

*"This table of search results is limited to 2000 targets. Narrow the results by using Refine Search or Search Target Name. See the tuning guide for how to modify this limit."*

Similar behaviors (and messages) are applied to other large tables throughout Enterprise Manager. The same OMS property (`oracle.sysman.core.uifwk.maxRows`) controls the maximum limit for all of them together. This matches the behavior (and reuses the existing property) from previous Enterprise Manager releases.

## 11.3 Overview of Repository and Sizing Requirements for Fusion Middleware Monitoring

A Fusion Middleware target is like any other Enterprise Manager target. Therefore any repository or sizing guideline that is applicable for an Enterprise Manager target would be applicable on a Fusion Middleware target.

One major concern in the case of Fusion Middleware discovery is that too many targets may be discovered, created and monitored. This adds additional load on the OMS instance, repository and agent. In the case of very large number of targets, after target discovery Oracle recommends that users should review all the targets and their respective metrics.

Based on requirements, users should finalize which targets and metrics should be monitored and the required frequency those targets should be monitored.

After discovery, Oracle recommends you allow Fusion Middleware/ADP/JVMD monitoring to run for some duration (a few days to possibly a few weeks) and continuously monitor the database size and Operating System file system growth (in the case of ADP; ADP Manager requires a minimum of 10GB of disk space) until it becomes constant. You can then fine tune various parameters associated with these different features.

In version 12c of Enterprise Manager, both ADP and JVMD use the Enterprise Manager repository as their repository. Their data are stored in the MGMT_AD4J_TS tablespace.

### 11.3.1 ADP Monitoring

Use the following information when utilizing ADP Monitoring.

- ADP Manager Resources Requirement

  While managing 70K managed entities, if the number of managed entities is high you must allocate resources accordingly.

| Resource | Amount |
|---|---|
| Physical Memory | 2 GB |
| Minimum Disk Space | 10 GB |

- ADP Data requirement

  To monitor each entity per JVM, the MGMT_AD4J_TS tablespace must have 8 MB available.

- ADP Data Retention Policy

  ADP maintains sophisticated multi-tiered logic for aggregation (or compression) of performance data. This helps to optimize performance of interaction with the internal data repository both when querying data for presentation or inserting new performance metrics.

  Users who want to store longer term data should look for this section in *Acsera.properties*:

```
#########################
# Production setting
# NOTE: use Model.GlobalSamplingRateSecs to configure Metric.Grain.0
#########################
Metric.Grain.0 0s
Metric.TableInterval.0 = 4h
Metric.DataLife.0 = 2d

Metric.Grain.1 = 3m
Metric.TableInterval.1 =1d
Metric.DataLife.1 = 8d

#Metric.Grain.2 = 30m
#Metric.TableInterval.2 = 7d
#Metric.DataLife.2 = 420d
```

Uncomment the last 3 lines for the *Metric.*.2* properties.

### 11.3.2 JVMD Monitoring

Use the following information when employing JVMD Monitoring.

- JVMD Manager Resources Requirement

  To manage 200-300 jvms, JVMD manager requires physical memory of 1 GB. JVMD manager caches monitoring data in the TEMP space for each pool and flushes to the database frequently. Usually, depending on the number of pools the manager is monitoring and the amount of data being gathered from each pool, the size requirement of these temporary cache files varies, but it is rare to see more than a few MBs for each pool. If this is a concern, the TEMP space should be allocated accordingly.

- JVMD Data requirement

  To monitor every JVM with OOB settings, the MGMT_AD4J_TS tablespace must have 50-100MB available.

- JVM Diagnostics Historical Data and its Retention policy

  Historical data is available at three summary levels 0, 1 and 2.

  - Summary level 0 - is raw sample data taken at the specified pool polling interval (default 2 seconds). If you look at data within one hour on the Performance Diagnostics page, it shows summary level 0 data. Level 0 data is retained for 24 hours and subsequently purged. It can be changed via the Console Setup page, but before increasing the value, you should ensure that the repository is tuned properly to handle such large amounts of data.
  - Summary level 1 - is aggregated data. If you view data after more than one hour but less than 5 hours, it is summary level 1 data. The default aggregation interval is 90 seconds. This value can be changed via the Console Setup page. Level 1 data is retained for 20 days and subsequently purged.
  - Summary level 2 - is further aggregated data. If you view data more than five hours old, it is summary level 2 data. This data is aggregated every 60 minutes. Level 2 data is retained for 400 days and subsequently purged.

There are two JVMD features that can drastically affect MGMT_AD4J_TS tablespace usage:

- JVMD Heap Dumps

Analyzing heap requires massive tablespace resources. Oracle recommends having 5 times the size of the heap dump file you are loading free in your tablespace. Since you will have the heap dump file and know its size before you run the load script, you should ensure that you have adequate space to accommodate the dump before you load it into your database.

- Thread Traces

  While these are smaller than heaps by an order of magnitude, these are loaded into the database automatically by default when you initiate a trace at the console. The size of these traces can vary dramatically depending on the number of active threads during the trace, the duration of the trace, and the sample interval of the trace. They should generally be under 100MB each, but a user utilizing a large number of these could manually fill up the database quickly. Again, since these are created only by manual intervention, you should ensure that there is adequate space to accommodate traces before initiating them.

# 12

# Installing ADP with Advanced Installation Options

This chapter describes how you can install Application Dependency and Performance (ADP) in the Enterprise Manager Cloud Control environment, using advanced installation options.

In particular, this chapter covers the following:

- Overview of Application Dependency and Performance Architecture
- Before you Begin Installing Application Dependency and Performance
- Prerequisites for Installing Application Dependency and Performance
- Installing Application Dependency and Performance Using Advanced Installation Options
- After Installing Application Dependency and Performance

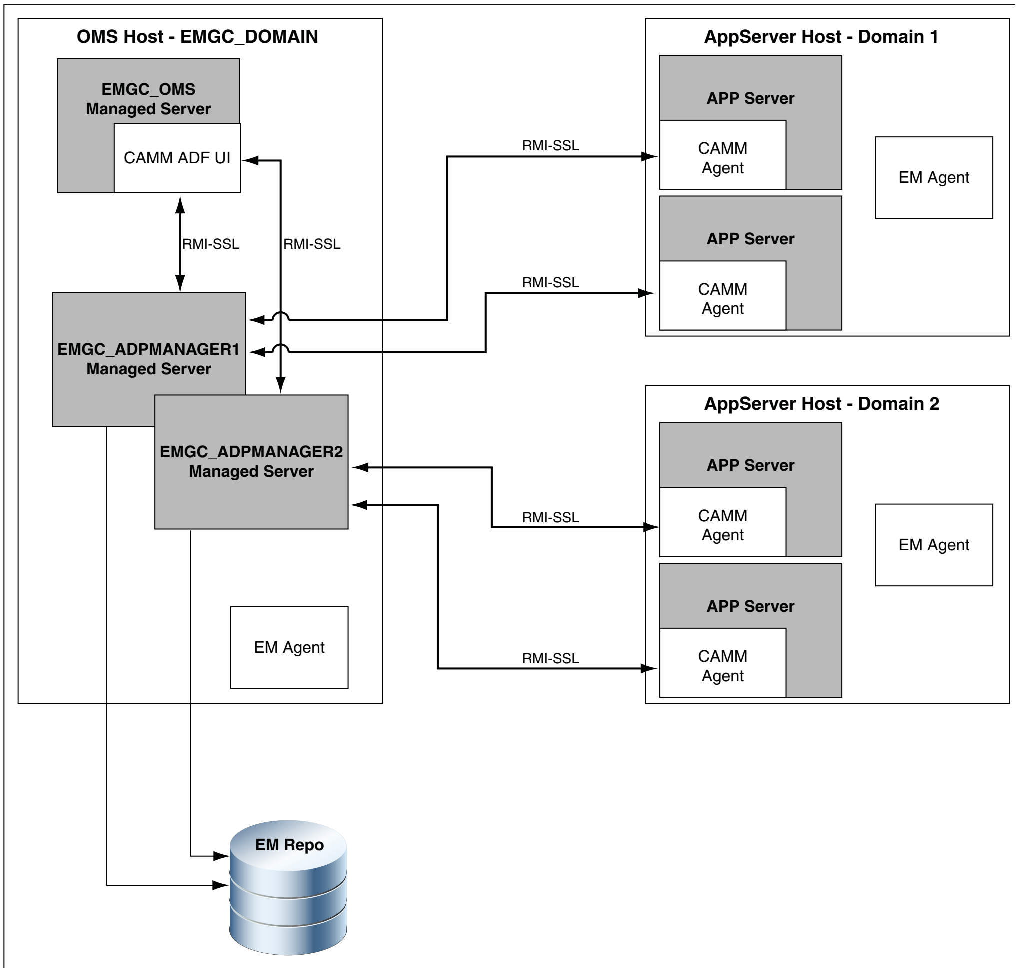
## 12.1 Overview of Application Dependency and Performance Architecture

Application Dependency and Performance (ADP) is one of the critical functionalities in Enterprise Manager Cloud Control that allows you to analyze Java EE, SOA, and Portal applications. It captures the complex relationships among various application building blocks in its application schema model - the core of the Oracle intelligent platform. To manage these applications effectively, enterprises must first gain an understanding of the complex relationships among the business functions, associated interconnected components, and the underlying runtime environments. To enable clear and accurate understanding, IT organizations need holistic, service-oriented views that span across heterogeneous environments.

Using the insights stored in Application Schema, ADP is able to deliver an Application Service Management (ASM) environment that self-customizes out-of-the-box, evolves with change, minimizes expert involvement, and delivers a holistic, service-oriented view across heterogeneous environments.

ADP employs a multi-tier, fully distributed, configurable architecture to provide the scalability and flexibility to meet the changing needs of enterprise deployments.

*Figure 12–1 ADP Architecture*



ADP Engine is the core analytical engine of the ADP ASM system. In real-time, ADP Engine performs complex mathematical modeling and statistical calculations with summarized data from all ADP Java Agents. ADP Engine can be configured with a backup to provide higher level of availability.

ADP Java Agents are the data collectors of the ADP ASM system. ADP Java Agents are deployed to all managed application servers to perform a series of tasks including collecting performance managements, tracking contextual relationships, and summarizing data in real-time while introducing as little overhead as possible.

## 12.2 Before you Begin Installing Application Dependency and Performance

Before installing ADP Engine or ADP Agent, review the points outlined in *Oracle Enterprise Manager Basic Installation Guide*.

## 12.3 Prerequisites for Installing Application Dependency and Performance

Before installing ADP Engine or ADP Agent, ensure that you meet the prerequisites described in *Oracle Enterprise Manager Basic Installation Guide.*

## 12.4 Installing Application Dependency and Performance Using Advanced Installation Options

This section describes how to install ADP manually, using scripts. It includes the following:

- Deploying ADP Engine Manually Using ApmEngineSetup.pl
- Deploying ADP Agents Manually Using deploy_adpagent.pl

### 12.4.1 Deploying ADP Engine Manually Using ApmEngineSetup.pl

You can deploy ADP Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

> **Important:** You can use the `ApmEngineSetup.pl` script to deploy ADP Engine only on a host that is running the OMS, and not on a remote host.

To deploy ADP Engine manually using the `ApmEngineSetup.pl` script, follow these steps:

1. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/engine/
   ```

2. View the `README.txt` file, for information on using the `ApmEngineSetup.pl` script.

3. Run the `ApmEngineSetup.pl` script.

   If you want to run the `ApmEngineSetup.pl` script in interactive mode, such that you are prompted for the input details, use the following command:

   ```
   perl ApmEngineSetup.pl
   ```

   Ensure that you specify the operation as `deploy`, and the Engine Type as `ADP`.

   If you want to run the `ApmEngineSetup.pl` script in silent mode, specify all the input details in a properties file, then use the following command:

   ```
   perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
   <password>
   ```

   `<properties_file_name>` is the name of the properties file where the ADP Engine and operation details are provided. `<password>` is the WebLogic console password.

   To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

### 12.4.2 Deploying ADP Agents Manually Using deploy_adpagent.pl

You can deploy ADP Agents manually, using the `deploy_adpagent.pl` script. You can run this script only in silent mode, that is, you must specify all the input details using a properties file.

To deploy ADP Agents manually using `deploy_adpagent.pl`, follow these steps:

1. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/agent/adp/
   ```

2. View the `README.txt` file, for information on using the `deploy_adpagent.pl` script.

3. Specify all the inputs in a properties file, then use the following command:

   ```
   perl deploy_adpagent.pl <properties_file_name>
   ```

   If you do not pass the name of the properties file as a parameter while running `deploy_adpagent.pl, deploy_adpagent.pl` looks for a properties file named `adpagent.properties` in the same folder. To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_adpagent.properties`.

## 12.5 After Installing Application Dependency and Performance

This section describes the tasks you can perform after installing ADP Engines and ADP Agents. It consists of the following:

- Verifying ADP Engine and ADP Agent Installation
- Configuring Oracle SOA Suite for Secure Connectivity (After Installing ADP)
- Configuring Oracle WebLogic Server or Oracle WebLogic Portal (WLP) for Secure Connectivity (After Installing ADP)
- Importing a Certificate into ADP Engine's Keystore
- Configuring ADP Agent When WebLogic Is Installed As a Windows Service

### 12.5.1 Verifying ADP Engine and ADP Agent Installation

For information on verifying the ADP Engine and ADP Agent installations, refer *Oracle Enterprise Manager Basic Installation Guide.*

### 12.5.2 Configuring Oracle SOA Suite for Secure Connectivity (After Installing ADP)

The Oracle SOA Suite may be configured to support RMIS (RMI over SSL) connectivity. In this case, ADP can be configured to use this secure connection. To configure ADP to do this, perform the following steps:

1. In the Oracle SOA Suite install, look at `ORACLE_HOME/j2ee/<instance>/config/rmi.xml`, locate the `<ssl-config>` element, and identify the path in the keystore attribute.

2. Copy the KeyStore file indicated to ADP Engine's `config` directory (for example, `em10/config`)

3. Import this KeyStore file following the instructions in Section 12.5.4.

### 12.5.3 Configuring Oracle WebLogic Server or Oracle WebLogic Portal (WLP) for Secure Connectivity (After Installing ADP)

To configure Oracle WebLogic Server 10.0 to handle connectivity using t3s, the location of the KeyStore files needs to be updated through the console. To do this, follow these steps:

1. Log in to the WebLogic Server Administration console and select the servers from the **Environment Servers** list that you plan to manage with ADP.

2. Select a server from the server list.
3. Select the **Keystores** tab, then click **Load & Edit** to update the KeyStore.
4. Identify the KeyStore and TrustStore file paths from the following properties:

   **Identity**

   Custom Identity Keystore

   **Trust**

   Custom Trust Keystore: location of the trust file
5. Repeat Steps 2 to 4 for additional server instances that you want to manage using ADP.
6. Copy the identified KeyStore and TrustStore files to the ADP Engine.
7. Copy the `BEA_HOME/license.bea` to the ADP Engine's `config` directory (for example, `em11g/config`).
8. Import the KeyStore and TrustStore files following the instructions in Section 12.5.4.
9. Locate the following properties in the `Acsera.properties` file, and set them as follows:

   ```
   weblogic.security.TrustKeyStore=CustomTrust
   weblogic.security.CustomTrustKeyStoreFileName=AcseraManagerTrust.jks
   weblogic.security.CustomTrustKeyStorePassPhrase=acseramanager
   ```

### 12.5.4 Importing a Certificate into ADP Engine's Keystore

To import entries from a Keystore or TrustStore, perform the following steps, replacing `ServerStoreFile.jks` with the KeyStore or TrustStore from your application server. You will generally need to complete these steps twice, once for the KeyStore and once for the TrustStore.

1. List the key aliases in the KeyStore/TrustStore file from the server:

   ```
   keytool -list -keystore ServerStoreFile.jks -storepass
   DemoIdentityKeyStorePassPhrase

   Output:

   Keystore type: jks
   Keystore provider: SUN

   Your keystore contains 1 entry:

   demoidentity, Wed Nov 19 13:34:56 PST 2008, keyEntry, Certificate fingerprint
   (MD5): 36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
   ```
2. Export a key entry to an intermediate file:

   ```
   keytool -export -alias demoidentity -keystore ServerStoreFile.jks -storepass
   DemoIdentityKeyStorePassPhrase -file demo103

   Output:

   Certificate stored in file <demo103>
   ```
3. Import the key into the ADP store file (either `AcseraManagerKey.jks` or `AcseraManagerTrust.jks` in the ADP Engine's `config` directory)

```
keytool -import -alias demoidentity1 -keystore AcseraManagerKey.jks
-storepass acseramanager -file demo103

Output:

Owner: CN=b91, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown, ST=MyState,
C=US
Issuer: CN=CertGenCAB, OU=FOR TESTING ONLY, O=MyOrganization, L=MyTown,
ST=MyState, C=US
Serial number: 510fb3d4b2872e3a093d436fcbe9b24b
Valid from: Tue Nov 18 13:34:47 PST 2008 until: Sun Nov 19 13:34:47 PST 2023
Certificate fingerprints:
             MD5:  36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
             SHA1: BB:85:6D:4C:0B:4A:92:63:CA:5E:E9:A8:54:42:80:2D:0D:BE:7C:91
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

4. Verify that the key was imported successfully:

```
keytool -list -keystore AcseraManagerKey.jks -storepass acseramanager

Output:

Keystore type: jks
Keystore provider: SUN

Your keystore contains 3 entries:

demoidentity1, Wed Apr 01 13:03:21 PST 2009, trustedCertEntry,Certificate
fingerprint (MD5): 36:06:C2:44:31:0A:28:FC:06:19:F7:AB:C0:7D:27:6A
demoidentity, Fri Mar 13 15:15:06 PST 2009, trustedCertEntry,Certificate
fingerprint (MD5): 0B:11:02:B5:44:0D:2A:CC:7F:C5:30:5C:1A:C9:A1:6C
mykey, Thu May 19 16:57:36 PDT 2005, keyEntry,Certificate fingerprint (MD5):
5D:B0:EC:28:14:33:26:1F:44:F5:BE:DD:A8:50:15:9D
```

5. Repeat Steps 2 to 4 for each key entry listed in Step 1.

6. Locate the following properties in the `Acsera.properties` file, and set them as follows:

```
weblogic.security.TrustKeyStore=CustomTrust
weblogic.security.CustomTrustKeyStoreFileName=AcseraManagerTrust.jks
weblogic.security.CustomTrustKeyStorePassPhrase=acseramanager
```

At present, with ADP running with a bundled Sun HotSpot JDK, it is not possible for ADP to configure with PKCS12 type key/trust stores for secure connections. IBM JDK has built-in enhancements that allow it to work with PKCS12 key/trust stores, such as WebSphere 6.1's default key.p12 and trust.p12 stores. Also, there is a WebSphere 6.1 automatic function that is enabled with the property `com.ibm.ssl.enableSignerExchangePrompt=true` that allows a client connecting to a secure WebSphere port that allows automatic download of server's signer certificate and update of client's truststore. However, this automatic function is only available when ADP is running with an IBM JDK, which is not the case at present. This is the reason why we need to follow the above procedure to connect with a secured WebSphere 6.1.

### 12.5.5 Configuring ADP Agent When WebLogic Is Installed As a Windows Service

When the monitored WebLogic Server is installed as a Windows service, the automatic startup changes to deploy ADP Agent need to be manually applied to the registry entries that control the WebLogic startup.

The parameters that need to be changed are in the Windows registry key:

```
HKEY_LOCAL_MACHINE\SYSTEM\Current
ControlSet\Services\$ServiceName\Parameters
```

Users should then consult the file on the ADP Engine:

```
deploy/agent/bea9/bin/agentoptions.bat (for WebLogic 9.x and higher)
```

Inspect this file and resolve the net results of its execution as parameters in the registry.

# 13

# Installing JVMD with Advanced Install Options

This chapter describes how you can install JVM Diagnostics (JVMD) manually in the Enterprise Manager Cloud Control environment.

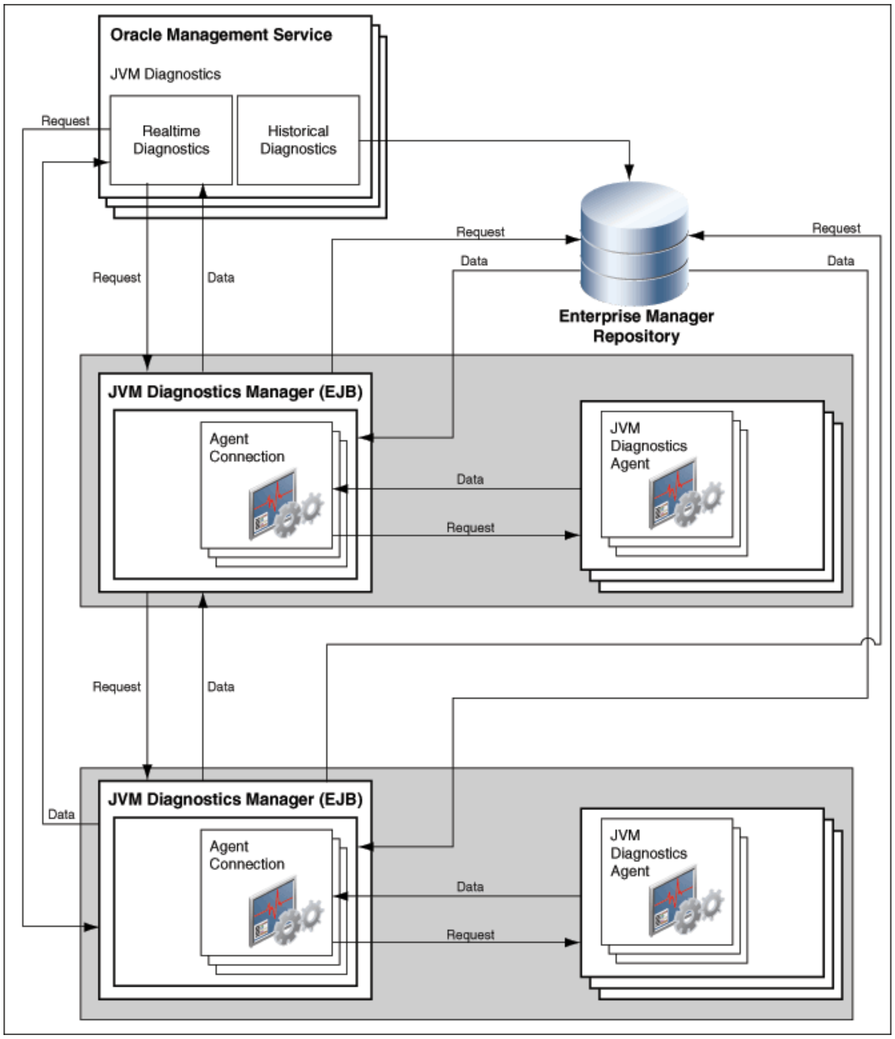
In particular, this chapter covers the following:

## 13.1 Overview of JVMD Architecture

JVM Diagnostics is integrated with Oracle Enterprise Manager Cloud Control. It primarily enables administrators to diagnose performance problems in Java applications in the production environment. By eliminating the need to reproduce problems, it reduces the time required to resolve these problems, thus improving application availability and performance. Using JVMD, administrators can identify the root cause of performance problems in the production environment, without having to reproduce them in the test or development environment.

The following diagram shows the JVMD Architecture:

*Figure 13–1 JVMD Architecture*



JVMD Engine is the core analytical engine of the JVMD monitoring system. JVMD Engine collects runtime data from JVMD Agents on request from the OMS, and stores the data in the repository. Multiple JVMD Engines can be configured.

JVMD Agents are the data collectors of the target JVM. JVMD Agents are deployed to managed application servers to collect JVM monitoring data related to JVM threads, stacks, heap and CPU usage, and so on, in real-time, while introducing minimal overhead.

The JVMD Engine runs as an Enterprise JavaBeans (EJB) technology on a WebLogic Server. The JVMD Agent is deployed on the targeted JVM (the one running a production WebLogic Server). It collects real-time data and transmits it to the JVM Diagnostics Engine. This data is stored in the Management Repository, and the collected information is displayed on the Enterprise Manager Cloud Control console for monitoring purposes. The communication between JVMD Engine and JVMD Agent can be secure (SSL), or non-secure.

## 13.2 Before you Begin Installing JVMD

Before installing JVMD Engine or JVMD Agent, review the points outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

## 13.3 Prerequisites for Installing JVMD

Before installing JVMD Engine or JVMD Agent, ensure that you meet the prerequisites described in *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

## 13.4 Installing JVMD Using Advanced Installation Options

This section describes how to deploy JVMD Engines and JVMD Agents manually. It consists of the following:

- Deploying JVMD Engine Manually Using ApmEngineSetup.pl
- Deploying JVMD Agents

### 13.4.1 Deploying JVMD Engine Manually Using ApmEngineSetup.pl

You can deploy JVMD Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

> **Important:** You can use the `ApmEngineSetup.pl` script to deploy JVMD Engine only on a host that is running the OMS, and not on a remote host.

To deploy JVMD Engine manually using the `ApmEngineSetup.pl` script, follow these steps:

1. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/engine/
   ```

2. View the `README.txt` file, for information on using the `ApmEngineSetup.pl` script.

3. Run the `ApmEngineSetup.pl` script.

   If you want to run the `ApmEngineSetup.pl` script in interactive mode, such that you are prompted for the input details, use the following command:

   ```
   perl ApmEngineSetup.pl
   ```

   Ensure that you specify the operation as `deploy,` and the Engine Type as `JVMD`.

   If you want to run the `ApmEngineSetup.pl` script in silent mode, specify all the input details in a properties file, then use the following command:

   ```
   perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
   <password>
   ```

   `<properties_file_name>` is the name of the properties file where the JVMD Engine and operation details are provided. `<password>` is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

## 13.4.2 Deploying JVMD Agents

This section describes how to deploy JVMD Agents manually. It consists of the following:

- Deploying JVMD Agents Manually by Downloading and Deploying javadiagnosticagent.ear or jamagent.war
- Deploying JVMD Agents Manually Using deploy_jvmdagent.pl
- Deploying JVMD Agents for High Availability
- Deploying JVMD Database Agent
- Ensuring Secure Communication by Connecting JVMD Agent to the JVMD Engine Secure Port

### 13.4.2.1 Deploying JVMD Agents Manually by Downloading and Deploying javadiagnosticagent.ear or jamagent.war

To deploy JVMD Agents manually, follow these steps:

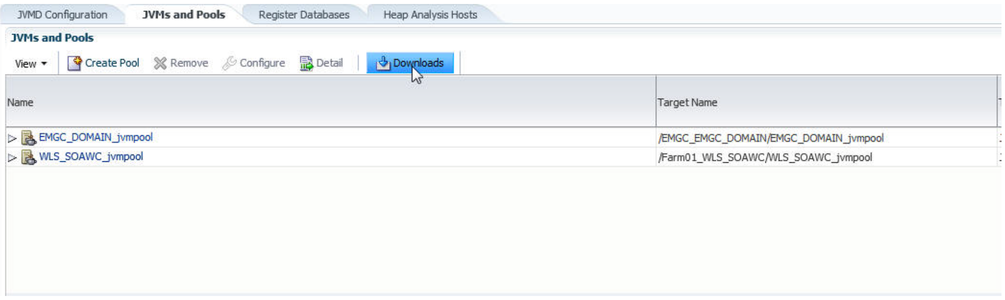
1. **Download javadiagnosticagent.ear or jamagent.war.**

> **Note:** Oracle recommends that you use `javadiagnosticagent.ear` to deploy a JVMD Agent on Oracle WebLogic Server. To deploy a JVMD Agent on an application server other than Oracle WebLogic Server, use `jamagent.war`.

**Downloading javadiagnosticagent.ear or jamagent.war Using Cloud Control**

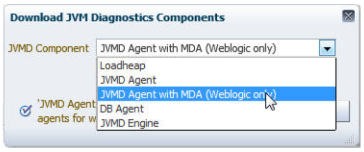
To download `javadiagnosticagent.ear` or `jamagent.war` using Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Middleware Management,** then select **Application Performance Management**.
2. On the Application Performance Management page, select **JVM Diagnostics Engine**.
3. Click **Configure.** The JVM Diagnostics Setup page appears.
4. On the JVM Diagnostics Setup page, click **JVMs and Pools**, then click **Download.** The Download JVM Diagnostics Component dialog box appears.



| Name | Target Name |
|---|---|
| ▷ EMGC_DOMAIN_jvmpool | /EMGC_EMGC_DOMAIN/EMGC_DOMAIN_jvmpool |
| ▷ WLS_SOAWC_jvmpool | /Farm01_WLS_SOAWC/WLS_SOAWC_jvmpool |

5. From the **JVMD Component** menu, to download `javadiagnosticagent.ear`, select **JVMD Agent with MDA (Weblogic only)**, then click **OK**. To download `jamagent.war`, from the **JVMD Component** menu, select **JVMD Agent,** then click **OK.** The JVM Diagnostics Agent `web.xml` parameters dialog box appears.



Download JVM Diagnostics Components

JVMD Component: JVMD Agent with MDA (Weblogic only)

6. From the **Available Engines** menu, select an option from the list, then click **Download**:

   Select the HTTP URL if you want the JVMD Agent to connect to the JVMD Engine using a non-secure connection.

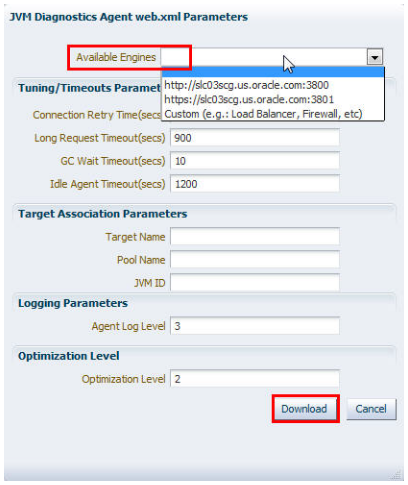
   Select the HTTPS URL if you want the JVMD Agent to connect to the JVMD Engine using a secure connection.

   Select **Custom** if you want the JVMD Agent to connect to a JVMD Engine through a load balancer. Specify the host name and the port that the JVMD Agent must connect to.

   For example:

   HTTP: `http://slc01.us.example.com:3800`

   HTTPS: `https://slc01.us.example.com:3801 (secure communication)`



JVM Diagnostics Agent web.xml Parameters

Available Engines

Tuning/Timeouts Paramet

Connection Retry Time(secs

Long Request Timeout(secs): 900

GC Wait Timeout(secs): 10

Idle Agent Timeout(secs): 1200

Target Association Parameters

Target Name

Pool Name

JVM ID

Logging Parameters

Agent Log Level: 3

Optimization Level

Optimization Level: 2

http://slc03scg.us.oracle.com:3800
https://slc03scg.us.oracle.com:3801
Custom (e.g.: Load Balancer, Firewall, etc)
Download
Cancel

7. Click **Download** to download `javadiagnosticagent.ear` or `jamagent.war`.

### Downloading jamagent.war Using javadiagnosticagent.ear

To download `jamagent.war` using `javadiagnosticagent.ear`, follow these steps:

1. Download the `javadiagnosticagent.ear` file to the following location:

   `<middleware_home>/oms/jvmd`

   The `javadiagnosticagent.ear` file can be downloaded from the following location:

   ```
   <MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/javadiagnosticagent.ear
   ```

2. Run the following command to extract `javadiagnosticagent.ear`:

   ```
   jar -xvf javadiagnosticagent.ear
   ```

   The extracted `javadiagnosticagent.ear` file contains `jamagent.war`.

3. Run the following command to extract `jamagent.war`:

   ```
   jar -xvf jamagent.war
   ```

4. Navigate to `WEB-INF/web.xml`.

5. Edit the `web.xml` file to update the values of the `jamconshost` and `jamconsport` parameters, where `jamconshost` is the IP of the host on which JVMD Engine is deployed, and `jamconsport` is the port of the same host.

   ---

   **Note:** To enable secure communication for the selected JVMD Engine, make the following change to the `web.xml` file:

   ```
   jamsecureCommunication = 1
   ```

   ---

   For example:

   ```
   <init-param>
          <param-name>jamconshost</param-name>
          <param-value>slc01axn</param-value>
          <description>Jam console host - demolnx.auptyma.com</description>
   </init-param>
   <init-param>
          <param-name>jamconsport</param-name>
          <param-value>3800</param-value>
          <description>Jam console port</description>
   </init-param>
   ```

   ---

   **Note:** Once JVMD Engine is deployed, the IP and the port appear on the JVMD Deployment page as: `<Machine Name:Port Number>`

   ---

6. Run the following command to reassemble the `jamagent.war` file:

   ```
   jar -cMvf jamagent.war META-INF WEB-INF jamagent oracle
   ```

   The updated `jamagent.war` file is now ready for deployment.

   If you encounter any errors during the deployment, see Section J.2.

2. **Deploy JVMD Agent manually.**

   **Deploying JVMD Agent on WebLogic Server**

   To deploy JVMD Agent on a WebLogic Managed Server manually, follow these steps:

   1. Make a copy of the deployment profile `sample_jvmdagent_deploy.properties` available in the `jvmd.zip` file. Update the location of the `javadiagnosticagent.ear` file, the name of the WebLogic domain, and the server information. Save the profile as `jvmdagent_deploy.properties`.

      For more information about the parameters, view the `README.txt` file present in the `customprov` folder of the `jvmd.zip` file.

2. Run the following perl script available in the `customprov` folder of the `jvmd.zip` file to deploy JVMD Agent on all the specified servers.

   ```
   perl deploy_jvmdagent.pl
   ```

   ---

   **Note:** Ensure that the deployment profile `jvmdagent_deploy.properties` and the perl scripts are available in the same folder.

   ---

### Deploying JVMD Agent on GlassFish

To deploy JVMD Agent on a GlassFish server manually, follow these steps:

1. Log in to the Glassfish Administration console.
2. In the Common Tasks section, click **Applications.**
3. In the Deployed Applications section, click **Deploy.**
4. For **Location,** select **Packaged File to Be Uploaded to the Server,** then specify the location on your local host where `jamagent.war` is present.
5. For **Selected Targets,** add the server on which you want to deploy `jamagent.war.`
6. Click **OK.**

### Deploying JVMD Agent on JBoss

To deploy JVMD Agent on JBoss manually, follow these steps:

1. Log in to the JBoss Administration console.
2. Under **Applications,** click **Web Application (WAR)s.**
3. Click **Add a new resource.**
4. Enter the absolute path to `jamagent.war` present on your local host.
5. For both **Deploy Exploded** and **Deploy Farmed,** select **No.**
6. Click **Continue.**

To deploy JVMD Agent on JBoss manually, you can also do the following:

1. Transfer `jamagent.war` to the following location:

   ```
   <JBOSS_HOME>/server/all/deploy
   ```

2. Restart the application server.

### Deploying JVMD Agent on Tomcat

To deploy JVMD Agent on Tomcat manually, follow these steps:

1. Transfer `jamagent.war` to the following location:

   ```
   $CATALINA_BASE/webapps
   ```

2. Restart the application server.

For the latest versions of Tomcat, if the `autoDeploy` flag is set to `true` in `$CATALINA_BASE/conf/server.xml,` you do not need to restart the application server. Tomcat will pick up `jamagent.war` at runtime.

### Deploying JVMD Agent on Websphere

To deploy JVMD Agent on Websphere manually, follow these steps:

1. Log in to the Websphere Administration console.
2. Expand **Applications,** then click **New Application.**
3. Click **New Enterprise Application.**
4. For **Path to the new application,** select **Local file system,** then specify the location on your local host where `jamagent.war` is present.
5. Provide the context root for `jamagent.war.`
6. Save the configuration.
7. Start the application**.**

### Deploying JVMD Agent on OC4J

To deploy JVMD Agent on OC4J manually, follow these steps:

1. Log in to the OC4J Administration console.
2. Click **Applications.**
3. Click **Deploy.**
4. Select **Archive is present on local host.** For **Archive Location,** specify the location on your local host where `jamagent.war` is present. Click **Next.**
5. For **Application Name,** enter `jamagent.` For **Context Root,** enter `/jamagent.`
6. Click **Deploy.**

### Deploying JVMD Agent on a Standalone JVM

A JVMD Agent can be deployed on a standalone JVM such that the inputs are read from `web.xml,` or such that you specify the inputs on the command line.

To deploy a JVMD Agent on a standalone JVM such that all the inputs are read from `web.xml,` run the following command from the command line:

```
java -cp <absolute_path_to_jamagent.war> jamagent.jamrun <java_class_
with_a_main_method>
```

To deploy a JVMD Agent on a standalone JVM by specifying all the inputs on the command line, run the following command from the command line:

```
java -cp <absolute_path_to_jamagent.war> jamagent.jamrun <java_class_
with_a_main_method> jamconshost=<jvmd_engine_host> jamconsport=<jvmd_
engine_listen_port> jamjvmid=<unique_jvmd_identifier>
jamtimeout=<timeout_period_in_seconds> jamloglevel=<jvmd_agent_log_
level>
```

**Note:** When `jamagent.war` is run using an IBM Java Development Kit (JDK), you may see the following warning in the logs:

```
******can_tag_objects capability is not set.Copy library
libjamcapability to another directory and restart Java with
argument "-agentpath:<absolute_path_to_libjamcapability.so>" ******
```

To troubleshoot this warning, include the `libjamcapability.so` library and restart the IBM JVM:

```
/scratch/IBM/WebSphere/AppServer/java/bin/java
-agentpath:/scratch/libjamcapability.so -cp
/scratch/jamagent.war jamagent.jamrun MyFirstProgram
```

#### 13.4.2.2 Deploying JVMD Agents Manually Using deploy_jvmdagent.pl

You can deploy JVMD Agents manually, using the `deploy_jvmdagent.pl` script. You can run this script only in silent mode, that is, you must specify all the input details using a properties file.

To deploy JVMD Agents manually using `deploy_jvmdagent.pl,` follow these steps:

1. Ensure that the latest version of `javadiagnosticagent.ear` or `jamagent.war` has been downloaded.

   For information on how to download `javadiagnosticagent.ear` or `jamagent.war,` see Step 1 in Section 13.4.2.1.

2. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/agent/jvmd/
   ```

3. View the `README.txt` file for information on how to use the `deploy_jvmdagent.pl` script.

4. Specify all the inputs in a properties file, then use the following command:

   ```
   perl deploy_jvmdagent.pl [-appserver <server_type>] [-file <name_of_
   properties_file>]
   ```

   For example, `perl deploy_jvmdagent.pl -appserver WLS -file wls_deploy.properties.`

   Deploying JVMD Agents using `deploy_jvmdagent.pl` is supported only on WebLogic Server and GlassFish, and not on other application servers. The `-appserver` parameter specifies the application server on which you want to deploy a JVMD Agent. If you are deploying a JVMD Agent on a WebLogic Managed Server, specify `WLS` for `-appserver.` If you are deploying a JVMD Agent on a GlassFish server, specify `GF` for `-appserver.` If you do not specify the `-appserver` parameter, it is assigned the value `WLS` by default.

   The `-file` parameter specifies the name of the properties file containing the deployment inputs. If you do not specify this parameter, and have specified `WLS` for `-appserver, deploy_jvmdagent.pl` searches for a properties file named `weblogic_deploy.properties` in the folder containing the script. If you do not specify the `-file` parameter, and have specified `GF` for `-appserver, deploy_jvmdagent.pl` looks for a properties file named `glassfish_deploy.properties` in the folder containing the script. To learn how to specify the input details in a properties file, view the sample properties files `sample_weblogic_deploy.properties` or `sample_glassfish_deploy.properties.`

### 13.4.2.3 Deploying JVMD Agents for High Availability

If you have multiple JVMD Engines deployed in your setup, and have configured a load balancer for them, you can deploy JVMD Agents such that they connect to the load balancer, and not to any of the individual JVMD Engines. This increases the availability of the JVMD Agents, and creates a failover mechanism, that is, even if a particular JVMD Engine goes down, the JVMD Agents remain active.

You can deploy JVMD Agents for high availability using the Application Performance Management page, or manually.

**Deploying JVMD Agents for High Availability Using the Application Performance Management Page**

To deploy JVMD Agents for high availability using the Application Performance Management page, follow these steps:

1. Follow the steps mentioned in *Oracle Enterprise Manager Cloud Control Basic Installation Guide* to deploy a JVMD Agent.
2. On the JVMD Agents Configurations page, for **Available JVMD Engines,** select **Other.** Provide the load balancer host name and port.

   Click **Next.**
3. On the Review page, review all the information, then click **Deploy.**

> **Note:** By default, the JVMD Agent connects to the load balancer using HTTP. If you want the JVMD Agent to connect to the load balancer using HTTPS, you must deploy the JVMD Agent manually, as described in Step 2 of Section 13.4.2.1.

**Deploying JVMD Agents for High Availability Manually**

To deploy JVMD Agents for high availability manually, follow these steps:

1. Follow the steps mentioned in Step 1 of Section 13.4.2.1 to download `javadiagnosticagent.ear` or `jamagent.war`.
2. When the JVM Diagnostics Agent `web.xml` parameters dialog box is displayed, from the **Available Engines** menu, select **Custom.** Provide the load balancer host name and port.

   Click **Download.**
3. Deploy the JVMD Agent as mentioned in Step 2 of Section 13.4.2.1.

> **Note:** By default, the JVMD Agent connects to the load balancer using HTTP. If you want the JVMD Agent to connect to the load balancer using HTTPS, you must use a certificate, as described in Section 13.4.2.5. Ensure that the common name of the certificate you use matches the host name of the load balancer.

### 13.4.2.4 Deploying JVMD Database Agent

To deploy JVMD Database Agent, download JVMD Agent from Cloud Control, as it can serve as a JVMD Database Agent too. If JVMD Agent is downloaded and deployed on the same host as Oracle Database, then you do not require a separate JVMD Database Agent. JVMD Agent itself orchestrates between the database and JVMD

Engine. However, if JVMD Agent and the database are on separate hosts, then you need a JVMD Database Agent to collect the database specific information, and transmit the collected data to JVMD Engine.

> **Note:** JVMD Database Agents are supported on the platforms on which JVMD Agents are supported, except for Microsoft Windows. JVMD Database Agent needs Java 1.4.X or higher to run.

To download and deploy JVMD Database Agent, do the following:

1. Follow the steps listed in Step 1 of Section 13.4.2.1 to download the `jamagent.war` file using Cloud Control.
2. To start the JVMD Database Agent, run the following command:

   ```
   $JAVA_HOME/bin/java -Xms126M -Xmx512M -cp ./jamagent.war jamagent.Dbagent
   jamconshost=<Host on which engine is running> jamconsport=<Port of the server
   on which JVMD Engine is installed>

   For Example: /usr/local/packages/jdk14/bin/java -Xms126M -Xmx512M -cp
   ./jamagent.war jamagent.Dbagent jamconshost=adc2190661.us.example.com
   jamconsport=3900
   ```

   > **Note:** If you encounter the error message `TIMEOUT from console JAM Agent: Error receiving data from console`, then restart the JVMD Database Agent with the option `jamconsretr = 5`.

### 13.4.2.5 Ensuring Secure Communication by Connecting JVMD Agent to the JVMD Engine Secure Port

To ensure secure communication with the JVMD Engine, the JVMD Agent must have access to a KeyStore in which the certificate of the Managed Server (on which the JVMD Engine is deployed) is added. The KeyStore of the Enterprise Manager Cloud Control domain (that is, the EMGC domain in which the JVMD Engine Managed Server is created) can be used for the same.

If the JVMD Engine and the JVMD Agent are running on the same host, the JVMD Agent will have access to the EMGC domain and the default KeyStore. In this case, follow these steps to ensure secure communication:

1. Locate the KeyStore. It is usually available in the following location:

   ```
   <WEBLOGIC_HOME>/server/lib/DemoTrust.jks
   ```

   `WEBLOGIC_HOME` refers to the installation directory of the WebLogic Server software.
2. Log in to the WebLogic Server Administration Console.
3. From the **Environment** menu, select **Servers.**
4. Select the Managed Server on which the JVMD Agent is deployed, then select the **Server Start** tab.
5. For **Arguments,** specify the following arguments:

   ```
   -Djavax.net.debug=ssl -Djavax.net.ssl.trustStore=<location_of_
   DemoTrust.jks> -Djavax.net.ssl.trustStorePassword=<DemoTrust.jks_
   KeyStore_password>
   ```

**Note:** The default password for the DemoTrust.jks KeyStore is `DemoTrustKeyStorePassPhrase.`

6. Restart the Managed Server.

If the JVMD Engine and the JVMD Agent are running on different hosts, which is the case in most environments, you must download the SSL certificate from the JVMD Engine Managed Server, then add the certificate to a new or an existing KeyStore on the target Managed Server where the JVMD Agent is deployed. This enables the JVMD Agent to access the certificate and communicate with the JVMD Engine secure port. To do this, follow these steps:

1. Follow these steps to download the JVMD Engine Managed Server certificate:
    1. Access the following URL using a browser:

       ```
       https://<jamconshost>:<jamconsport(secure)>
       ```

    2. From the **Tools** menu, select **Options.**
    3. Select the **Advanced** tab, then select the **Encryption** tab.
    4. Click **View Certificates.**
    5. Select the **Servers** tab, search for the `<jamconshost>:<jamconsport(secure)>` certificate, then select it. Click **Export.**
    6. Save the certificate as `JVMDCert.crt.`
2. Add the certificate to an existing KeyStore (for example, `DemoTrust.jks),` or create a new KeyStore (for example, `keystore.jks)` and then add the certificate to it. To do this, run the following command:

   ```
   keytool -import -trustcacerts -alias root -file JVMDCert.crt -keystore
   <name_of_existing_or_new_KeyStore>
   ```

   If you specify an existing KeyStore name for the `-keystore` parameter, you are prompted for the KeyStore password. If you specify a new KeyStore name for the `-keystore` parameter, a new KeyStore is created with the default password `changeit.`
3. Log in to the WebLogic Server Administration Console.
4. From the **Environment** menu, select **Servers.**
5. Select the Managed Server on which the JVMD Agent is deployed, then select the **Server Start** tab.
6. For **Arguments,** specify the following arguments:

   ```
   -Djavax.net.debug=ssl -Djavax.net.ssl.trustStore=<location_of_KeyStore>
   -Djavax.net.ssl.trustStorePassword=<KeyStore_password>
   ```

   **Note:** The default password for the DemoTrust.jks KeyStore is `DemoTrustKeyStorePassPhrase.`

7. Restart the Managed Server.

**Note:** When a WebLogic Managed Server running on a Sun or JRockit Java Virtual Machine (JVM) attempts to connect to an external resource using HTTPS, you may encounter the following exception:

```
java.lang.ClassCastException:
weblogic.net.http.SOAPHttpsURLConnection
```

This exception occurs because a HTTP API attempts to use an underlying WebLogic implementation, instead of using the Sun implementation. To avoid this exception, using the runtime argument, set the following flag:

```
-DUseSunHttpHandler=true
```

## 13.5 After Installing JVMD

After installing JVMD Engine or JVMD Agent, follow the steps outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

# 14 Configuring BI Publisher with Enterprise Manager

Oracle Business Intelligence (BI) Publisher is Oracle's primary reporting tool for authoring, managing, and delivering all your highly formatted documents. BI Publisher ships standard with Enterprise Manager Cloud Control 12*c*.

This chapter covers the following topics:

## 14.1 Overview

For Enterprise Manager 12c Release 4 (12.1.0.4) or greater, BI Publisher binaries are installed by default, alongside Enterprise Manager. Configuration of BI Publisher is accomplished using the *configureBIP* script. The configureBIP script performs the following operations:

- Installs the BI Publisher schema into the Enterprise Manager repository database
- Integrates BI Publisher into the same WebLogic server domain as Enterprise Manager.

> **Note:** It is not necessary to perform a software-only install of BI Enterprise Edition (BIEE). Do not install any version of BIEE into the Middleware Home that contains Enterprise Manager.

This process will configure the primary BI Publisher server named "BIP." The primary BI Publisher server is always named BIP.

- Highly formatted, professional quality, reports, with pagination and headers/footers.
- PDF, Excel, PowerPoint, Word, and HTML report formats.
- Develop your own custom reports against the Enterprise Manager repository (read-only repository access).
- Integration with Enterprise Manager Security.
- Grant varying levels of BI Publisher functionality to different Enterprise Manager administrators.
- Use BI Publisher's scheduling capabilities and delivery mechanisms such as e-mail and FTP.

> **Note:** The Information Publisher (IP) reporting framework, though still supported in Enterprise Manager 12c Cloud Control, was deprecated as of Enterprise Manager 12c Release 1 (12.1.0.1). No further report development will occur using the IP framework.

### 14.1.1 Limitations

The following limitations apply to the use of reports and data sources.

- Out-of-box reports cannot be edited.
- If Out-of-box reports are copied, there is no guarantee that the copies will work with future product releases.

## 14.2 BI Publisher Configuration and Integration with Enterprise Manager 12c

The following procedures assume that you are familiar with both BI Publisher and Enterprise Manager. Refer to the *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide* for detailed information about Enterprise Manager.

**For More Information:** For information on developing BI Publisher reports, see the Oracle® Fusion Middleware Report Designer's Guide for Oracle Business Intelligence Publisher.

## 14.2.1 Installing Enterprise Manager and Required Infrastructure

In order to support the required resources for BI Publisher, the first OMS system (where BI Publisher is initially installed and eventually configured) needs the following additional system requirements above and beyond what is already required by Enterprise Manager:

- +1.5 GB of RAM minimum. 4 - 5 GB of RAM is recommended for best performance.
- For Enterprise Manager 12c Release 4 (12.1.0.4) or greater, there are no longer any specific disk space requirements, as the BI Publisher footprint has been dramatically reduced.

For additional resource requirements, see the following support note:

*How to Determine the Number of Servers Needed to Run BI Publisher Enterprise in a Production 10g or 11g Environment?* (Doc ID 948841.1)

### 14.2.1.1 Integrating BI Publisher with Enterprise Manager using the configureBIP Script

Integrating BI Publisher with Enterprise Manager requires changing the domain configuration. However, you must first back up Enterprise Manager using standard procedures covered in Enterprise Manager High Availability documentation using the command:

```
emctl exportconfig oms [-sysman_pwd <sysman password>]
          [-dir <backup dir>]      Specify directory to store backup file
          [-oms_only]              Specify OMS-only backup on Admin Server host
          [-keep_host]             Specify to backup hostname if no slb defined
                                   (Use this option only if recovery will be done
                                    on machine that responds to this hostname)
```

**IMPORTANT:** The *configureBIP* script must be run as the same operating system user who owns the Oracle Middleware Home.

DO NOT run *configureBIP* as the Unix Super User (root).

There are two scenarios in which you would run configureBIP:

- Scenario 1: Fresh Configuration of BI Publisher in Enterprise Manager Release 4 (12.1.0.4) or Release 5 (12.1.0.5).

  The fresh configuration case is used when either of these conditions are met:

  – You are installing Enterprise Manager 12c for the first time. A previous version of Enterprise Manager 12c was not installed previously

  – You are upgrading to Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5) from a previous version of Enterprise Manager 12c and you had not previously installed and integrated the appropriate version of BI Publisher with that prior version of Enterprise Manager 12c.

- Scenario 2: Upgrade configuration of BI Publisher in Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5) from a previous installation of Enterprise Manager 12c to Enterprise Manager Release 4 (12.1.0.4) or Release 5 (12.1.0.5).

  Use the *configureBIP* script in upgrade configuration mode if both of the following conditions are true:

  - You have already upgraded a previous release of Enterprise Manager 12c Release 2 (12.1.0.2) or  Enterprise Manager 12c Release 3 (12.1.0.3) to Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5).
  - The previous installation of Enterprise Manager 12c had been integrated with the appropriate version of BI Publisher.

The *configureBIP* script requires the following credentials in order to operate:

- An Oracle account with SYSDBA privilege; normally the SYS account.
- The database password for this account.
- The WebLogic Admin Server password.

> **IMPORTANT:** Make sure to run the *configureBIP* from the new Enterprise Manager Release 12.1.0.4 or 12.1.0.5 installation.

Make sure to gather the above credentials before proceeding.

Both the normal mode and upgrade mode of *configureBIP* are discussed in detail in the following two sections. Be sure to operate the *configureBIP* script in the appropriate mode for your installation scenario.

## 14.3 Configure BI Publisher that gets Deployed with Enterprise Manager Release 4 (12.1.0.4) or Release 5 (12.1.0.5)

The following steps are performed for a fresh configuration of BI Publisher in Enterprise Manager Release 4/5. The script performs three major operations:

- **Step 1** - Command invocation and credential gathering.
- **Step 2** - The creation of the BI Publisher database schema, which is named SYSMAN_BIPLATFORM. This is accomplished using the Oracle Repository Creation Utility (RCU).
- **Step 3** - The WebLogic domain that contains Enterprise Manager is extend to include BI Publisher, and BI Publisher is configured.

### Step 1: Command Invocation and Credential Gathering

1. From the OMS instance's ORACLE_HOME/oms/bin directory (of the current Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5) installation), execute the *configureBIP* script from the command line. For example:

   ```
   cd /oracle/middleware/oms/bin
   configureBIP
   ```

2. The script prompts for the necessary credentials.
3. The script executes the Repository Creation Utility (RCU), since this is normal mode, to create the BI Publisher database schema.

4. The script prompts for two inputs for the port(s) to use for the BI Publisher Managed Server: One port for non-SSL and one port for SSL. For Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5), it is required that both of these port values be provided.
5. The script then performs the extend-domain operations.
6. Enterprise Manager, including BI Publisher, will be set to the same "Lock" mode as it was prior to running configureBIP. This is done via the command "emctl secure {lock | unlock}.
7. Enterprise Manager is stopped and then started
8. The Enterprise Manager-supplied BI Publisher Reports are deployed to the newly installed BI Publisher Web application.
9. The Enterprise Manager WebLogic domain target is refreshed to include the newly added BI Publisher targets.
10. A backup of Enterprise Manager is performed using `emctl exportconfig oms`.

    This backup is stored in the instance home directory, under the `em/sysman/backup` sub-directory. The backup created during the *configureBIP* script will be the newest file in this directory, after *configureBIP* is run.

### Step 2: Run the Repository Configuration Utility (RCU)

Since you are installing BI Publisher for the first time, the schema will be created using the RCU utility. You should see the something like the following output:

```
Creating SYSMAN_BIPPLATFORM Schema in EM Repository Database

Configuring BI Publisher in Oracle Home located in /oracle/middleware/Oracle_BI1
...
Processing command line ....
Repository Creation Utility - Checking Prerequisites
Checking Global Prerequisites
Repository Creation Utility - Checking Prerequisites
Checking Component Prerequisites
Repository Creation Utility - Creating Tablespaces
Validating and Creating Tablespaces
Repository Creation Utility - Create
Repository Create in progress.
Percent Complete: 0
Percent Complete: 10
Percent Complete: 30
Percent Complete: 50
Percent Complete: 50
Percent Complete: 100
Repository Creation Utility: Create - Completion Summary
Database details:
Connect Descriptor                      : (DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=em.example.com)(PORT=15044)))(CONNECT_
DATA=(SID=emsid)))
Connected As                    : sys
Prefix for (prefixable) Schema Owners : SYSMAN
RCU Logfile                     :
/oracle/middleware/oms/cfgtoollogs/bip/emBIPLATFORM.log
Component schemas created:
Component                       Status  Logfile
Business Intelligence Platform          Success
/oracle/middleware/oms/cfgtoollogs/bip/biplatform.log
```

```
Repository Creation Utility - Create : Operation Completed

Successfully created SYSMAN_BIPLATFORM schema...
```

### Step 3: WebLogic Domain Configuration

Successful execution of this step displays screen output similar to the following:

```
Configuring BI Publisher in Oracle Home located in /oracle/work/middleware/Oracle_
BI1 ...
Extending domain with BI Publisher. This operations can take some time. Do not
interrupt this command while it is running...
Locking Enterprise Manager ...
OMS Console is locked. Access the console over HTTPS ports.
Restart OMS.
Restarting Enterprise Manager ...
Stopping Enterprise Manager, this can take some time  ...
Starting Enterprise Manager. This operation can take some time. Do not interrupt
this command while it is running.
OMS Started Successfully
BI Publisher server named :BIP: running at https://em.example.com:9702/xmlpserver.
Registering BI Publisher with Enterprise Manager and deploying reports...
Performing automatic backup of Enterprise Manager.
Successfully backed up Enterprise Manager.
Successfully setup BI Publisher with Enterprise Manager
```

## 14.4 Upgrade Configuration of BI Publisher from an Old BI Publisher Home to a New BI Publisher under the 12.1.0.4/12.1.0.5 Middleware Home

**Note:** If you are upgrading from Enterprise Manager 12.1.0.4, and multiple BI Publisher Servers were configured, this upgrade process only configures and upgrades the primary BI Publisher server. After the primary BI Publisher is configured, It is necessary to re-configure the additional BI Publisher Servers, on OMS2, OMS3, etc. Follow the instructions in Chapter 20, "Running Multiple BI Publisher Servers." Please note that the existing shared storage, from the prior release of Enterprise Manager, will continue to be used. Therefore, insure that this shared storage is mounted and available on all of the Enterprise Manager systems that host a OMS.

**IMPORTANT:** **Stop the BI Publisher server before upgrading.** Before beginning the Enterprise Manager upgrade process, you will have stopped the BI Publisher server process using the WLS console. If this has not been performed, then you must use manual system commands to gracefully terminate the BI Publisher server process. For example, on Unix, use the 'kill' command (without the '-9' argument).

The following steps are performed for a upgrade configuration of BI Publisher in Enterprise Manager Release 4 (12.1.0.4) or Release 5 (12.1.0.5). There script executes two major functions:

- **Step 1** - Command invocation and credential gathering

- **Step 2** - The upgrade of the BI Publisher database schema, which is named SYSMAN_BIPLATFORM. This is accomplished using the Oracle Patch Set Assistant (PSA)
- **Step 3** - The WebLogic domain that contains Enterprise Manager is extend to include BI Publisher, and BI Publisher is configured.

From the OMS instance's `ORACLE_HOME/oms/bin` directory (of the current Enterprise Manager 12*c* Release 4 (12.1.0.4) or Release 5 (12.1.0.5) installation), execute the *configureBIP* script with the *-upgrade* command-line argument. For example:

```
cd /oracle/middleware/oms/bin
configureBIP -upgrade
```

**Optional:** If you do not wish the script to execute step 6 below (the migration of reports and certain configuration data) then an optional command-line argument can be provided. In this situation, you can run configureBIP using the following syntax:

```
configureBIP -upgrade -nomigrate
```

1. The script prompts for the necessary credentials.
2. The script prompts for the full directory path to the domain of the prior Enterprise Manager 12c installation. This installation already contains the BI Publisher report definitions and certain configuration data.
3. The script then executes the Patch Set Assistant (PSA) steps to upgrade the BI Publisher database schema, since this is an upgrade from a prior release of the BI Publisher.
4. The script prompts for the two required inputs for the port(s) to use for the BI Publisher Managed Server. One port for non-SSL and one for SSL.
5. The script then performs the extend-domain and configuration of the new BI Publisher.The BI Publisher Managed Server is not started in this step.
6. The script migrates the reports and certain configuration data from the prior installation of BI Publisher, if needed, that was installed onto the prior release of Enterprise Manager 12c.
7. The script then starts the BI Publisher Managed Server.
8. Enterprise Manager, including BI Publisher, will be set to the same "Lock" mode as it was prior to running configureBIP. This is done via the command "emctl secure {lock | unlock}.
9. Enterprise Manager is stopped and then started, including BI Publisher
10. The Enterprise Manager-supplied BI Publisher Reports are deployed to the newly installed BI Publisher Web application.
11. The Enterprise Manager WebLogic domain target is refreshed to include the newly added BI Publisher targets.
12. The Enterprise Manager-supplied BI Publisher Reports are deployed to the newly installed BI Publisher Web application.
13. The final step performs a backup of Enterprise Manager using the "`emctl exportconfig oms`" command.

**Note:** During an upgrade of BI Publisher 11.1.1.6.0 onto Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5), the existing BI Publisher schema will be upgraded from the prior version to 11.1.1.7.0. This means that when performing an upgrade, all existing BI Publisher schedules will be carried over to the new installation of BI Publisher.

### Step 1 - Command invocation and credential gathering

Step 1 generates the following output.

```
Configuring BI Publisher Version "11.1.1.7.0" to work with Enterprise Manager
Logging started at /oracle/work/middleware/oms/cfgtoollogs/bip/bipca_
20140227144257.log.
This command is meant to be run from Oracle Enterprise Manager Cloud Control 12c
Release 4. Please confirm? (Y|N):y
Before this command is run, a backup of Enterprise Manager should be performed
using the :emctl exportconfig oms: command. Have you made a valid backup of
Enterprise Manager (yes/no) [no] ? yes
Enter sysdba user name (sys):
Enter sysdba user password:
Enter Administration Server user password:
Enter the fully qualified path to the domain you are upgrading from:
/oracle/EM12cR3/gc_inst/user_projects/domains/GCDomain
Upgrading from a prior release of BI Publisher With a file-system repository
Located at: //oracle/EM12cR3/gc_inst/user_projects/domain/GCDomain
Configuring BI Publisher in Oracle Home located in /oracle/work/middleware/Oracle_
BI1 ...
```

### Step 2 - The upgrade of the BI Publisher database schema

The schema is named SYSMAN_BIPLATFORM. This operation is performed using the Oracle Patch Set Assistant (PSA).

The patch set assistant runs to upgrade the BI Publisher schema. Output similar to the following will be generated.

```
EM 12c BIPLATFORMversion 11.1.1.6.0  schema detected. Begin upgrade process to
version 11.1.1.7.0
Begin to execute Oracle Fusion Middleware Patch Set Assistant (PSA) ...
PSA returns with status: 0
Successfully upgraded SYSMAN_BIPLATFORM schema...
```

### Step 3 - The WebLogic domain that contains Enterprise Manager is extend to include BI Publisher, and BI Publisher is configured.

Successful operation of the script generates screen output similar to the following:

```
Enter an integer between 9701 and 49152 for the BI Publisher HTTP server port.
(9701):
Enter an integer between 9713 and 49152 for the BI Publisher HTTPS server port.
(9702)):
Extending domain with BI Publisher. This operations can take some time. Do not
interrupt this command while it is running...
Migrating BI Publisher Filesystem repository from "/ /oracle/EM12cR3/user_
projects/domains/GCDomain/config/bipublisher/repository" to "/oracle/gc_inst/user_
projects/domains/GCDomain/config/bipublisher/repository"...
Starting the Upgraded BI Publisher Managed Server...
Locking Enterprise Manager ...
OMS Console is locked. Access the console over HTTPS ports.
Restart OMS.
```

```
Restarting Enterprise Manager ...
Stopping Enterprise Manager, this can take some time  ...
Starting Enterprise Manager. This operation can take some time. Do not interrupt
this command while it is running.
OMS Started Successfully
BI Publisher server named :BIP: running at
https://slc03sag.example.com:9702/xmlpserver.
Registering BI Publisher with Enterprise Manager and deploying reports...
Performing automatic backup of Enterprise Manager.
Successfully backed up Enterprise Manager.
Successfully setup BI Publisher with Enterprise Manager
```

## 14.5 Verifying Integration of BI Publisher with Enterprise Manager

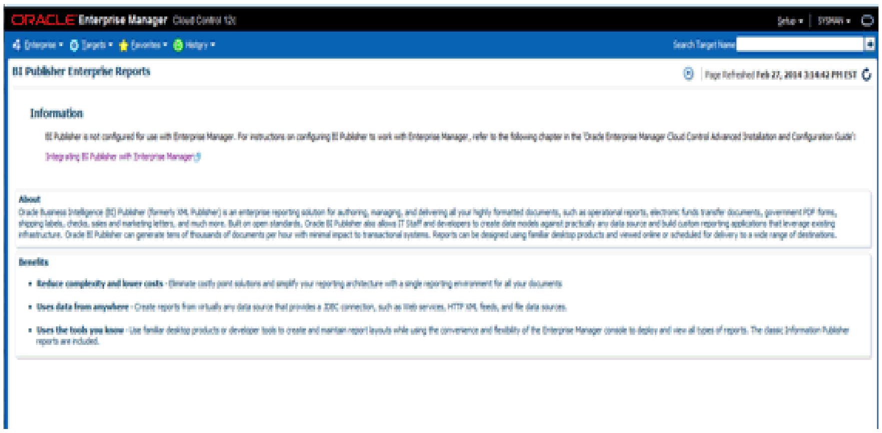
**Note:** If you are running Enterprise Manager in a High Availability environment (behind a Server Load Balancer (SLB)) be aware of the following:

- If the first BI Publisher server has been configured on the primary OMS system, it is necessary to configure BI Publisher on all other Enterprise Manager systems that reside behind the Server Load Balancer.
- If an Enterprise Manager system has a running OMS, and the corresponding BI Publisher server is not configured, or is not running, then running BI Publisher reports from Enterprise Manager will fail some of the time. In this situation, configure BI Publisher on the additional Enterprise Manager systems. If BI Publisher is already configured on an additional system, bring it up using the Enterprise Manager command line utility (EMCTL).
- For details on configuring multiple BI Publisher servers, see Chapter 20, "Running Multiple BI Publisher Servers.".

Verification can be performed in either fresh configuration mode or upgrade configuration mode.

1. Log in to Enterprise Manager as a Super Administrator.
2. From the **Enterprise** menu, select **Reports** and then **BI Publisher Enterprise Reports**.

   Prior to BI Publisher being integrated with Enterprise Manager, the BI Publisher Reports page appears as follows:



BI Publisher Enterprise Reports

Page Refreshed Feb 27, 2014 3:14:42 PM EST

Information

BI Publisher is not configured for use with Enterprise Manager. For instructions on configuring BI Publisher to work with Enterprise Manager, refer to the following chapter in the 'Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide':

Integrating BI Publisher with Enterprise Manager

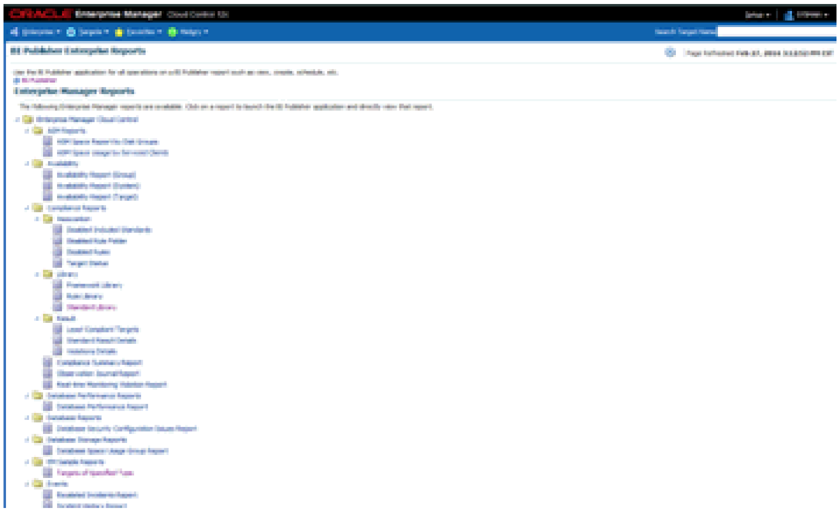
About

Oracle Business Intelligence (BI) Publisher (formerly XML Publisher) is an enterprise reporting solution for authoring, managing, and delivering all your highly formatted documents, such as operational reports, electronic funds transfer documents, government PDF forms, shipping labels, checks, sales and marketing letters, and much more. Built on open standards, Oracle BI Publisher also allows IT Staff and developers to create data models against practically any data source and build custom reporting applications that leverage existing infrastructure. Oracle BI Publisher can generate tens of thousands of documents per hour with minimal impact to transactional systems. Reports can be designed using familiar desktop products and viewed online or scheduled for delivery to a wide range of destinations.

Benefits

- **Reduce complexity and lower costs** - Eliminate costly point solutions and simplify your reporting architecture with a single reporting environment for all your documents
- **Uses data from anywhere** - Create reports from virtually any data source that provides a JDBC connection, such as Web services, HTTP XML feeds, and file data sources.
- **Uses the tools you know** - Use familiar desktop products or developer tools to create and maintain report layouts while using the convenience and flexibility of the Enterprise Manager console to deploy and view all types of reports. The classic Information Publisher reports are included.

3. After BI Publisher is configured, this same page will display a tree list showing all of the Enterprise Manager-supplied BI Publisher reports, as shown in the following graphic.



BI Publisher Enterprise Reports

Page Refreshed Feb 27, 2014 3:32:50 PM EST

Use the BI Publisher application for all operations on a BI Publisher report such as view, create, schedule, etc.

BI Publisher

Enterprise Manager Reports

The following Enterprise Manager reports are available. Click on a report to launch the BI Publisher application and directly view that report.

- Enterprise Manager Cloud Control
  - ASM Reports
    - ASM Space Report for Disk Groups
    - ASM Space Usage for Serviced Clients
  - Availability
    - Availability Report (Group)
    - Availability Report (System)
    - Availability Report (Target)
  - Compliance Reports
    - Association
      - Disabled Included Standards
      - Disabled Rule Folder
      - Disabled Rules
      - Target Status
    - Library
      - Framework Library
      - Rules library
      - Standard Library
    - Result
      - Least Compliant Targets
      - Standard Result Details
      - Violations Details
    - Compliance Summary Report
    - Observation Journal Report
    - Real-time Monitoring Violation Report
  - Database Performance Reports
    - Database Performance Report
  - Database Reports
    - Database Security Configuration Issues Report
  - Database Storage Reports
    - Database Space Usage Group Report
  - EM Sample Reports
    - Targets of Specified Type
  - Events
    - Escalated Incidents Report
    - Incident History Report

This graphic shows the list of reports after all plug-ins have been installed. The report list will vary in size depending on the number of plug-ins that have been installed.

4. Click on the provided **EM Sample Reports** and the select **Targets of Specified Type**.

5. Log in to BI Publisher using your Enterprise Manager credentials.

6. You will see the sample report rendered on the screen. You can then use the full capabilities of BI Publisher such as PDF report generation and e-mail delivery.

## 14.6 Allowing Access to BI Publisher for Enterprise Manager Administrators

BI Publisher shares the same security model, via WebLogic, that Enterprise Manager is configured to use. The security model is used both for authenticating access to BI Publisher, and also setting up access to different features of BI Publisher. The items to be discussed in the following sections are:

- Enterprise Manager Authentication Security Model

- BI Publisher Security Model
- BI Publisher Permissions
- BI Publisher OPSS Application Roles
- Authenticating and limiting access BI Publisher features

### 14.6.1 Enterprise Manager Authentication Security Model

Once integrated, BI Publisher Reports conform to the Enterprise Manager authentication security model. Enterprise Manager supports a variety of security models, as defined in the Oracle® Enterprise Manager Security Guide.

To summarize, the security models that Enterprise Manager 12c supports are:

1. Repository-based Authentication
2. Enterprise User Security Based  (EUS) Authentication
3. Oracle Access Manager (OAM) SSO
4. Oracle Single-sign-on (OSSO) -Based Authentication
5. LDAP Authentication Options: Oracle Internet Directory and Microsoft Active Directory

### 14.6.2 BI Publisher Security Model

When BI Publisher is integrated with Enterprise Manager, it shares the same security model as Enterprise Manager.

Security Model 1 - Repository-Based authentication, uses the Oracle database for authentication.

Security Model 2, Enterprise User Security Authentication (EUS), uses the Oracle database for authentication. In this security configuration, the Oracle database delegates authentication to an LDAP server. However, this LDAP server is not directly accessed by WebLogic, and therefore BI Publisher does not have direct access to the LDAP server.

The remaining three security models use an underlying LDAP server, which is accessed directly by WebLogic, to authenticate users.

For the purposes of this document, we classify the BI Publisher security model into one of these two categories:

1. Repository-Based Authentication
2. Underlying LDAP-based Authentication

> **Note:** When the BI Publisher security model is configured to use Underlying LDAP-based Authentication, no additional BI Publisher-specific configuration is required. For example, you do not need to access the BI Publisher Administration screen and change the security model to LDAP. Because Enterprise Manager and BI Publisher are configured in the same WebLogic domain, they automatically share the same security and authentication mechanisms.

> **IMPORTANT:** If Enterprise Manager was previously configured to use an LDAP or SSO server, these LDAP or SSO configuration steps will have to be repeated. This is required to incorporate required BI Publisher configuration details.

The primary security attributes that apply to BI Publisher Reports are:

- BI Publisher Permissions
- BI Publisher OPSS Application Roles

Each of these security attributes is detailed in the following sections.

### 14.6.3 BI Publisher Permissions

Enterprise Manager ships with certain Oracle-provided BI Publisher catalog objects. These catalog objects consist of:

- Folders
- Reports (layout definitions and translations)
- Datamodels (SQL queries against the Enterprise Manager repository)
- Sub-templates (standard Enterprise Manager header shown above all pages of all report output)

These catalog objects are created when BI Publisher is installed and integrated with Enterprise Manager. They are placed in the "Enterprise Manager Cloud Control" folder. These catalog objects are created with certain permissions that, combined with the roles/groups discussed below, achieve the desired security model.

### 14.6.4 BI Publisher OPSS Application Roles

The domain policy store (OPSS) is used to control Enterprise Manager administrator access to objects in the BI Publisher catalog and conditional access to the BI Publisher "Administration" button.

OPSS is the repository of system and application-specific policies. Details regarding OPSS can be found in the Oracle® Fusion Middleware Application Security Guide. In a given domain, there is one store that stores all policies (and credentials) that all applications deployed in the domain may use. As both Enterprise Manager and BI Publisher are separate applications in the same domain, it is necessary to grant specific BI Publisher OPSS application roles to Enterprise Manager administrators in order for them to access and use BI Publisher.

When BI Publisher is installed, four OPSS application roles are created. These four OPSS application roles are combined with the permissions on the BI Publisher catalog objects in the "Enterprise Manager Cloud Control Folder" to achieve the rules shown in the following sections. In addition, when the underlying LDAP authentication security model is used, the LDAP groups can be mapped to these OPSS application roles.

In the Repository-based authentication security model, the domain policy store (OPSS) is used solely to control Enterprise Manager administrator's access to BI Publisher.

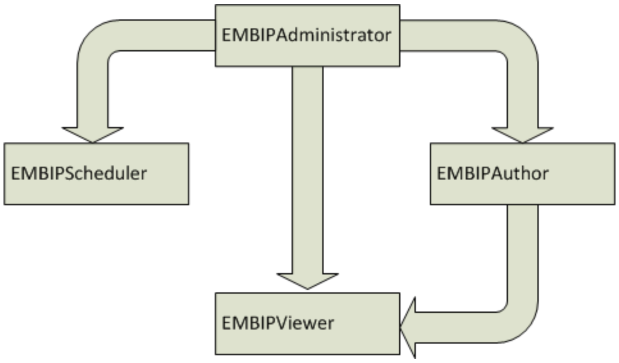
### 14.6.5 Authenticating and limiting access BI Publisher features

Below is a list of the OPSS application roles, and a description of the effective security model placed on BI Publisher catalog objects that ship with Enterprise Manager.

- *None* - Enterprise Manager administrators without any BI Publisher role can access BI Publisher Reports via any delivery channel that BI Publisher supports, and that has been configured and made accessible the BI Publisher System Administrator. For example, any user can receive BI Publisher Reports via the BI Publisher scheduling and e-Mail delivery mechanism, if configured.
- **EMBIPViewer** - Enterprise Manager administrators with this BI Publisher role can receive e-mails plus can view the Enterprise Manager-supplied BI Publisher reports.
- **EMBIPScheduler** - Enterprise Manager administrators with this BI Publisher role can receive e-mails and can schedule the Enterprise Manager-supplied BI Publisher reports if they also have the **EMBIPViewer** role.
- **EMBIPAuthor** - Enterprise Manager administrators with this BI Publisher role can receive e-mails, view the Enterprise Manager-supplied BI Publisher reports, and can create new reports in their private folder. They can also copy the Enterprise Manager-supplied BI Publisher reports into their private folder and customize them.
- **EMBIPAdministrator** (Super Users) - Enterprise Manager administrators with this BI Publisher role have complete access to BI Publisher.

The following diagram shows the hierarchy of the above roles:

**Note:** Access to the BI Publisher "Administration" button is granted via the OPSS application role. This button is used to perform advanced configuration on BI Publisher, such as setting up the e-mail server.



#### Enterprise Manager Super Administrators

When the repository-based authentication security model is used, all Enterprise Manager Super Administrators are automatically granted the **EMBIPAdministrator** OPSS application role to facilitate setting up BI Publisher.

When an underlying LDAP authentication security model is used, Enterprise Manager Super Administrators are not automatically granted EMBIPAdministrator access to BI Publisher. See Section 16.x for more information on allowing access to BI Publisher for

Enterprise Manager Administrators in an underlying LDAP-based Authentication security Model environment.

## 14.7 Limiting access to BI Publisher features

Granting the previously discussed four OPSS application roles is somewhat different depending on the BI Publisher security model that is in place. To review, the 2 security models that BI Publisher supports are:

- Repository-Based Authentication
- Underlying LDAP-based Authentication

### 14.7.1 Granting BI Publisher OPSS Application Roles to Enterprise Manager Administrators in Repository-Based Authentication Mode Using wlst

An EM CLI command can be used to grant one or more OPSS application roles to Enterprise Manager administrator(s). The following usage example demonstrates using EM CLI to grant VIEW and AUTHOR access to the Enterprise Manager administrators named "JERRY" and "LESLIE".

> **Note:** Even though Enterprise User Security (EUS) uses an LDAP server for user authentication, this is handled strictly by the database. Therefore, this section also applies when using EUS.

To run the script:

1. Connect the Enterprise Manager EM CLI to Enterprise Manager
2. Run `emcli grant_bipublisher_roles` to grant access to BI Publisher for Enterprise Manager user(s).

#### Example Session

```
$ emcli login -username=sysman
Enter password :
Login successful
$ emcli sync
Synchronized successfully
$ emcli grant_bipublisher_roles  -roles="EMBIPViewer;EMBIPAuthor"
-users="JERRY;LELSIE"
EMBIPViewer role successfully granted to JERRY
EMBIPViewer role successfully granted to LESLIE
EMBIPAuthor role successfully granted to JERRY
EMBIPAuthor role successfully granted to LESLIE
```

#### Revoking VIEW Access to BI Publisher Reports

In the following example session you revoke VIEW access to BI Publisher reports from user "JERRY".

```
$ emcli login -username=sysman
Enter password :
Login successful
$ emcli sync
Synchronized successfully
$ emcli revoke_bipublisher_roles -roles="EMBIPViewer" -users=JERRY
EMBIPViewer role successfully revoked from JERRY
```

### 14.7.2 Propagation Time for Changes to OPSS

When changing an Enterprise Manager administrator's BI Publisher access privileges (**EMBIPViewer**, **EMBIPAdministrator**, **EMBIPScheduler**, **EMBIPAuthor**) the Super Administrator needs to wait 15 or more minutes for the changes to propagate through OPSS and become effective. The change will then be effective the next time the administrator logs into BI Publisher.

## 14.8 Allowing Access to BI Publisher for Enterprise Manager Administrators in an Underlying LDAP Authentication Security Environment

Enterprise Manager and BI Publisher are separate applications. When using an underlying LDAP-based authentication model (except for Enterprise User Security (EUS)), LDAP groups defined in the external LDAP server can also be used to manage access to BI Publisher. These LDAP groups allow varying levels of access to BI Publisher. Hence, you can add an LDAP user as a member of one or more of these LDAP group and appropriate capabilities of BI Publisher will be exposed. These LDAP groups, which either need to be created or existing ones used, are coordinated with the permissions of the catalog object in the "Enterprise Manager Cloud Control" folder.

**Note:** This section does not apply when Enterprise Manager is configured to use Enterprise User Security (EUS). See Section 14.7.1, "Granting BI Publisher OPSS Application Roles to Enterprise Manager Administrators in Repository-Based Authentication Mode Using wlst."

**Note:** Because BI Publisher and Enterprise Manager are configured within the same WebLogic domain, it is not necessary to perform any specific LDAP configuration in the BI Publisher application. The following steps are sufficient to configure LDAP.

In an underlying LDAP-based authentication security model, the following steps are required:

- The administrator of the LDAP server needs to use four external groups of any chosen name. These groups need to be grouped hierarchically. Existing groups can be used, or new ones can be created.

  **Important:** The group names must be all upper-case.

  Group Name Examples:

  - EMBIPADMINISTRATOR
  - EMBIPVIEWER
  - EMBIPSCHEDULER
  - EMBIPAUTHOR

- The administrator of the LDAP server must then make the additional changes below in order to achieve the necessary hierarchical structure shown in the hierarchy diagram above. For example, using the sample LDAP group names above:

Make EMBIPADMINISTRATOR a member of EMBIPAUTHOR

Make EMBIPADMINISTRATOR a member of EMBIPSCHEDULER

Make EMBIPAUTHOR a member of EMBIPVIEWER

**Note:** In LDAP, the terminology and concepts can seem backwards and confusing. For example, you want the EMBIPAUTHORS group to have as a member the EMBIPADMINISTRATORS group.

Then, in order to grant access to BI Publisher and its catalog objects, the administrator of the LDAP server needs to make respective LDAP users a members of one or more of the above LDAP groups.

### 14.8.1 Mapping LDAP Groups to BI Publisher OPSS Application Roles

In order to map the four LDAP groups to the OPSS application roles described above, the LDAP groups need to be mapped using EM CLI.

**Note:** If you have just upgraded to BI Publisher 11.1.1.7.0 on Enterprise Manager 12c Release 4 (12.1.0.4) or Release 5 (12.1.0.5) from a prior installation of BI Publisher on Enterprise Manager 12c and the names of your LDAP groups have not changed, this step is not necessary, as the prior OPSS application grants are carried over to the new installation.

**Example Session**

```
emcli grant_bipublisher_roles -roles="EMBIPViewer" -external_role="EMBIPVIEWER"
EMBIPViewer successfully granted to EMBIPVIEWER
emcli grant_bipublisher_roles -roles="EMBIPAuthor" -external_role="EMBIPAUTHOR"
EMBIPAuthor successfully granted to EMBIPAUTHOR
emcli grant_bipublisher_roles -roles="EMBIPScheduler" -external_
role="EMBIPSCHEDULER"
EMBIPScheduler successfully granted to EMBIPSCHEDULER
emcli grant_bipublisher_roles -roles="EMBIPAdministrator" -external_
role="EMBIPADMINISTRATOR"
EMBIPAdministator successfully granted to EMBIPADMINISTRATOR
```

## 14.9 Securing BI Publisher with a Secure Socket Layer (SSL) Certificate

The BI Publisher WebLog Server is configured with a default identity keystore ( DemoIdentity.jks) and a default trust keystore ( DemoTrust.jks). In addition, WebLogic Server trusts the CA certificates in the JDK cacerts file. This default keystore configuration is appropriate for testing and development purposes. However, these keystores should not be used in a production environment.

If Enterprise Manager has previously been secured with an SSL certificate, using the `emctl secure wls` command, this command will need to be re-issued once BI Publisher has been configured. See the Enterprise Manager Administrator's guide for more information on how these commands are used.

## 14.10 BI Publisher Administration

Please refer to the BI Publisher documentation for instructions on configuring BI Publisher settings.

Common administrative tasks:

- Configuring server properties, such as e-mail servers.
- Configuring report delivery channels, such as FTP.

## 14.11 Post-Configuration Steps to take after Configuring BI Publisher

Installing Plug-in-Specific Reports

Some Enterprise Manager-provided BI Publisher reports belong to specific plug-ins. These plug-ins must be installed in order for these reports to be available. A plug-in can be installed before or after BI Publisher is configured to work with Enterprise Manager 12c. Enterprise Manager plug-ins can be installed using different mechanisms. All of these mechanisms support the installation of BI Publisher reports that are part of a plug-in.

**Note:** Refer to the *Oracle Enterprise Manager Basic Installation Guide* for complete installation specifics.

If a Enterprise Manager plug-in was installed prior to BI Publisher being configured, it is necessary to deploy these new BI Publisher reports from Enterprise Manager to BI Publisher. The following command can be used for this purpose:

```
emcli deploy_bipublisher_reports
```

For complete usage and examples using this command, execute the following:

```
emcli help deploy_bipublisher_reports
```

## 14.12 EMBIP* Roles: Granting Access to Folders and Catalog Objects

By default, the shipping security model (as described in Section 14.6.5, applies to BI Publisher catalog objects that are inside the "Enterprise Manager Cloud Control" folder. This is due to the fact that the catalog objects that exist in this folder are set up with a default set of permissions. See Section 14.6.3. BI Publisher catalog objects that are outside of this folder will not automatically contain these same permissions. For example, BI Publisher ships with numerous reports in a shared folder called "Samples". If it is desired to grant access to this folder to Enterprise Manager/BI Publisher users, other than EMBIPAdministrator, it is necessary for a BI Publisher super administrator (EMBIPAdministrator) to change the permissions of this folder. They do so by selecting the folder "Samples" and choosing "Permissions" in the bottom left task bar. They then need to add the four privileges (EMBIPAdministrator, EMBIPViewer, EMBIPAuthor, EMBIPScheduler) and grant appropriate access to that privilege such as VIEW report, run report online, to EMBIPViewer. The administrator can model the appropriate privileges to grant based on any of the shipping Enterprise Manager reports (for example, *Targets of Specified Type*).

Individual users, who have the EMBIPAuthor OPSS application role, can develop reports in their own private folders. These reports will not be available to other users.

**Note:** The shared folder "Enterprise Manager Cloud Control" contains Enterprise Manager-provided BI Publisher Reports and is reserved for such. No custom-developed reports may be added to this folder hierarchy. The default security model that ships with Enterprise Manager specifically prohibits this.

**Note:** Only reports in the "Enterprise Manager Cloud Control" folder will show up in the Enterprise Manager BI Publisher Enterprise Reports menu (From the **Enterprise** menu, select **Reports**, and then **BI Publisher Enterprise Reports**).

If a BI Publisher administrator (EMBIPAdministrator) wishes to create a new shared folder outside of the "Enterprise Manager Cloud Control" folder, they can do so. These reports would not show up in the Enterprise Manager BI Publisher reports menu but would be available to other Enterprise Manager administrators as long as appropriate permissions are granted as previously described.

## 14.13 Access to Enterprise Manager Repository

All BI Publisher reports are granted read-only access to the Enterprise Manager Repository. This access is via the BI Publisher data source named **EMREPOS**. This access is via the Enterprise Manager user **MGMT_VIEW**, which is a special internal Enterprise Manager user who has read-only access to the Enterprise Manager Published **MGMT$** database views. In addition, when reports are run, they are further restricted to the target-level security of the user running the report. For example, if user JOE has target-level access to "hostabc" and "database3", when user JOE runs a BI Publisher report (any report) he can only view target-level data associated with these two targets.

## 14.14 Troubleshooting

The following sections provide common strategies that can be used if problems occur with the Enterprise Manager/BI Publisher integration.

### 14.14.1 Rerunning configureBIP

It is sometimes necessary to rerun configureBIP, either during a fresh BI Publisher configuration, or during an upgrade BI Publisher configuration.Before running to re-run the configureBIP command, stop BI Publisher using this command:

```
emctl stop oms -bip_only
```

### 14.14.2 BI Publisher Log File Locations

The following log files can be used to trace problems to their point of origin.

#### 14.14.2.1 configureBIP Log Files

Location: `ORACLE_HOME(oms)/cfgtoollogs/bip/*`

- Creating/upgrading the BI Publisher schema in the database
  - "emBIPLATFORM.log

  - "emBIPLATFORMcreate_<date>.log
  - "biplatform.log
  - "emBIPLATFORMcreate.err
- Extending the Enterprise Manager domain with BI Publisher
  - bipca_<date>.log

#### 14.14.2.2 Enterprise Manager BI Publisher Tree and EM CLI Log File Output

emoms.trc

emoms.log

Messages specific to the BI Publisher integration can be found by searching for "BIP" (all caps) in the log files.

#### 14.14.2.3 BI Publisher Runtime

Location: Domain home. For example, `gc_inst/user_projects/domains/GCDomain`

- servers/BIP/logs/*
- servers/BIP/logs/bipublisher.log

### 14.14.3 Additional Troubleshooting

If BI Publisher is able to run successfully, but BI Publisher registration with Enterprise Manager fails, you can retry the registration by running:

```
emcli login -username=<admin username> -password=<admin password>
emcli sync
emcli setup_bipublisher -proto=http[s] -host=<bip_host> -port=<bip_port>
-uri=xmlpserver
```

### 14.14.4 Redeploying All Enterprise Manager-Supplied BI Publisher Reports

If a plug-in is installed subsequent to BI Publisher being installed and configured to work with Enterprise Manager, the BI Publisher reports that are part of the plug-in can be deployed from the Enterprise Manager installation to BI Publisher using the following commands:

```
emcli login -username=sysman
Password: <pw>
emcli sync
emcli deploy_bipublisher_reports -force
```

This procedure can also be used to restore reports on BI Publisher if they become damaged.

### 14.14.5 Enabling BI Publisher Debugging

When troubleshooting BI Publisher, there may be situations that require detailed BI Publisher debugging information to resolve the issues. You can enable BIP debugging using the WebLogic Scripting Tool (WLST). When debugging is enabled, detailed diagnostic and error information will be sent to the standard locations discussed previously, such as *bipublisher.log*. The following procedure steps you through turning on debugging for the primary BI Publisher server.

> **Note:** In the following command examples, *BIP* is the name of the primary BI Publisher server. If there are multiple BI Publisher servers that require debugging, replace the *BIP* with the individual server names such as *BIP2* or *BIP3*

Once you have finished debugging BI Publisher, be sure to turn off debugging.

#### 14.14.5.1 Turning on BI Publisher Debugging

1. Before running WLST, set WLST environment properties so that the WebLogic Server trusts the CA certificates in the demonstration trust keystore.

   **Linux sh/bash**:

   ```
   export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=DemoTrust"
   ```

   **Linux csh/tcsh:**

   ```
   setenv WLST_PROPERTIES "-Dweblogic.security.TrustKeyStore=DemoTrust"
   ```

   **Windows:**

   ```
   set WLST_PROPERTIES=-Dweblogic.security.TrustKeyStore=DemoTrust
   ```

2. Connect to WLST.

   **Linux**:

   ```
   $MW_HOME/oracle_common/common/bin/wlst.sh
   ```

   **Windows**:

   ```
   %MW_HOME%\oracle_common\common\bin\wlst.cmd
   ```

3. Execute the commands shown in the following WLST session example to enable debugging.

   ```
   ...
   ...
   Initializing WebLogic Scripting Tool (WLST) ...
   Welcome to WebLogic Server Administration Scripting Shell
   Type help() for help on available commands
   wls:/offline> connect('weblogic','<pw>','t3s://host:port')
   ...
   ...
   Successfully connected to Admin Server 'EMGC_ADMINSERVER' that belongs to
   domain 'GCDomain'.
   wls:/GCDomain/serverConfig>
   setLogLevel(target='BIP',logger='oracle.xdo',level='TRACE:32')
   wls:/GCDomain/serverConfig> getLogLevel(logger='oracle.xdo',target='BIP')
   TRACE:32
   wls:/GCDomain/serverConfig> exit()
   ```

#### 14.14.5.2 Turning Off BI Publisher Debugging

Once you have finished debugging BI Publisher, you must reset the log-level back to the default setting.

1. Connect to WLST.

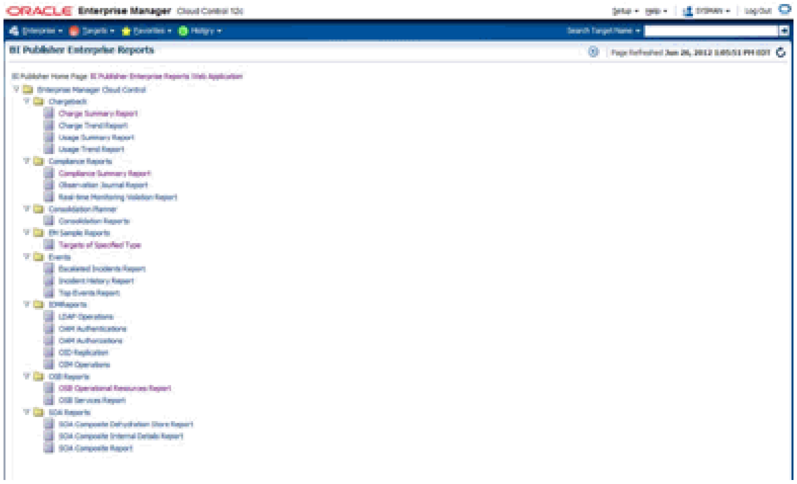
2. Execute the commands shown in the following WLST session example to disable debugging.

   ```
   wls:/offline> connect('weblogic','<pw>','t3s://host:port')
   ```

```
...
...
Successfully connected to Admin Server 'EMGC_ADMINSERVER' that belongs to
domain 'GCDomain'.
wls:/GCDomain/serverConfig>
setLogLevel(target='BIP',logger='oracle.xdo',level=' 'WARNING:1')
wls:/GCDomain/serverConfig> getLogLevel(logger='oracle.xdo',target='BIP')
'WARNING:1'
```

## 14.15 Managing Enterprise Manager - BI Publisher Connection Credentials

Accessing BI Publisher from Enterprise Manager requires a direct connection between the two products in order to retrieve, display, and manage report definitions. Example: From the **Enterprise** menu, choose **Reports** and then **BI Publisher Enterprise Reports**. A tree view displaying BI Publisher reports within the Enterprise Manager Cloud Control shared folder appears as shown in the following graphic.



ORACLE Enterprise Manager Cloud Control 12c
Enterprise
Targets
Favorites
History
BI Publisher Enterprise Reports
BI Publisher Home Page BI Publisher Enterprise Reports Web Application
Enterprise Manager Cloud Control
Chargeback
Charge Summary Report
Charge Trend Report
Usage Summary Report
Usage Trend Report
Compliance Reports
Compliance Summary Report
Observation Journal Report
Real-time Monitoring Violation Report
Consolidation Planner
Consolidation Reports
EM Sample Reports
Targets of Specified Type
Events
Escalated Incidents Report
Incident History Report
Top Events Report
IDMReports
LDAP Operations
OAM Authentications
OAM Authorizations
OID Replication
OIM Operations
OSB Reports
OSB Operational Resources Report
OSB Services Report
SOA Reports
SOA Composite Dehydration Store Report
SOA Composite Internal Details Report
SOA Composite Report

The first time you run the `configureBIP` script to configure BI Publisher to integrate with Enterprise Manager, a dedicated WebLogic user is automatically created with the requisite credentials solely for the purpose of installation/configuration. Beginning with Enterprise Manager 12*c* Cloud Control release 12.1.0.1, you can configure these credentials using the EMCTL command `config oms`.

### Verb Syntax

```
emctl config oms -store_embipws_creds [-admin_pwd <weblogic_pwd>] [-embipws_user
<new_embipws_username>] [-embipws_pwd <new_embipws_pwd>]
```

The `config oms` command allows you to change the password, and optionally the username, used by Enterprise Manager to access the installed BI Publisher Web Server. Running the `config oms` command requires the WebLogic Admin user's password.

**Note 1:** The `config oms` command only changes the user credentials required for the Enterprise Manager - BI Publisher connection. The Enterprise Manager - BI Publisher connection credentials should match the credentials used elsewhere by the user. Example: Enterprise Manager users (database authentication), LDAP users, and WebLogic Server users. Use the corresponding application/console to create or manage the user within the installed credential store.

**Note 2:** This command is operational only if BI Publisher has been installed.

**Note 3:** It is not necessary to restart any managed server, such as EMGC_OMS*nnnn* or BIP*nnnn*.

Any valid credential that WebLogic supports is acceptable as long as that user also has the *EMBIPAdministrators* privilege (either in OPSS or LDAP, as appropriate).

**Example:** You have configured Enterprise Manager to use single sign-on (SSO) (backed by an LDAP credential store). The following steps illustrate the credential update process:

1. Create the LDAP user. Example: Create EM_BIP_INTERNAL_USER and assign this LDAP user a password such as XYZ123.
2. Make EM_BIP_INTERNAL_USER a member of the EMBIPADMINISTRATORS LDAP group. For more information about LDAP groups and Enterprise Manager-BI Publisher integration, see Section 14.8, "Allowing Access to BI Publisher for Enterprise Manager Administrators in an Underlying LDAP Authentication Security Environment".
3. Execute the EMCTL `config oms` command:

   ```
   emctl config oms -store_embipws_creds -embipws_user EM_BIP_INTERNAL_USER
   Oracle Enterprise Manager Cloud Control 12c Release 2
   Copyright (c) 1996, 2012 Oracle Corporation.  All rights reserved.
   Enter Admin User's Password: <pw>
   Enter new password that Enterprise Manager will use to connect to BI Publisher:
   XYZ123
   Successfully updated credentials used by Enterprise Manager to connect to BI
   Publisher.
   ```

   If you later change the EM_BIP_INTERNAL_USER password in the LDAP server, you can change the LDAP user's password by executing the `config oms` command with the `-store_embipws_creds` option. In the following example, the password is changed to *ABC123*.

   ```
   emctl config oms -store_embipws_creds
   Oracle Enterprise Manager Cloud Control 12c Release 2
   Copyright (c) 1996, 2012 Oracle Corporation.  All rights reserved.
   Enter Admin User's Password: <pw>
   Enter new password that Enterprise Manager will use to connect to BI Publisher
   : ABC123
   Successfully updated credentials used by Enterprise Manager to connect to BI
   Publisher.
   ```

## 14.16 Managing the BI Publisher Server

BI Publisher operates as a separate, managed server in the same WebLogic domain that contains the OMS(s) and the AdminServer. After BI Publisher is configured, the Enterprise Manager `emctl` command can now be used to also manage BI Publisher.

### Usage Examples:

```
emctl start oms
  Starts the Oracle Application Server components required
```

```
  to run the Management Service application.
  Specifically, this command starts the Oracle HTTP Server,
  Oracle Management Service, BI Publisher server and
  applications associated with it.

emctl start oms -bip_only
  Starts just the BI publisher server.

emctl stop oms [-all] [-force]
  Stops Oracle Management Service.
     -all :  Additionally Stops BI publisher server and
             Admin server
     -force : kills the process instead of gracefull shutdown
              (not recommended)

emctl stop oms -bip_only [-force]
  Stops BI Publisher server only
     -force : kills the process instead of gracefull shutdown
              (not recommended)

emctl status oms
  Displays a message indicating whether Oracle Management
  Service and BI Publisher are running.

emctl status oms -bip_only
  Displays a message indicating whether BI Publisher is
  running.

emctl status oms -details [-sysman_pwd <pwd>]
  Displays status of Oracle Management Service. It displays
  detailed information which includes :
    1) Http and Https upload port for Console and Pbs. and
       respective URL.
    2) Instance Home Location
    3) Oracle Management Service Log directory
    4) Software Load Balancer
    5) Administration Server machine, port and URL
    6) Oracle BI Publisher details
    -sysman_pwd : Enterprise Manager SYSMAN Password. If not
                  provided, you will be prompted for this
```

## 14.17 Using BI Publisher

For comprehensive information on using BI Publisher, see the BI Publisher documentation library.

http://www.oracle.com/technetwork/middleware/bi-publisher/documentation/index.html

## 14.18 Paths to access BI Publisher

Various paths that are used to communicate with BI Publisher. You can obtain the specific paths that are currently configured for your BI Publisher installation using the `emctl status oms -details` command.

**Note:** Corporate firewall configuration may be required to restrict specific TCP/IP ports from being used to access the OMS or BI Publisher.

**Access to BI Publisher via the list of BI Publisher reports** (discussed in a previous section): This is the easiest way to access BI Publisher, and requires no special understanding, for users of Enterprise Manager, on the configuration of the paths discussed below. We call this the *direct channel*. The direct channel is automatically determined using a heuristic algorithm, based on various configuration settings.

**Access from the Oracle Management Server (OMS) to BI Publisher**: The OMS needs to communicate with BI Publisher in order to perform various operations, such as presenting the list of BI Publisher reports, and deploying new reports. We call this the *internal channel*. The internal channel is automatically configured when Enterprise Manager is installed or upgraded. The internal channel can also be manually changed at any time using the `emcli setup_bipublisher` command. See the Enterprise Manager Command Line Interface Guide for more information about this command.

### Communication Channels

- *Direct Channel*: one of the following TCP/IP ports, and communication protocols (HTTP or HTTPS) is used, depending on the method used to access Enterprise Manager, and depending on the Enterprise Manager Authentication Model. The command 'emctl status oms –details' can assist with determining these.
- If Enterprise Manager has been configured for use with a Server Load Balancer, one or both of the following channels is used to access BI Publisher. For further details on the 'emctl secure oms' command and the configuration of a Server Load Balancer for use with Enterprise Manager, see the "Configuring Enterprise Manager for High Availability" section in this guide.
  - Normally, access to BI Publisher is by the Server Load Balancer HTTPS port. This port can be determined using the `emctl status oms -details` command. This port can be reconfigured using the `emctl secure oms` command. This command must be run on each OMS system during a rolling down-time procedure. For example .

    ```
    emctl secure oms -host slb.example.com -slb_console_port 443
    ```

    **Note:** make sure not to provide the argument : `-slb_port` : as this will require re-securing of all Enterprise Manager agents.

  - If Enterprise Manager has been *unlocked* using `emctl secure oms -unlock_console` or `emctl secure unlock`, access to BI Publisher, via the Server Load Balancer port, in HTTP mode is also supported. This channel will be used if Enterprise Manager has been accessed using the Server Load Balancer in insecure mode using HTTP. This only needs to be done on one OMS system, and no down-time is required. For example:

    ```
    $ORACLE_HOME/bin/emctl set property -name
    oracle.sysman.core.eml.ip.bip.gcha.SLBEMBIPConsoleHTTPPort -value 80
    ```

  - Access to BI Publisher via the secure Oracle HTTPS Server Port (OHS). This will be used if Enterprise Manager has been accessed via the OHS HTTPS port, only if a Server Load Balancer is NOT configured.

  - The OHS port will also be used if Enterprise Manager is configured with a Virtual Hostname.
  - If Enterprise Manager has been *unlocked*, access via the Insecure Oracle HTTP Server Port (OHS) is not supported with BIP if a load balancer is also configured.
  - If Enterprise Manager is configured to use Single Sign On, and Enterprise Manager is accessed directly on the OMS WebLogic managed server port, BI Publisher will always be accessed on the secure HTTPS port (thereby bypassing the SSO login screen). This is true regardless of whether Enterprise Manager has been accessed via HTTP or HTTPS mode.

- *Internal Channel*: For Enterprise Manager 12.1.0.4 and 12.1.0.5, all communications via this channel must remain in HTTPS mode and must be made directly to a specific BIP managed server, on a specific Enterprise Manager host, using the WebLogic managed server port.

  For Enterprise Manager 12.1.0.4 and 12.1.0.5, the internal channel cannot use either the SLB nor the OHS port.

  The currently configured internal channel can be determined using the following commands:

  ```
  emcli login -username=sysman
  emcli sync
  emcli unregister_bipublisher
  ```

- *Auxiliary Channel*: If Enterprise Manager has been *unlocked*, access to the BIP WebLogic managed server(s) can occur on the HTTP port for testing purposes.

### Example

The following example demonstrates using `emctl status oms -details` to determine the various channels. The bolded items will help determine the ports used:

```
emctl status oms -details
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host        : emoms1.example.com
HTTP Console Port          : 7788
HTTPS Console Port         : 7799
HTTP Upload Port           : 4889
HTTPS Upload Port          : 4900
EM Instance Home           : /oracle/gc_inst/em/EMGC_OMS1
OMS Log Directory Location : /oracle/gc_inst/em/EMGC_OMS1/sysman/log
SLB or virtual hostname: slb.example.com
HTTPS SLB Upload Port : 4900
HTTPS SLB Console Port : 443
Agent Upload is unlocked.
OMS Console is unlocked.
Active CA ID: 1
Console URL: https://slb.example.com:443/em
Upload URL: https://slb.example.com:4900/empbs/upload

WLS Domain Information
Domain Name            : GCDomain
Admin Server Host      : emoms1.example.com
Admin Server HTTPS Port: 7101
Admin Server is RUNNING
```

```
Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS1
Oracle Management Server Instance Host: emoms1.example.com
WebTier is Up
Oracle Management Server is Down

BI Publisher Server Information
BI Publisher Managed Server Name: BIP
BI Publisher Server is Up

BI Publisher Server named 'BIP' running at URL:
https://slb.example.com:443/xmlpserver
BI Publisher Server Logs: /oracle/gc_inst/user_
projects/domains/GCDomain/servers/BIP/logs/
BI Publisher Log        : /oracle/gc_inst/user_
projects/domains/GCDomain/servers/BIP/logs/bipublisher/bipublisher.log
```

## 14.19 De-installing BI Publisher that was Not Installed Along with Enterprise Manager 12.1.0.5

**IMPORTANT**: Do not proceed with this section until the installation of Enterprise Manager 12.1.0.5 has been completed.

If you have followed this chapter to upgrade BI Publisher from a prior release of Enterprise Manager (12.1.0.2 or 12.1.0.3) to 12.1.0.5, and the prior release of Enterprise Manager also contained BI Publisher 11.1.1.6, you can safely remove the prior installation of the BI Publisher Oracle Home, along with the prior installation of the OMS home. As an Oracle-recommended best practice, you should also delete the Oracle home associated with the prior BI Publisher Oracle home since it consumes a significant amount of disk space.

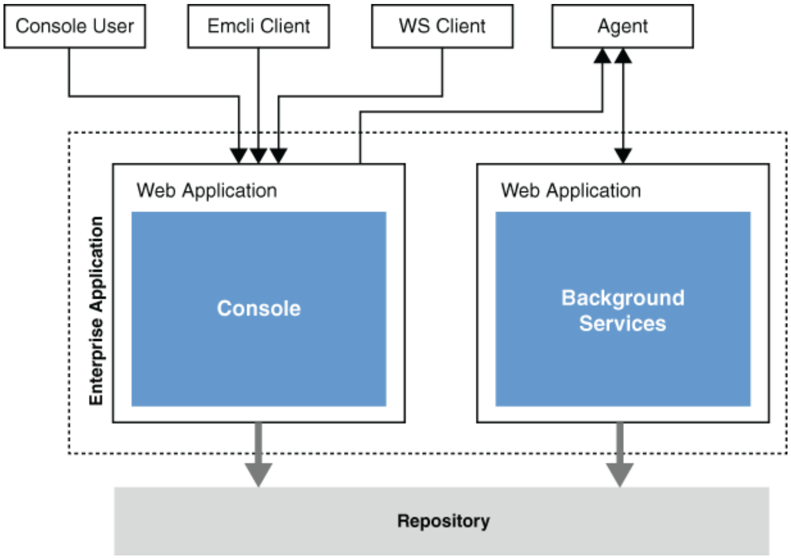
For more information in upgrading Enterprise Manager, when to de-install older Enterprise Manager software, and various de-installation methods, see the *Oracle® Enterprise Manager Cloud Control Upgrade Guide*.

# 15 Running the OMS in Console-Only Mode

Oracle Management Service (OMS) is designed to run two types of services, mainly the console services and the background services. While the console services are required to render a GUI-rich console for Enterprise Manager, the background services are required to run critical jobs, upload operations, business logics, and so on.

Figure 15–1 illustrates the functioning of an OMS where both console services and background services are running.

*Figure 15–1 Functioning of OMS with Active Console and Background Services*



In a multi-OMS environment, if you want to have a dedicated OMS for User Interface (UI) operations or if you do not want to run background services in SSA OMS *(external-facing OMS in a private or public cloud environment)*, then you can choose to shut down the background services and run only the UI services, thus turning the OMS into a pure, console-only mode. In such a case, the Management Agents upload data to other OMS instances where both background services and UI services are running. However, note that you cannot shut down the background services and run only the UI services of an OMS that is deployed in a remote location.

**Note:**

- Only the additional OMS instances can be run in console-only mode, while the OMS instance that shares the host with the Administration Server cannot.
- Only the additional OMS instances of the same location can be run in console-only mode, while the additional OMS in a remote location cannot. For example, if you have four OMS instances in the US and one in Australia, then the OMS in Australia cannot be run in console-only mode.

To run the OMS in console-only mode, follow these steps:

1. Stop the OMS using the following command.

   ```
   $emctl stop oms
   ```

2. Set the start up mode to  console-only, using the following command.

   ```
   $emctl config oms -set_startup_mode console_only
   ```

3. Start the OMS using the following command.

   ```
   $emctl start oms
   ```

To revert the OMS instances to Normal mode, run the following command, and restart the OMS.

```
$emctl config oms -set_startup_mode normal
```

# Part VI

# Configuring Enterprise Manager for High Availability

This section covers Enterprise Manager high availability best practices and strategies that allow you to safeguard your Oracle Enterprise Manager installation.

# 16 High Availability Solutions

Highly Available systems are critical to the success of virtually every business today. It is equally important that the management infrastructure monitoring these mission-critical systems are highly available. The Enterprise Manager Cloud Control architecture is engineered to be scalable and available from the ground up. It is designed to ensure that you concentrate on managing the assets that support your business, while it takes care of meeting your business Service Level Agreements.

When you configure Cloud Control for high availability, your aim is to protect each component of the system, as well as the flow of management data in case of performance or availability problems, such as a failure of a host or a Management Service.

Maximum Availability Architecture (MAA) provides a highly available Enterprise Manager implementation by guarding against failure at each component of Enterprise Manager.

The impacts of failure of the different Enterprise Manager components are:

- Management Agent failure or failure in the communication between Management Agents and Management Service

  Results in targets monitored by the agent no longer being monitored by Enterprise Manager.

- Management Service failure

  Results in downtime for Enterprise Manager.

- Management Repository failure

  Results in downtime for Enterprise Manager.

- Software Library Failure

  Results in a sub-set of Enterprise Manager operations being unavailable. These operations include self-update and provisioning and patching operations including Agent deployment.

Overall, failure in any component of Enterprise Manager can result in substantial service disruption. Therefore it is essential that each component be hardened using a highly available architecture.

> **Note:** For information about setting up a high availability solution for BI Publisher, see Chapter 20, "Running Multiple BI Publisher Servers."

## 16.1 Latest High Availability Information

Because of rapidly changing technology, and the fact that high availability implementations extend beyond the realm of Oracle Enterprise Manager, the following resources should be checked regularly for the latest information on third-party integration with Oracle's high availability solutions (F5 or third-party cluster ware, for example).

- Oracle Maximum Availability Architecture Web site

  HTTP://www.oracle.com/goto/maa

- Enterprise Manager 12c Framework and Infrastructure Web site

  HTTP://www.oracle.com/technetwork/oem/frmwrk-infra-496656.html

## 16.2 Defining High Availability

Oracle Enterprise Manager's flexible, distributed architecture permits a wide range of deployment configurations, allowing it to meet the monitoring and management needs of your business, as well as allowing for expansion as business needs dictate.

For this reason, high availability for Enterprise Manager cannot be narrowly defined as a singular implementation, but rather a range of protection levels based on your available resources, Oracle technology and best practices that safeguard the investment in your IT infrastructure. Depending on your Enterprise Manager deployment and business needs, you can implement the level of high availability necessary to sustain your business. High availably for Enterprise Manager can be categorized into four levels, each level building on the previous and increasing in implementation cost and complexity, but also incrementally increasing the level of availability.

### 16.2.1 Levels of High Availability

Each high availability solution level is driven by your business requirements and available IT resources. However, it is important to note that the levels represent a subset of possible deployments that are useful in presenting the various options available. Your IT organization will likely deploy its own configuration which need not exactly match one of the levels.

The following table summarizes four example high availability levels for Oracle Enterprise Manager installations as well as general resource requirements.

***Table 16–1 Enterprise Manager High Availability Levels***

| Level | Description | Minimum Number of Nodes | Recommended Number of Nodes | Load Balancer Requirements |
|---|---|---|---|---|
| Level 1 | OMS and repository database. Each resides on their own host with no failover. | 1 | 2 | None |
| Level 2 | OMS installed on shared storage with a VIP based failover. Database is using Local Data Guard. | 2 | 4 | None |
| Level 3 | OMS in Active/Active configuration. The database is using RAC + Local Data Guard | 3 | 5 | Local Load Balancer |

*Table 16–1 (Cont.) Enterprise Manager High Availability Levels*

| Level | Description | Minimum Number of Nodes | Recommended Number of Nodes | Load Balancer Requirements |
|---|---|---|---|---|
| Level 4 | OMS on the primary site in Active/Active Configuration. Repository deployed using Oracle RAC.<br>Duplicate hardware deployed at the standby site.<br>DR for OMS and Software Library using Storage Replication between primary and standby sites.<br>Database DR using Oracle Data Guard.<br>**Note**: Level 4 is a MAA Best Practice, achieving highest availability in the most cost effective, simple architecture. | 4 | 8 | **Required**: Local Load Balancer for each site.<br>**Optional**: Global Load Balancer |

## 16.3 Comparing Availability Levels

The following tables compare the protection levels and recovery times for the various HA levels.

*Table 16–2 High Availability Levels of Protection*

| Level | OMS Host Failure | OMS Storage Failure | Database Host Failure | Database Storage Failure | Site Failure/Disaster Recovery |
|---|---|---|---|---|---|
| Level 1 | No | No | No | No | No |
| Level 2 | Yes | No | Yes | Yes | No |
| Level 3 | Yes | Yes | Yes | Yes | No |
| Level 4 | Yes | Yes | Yes | Yes | Yes |

*Table 16–3 High Availability Level Recovery Times*

| Level | Node Failure | Local Storage Failure | Site Failure | Cost |
|---|---|---|---|---|
| Level 1 | Hours-Days | Hours-Days | Hours-Days | $ |
| Level 2 | Minutes | Hours-Days | Hours-Days | $$ |
| Level 3 | No Outage | Minutes | Hours-Days | $$$ |
| Level 4 | No Outage | Minutes | Minutes | $$$$ |

One measure that is not represented in the tables is that of scalability. Levels three and four provide the ability to scale the Enterprise Manager installation as business needs grow. The repository, running as a RAC database, can easily be scaled upwards by adding new nodes to the RAC cluster and it is possible to scale the Management Service tier by simply adding more OMS servers.

If you need equalized performance in the event of failover to a standby deployment, whether that is a local standby database or a Level four standby site including a standby RAC database and standby OMS servers, it is essential to ensure that the deployments on both sites are symmetrically scaled. This is particularly true if you want to run through planned failover routines where you actively run on the primary or secondary site for extended periods of time. For example, some finance institutions mandate this as part of operating procedures.

If you need survivability in the event of a primary site loss you need to go with a Level four architecture.

## 16.4 Implementing High Availability Levels

Once you have determined the high availability requirements for your enterprise, you are ready to begin implementing one of the high availability levels that is suitable for your environment. Use the following information roadmap to find implementation instructions for each level.

| Level | Where to find information |
|---|---|
| Level 1 | *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide* |
| Level 2 | *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide*<br>PLUS<br>■ Configuring the Cloud Control OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names<br>■ Configuring a Standby Database for the Management Repository |
| Level 3 | *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide*<br>PLUS<br>■ Oracle Management Service High Availability<br>■ Configuring a Load Balancer<br>■ Configuring the Software Library<br>■ Installing Additional Management Services<br>■ Configuring a Standby Database for the Management Repository |
| Level 4 | *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide*<br>PLUS<br>■ Configuring a Standby Database for the Management Repository<br>■ Management Service Disaster Recovery |

# 17

# Enterprise Manager High Availability

This chapter discusses best practices for installation and configuration of each Cloud Control component and covers the following topics:

- Agent High Availability
- Repository High Availability
- Oracle Management Service High Availability

## 17.1 Agent High Availability

The following sections discuss best practices for installation and configuration of the Management Agent.

### 17.1.1 Configuring the Management Agent to Automatically Start on Boot and Restart on Failure

The Management Agent is started manually. It is important that the Management Agent be automatically started when the host is booted to insure monitoring of critical resources on the administered host. To that end, use any and all operating system mechanisms to automatically start the Management Agent. For example, on UNIX systems this is done by placing an entry in the UNIX `/etc/init.d` that calls the Management Agent on boot or by setting the Windows service to start automatically.

### 17.1.2 Configuring Restart for the Management Agent

Once the Management Agent is started, the watchdog process monitors the Management Agent and attempts to restart it in the event of a failure. The behavior of the watchdog is controlled by environment variables set before the Management Agent process starts. The environment variables that control this behavior follow. All testing discussed here was done with the default settings.

- EM_MAX_RETRIES – This is the maximum number of times the watchdog will attempt to restart the Management Agent within the EM_RETRY_WINDOW. The default is to attempt restart of the Management Agent three times.
- EM_RETRY_WINDOW - This is the time interval in seconds that is used together with the EM_MAX_RETRIES environmental variable to determine whether the Management Agent is to be restarted. The default is 600 seconds.

The watchdog will not restart the Management Agent if the watchdog detects that the Management Agent has required restart more than EM_MAX_RETRIES within the EM_RETRY_WINDOW time period.

### 17.1.3 Installing the Management Agent Software on Redundant Storage

The Management Agent persists its configuration, intermediate state and collected information using local files in the Agent State Directory.

In the event that these files are lost or corrupted before being uploaded to the Management Repository, a loss of monitoring data and any pending alerts not yet uploaded to the Management Repository occurs.

To protect from such losses, configure the Agent State Directory on redundant storage. The Agent State Directory can be determined by entering the command '$AGENT_HOME/agent_inst/bin/emctl getemhome', or from the Agent Homepage in the Cloud Control console.

## 17.2 Repository High Availability

The following sections document best practices for repository configuration.

### 17.2.1 General Best Practice for Repository High Availability

Before installing Enterprise Manager, you should prepare the database, which will be used for setting up Management Repository. Install the database using Database Configuration Assistant (DBCA) to make sure that you inherit all Oracle install best practices.

- Choose Automatic Storage Management (ASM) as the underlying storage technology.
- Enable ARCHIVELOG Mode
- Enable Block Checksums
- Configure the Size of Redo Log Files and Groups Appropriately
- Use a Flash Recovery Area
- Enable Flashback Database
- Use Fast-Start Fault Recovery to Control Instance Recovery Time
- Enable Database Block Checking
- Set DISK_ASYNCH_IO

Use the MAA Advisor for additional high availability recommendations that should be applied to the Management Repository. MAA Advisor can be accessed by selecting Availability > MAA Advisor from the Homepage of the Repository Database.

See Oracle Database High Availability Best Practices for more information on these and other best practices to ensure the database that hosts the Management Repository is configured to provide required availability.

### 17.2.2 Configuring RAC for the Management Repository

If the Management Repository is a Real Application Cluster (RAC) database, the Management Services should be configured with the appropriate connect strings. SCAN connect strings are recommended to avoid reconfiguration of the Repository connect descriptor following addition or removal of nodes in the Repository tier. SERVICE_NAME should always be used in connect strings instead of SID_NAME

Refer to the Oracle Database Net Services Administrator's Guide for details.

The following example shows a connect string for Repository where database version is lower than 11g Release 2.

```
(DESCRIPTION= (ADDRESS_LIST=(FAILOVER=ON)
(ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_
DATA=(SERVICE_NAME=EMREP)))
```

The following example shows a connect string for Repository where database version is 11g Release 2 or higher

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=primary-cluster-scan.example.com)(PORT=1
521))(CON
NECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=PDB.example.com)))
```

The Repository connect descriptor is configured by running the emctl command from Management Service. If you have multiple Management Services configured, this command must be run on each Management Service.

```
emctl config oms -store_repos_details -repos_conndesc '(DESCRIPTION= (ADDRESS_
LIST=(FAILOVER=ON) (ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_
DATA=(SERVICE_NAME=EMREP)))' -repos_user sysman
```

After updating the Repository connect descriptor, run the following command from any one OMS to make the same change to the monitoring configuration used for the Management Services and Repository target:

```
emctl config emrep -conn_desc <repository_connect descriptor as above>
```

## 17.3 Oracle Management Service High Availability

The following sections document configuring the OMS for high availability.

OMS high availability begins with ensuring there is at least one OMS available at any given time. Depending upon your Recovery Time Objective (RTO), this can be accomplished without downtime from loss of a node in an active/active configuration by adding at least one additional OMS, or with limited downtime from loss of a node in an active/passive configuration by ensuring that the OMS can be run with the same address on a different server if the primary server fails. See Chapter 16, "High Availability Solutions" for more details on architectural options for achieving high availability.

Regardless of the manner selected to provide high availability, and the level of availability selected for initial installation, there are a number of steps that can be taken to best prepare the environment for a future move to higher levels of availability including disaster recovery. See "Best Practices for Configuring the Cloud Control OMS to be Compatible with Disaster Recovery using Alias Host Names and Storage Replication" on page 17-4 for details on these steps.

To ensure OMS high availability, there also must be a sufficient number of OMSs to support the size and scope of the environment managed by Enterprise Manager as well as the scale and complexity of the usage of Enterprise Manager including the number of administrators and the breadth of capability employed. See EM Operational Considerations and Troubleshooting Whitepaper Master Index in My Oracle Support note 1940179.1 for more information, including understanding how to configure and monitor for availability and how to determine how many OMSs are needed based on operational experience.

Once an environment requires more than one active OMS, whether to ensure sufficient capacity for the environment or to prevent the downtime associated with failover to a passive OMS, a Server Load Balancer (SLB) is required. A SLB provides a single address for Management Agents and administrators to communicate with the set of OMS servers, monitors the OMSs to know which OMSs are available, and routes the communication to an available OMS.

It can be expensive to implement a SLB. If the environment does not need more than one OMS to handle the processing requirements, and if the minutes of downtime associated with an active/passive failover of the OMS meets RTO requirements, a SLB is not required to provide high availability. The instructions in "Configuring the Cloud Control OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names" on page 17-7 provide an example of how to configure for high availability using a virtual IP address and shared storage.

If you need to add one or more additional OMSs to support your RTO and/or the processing needs of the environment, see "Installing Additional Management Services" on page 17-10. Once you've added additional OMS(s), see "Configuring Multiple Management Services Behind a Server Load Balancer (SLB)" on page 17-10 for information on how to configure multiple OMSs behind a SLB.

## 17.3.1 Best Practices for Configuring the Cloud Control OMS to be Compatible with Disaster Recovery using Alias Host Names and Storage Replication

This section provides best practices for Cloud Control administrators who want to install the Cloud Control OMS in a manner that will ensure compatibility with Disaster Recovery using Alias Host Names and Storage Replication. This will reduce the steps required to implement a Disaster Recovery configuration should it be required at a future date. These best practices are applicable for every MAA high availability level installation. Installing even a standalone OMS in a manner that considers the needs of the highest MAA high availability level will provide the greatest flexibility and easiest migration to higher MAA high availability levels in the future.

### 17.3.1.1 Overview and Requirements

The following installation conditions must be met in order for a Cloud Control OMS installation to support Disaster Recovery using alias host names and storage replication:

- The Middleware Home, OMS Instance Base, Agent Base, and Oracle Inventory directories must be installed on storage that can be replicated to the standby site.
- The installation of the OMS must be performed in a manner that maintains an Alias Host Name that is the same for the primary and standby site hosts for the OMS. This Alias Host Name allows the software to be configured such that the same binaries and configuration can be used either on the OMS host at the primary or standby site without changes.
- The Middleware Home, OMS Instance Base, and Agent Base must be installed using the Oracle Inventory location on the storage that can be replicated to the standby site.
- The software owner and time zone parameters must be the same on all nodes that will host this Oracle Management Service (OMS).
- The path to the Middleware, Instance, OMS Agent, and Oracle Inventory directories must be the same on all nodes that will host this OMS.

#### 17.3.1.2 Create an OMS installation base directory under ORACLE_BASE

To support disaster recovery, the Middleware Home, OMS Instance Base, Agent Base, and Oracle Inventory directories must be installed on storage that can be replicated to the standby site. Each of these directories is traditionally located directly underneath ORACLE_BASE. Once an OMS is installed, its directory path cannot be changed. Transitioning an installation with each of these directories located directly underneath ORACLE_BASE to replicated storage later can add complications such as requiring the ORACLE_BASE to be relocated to replicated storage to maintain the original directory paths for the installed software, which would require any locally installed software under that path to be uninstalled and reinstalled in an alternate local storage directory.

To provide the greatest flexibility for future storage migrations, create a directory under ORACLE_BASE that will be the base directory for all OMS software, including the Middleware Home, OMS Instance Base, Agent Base, and Oracle Inventory directories. For example, if the ORACLE_BASE is /u01/app/oracle, create a new OMS installation base directory, such as /u01/app/oracle/OMS. This directory will serve as the mount point for the replicated storage. If the software is installed locally under this directory, this directory can become a single mount point to the replicated storage enabling a simple migration.

When providing and reviewing directory locations while installing the OMS, ensure the Middleware Home, OMS Instance Base, Agent Base, and Oracle Inventory are installed under this directory.

#### 17.3.1.3 Configure an Alias Host Name

To support disaster recovery, a host at the primary site and a host at the standby site must be capable of running with the same host name used in the OMS installation. This can be accomplished using an alias host name.

Configure an alias host name to use in the installation using the guidance in "Planning Host Names" in chapter 18. Option 2: Alias host names on both sites in this section provides the greatest flexibility and is recommended as a best practice for new installations.

To implement Option 2, specify the alias host name when installing the OMS, either by using the ORACLE_HOSTNAME=<ALIAS_HOST_NAME> parameter or by specifying the alias host name in the Host Name field in the OUI installation. For example, include the following parameter on the runInstaller command line:

```
ORACLE_HOSTNAME=oms1.example.com
```

#### 17.3.1.4 Configure an Oracle Inventory located under OMS installation base directory

To support disaster recovery, a single OMS installation is shared by a host at the primary site and a host at the standby site using replicated storage. Only the active OMS mounts the replicated storage. Software maintenance activities may need to be performed when either the primary or standby site is the active site. As such, it is important to ensure that the Oracle Inventory containing the details of the installation is available from either location.

To prevent the need to perform manual migration activities to move the OMS installation from a local Oracle Inventory to a replicated storage Oracle Inventory, create the Oracle Inventory under the OMS installation base directory.

Use the following steps to prepare the installer to set up an inventory located under the OMS installation base directory:

1. Create the OMS installation base directory.

2. Create the Oracle Inventory directory under the new OMS installation base directory:

   ```
   $ cd <OMS installation base directory>
   ```

   ```
   $ mkdir oraInventory
   ```

3. Create the oraInst.loc file. This file contains the Oracle Inventory directory path information needed by the Universal Installer.

   ```
   $ cd oraInventory
   ```

   ```
   $ vi oraInst.loc
   ```

   Enter the path information to the Oracle Inventory directory and specify the group of the software owner as the oinstall user. For example:

   ```
   inventory_loc=/u01/app/oracle/OMS/oraInventory
   ```

   ```
   inst_group=oinstall
   ```

Specify the Oracle Inventory under the OMS installation base directory when installing the OMS by providing the -invPtrloc <oraInst.loc file with path> parameter on the runInstaller command line, for example:

```
 -invPtrloc /u01/app/oracle/OMS/oraInventory/oraInst.loc
```

The installer will create the inventory in the specified location. Use this inventory for all installation, patching, and upgrade activities for this OMS and OMS agent.

#### 17.3.1.5 Configure a Software Owner and Group that can be configured identically on all nodes

Just as the OMSs at the primary site are installed using the same software owner and group, to support disaster recovery, the software owner and group need to be configured identically on the standby site OMS hosts. Ensure that both the owner name and ID and the group name and ID selected for use at the primary site will also be available for use at the standby site.

Verification that the user and group of the software owner are configured identically on all OMS nodes can be performed using the 'id' command as in the example below:

```
$ id -a
```

```
uid=550(oracle) gid=50(oinstall) groups=501(dba)
```

#### 17.3.1.6 Select a time zone that can be configured identically on all nodes

Just as the OMSs at the primary site are installed using the same time zone, to support disaster recovery, the time zone should be configured identically on the standby site OMS hosts. Select a time zone that can be used at both sites and ensure that the time zone is the same on all OMS hosts.

#### 17.3.1.7 Installation and Configuration

The following are high level installation steps that reinforce the best practices listed in this section. Reference the detailed instructions in the Enterprise Manager Basic Installation Guide for details on the installation steps, including required pre-requisites and additional post installation operations.

If you are using an NFS mounted volume for the installation, please ensure that you specify rsize and wsize in your mount command to prevent running into I/O issues.

For example:

```
nas.example.com:/export/share1 /u01/app/oracle/OMS nfs
rw,bg,rsize=32768,wsize=32768,hard,nointr,tcp,noacl,vers=3,timeo=600 0 0
```

> **Note:** Review the NFS Mount Point Location Requirements in Oracle Enterprise Manager Cloud Control Basic Installation Guide for additional important NFS-related requirements.

Refer to the following steps when installing the software:

1. Create an OMS installation base directory under ORACLE_BASE. If installing on replicated storage now, ensure that the replicated storage is mounted to this directory.
2. Configure the Alias Host Names for all OMSs being installed on each of the OMS hosts.
3. Configure a Software Owner and Group that will be consistently defined on all OMS hosts.
4. Configure the time zone that will be consistently set on all OMS hosts.
5. Follow the detailed preparation and installation instructions in Installing an Enterprise Manager System in the Enterprise Manager Basic Installation Guide, specifying the following information as part of the installation process:
   1. Ensure that the Middleware Home, OMS Instance Base, and Agent Base are located under the OMS installation base directory.
   2. Specify the inventory location file and the Alias Host Name of the OMS. These can be specified on the command line as in the following example:

      ```
      $ runInstaller -invPtrloc
      /u01/app/oracle/OMS/oraInventory/oraInst.loc ORACLE_
      HOSTNAME=oms1.example.com
      ```

      You can also provide the ORACLE_HOSTNAME when prompted for this information from within the Enterprise Manager *runInstaller* UI.
6. Continue the remainder of the installation.

## 17.3.2 Configuring the Cloud Control OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names

This section provides a general reference for Cloud Control administrators who want to configure Enterprise Manager Cloud Control in Cold Failover Cluster (CFC) environments.

### 17.3.2.1 Overview and Requirements

The following conditions must be met for Cloud Control to fail over to a different host:

- The installation must be done using a Virtual Host Name and an associated unique IP address.
- Install on a shared disk/volume which holds the binaries and the gc_inst directory.
- The Inventory location must failover to the surviving node.

- The software owner and time zone parameters must be the same on all cluster member nodes that will host this Oracle Management Service (OMS).

#### 17.3.2.2 Installation and Configuration

To override the physical host name of the cluster member with a virtual host name, software must be installed using the parameter ORACLE_HOSTNAME.

The software must be installed using the command line parameter -invPtrLoc to point to the shared inventory location file, which includes the path to the shared inventory location.

If you are using an NFS mounted volume for the installation, please ensure that you specify rsize and wsize in your mount command to prevent running into I/O issues.

For example:

```
nas.example.com:/export/share1 /u01/app/share1 nfs
rw,bg,rsize=32768,wsize=32768,hard,nointr,tcp,noac,vers=3,timeo=600 0 0
```

> **Note:** Any reference to shared failover volumes could also be true for non-shared failover volumes which can be mounted on active hosts after failover.

#### 17.3.2.3 Setting Up the Virtual Host Name/Virtual IP Address

You can set up the virtual host name and virtual IP address by either allowing the clusterware to set it up, or manually setting it up yourself before installation and startup of Oracle services. The virtual host name must be static and resolvable consistently on the network. All nodes participating in the setup must resolve the virtual IP address to the same host name. Standard TCP tools such as *nslookup* and *traceroute* can be used to verify the host name. Validate using the following commands:

```
nslookup <virtual hostname>
```

This command returns the virtual IP address and full qualified host name.

```
nslookup <virtual IP>
```

This command returns the virtual IP address and fully qualified host name.

Be sure to try these commands on every node of the cluster and verify that the correct information is returned.

#### 17.3.2.4 Setting Up Shared Storage

Storage can be managed by the clusterware that is in use or you can use any shared file system (FS) volume, such as NFS, as long as it is not an unsupported type, such as OCFS V1.

> **Note:** Only OCFS V1 is not supported. **All other versions of OCFS are supported.**

If the OHS directory is on a shared storage, the LockFile directive in the httpd.conf file should be modified to point to a local disk, otherwise there is a potential for locking issues.

### 17.3.2.5 Setting Up the Environment

Some operating system versions require specific operating system patches be applied prior to installing 12c. The user installing and using the 12c software must also have sufficient kernel resources available. Refer to the operating system's installation guide for more details. Before you launch the installer, certain environment variables need to be verified. Each of these variables must be identically set for the account installing the software on ALL machines participating in the cluster:

- **OS variable TZ**

  Time zone setting. You should unset this variable prior to installation.

- **PERL variables**

  Variables such as PERL5LIB should also be unset to avoid association to the incorrect set of PERL libraries

### 17.3.2.6 Synchronizing Operating System IDs

The user and group of the software owner should be defined identically on all nodes of the cluster. This can be verified using the 'id' command:

```
$ id -a

uid=550(oracle) gid=50(oinstall) groups=501(dba)
```

### 17.3.2.7 Setting Up Shared Inventory

Use the following steps to set up shared inventory:

1. Create your new ORACLE_HOME directory.
2. Create the Oracle Inventory directory under the new ORACLE_HOME:

   ```
   $ cd <shared oracle home>

   $ mkdir oraInventory
   ```

3. Create the oraInst.loc file. This file contains the Oracle Inventory directory path information needed by the Universal Installer.

   ```
   vi oraInst.loc
   ```

   Enter the path information to the Oracle Inventory directory and specify the group of the software owner as the oinstall user. For example:

   ```
   inventory_loc=/app/oracle/share1/oraInventory

   inst_group=oinstall
   ```

### 17.3.2.8 Installing the Software

Refer to the following steps when installing the software:

1. Create the shared disk location on both the nodes for the software binaries.
2. Point to the inventory location file oraInst.loc (under the ORACLE_BASE in this case), as well as specifying the host name of the virtual group. For example:

   ```
   $ runInstaller -invPtrloc /app/oracle/share1/oraInst.loc ORACLE_
   HOSTNAME=lxdb.example.com -debug
   ```

   You can also provide the ORACLE_HOSTNAME when prompted for this information from in Enterprise Manager runInstaller UI.

3. Install Oracle Management Services on cluster member Host1.

4. Continue the remainder of the installation normally.
5. Once completed, copy the files oraInst.loc and oratab to /etc on all cluster member hosts (Host2, Host3, ...)

#### 17.3.2.9 Starting Up Services

Ensure that you start your services in the proper order. Use the order listed below:

1. Establish the IP address on the active node.
2. Start the TNS listener (if it is part of the same failover group).
3. Start the database (if it is part of the same failover group).
4. Start Cloud Control using `emctl start oms`
5. Test functionality.

In case of failover, refer to "Performing Switchover and Failover Operations" on page 18-17.

### 17.3.3 Installing Additional Management Services

There are two ways to install additional Management Services:

- Using the "Add Oracle Management Service" Deployment Procedure (preferred method). For more information about using this Deployment Procedure, see the chapter on Adding Additional Oracle Management Services in the *Oracle® Enterprise Manager Cloud Control Basic Installation Guide*.
- Installing Additional Oracle Management Service in Silent Mode (alternative method). For more information about silent mode installation, see the chapter on Installing Additional OMSs in Silent Mode in the *Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

### 17.3.4 Configuring Multiple Management Services Behind a Server Load Balancer (SLB)

The following sections discuss how to configure the OMS for high availability in an Active/Active configuration using a Server Load Balancer.

#### 17.3.4.1 Configuring the Software Library

The Software Library location must be accessible by all active Management Services. If the Software Library is not configured during installation, it needs to be configured post-install using the Enterprise Manager console:

1. On the Enterprise Manager home page, from the **Setup** menu, select P**rovisioning and Patching**, and then select **Software Library**.
2. Click the **Provisioning** subtab.
3. On the Provisioning page, click the **Administration** subtab.
4. In the **Software Library Configuration** section, click **Add** to set the Software Library Directory Location to a shared storage that can be accessed by any Management Service hosts.

#### 17.3.4.2 Configuring a Load Balancer

This section describes the guidelines for setting up a Server Load Balancer (SLB) to distribute the Agent and Browser traffic to available Management Services.

### Server Load Balancer Requirements

In order to configure your OMS's in an active/active configuration behind an SLB, your SLB must meet the following requirements:

- The SLB must provide support for multiple virtual server ports.

  Depending on your configuration, you may require up to 5 ports on the SLB (Secure Upload, Agent Registration, Secure Console, Unsecure Console, BI Publisher)

- Support for persistence.

  HTTP and HTTPS traffic between the browser and the OMS requires persistence.

- Support for application monitoring.

  The SLB must be capable of monitoring the health of the OMSs and detecting failures, so that requests will not be routed to OMSs that are not available.

SLB configuration is a two-step process:

1. Configure the SLB.
2. Make requisite changes on the Management Services.

**17.3.4.2.1 SLB Side Setup** Use the following table as reference for setting up the SLB with Cloud Control Management Services.

*Table 17–1 Management Service Ports*

| Cloud Control Service | TCP Port | Monitor Name | Persistence | Pool Name | Load Balancing | Virtual Server Name | Virtual Server Port |
|---|---|---|---|---|---|---|---|
| Secure Upload | 1159 | mon_gcsu4900 | None | pool_gcsu4900 | Round Robin | vs_gcsu4900 | 1159 |
| Agent Registration | 4889 | mon_gcar4889 | Active Cookie Insert | pool_gcar4889 | Round Robin | vs_gcar4889 | 4889 |
| Secure Console | 7799 | mon_gcsc7799 | Source IP | pool_gcsc7799 | Round Robin | vs_gcsc443 | 443 |
| Unsecure Console (optional) | 7788 | mon_gcuc7788 | Source IP | pool_gcuc7788 | Round Robin | vs_gcuc80 | 80 |

Use the administration tools that are packaged with your SLB. A sample configuration follows. This example assumes that you have two Management Services running on host A and host B using the default ports as listed in Table 33–1.

1. Create Pools

   A *pool* is a set of servers grouped together to receive traffic on a specific TCP port using a load balancing method. Each pool can have its own unique characteristic for a persistence definition and the load-balancing algorithm used.

*Table 17–2 Pools*

| Pool Name | Usage | Members | Persistence | Load Balancing |
|---|---|---|---|---|
| pool_gcsu4900 | Secure upload | HostA:4900<br>HostB:4900 | None | Round Robin |
| pool_gcar4889 | Agent registration | HostA:4889<br>HostB:4889 | Active cookie insert; expiration 60 minutes | Round Robin |
| pool_gcsc7799 | Secured console access | HostA:7799<br>HostB:7799 | Source IP; expiration 60 minutes | Round Robin |
| pool_gcuc7788 (optional) | Unsecured console access | HostA:7788<br>HostB:7788 | Source IP; expiration 60 minutes | Round Robin |

2. Create Virtual Servers

   A *virtual server*, with its virtual IP Address and port number, is the client-addressable hostname or IP address through which members of a load balancing pool are made available to a client. After a virtual server receives a request, it directs the request to a member of the pool based on a chosen load balancing method.

*Table 17–3 Virtual Servers*

| Virtual Server Name | Usage | Virtual Server Port | Pool |
|---|---|---|---|
| vs_gcsu4900 | Secure upload | 4900 | pool_gcsu4900 |
| vs_gcar4889 | Agent registration | 4889 | pool_gcar4889 |
| vs_gcsc443 | Secure console access | 443 | pool_gcsc7799 |
| vs_gcuc80 (optional) | Unsecure console access | 80 | pool_gcuc7788 |

3. Create Monitors

   *Monitors* are used to verify the operational state of pool members. Monitors verify connections and services on nodes that are members of load-balancing pools. A monitor is designed to check the status of a service on an ongoing basis, at a set interval. If the service being checked does not respond within a specified timeout period, the load balancer automatically takes it out of the pool and will choose the other members of the pool. When the node or service becomes available again, the monitor detects this and the member is automatically accessible to the pool and able to handle traffic.

*Table 17–4 Monitors*

| Monitor Name | Configuration | Associate With |
|---|---|---|
| mon_gcsu4900 | Type: https<br>Interval: 60<br>Timeout: 181<br>Send String: GET /empbs/upload<br>Receive String: Http Receiver Servlet active! | HostA:4900<br>HostB:4900 |
| mon_gcar4889 | Type: http<br>Interval: 60<br>Timeout: 181<br>Send String: GET /empbs/genwallet<br>Receive String: GenWallet Servlet activated | HostA:4889<br>HostB:4889 |
| mon_gcsc7799 | Type: https<br>Interval: 5<br>Timeout: 16<br>Send String: GET /em/consoleStatus.jsp<br>Receive String: Enterprise Manager Console is UP | HostA:7799<br>HostB:7799 |
| mon_gcuc7788 (optional) | Type: http<br>Interval: 5<br>Timeout: 16<br>Send String: GET /em/consoleStatus.jsp<br>Receive String: Enterprise Manager Console is UP | HostA:7788<br>HostB:7788 |
| mon_gcscbip7799 | Type: https<br>Interval: 5<br>Timeout: 16<br>Send String: GET /xmlpserver/services<br>Receive String: getDocumentData | HostA:7799<br>HostB:7799 |
| mon_gcucbip7788 | Type: https<br>Interval: 5<br>Timeout: 16<br>Send String: GET /xmlpserver/services<br>Receive String: getDocumentData | HostA:7799<br>HostB:7799 |

**Note:** Some Load Balancers require <CR><LF> characters to be added explicitly to the Send String using literal "\r\n". This is vendor-specific. Refer to your SLB documentation for details.

#### 17.3.4.2.2 Enterprise Manager Side Setup

Perform the following steps:

1. Resecure the Oracle Management Service

   By default, the service name on the Management Service-side certificate uses the name of the Management Service host. Management Agents do not accept this certificate when they communicate with the Oracle Management Service through a load balancer. You must run the following command to regenerate the certificate on each Management Service:

```
emctl secure oms
  -host slb.example.com
  -secure_port 4900
  -slb_port 4900
  -slb_console_port 443
  -console
  [-lock]  [-lock_console]
```

Output:

```
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Securing OMS... Started.
Enter Enterprise Manager Root (SYSMAN) Password :
Enter Agent Registration Password :
Securing OMS... Successful
Restart OMS
```

2. Resecure all Management Agents

   Management Agents that were installed prior to SLB setup, including the Management Agent that comes with the Management Service install, would be uploading directly to the Management Service. These Management Agents will not be able to upload after SLB is setup. Resecure these Management Agents to upload to the SLB by running the following command on each Management Agent:

   ```
   emctl secure agent -emdWalletSrcUrl https://slb.example.com:<upload port>/em
   ```

#### 17.3.4.2.3 Configuring SSL on Enterprise Manager and the SLB (Release 12.1.0.2 and later)

If the SLB is configured to use Third-Party/Custom SSL certificates, you must ensure that the CA certificates are properly configured in order for the trust relationship to be maintained between the Agent, SLB, and the OMS. Specifically, the following must be carried out:

- Import the CA certificates of the SLB into the OMS trust store.
- Copy the Enterprise Manager CA certificates to the trust store of the SLB

Enterprise Manager uses the default Enterprise Manager certificates and not the Custom certificates. In order for Agents to upload information successfully to the OMS through the SLB, these custom trusted certificates need to be copied/imported to the trust store of the OMS and Agents

The following procedures illustrate the process used to secure the 12c OMS and Agent when an SLB is configured with Third Party/Custom SSL certificates.

**Verifying the SSL Certificate used at the SLB**

Perform the following steps to determine whether the SLB is using different certificates than the OMS:

1. To check the certificate chain used by any URL, run the following command:

   ```
   <OMS_HOME>/bin>./emctl secdiag openurl -url <HTTPS URL>
   ```

   To check the certificates used by the SLB URL, run the following command:

   ```
   <OMS_HOME>/bin>./emctl secdiag openurl -url https://<SLB
   Hostname>:<HTTPS Upload port>/empbs/upload
   ```

To check the certificates used by the OMS URL, run the following command:

```
<OMS_HOME>/bin>./emctl secdiag openurl -url https://<OMS
Hostname>:<HTTPS Upload port>/empbs/upload
```

2. If the default Enterprise Manager self-signed certificates are used in the SLB, the output of both the commands will appear as follows:

   **Issuer : CN=<OMS Hostname>, C=US, ST=CA, L=EnterpriseManager on <OMS Hostname>, OU=EnterpriseManager on <OMS Hostname>, O=EnterpriseManager on <OMS Hostname>**

3. If a custom or self-signed SSL certificate is used in the SLB, then output of the command executed with the SLB Name will provide details shown here:

   **Issuer : CN=Entrust Certification Authority - L1C, OU="(c) 2014 Entrust, Inc.", OU=www.entrust.net/rpa is incorporated by reference, O="Entrust, Inc.", C=US**

   In this example, the SLB is using the custom certificate (CN=Entrust Certification Authority - L1C, OU="(c) 2014 Entrust, Inc."), which needs to be imported as trusted certificate into the OMS.

4. If OpenSSL is available on the OS, you can also check the value of CN by running the following command:

   ```
   $openssl s_client -connect <HOSTNAME>:<PORT>
   ```

**Importing the SSL Certificate of the SLB to the Trust Store of the OMS and Agent**

1. Export the SLB certificate in base64 format to a text file named: `customca.txt`.

2. Secure the OMS:

   ```
   cd <OMS_HOME>/bin>
   ```

   ```
   ./emctl secure oms -host <SLB Host name> -secure_port <HTTPS Upload
   Port> -slb_port <SLB upload Port> -slb_console_port <SLB Console port>
   -console -trust_certs_loc <path to customca.txt>
   ```

   > **Note:** All the OMS's behind the SLB need to be secured using the *emctl secure oms* command.
   >
   > The CA certificate of the OMS is present in the `<EM_INSTANCE_HOME>/em/EMGC_OMS1/sysman/config/b64LocalCertificate.txt` file and needs to be copied to the SSL trust store of the SLB.

3. Restart all the OMS:

   ```
   cd <OMS_HOME>/bin
   ```

   ```
   emctl stop oms -all
   ```

   ```
   emctl start oms
   ```

4. Secure all the Agents pointing to this Enterprise Manager setup:

   ```
   cd <AGENT_HOME>/bin
   ```

   ```
   ./emctl secure agent -emdWalletSrcUrl <SLB Upload URL>
   ```

# 18 Enterprise Manager Disaster Recovery

While the high availability solutions described in the previous chapter typically protect against component failure or system-level problems, in many enterprises it is also necessary to protect Enterprise Manager against larger outages such as catastrophic data center failure due to natural disasters, fire, electrical failure, evacuation, or pervasive sabotage.

Maximum Availability Architecture for Enterprise Manager involves deploying a remote failover architecture that allows a secondary data center to take over the management infrastructure in the event that disaster strikes the primary management infrastructure.

> **Note:** The recommended approach for OMS Disaster Recovery differs according to the version of Enterprise Manager.
>
> **For Cloud Control 12.1.0.2 and earlier** - Standby OMSs using Standby WebLogic Domain should be used. See Appendix I, "Standby OMSs Using Standby WebLogic Domain" for more information
>
> **For Cloud Control 12.1.0.3 and later** - Standby OMSs using Storage Replication is the preferred approach and is discussed in this chapter.
>
> BI Publisher server configuration is not supported on standby OMSs using Standby Weblogic Domain for Cloud Control 12.1.0.4 and later.

Advantages of Standby OMSs using Storage Replication are:

- OMS patching and upgrade only needs to be performed at one site.
- Plug-ins only need to be managed at one site.

This chapter covers the following topics:

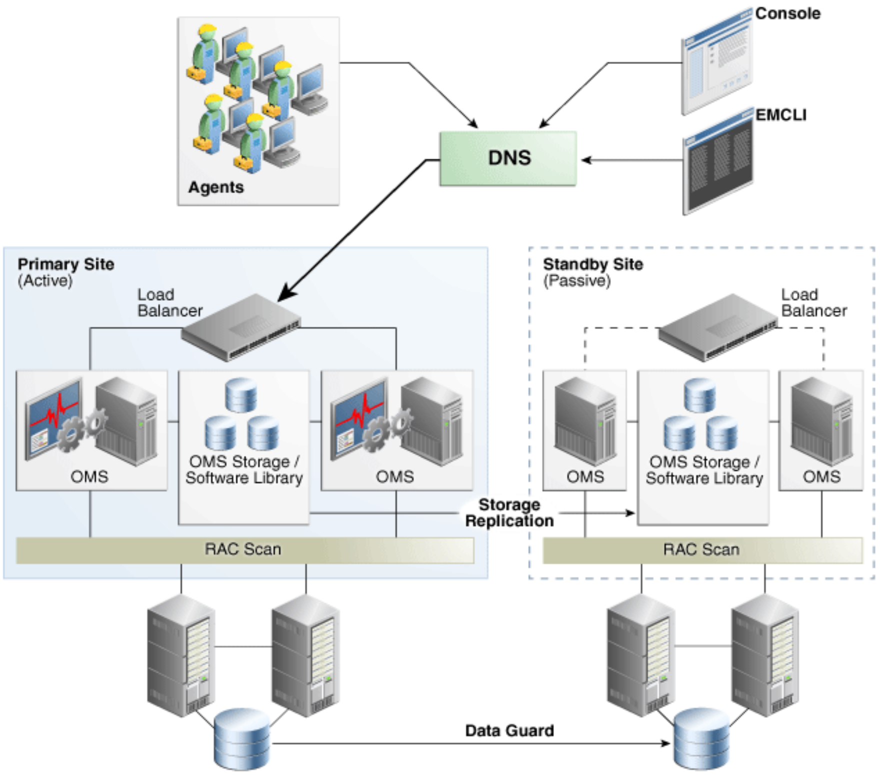
- Disaster Recovery Overview and Topology
- Design Considerations
- Setting Up Management Repository Disaster Recovery
- Setting Up the OMS, Bi Publisher Shared Storage and Software Library Disaster Recovery
- Performing Switchover and Failover Operations
- Keeping the Standby Site in Sync with the Primary
- Disaster Recovery Solution with ACFS Replication

## 18.1 Disaster Recovery Overview and Topology

The Disaster Recovery solution for a Cloud Control deployment involves replication of the OMS, Software Library and Repository components at a standby site. This solution can be combined with the high availability solution described in the previous chapter to ensure that failures ranging from component failure to a complete site outage can be recovered from with minimal disruption to the availability of Cloud Control.

A complete implementation of the Enterprise Manager Cloud Control combining the High Availability design from the previous chapter with the Disaster Recovery described in this chapter solution is shown in the following figure.

***Figure 18–1 High Availability with Disaster Recovery Topology***



Key aspects of the DR solution shown in the figure are:

- The solution has two sites. The Primary Site is running and active, while the Standby Site is in passive mode.
- The traffic from the Enterprise Manager users and Agents is directed to the Primary Site by a Global Load Balancer or a DNS entry that resolves to an IP address hosted at the Primary Site.
- The Standby Site is similar to the Primary Site in terms of hardware and network resources which ensures there will be no loss of performance when failover happens.
- It is not necessary to perform an OMS installation at the Standby Site. Oracle Inventory, OMS Software, Agent and Software Library and all located on replicated storage. When the Production Site storage is replicated at the Standby Site the equivalent data are written to the Standby Site

- The OMS hostnames must resolve to the IP addresses of the Primary OMSs when queried from the Primary Site and to the IP addresses of the corresponding standby hosts when queried from the Standby Site.
- OMS software, Oracle Inventory, Software Library and Agent binaries and configuration files for all OMS(s) are on replicated storage.
- OMS hosts on each site access the replicated storage using the same mount points
- Replication between the sites takes place should take place at regular scheduled intervals and following configuration changes.
- Oracle Data Guard Physical Standby is used to replicate the Repository database at the standby site.
- There must be sufficient network bandwidth between the primary and standby sites to handle peak redo data generation.
- When there is a failure or planned outage of the Primary Site, you perform the following steps to enable the Standby Site to assume the Primary role in the topology:
  - Stop OMSs at the primary site
  - Perform on-demand replication of storage (if primary site is available)
  - Failover/switchover of the database to the standby site
  - Reverse storage replication and activate replicated storage read/write at standby site
  - Start OMSs at standby site
  - Update DNS or global load balancer to re-route user requests to the standby site. At this point, the standby site has assumed the production role.

## 18.2 Design Considerations

This section discusses design considerations for a Cloud Control Disaster Recovery solution for an enterprise deployment.

The following topics are covered:

- Network Considerations
- Storage Considerations
- Database Considerations
- Starting Points

### 18.2.1 Network Considerations

The following sections discuss network considerations that must be taken into account when implementing standby Management Services using storage replication

#### 18.2.1.1 Planning Host Names

In a Disaster Recovery topology, the production site host names must be resolvable to the IP addresses of the corresponding peer systems at the standby site. Therefore, it is important to plan the host names for the production site and standby site. After switchover or failover from a primary site to a standby site, it should be possible to start applications on the standby hosts without requiring you to change the hostname for hosts on the standby site.

This can be achieved in either of the following ways:

- Option 1: Physical host names on primary site and alias on standby site: OMSs at the primary site are configured using physical host names and aliases for these host names are configured on the corresponding hosts at the standby site.
- Option 2: Alias host names on both sites: OMSs at the primary site are configured using an alias host name that can be configured at both the primary and standby sites.

The choice between these options would depend on your network infrastructure and corporate policies. From a setup procedure perspective, Option 1 is easier to implement if you have an existing single site Cloud Control installation which uses the physical host names as it does not require any transformation of your existing site to setup DR. Option 2 is easier to implement if you are setting up a new Cloud Control installation and start with alias host names or you have an existing Cloud Control installation using alias host names.

**Note:** If using Option 2, you should set ORACLE_HOSTNAME as the Alias host name when invoking the installer. For example:

```
$ runInstaller ORACLE_HOSTNAME=oms1.example.com
```

You can also provide the ORACLE_HOSTNAME when prompted for this information from in Enterprise Manager runInstaller UI.

Host name resolution at each site can be done using either local resolution (/etc/hosts) or DNS based resolution or a combination of both. The following examples use these physical host names and IP addresses:

```
HOSTNAME             IP ADDRESS      DESCRIPTION
oms1-p.example.com   123.1.2.111     Physical host for OMS1 on Primary site
oms2-p.example.com   123.1.2.112     Physical host for OMS2 on Primary site
oms1-s.example.com   123.2.2.111     Physical host for OMS1 on Standby site
oms2-s.example.com   123.2.2.112     Physical host for OMS2 on Standby site
```

**Note:** If using local resolution for either Option 1 or Option 2, ensure that the /etc/hosts file on each OMS at a site where alias host names are being used contains the physical and alias host names for all OMSs at the site as depicted in the examples below.

**Example for Option 1**: /etc/hosts configurations when OMSs are installed at primary site using primary site physical host names (oms1-p.example.com and oms2-p.example.com):

```
Primary Site

127.0.0.1      localhost.localdomain  localhost
123.1.2.111    oms1-p.example.com     oms1-p #OMS1
123.1.2.112    oms2-p.example.com     oms2-p #OMS2

Standby Site

127.0.0.1      localhost.localdomain  localhost
123.2.2.111    oms1-s.example.com     oms1-s      oms1-p.example.com #OMS1
123.2.2.112    oms2-s.example.com     oms2-s      oms2-p.example.com #OMS2
```

If the network has been configured correctly, a ping of the OMS host name from the primary site should result in a reply from the primary host, and a ping of the OMS host name from the standby site should result in a reply from the standby host.

Ping results from primary site (reply from primary site):

```
[oracle@oms1-p ~]$ ping oms1-p.example.com
PING oms1-p.example.com (123.1.2.111) 56(84) bytes of data.
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

Ping results from standby site (reply from standby site)

```
[oracle@oms1-s ~]$ ping oms1-p.example.com
PING oms1-s.example.com (123.2.2.111) 56(84) bytes of data.
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

**Example for Option 2**: /etc/hosts configuration when OMSs are installed using alias host names (oms1.example.com and oms2.example.com):

```
Primary Site

127.0.0.1     localhost.localdomain   localhost
123.1.2.111   oms1-p.example.com      oms1-p     oms1.example.com #OMS1
123.1.2.112   oms2-p.example.com      oms2-p     oms2.example.com #OMS2

Standby Site

127.0.0.1    localhost.localdomain    localhost
123.2.2.111  oms1-s.example.com       oms1-s     oms1.example.com #OMS1
123.2.2.112  oms2-s.example.com       oms2-s     oms2.example.com #OMS2
```

If the network has been configured correctly, a ping of the OMS host name from the primary site should result in a reply from the primary host, and a ping of the OMS host name from the standby site should result in a reply from the standby host.

**Example**:

Ping results from primary site (reply from primary site):

```
[oracle@oms1-p ~]$ ping oms1.example.com
PING oms1-p.example.com (123.1.2.111) 56(84) bytes of data.
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

Ping results from standby site (reply from standby site)

```
[oracle@oms1-s ~]$ ping oms1.example.com
PING oms1-s.example.com (123.2.2.111) 56(84) bytes of data.
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

#### 18.2.1.2 Load Balancers Consideration

If there is more than one OMS at each site, both Primary and Standby Sites require their own server load balancer. See "Configuring a Load Balancer". The SLB pools on each site will reference the IP addresses of the respective OMS hosts.

#### 18.2.1.3 Application Virtual Host Name Consideration

A hostname through which the Cloud Control clients (agents and users) should access Cloud Control is required. When the primary site is active, this hostname should be configured in DNS to resolve to the IP address hosted by the primary site SLB. When the standby site is activated, the DNS entry should be updated so that the hostname resolves to the IP address hosted by the standby site SLB.

A sample DNS configuration for the Cloud Control application hostname when using multiple OMSs with an SLB at each site is shown in the table below:

***Table 18–1 DNS Configuration***

| DNS NAME | DNS RECORD TYPE | VALUE | COMMENTS |
|---|---|---|---|
| em.example.com | CNAME | slb_primary.example.com | Virtual Hostname used by Cloud Control clients to communicate with Management Service. Should point to the currently active site. |
| slb_primary.example.com | A | 123.1.2.110 | Primary Site SLB address |
| slb_standby.example.com | A | 123.2.2.110 | Standby Site SLB address |

The DNS switchover can be accomplished by either using a global load balancer or manually changing DNS names.

- A global load balancer can provide authoritative DNS name server equivalent capabilities. One advantage of using a global load balancer is that the time for a new name-to-IP mapping to take effect can be almost immediate. The downside is that an additional investment must be made for the global load balancer
- Manually changing the DNS names. To ensure that DNS records cached by the Cloud Control clients are updated in a timely fashion after an update, it is recommended to set the TTL for the em.example.com CNAME to a low value such as 60 seconds. This will ensure that DNS changes will quickly propagate to all clients. However due to the shortened caching period, an increase in DNS requests can be observed.

### 18.2.2 Storage Considerations

The Disaster Recovery solution for a Cloud Control deployment involves installing the Software Library, OMS installation, Agent installation and Oracle inventory on replicated storage.

**Storage Replication Requirements**

Your chosen method of storage replication should support the following:

- Snapshots and consistent filesystem copies
- Ability to perform scheduled and on-demand replication between sites

The following section details the storage structure recommended by Oracle.

- Create one volume per OMS host.
- Mount the above volumes to each OMS host using the same mount point e.g. /u01/app/oracle/OMS. On each host, this volume would contain the OMS installation, Agent installation and Oracle inventory.

- Create a consistency group for the above volumes so that consistent replication can be done for all the volumes.
- Create one volume for the software library. This volume must be mounted simultaneously to all the OMS hosts using the same mount point. For example, `/swlib`.
- Create one volume for the BIP. This volume must be mounted simultaneously to all OMS hosts using the same mount point. For example, `/bip`.
- Decide on appropriate replication frequency for the OMS file systems, software library and BIP based on your infrastructure. Oracle recommends a minimum frequency of 24 hours for the OMS file system and continuous or hourly replication for the software library.

Once these volumes are mounted, ensure that the mounted directories are owned by the Oracle Software Owner User (typically, oracle) and the Oracle Inventory Group (typically, *oinstall*), and that the Oracle Software Owner User has read and write access to the directories.

Example: The following table shows an example configuration.

***Table 18–2 Storage Configuration***

| Volume | Mounted on Host | Mount Point | Comments |
|---|---|---|---|
| VOLOMS1 | oms1-p.example.com | /u01/app/oracle/OMS | Installation of Enterprise Manager on Primary Site OMS1 |
| VOLOMS2 | oms2-p.example.com | /u01/app/oracle/OMS | Installation of Enterprise Manager on Primary Site OMS2 |
| VOLSWLIB | oms1-p.example.com and oms2-p.example.com | /swlib | Software library on Primary Site OMS1 and OMS2 |
| VOLBIP | oms1-p.example.com and oms2-p.example.com | /bip | BIP Shared Storage on Primary Site OMS1 and OMS2 (If BIP is configured.) |

## 18.2.3 Database Considerations

This section provides the recommendations and considerations for setting up Repository databases for Disaster Recovery.

- Oracle recommends creating Real Application Cluster databases on both the production site and standby site.
- The Oracle Data Guard configuration used should be decided based on the data loss requirements of the database as well as the network considerations such as the available bandwidth and latency when compared to the redo generation. Make sure that this is determined correctly before setting up the Oracle Data Guard configuration.
- To enable Data Guard to restart instances during the course of broker operations, a service with a specific name must be statically registered with the local listener of each instance.

- To enable the most effective use of *dgmgrl* for Repository database switchover and failover operations, the TNS aliases for all primary and standby Repository databases must be added to the *tnsnames.ora* file under the ORACLE_HOME of each database instance.
- It is strongly recommended to force Data Guard to perform manual database synchronization whenever middle tier synchronization is performed. This is especially true for components that store configuration data in the metadata repositories.
- Once the connect descriptor is selected based on the recommendations discussed in Section 18.2.3.1, "Considerations Where Oracle Database Versions are Lower than 11g Release 2" and Section 18.2.3.2, "Considerations Where Oracle Database Versions are 11g Release 2 or Higher," run the following command on each OMS at the primary site to configure the connect descriptor.

  ```
  emctl config oms -store_repos_details -repos_conndesc <connect descriptor>
  -repos_user <username>
  ```

  The following usage example follows the connect descriptor recommendation discussed in Section 18.2.3.2.

  ```
  emctl config oms -store_repos_details -repos_conndesc "(DESCRIPTION_LIST=(LOAD_
  BALANCE=off)(FAILOVER=on)(DESCRIPTION=(CONNECT_TIMEOUT=5)(TRANSPORT_CONNECT_
  TIMEOUT=3)(RETRY_COUNT=3)(ADDRESS_LIST=(LOAD_
  BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=primary_cluster_
  scan.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
  NAME=haemrep.example.com)))(DESCRIPTION=(CONNECT_TIMEOUT=5)(TRANSPORT_CONNECT_
  TIMEOUT=3)(RETRY_COUNT=3)(ADDRESS_LIST=(LOAD_
  BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=standby_cluster_
  scan.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_
  NAME=haemrep.example.com))))" -repos_user SYSMAN
  ```

#### 18.2.3.1 Considerations Where Oracle Database Versions are Lower than 11g Release 2

It is strongly recommended to set up aliases for the database host names on both the production and standby sites. This enables seamless switchovers, switchbacks and failovers. For example:

| Site | Repository Host Names | Repository Connect String |
|---|---|---|
| Primary | repos1-p.example.com | (DESCRIPTION=(ADDRESS_LIST=(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=repos1-p.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=repos2-p.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=EMREP))) |
| | repos2-p.example.com | |
| Standby | repos1-s.example.com | (DESCRIPTION=(ADDRESS_LIST=(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=repos1-s.example.com)(PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=repos2-s.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=EMREP))) |
| | repos2-s.example.com | |

In the above example, after a failover or switchover operation, the OMS on the standby site must be switched to use the standby repository connection string. You can avoid changing of connect strings by optionally setting up a host name alias for the repository database hosts. For example:

| Site | Repository Host Names | Host Name Alias |
|---|---|---|
| Primary | repos1-p.example.com | repos1.example.com |
| | repos2-p.example.com | repos2.example.com |
| Standby | repos1-s.example.com | repos1.example.com |
| | repos2-s.example.com | repos2.example.com |

Thus the connect string on each site can be the same, alleviating the need to do a change during failover or switchover.

(DESCRIPTION=(ADDRESS_
LIST=(FAILOVER=ON)(ADDRESS=(PROTOCOL=TCP)(HOST=repos1.example.com)(
PORT=1521))(ADDRESS=(PROTOCOL=TCP)(HOST=repos2.example.com)(PORT=152
1)))(CONNECT_DATA=(SERVICE_NAME=EMREP))).

### 18.2.3.2 Considerations Where Oracle Database Versions are 11g Release 2 or Higher

Oracle Database 11g Release 2 introduces two technologies that together dramatically improve the simplicity of connection string management for Repository databases for Disaster Recovery: Single Client Access Name (SCAN) addresses and role-based database services.

SCAN addresses provide a single address for a RAC cluster, eliminating the need to specify multiple VIP addresses in the connection string. For more information on SCAN addresses, please see the Oracle Clusterware Administration and Deployment Guide.

Role-based database services allow the creation of a database service that will run on a RAC cluster based on the role of the database without requiring the administrator to create and maintain database triggers to manage the database service. With a role-based database service, Oracle Clusterware will automatically start and stop the database service based upon the specified role (Primary or Standby). For more information on role-based database services, please see the Oracle Real Application Clusters Administration and Deployment Guide and the `Client Failover Best Practices for Highly Available Oracle Databases: Oracle Database 12c` technical whitepaper.

Combining these two technologies allows the creation of a Repository connection string that contains a single entry for the primary database and a single entry for the standby database. This connection string can be used from both the primary and standby sites, which removes the need to manually change the connection string during switchover or failover operations.

To create a role-based database service for use in connecting to the repository in a Level 4 MAA configuration, perform commands similar to the following to create the database service on both primary and standby clusters.

Primary cluster:

```
srvctl add service -d emrepa -s haemrep.example.com -l PRIMARY -r
emrepa1,emrepa2
```

Standby cluster:

```
srvctl add service -d emreps -s haemrep.example.com -l PRIMARY -r
emreps1,emreps2
```

Perform the following on a node of the primary cluster to start the service initially.

```
srvctl start service -d emrepa -s haemrep.example.com
```

The role-based database service is now active and will run on whichever cluster hosts the active database.

Oracle recommends the use of a connection string similar to the following in an environment using Oracle Database 11.2, Data Guard, and RAC, replacing the names of the scan addresses for each cluster and the role-based database service name with the appropriate values in your environment:

```
(DESCRIPTION_LIST=(LOAD_BALANCE=off)(FAILOVER=on)(DESCRIPTION=(CONNECT_
TIMEOUT=5)(TRANSPORT_CONNECT_TIMEOUT=3)(RETRY_COUNT=3)(ADDRESS_LIST=(LOAD_
BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=primary-cluster-scan.example.com)(
PORT=1521)))(CONNECT_DATA=(SERVICE_
NAME=haemrep.example.com)))(DESCRIPTION=(CONNECT_TIMEOUT=5)(TRANSPORT_
CONNECT_TIMEOUT=3)(RETRY_COUNT=3)(ADDRESS_LIST=(LOAD_
BALANCE=on)(ADDRESS=(PROTOCOL=TCP)(HOST=standby-cluster-scan.example.com)(
PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=haemrep.example.com))))
```

## 18.2.4 Starting Points

Before setting up the standby site, the administrator must evaluate the starting point of the project. The starting point for designing an Enterprise Manager Cloud Control Disaster Recovery topology is usually one of the following:

- The primary site is already created, standby site is being planned
- The primary site is already created, standby site is already created using the deprecated "Standby WLS Domain" method
- No installation exists, both primary and standby sites are being planned

### 18.2.4.1 The primary site is already created, standby site is being planned

When the starting point is an existing primary site, the OMS installation for the primary site already exist on the file system. Also, the host names, ports, and user accounts are already defined. The following procedure must be used to transform the site and prepare it for Disaster Recovery topology.

1. Review the Network Considerations and plan your host names

   If using option 1, no host name changes are required on the primary site. Prepare your standby site hosts by adding appropriate alias host names.

   If using option 2, change the OMS host name to move your existing OMS installation to use alias host names. Prepare your standby site hosts by adding the appropriate alias host names.

2. Review the Storage Considerations and move your OMS installation to shared storage

   Migrate the primary site to shared storage. See "Migrating an Existing Site to Shared Storage" on page 18-16.

3. Review the Database considerations and plan your repository host names and connect descriptors

To achieve seemless failover/switchover consider if you want to use hostname alias for the repository database. If so, migrate your repository database to use alias hostname.

4. Now that your primary site is ready, use the procedures in ""Setting Up Management Repository Disaster Recovery" on page 18-11 and "Setting Up the OMS, Bi Publisher Shared Storage and Software Library Disaster Recovery" on page 18-13 to complete the DR setup.

#### 18.2.4.2 The primary site is already created, standby site is already created using the deprecated "Standby WLS Domain" method.

1. Use the deleting standby OMS procedure to delete the Standby OMS. See Removing Additional Standby OMS Instances in the *Enterprise Manager Advanced Installation and Configuration Guide*.
2. Use the procedure documented in "The primary site is already created, standby site is being planned" on page 18-10.

#### 18.2.4.3 No installation exists, both primary and standby sites are being planned

When you are designing a new primary site (not using a pre-existing primary site), its easier as the site planning can be done before starting the installation of software.

1. Review the Network Considerations and plan your host names.
2. Review the Storage Considerations and prepare your storage volumes.
3. Review the Database Considerations and prepare your repository host names.
4. Perform your primary site installation using the procedures in Chapter 17, "Enterprise Manager High Availability," taking care to use the correct host names and installing on the shared storage.
5. Now that your primary site is ready, see the following sections for procedures to complete the DR setup.
    - Setting Up Management Repository Disaster Recovery
    - Setting Up the OMS, Bi Publisher Shared Storage and Software Library Disaster Recovery

## 18.3 Setting Up Management Repository Disaster Recovery

The Management Repository should use Data Guard as a Disaster Recovery solution.

### 18.3.1 Configuring a Standby Database for the Management Repository

The following steps describe the procedure for setting up a standby Management Repository database.

1. Prepare Standby Management Repository hosts for Data Guard.

   Install a Management Agent on each of the standby Management Repository hosts. Configure the Management Agents to upload by the SLB on the primary site. Install Grid infrastructure and RAC Database software on the standby Management Repository hosts. The version used must be the same as that on the primary site.

2. Prepare the primary Management Repository database for Data Guard.

If the primary Management Repository database is not already configured, enable archive log mode, setup flash recovery area and enable flashback database on the primary Management Repository database.

> **Note:** Ensure that the database is put into FORCE LOGGING mode to prevent standby database corruption during upgrades.
>
> When the primary Management Repository database is in FORCE LOGGING mode, all database changes are logged except for those in temporary tablespaces and temporary segments. FORCE LOGGING mode ensures that the standby database remains consistent with the primary Management Repository database.

3. Create the Physical Standby Database.

   Use the Enterprise Manager console to set up a physical standby database in the standby environment. The Standby Management Repository database must be a Physical Standby. Logical standby Management Repository databases are not supported.

   The Enterprise Manager console does not support creating a standby RAC database. If the standby database has to be RAC, configure the standby database using a single instance and then use the 'Convert to RAC' option from the Enterprise Manager Console to convert the single instance standby database to RAC. Note that the Convert to RAC option is available for Oracle Database releases 10.2.0.5, 11.1.0.7, and above. Oracle Database release 11.1.0.7 requires patch 8824966 for the Convert to RAC option to work.

   During single instance standby creation, best practice is to create the database files on shared storage, ideally ASM, to facilitate conversion to RAC later.

4. Add Static Service to the Listener.

   To enable Data Guard to restart instances during the course of broker operations, a service with a specific name must be statically registered with the local listener of each instance. The value for the GLOBAL_DBNAME attribute must be set to a concatenation of <db_unique_name>_DGMGRL.<db_domain>. For example, in the LISTENER.ORA file:

   ```
   SID_LIST_LISTENER=(SID_LIST=(SID_DESC=(SID_NAME=sid_name)
   (GLOBAL_DBNAME=db_unique_name_DGMGRL.db_domain)
   (ORACLE_HOME=oracle_home)))
   ```

5. Enable Flashback Database on the Standby Database.

   To allow re-instate of an old primary database as a standby database after a failover, flashback database must be enabled. Hence do so for both the primary and the standby databases.

6. To allow Enterprise Manager to monitor a Physical Standby database (which is typically in a mounted state), specify sysdba monitoring privileges. This can be specified either during the Standby creation wizard itself or post creation by modifying the Monitoring Configuration for the standby database target.

7. Verify the Physical Standby

   Verify the Physical Standby database through the Enterprise Manager Console. Click the Log Switch button on the Data Guard page to switch log and verify that it is received and applied to the standby database.

## 18.4 Setting Up the OMS, Bi Publisher Shared Storage and Software Library Disaster Recovery

The Disaster Recovery solution for a Cloud Control deployment involves installing the Software Library, OMS installation, Agent installation and Oracle inventory on replicated filesystem. This solution can also involve configuring BI Publisher shared storage.

Standby OMSs implemented using Standby WebLogic Domain are still supported but have been deprecated and may be desupported in a future release (see My Oracle Support Note 1563541.1 for details). The recommended method for creating Standby OMSs is to use storage replication as documented in this chapter. Creating standby OMSs using a Standby WebLogic Domain is documented in Appendix I, "Standby OMSs Using Standby WebLogic Domain."

#### Storage Replication Requirements

Your chosen method of storage replication should support the following:

- Snapshots and consistent filesystem copies
- Ability to perform an on-demand replication between sites

### 18.4.1 Management Service Disaster Recovery

1. Ensure that the primary OMS host names are resolvable to the IP addresses of the corresponding standby hosts at the standby site. This can be achieved in either of the following ways:

   - By installing OMSs at the primary site using physical host names and configuring aliases for these host names on the corresponding hosts at the standby site.
   - By installing each OMS using an alias host name that can be configured at both the primary and standby sites.

   Host name resolution at each site can be done using either local resolution (/etc/hosts) or DNS based resolution or a combination of both.

   Example /etc/hosts configurations when OMSs are installed at primary site using primary site physical host names (oms1-p.example.com and oms2-p.example.com):

   **Primary Site**

   ```
   127.0.0.1     localhost.localdomain
   123.1.2.111   oms1-p.example.com  oms1-p #OMS1
   123.1.2.112   oms2-p.example.com  oms2-p #
   ```

   **Standby Site**

   ```
   127.0.0.1     localhost.localdomain
   123.2.2.111   oms1-s.example.com  oms1-s oms1-p.example.com #OMS1
   123.2.2.112   oms2-s.example.com  oms2-s oms2-p.example.com #OMS2
   ```

   Example /etc/hosts configuration when OMSs are installed using alias host names (oms1.example.com and oms2.example.com):

   **Primary Site**

   ```
   127.0.0.1     localhost.localdomain
   123.1.2.111   oms1-p.example.com  oms1-p oms1.example.com #OMS1
   123.1.2.112   oms2-p.example.com  oms2-p oms2.example.com #OMS2
   ```

**Standby Site**

```
127.0.0.1    localhost.localdomain
123.2.2.111  oms1-s.example.com  oms1-s oms1.example.com #OMS1
123.2.2.112  oms2-s.example.com  oms2-s oms2.example.com #OMS2
```

If the network has been configured correctly, a ping of the OMS host name from the primary site should result in a reply from the primary host, and a ping of the OMS host name from the standby site should result in a reply from the standby host.

**Example**

Ping results from primary site (reply from primary site):

```
[oracle@oms1-p ~]$ ping oms1-p.example.com
PING oms1-p.example.com (123.1.2.111) 56(84) bytes of data.
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-p.example.com (123.1.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

Ping results from standby site (reply from standby site)

```
[oracle@oms1-s ~]$ ping oms1-p.example.com
PING oms1-s.example.com (123.2.2.111) 56(84) bytes of data.
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=2 ttl=64 time=0.020 ms
64 bytes from oms1-s.example.com (123.2.2.111): icmp_seq=3 ttl=64 time=0.022 ms
```

2. Ensure that the OMS installation, Agent Installation and Oracle Inventory for each OMS at the primary site is placed on replicated storage. This can either be done by specifying replicated storage during OMS installation or by moving these components onto replicated storage after installation.

   > **Note:** If the components are moved to shared storage after installation they must retain their original pathnames.

3. Configure an application virtual host name in DNS to point to Primary site.

   - If there is a single OMS at the primary site the DNS entry for the application virtual host name should point to this OMS.
   - If there are multiple OMSs at the primary site the DNS entry for the application virtual host name should point to the SLB.
   - This host name should be configured with a short TTL value (30-60 seconds) so that it will not be cached by clients for extended periods.

4. Configure SLB at the standby site (only required if multiple OMSs are required at the standby site). See "Configuring a Load Balancer" on page 17-10 for more information. The SLB pools on the standby site will reference the IP addresses of the standby OMS hosts.

5. Resecure all Agents and OMSs using application virtual host name.

   **Examples**

   *For OMS*

```
emctl secure oms -sysman_pwd <sysman_pwd>
  -reg_pwd <agent_reg_password>
```

```
-host em.example.com
-secure_port 4900
-slb_port 4900
-slb_console_port 443
-console
-lock_upload  -lock_console
```

*For Agent*

```
emctl secure agent -emdWalletSrcUrl https://em.example.com:4901/em
```

6. Configure the storage replication schedule for as frequently as the network infrastructure will allow (minimum every 24 hours).

   > **Note:** Refer to your storage/network documentation to determine a replication schedule that maximizes the resource utilization performance of your network infrastructure.

7. Move HTTP Lock files to local filesystem. See the *Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* for more information.

### 18.4.2 Monitoring Standby OMS Hosts

Monitoring the availability of the standby OMS hosts is necessary to ensure that they are ready for switchover/failover operations. In order to monitor these hosts, Agents should be deployed to local file systems on each standby OMS host.

To avoid conflicts with the components that will be started on the standby site after a switchover/failover, when deploying Agents on the standby OMS hosts the following points should be considered:

- The Agents deployed to the standby OMS hosts should not use the replicated Oracle Inventory.  They should be installed using a local inventory that does not include the replicated OMS and Agent installs.
- The Agents deployed to the standby OMS hosts should be deployed on a different port to that used by the replicated Agents. This will avoid port conflicts when the replicated OMS and Agent are started on the standby OMS host.
- Regardless of which network topology is used (aliases at both sites or aliases only at the standby site), these Agents should be deployed using the physical hostnames of the standby OMS hosts.
- These Agents should be deployed into a separate inventory so that they are kept apart from the inventory used for the OMS installation.
- After deploying Agents to the standby OMS hosts, confirm that all OMS Agents (those installed with alias host names on replicated storage and those installed with physical host names on local storage) are configured consistently with the same time zone. See Changing the Management Agent Time Zone in the Enterprise Manager Cloud Control Administrator's Guide for details on changing the agent time zone.

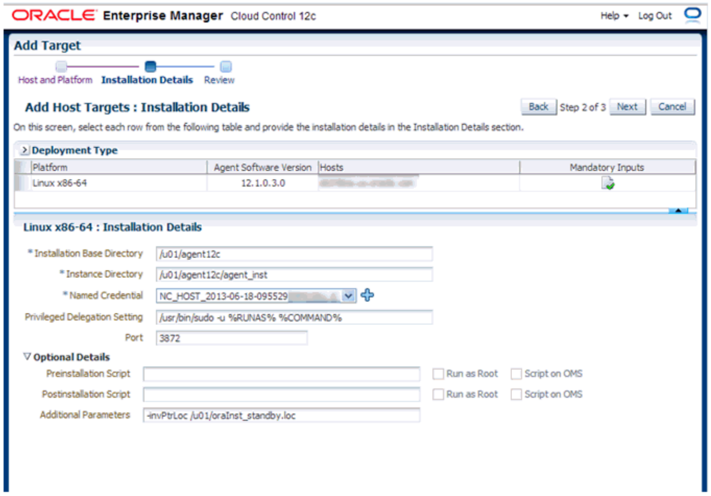
To specify an inventory location for Agent installation, an inventory pointer file can be created and the `-invPtrLoc` flag can be used during installation.

The following example shows an inventory pointer file that specifies the inventory location as */u01/oraInventory_standby*

```
more /u01/oraInst_standby.loc
```

```
inventory_loc=/u01/oraInventory_standby
inst_group=dba
```

The `-invPtrLoc` flag can then be passed during Agent installation.



Add Host Targets : Installation Details

On this screen, select each row from the following table and provide the installation details in the Installation Details section.

Deployment Type

| Platform | Agent Software Version | Hosts | Mandatory Inputs |
|---|---|---|---|
| Linux x86-64 | 12.1.0.3.0 | [redacted] | ✓ |

Linux x86-64 : Installation Details

| | |
|---|---|
| * Installation Base Directory | /u01/agent12c |
| * Instance Directory | /u01/agent12c/agent_inst |
| * Named Credential | NC_HOST_2013-06-18-095529[redacted] |
| Privileged Delegation Setting | /usr/bin/sudo -u %RUNAS% %COMMAND% |
| Port | 3872 |

Optional Details

| | | | |
|---|---|---|---|
| Preinstallation Script | | □ Run as Root | □ Script on OMS |
| Postinstallation Script | | □ Run as Root | □ Script on OMS |
| Additional Parameters | -invPtrLoc /u01/oraInst_standby.loc | | |

## 18.4.3 Software Library Disaster Recovery

1. The Software Library should be located on a file system that is replicated using storage replication. If the Software Library is currently located on another file system it can be migrated using the 'Migrate and Remove' option in the Software Library Administration page.

   See the chapter on *Configuring a Software Library* in the Enterprise Manager Cloud Control Administrator's Guide for more information.

2. Configure the storage replication schedule for as frequently as the network infrastructure as the network infrastructure will allow. Oracle recommends continuous replication to occur every 2 hours (minimum).

## 18.4.4 BI Publisher Shared Storage Disaster Recovery

If BI Publisher has been configured then the BI Publisher shared storage must also participate in the disaster recovery scenarios.

1. The BI Publisher shared storage location should be located on a filesystem that is replicated using storage replication.

2. Configure the storage replication schedule for as frequently as the network infrastructure as the network infrastructure will allow. Oracle recommends continuous replication to occur every 2 hours (minimum).

## 18.4.5 Migrating an Existing Site to Shared Storage

**Note:** You can migrate from your existing site to a shared storage file system even if you want to use Level 4 of the high-availability solution for your existing environment.

- Use file system backups to move existing OMS and agent installations to shared storage.
- Use the following guidelines to migrate from local file system to shared storage
  - All backups must be offline backups, i.e. OMS and agent processes on a host must be shut down completed before backing up and restoring.
  - The backups must be performed as root user and permissions must be preserved.
  - The directory paths for Middleware Home and Instance Home must not change.
  - The migration can be done in a rolling fashion to avoid complete downtime of Cloud Control.
- Use the process documented in "Removing (and Migrating) Software Library Storage Location" to move the software library to shared storage.

## 18.5 Performing Switchover and Failover Operations

Activating the standby site can take place either by using a switchover or a failover. These are used in different situations as described below:

- **Switchover** - A pre-planned role reversal of the primary and standby sites. In a switchover, functionality is transferred from the primary site to a standby site in an orderly, coordinated operation. As such, both sites must be available for a switchover to complete. Switchover is usually performed for testing and validation of Disaster Recovery (DR) scenarios and for planned maintenance activities on the primary infrastructure. A switchover is the preferred method of activating the standby site as the primary.
- **Failover** - Activation of the standby site as the primary site when the original primary site becomes unavailable.

**Note:** If BI Publisher is configured in your environment, and if your disaster recovery approach uses *Standby OMSs using Storage Replication* as discussed in this chapter, BI Publisher will be functional on the standby site when switchover/failover occurs.

**Note:** If an error is encountered unmounting the OMS filesystem as part of a switchover or failover operation, it may be because Oracle Configuration Manager (OCM) is configured and running from the OMS home. If OCM is running, it should be stopped before unmounting the OMS filesystem. To check OCM status, run the following command:

```
<OMS_HOME>/ccr/bin/emCCR status.
```

To stop OCM, run the following command:

```
<OMS_HOME>/ccr/bin/emCCR stop.
```

To start OCM after a switchover or failover, run the following command:

```
<OMS_HOME>/ccr/bin/emCCR start.
```

### 18.5.1 Switchover Procedure

This section describes the steps to switchover to the standby site. The same procedure is applied to switchover in either direction.

1. Shut down all OMS components at the primary site.
2. Shut down all virtual Management Agents at the primary site.
3. Unmount the OMS filesystem and the software library filesystems from OMS hosts at the primary site.
4. Perform on-demand replication of OMS and software library filesystems.

   > **Note:** Refer to your storage documentation for steps required to perform an on-demand replication.

5. Update DNS entry for the application virtual hostname.
6. Switchover Oracle Database using Data Guard switchover.

   Use DGMGRL to perform a switchover to the standby database. The command can be run on the primary site or the standby site. The switchover command verifies the states of the primary database and the standby database, affects switchover of roles, restarts the old primary database, and sets it up as the new standby database.

   ```
   SWITCHOVER TO <standby database name>;
   ```

   Verify the post switchover states. To monitor a standby database completely, the user monitoring the database must have SYSDBA privileges. This privilege is required because the standby database is in a mounted-only state. A best practice is to ensure that the users monitoring the primary and standby databases have SYSDBA privileges for both databases.

   ```
   SHOW CONFIGURATION;
   ```

   ```
   SHOW DATABASE <primary database name>;
   ```

   ```
   SHOW DATABASE <standby database name>;
   ```

7. Perform role reversal of the Software Library and OMS storage (refer to your storage documentation for instructions).
8. Re-enable replication schedules for SWLIB and OMS storage.

   If BI Publisher has been configured, re-enable replication schedules for the BI Publisher shared storage location.

9. Mount OMS and Software Library filesystems on OMS hosts at Standby site.

   If BI publisher has been configured, mount the BI Publisher shared storage filesystems on OMS hosts at the standby site.

10. Start the first OMS Admin Server at the standby site.

    > **Note:** This step is not required if using a connection string that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services as described in Section 18.2.3, "Database Considerations."

11. Point OMS to new Primary Repository Database using the following command:

```
emctl config oms -store_repos_details -repos_conndesc <connect descriptor>
-repos_user <username>
```

### Example

```
emctl config oms -store_repos_details -repos_conndesc '(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=newscan.domain)(PORT=1521)))(CONNECT_
DATA=(SERVICE_NAME=emreps.domain)))' -repos_user SYSMAN
```

> **Note:** This step is not required if using a connection string that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services as described in Section 18.2.3, "Database Considerations."

This step should be repeated on each OMS.

12. Start the OMSs at the standby site.
13. Start the Management Agents at the standby site using the following command:

    ```
    emctl start agent
    ```

14. Relocate Management Services and Repository target using the following command:

    ```
    emctl config emrep -agent <agent name> -conn_desc <repository connection>
    ```

    The Management Services and Management Repository target is monitored by a Management Agent on one of the Management Services on the primary site. To ensure that the target is monitored after switchover/failover, relocate the target to a Management Agent on the standby site by running the following command on one of the Management Service standby sites.

    > **Note:** This step is not required if the following two conditions are met:
    >
    > - Using a Repository Connect Descriptor that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services. Under this condition, the connection descriptor does not need to be updated in order to monitor the Management Services and Management Repository target.
    > - Management Services and Management Repository target is monitored by a Management Agent installed on replicated storage using an Alias Host Name. Under this condition, the same agent will now be running on the standby site; therefore a different Agent does not need to be configured.

15. Update the URI for the WebLogic Admin Console from within Cloud Control.

    Navigate to the target homepage for *GCDomain*. From the **WebLogic Domain** menu, select **Target Setup**, and then **Monitoring Configuration**.

### 18.5.2 Failover Procedure

This section describes the steps to failover to the standby site, recover the Enterprise Manager application state by resynchronizing the Management Repository database with all Management Agents, and finally enabling the original primary database

1. Shut down all OMS components at the primary site if running.
2. Shut down all virtual agents at primary site if running.
3. Unmount OMS and Software Library filesystems from OMS hosts at primary site.

   If BI Publisher has been configured, umount the BI Publisher shared storage filesystem from OMS hosts at the primary site.
4. Perform on-demand replication of the OMS and Software Library file systems. (Depending on the type of failure encountered this may not be possible.) If BI Publisher has been configured, also perform an on-demand replication of the BI Publisher shared storage filesystem.

   **Note:** Refer to your storage documentation for steps required to perform an on-demand replication.

5. Update the DNS entry for the application virtual hostname.
6. Failover Oracle Database using Data Guard failover.
7. Perform role reversal of Software Library and OMS storage.
8. Re-enable replication schedules for SWLIB and OMS storage
9. Mount the OMS and Software Library filesystems on OMS hosts at the standby site
10. Start the first OMS Admin Server.

    **Note:** This step is not required if the following two conditions are met:

    1. Using a Repository Connect Descriptor that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services.
    2. Running in Data Guard Maximum Protection or Maximum Availability level as there is no data loss on failover.

11. Modify the OMS connect descriptor to point to the new Primary Repository Database.

    ```
    emctl config oms -store_repos_details -repos_conndesc <connect descriptor>
    -repos_user <username>
    ```

    **Example**

    ```
    emctl config oms -store_repos_details -repos_conndesc '(DESCRIPTION=(ADDRESS_
    LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=newscan.domain)(PORT=1521)))(CONNECT_
    DATA=(SERVICE_NAME=emreps.domain)))' -repos_user SYSMAN
    ```

> **Note:** This step is not required if using a Repository Connect Descriptor that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services.

This step should be repeated on each OMS.

12. Perform a Repository Resynchronization to resync the Agents with the new Primary database.

    Skip this step if you are running in Data Guard Maximum Protection or Maximum Availability level as there is no data loss on failover. However, if there is data loss, synchronize the new primary database with all Management Agents.

    On any one Management Service on the standby site, run the following command:

    ```
    emctl resync repos -full -name "<name for recovery action>"
    ```

    This command submits a resync job that is executed on each Management Agent when the Management Services on the standby site are brought up.

13. Start the Agents at the standby site.

14. Start the OMSs at the standby site.

15. Modify Management Services and Repository target connect descriptor.

    From the **Setup** menu, select **Manage Cloud Control** and then **Health Overview**. The Management Services and Repository page displays. From the **OMS and Repository** menu, select **Target Setup** and then **Monitoring Configuration**.

    The Repository Connect Descriptor should be modified to connect to the database that is currently active.

    > **Note:** This step is not required if using a Repository Connect Descriptor that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services

16. Update the URI for the WebLogic Admin Console from within Cloud Control.

    Navigate to the target homepage for *GCDomain*. From the **WebLogic Domain** menu, select **Target Setup**, and then **Monitoring Configuration**.

## 18.6 Keeping the Standby Site in Sync with the Primary

The standby site will be kept in sync with the primary automatically through the combination of Data Guard and storage replication.

The administrator should ensure that an on-demand replication to the standby site takes place before and after the following operations on the OMS or the agent:

- Plug-in deployment/undeployment, or existing plug-in upgrade
- Upgrade
- Patch
- emctl commands (other than lifecycle verbs (start/stop/status oms))
- Configuration of ADP/JVMD/BI Publisher

---

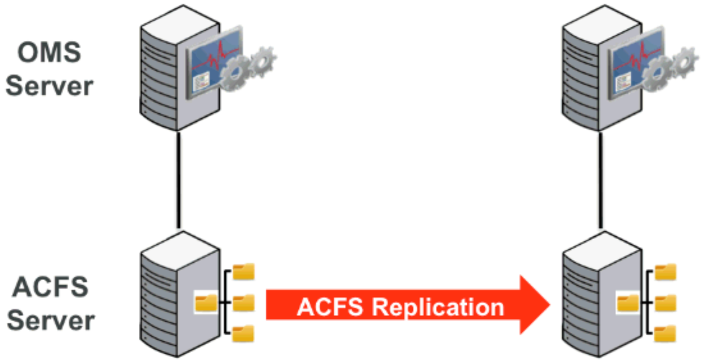
**Note:** Refer to your storage documentation for steps required to perform an on-demand replication.

---

## 18.7 Disaster Recovery Solution with ACFS Replication

Automatic Storage Management Cluster File System (ACFS) replication enables replication of an ACFS file system across a network to a remote site. This capability is useful for providing disaster recovery capability. The following diagram shows how this feature can be leveraged to provide disaster recovery for an Enterprise Manager installation.

***Figure 18–2 ACFS Replication***



### Configuring ACFS Replication

1. Install Grid Infrastructure and create an ACFS Server.

   ACFS storage replication requires Grid Infrastructure to be installed for a Cluster, but it can also be installed using a single node (one node cluster).

2. Create an ACFS file system on the ACFS server (created in step 1) to be used for the OMS installation and Software Library.

3. Export the ACFS file system using NFS.

   Disable root squash for the ACFS mount point, otherwise root.sh will not run after Enterprise Manager is installed on the client.

4. Mount the file system on a different node (to be used for the OMS) using the following options:

   ```
   nfs rw,bg,hard,nointr,rsize=131072,wsize=131072,tcp,vers=3,
   timeo=300,actimeo=120
   ```

5. Install Enterprise Manager on the NFS (ACFS) file system.

6. Create a second ACFS server (one node cluster) with another ACFS file system to be used as a standby.

7. Establish ACFS replication between the primary and standby ACFS servers:

   1. On the standby server, initiate the replication using the following command:

      ```
      /sbin/acfsutil repl init standby -p
      ```

      by the root user.

  2. Verify that the standby file system is initiated using the following command:

     ```
     /sbin/acfsutil repl info
     ```

  3. On the primary server, initiate replication using the following command:

     ```
     /sbin/acfsutil repl init primary -s
     ```

  4. Verify that the primary file system is initiated using the following command:

     ```
     /sbin/acfsutil repl info -c
     ```

8. Switch over from the primary server to the standby. Refer to Section 18.5.1, "Switchover Procedure" for explicit instructions on performing the switchover operation with the following modifications:

   **At step 4**:

   Perform on-demand replication of the OMS and Software Library file systems by performing the following:

   Run *ACFS sync* for the Enterprise Manager file system from the primary server using the following command:

   ```
   /sbin/asfsutil repl sync apply
   ```

   **At step 7:**

   Perform role reversal of the Software Library and OMS storage by performing the following:

   Terminate ACFS replication using the following command:

   ```
   /sbin/acfsutil repl terminate standby
   ```

   To reconfigure ACFS replication, follow the instructions listed above in this section in step 7 *Establish ACFS replication between the primary and standby ACFS servers*.

19

# Backing Up and Recovering Enterprise Manager

As the monitoring and management framework for your ecosystem, an important part of your high availability strategy is to ensure Enterprise Manager is regularly backed up so that it can be restored in the event of failure.

This chapter covers the following topics:

## 19.1 Backing Up Your Deployment

Although Enterprise Manager functions as a single entity, technically, it is built on a distributed, multi-tier software architecture composed of the following software components:

- Oracle Management Services (OMS)
- Management Agent
- Management Repository
- Software Library

Each component, being uniquely different in composition and function, requires different approaches to backup and recovery. For this reason, the backup strategies are discussed on a per-tier basis in this chapter. For an overview of Enterprise Manager architecture, refer to the Oracle® Enterprise Manager Cloud Control Basic Installation Guide.

## 19.2 Software Library Backup

The software library is a centralized media storage for Enterprise Manager software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. The software library is an essential part of Enterprise Manager framework and is required by many Enterprise

Manager features in order to function properly. The software library storage locations should be backed up periodically using file system backup. Oracle recommends the backup be performed at a frequency of 1 to 24 hours.

## 19.3 Management Repository Backup

The Management Repository is the 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. Because it is configured in an Oracle Database, the backup and recovery strategies for the Management Repository are essentially the same as those for the Oracle Database. Backup procedures for the database are well established standards and can be implemented using the RMAN backup utility, which can be accessed via the Cloud Control console.

### Management Respository Backup

Oracle recommends using High Availability Best Practices for protecting the Management Repository database against unplanned outages. As such, use the following standard database backup strategies.

- Database should be in *archivelog* mode. Not running the repository database in *archivelog* mode leaves the database vulnerable to being in an unrecoverable condition after a media failure.
- Perform regular hot backups with RMAN using the *Recommended Backup Strategy* option via the Cloud Control console. Other utilities such as DataGuard and RAC can also be used as part of a comprehensive HA and data protection strategy typically implemented with HA levels 3 and 4. For more information about the various HA levels, see Chapter 16.4, "Implementing High Availability Levels."

Adhering to these strategies will create a full backup and then create incremental backups on each subsequent run. The incremental changes will then be rolled up into the baseline, creating a new full backup baseline.

Using the *Recommended Backup Strategy* also takes advantage of the capabilities of Enterprise Manager to execute the backups: Jobs will be automatically scheduled through the Job sub-system of Enterprise Manager. The history of the backups will then be available for review and the status of the backup will be displayed on the repository database target home page. This backup job along with archiving and flashback technologies will provide a restore point in the event of the loss of any part of the repository. This type of backup, along with archive and online logs, allows the repository to be recovered to the last completed transaction.

You can view when the last repository backup occurred on the Management Services and Repository Overview page under the Repository details section.

A thorough summary of how to configure backups using Enterprise Manager is available in the *Oracle Database 2 Day DBA* guide. For additional information on Database high availability best practices, review the *Oracle Database High Availability Best Practices* documentation.

## 19.4 Oracle Management Service Backup

The Oracle Management Service (OMS) orchestrates with Management Agents 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 Web interface for the Enterprise Manager console.

### Backing Up the OMS

The OMS is generally stateless. Some configuration data is stored on the OMS file system.

A snapshot of OMS configuration can be taken using the `emctl exportconfig oms` command.

```
$ <OMS_HOME>/bin/emctl exportconfig oms [-sysman_pwd <sysman password>]
[-dir <backup dir>] Specify directory to store backup file
[-keep_host] Specify this parameter if the OMS was installed using a virtual
hostname (using
ORACLE_HOSTNAME=<virtual_hostname>)
```

Running *exportconfig* captures a snapshot of the OMS at a given point in time, thus allowing you to back up the most recent OMS configuration on a regular basis. *exportconfig* should always be run on the OMS running the WebLogic Admin Server. If required, the most recent snapshot can then be restored on a fresh OMS installation on the same or different host.

Backup strategies for the OMS components are as follows:

- **Software Homes**

  Composed of Fusion Middleware Home, the OMS Oracle Home and the WebTier (OHS) Oracle Home and multiple Management Plug-in Oracle Homes.

  Software Homes changes when patches or patchsets are applied or updates are applied through the new Self Update feature. For this reason, filesystem-level backups should be taken after each patch/patchset application or application of updates through Self Update. You should back up the Oracle inventory files along with the Software Homes and save the output of opatch lsinventory –detail to make it easy to determine which patches are applied to the backed up Oracle Homes.

  > **Note:** If you do not have filesystem-level backups, you can also reinstall the software homes using the “Installing Software Only” install method.
  >
  > **Important**: The location of the OMS Oracle Home must be the same for all OMS instances in your Cloud Control deployment.

- **Instance Home**

  The gc_inst directory, composed of WebLogic Server, OMS and web tier configuration files.

  The Instance Home can be backed up using the `emctl exportconfig oms` command.

- **Administration Server**

  The Administration Server operates as the central control entity for the configuration of the entire OMS instance domain. The Administration Server is an integral part of the first OMS installed in your Cloud Control deployment and shares the Software Homes and Instance Home.

  The Administration Server is backed up at the same time as the Instance Home, the `emctl exportconfig oms` command (only run on the first OMS with the Administration Server).

## 19.5 Management Agent Backup

The Management Agent is an integral software component that is deployed on each monitored host. It is responsible for monitoring all the targets running on those hosts, communicating that information to the middle-tier OMS and managing and maintaining the hosts and its targets.

#### Backing Up Management Agents

There are no special considerations for backing up Management Agents. As a best practice, reference Management Agent installs should be maintained for different platforms and kept up-to-date in terms of customizations in the emd.properties file and patches applied. Use Deployment options from the Cloud Control console to install and maintain reference Agent installs.

If a Management Agent is lost, it should be reinstalled by cloning from a reference install.

## 19.6 Recovery of Failed Enterprise Manager Components

Recovering Enterprise Manager means restoring any of the three fundamental components of the Enterprise Manager architecture.

- Management Repository
- Management Service
- Management Agent
- Software Library

### 19.6.1 Repository Recovery

Recovery of the Repository database must be performed using RMAN since Cloud Control will not be available when the repository database is down. There are two recovery cases to consider:

- **Full Recovery**: No special consideration is required for Enterprise Manager.
- **Point-in-Time/Incomplete Recovery**: Recovered repository may be out of sync with Agents because of lost transactions. In this situation, some metrics may show up incorrectly in the Cloud Control console unless the repository is synchronized with the latest state available on the Agents.

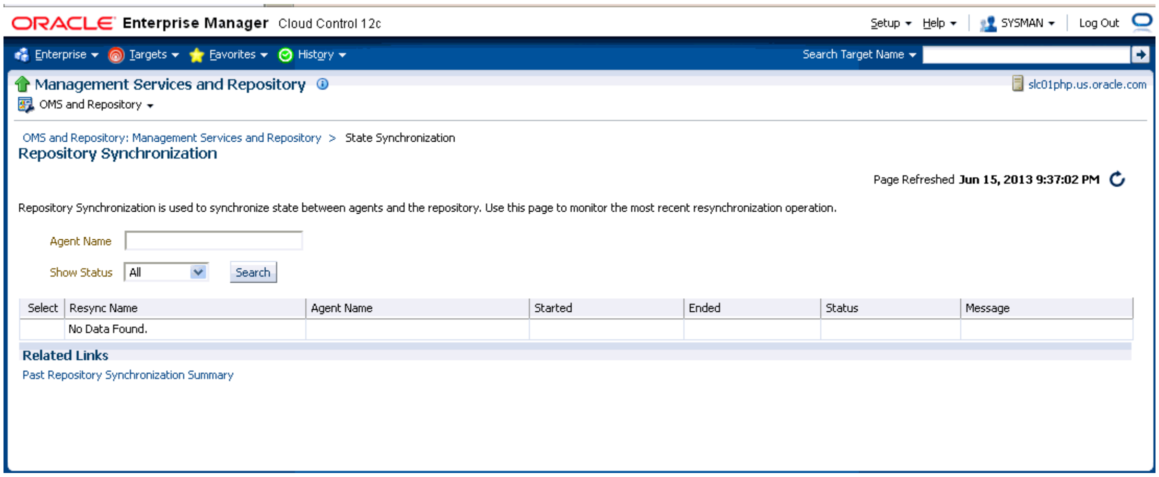
A repository resync feature allows you to automate the process of synchronizing the Enterprise Manager repository with the latest state available on the Management Agents.

To resynchronize the repository with the Management Agents, you use Enterprise Manager command-line utility (emctl) `resync repos` command:

```
emctl resync repos -full -name "<descriptive name for the operation>"
```

You must run this command from the OMS Oracle Home AFTER restoring the Management Repository, but BEFORE starting the OMS. After submitting the command, start up all OMS instances and monitor the progress of repository resychronization from the Enterprise Manager console's Repository Resynchronization page, as shown in the following figure.

*Figure 19–1 Repository Synchronization Page*


ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
SYSMAN
Log Out
Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
OMS and Repository
slc01php.us.oracle.com
OMS and Repository: Management Services and Repository > State Synchronization
Search

Repository Synchronization

Page Refreshed **Jun 15, 2013 9:37:02 PM**

Repository Synchronization is used to synchronize state between agents and the repository. Use this page to monitor the most recent resynchronization operation.

Agent Name

Show Status All

| Select | Resync Name | Agent Name | Started | Ended | Status | Message |
|---|---|---|---|---|---|---|
| | No Data Found. | | | | | |

**Related Links**

Past Repository Synchronization Summary

Management Repository recovery is complete when the resynchronization jobs complete on all Management Agents.

Oracle strongly recommends that the Management Repository database be run in *archivelog* mode so that in case of failure, the database can be recovered to the latest transaction. If the database cannot be recovered to the last transaction, *Repository Synchronization* can be used to restore monitoring capabilities for targets that existed when the last backup was taken. Actions taken after the backup will not be recovered automatically. Some examples of actions that will not be recovered automatically by *Repository Synchronization* are:

- Incident Rules
- Preferred Credentials
- Groups, Services, Systems
- Jobs/Deployment Procedures
- Custom Reports
- New Agents

## 19.6.2 Recovery Scenarios

A prerequisite for repository (or any database) recovery is to have a valid, consistent backup of the repository. Using Enterprise Manager to automate the backup process ensures regular, up-to-date backups are always available if repository recovery is ever required. Recovery Manager (RMAN) is a utility that backs up, restores, and recovers Oracle Databases. The RMAN recovery job syntax should be saved to a safe location. This allows you to perform a complete recovery of the Enterprise Manager repository database. In its simplest form, the syntax appears as follows:

```
run {
restore database;
recover database;
}
```

Actual syntax will vary in length and complexity depending on your environment. For more information on extracting syntax from an RMAN backup and recovery job, or using RMAN in general, see the *Oracle Database Backup and Recovery Advanced User's Guide*.

The following scenarios illustrate various repository recovery situations along with the recovery steps.

#### 19.6.2.1 Full Recovery on the Same Host

Repository database is running in *archivelog* mode. Recent backup, archive log files and redo logs are available. The repository database disk crashes. All datafiles and control files are lost.

**Resolution:**

1. Stop all OMS instances using `emctl stop oms -all`.
2. Recover the database using RMAN
3. Bring the site up using the command `emctl start oms` on all OMS instances.
4. Verify that the site is fully operational.

#### 19.6.2.2 Incomplete Recovery on the Same Host

Repository database is running in *noarchivelog* mode. Full offline backup is available. The repository database disk crashes. All datafiles and control files are lost.

**Resolution:**

1. Stop the OMS instances using `emctl stop oms -all`.
2. Recover the database using RMAN.
3. Initiate Repository Resync using `emctl resync repos -full -name` "<resync name>" from one of the OMS Oracle Home.
4. Start the OMS instances using `emctl start oms`.
5. Log in to Cloud Control. From the Setup menu, select Manage Cloud Control, and then Health Overview. The Management Services and Repository page displays.
6. From the **OMS and Repository** menu, select R**epository Synchronization**.
7. Verify that the site is fully operational.

#### 19.6.2.3 Full Recovery on a Different Host

The Management Repository database is running on host "A" in *archivelog* mode. Recent backup, archive log files and redo logs are available. The repository database crashes. All datafiles and control files are lost.

**Resolution:**

1. Stop the OMS instances using the command `emctl stop oms`.
2. Recover the database using RMAN on a different host (host "B").
3. Correct the connect descriptor for the repository by running the following command on each OMS.

   ```
   $emctl config oms -store_repos_details -repos_conndesc <connect descriptor>
   -repos_user sysman
   ```

4. Stop the OMS using the following command:

   ```
   emctl stop oms -all
   ```

5. Start the OMS instances using the command

   ```
   emctl start oms.
   ```

6. Relocate the Management Repository database target to the Agent running on host "B" by running the following command from the OMS:

   ```
   $emctl config repos -host <hostB> -oh <OH of repository on hostB>  -conn_desc
   "<TNS connect descriptor>"
   ```

   > **Note:** This command can only be used to relocate the repository database under the following conditions:
   >
   > - An Agent is already running on this machine.
   > - No database on host "B" has been discovered.

7. Change the monitoring configuration for the OMS and Repository target: by running the following command from the OMS:

   ```
   $emctl config emrep -conn_desc "<TNS connect descriptor>"
   ```

8. Verify that the site is fully operational.

#### 19.6.2.4 Incomplete Recovery on a Different Host

The Management Repository database is running on host "A" in *noarchivelog* mode. Full offline backup is available. Host "A" is lost due to hardware failure. All datafiles and control files are lost.

**Resolution:**

1. Stop the OMS instances using `emctl stop oms`.
2. Recover the database using RMAN on a different host (host "B").
3. Correct the connect descriptor for the repository in credential store.

   ```
   $emctl config oms -store_repos_details -repos_conndesc <connect descriptor>
   -repos_user sysman
   ```

   This commands will prompt you to stop and start the oms.
4. Initiate Repository Resync:

   ```
   $emctl resync repos -full -name "<resync name>"
   ```

   from one of the OMS Oracle Homes.
5. Start the OMS using the command `emctl start oms.`
6. Run the command to relocate the repository database target to the Management Agent running on host "B":

   ```
   $emctl config repos -agent <agent on host B> -host <hostB> -oh <OH of
   repository on hostB> -conn_desc "<TNS connect descriptor>"
   ```

7. Run the command to change monitoring configuration for the OMS and Repository target:

   ```
   emctl config emrep -conn_desc "<TNS connect descriptor>"
   ```

8. Log in to Cloud Control. From the Setup menu, select Manage Cloud Control, and then select Health Overview.

9. From  the OMS and Repository menu, select **Repository Synchronization.** Monitor the status of resync jobs. Resubmit failed jobs, if any, after fixing the error mentioned.

10. Verify that the site is fully operational.

## 19.6.3 Recovering the OMS

If an Oracle Management Service instance is lost, recovering it essentially consists of three steps: Recovering the Software Homes, configuring the Instance Home and recovering the Software Library if configured on same host as Enterprise Manager.

### 19.6.3.1 Recovering the Software Homes

When restoring on the same host, the software homes can be restored from filesystem backup. In case a backup does not exist, or if installing to a different host, the Software Homes can be reconstructed using the “Install Software Only" option from the Cloud Control software distribution. Care should be taken to select and install **ALL** Management Plug-ins that existed in your environment prior to crash.

1. Connect to the Management Repository as SYSMAN and run the following SQL query to retrieve a list of installed plug-ins:

   ```
   SELECT epv.display_name, epv.plugin_id, epv.version, epv.rev_version,
   decode(su.aru_file, null, 'Media/External',
   'https://updates.oracle.com/Orion/Services/download/'||aru_file||'?aru='||aru_
   id||chr(38)||'patch_file='||aru_file) URL
   FROM em_plugin_version epv, em_current_deployed_plugin ecp, em_su_entities su
   WHERE epv.plugin_type NOT IN ('BUILT_IN_TARGET_TYPE', 'INSTALL_HOME')
   AND ecp.dest_type='2'
   AND epv.plugin_version_id = ecp.plugin_version_id
   AND su.entity_id = epv.su_entity_id;
   ```

   The above query returns the list of plug-ins along with the URLs to download them if they were downloaded through self update. If plug-ins are present in the install media or are third party plug-ins not available through Self Update, the URLs are marked as "Media/Unknown".

2. Download the additional plug-ins, if any, from the URLs in the list returned by the query in step 1 and place them in a single directory. Change the filename extension from *.zip* to *.opar*.

3. Invoke the installer and select the Software-Only option to install the Middleware and OMS Oracle Home.

4. To install the required plug-ins, you must then run the PluginInstall.sh script (OMS_HOME/sysman/install/PluginInstall.sh) with the -pluginLocation <absolute path to plugin dir> specifying the path to the directory where downloaded plugins are kept. When asked to select plugins, make sure you select the same plugins as were listed in the SQL query.

   **Note:** Recovery will fail if all required plug-ins have not been installed.

After the software-only mode, all patches that were installed prior to the crash must be re-applied. Assuming the Management Repository is intact, the post-scripts that run SQL against the repository can be skipped as the repository already has those patches applied.

As stated earlier, the location of the OMS Oracle Home is fixed and cannot be changed. Hence, ensure that the OMS Oracle Home is restored in the same location that was used previously.

#### 19.6.3.2 Recreating the OMS

Once the Software Homes are recovered, the instance home can be reconstructed using the omsca command in recovery mode:

```
omsca recover -as -ms -nostart -backup_file <exportconfig file>
```

Use the export file generated by the `emctl exportconfig` command shown in the previous section.

### 19.6.4 OMS Recovery Scenarios

The following scenarios illustrate various OMS recovery situations along with the recovery steps.

---

**Important:** A prerequisite for OMS recovery is to have recent, valid OMS configuration backups available. Oracle recommends that you back up the OMS using the `emctl exportconfig oms` command whenever an OMS configuration change is made. This command must be run on the primary OMS running the WebLogic AdminServer.

Alternatively, you can run this command on a regular basis using the Enterprise Manager Job system.

Each of the following scenarios cover the recovery of the Software homes using either a filesystem backup (when available and only when recovering to the same host) or using the Software only option from the installer. In either case, the best practice is to recover the instance home (gc_inst) using the omsca recover command, rather than from a filesystem backup. This guarantees that the instance home is valid and up to date.

---

#### 19.6.4.1 Single OMS, No Server Load Balancer (SLB), OMS Restored on the same Host

Site hosts a single OMS. No SLB is present. The OMS configuration was backed up using the `emctl exportconfig oms` command on the primary OMS running the AdminServer. The OMS Oracle Home is lost.

**Resolution:**

1. Perform cleanup on failed OMS host.

   Make sure there are no processes still running from the Middleware home using a command similar to the following:

   ```
   ps -ef | grep -i -P "(Middleware|gc_inst)" | grep -v grep | awk '{print $2}' |
   xargs kill -9
   ```

---

**Note:** Change *Middleware|gc_inst* to strings that match your own middleware and instance homes.

---

If recovering the software homes using the software only install method, first de-install the existing Oracle Homes using the Cloud Control software distribution installer. This is required even if the software homes are no longer available as it is necessary to remove any record of the lost Oracle Homes from the Oracle inventory.

If they exist, remove the 'Middleware' and 'gc_inst' directories.

2. Ensure that software library locations are still accessible and valid. If a Software library is accessible but corrupt, it will affect OMSCA recovery.

3. Restore the Software Homes. See Section 19.6.3.1, "Recovering the Software Homes" for more information.

   If restoring from a filesystem backup, delete the following file:

   ```
   OMS_HOME/sysman/config/emInstanceMapping.properties
   ```

   In addition, delete any `gc_inst` directories that may have been restored, if they exist.

4. Run omsca in recovery mode specifying the export file taken earlier to configure the OMS:

   ```
   <OMS_HOME>/bin/omsca recover -as -ms -nostart -backup_file <exportconfig file>
   ```

   **Note:** The -backup_file to be passed must be the latest file generated from emctl exportconfig oms command.

5. Start the OMS.

   ```
   OMS_HOME/bin/emctl start oms
   ```

6. Recover the Agent (if necessary).

   If the Management Agent Software Home was recovered along with the OMS Software Homes (as is likely in a single OMS install recovery where the Management Agent and agent_inst directories are commonly under the Middleware home), the Management Agent instance directory should be recreated to ensure consistency between the Management Agent and OMS.

   1. Remove the agent_inst directory if it was restored from backup

   2. Use `agentDeploy.sh` to configure the agent:

      ```
      <AGENT_BASE_DIR>/core/12.1.0.4.0/sysman/install/agentDeploy.sh AGENT_BASE_
      DIR=<AGENT_BASE_DIR> AGENT_INSTANCE_HOME=<AGENT_INSTANCE_HOME> ORACLE_
      HOSTNAME=<AGENT_HOSTNAME> AGENT_PORT=<AGENT_PORT> -configOnly OMS_HOST=<oms
      host> EM_UPLOAD_PORT=<OMS_UPLOAD_PORT> AGENT_REGISTRATION_PASSWORD=<REG_
      PASSWORD>
      ```

      If the Management Agent configuration fails, see `<AGENT_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent_<time_stamp>.log`

   3. The OMS may block the Management Agent. Synchronize the agent with repository using the following command:

      ```
      <OMS_HOME>/bin/emcli resyncAgent -agent=<agent target name
      myhost.example.com:3872>
      ```

If the Management Agent software home was not recovered along with the OMS but the Agent still needs to be recovered, follow the instructions in section *Agent Reinstall Using the Same Port*.

> **Note:** This is only likely to be needed in the case where a filesystem recovery has been performed that did not include a backup of the Agent software homes. If the OMS software homes were recovered using the Software only install method, this step will not be required because a Software only install installs an Agent software home under the Middleware home.

7. Verify that the site is fully operational.

#### 19.6.4.2 Single OMS, No SLB, OMS Restored on a Different Host

Site hosts a single OMS. The OMS is running on host "A." No SLB is present. The OMS configuration was backed up using the `emctl exportconfig oms` command. Host "A" is lost.

**Resolution:**

1. Ensure that software library locations are accessible from “Host B”.
2. Restore the software homes on “Host B”. See Section 19.6.3.1, "Recovering the Software Homes" for more information.
3. Run omsca in recovery mode specifying the export file taken earlier to configure the OMS:

```
<OMS_HOME>/bin/omsca recover -as -ms -nostart -backup_file <exportconfig file>
```

> **Note:** The -backup_file to be passed must be the latest file generated from emctl exportconfig oms command.

4. Start the OMS.

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

An agent is installed as part of the Software only install and needs to be configured using the agentDeploy.sh command:

5. Configure the Agent.

```
<AGENT_BASE_DIR>/core/12.1.0.4.0/sysman/install/agentDeploy.sh AGENT_BASE_
DIR=<AGENT_BASE_DIR> AGENT_INSTANCE_HOME=<AGENT_INSTANCE_HOME> ORACLE_
HOSTNAME=<AGENT_HOSTNAME> AGENT_PORT=<AGENT_PORT> -configOnly OMS_HOST=<oms
host> EM_UPLOAD_PORT=<OMS_UPLOAD_PORT> AGENT_REGISTRATION_PASSWORD=<REG_
PASSWORD>
```

If the Management Agent configuration fails, see `<AGENT_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent_<time_stamp>.log`

6. Relocate the oracle_emrep target to the Management Agent of the new OMS host using the following commands:

```
<OMS_HOME>/bin/emcli login -username=sysman
<OMS_HOME>/bin/emcli sync
<OMS_HOME>/bin/emctl config emrep -agent <agent on host "B", e.g
myNewOMSHost.example.com:3872>
```

> **Note:** If you run `emctl config emrep -agent` and set the flag `-ignore_timeskew`, there may a loss of monitoring data as the availability of monitored targets may be affected when the Management Services and Repository target is moved to the new Agent.

7. In the Cloud Control console, locate the 'WebLogic Domain' target for the Cloud Control Domain. Go to 'Monitoring Credentials' and update the adminserver host to host B. Then do a Refresh Weblogic Domain to reconfigure the domain with new hosts.

8. Locate duplicate targets from the Management Services and Repository Overview page of the Enterprise Manager console. Click the Duplicate Targets link to access the Duplicate Targets page. To resolve duplicate target errors, the duplicate target must be renamed on the conflicting Agent. Relocate duplicate targets from Agent "A" to Agent "B".

9. Change the OMS to which all Management Agents point and then resecure all Agents.

   Because the new machine is using a different hostname from the one originally hosting the OMS, all Agents in your monitored environment must be told where to find the new OMS. On each Management Agent, run the following command:

   ```
   <AGENT_INST_DIR>/bin/emctl secure agent -emdWalletSrcUrl "http://hostB:<http_
   port>/em"
   ```

10. Assuming the original OMS host is no longer in use, remove the Host target (including all remaining monitored targets) from Cloud Control by selecting the host on the Targets > Hosts page and clicking ‘Remove’. You will be presented with an error that informs you to remove all monitored targets first. Remove those targets then repeat the step to remove the Host target successfully.

11. Verify that the site is fully operational.

#### 19.6.4.3 Single OMS, No SLB, OMS Restored on a Different Host using the Original Hostname

Site hosts a single OMS. The OMS is running on Host "A." No SLB is present. The OMS configuration was backed up using the `emctl exportconfig oms` command. Host "A" is lost. Recovery is to be performed on “Host B” but retaining the use of “Hostname A”.

**Resolution:**

1. Ensure that the software library location is accessible from Host "B".

2. Restore the software homes on Host B. See Section 19.6.3.1, "Recovering the Software Homes" for more information.

3. Modify the network configuration such that “Host B” also responds to hostname of “Host A”. Specific instructions on how to configure this are beyond the scope of this document. However, some general configuration suggestions are:

   Modify your DNS server such that both “Hostname B” and “Hostname A” network addresses resolve to the physical IP of “Host B”.

Multi-home “Host B”. Configure an additional IP on “Host B” for the IP address that “Hostname A” resolves to. For example, on “Host B” run the following commands:

```
ifconfig eth0:1 <IP assigned to “Hostname A”> netmask <netmask>
/sbin/arping -q -U -c 3 -I eth0 <IP of HostA>
```

4. Run omsca in recovery mode specifying the export file taken earlier to configure the OMS:

```
<OMS_HOME>/bin/omsca recover -as –ms -nostart –backup_file <exportconfig file>
-AS_HOST <hostA> -EM_INSTANCE_HOST <hostA>
```

**Note:** The -backup_file to be passed must be the latest file generated from emctl exportconfig oms command.

5. Start the OMS.

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

6. Configure the agent.

   An agent is installed as part of the Software only install and needs to be configured using the agentDeploy.sh command:

```
<AGENT_HOME>/core/12.1.0.0.0/sysman/install/agentDeploy.sh AGENT_BASE_
DIR=<AGENT_BASE_DIR> AGENT_INSTANCE_HOME=<AGENT_INSTANCE_HOME> ORACLE_
HOSTNAME=<AGENT_HOSTNAME> AGENT_PORT=<AGENT_PORT> -configOnly OMS_HOST=<oms
host> EM_UPLOAD_PORT=<OMS_UPLOAD_PORT> AGENT_REGISTRATION_PASSWORD=<REG_
PASSWORD>
```

   The OMS may block the Management Agent. Synchronize the Agent with repository using the following command:

```
<OMS_HOME>/bin/emcli resyncAgent -agent=<agent target name
myhost.example.com:3872>
```

7. Verify that the site is fully operational.

#### 19.6.4.4 Multiple OMS, Server Load Balancer, Primary OMS Recovered on the Same Host

Site hosts multiple OMS instances. All OMS instances are fronted by a Server Load Balancer. OMS configuration backed up using the `emctl exportconfig oms` command on the primary OMS running the WebLogic AdminServer. The primary OMS is lost.

**Resolution:**

1. Perform a cleanup on the failed OMS host.

   Make sure there are no processes still running from the Middleware home using a command similar to the following:

```
ps -ef | grep -i -P "(Middleware|gc_inst)" | grep -v grep | awk '{print $2}' |
xargs kill -9
```

---

**Note:** Change *Middleware*|*gc_inst* to strings that match your own middleware and instance homes.

---

If recovering the software homes using the software only install method, first de-install the existing Oracle Homes using the Cloud Control software distribution installer. This is required even if the software homes are no longer available as it is necessary to remove any record of the lost Oracle Homes from the Oracle inventory.

If they exist, remove the 'Middleware' and 'gc_inst' directories.

2. Ensure that software library locations are still accessible.
3. Restore the software homes. See Section 19.6.3.1, "Recovering the Software Homes" for more information.

   If restoring from a filesystem backup, delete the following file:

   <OMS_HOME>/sysman/config/emInstanceMapping.properties
4. Run omsca in recovery mode specifying the export file taken earlier to configure the OMS:

   ```
   <OMS_HOME>/bin/omsca recover -as -ms -nostart -backup_file <exportconfig file>
   ```

   ---

   **Note:** The -backup_file to be passed must be the latest file generated from emctl exportconfig oms command.

   ---
5. Start the OMS.

   ```
   <OMS_HOME>/bin/emctl start oms
   ```
6. Recover the Management Agent.

   If the Management Agent software home was recovered along with the OMS software homes (as is likely in a Primary OMS install recovery where the agent and agent_inst directories are commonly under the Middleware home), the Management Agent instance directory should be recreated to ensure consistency between the Management Agent and OMS.

   1. Remove the agent_inst directory if it was restored from backup.
   2. Use agentDeploy.sh to configure the Management Agent:

      ```
      <AGENT_HOME>/core/12.1.0.0.0/sysman/install/agentDeploy.sh AGENT_BASE_
      DIR=<AGENT_BASE_DIR> AGENT_INSTANCE_HOME=<AGENT_INSTANCE_HOME> ORACLE_
      HOSTNAME=<AGENT_HOSTNAME> AGENT_PORT=<AGENT_PORT> -configOnly OMS_HOST=<oms
      host> EM_UPLOAD_PORT=<OMS_UPLOAD_PORT> AGENT_REGISTRATION_PASSWORD=<REG_
      PASSWORD>
      ```
   3. The OMS may block the Management Agent. Synchronize the Agent with the repository using the following command:

      ```
      <OMS_HOME>/bin/emcli resyncAgent -agent=<agent target name e.g.
      myhost.example.com:3872>
      ```

   If the Management Agent software home was not recovered along with the OMS but the Management Agent still needs to be recovered, follow the instructions in section *Agent Reinstall Using the Same Port.*

> **Note:** This is only likely to be needed in the case where a filesystem recovery has been performed that did not include a backup of the Management Agent software homes. If the OMS software homes were recovered using the Software only install method, this step will not be required because a Software only install installs an Management Agent software home under the Middleware home.

7. Verify that the site is fully operational.

#### 19.6.4.5 Multiple OMS, Server Load Balancer Configured, Primary OMS Recovered on a Different Host

Site hosts multiple OMS instances. OMS instances fronted by a Server Load Balancer. OMS Configuration backed up using emctl exportconfig oms command. Primary OMS on host "A" is lost and needs to be recovered on Host "B".

1. If necessary, perform cleanup on failed OMS host.

   Make sure there are no processes still running from the Middleware home using a command similar to the following:

   ```
   ps -ef | grep -i -P "(Middleware|gc_inst)" | grep -v grep | awk '{print $2}' |
   xargs kill -9
   ```

2. Ensure that software library locations are accessible from “Host B”.

3. Restore the software homes on “Host B”. See Section 19.6.3.1, "Recovering the Software Homes" for more information.

4. Run omsca in recovery mode specifying the export file taken earlier to configure the OMS:

   ```
   <OMS_HOME>/bin/omsca recover -as -ms -nostart -backup_file <exportconfig file>
   ```

   > **Note:** The -backup_file to be passed must be the latest file generated from emctl exportconfig oms command.

5. Start the OMS.

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

6. Configure the Management Agent.

   An Agent is installed as part of the Software only install and needs to be configured using the agentDeploy.sh command:

   ```
   <AGENT_HOME>/core/12.1.0.0.0/sysman/install/agentDeploy.sh AGENT_BASE_
   DIR=<AGENT_BASE_DIR> AGENT_INSTANCE_HOME=<AGENT_INSTANCE_HOME> ORACLE_
   HOSTNAME=<AGENT_HOSTNAME> AGENT_PORT=<AGENT_PORT> -configOnly OMS_HOST=<oms
   host> EM_UPLOAD_PORT=<OMS_UPLOAD_PORT> AGENT_REGISTRATION_PASSWORD=<REG_
   PASSWORD>
   ```

   If any non-default plug-ins were previously deployed on the failed agent, they must be re-deployed after recovery of the Agent. Note that this pertains to plug-ins that existed on the recovering Agent before it failed (that are not related to the OMS/Repository target), and any plug-ins for additional targets the OMS Agent happened to be also monitoring. To re-deploy the plug-ins , run the following command (not as part of config emrep, or manually):

```
emcli relocate_targets
```

7. Additional Management Services, if any, must be re-enrolled with the Admin Server that is now running on host B. To re-enroll the Management Services, run the following command on each additional OMS:

   ```
   <OMS-HOME>/bin/emctl enroll oms -as_host <new Admin Server host, i.e.
   host B> -as_port <admin server port>
   ```

8. Add the new OMS to the SLB virtual server pools and remove the old OMS.
9. Relocate the oracle_emrep target to the Management Agent of the new OMS host using the following commands:

   ```
   <OMS_HOME>/bin/emcli sync
   <OMS_HOME>/bin/emctl config emrep -agent <agent on host "B", e.g
   myNewOMSHost.example.com:3872>
   ```

   **Note:** If you run `emctl config emrep -agent` and set the flag `-ignore_timeskew`, there may a loss of monitoring data as the availability of monitored targets may be affected when the Management Services and Repository target is moved to the new Agent.

10. In the Cloud Control console, locate the 'WebLogic Domain' target for the Cloud Control Domain. Go to 'Monitoring Credentials' and update the adminserver host to host B. Then do a Refresh Weblogic Domain to reconfigure the domain with new hosts.
11. Locate duplicate targets from the Management Services and Repository Overview page of the Enterprise Manager console. Click the Duplicate Targets link to access the Duplicate Targets page. To resolve duplicate target errors, the duplicate target must be renamed on the conflicting Management Agent. Relocate duplicate targets from Management Agent "A" to Management Agent "B".
12. Assuming the original OMS host is no longer in use, remove the Host target (including all remaining monitored targets) from Cloud Control by selecting the host on the Targets > Hosts page and clicking ‘Remove’. You will be presented with an error that informs you to remove all monitored targets first. Remove those targets then repeat the step to remove the Host target successfully.
13. All other OMSs in the system must re-enroll with the newly recovered OMS using the following command:

    ```
    emctl enroll oms -as_host <new OMS host> -as_port <port #, default 7101>
    ```

14. Verify that the site is fully operational.

#### 19.6.4.6 Multiple OMS, SLB configured, additional OMS recovered on same or different host

Multiple OMS site where the OMS instances are fronted by an SLB. OMS configuration backed up using the `emctl exportconfig oms` command on the first OMS. Additional OMS is lost and needs to be recovered on the same or a different host.

1. If recovering to the same host, ensure cleanup of the failed OMS has been performed:

   Make sure there are no processes still running from the Middleware home using a command similar to the following:

```
ps -ef | grep -i -P "(Middleware|gc_inst)" | grep -v grep | awk '{print $2}' |
xargs kill -9
```

First de-install the existing Oracle Homes using the Cloud Control software distribution installer. This is required even if the software homes are no longer available as it is necessary to remove any record of the lost Oracle Homes from the Oracle inventory.

If they exist, remove the *Middleware* and *gc_inst* directories.

2. Ensure that shared software library locations are accessible.
3. Install an Management Agent on the required host (same or different as the case may be).
4. For procedures on installing additional Oracle Management Services, see the chapter on Installing Additional Oracle Management Services in Silent Mode in the Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.
5. Verify that the site is fully operational.

## 19.6.5 Recovering the Software Library

If the software library is lost, it should be restored from the last available backup. After restoring the backup, the following commands must be run to verify and re-import missing entities:

1. `emcli verify_swlib` - This command verifies the accessibility of the software library storage locations and reports if entities are missing any files on the file system.
2. `emcli reimport_swlib_metadata` - This command re-imports all Oracle-supplied entities that are shipped along with the product. If you have a recent backup, this should not be required. Run `emcli reimport_swlib_metadata` if the `emcli verify_swlib` command reports Oracle-owned entities with files missing from the filesystem.
3. `emcli verify_updates` - This command verifies whether entities downloaded by Self Update are missing from the software library. For each missing entity, the command also displays the instructions to re-import the entitiy into the software library.

## 19.6.6 Recovering Management Agents

If a Management Agent is lost, it should be reinstalled by cloning from a reference install. Cloning from a reference install is often the fastest way to recover a Management Agent install because it is not necessary to track and reapply customizations and patches. Care should be taken to reinstall the Management Agent using the same port. Using the Enterprise Manager's Management Agent *Resynchronization* feature, a reinstalled Management Agent can be reconfigured using target information present in the Management Repository.

**Note:** Management Agent resynchronization can only be performed by Enterprise Manager Super Administrators.

When the Management Agent is reinstalled using the same port, the OMS detects that it has been re-installed and blocks it temporarily to prevent the auto-discovered targets in the re-installed Management Agent from overwriting previous customizations.

---

**Blocked Management Agents:** This is a condition in which the OMS rejects all heartbeat or upload requests from the blocked Management Agent. Hence, a blocked Agent will not be able to upload any alerts or metric data to the OMS. However, blocked Management Agents continue to collect monitoring data.

An Agent can be blocked due to one of several conditions. They are:

- Enterprise Manager has detected that the Agent has been restored from a backup.
- Plug-ins on the Agent do not match the records in the Management Repository.
- The user has manually blocked the Agent.

For the first two conditions, an Agent resynchronization is required to unblock the agent by clearing the states on the Agent and pushing plug-ins from the Management Repository.

---

The Management Agent can be resynchronized and unblocked from the Management Agent homepage by using the `emcli resyncAgent <agent target name>` command. Resynchronization pushes all targets from the Management Repository to the Management Agent and then unblocks the Agent.

## 19.6.7 Management Agent Recovery Scenarios

The following scenarios illustrate various Management Agent recovery situations along with the recovery steps. The Management Agent resynchronization feature requires that a reinstalled Management Agent use the same port and location as the previous Management Agent that crashed.

---

**Note:** Management Agent resynchronization can only be performed by Enterprise Manager Super Administrators.

---

### 19.6.7.1 Management Agent Reinstall Using the Same Port

A Management Agent is monitoring multiple targets. The Agent installation is lost.

1. De-install the Agent Oracle Home using the Oracle Universal Installer.

---

**Note:** This step is necessary in order to clean up the inventory.

---

2. Install a new Management Agent or use the Management Agent clone option to reinstall the Management Agent though Enterprise Manager. Specify the same port that was used by the crashed Agent. The location of the install must be same as the previous install.

   The OMS detects that the Management Agent has been re-installed and blocks the Management Agent.

3. Initiate Management Agent Resynchronization using the following command:

```
emcli resyncAgent -agent="Agent Host:Port"
```

All targets in the Management Repository are pushed to the new Management Agent. The Agent is instructed to clear backlogged files and then do a clearstate. The Agent is then unblocked.

4. Reconfigure User-defined Metrics if the location of User-defined Metric scripts have changed.

5. Verify that the Management Agent is operational and all target configurations have been restored using the following emctl commands:

   ```
   emctl status agent
   emctl upload agent
   ```

   There should be no errors and no XML files in the backlog.

#### 19.6.7.2 Management Agent Restore from Filesystem Backup

A single Management Agent is monitoring multiple targets. File system backup for the Agent Oracle Home exists. The Agent install is lost.

1. Restore the Management Agent from the filesystem backup then start the Management Agent.

   The OMS detects that the Management Agent has been restored from backup and blocks the Management Agent.

2. Initiate Management Agent Resynchronization using the following command:

   ```
   emcli resyncAgent -agent="Agent Host:Port"
   ```

   All targets in the Management Repository are pushed to the new Management Agent. The Agent is instructed to clear backlogged files and performs a clearstate. The Management Agent is unblocked.

3. Verify that the Management Agent is functional and all target configurations have been restored using the following emctl commands:

   ```
   emctl status agent
   emctl upload agent
   ```

   There should be no errors and no XML files in the backlog.

## 19.7 Recovering from a Simultaneous OMS-Management Repository Failure

When both OMS and Management Repository fail simultaneously, the recovery situation becomes more complex depending upon factors such as whether the OMS and Management Repository recovery has to be performed on the same or different host, or whether there are multiple OMS instances fronted by an SLB. In general, the order of recovery for this type of compound failure should be Management Repository first, followed by OMS instances following the steps outlined in the appropriate recovery scenarios discussed earlier. The following scenarios illustrate two OMS-Management Repository failures and the requisite recovery steps.

### 19.7.1 Collapsed Configuration: Incomplete Management Repository Recovery, Primary OMS on the Same Host

Management Repository and the primary OMS are installed on same host (host "A"). The Management Repository database is running in noarchivelog mode. Full cold backup is available. A recent OMS backup file exists ( emctl exportconfig oms). The Management Repository, OMS and the Management Agent crash.

1. Follow the Management Repository recovery procedure shown in Incomplete Recovery on the Same Host with the following exception:

   Since the OMS OracleHome is not available and Management Repository resynchronization has to be initiated before starting an OMS against the restored Management Repository, submit "resync" via the following PL/SQL block. Log into the Management Repository as SYSMAN using SQLplus and run:

   ```
   begin emd_maintenance.full_repository_resync('<resync name>'); end;
   ```

2. Follow the OMS recovery procedure shown in Section 19.6.4.1, "Single OMS, No Server Load Balancer (SLB), OMS Restored on the same Host."
3. Verify that the site is fully operational.

### 19.7.2 Distributed Configuration: Incomplete Management Repository Recovery, Primary OMS and additional OMS on Different Hosts, SLB Configured

The Management Repository, primary OMS, and additional OMS all reside on the different hosts. The Management Repository database was running in noarchivelog mode. OMS backup file from a recent backup exists (emctl exportconfig oms). Full cold backup of the database exists. All three hosts are lost.

1. Follow the Management Repository recovery procedure shown in Section 19.6.2.2, "Incomplete Recovery on the Same Host." with the following exception:

   Since OMS Oracle Home is not yet available and Management Repository resync has to be initiated before starting an OMS against the restored Management Repository, submit resync via the following PL/SQL block. Log into the Management Repository as SYSMAN using SQLplus and run the following:

   ```
   begin emd_maintenance.full_repository_resync('resync name'); end;
   ```

2. Follow the OMS recovery procedure shown in Section 19.6.4.5, "Multiple OMS, Server Load Balancer Configured, Primary OMS Recovered on a Different Host" with the following exception:

   Override the Management Repository connect description present in the backup file by passing the additional omsca parameter:

   ```
   -REPOS_CONN_STR <restored repos descriptor>
   ```

   This needs to be added along with other parameters listed in Section 19.6.4.5, "Multiple OMS, Server Load Balancer Configured, Primary OMS Recovered on a Different Host."

3. Follow the OMS recovery procedure shown in Section 19.6.4.6, "Multiple OMS, SLB configured, additional OMS recovered on same or different host."
4. Verify that the site is fully operational.

# 20 Running Multiple BI Publisher Servers

---

**Note:** If you have upgraded from a prior release of Enterprise Manager that was configured for multiple BI Publisher Servers, it is necessary to repeat the steps in this chapter. Please note that the existing shared storage, from the prior release of Enterprise Manager, will continue to be used.

---

---

**Note:** If you are running Enterprise Manager in a High Availability environment (behind a Server Load Balancer (SLB)) be aware of the following caveats:

- If you have configured a primary BI Publisher server, on the primary OMS system, then you need to insure that BI Publisher is also configured and running on the additional OMS systems that you have added. See the following sections in this chapter, on the different paths to configure additional BI Publisher servers on additional OMS systems.
- If an Enterprise Manager system has a running OMS, and the corresponding BI Publisher server is not running, then running BI Publisher reports from Enterprise Manager will fail some of the time. In this case, either bring up BI Publisher on that system using:

  ```
  emctl start oms -bip_only
  ```

  or bring down that OMS on that system using:

  ```
  emctl stop oms -all
  ```

---

Enterprise Manager 12c Release 4 (12.1.0.4) or greater allows you to configure Enterprise Manager to work with multiple BI Publisher servers.

---

**Important:** Older versions of Enterprise Manager do not support the BI Publisher multi-server environment described in this chapter.

---

This chapter covers the following:

- Introduction BI Publisher Multi-Server Environments
- Reconfiguring BI Publisher to Use a Shared Storage Device

- Adding Secondary BI Publisher Server(s)
- Confirming Correct Operation of Secondary BI Publisher Servers on an Additional OMS System
- Confirming Details of the Secondary BI Publisher Server

---

**Note:** BI Publisher software is automatically installed on all systems where Enterprise Manager 12.1.0.4 or greater was installed. This chapter covers steps to configure the BI Publisher Server to run on these systems.

---

## 20.1 Introduction BI Publisher Multi-Server Environments

Enterprise Manager 12c Release 4 (12.1.0.4) or greater permits multiple BI Publisher servers to be integrated with Enterprise Manager.

Before additional BI Publisher servers can be added, the first BI Publisher must be configured. Refer to the chapter *Integrating BI Publisher with Enterprise Manager* in the Enterprise Manager Advanced Installation and Configuration guide for more information. This "first" BI Publisher server, called "BIP", will be referred to as the primary BI Publisher server.

---

**Note:** BI Publisher multi-server deployments are not supported in Enterprise Manager 12c Release 4 (12.1.0.4) or greater on Microsoft Windows platforms.

---

BI Publisher stores all configuration data and report definitions in an Operating System file system-based repository. Therefore, in order to support multiple BI Publisher servers, read/write permissions must be available to this file system from all the OMS systems in which you are to run BI Publisher. This is accomplished using standard Network file system technologies.

If you are implementing multiple BI Publisher servers you must also make the BI Publisher shared storage file system highly available. This file system needs to be periodically backed up (for example, daily or hourly) using standard Operating System commands, or a professional backup solution. It is also highly recommended that a high availability disk solution be used such as a RAID (Redundant Array of Inexpensive Drives) storage device. At least RAID 1 (redundancy) should be used. Other RAID levels (such as RAID5 and RAID0+1) are also acceptable. **Do not use RAID0,** as this is intended for speed, and not redundancy. RAID1 is not by itself a backup solution. Raid 1 protects against disk drive failures, but periodic backups are still required. If the files stored on this network storage device are lost, all BI Publisher servers (both primary and secondary) will no longer be functional.

Once the RAID storage device is configured, it must be mounted on all systems where you intend to install BI Publisher. Standard Operating System commands can be used for this mount (for example, NFS). Two directories on the storage device must be dedicated for BI Publisher files. These are known as the "Cluster Volume" and "Config Volume".

**Note:** The space requirements for configuring BI Publisher shared storage depends on the amount of space required for storing the report catalog and associated management information.

At install time, the BI Publisher repository uses approximately 400 MB of storage. Initially, 10 G should be made available for the BI Publisher shared storage. This space requirement increases over a period of time as you install additional Enterprise Manager plug-ins and create more reports. Hence, you should ensure that this storage can easily be extended in future.

Before additional BI Publisher servers are added to Enterprise Manager, BI Publisher needs to be reconfigured to use this shared storage device. This is accomplished by running the following the command on the primary OMS system:

```
emctl config oms -bip_shared_storage -config_volume <vol1> -cluster_volume <vol2>
```

Once the primary BI Publisher server is configured, and shared storage has been configured, there are several paths that can be taken to enable secondary BI Publisher server(s), on additional OMS systems:

- Using the standard "Add an Oracle Management Service" provisioning job. If this provisioning job is run after the primary BI Publisher server is configured, then the additional OMS system will automatically be configured with a secondary BI Publisher server.

  **Note:** If the primary BI Publisher server is configured, the "Add an Oracle Management Service" provisioning job will not be available until BI Publisher is reconfigured to use the shared storage device.

- If the "Add and Oracle Management Service" provisioning job has already been run, or an additional OMS system has been configured, a secondary BI Publisher can be added to an existing additional OMS system using the command:

  ```
  configureBIP -addBIP
  ```

  This command should be run on the system where the additional OMS resides.

### Determining BI Publisher Shared Storage Locations

The BI Publisher shared storage locations are stored as Enterprise Manager OMS properties. You can query for the shared storage locations using the following emctl commands:

```
emctl get property -name
oracle.sysman.core.eml.ip.bip.SharedStorageConfigVolume

emctl get property -name
oracle.sysman.core.eml.ip.bip.SharedStorageClusterVolume
```

**Example**:

```
-bash-3.2$ emctl get property -name
oracle.sysman.core.eml.ip.bip.SharedStorageConfigVolume

Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
SYSMAN password:
```

```
Value for property oracle.sysman.core.eml.ip.bip.SharedStorageConfigVolume at
Global level is /oracle/BIP/config
```

## 20.2 Reconfiguring BI Publisher to Use a Shared Storage Device

> **Important:** If you decide to use the Unix Network File System (NFS) for the BI Publisher shared storage, do not use NFS volumes that are managed by the NFS automounter as it typically mounts the */net* directory (non-fixed mount point). Instead, use NFS mounts that use a fixed mount point. For example: */oracle/em/BIP*.

As broadly outlined above, in order to support multiple BI Publisher servers, the following command must be run:

```
emctl config oms -bip_shared_storage -config_volume <vol1> -cluster_volume <vol2>
```

Be sure to keep the storage location for these volumes (for example, vol1 and vol2 shown in the previous section) available. Do not delete these files.

This command will prompt for the WebLogic Administration Server password as well as the Repository User (SYSMAN) Password.

The command executes the following steps:

1. The supplied credentials are validated.
2. Certain pre-requisite tests are run. These include:
   - The two volumes must not be the same as the previously configured shared storage volumes (if any).
   - The two volumes must be distinct
   - The file system mount points for the two volumes must exist.
   - The two volumes must be completely empty.
   - The two volumes must be writable.
3. The BI Publisher server on the local system (the primary BI Publisher server named "BIP") is stopped.
4. The existing BI Publisher file system-based repository, which was installed when the primary BI Publisher was configured, is copied to the Configuration Volume (-config_volume).
5. The primary BI Publisher server, named "BIP", is reconfigured to use WebLogic JMS Queues and WebLogic Persistence Stores (used by the BI Publisher scheduler) that are stored in the Cluster Volume (-cluster_volume).
6. The BI Publisher scheduler is reconfigured to support multiple BI Publisher servers and to use the new locations discussed previously.
7. The values for the two volumes are stored as OMS properties in the Enteprise Manager repository database.
8. The primary BI Publisher is configured to point at the new Configuration Volume.
9. BI Publisher is started.
10. An overall status is displayed.

The following example shows output generated by running the `emctl config oms -bip_shared_storage` command:

```
$ emctl config oms -bip_shared_storage -config_volume /BIP_STORAGE/config
-cluster_volume /BIP_STORAGE/cluster
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Enter Admin User's Password :
Enter Enterprise Manager Root (SYSMAN) Password :
Stopping BI Publisher Server...
BI Publisher Server Successfully Stopped
BI Publisher Server is Down
Copying The BI Publisher repository from the location '...........gc_inst/user_
projects/domains/GCDomain/config/bipublisher/repository' to the location '/BIP_
STORAGE/config/bipublisher/repository'. This can take some time.  Do not interrupt
this command while it is running.
Copied BI Publisher repository to the location '/BIP_
STORAGE/config/bipublisher/repository'
Configuring BI Publisher server named 'BIP' for use in a High Availability
environment. This operation can take some time. Do not interrupt this command
while it is running.
Updating BI Publisher Scheduler configuration ...
Updating BI Publisher shared storage properties ...
The BI Publisher properties have been updated.
The BI Publisher storage for configuration data is in the location '/BIP_
STORAGE/config'
The BI Publisher storage for cluster data is '/BIP_STORAGE/cluster'
BI Publisher has been configured to point to the BI Publisher repository in the
location '/BIP_STORAGE/config'
Starting BI Publisher Server ...
BI Publisher Server Successfully Started
BI Publisher Server is Up
BI Publisher storage has been configured for the BI Publisher server named 'BIP'
running at the URL: https://em.example.com:9702/xmlpserver
Overall result of operations: SUCCESS
```

## 20.3 Adding Secondary BI Publisher Server(s)

As discussed earlier, there are two methods to configure additional BI Publisher servers. The method used will depend on when the primary BI Publisher server is configured, in relation to when the additional OMS server(s) is created using the *Add an OMS* provisioning job (or other means). The following paths illustrate these methods:

### Path A

Install Enterprise Manager

1. Configure the primary BI Publisher Server using *configureBIP* or *configureBIP -upgrade*.
2. Configure BI Publisher shared storage using *emctl config oms -bip_shared_storage*
3. Add OMS using the *Add OMS provisioning job*

   A secondary BI Publisher server is automatically configured along with the additional OMS system.

### Path B

Install Enterprise Manager

1. Add OMS's using *Add OMS provisioning job* or other means, such as a software-only install.
2. Configure primary BI Publisher server, using *configureBIP* or *configureBIP -upgrade*
3. Configure BI Publisher shared storage using *emctl config oms -bip_shared_storage*
4. Configure additional BI Publisher servers using *configureBIP -addBIP* on the additional OMS system where you wish to run multiple BI Publisher servers.

> **Note:** In order to run the *configureBIP -addBIP* command, the OMS for the current system must be up and running. This can be verified by running the *emctl status oms* command as shown in the following example:
>
> ```
> $ emctl status oms
> Oracle Enterprise Manager Cloud Control 12c Release 4
> Copyright (c) 1996, 2015 Oracle Corporation.  All rights reserved.
> WebTier is Up
> Oracle Management Server is Up
> ```

As these two paths illustrate, you can see the necessary prerequisite to adding secondary BI Publisher server(s), depending on when you decide to configure the primary BI Publisher server.

## 20.3.1 Path A - Configuring a Secondary BI Publisher Server Automatically using the "add OMS Provisioning" Job

If you are planning on building an Enterprise Manager HA installation that will leverage the reporting capabilities of BI Publisher, then path A will be more straightforward. All additional OMS systems that are added will automatically get secondary BI Publisher servers.

### 20.3.1.1 Configuring the Primary BI Publishser Server

See the Advanced Installation and Configuration Guide " Integrating BI Publisher with Enterprise Manager".

### 20.3.1.2 Reconfiguring BI Publisher to Use Shared Storage

After the primary BI Publisher server is installed, and you have verified it is operating correctly (as detailed in this chapter) you can proceed to reconfigure BI Publisher to use shared storage. See "Reconfiguring BI Publisher to Use a Shared Storage Device" on page 20-4.

### 20.3.1.3 Adding an Additional OMS System and Automatically Configuring a Secondary BI Publisher Server

Once the BI Publisher shared storage is configured, the "add OMS Provisioning job" will be aware of the configured BI Publisher server. All that will be required is to enter the HTTP and HTTPS ports to use, on the additional OMS system, for the secondary BI Publisher server. The "add OMS provisioning job" performs pre-requisite steps to insure tha the BI Publisher shared storage has been configured. In the event of failure in automatically configuring the secondary BI Publisher server, you can fallback to Path B.

### 20.3.2 Path B: Configuring Secondary BI Publisher Server(s) after Additional OMS Systems have already been added

If the Enterprise Manager topology already includes additional OMS systems, and the primary BI Publisher server has not yet been configured, there are additional steps to follow to enable the primary BI Publisher server and one or more steps to configure secondary BI Publisher server(s) on additional OMS system(s).

#### 20.3.2.1 Configuring primary BI Publisher Server

See the "Integrating BI Publisher with Enterprise Manager" in the Enterprise Manager Advanced Installation and Configuration Guide.

#### 20.3.2.2 Reconfiguring BI Publisher to Use Shared Storage

After the primary BI Publisher server is installed (and you have verified it operates correctly as documented above) you can proceed to reconfigure BI Publisher to use shared storage.

#### 20.3.2.3 Configuring a Secondary BI Publisher server(s)

For each additional OMS system on which you are also going to run a secondary BI Publisher server, the "configureBIP -addBIP" command must be run.

> **Note:** This command is run on the system that hosts the additional OMS system, and not the system on which the primary OMS system resides.

The following example lists command output when configuring a secondary BI Publisher server on an additional OMS system.

```
$ configureBIP -addBIP
Configuring BI Publisher Version "11.1.1.7.0" to work with Enterprise Manager
Logging started at /oracle/Middleware/oms/cfgtoollogs/bip/bipca_
20140221125351.log.
A new BI Publisher server is going to be added.
Do You really want to add a BI Publisher server (Y|N):y
Enter sysdba user name (sys):
Enter sysdba user password:
Enter Administration Server user password:
Configuring BI Publisher in Oracle Home located in /oracle/Middleware/Oracle_BI1
...
Enter an integer between 9701 and 49152 for the BI Publisher HTTP server port.
(9701):
Enter an integer between 9702 and 49152 for the BI Publisher HTTPS server port.
(9702):
Configuring BI publisher on additional OMS system.  This operation can take some
time. Do not interrupt this command while it is running...
Locking Enterprise Manager ...
OMS Console is locked. Access the console over HTTPS ports.
Restart OMS.
Restarting Enterprise Manager ...
Stopping Enterprise Manager, this can take some time  ...
Starting Enterprise Manager. This operation can take some time. Do not interrupt
this command while it is running.
OMS Started Successfully
Successfully configured additional BI Publisher server.
```

## 20.4 Confirming Correct Operation of Secondary BI Publisher Servers on an Additional OMS System

Regardless of whether Path A or B is chosen to configure a secondary BI Publisher server, the "emctl status oms" command can be used to confirm successful configuration.

```
$ emctl status oms
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
WebTier is Up
Oracle Management Server is Up
BI Publisher Server is Up
```

## 20.5 Confirming Details of the Secondary BI Publisher Server

To obtain information about secondary BI Publisher servers, run the following command

```
emctl status oms -details
```

Notice that secondary BI Publisher servers have the server name "BIPx", where "x" matches the server number of the OMS (for example, EMGC_OMS2 : BIP2, EMGC_OMS3 : BIP3).

```
$ emctl status oms -details
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host        : em.example.com
HTTP Console Port          : 7788
HTTPS Console Port         : 7799
HTTP Upload Port           : 4889
HTTPS Upload Port          : 4900
EM Instance Home           : /oracle/gc_inst/em/EMGC_OMS2
OMS Log Directory Location : /oracle/gc_inst/em/EMGC_OMS2/sysman/log
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is locked.
Active CA ID: 1
Console URL: https://em.example.com:7799/em
Upload URL: https://em.example.com:4900/empbs/upload

WLS Domain Information
Domain Name            : GCDomain
Admin Server Host      : emas.example.com
Admin Server HTTPS Port: 7101

Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS2
Oracle Management Server Instance Host: em.example.com
WebTier is Up
Oracle Management Server is Up

BI Publisher Server is Up
BI Publisher Server named 'BIP2' running at local URL:
https://em.example.com:7799/xmlpserver
BI Publisher Server Logs: /oracle/gc_inst/user_
projects/domains/GCDomain/servers/BIP2/logs/
BI Publisher Log        : /oracle/gc_inst/user_
```

```
projects/domains/GCDomain/servers/BIP2/logs/bipublisher/bipublisher.log
```

# Part VII

## Deinstallation

In particular, this part contains the following chapters:

# 21

# Deinstalling Enterprise Manager (Single and Multi-OMS Environments)

This chapter describes how you can deinstall an entire Enterprise Manager system, and also how you can remove the entries of an Oracle Management Service (OMS) from the Oracle Management Repository (Management Repository) in case you lost the host where the OMS was running.

In particular, this chapter covers the following:

- Deinstalling Enterprise Manager
- Deinstalling or Undeploying Only Plug-ins from the OMS
- Deleting OMS Entries from the Management Repository

## 21.1 Deinstalling Enterprise Manager

This section covers the following subsections to describe how you can deinstall the entire Enterprise Manager system—single OMS environment or multi-OMS environment with additional Oracle Management Services (OMS).

- Prerequisites for Deinstalling Only the OMS and Retaining the Management Repository
- Prerequisites for Deinstalling the Entire Enterprise Manager System
- Procedure for Deinstalling Enterprise Manager
- After Deinstalling Enterprise Manager

**Caution: Make sure you meet the prerequisites before deinstalling the software. Make sure you follow the flow or sequence outlined in this chapter. For example, make sure you drop the schemas as described in the prerequisites section before deinstalling the software binaries. Do NOT change the order of instructions.**

### 21.1.1 Prerequisites for Deinstalling Only the OMS and Retaining the Management Repository

Before you deinstall Enterprise Manager, meet the following prerequisites:

1. *(For Multi-OMS Environment, and if Oracle BI Publisher is Configured on Additional OMS Instances)* Stop all the Oracle BI Publisher managed servers, which are running on the additional OMS hosts, by running the following command from the OMS home on each host:

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

**Note:** If any Oracle BI Publisher managed server fails to stop, then manually kill it using the operating system commands.

2. *(For Multi-OMS Environment, and if Oracle BI Publisher is Configured on Additional OMS Instances)* Delete all the Oracle BI Publisher managed servers, which you stopped in the previous step, by running the following command:

   ```
   $<OMS_HOME>/bin/configureBIP -delete
   ```

3. *(For Multi-OMS Environment)* Deconfigure and delete all the additional OMS instances by running the following command from each of their homes:

   ```
   $<OMS_HOME>/bin/omsca delete -OMSNAME <oms_name>
   ```

   **Note:**

   - Run this command on each of the additional OMS instances.
   - You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.

   For example, if you have two additional OMS instances named `EMGC_Addln_OMS2` and `EMGC_Addln_OMS3`, on two different hosts, then on the first additional OMS, run the following command:

   ```
   /u01/app/Oracle/Middleware/oms/bin/omsca delete -OMSNAME EMGC_Addln_OMS2
   ```

   Then, on the second additional OMS, run the following command:

   ```
   /u01/app/Oracle/Middleware/oms/bin/omsca delete -OMSNAME EMGC_Addln_OMS3
   ```

4. *(For Multi-OMS Environment)* Manually delete the following WebLogic targets of the deleted OMS:

   - /EMGC_GCDomain/GCDomain/EMGC_OMS2 (Oracle WebLogic Server)
   - /EMGC_GCDomain/instance2/ohs2 (Oracle HTTP Server)

5. *(For Multi-OMS Environment)* Stop all the Oracle Management Agents (Management Agent), which are running on the additional OMS hosts, by running the following command from each of their homes:

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

   **Note:** Run this command on each of the Management Agents configured with the additional OMS instances.

   For example, if you have two additional OMS instances with a Management Agent on each of them, then on the first additional OMS host where the first Management Agent is running, run the following command:

   ```
   /u01/app/Oracle/agent/core/12.1.0.5.0/bin/emctl stop agent
   ```

Then, on the second additional OMS host where the second Management Agent is running, run the following command:

```
/u01/app/Oracle/agent/core/12.1.0.5.0/bin/emctl stop agent
```

6. *(If Oracle BI Publisher is Configured on the First [Main] OMS)* Stop the Oracle BI Publisher managed server running on the first (main) OMS, by running the following command from the OMS home:

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

   **Note:** If any Oracle BI Publisher managed server fails to stop, then manually kill it using the operating system commands.

7. Deconfigure and delete the first (main) OMS where the Admin Server is configured:

   ```
   $<OMS_HOME>/bin/omsca delete -full
   ```

   For example,

   ```
   /u01/app/Oracle/Middleware/oms/bin/omsca delete -full
   ```

   You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.

   **Note:** If the Oracle Database where the Management Repository is configured, is set with a service name, then run the following command:

   - On UNIX platforms:

     ```
     ./omsca delete -full -REP_CONN_STR
     '(DESCRIPTION=(ADDRESS_
     LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<>)(PORT=<>)))(CONNECT_
     DATA=(SERVICE_NAME=<>)))'
     ```

     For example,

     ```
     /u01/app/Oracle/Middleware/oms/bin/omsca delete -full -REP_
     CONN_STR '(DESCRIPTION=(ADDRESS_
     LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=example.com)(PORT=1521)))(CON
     NECT_DATA=(SERVICE_NAME=srvc.example.com)))'
     ```

   - On Microsoft Windows platforms:

     ```
     .\omsca delete -full -REP_CONN_STR
     "(DESCRIPTION=(ADDRESS_
     LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<>)(PORT=<>)))(CONNECT_
     DATA=(SERVICE_NAME=<>)))"
     ```

     For example,

     ```
     C:\Program Files\Oracle\Middleware\oms\bin\omsca delete -full
     -REP_CONN_STR "(DESCRIPTION=(ADDRESS_
     LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=example.com)(PORT=1521)))(CON
     NECT_DATA=(SERVICE_NAME=srvc.example.com)))"
     ```

> **Note:** When you run `omsca delete -full` on the first (main) OMS, the command also deletes the primary Oracle BI Publisher managed server, if configured on the first OMS.

8. Stop the Management Agent running on the first (main) OMS, by running the following command from its home:

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

   For example,

   ```
   /u01/app/Oracle/agent/core/12.1.0.5.0/bin/emctl stop agent
   ```

9. Stop the Oracle WebLogic Server so that it does not access the schemas you are going to drop in the next step. For instructions, see the chapter on starting and stopping Oracle Fusion Middleware components in the *Oracle Fusion Middleware Administrator's Guide*.

## 21.1.2 Prerequisites for Deinstalling the Entire Enterprise Manager System

Before you deinstall Enterprise Manager, meet the following prerequisites:

1. Perform the steps outlined in Section 21.1.1.
2. Drop the Oracle Management Repository (Management Repository):

   > **WARNING: Once the Management Repository is dropped, it CANNOT be retrieved. Therefore, drop the Management Repository ONLY IF you want to deinstall the entire Enterprise Manager system, that is, all your OMS instances, Management Agents, and also the Management Repository. If you want to deinstall only the OMS (or any additional OMS), then do not drop the Management Repository.**

   > **WARNING: The RepManager in drop mode puts the database in quiesce mode by "ALTER SYSTEM QUIESCE RESTRICTED;" command.**

   a. Ensure that there are no SYSMAN users logged in.

   b. Drop the Enterprise Manager Cloud Control schema (SYSMAN schema) and the Metadata schema (MDS schema) from the Management Repository by running the following command from the OMS home:

   ```
   $<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <database_host>
   <repository_database_port> <repository_database_sid> -action drop
   -dbUser <repository_database_user> -dbPassword <repository_
   database_password> -dbRole <repository_database_user_role>
   -reposName <repository_name> -mwHome <middleware_home> -mwOraHome
   <middleware_ora_home> -oracleHome <OMS_HOME>
   ```

   For example,

   ```
   /u01/app/Oracle/Middleware/oms/sysman/admin/emdrep/bin/RepManager
   example.com 1234 sid_em -action drop -dbUser sys -dbPassword letmein
   -dbRole sysdba -reposName SYSMAN -mwHome /u01/app/Oracle/Middleware/
   ```

```
-mwOraHome /u01/app/Oracle/Middleware/ -oracleHome
/u01/app/Oracle/Middleware/oms/
```

**Note:**

- For Microsoft Windows, invoke `RepManager.bat`.
- On Microsoft Windows, if you are invoking `RepManager.bat` from outside of `<OMS_HOME>\sysman\admin\emdrep\bin` directory, then set the `ORACLE_HOME` environment variable to the OMS home.

  For example,

  ```
  set ORACLE_HOME=c:\oracle\middleware\oms
  ```

- OMS home or `$<OMS_HOME>` refers to the first (main) OMS where the Admin Server is configured.
- `-mwHome` and `-mwOraHome` refer to the middleware home where the first (main) OMS is configured. The first (main) OMS is the OMS where the Admin Server is configured.
- `-oracleHome` refers to the Oracle home of the first (main) OMS where the Admin Server is configured.
- If you are dropping the schemas that belong to a 10*g* Release 2 (10.2.x.x) Management Repository, then run the command without these arguments: `-mwHome <middleware_home> -mwOraHome <middleware_ora_home> -oracleHome <oracle_home>`

  For example,

  ```
  /u01/app/Oracle/Middleware/oms/sysman/admin/emdrep/bin/Re
  pManager example.com 1234 sid_em -action drop -dbUser sys
  -dbPassword letmein -dbRole sysdba -reposName SYSMAN
  ```

- For information on the support for `-action drop` and `-action dropall`, see Table 2–3.
- The `-action drop` command drops all the schemas and provides a confirmation message. If the action was unsuccessful, then it lists all the entities that could not be cleaned or dropped. For example, X schema is not cleaned, synonyms are not cleaned, tablespaces are not cleaned. In this case, rerun the command.

  If you do not have RepManager, or if you want to manually clean up the leftover entities, then see *My Oracle Support* note 1365820.1.

- If you want to drop the Enterprise Manager schema completely, then use the RepManager available in the OMS home. Do not use the one in database home because it cannot remove the Enterprise Manager schema completely.

**c.** Manually delete the data files `mgmt.dbf` and `mgmt_ecm_depot1.dbf` from the database home.

**Note:** On Microsoft Windows, if you see the following error while deleting the `.dbf` files, then stop the database service, and try deleting the files again.

```
The process cannot access the file because it is being used
by another process
```

### 21.1.3 Procedure for Deinstalling Enterprise Manager

This section describes the following:

- Deinstalling Enterprise Manager in Graphical Mode
- Deinstalling Enterprise Manager in Silent Mode

#### 21.1.3.1 Deinstalling Enterprise Manager in Graphical Mode

To deinstall Enterprise Manager—single OMS environment or multi-OMS environment with additional OMS instances—in graphical mode, follow these steps:

**Note:**

- Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.
- **For a multi-OMS environment, perform the steps outlined in this section on each of the additional OMS instances.**

1. Invoke the installer from the OMS home by running the following command:

   ```
   $<OMS_HOME>/oui/bin/runInstaller -deinstall ORACLE_HOME=<absolute_path_
   to_oms_home> -jreLoc <path> [-removeallfiles] [-invPtrLoc <absolute_
   path_to_oraInst.loc>]
   ```

   For example,

   ```
   /u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall
   ORACLE_HOME=/u01/app/Oracle/Middleware/oms/ -jreLoc
   /u01/app/Oracle/Middleware/jdk16/jdk -removeallfiles -invPtrLoc
   /u01/oraInst.loc
   ```

   **Note:**

   - You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/`.
   - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
   - When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.

2. On the Inventory screen, select the plug-in homes, and click **Remove**.

   - If you are deinstalling the entire Enterprise Manager system (with or without the Management Repository), then deinstall all the plug-in homes, including the OMS and Management Agent plug-in homes.

- If you are deinstalling an additional OMS, then deinstall only the OMS plug-in homes.

3. On the Inventory screen, select the `sbin` home, and click **Remove**.

4. On the Inventory screen, select the Java Development Kit (JDK) home, and click **Remove**.

> **Note:** Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

> **Note:** After deinstalling JDK, do NOT exit the installer. If you exit the installer inadvertently, then follow these steps:
>
> 1. Manually download and install JDK 1.6.0.43.0 on the OMS host. If you already have this supported version, then you can reuse it.
> 2. Invoke the installer again and pass the absolute path to the location where you have JDK:
>
> ```
> $<OMS_HOME>/oui/bin/runInstaller -deinstall -jreLoc <JDK_
> HOME> [-removeallfiles] [-invPtrLoc <absolute_path_to_
> oraInst.loc>]
> ```

5. On the Inventory screen, select the Oracle WebTier home, and click **Remove**.

6. On the Inventory screen, select the Oracle BI Publisher home, and click **Remove.**

> **Note:** You must perform this step even if you have not configured Oracle BI Publisher.

7. On the Inventory screen, select the OMS home, the Management Agent home, and the Oracle Common directory, and click **Remove**.

   - If you are deinstalling the entire Enterprise Manager system (with or without the Management Repository), then select and deinstall the OMS home, the Management Agent home, and the Oracle Common directory.
   - If you are deinstalling an additional OMS, then do one of the following:
     - If you plan to install another additional OMS on that host later, then select and deinstall only the OMS home and the Oracle Common directory.

       In this case, do NOT select and deinstall the Management Agent home. This Management Agent home belongs to the standalone Management Agent that was installed as a prerequisite for additional OMS installation. You will need this Management Agent when you install the new additional OMS. If you deinstall it now, then you will have to reinstall it later when you plan to install the new additional OMS.
     - If you do not plan to install another OMS on that host, then select and deinstall the OMS home, the Management Agent home, and the Oracle Common directory.

8. On the Inventory screen, click **Close** to exit the wizard.

9. Manually delete the middleware home:

For UNIX platforms:

```
rm -rf <absolute_path_to_middleware_home>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_middleware_home>
```

---

**Note:** If you see an error stating that the middleware home could not be deleted because of a long path, then shorten the middleware home name in one of the following ways:

- Rename the middleware home to a short name.

  For example, change `C:\Oracle\Middleware` to `C:\OR\MW`.

- Mount a drive to the middleware home path.

  For example, if `C:\Oracle\Middleware\oms\bin` is the directory that is causing an issue, then shorten the path in such a way that path length decreases to a reasonable extent *(the file path limits differ from one operating system to another)*.

  Mount `C:\Oracle\Middleware\oms` to drive `Z`.

  - Navigate to drive `Z,` and delete the files:

    ```
    prompt>Z:
    ```

    ```
    prompt>del bin
    ```

  - Navigate to the middleware home, and delete the leftover files:

    ```
    prompt:>C:
    ```

    ```
    prompt>del C:\Oracle\Middleware\
    ```

---

#### 21.1.3.2 Deinstalling Enterprise Manager in Silent Mode

To deinstall Enterprise Manager—single OMS environment or multi-OMS environment with additional OMS instances—in silent mode, follow these steps:

---

**Note:**

- Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.
- **For a multi-OMS environment, perform the steps outlined in this section on each of the additional OMS instances.**

---

1. Deinstall Oracle WebLogic Server 11*g* Release 1 (10.3.6) following the instructions outlined in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*. See the chapter that describes how you can deinstall the software.

   The *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* is available in the Oracle WebLogic Server documentation library available at:

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

> **Note:** Deinstall Oracle WebLogic Server 11*g* Release 1 (10.3.6) only if it was installed by the installation wizard while installing the Enterprise Manager system.

2. Deinstall the plug-in homes:

   - If you are deinstalling the entire Enterprise Manager system (with or without the Management Repository), then deinstall all the plug-in homes, including the OMS and Management Agent plug-in homes.
   - If you are deinstalling an additional OMS, then deinstall only the OMS plug-in homes.

   To deinstall the plug-in homes, run the following command:

   ```
   $<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
   HOMES={absolute_path_to_plug-in_home}" ORACLE_HOME=<absolute_path_to_
   oms_home> -jreLoc <JDK_HOME> [-removeallfiles] [-invPtrLoc <absolute_
   path_to_oraInst.loc>]
   ```

   For example,

   ```
   /u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
   HOMES={/u01/app/Oracle/Middleware/plugins/oracle.sysman.db.oms.plugin_
   12.1.0.2.0,/u01/app/Oracle/agent/plugins/oracle.sysman.db.discovery.plugin_
   12.1.0.2.0}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms -jreLoc
   /u01/app/Oracle/Middleware/jdk16/jdk -removeAllFiles -invPtrLoc
   /u01/oraInst.loc
   ```

   > **Note:**
   >
   > - You can invoke the installer even from the directory where you downloaded the software. If you do so, then do NOT pass `-removeallfiles.`
   >
   >   For example, if you have downloaded the software to `/u01/app/Oracle/Downloads`, then run the following command, skipping the `-removeallfiles` argument.
   >
   >   ```
   >   /u01/app/Oracle/Downloads/Disk1/runInstaller -deinstall -silent
   >   "REMOVE_
   >   HOMES={/u01/app/Oracle/Middleware/plugins/oracle.sysman.db.oms.
   >   plugin_
   >   12.1.0.2.0,/u01/app/Oracle/agent/plugins/oracle.sysman.db.disco
   >   very.plugin_12.1.0.2.0}" ORACLE_
   >   HOME=/u01/app/Oracle/Middleware/oms -jreLoc
   >   /u01/app/Oracle/Middleware/jdk16 -invPtrLoc /u01/oraInst.loc
   >   ```
   >
   > - When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
   > - To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.
   > - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

3. Deinstall the `sbin` home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_sbin_home}" ORACLE_HOME=<absolute_path_to_oms_
home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_
to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/agent/sbin}" ORACLE_HOME=/u01/app/Oracle/Middleware/oms
-jreLoc /u01/app/Oracle/Middleware/jdk16 -removeAllFiles -invPtrLoc
/u01/oraInst.loc
```

4. Deinstall the Java Development Kit (JDK) home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_jdk_home}" ORACLE_HOME=<absolute_path_to_oms_
home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_
to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/Middleware/jdk16}" ORACLE_
HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16
-removeAllFiles -invPtrLoc /u01/oraInst.loc
```

**Note:** Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

5. Manually download and install JDK 1.6.0.43.0 on the OMS host. If you already have this supported version, then you can reuse it.

   You must reinstall JDK because the installer has a dependency on it. The new JDK can be installed anywhere on the OMS host, not necessarily in the same location where it existed before. However, ensure that you pass the `-jreLoc` parameter (as described in the following steps) while invoking the installer to indicate the location where you have installed the JDK.

6. Deinstall the Oracle WebTier home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_web_tier}" ORACLE_HOME=<absolute_path_to_oms_
home> -jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_
to_oraInst.loc>]
```

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/Middleware/Oracle_WT}" ORACLE_
HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16
-removeAllFiles -invPtrLoc /u01/oraInst.loc
```

7. Deinstall the Oracle BI Publisher home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_bip}" ORACLE_HOME=<absolute_path_to_oms_home>
-jreLoc <JDK_HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_to_
oraInst.loc>]
```

**Note:** You must perform this step even if you have not configured Oracle BI Publisher.

For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/Middleware/Oracle_BI1}" ORACLE_
HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16
-removeAllFiles -invPtrLoc /u01/oraInst.loc
```

8. Deinstall the OMS home, the Management Agent home, and the Oracle Common directory.

   - If you are deinstalling the entire Enterprise Manager system (with or without the Management Repository), then deinstall the OMS home, the Management Agent home, and the Oracle Common directory.
   - If you are deinstalling an additional OMS, then do one of the following:
     - If you plan to install another additional OMS on that host later, then deinstall only the OMS home and the Oracle Common directory.

       In this case, do NOT select and deinstall the Management Agent home. This Management Agent home belongs to the standalone Management Agent that was installed as a prerequisite for additional OMS installation. You will need this Management Agent when you install the new additional OMS. If you deinstall it now, then you will have to reinstall it later when you plan to install the new additional OMS.
     - If you do not plan to install another OMS on that host, then deinstall the OMS home, the Management Agent home, and the Oracle Common directory.

   To deinstall the OMS home, the Management Agent home, and the Oracle Common directory, run the following command:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_oracle_homes_and_directories_to_be_
deinstalled}" ORACLE_HOME=<absolute_path_to_oms_home> -jreLoc <JDK_
HOME> [-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

   **Note:** The argument `REMOVE_HOMES` accepts more than one path separated by a comma.

   For example,

```
/u01/app/Oracle/Middleware/oms/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/u01/app/Oracle/Middleware/oms,/u01/app/Oracle/agent/core/12.1.0.5.0,/u0
1/app/Oracle/Middleware/oracle_common}" ORACLE_
HOME=/u01/app/Oracle/Middleware/oms -jreLoc /u01/app/Oracle/Middleware/jdk16
-removeAllFiles -invPtrLoc /u01/oraInst.loc
```

9. Manually delete the middleware home:

   For UNIX platforms:

```
rm -rf <absolute_path_to_middleware_home>
```

   For Microsoft Windows platforms:

```
del <absolute_path_to_middleware_home>
```

### 21.1.4 After Deinstalling Enterprise Manager

After you deinstall, perform these steps:

1. The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. You might also see the OMS instance base directory and the Oracle home for Web Tier. You can manually delete these files and directories.
2. The deinstallation process removes the entry of the `S98gcstartup` script, an auto-start script, from the `/etc/oragchomelist` file, but does not remove the script itself. You can leave this script and the soft links associated with it because when you install Enterprise Manager again on the same host, the installer automatically overwrites the script and re-create the soft links.

   However, if you want to clear the host of any Oracle products, then Oracle recommends that you manually delete this script and the soft links associated with it. To do so, navigate to the `/etc/rc.d/` directory, and search for the script `S98gcstartup.` This script is usually present in a subdirectory within the `/etc/rc.d/` directory. Navigate to the subdirectory where the script is found and delete the script. For example, `/etc/rc.d/rc3.d/S98gcstartup` or `/etc/rc.d/init.d/gcstartup/S98gcstartup.`
3. The JDK, which was installed as part of Step (5) of Section 21.1.3.2 to allow complete removal of the Enterprise Manager system, can now be removed manually (by deletion of the installed directory) if it is no longer needed for other purposes and if it did not replace the system-registered JDK.

## 21.2 Deinstalling or Undeploying Only Plug-ins from the OMS

If you want to deinstall or undeploy only the plug-ins from the OMS, and not the entire Enterprise Manager system, then use the Plug-ins page within the Enterprise Manager Cloud Control Console. For instructions, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*. **Do NOT use runInstaller to undeploy only the plug-ins.**

## 21.3 Deleting OMS Entries from the Management Repository

If you lose the host where an additional OMS is running, then make sure you manually delete the entry for that OMS from the Management Repository. To do so, follow these steps:

1. Run the following command to deconfigure Oracle WebLogic Server, applications, and so on from the WebLogic Domain; remove all OMS-related entries from the Management Repository; and delete these targets of the OMS: oracle_oms, oracle_oms_pbs, oracle_oms_console.

   $ORACLE_HOME/bin/omsca delete
2. Manually delete the following WebLogic targets of the OMS.
   - /EMGC_GCDomain/GCDomain/EMGC_OMS2 (weblogic_j2eeserver)
   - /EMGC_GCDomain/instance2/ohs2 (oracle_apache)

Now Enterprise Manager will not have any reference of the deleted additional OMS. If you want to delete the OMS, follow the instructions outlined in Section 21.1.

# 22

# Deinstalling Oracle Management Agents

This chapter describes how you can deinstall Oracle Management Agent (Management Agent). In particular, this chapter covers the following:

- Deinstalling Oracle Management Agents
- Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent

> **Note:** On a cluster, ensure that you deinstall the Management Agents from all the nodes one by one. To do so, follow the instructions outlined in this chapter.

> **Note:** When you deinstall an old Management Agent and install a new Management Agent on the same host, you will lose all historical target information from the Management Repository.
>
> To avoid losing all historical target information, first install the new Management Agent, then run the `emcli relocate targets` command to hand over the targets from the old Management Agent to the new Management Agent, and then deinstall the old Management Agent.
>
> For information about the `emcli relocate targets` command, see the *Oracle Enterprise Manager Cloud Control Command Line Interface Guide*.

## 22.1 Deinstalling Oracle Management Agents

This section describes how to remove an Oracle Management Agent using various deinstallation methods. This section covers the following:

- Prerequisites for Deinstalling Oracle Management Agents
- Procedure for Deinstalling Oracle Management Agents
- After Deinstalling Oracle Management Agents

### 22.1.1 Prerequisites for Deinstalling Oracle Management Agents

Before you deinstall a Management Agent, do the following:

1. Shut down the Management Agent by running the following command from its home. If it is already shut down, then skip this step.

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

2. Wait for the Management Agent to go to the *down* or *unreachable* state in the Cloud Control console. If it is already in the *down* or *unreachable* state, then go to the next step.

3. Delete the Management Agent targets and their monitored targets (from any host where EM CLI is installed):

   ```
   emcli delete_target

       -name="example.com:1836"

        -type="oracle_emd"

        -delete_monitored_targets
   ```

   > **Note:** For information on EM CLI and instructions to set it up, see *Oracle Enterprise Manager Command Line Interface Guide*.

## 22.1.2 Procedure for Deinstalling Oracle Management Agents

This section describes the following:

- (Most Recommended) Deinstalling Oracle Management Agents Using the AgentDeinstall.pl Script
- Deinstalling Oracle Management Agents Using the Installation Wizard in Graphical Mode
- Deinstalling Oracle Management Agent Using the Installation Wizard in Silent Mode
- Deinstalling Shared Agents
- Deinstalling Oracle Management Agent Installed Using an RPM File

### 22.1.2.1 (Most Recommended) Deinstalling Oracle Management Agents Using the AgentDeinstall.pl Script

The most recommended and the easiest way of deinstalling Management Agents is to use the AgentDeinstall.pl script. The script orchestrates the deinstallation of not only the Management Agent home but also the dependent homes such as the plug-in homes and the `sbin` home. This saves time and effort as you do not have to manually and explicitly select each component in a specific order to deinstall them, unlike the other deinstallation methods described in this chapter. The script automates the entire deinstallation operation.

To deinstall a Management Agent using the AgentDeinstall.pl script, follow these steps:

> **WARNING: By default, the AgentDeinstall.pl script deinstalls the Management Agent, removes the dependent entries from the inventory, and removes the entire agent base directory. If you want to retain the agent base directory for some reason, then pass the `-skipRemoval` argument to the script. This argument ensures that only the Management Agent home from agent base directory is removed, but the agent base directory and the rest of the subdirectories are retained.**

1. Invoke the `AgentDeinstall.pl` script:

```
$<AGENT_HOME>/perl/bin/perl <AGENT_
HOME>/sysman/install/AgentDeinstall.pl -agentHome <AGENT_HOME>
```

For example, if you want to deinstall the Management Agent and also remove the agent base directory, then run the following command:

```
$/u01/app/Oracle/core/12.1.0.5.0/perl/bin/perl
/u01/app/Oracle/core/12.1.0.5.0/sysman/install/AgentDeinstall.pl
-agentHome /u01/app/Oracle/core/12.1.0.5.0/
```

For example, if you want to deinstall the Management Agent but NOT remove the agent base directory, then run the following command:

```
$/u01/app/Oracle/core/12.1.0.5.0/perl/bin/perl
/u01/app/Oracle/core/12.1.0.5.0/sysman/install/AgentDeinstall.pl
-agentHome /u01/app/Oracle/core/12.1.0.5.0/ -skipRemoval
```

2. Manually remove the targets, which were being monitored by the Management Agent you deinstalled, from the Enterprise Manager Cloud Control console.

3. Manually delete the agent base directory. For information on agent base directory, see Section 2.3.5.

   For UNIX platforms:

   ```
   rm -rf <absolute_path_to_install_base_dir>
   ```

   For Microsoft Windows platforms:

   ```
   del <absolute_path_to_install_base_dir>
   ```

> **Note:** During the Management Agent deinstall process, the Management Agent service is not removed automatically. You must remove it manually after the deinstall, by running the following command:
>
> ```
> sc delete <service_name>
> ```

#### 22.1.2.2 Deinstalling Oracle Management Agents Using the Installation Wizard in Graphical Mode

To deinstall a Management Agent using the Enterprise Manager Cloud Control Wizard in graphical mode, follow these steps:

> **Note:** Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Invoke the installer from the Management Agent home by running the following command:

   ```
   $<AGENT_HOME>/oui/bin/runInstaller -deinstall ORACLE_HOME=<absolute_
   path_to_agent_home> [-removeallfiles] [-invPtrLoc <absolute_path_to_
   oraInst.loc>]
   ```

   For example,

   ```
   /u01/app/oracle/agent/core/12.1.0.5.0/oui/bin/runInstaller -deinstall
   ORACLE_HOME=/u01/app/oracle/agent/core/12.1.0.5.0/ -removeallfiles
   ```

**Note:**

- You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/`.
- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
- The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
- For Microsoft Windows, invoke the `setup.exe` file.

**Note:** When you invoke `runInstaller` or `setup.exe,` if the Enterprise Manager Cloud Control Installation Wizard does not appear, then it is possible that you do not have access to the `/stage` directory.

There is a classpath variable that the installation wizard computes for OPatch as `../stage/Components/,` and when the TEMP variable is set to `/tmp,` the installation wizard tries to look for the opatch JAR file in the `/tmp/../stage` directory, which is equivalent to `/stage.` However, if you do not have the permission on `/stage,` then the installation wizard can hang. Under such circumstances, verify if you have access to the `/stage` directory. If you do not have access to it, then set the TEMP variable to a location where the install user has access to, and then relaunch the installation wizard.

2. In the installation wizard, click **Installed Products.**
3. On the Inventory screen, select the plug-in homes under the required Management Agent home, then click **Remove.**
4. On the Inventory screen, select the `sbin` home, and click **Remove.**
5. On the Inventory screen, select the Management Agent, and click **Remove.**
6. Manually delete the agent base directory. For information on installation base directory, see Section 2.3.5.

   For UNIX platforms:

   ```
   rm -rf <absolute_path_to_agent_base_dir>
   ```

   For Microsoft Windows platforms:

   ```
   del <absolute_path_to_agent_base_dir>
   ```

#### 22.1.2.3 Deinstalling Oracle Management Agent Using the Installation Wizard in Silent Mode

To deinstall a Management Agent using the Enterprise Manager Cloud Control Installation Wizard in silent mode, follow these steps:

**Note:** Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Deinstall the plug-in homes:

   ```
   $<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
   HOMES={absolute_path_to_plug-in_home}" ORACLE_HOME=<absolute_path_to_
   agent_home> [-removeallfiles] [-invPtrLoc <absolute_path_to_
   oraInst.loc>]
   ```

   **Note:**

   - When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
   - On Microsoft Windows, invoke the `setup.exe` file.
   - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
   - To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.

   For example,

   ```
   /home/oracle/agent/core/12.1.0.5.0/oui/bin/runInstaller -deinstall
   -silent "REMOVE_
   HOMES={/home/oracle/agent/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.2.0,/home/oracle/agent/plugins/oracle.sysman.emct.oms.plugin_
   12.1.0.2.0}" ORACLE_HOME=/home/oracle/agent/core/12.1.0.5.0
   -removeAllFiles -invPtrLoc
   /home/oracle/agent/core/12.1.0.5.0/oraInst.loc
   ```

2. Deinstall the `sbin` home:

   ```
   $<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent  "REMOVE_
   HOMES={absolute_path_to_sbin_directory}" ORACLE_HOME=<absolute_path_to_
   agent_home> [-removeAllFiles] [-invPtrLoc <absolute_path_to_
   oraInst.loc>]
   ```

   For example,

   ```
   /home/oracle/agent/core/12.1.0.5.0/oui/bin/runInstaller -deinstall
   -silent "REMOVE_HOMES={/home/oracle/agent/sbin}" ORACLE_
   HOME=/home/oracle/agent/core/12.1.0.5.0 -removeAllFiles -invPtrLoc
   /home/oracle/agent/core/12.1.0.5.0/oraInst.loc
   ```

3. Deinstall the Management Agent:

   ```
   $<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
   HOMES={absolute_path_to_agent_oracle_home}" ORACLE_HOME=<absolute_path_
   to_agent_home> -removeAllFiles -invPtrLoc <absolute_path_to_
   oraInst.loc>
   ```

   For example,

   ```
   /home/oracle/agent/core/12.1.0.5.0/oui/bin/runInstaller -deinstall
   -silent  "REMOVE_HOMES={/home/oracle/agent/core/12.1.0.5.0}" ORACLE_
   HOME=/home/oracle/agent/core/12.1.0.5.0 -removeAllFiles -invPtrLoc
   /home/oracle/agent/core/12.1.0.5.0/oraInst.loc
   ```

4. Manually delete the agent base directory. For information on agent base directory, see Section 2.3.5.

For UNIX platforms:

```
rm -rf <absolute_path_to_install_base_dir>
```

For Microsoft Windows platforms:

```
del <absolute_path_to_install_base_dir>
```

#### 22.1.2.4 Deinstalling Shared Agents

To deinstall a Shared Agent, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/perl/bin/perl  <AGENT_
HOME>/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_HOME=<absolute_
path_to_agent_instance_home> ORACLE_HOME=<absolute_path_to_agent_home>
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.5.0/perl/bin/perl
/home/john/software/oracle/agent/core/12.1.0.5.0/sysman/install/NFSAgentDe
Install.pl AGENT_INSTANCE_HOME=/home/john/software/oracle/agent/agent_inst
ORACLE_HOME=/home/john/software/oracle/agent/core/12.1.0.5.0
```

**Note:** If you encounter an error while deinstalling the *Shared Agent*, then refer to Section J.4.

#### 22.1.2.5 Deinstalling Oracle Management Agent Installed Using an RPM File

To deinstall a Management Agent that was installed using a `.rpm` file, ensure that you have Resource Package Manager (RPM) installed on the Management Agent host, then follow these steps:

1. Run the following command on the Management Agent host to obtain the RPM name:

   ```
   rpm -qa | grep oracle-agt
   ```

2. Run the following command as a *root* user to deinstall the Management Agent:

   ```
   rpm -e <rpm_name>
   ```

   Here, `<rpm_name>` is the RPM name that is displayed in the output of the command you ran in Step 1.

### 22.1.3 After Deinstalling Oracle Management Agents

After you deinstall the Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify whether the Oracle homes and other directories were successfully deinstalled. To do so, follow these steps:

   a. Invoke the installation wizard by running the following command from the Management Agent home:

      ```
      <DVD>/runInstaller
      ```

      **Note:** On Microsoft Windows, invoke the `setup.exe` file.

   b. In the installation wizard, on the My Oracle Support Details screen, click **Installed Products**.

c. On the Inventory screen, check whether or not the Oracle homes and other directories you deinstalled appear. If the deinstallation was successful, then those Oracle homes and directories should not appear.

2. The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. If they do, you can manually delete them.

   You must also manually delete the auto-startup script called gcstartup which will be present under `/etc/init.d` directory.

   > **Note:** These auto-start scripts are not available on Microsoft Windows.

3. If you deinstalled on a Microsoft Windows platform, then follow these steps. Ensure that you are logged in as a user with Administrator privileges on that host.

   **Remove Entries from Microsoft Windows Registry**

   a. Start the registry editor by selecting **Start** and then **Run**. Type `regedit` and click **OK**.

   b. In the Registry Editor window, in the left pane, expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, and then **Oracle**. Under the **Oracle** directory, delete the following:

   (a) KEY_agent12g*n*

   (b) KEY_sbin12g*n*

   > **Note:** Here, *n* refers to a numeral indicating the agent instance. For example, `KEY_sbin12g9` for the first agent installation.

   c. Expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Oracle**, and then **Sysman**. Under the **Sysman** directory, delete the Management Agent service. For example, `Oracleagent12g9Agent`.

   d. Expand **HKEY_LOCAL_MACHINE**, **SYSTEM**, **CurrentControlSet**, and then **Services**. Under the **Services** directory, delete the Management Agent keys.

   e. Expand **HKEY_LOCAL_MACHINE**, **SYSTEM**, **ControlSet002**, and then **Services**. Under the **Services** directory, delete the Management Agent service.

   f. Close the registry editor.

   **Clean Up Environment Settings**

   1. Open the Environment Variables window.

      On Microsoft Windows NT, select **Start**, **Settings**, **Control Panel**, **System**, and then **Environment**.

      On Microsoft Windows XP or 2000, select **Start**, **Settings**, **Control Panel**, **System**, **Advanced**, and then **Environment Variables**.

   2. In the System Variables section, click the variable PATH and modify the value.

   3. Delete Management Agent home.

   4. Click **Apply** and then click **OK**.

5. Close the Control Panel window.
6. Restart the host.

## 22.2 Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent

If you want to deinstall or undeploy only the plug-ins from the Management Agent, and not the Management Agent itself, then use the Plug-ins page within the Enterprise Manager Cloud Control Console. For instructions, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*. **Do NOT use runInstaller to undeploy only the plug-ins.**

# 23

# Deinstalling ADP and JVMD

This chapter describes how you can deinstall Application Dependency and Performance (ADP), and Java Virtual Machine Diagnostics (JVMD) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

- Deinstalling ADP
- Deinstalling JVMD

## 23.1 Deinstalling ADP

This section describes how to remove ADP Engines and Agents, using the Application Performance Management page, as well as manually. This section consists of the following:

- Removing ADP Engine
- Removing ADP Agents

### 23.1.1 Removing ADP Engine

This section describes the methods to remove ADP Engines. It consists of the following:

- Removing ADP Engine Using Application Performance Management Page
- Removing ADP Engine Manually
- Removing ADP Engine Manually Using ApmEngineSetup.pl

#### 23.1.1.1 Removing ADP Engine Using Application Performance Management Page

To remove the ADP Engine applications running on Managed Servers using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Application Performance Management**.
2. If you want to remove a single ADP Engine, on the Application Performance Management page, select the ADP Engine you want to remove, then click **Remove.**

   If you want to remove more than one ADP Engine, on the Application Performance Management page, select the **ADP Engines** node, then click **Remove.**
3. On the Remove ADP Engines page, select the ADP Engines you want to remove.

4. For each ADP Engine you select, select **Remove WebLogic Managed Server,** if you want to remove the WebLogic Managed Server on which the ADP Engine is deployed.

5. Specify values for **Admin WebLogic Host Credentials** and **Admin WebLogic Credentials.**

   Admin WebLogic Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Admin WebLogic Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain.

6. Click **Remove.**

### 23.1.1.2 Removing ADP Engine Manually

To remove the ADP Engine application running on a Managed Server manually, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **Middleware**.

2. On the Middleware page, from the **Middleware Features** menu, select **Application dependency and Performance**.

   The Application Dependency and Performance is displayed.

3. From the **Registration** tab, select the ADP Engine application, then click **Remove**.

4. Log in to the WebLogic Administration Console of the Enterprise Manager domain.

5. On the Home Page, click **Servers**.

6. From the Summary of Servers page, click the **Control** tab, then select the ADP Engine Servers.

7. From the **Shutdown** menu, select **Force Shutdown Now** to stop the servers.

8. Click the Lock and Edit button present in the WebLogic Administration console.

9. Click the **Configuration** tab, select **ADP Engine Servers**, then click **Delete**.

10. Undeploy the ADP applications. For example, `ADPManager_EMGC_ADPMANAGER1` for ADP.

11. Connect to the host machine where the Managed Server was present, and navigate to the following location to manually delete the Managed Server:

    ```
    $DOMAIN_HOME/<ADP_managed_server>
    ```

    Where `$DOMAIN_HOME` is the location of the Enterprise Manager Cloud Control domain.

### 23.1.1.3 Removing ADP Engine Manually Using ApmEngineSetup.pl

You can remove ADP Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner

- In silent mode, where you specify all the input details using a properties file

**Important:** You can use the ApmEngineSetup.pl script to remove ADP Engine only on a host that is running the OMS, and not on a remote host.

To remove ADP Engine manually using the ApmEngineSetup.pl script, follow these steps:

1. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/engine/
   ```

2. View the README.txt file, for information on using the ApmEngineSetup.pl script.

3. Run the ApmEngineSetup.pl script.

   If you want to run the ApmEngineSetup.pl script in interactive mode, such that you are prompted for the input details, use the following command:

   ```
   perl ApmEngineSetup.pl
   ```

   Ensure that you specify the operation as remove, and the Engine Type as ADP.

   If you want to run the ApmEngineSetup.pl script in silent mode, specify all the input details in a properties file, then use the following command:

   ```
   perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
   <password>
   ```

   <properties_file_name> is the name of the properties file where the ADP Engine and operation details are provided. <password> is the WebLogic console password.

   To learn how to specify the input details in a properties file, view the sample properties file SAMPLE_engine.properties.

## 23.1.2 Removing ADP Agents

This section describes the methods to remove ADP Agents. It consists of the following:

- Removing ADP Agents Using Application Performance Management Page
- Removing ADP Agents Manually

### 23.1.2.1 Removing ADP Agents Using Application Performance Management Page

To remove the ADP Agents (that are deployed on monitored WebLogic domains) using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Application Performance Management.**

2. On the Application Performance Management page, under the Application Performance Management Agents section, click **Manage Diagnostics Agents.**

   **Note:** If no active JVMD or ADP Engines are present, and no JVMD or ADP Agents are deployed, the **Manage Diagnostics Agents** button is disabled.

3. For **Operation,** select **Remove.**

If you select **Expand All** from the **View** menu, you can view the target name, target type, target host, target status, platform, and so on of all the Managed Servers on which JVMD or ADP Agents are deployed.

Select the ADP Agents you want to remove. Click **Next.**

4. On the Target Credentials page, for each WebLogic domain, specify a value for **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials,** then click **Apply.**

   Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the Management Agent that is monitoring the selected WebLogic domain is running. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the selected WebLogic domain.

   Click **Next.**

5. On the ADP Agents Configurations page, specify values for the **WebLogic Home** and **Middleware Home** fields.

   These fields are displayed only if their values could not be obtained internally. Also, sometimes when the WebLogic Administration Server is behind a firewall or on a virtual host, the application may not be able to connect to it, using the default host value. In this case, you may need to provide some additional information in the Additional Configuration section. For example, if the WebLogic Administration Server is on a virtual host, and the application cannot connect to it using the default host value, you may have to provide the virtual host IP address in the Additional Configuration section.

6. On the Enterprise Manager OMS Credentials page, specify a value for **Oracle Enterprise Manager WebLogic Administration Server Host Credentials,** and **Oracle Enterprise Manager WebLogic Domain Credentials.**

   Oracle Enterprise Manager WebLogic Administration Server Host Credentials are the host credentials of the OMS host. The Oracle Enterprise Manager WebLogic Domain Credentials are the domain credentials of the Enterprise Manager WebLogic domain.

   Click **Next.**

7. On the Review page, review all the information, then click **Remove.**

#### 23.1.2.2 Removing ADP Agents Manually

To manually remove the ADP Agent deployed to a target, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **Middleware.**

2. On the Middleware page, from the **Middleware Features** menu, select **Application dependency and Performance**.

   The Application Dependency and Performance is displayed.

3. From the **Configuration** tab, select the desired ADP Engine application on which the ADP Agents have been deployed.

4. Expand the **ADP Engine** menu, then select **Resource Configuration**.

5. From the Resource table, select the ADP Agent name, click **Edit Resource**, then click **Deploy**.

6. From the Deploy Parameters table, select the servers from which you want to undeploy the ADP Agents. Change the default menu selection from **Deploy** to:

   - **Remove**, to erase all the ADP Agent files from the Managed Servers.

- **Disable**, to remove the ADP Agent startup arguments from the Managed Servers.

> **Note:** Select the **Server Started by Node Manager** option only when the node manager is used.

## 23.2 Deinstalling JVMD

This section describes how to remove JVMD Engines and Agents, using the Application Performance Management page, as well as manually. This section consists of the following:

- Removing JVMD Engine
- Removing JVMD Agents

### 23.2.1 Removing JVMD Engine

This section describes the methods to remove JVMD Engines. It consists of the following:

- Removing JVMD Engine Using Application Performance Management Page
- Removing JVMD Engine Manually
- Removing JVMD Engine Manually Using ApmEngineSetup.pl

#### 23.2.1.1 Removing JVMD Engine Using Application Performance Management Page

To remove the JVMD Engine applications running on Managed Servers using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Application Performance Management**.
2. If you want to remove a single JVMD Engine, on the Application Performance Management page, select the JVMD Engine you want to remove, then click **Remove.**

   If you want to remove more than one JVMD Engine, on the Application Performance Management page, select the **JVM Diagnostics Engines** node, then click **Remove.**
3. On the Remove JVMD Engines page, select the JVMD Engines you want to remove.
4. For each JVMD Engine you select, select **Remove WebLogic Managed Server,** if you want to remove the WebLogic Managed Server on which the JVMD Engine is deployed.
5. Specify values for **Admin WebLogic Host Credentials** and **Admin WebLogic Credentials.**

   Admin WebLogic Host Credentials are the host credentials for the host on which the WebLogic Administration Server (for the Enterprise Manager WebLogic domain) is deployed. Admin WebLogic Credentials are the credentials for the Administration Server of the Enterprise Manager WebLogic domain.
6. Click **Remove.**

#### 23.2.1.2 Removing JVMD Engine Manually

To remove the JVMD Engine application running on a Managed Server manually, perform the following steps:

1. Log in to the WebLogic Administration console of the Enterprise Manager Cloud Control domain.
2. On the Home Page, click **Deployments**.
3. Select the JVMD applications (for example, `jammanagerEMGC_JVMDMANAGER1`, `jammanagerEMGC_JVMDMANAGER2`). From the **Stop** menu, select **Force Stop Now.**
4. Click the Lock and Edit button present in the WebLogic Administration console.
5. After the applications are stopped, select the same applications, then click **Delete.**
6. Click **Home** to go back to the WebLogic Administration home page. From the Environment table, select **Servers.**
7. On the Summary of Servers page, select the **Control** tab, then select the JVMD Engine servers that need to be shut down.
8. From the **Shutdown** menu, select **Force Shutdown Now** to stop the servers.
9. Click the Lock and Edit button present in the WebLogic Administration console.
10. Click the **Configuration** tab, select the JVMD Engine servers, then click **Delete**.

#### 23.2.1.3 Removing JVMD Engine Manually Using ApmEngineSetup.pl

You can remove JVMD Engine manually, using the `ApmEngineSetup.pl` script. You can run this script in the following ways:

- In interactive mode, where you are prompted for input details in an interactive manner
- In silent mode, where you specify all the input details using a properties file

> **Important:** You can use the `ApmEngineSetup.pl` script to remove JVMD Engine only on a host that is running the OMS, and not on a remote host.

To remove JVMD Engine manually using the `ApmEngineSetup.pl` script, follow these steps:

1. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_
   12.1.0.8.0/archives/jvmd/deployment_Scripts/engine/
   ```

2. View the `README.txt` file, for information on using the `ApmEngineSetup.pl` script.
3. Run the `ApmEngineSetup.pl` script.

   If you want to run the `ApmEngineSetup.pl` script in interactive mode, such that you are prompted for the input details, use the following command:

   ```
   perl ApmEngineSetup.pl
   ```

   Ensure that you specify the operation as `remove,` and the Engine Type as `JVMD.`

   If you want to run the `ApmEngineSetup.pl` script in silent mode, specify all the input details in a properties file, then use the following command:

```
perl ApmEngineSetup.pl -silent -file <properties_file_name> -password
<password>
```

`<properties_file_name>` is the name of the properties file where the JVMD Engine and operation details are provided. `<password>` is the WebLogic console password.

To learn how to specify the input details in a properties file, view the sample properties file `SAMPLE_engine.properties`.

## 23.2.2 Removing JVMD Agents

This section describes the methods to remove JVMD Agents. It consists of the following:

- Removing JVMD Agents Using Application Performance Management Page
- Removing JVMD Agents Manually

### 23.2.2.1 Removing JVMD Agents Using Application Performance Management Page

To remove the JVMD Agents (that are deployed on monitored WebLogic domains) using the Application Performance Management page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Application Performance Management.**
2. On the Application Performance Management page, under the Application Performance Management Agents section, click **Manage Diagnostics Agents.**

   > **Note:** If no active JVMD or ADP Engines are present, and no JVMD or ADP Agents are deployed, the **Manage Diagnostics Agents** button is disabled.

3. For **Operation,** select **Remove.**

   If you select **Expand All** from the **View** menu, you can view the target name, target type, target host, target status, platform, and so on of all the Managed Servers on which JVMD or ADP Agents are deployed.

   Select the JVMD Agents you want to remove. Click **Next.**
4. On the Target Credentials page, for each WebLogic domain, specify a value for **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials,** then click **Apply.**

   Oracle WebLogic Administration Server Host Credentials are the host credentials for the host on which the Management Agent that is monitoring the selected WebLogic domain is running. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the selected WebLogic domain.

   Click **Next.**
5. On the JVMD Agents Configurations page, specify values for the **WebLogic Home** and **Middleware Home** fields.

   These fields are displayed only if their values could not be obtained internally. Also, sometimes when the WebLogic Administration Server is behind a firewall or on a virtual host, the application may not be able to connect to it, using the default host value. In this case, you may need to provide some additional information in the Additional Configuration section. For example, if the WebLogic Administration Server is on a virtual host, and the application cannot connect to it using the default host value, you may have to provide the virtual host IP address in the Additional Configuration section.

6. On the Review page, review all the information, then click **Remove.**

#### 23.2.2.2 Removing JVMD Agents Manually

To manually remove the JVMD Agent deployed to a target, perform the following steps:

1. Log in to the Administration Console of the target server.
2. On the Home Page, click **Deployments**.
3. Select the JVMD Agent application `(javadiagnosticagent.ear or jamagent.war)`. From the **Stop** menu, select **Force Stop Now.**
4. After the applications are stopped, select the same applications, then click **Delete.**
5. Log in to Enterprise Manager Cloud Control.
6. In Cloud Control, from the **Targets** menu, select **Middleware**.
7. On the Middleware page, in the Search table, search for targets of type **Java Virtual Machine,** select the target corresponding to the server, then click **Remove.**

# 24

# Removing Standby Oracle Management Services

This chapter describes how to remove standby Oracle Management Services (OMS) from a Level 4 High Availability (HA) configuration. The following OMS removal scenarios are covered:

- Removing Additional Standby OMS Instances
- Removing the First Standby OMS

## 24.1 Removing Additional Standby OMS Instances

To remove an additional standby OMS instance, follow these steps:

1. Deconfigure and delete an additional standby OMS instance by running the following command from the OMS home:

   ```
   $<OMS_HOME>/bin/omsca delete -OMSNAME <oms_name>
   ```

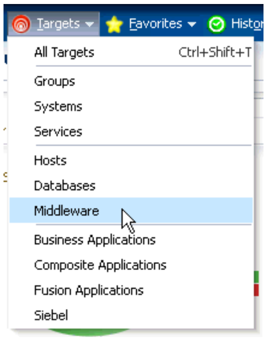
   When prompted, enter the repository login credentials.

   > **Note:** Run this command on each of the additional standby OMS instances.

2. From the Enterprise Manager console, refresh the Weblogic domain.

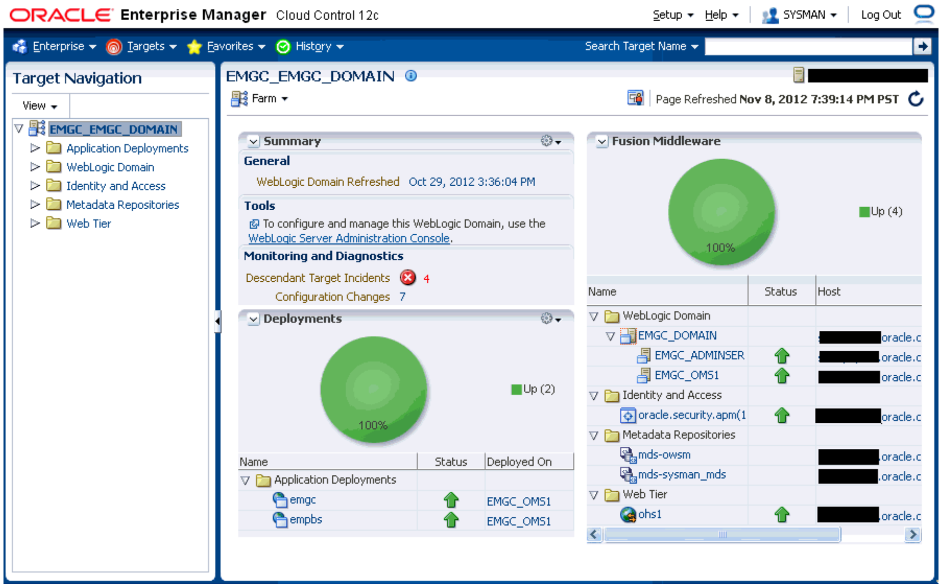
   1. From the **Targets** menu, select **Middleware**.

***Figure 24–1 Middleware Menu***



2. Click the **WebLogic Domain** you want to refresh. The domain home page displays.

*Figure 24–2 Domain Home Page*



[redacted]

Page Refreshed **Nov 8, 2012 7:39:14 PM PST**

**General**

WebLogic Domain Refreshed Oct 29, 2012 3:36:04 PM

**Tools**

To configure and manage this WebLogic Domain, use the WebLogic Server Administration Console.

**Monitoring and Diagnostics**

Descendant Target Incidents ✖ 4

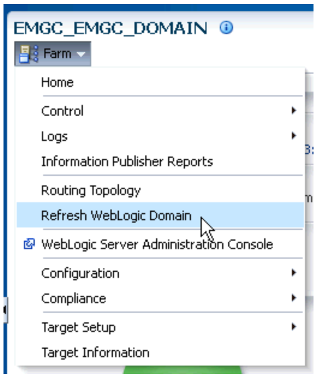
Configuration Changes 7

| Name | Status | Deployed On |
|---|---|---|
| Application Deployments | | |
| emgc | ⇧ | EMGC_OMS1 |
| empbs | ⇧ | EMGC_OMS1 |

| Name | Status | Host |
|---|---|---|
| WebLogic Domain | | |
| EMGC_DOMAIN | | [redacted]oracle.c |
| EMGC_ADMINSER | ⇧ | [redacted]oracle.c |
| EMGC_OMS1 | ⇧ | [redacted]oracle.c |
| Identity and Access | | |
| oracle.security.apm(1 | ⇧ | [redacted]oracle.c |
| Metadata Repositories | | |
| mds-owsm | | [redacted]oracle.c |
| mds-sysman_mds | | [redacted]oracle.c |
| Web Tier | | |
| ohs1 | ⇧ | [redacted]oracle.c |

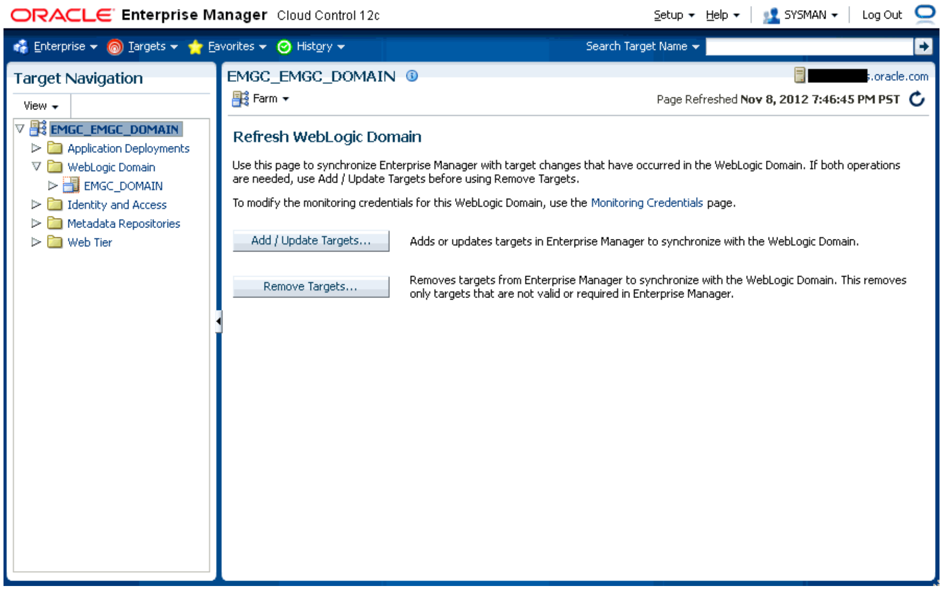
3. From either the **Farm** or **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

*Figure 24–3 Refresh WebLogic Domain*



Enterprise Manager displays available **Refresh WebLogic Domain** options.

*Figure 24–4 Refresh WebLogic Domain*



Refresh WebLogic Domain

Use this page to synchronize Enterprise Manager with target changes that have occurred in the WebLogic Domain. If both operations are needed, use Add / Update Targets before using Remove Targets.

To modify the monitoring credentials for this WebLogic Domain, use the Monitoring Credentials page.

Add / Update Targets... Adds or updates targets in Enterprise Manager to synchronize with the WebLogic Domain.

Remove Targets... Removes targets from Enterprise Manager to synchronize with the WebLogic Domain. This removes only targets that are not valid or required in Enterprise Manager.

4. Click **Add/Update Targets**. The Management Agent refreshes by connecting to the Administration Server. The Administration Server must be up for the refresh to occur.

   Click **Close** on the Confirmation page. Cloud Control will search the domain for new and modified targets.

3. Delete the OMS target associated with the OMS.

   1. From the **Target Navigation** area, click the target associated with the additional standby OMS you deconfigured earlier.

   2. From the **WebLogic** menu, select **Target Setup** and then **Remove Target**. Enterprise Manager displays a Warning dialog asking if you wish to continue. Click **Yes**.

4. Repeat this deinstallation procedure for all remaining additional standby OMSs.

## 24.2 Removing the First Standby OMS

To remove the first standby OMS, follow these steps:

---

**Important:** DO NOT attempt to deinstall the first standby OMS if there are any remaining additional standby OMSs within your environment. See "Removing Additional Standby OMS Instances" on page 24-1 for instructions on removing additional standby OMSs.

---

1. Deconfigure and delete the first standby OMS instance by running the following command from the OMS home:

   ```
   $<OMS_HOME>/bin/omsca delete -full
   ```

**Note:** You are prompted to confirm your action, and furnish the AdminServer credentials and the repository database details such as the database host name, listener port, SID, and password. Once you provide the required details, the command automatically stops the OMS, Oracle WebLogic Server, and also Oracle WebTier.

2. Delete the OMS target associated with the OMS.

    1. From the **Target Navigation** area, click the target associated with the first standby OMS you deconfigured earlier.

    2. From the **WebLogic** menu, select **Target Setup** and then **Remove Target**. Enterprise Manager displays a Warning dialog asking if you wish to continue. Click **Yes**.

# Part VIII

## Appendixes

This part contains the following appendixes:

- Appendix A, "Understanding the Enterprise Manager Directory Structure"
- Appendix B, "Overview of the Installation and Configuration Log Files"
- Appendix C, "Redirecting Oracle Management Agent to Another Oracle Management Service"
- Appendix D, "Applying Patches to Oracle Management Agents While Deploying or Upgrading Them"
- Appendix E, "Using the RepManager Utility"
- Appendix F, "Collecting OCM Data Using Oracle Harvester"
- Appendix G, "Enabling the Enterprise Manager Accessibility Features"
- Appendix H, "Configuring Targets for Failover in Active/Passive Environments"
- Appendix J, "Troubleshooting"

# A

# Understanding the Enterprise Manager Directory Structure

Before you perform maintenance and advanced configuration tasks, you must be familiar with the directories and files that are copied to disk when you install Enterprise Manager. Understanding where specific files are located can help you if you need to troubleshoot installation or configuration problems.

When installing Enterprise Manager, if you select a location that does not contain WebLogic Server, then JDK will be installed in the `jdk16` directory before installation of WebLogic Server.

Use the following sections to become familiar with the directories that are created on your disk when you install Enterprise Manager:

- Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12*c*
- Understanding the Enterprise Manager Directories Installed with an Oracle Management Service
- Understanding the Enterprise Manager Directories Installed with Management Agent

## A.1 Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c

When you install Oracle Enterprise Manager Cloud Control 12*c*, you install the Oracle Management Service. With the Oracle Management Service, you install the following Oracle home directories:

- Oracle Management Service home directory
- Middleware WebTier home directory
- Middleware Common home directory
- Oracle Management Service Instance home directory
- Oracle Management Agent home directory
- Oracle Management Agent Instance home directory
- Oracle Management Service Plug-in homes
- Oracle Management Agent Plug-in homes
- Oracle Business Intelligence Publisher home

### A.1.1 About the Oracle Management Service Home Directory

The Oracle Management Service is a J2EE application that is installed and deployed using the Oracle WebLogic Server.

The installation procedure installs the Enterprise Manager components within the Cloud Control Home, including the Oracle Management Service.

Information about the directories that are specific to the Fusion Middleware installation can be found in the Fusion Middleware documentation.

### A.1.2 About the Oracle Management Agent Home (AGENT_HOME) Directory

The Oracle Management Agent Home `(AGENT_HOME)` directory contains all the binaries required to configure and run the Oracle Management Agent on the host.

This directory serves as the Oracle Home for the Oracle Management Agent.

Information about the directories that are specific to the Fusion Middleware installation can be found in the Fusion Middleware documentation.

### A.1.3 About Business Intelligence Publisher Home Directory

The Business Intelligence Publisher is a J2EE application that is installed in the `Oracle_BI1` directory. This directory contains all the Business Intelligence Publisher configuration files and software binaries.

The business intelligence publisher directory is created in the Middleware home `(middleware_home)` directory.

To use the Business Intelligence Publisher, configure it as described in Chapter 14.

### A.1.4 Summary of the Important Directories in the Oracle Management Service Home

Figure A–1 shows some of the important directories you should be familiar with in a typical Cloud Control installation. You can use this information as you begin to maintain, troubleshoot, and configure the Oracle Management Service installation.

***Figure A–1***

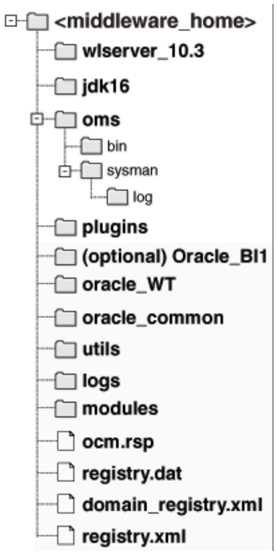


*Table A–1 Directories Installed with Enterprise Manager*

| Directory | Description |
|---|---|
| wlserver_10.3, logs, utils, modules | These directories contain Fusion Middleware files. |
| jdk16 | This directory contains JDK configuration files. |
| oms | This directory contains OMS configuration files. For more information, see Section 10.2.2. |
| plugins | This directory contains metadata plug-ins configuration files installed on the OMS. |
| agent | This directory contains agent configuration files. |
| [optional] Oracle_BI1 | This directory contains the Oracle Business Intelligence Publisher configuration files. |
| oracle_WT | This directory contains Oracle WebTier configuration files. |
| oracle_common | This directory contains common files used by OMS, Oracle WebTier, and WebLogic Server directories. |

## A.2 Understanding the Enterprise Manager Directories Installed with Management Service

Table A–2 describes in detail the Oracle Management Service directories installed with Oracle Management Service. In the table, ORACLE_HOME refers to the Oracle Management Service home directory in which the Oracle Management Service is installed and deployed.

*Table A–2 Important Directories in the Management Service Oracle Home*

| Directory | Description |
|---|---|
| `ORACLE_HOME/bin` | The bin directory in the Management Service home contains commands used to control the components of the Cloud Control installation. |
| `OMS_INSTANCE_HOME/WebTierIH1` | This directory contains WebTier instance Oracle Home corresponding to `EMGC_OMS#`. |
| `OMS_INSTANCE_HOME/NodeManager` | This directory contains WebLogic Node Manager properties, logs, and domain information. |
| `OMS_INSTANCE_HOME/em` | This is the OMS instance directory and contains emgc.properties and Enterprise Manager log files. |
| `OMS_INSTANCE_HOME/user_projects` | This directory contains `EMGC_ADMINSERVER` and `EMGC_OMS#` domains and their logs. |
| `ORACLE_HOME/sysman/log` | This directory contains schema log files. The repository log files are under `sysman/log/schemamanager`. The install logs are under `ORACLE_HOME/cfgtoollogs`. The operation logs are under `OMS_INSTANCE_HOME/em/EMGC_OMS1/sysman/log`. |

## A.3 Understanding the Enterprise Manager Directories Installed with Management Agent

The Oracle Management Agent is installed automatically when you install Oracle Management Service. This local instance of the Oracle Management Agent gathers management information about the targets on the Oracle Management Service host.

You can then manage those targets, such as the host itself, from the Cloud Control Console.

You can install additional Oracle Management Agents using different installation methods. This enables you to install the Oracle Management Agent on the hosts throughout your enterprise. The Oracle Management Agent can then gather management data about the targets on each host so those targets can be managed from the Cloud Control Console.

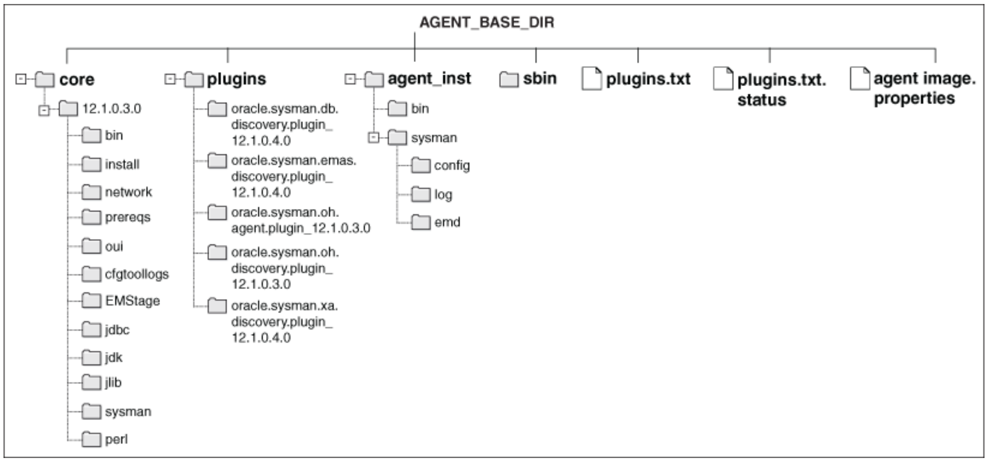
Specifically, the Oracle Management Agent files are installed into the same directory structure shown in the agent directory when you install the Oracle Management Service (Figure A–1).

The agent directory structure, when you install a standalone agent or install the OMS is the same. The AGENT_BASE_DIR is the directory where agent is installed and contains the following main directories:

- AGENT_HOME
- AGENT_INSTANCE_HOME
- SBIN_HOME
- PLUGIN_HOME

The directory that contains the files required to run the Oracle Management Agent is referred to as the `AGENT_INSTANCE_HOME` directory. For example, to start or stop an Oracle Management Agent, you use the emctl command located in the bin directory of the `AGENT_INSTANCE_HOME`. Similarly, to configure files for the Oracle Management Agent, you modify the configuration files in the `sysman/config` directory of the `AGENT_INSTANCE_HOME`. See Figure A–2 for the agent directory structure.

***Figure A–2 Agent Directory Structure***


AGENT_BASE_DIR
core
12.1.0.3.0
bin
install
network
prereqs
oui
cfgtoollogs
EMStage
jdbc
jdk
jlib
sysman
perl
plugins
oracle.sysman.db.discovery.plugin_12.1.0.4.0
oracle.sysman.emas.discovery.plugin_12.1.0.4.0
oracle.sysman.oh.agent.plugin_12.1.0.3.0
oracle.sysman.oh.discovery.plugin_12.1.0.3.0
oracle.sysman.xa.discovery.plugin_12.1.0.4.0
agent_inst
bin
sysman
config
log
emd
sbin
plugins.txt
plugins.txt.status
agent image.properties

## A.3.1 Summary of the Important Directories in the Oracle Management Agent Home

Table A–3 describes some of the important agent directories.

*Table A–3 Important Directories in Oracle Management Agent Home*

| Directory | Description |
|---|---|
| AGENT_HOME | The AGENT_HOME directory contains all the binaries required to configure and run the Oracle Management Agent on this host.<br>The default AGENT_HOME location is AGENT_BASE_DIR/core/12.1.0.5.0.<br>This directory serves as the Oracle Home for the Oracle Management Agent. |
| AGENT_HOME/bin | This directory contains binaries for the Oracle Management Agent. |
| AGENT_HOME/install | This directory contains installation-related files for deploying the agent. |
| AGENT_HOME/prereqs | This directory contains prerequisite files for EMPrereqKit. |
| AGENT_HOME/oui | This directory contains files related to the installer framework. |
| AGENT_HOME/cfgtoollogs | This directory contains agent deployment and configuration log files. |
| AGENT_HOME/EMStage | This directory is used by the provisioning framework for provisioning activities. |
| AGENT_HOME/sysman/admin | This directory contains the files used by the Oracle Management Agent to define agent core target types (such as databases, hosts, and so on), to run configuration scripts, and other administrative tasks. |
| AGENT_INSTANCE_HOME | The AGENT_INSTANCE_HOME directory contains agent-related configuration files after agent is installed and configured.<br>The default AGENT_INSTANCE_HOME location is AGENT_BASE_DIR/agent_inst. |
| AGENT_INSTANCE_HOME/bin | The AGENT_INSTANCE_HOME/bin directory in the Cloud Control Home contains the emctl command that controls the Oracle Management Agent for this host.<br>You use the following emctl commands in this directory to start and stop the Oracle Management Agent on this host:<br>`<AGENT_INSTANCE_HOME>/bin/emctl start agent`<br>`<AGENT_INSTANCE_HOME>/bin/emctl stop agent` |
| AGENT_INSTANCE_HOME/sysman/config | This directory contains the configuration files for the Oracle Management Agent. For example, this is where Enterprise Manager stores the emd.properties file. The emd.properties file defines settings such as the Oracle Management Service upload URL for this particular agent. |
| AGENT_INSTANCE_HOME/sysman/log | This directory contains the log files for the Oracle Management Agent. |
| AGENT_INSTANCE_HOME/sysman/emd | The emd directory contains information about targets discovered on hosts. |
| SBIN_HOME | This directory contains set UIDs for the agent. The default location is AGENT_BASE_DIR/sbin. |
| PLUGIN_HOME | This directory contains all the discovery and monitoring plug-ins required for the agent.<br>The default location is AGENT_BASE_DIR/plugins. |

### A.3.2 Understanding the Oracle Management Agent Directory Structure in Windows

When you install the Oracle Management Agent on a Windows system, the directory structure of the AGENT_HOME directory is the same as the directory structure for installations on a UNIX system.

## A.4 Identifying the Agent Instance Home When Using the emctl Command

When you install Cloud Control, the resulting directory structure can often include multiple subdirectories with the same name. For example, you can have a bin directory within the agent_instance_home directory. Use the emctl command within the agent_instance_home/bin directory to control the Oracle Management Agent.

In addition, you can have a bin directory within the Oracle Management Service Oracle home. Use the emctl command in this directory to control the Oracle Management Service.

To quickly identify the Agent Instance home that is controlled by the files in a particular bin directory, use the following command:

```
$PROMPT> emctl getemhome
```

This command displays the path to the current Agent Instance home that will be affected by commands executed by this instance of the emctl command.

# B

# Overview of the Installation and Configuration Log Files

This appendix lists the locations of the various log files that are created during the prerequisites check, installation, and configuration phases of Enterprise Manager Cloud Control components.

In particular, this appendix covers the following:

- Enterprise Manager Cloud Control Installation Logs
- Add Host Log Files
- Manual Management Agent Installation Logs
- Additional OMS Installation Logs

## B.1 Enterprise Manager Cloud Control Installation Logs

This section describes the following log files that are created while installing Enterprise Manager Cloud Control:

- Installation Logs
- Configuration Logs

### B.1.1 Installation Logs

The following are the installation logs, which provide complete information on the installation status:

- `<ORACLE_INVENTORY_HOME>/logs/installActions<timestamp>.log`
- `<ORACLE_HOME>/cfgtoollogs/oui/installActions<timestamp>.log`

> **Note:** The `installActions` log file is located in the `<ORACLE_INVENTORY_HOME>` directory by default. This log file will be copied on to the above-mentioned Oracle home location after the installation is complete.

### B.1.2 Configuration Logs

This section describes the following configuration logs:

- General Configuration Logs
- Repository Configuration Logs

- Secure Logs

### B.1.2.1 General Configuration Logs

The Oracle Management Service (OMS) configuration logs are located in the following location of the Oracle home of the OMS.

```
<ORACLE_HOME>/cfgtoollogs/omsca
```

Table B–1 lists the configuration logs for different installation types.

*Table B–1 General Configuration Logs*

| Installation Type | Location |
|---|---|
| Install a new or Upgrade Enterprise Manager system | - `<ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger<timestamp>.log`<br>- `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log`<br>**Note:** `<ORACLE_HOME>` refers to the Oracle home of the OMS. |
| Add an additional Management Service | - `<ORACLE_HOME>/cfgtoollogs/omsca/logs/omsca<timestamp.log>`<br>- `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log`<br>**Note:** `<ORACLE_HOME>` refers to the Oracle home of the OMS. |
| Install Oracle Management Agent | - `<ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger`<br>- `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent.<timestamp>.log`<br>**Note:** `<ORACLE_HOME>` refers to the Oracle home of the Management Agent. |

### B.1.2.2 Repository Configuration Logs

This section describes the following repository configuration logs:

- SYSMAN Schema Operation Logs
- MDS Schema Operation Logs

#### B.1.2.2.1 SYSMAN Schema Operation Logs

The SYSMAN schema operation logs are available in the following location of the Oracle home of the OMS. Listed in this directory is an overall log file, `emschema.log`, which logs all the actions performed by all the instances of RepManager run.

```
$<ORACLE_HOME>/sysman/log/schemanager/
```

In this location, for each run of RepManager, a new subdirectory is created based on the time at which the RepManager was run.

For example, if the RepManager was run and an instance was created at 09/29/2007 12:50PM, then the following subdirectory is created.

```
$<ORACLE_HOME>/sysman/log/schemananager/m_092907_1250_PM/
```

An instance of RepManager (or equivalently RepManager) can have  schema actions, mainly CREATE, DROP, UPGRADE, TRANSX, and RESUME_RETRY. For each action, a subdirectory is created.

For example, if a CREATE action is performed by a RepManager instance at 09/29/2006 12:51PM, then the following subdirectory is created. Listed under this subdirectory are RCU-related log files and `emschema.log.CREATE` log file that logs the CREATE action-specific messages.

```
$<ORACLE_HOME>/sysman/log/schemananager/m_092907_1250_PM/m_092907_
1251PM.CREATE/
```

In general, in `$<ORACLE_HOME>/sysman/log/schemananager/m_<time-stamp>/m_<time-stamp>.<schema-action>`, the following files are created:

- RCU per component (i.e. init, common, modify, drop, config, outofbox, preupgrade log
- RCU log
- Schema action-specific RCU logs
- TransX action-specific log (`emrep_config.log`)

If the any of the schema operations (CREATE/UPGRADE/PREUPGRADE/DROP) fail in SQL execution, and if you retry the operation by clicking **Retry**, then a separate subdirectory titled `m_<time-stamp>.RESUME_RETRY` is created.

The following shows the overall directory structure of repository operation logs for different schema actions:

```
$<ORACLE_HOME>/sysman/log/schemamanager
               emschema.log
        m_030210_0349_AM
            m_030210_0325_AM.TRANSX
                emrep_config.log
                emschema.log.TRANSX
        m_030210_0438_AM
            m_030210_0438_AM.DROP (Same structure for Drop and Dropall actions)
                rcu.log
                emschema.log.DROP
                em_repos_drop.log
        m_030210_0450_AM
            m_030210_0450_AM.CREATE
                 custom_comp_create_tbs.log
                 em_repos_common.log
                 em_repos_init.log
                 emrep_config.log.3
                 emrep_config.log.2
                 emrep_config.log.1
                 emrep_config.log
                 emschema.log
                 rcu.log
                 emschema.log.CREATE
                 em_repos_config.log
        m_030210_1006_PM
            m_030210_1006_PM.RESUME_RETRY
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                emschema.log
                rcu.log
                emschema.log.RESUME_RETRY
                em_repos_modify.log
        m_030210_1021_PM
            m_030210_1021_PM.UPGRADE
```

```
                em_repos_init.log
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                emschema.log
                rcu.log
                emschema.log.UPGRADE
                em_repos_modify.log
        m_030210_1100_PM
            m_030210_1100_PM.PREUPGRADE
                em_repos_preupgrade.log
                emschema.log.PREUPGRADE
                rcu.log
                em_repos_init.log
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                em_repos_common.log
        m_030210_1125_PM
            m_030210_1125_PM.MY_ORACLE_SUPPORT
                emschema.log.MY_ORACLE_SUPPORTm_030210_1135_PM
            m_030210_1135_PM.PLUGINPURGE
                emschema.log.PLUGINPURGE
em_repos_pluginpurge.log
rcu.log
```

#### B.1.2.2.2 EMPrereqKit Logs

For EMPrereqKit, the logs are available at the `<oraInventoryLoc>/logs/` location.

The details of execution of the prerequisites per prerequisite component location is available at:

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/componentLog/<log_filename>
```

For example,

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/componentLog/repository.log
```

The details of execution of the EMPrereqkit is available at:

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/emprereqkit.log
```

The errors are located at:

```
<oraInventoryLoc>/logs/emdbprereqs/LATEST/emprereqkit.err
```

#### B.1.2.2.3 MDS Schema Operation Logs

**MDS Schema Creation Log**

For MDS schema creation operation, the following log is available in the Oracle home of the OMS:

```
$<ORACLE_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

For more information, review the following logs from the Oracle home of the OMS:

```
$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_
<timestamp>.CREATE/mds.log
```

```
$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_
<timestamp>.CREATE/rcu.log
```

**MDS Schema Drop Logs**

For MDS schema drop operation, the following logs are available in the location you specified by using the `-logDir` argument while invoking the MDS schema drop command:

```
$<user_specified_location>/mds.log
```

```
$<user_specified_location>/emmdsdrop_<timestamp>.log
```

However, if you did not specify any custom location while invoking the MDS schema drop command, then the logs are created in the Oracle home of the OMS. For example, `/scratch/OracleHomes/oms12c/mds.log` and `/scratch/OracleHomes/oms12c/emmdsdrop_<timestamp>.log`.

### B.1.2.3 Secure Logs

For OMS, the following secure log is available in the OMS Instance Base location. Here, <*oms_name*>, for example, can be *EMGC_OMS1*.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/secure.log
```

For Management Agents, the following secure log is available in the Oracle home of the Management Agent.

```
<Agent_Instance_Home/sysman/log/secure.log
```

### B.1.2.4 Oracle Management Service Logs

The following log files that provide information about the running OMS are available in the OMS Instance Base location. Here, <*oms_name*>, for example, can be *EMGC_OMS1*.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.trc
```

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.log
```

# B.2 Add Host Log Files

This section describes the locations for the following Add Host log files:

- Initialization Logs
- Application Prerequisite Logs
- System Prerequisite Logs
- Agent Installation Logs
- Other Add Host Logs

## B.2.1 Initialization Logs

Table B–2 lists the initialization logs of the remote host and their locations. Note that `<OMS_INSTANCE_HOME>` mentioned in this table refers to the OMS instance base directory (by default, it is `gc_inst/em/EMGC_OMS1`, which is present in the parent directory of the middleware home, by default).

***Table B–2 Initialization Logs***

| Log File | Location |
|---|---|
| `<hostname>_deploy.log` | `<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs` |

## B.2.2 Application Prerequisite Logs

Table B–3 lists the application prerequisite logs and their locations. Note that <OMS_INSTANCE_HOME> mentioned in this table refers to the OMS instance base directory (by default, it is gc_inst/em/EMGC_OMS1, which is present in the parent directory of the middleware home, by default), and <install_type> mentioned in this table refer to one of the installation types mentioned in Table B–4.

*Table B–3 Prerequisite Logs*

| Log File | Location |
|---|---|
| prereq<time_stamp>.log | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/ |
| prereq<time_stamp>.out | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/ |
| prereq<time_stamp>.err | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/ |

*Table B–4 Install Types*

| Install Type | Description | Target Operating System Type |
|---|---|---|
| emagent_install | New Agent Installation | UNIX |
| emagent_clone | Agent Cloning | UNIX |
| nfs_install | Shared Agent Installation | UNIX |

## B.2.3 System Prerequisite Logs

Table B–5 lists the system prerequisite logs and their locations. Note that <OMS_INSTANCE_HOME> mentioned in this table refers to the OMS instance base directory (by default, it is gc_inst/em/EMGC_OMS1, which is present in the parent directory of the middleware home, by default).

*Table B–5 System Prerequisite Logs*

| Log File | Location |
|---|---|
| prereq<time_stamp>.log | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/ |
| prereq<time_stamp>.out | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/ |
| prereq<time_stamp>.err | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/ |

## B.2.4 Agent Installation Logs

Table B–6 lists the agent installation logs and their locations. Note that <OMS_INSTANCE_HOME> mentioned in this table refers to the OMS instance base directory (by default, it is gc_inst/em/EMGC_OMS1, which is present in the parent directory of the middleware home, by default).

*Table B–6 Agent Installation Logs*

| Log File | Location | Description |
|---|---|---|
| install.log/.err | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/logs/<hostname> | Fresh and Cloned Agent install logs |
| nfs_install.log/.err | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/logs/<hostname> | Shared Agent installation logs |
| cfgfw/*.log | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/cfgtoollogs/<hostname> | Agent Configuration logs |

### B.2.5 Other Add Host Logs

Table B–7 lists all the other installation logs that are created during an agent installation using the Add Host wizard. Note that <OMS_INSTANCE_HOME> mentioned in this table refers to the OMS instance base directory (by default, it is gc_inst/em/EMGC_OMS1, which is present in the parent directory of the middleware home, by default).

*Table B–7 Other Add Host Logs*

| Logs | Location | Description |
|---|---|---|
| EMAgentPushLogger<TIMESTAMP>.log | <OMS_INSTANCE_HOME>/sysman/agentpush/logs/ | Agent Deploy application logs. |
| remoteInterfaces<TIMESTAMP>.log | <OMS_INSTANCE_HOME>/sysman/agentpush/logs/ | Logs of the remote interfaces layer. |
| deployfwk.log | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs/ | Add Host Deployment Framework logs |
| ui.log | <OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs/ | Add Host User Interface logs. |

## B.3 Manual Management Agent Installation Logs

Table B–8 lists the installation logs that are created when a Management Agent is installed manually, that is, in silent mode. Note that <ORACLE_HOME> mentioned in this table refers to the target Management Agent Oracle Home, that is, <AGENT_BASE_DIR>/core/12.1.0.4.0/.

*Table B–8 Manual Management Agent Installation Logs*

| Logs | Location | Description |
|---|---|---|
| agentDeploy<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/agentDeploy/ | Installation logs |
| prereq<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/agentDeploy/ | Installation prerequisite logs |
| CfmLogger<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/cfgfw/ | Configuration logs |
| AttachHome<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/agentDeploy/ | Attach home logs |
| UpdateHomeDeps<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/agentDeploy/ | Update home logs |

*Table B–8 (Cont.) Manual Management Agent Installation Logs*

| Logs | Location | Description |
|---|---|---|
| cloneActions<TIMESTAMP>.log | <ORACLE_HOME>/cfgtoollogs/agentDeploy/ | Clone action logs |

## B.4 Additional OMS Installation Logs

Table B–9 lists the installation logs that you can view when adding an OMS fails:

**Note:**

- ORACLE_HOME refers to the home for the new additional OMS. However, for Admin logs, ORACLE_HOME refers to the home for the primary OMS.
- INSTANCE_HOME refers to the OMS instance directory (that is, gc_inst, which is present in the parent directory of the middleware home, by default).

*Table B–9 Additional OMS Installation Logs*

| Logs | Location |
|---|---|
| omsca failure | $ORACLE_HOME/cfgtoollogs/omsca |
| Plug-in failure | $ORACLE_HOME/cfgtoollogs/pluginca |
| Managed server logs<br>■ emLogs (emoms logs)<br>■ msLogs (Managed server logs, if server fails to start)<br>■ nmLogs | $ORACLE_HOME/cfgtoollogs/omsca/log_<timestamp>/ |
| Admin logs | $INSTANCE_HOME/user_projects/domains/GCDomain/servers/EMGC_ADMINSERVER/logs<br>(If out of memory error or space issue occurs, this logs on the primary OMS) |
| Deployment procedure output | Deployment procedure screenshots |
| Clone logs | $ORACLE_HOME/cfgtoollogs/clone |

# C

# Redirecting Oracle Management Agent to Another Oracle Management Service

This appendix explains how to redirect or repoint your Oracle Management Agent (Management Agent), that is already communicating with an Oracle Management Service (OMS), to communicate and upload data to a different OMS that is part of a different Enterprise Manager Cloud Control (Cloud Control) deployment.

---

**Note:**

- Redirecting Management Agents to a different OMS that is part of a different Cloud Control deployment is supported only for Management Agents that were deployed fresh, and were not upgraded from an earlier version. You cannot redirect a Management Agent that was upgraded from an earlier version.
- When you redirect a Management Agent to a different OMS that is part of a different Cloud Control deployment, you lose all the changes made to the agent instance home, such as user defined metric collections, changes made to the `emd.properties` file, and so on.

---

In particular, this appendix covers the following:

- Prerequisites for Redirecting a Management Agent to Another OMS
- Redirecting a Management Agent to Another OMS

## C.1 Prerequisites for Redirecting a Management Agent to Another OMS

Before redirecting or repointing a Management Agent, ensure that you meet the following prerequisites:

- Ensure that the new OMS that you want to point the Management Agent to is of the same version as the Management Agent, or of a higher version.

  To view the version of the Management Agent you want to repoint, from the **Setup** menu, select **Manage Cloud Control,** then select **Agents.** Click the name of the Management Agent. The Management Agent version is displayed in the Summary section.

  To view the version of the new OMS, from the **Setup** menu, select **Manage Cloud Control,** then select **Management Services.** Click the name of the new OMS. The OMS version is displayed in the Summary section.

You can repoint the Management Agent only if the new OMS is compatible with the Management Agent. Using the Enterprise Manager certification matrix, you can view the compatibility between an OMS version and a Management Agent version. For information on accessing this matrix, refer *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

- Ensure that the previous OMS that the Management Agent was pointing to, and the new OMS that you want to point the Management Agent to have the same set of plug-ins deployed on them, and that all the plug-ins configured on the Management Agent are deployed on the new OMS. Also, ensure that all these plug-ins deployed on the new OMS are of the same version, (that is, the version configured on the Management Agent or the previous OMS) or a higher version.

  To view the list of plug-ins deployed on a particular OMS, log in to the Enterprise Manager system, from the **Setup** menu, select **Extensibility,** then select **Plug-ins.**

  To view the list of plug-ins configured on a particular Management Agent, run the following command:

  ```
  $<AGENT_INSTANCE_HOME>/bin/emctl listplugins agent -type all
  ```

- Ensure that the Management Agent that you want to redirect is up and running, then run the following command to re-create the `plugins.txt` file:

  ```
  $AGENT_HOME/perl/bin/perl $AGENT_HOME/sysman/install/create_plugin_
  list.pl -instancehome <AGENT_INSTANCE_HOME>
  ```

  **Note:** By default, the Perl install location is specified as `/usr/local/bin` in `create_plugin_list.pl`. If Perl is installed on the Management Agent host in a different location, ensure that you edit the first line of `create_plugin_list.pl`, and specify the location where Perl is installed.

- Ensure that all the patches applied on the Management Agent that change the target type or collection metadata are also applied on the new OMS that you want to point the Management Agent to.

  To view all the patches applied on the Management Agent, from the **Targets** menu, select **All Targets.** Click the name of the Management Agent Oracle Home target. All the patches applied on the Management Agent are displayed in the Applied Patches section.

  From the displayed list of patches, apply the required patches (the patches that change the target type or collection metadata) on the new OMS. For information on how to apply a patch on an OMS, refer the Patching Enterprise Manager chapter present in *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

- If you have applied any one-off patches on the Management Agent you want to repoint, ensure that you apply the fix for Bug 15904425 on the Management Agent and the new OMS.

## C.2 Redirecting a Management Agent to Another OMS

To redirect or repoint a Management Agent, follow these steps:

1. Run the following command to stop the Management Agent:

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

2. Run the following EM CLI command to delete the Management Agent target on the old OMS:

   ```
   $<OMS_HOME>/bin/emcli delete_target -delete_monitored_targets
   -name=<name_of_agent_target> -type="oracle_emd"
   ```

   For more information about the `delete_target` EMCLI command, refer *Oracle Enterprise Manager Command Line Interface Guide.*

3. Run the following command to remove the Management Agent instance home:

   ```
   rm -rf <absolute_path_to_agent_instance_home>
   ```

   If the agent base directory and the agent instance home point to the same physical location, do not run this command. Instead, remove the `<AGENT_INSTANCE_HOME>/bin`, `<AGENT_INSTANCE_HOME>/sysman`, `<AGENT_INSTANCE_HOME>/diag`, and `<AGENT_INSTANCE_HOME>/install` directories.

4. Run the `agentDeploy.sh (agentDeploy.bat` for Microsoft Windows hosts) script with the `-configOnly` option to create a new instance home for the Management Agent and redirect it to the new OMS:

   ```
   $<AGENT_BASE_DIR>/core/12.1.0.5.0/sysman/install/agentDeploy.sh AGENT_
   BASE_DIR=<absolute_path_to_agent_base_dir> AGENT_INSTANCE_
   HOME=<absolute_path_to_agent_base_dir>/agent_inst AGENT_PORT=<port_for_
   agent_process> OMS_HOST=<new_oms_host_name> EM_UPLOAD_PORT=<upload_
   port> AGENT_REGISTRATION_PASSWORD=<agent_reg_password> b_upgrade=false
   b_12cupgrade=false b_agentUpgrade=false b_noUpgrade=true -configOnly
   ```

   For more information about the parameters you can specify while running `agentDeploy.sh` or `agentDeploy.bat,` refer Table 6–3. For more information about the `-configOnly` option, refer Table 6–6.

   > **Note:** The specified agent base directory location and the new agent instance home location map to locations on the same host, where the Management Agent was already configured. The OMS host name, of course, maps to the other host where the new OMS is configured, that is, the OMS with which you want the Management Agent to communicate now.

# D

# Applying Patches to Oracle Management Agents While Deploying or Upgrading Them

In Enterprise Manager Cloud Control 12c Release 4 (12.1.0.5.0), you can combine Management Agent binaries with Management Agent patches and plug-in patches, so that you do not have to apply these patches every time you deploy or upgrade a Management Agent. You can save the Management Agent one-off patches that you want to apply on a particular version of the Management Agent software, such that these patches are automatically applied on the software whenever a new Management Agent of the same version is deployed, or an old Management Agent is upgraded to that version. This is a one-time operation, that is, you do not have to perform this action every time you deploy or upgrade a Management Agent.

If you save the Management Agent one-off patches on the OMS host as described in this appendix, any Management Agent deployment or upgrade activity will automatically pick up these patches for the respective Management Agent versions and platforms. Hence, this feature saves you a considerable amount of time and effort.

For information on applying patches on a plug-in and ensuring that the patched plug-in is deployed on all the new Management Agents that you deploy, and all the old Management Agents that you upgrade, see *Oracle Enterprise Manager Cloud Control Administration Guide.*

Ensure that you follow the steps mentioned in this appendix and the section referenced in the previous para before scheduling a Management Agent deployment or upgrade session, so that the patches that you want to apply on the Management Agent and plug-ins are applied automatically after the Management Agent deployment or upgrade.

This appendix contains the following sections:

- Saving Management Agent Patches to an OMS Host
- Verifying Patch Application After Management Agent Deployment or Upgrade

## D.1 Saving Management Agent Patches to an OMS Host

To save Management Agent one-off patches to your OMS host, such that they are applied whenever a new Management Agent is deployed, or a Management Agent is upgraded, follow these steps:

1. Download the required Management Agent one-off patches from My Oracle Support, available at the following URL:

   `https://support.oracle.com/`

Ensure that the size of the patch zip file you downloaded is the same as what is displayed on the My Oracle Support page.

For information on how to download a patch from My Oracle Support, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

2. Create the following directory on the OMS host, and transfer all the generic Management Agent one-off patches to it:

   ```
   $<OMS_HOME>/install/oneoffs/<agent_version>/Generic/
   ```

   Here, `<agent_version>` is the version of the Management Agent that the patch is for. Ensure that you use the five-digit Management Agent version while creating this directory.

   For example, if you want to apply Patch 11180406, a generic Management Agent one-off patch for a 12.1.0.5.0 Management Agent, whenever a 12.1.0.5.0 Management Agent is deployed, or an old Management Agent is upgraded to 12.1.0.5.0, download this patch from My Oracle Support, create the following directory, then transfer the patch to it:

   ```
   $<OMS_HOME>/install/oneoffs/12.1.0.5.0/Generic/
   ```

3. Create the following directories on the OMS host, and transfer all the platform-specific Management Agent one-off patches to them:

   ```
   $<OMS_HOME>/install/oneoffs/<agent_version>/<platform>/
   ```

   Here, `<agent_version>` is the version of the Management Agent that the patch is for. Ensure that you use the five-digit Management Agent version while creating these directories.

   `<platform>` is the platform directory name, which is different for different patch platforms. Table D–1 lists the platform directories that you must create for various patch platforms.

***Table D–1 Platform Directory Names for Transferring Platform-Specific Management Agent Patches***

| Patch Platform | Platform Directory Name |
|---|---|
| Linux x86 | linux |
| Linux x86-64 | linux_x64 |
| Oracle Solaris on SPARC (64-bit) | solaris |
| Oracle Solaris on x86-64 (64-bit) | solaris_x64 |
| HP-UX PA-RISC (64-bit) | hpunix |
| HP-UX Itanium | hpi |
| IBM S/390 Based Linux (31-bit) | linux_zseries64 |
| IBM AIX on POWER Systems (64-bit) | aix |
| IBM: Linux on POWER Systems | linux_ppc64 |
| Microsoft Windows x64 (64-bit) | windows_x64 |
| Microsoft Windows (32-bit) | win32 |

---

**Note:** If you have a multi-OMS environment, ensure that you perform these steps on all the OMS hosts. Ensure that you download and transfer the same patches to the same directories on all the OMS hosts. Failing to do so may result in inconsistency and unexpected errors.

---

For example, if you want to apply Patch 11878907 (which is for a 12.1.0.5.0 Linux x86-64 Management Agent), and Patch 11993577 (which is for a 12.1.0.5.0 Microsoft Windows x64 Management Agent), whenever these Management Agents are deployed, or older versions of these Management Agents are upgraded to 12.1.0.5.0, download these patches from My Oracle Support, create the following directories, then transfer the patches to them:

**For Patch 11878907:**

```
$<OMS_HOME>/install/oneoffs/12.1.0.5.0/linux_x64/
```

**For Patch 11993577:**

```
$<OMS_HOME>/install/oneoffs/12.1.0.5.0/windows_x64/
```

## D.2 Verifying Patch Application After Management Agent Deployment or Upgrade

You can use these methods to verify whether the Management Agent one-off patches that you saved to your OMS host (described in Section D.1) have been applied on a Management Agent that you deployed or upgraded:

- Run the following command from the Management Agent home:

  ```
  $<AGENT_HOME>/OPatch/opatch lsinventory -oh <AGENT_HOME> -invPtrLoc
  <AGENT_HOME>/oraInst.loc
  ```

  This command displays all the patches applied on the Management Agent.

- In the Cloud Control console, from the **Setup** menu, select **Manage Cloud Control,** then select **Agents.** Click the name of the required Management Agent to navigate to its home page. In the Configuration section, click **Oracle Home and Patch Details.** The patches applied on the Management Agent are displayed in the Patches Applied section.

# E

# Using the RepManager Utility

This appendix describes the RepManager utility. In particular, this appendix covers the following:

- Overview of the RepManager Utility
- Actions and Commands Supported by the RepManager Utility

## E.1 Overview of the RepManager Utility

RepManager is a utility that enables you to upgrade and drop Oracle Management Repository, selectively purge plug-ins, and load dlf messages to Oracle Management Repository. This utility is available in the Oracle Management Service (OMS) home:

For UNIX operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager
```

For Microsoft Windows operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager.bat
```

This utility is invoked by Repository Configuration Assistant while installing a complete Enterprise Manager system, and by Repository Upgrade Configuration Assistant while upgrading to Enterprise Manager Cloud Control.

> **Note:** If you want to drop the Enterprise Manager schema completely, then use the RepManager available in the OMS home. Do not use the one in database home because it cannot remove the Enterprise Manager schema completely.

## E.2 Actions and Commands Supported by the RepManager Utility

Table E–1 shows the list of actions and their associated commands supported by the RepManager utility.

> **WARNING: The RepManager in drop mode puts the database in quiesce mode by "ALTER SYSTEM QUIESCE RESTRICTED;" command.**

***Table E–1 Actions and Commands Supported by RepManager***

| Action | Command | Description | Example |
|---|---|---|---|
| preupgrade | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action preupgrade <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"` | Use this action to perform steps before upgrading an Oracle Management Repository with the following parameters:<br>■ Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded.<br>■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to upgrade the Oracle Management Repository.<br>■ Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the `-pluginDepList` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list:<br>`$<OMS_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList`<br>■ Depending on how the plug-ins can be deployed, specify whether they must be deployed as `SYS` or `SYSMAN,` which is the repository user. To deploy them as `SYSMAN,` set the `-runAsReposUser` parameter to `TRUE.` If you do not pass this parameter, by default, the plug-ins will be deployed as `SYS` user.<br>■ Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the `-dlfSources` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations:<br>`$<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources`<br>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up. | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action preupgrade example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -mwHome /scratch/weblogic/middleware -pluginDepList <pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>` |

*Table E–1 (Cont.) Actions and Commands Supported by RepManager*

| Action | Command | Description | Example |
|---|---|---|---|
| upgrade | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action upgrade <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman  [-mwHome <Middleware home>]-pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"`<br>**Note:** Run preupgrade before performing upgrade action. | Use this action to upgrade an Oracle Management Repository with the following parameters:<br>■ Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded.<br>■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to upgrade the Oracle Management Repository.<br>■ Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the `-pluginDepList` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list:<br>`$<OMS_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList`<br>■ Depending on how the plug-ins can be deployed, specify whether they must be deployed as `SYS` or `SYSMAN,` which is the repository user. To deploy them as `SYSMAN,` set the `-runAsReposUser` parameter to TRUE. If you do not pass this parameter, by default, the plug-ins will be deployed as `SYS` user<br>■ Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the `-dlfSources` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations:<br>`$<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources`<br>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up. | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action upgrade example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -mwHome /scratch/weblogic/middleware -pluginDepList <pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>` |

*Table E–1 (Cont.) Actions and Commands Supported by RepManager*

| Action | Command | Description | Example |
|---|---|---|---|
| transX | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action transx <repository_database_host> <repository_database_port> <repository_database_sid> -reposName sysman [-mwHome <Middleware home>] -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"`<br>**Note:** You can also run `-doTransX`. By default, it is set to true. If you set the value to false, no translation bundles are loaded. This is applicable for `-dlfSources` for preupgrade and upgrade actions. | Use this action to load the translation resources to the Oracle Management Repository with the following parameters:<br>■ Specify the host, port, and SID to connect to Oracle RDBMS to load translation resources to Oracle Management Repository.<br>■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home to load translation resources to Oracle Management Repository.<br>■ Specify a comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plugins. If the `-dlfSources` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations:<br>`$<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources`<br>If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up. | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action transx example.com 1521 db3 -reposName sysman -mwHome /scratch/WLS/middleware` |
| resume | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -resume retry <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -checkpointLocation <directory where schemamanager stores checkpoints>` | Use this action to resume the last failed action, for example, upgrade.<br>■ Specify the host, port, and SID to connect to Oracle RDBMS where the action is to be resumed.<br>■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home where the action is to be resumed.<br>■ Specify the location at which to resume the step. The checkpoint location is $<OMS_HOME>/sysman/log/schemamanager. | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -resume retry -checkpointLocation /scratch/weblogic/middleware/oms/sysman/log/schemamanager -mwHome /scratch/weblogic/middleware` |

*Table E–1 (Cont.) Actions and Commands Supported by RepManager*

| Action | Command | Description | Example |
|---|---|---|---|
| drop | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action drop <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] [-mwOraHome <Oracle Home>]`<br>OR<br>`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action drop <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] [-mwOraHome <Oracle Home>]`<br>Ensure that there are no active sessions, scheduler jobs, and dbms_jobs running for SYSMAN, SYSMAN_MDS SYSMAN_OPSS, and SYSMAN_APM. Ensure that none of these users are logged in. To ensure this, stop the OMS using the command emctl stop oms -all on all OMS instances.<br>**Note:** If BI Publisher (BIP) had been installed and configured, then BIP should be stopped using the Admin Server before running this command. | Use this action to remove all Enterprise Manager repository schemas as follows:<br>■ Specify the host, port, and SID to connect to Oracle RDBMS from which all schemas are to be dropped.<br>■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and Middleware home.<br>At the end, a confirmation message appears to confirm the status of this operation. If all the schemas were successfully dropped, then a message confirming the same appears. Otherwise, a message providing details on each of the schemas appears.<br>For example,<br>`SYSMAN_OPSS schema is not cleaned.`<br>`EM_X synonyms are not dropped.` | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action drop -mwHome /scratch/weblogic/middleware`<br>OR<br>`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action drop -mwHome /scratch/weblogic/middleware -mwOraHome /scratch/weblogic/middleware` |

*Table E–1 (Cont.) Actions and Commands Supported by RepManager*

| Action | Command | Description | Example |
|---|---|---|---|
| plugin purge | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager -action pluginpurge <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -pluginPurgeList "<plugin_name>=<plugin_location>" [-mwHome <Middleware home>] -mwOraHome <Oracle Home>`<br>**Note:** To purge multiple plug-ins, for the -pluginPurgeList argument, enter the plug-ins separated by a command. For example, `<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>` | Use this action to deinstall a plug-in from the repository as follows:<br>■ Specify the host, port, and SID to connect to Oracle RDBMS from which the plug-in is to be deinstalled.<br>■ Specify a comma-separated list of plug-ins to be purged from Enterprise Manager Repository with EM-EXT model. | `$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action pluginpurge -pluginPurgeList "oracle.sysman.myyempwpax.oms.plugin_12.1.0.2.0=/scratch/weblogic/middleware/plugins/oracle.sysman.myyempwpax.oms.plugin_12.1.0.2.0" -mwHome /scratch/weblogic/middleware` |

**Note:** For information on the support for `-action drop` and `-action dropall` commands, see Table 2–3.

**Note:** If you do not specify passwords during RepManager actions, you will be prompted to do so.

# F

# Collecting OCM Data Using Oracle Harvester

This appendix provides information for using the Oracle Harvester to collect Oracle Configuration Manager (OCM) data for submission to My Oracle Support (MOS).

My Oracle Support provides a key set of features and functionality that greatly enhance the customer's interaction with Oracle Support. My Oracle Support streamlines the Service Request submission process by providing in-context information specific to a customer’s configurations, as well as proactive support. To enable these features within My Oracle Support, the customer's configuration information must be uploaded to Oracle. When the configuration data is uploaded on a regular basis, customer support representatives can analyze this data and provide better service to customers.

The following mechanisms are provided to customers for collecting and uploading configuration data to Oracle.

- Oracle Enterprise Manager Harvester (Oracle Harvester)
- Oracle Configuration Manager (OCM)

In particular:

- Oracle Configuration Manager is installed and configured automatically when you install an Oracle product.

  When installing any product, the first screen asks for My Oracle Support credentials. THIS IS A PIVOTAL SCREEN in the installation. The user name and password that you provide are the credentials against which the configuration data is uploaded to Oracle.

- Configuration collections run and the configuration data is uploaded to Oracle every 24 hours.
- Once the data is uploaded, it can be viewed by logging into My Oracle Support (`https://support.oracle.com`) using the same credentials supplied during product installation.

**Note:** If you use Enterprise Manager to manage your applications, we recommend that you use Oracle Harvester to upload your configurations to Oracle. Otherwise, use OCM.

The sections below provide information on the following topics:

- Oracle Harvester
- Oracle Configuration Manager
- Additional Information About MOS and OCM
- Troubleshooting Configuration Data Collection Tools

# F.1 Oracle Harvester

Oracle Harvester only harvests data for targets that are managed by Enterprise Manager. Because Oracle Harvester has the same OCM dependencies, Oracle Harvester enables the gathering of target configuration data by leveraging Enterprise Manager collection methods thus precluding the need to install OCM on target homes managed by Oracle Harvester. The following topics are presented:

- Highlights of Oracle Harvester
- Oracle Harvester and OCM
- Support For Enterprise Manager Release 12.1
- Viewing CSIs in Enterprise Manager
- Harvester Target Lifecycle Properties from Enterprise Manager
- Harvester Job Status Metric
- Supported Targets in Oracle Harvester
- Configuration Data Not Available in My Oracle Support

## F.1.1 Highlights of Oracle Harvester

The following are highlights of Oracle Harvester:

- Data is uploaded by default for all targets against the same credentials with which OCM in the Oracle Management Service (OMS) home is configured. From Enterprise Manager Cloud Control 12*c*, you can change this default value for a target by assigning a CSI from the CSI Assignment page. Click **Setup,** then **My Oracle Support** to get started.
- Requires OCM to be configured and running in the OMS home for Enterprise Manager.
- Gathers target configuration data from the Management Repository
- Automatically runs periodically so no user intervention is required

## F.1.2 Oracle Harvester and OCM

When you install Enterprise Manager, Oracle Harvester and Oracle Configuration Manager (OCM) are automatically installed as are all the necessary subcomponents. The Oracle Harvester will run as long as the OCM in the OMS home is configured and running.

OCM *must* be enabled in the Oracle Home of the OMS and configured (and running in connected mode) in the Instance Home of the OMS. The reason is that the Oracle OMS target will *not* be discovered by the OCM collector if `ORACLE_CONFIG_HOME` is not set.

Perform the following steps to ensure the Oracle OMS target is discovered:

1. Locate the OMS instance home.

   In the `$ORACLE_HOME/sysman/config/emInstanceMapping.properties` file (where `ORACLE_HOME` is the Oracle Home of the OMS), there is an entry referencing a file called `emgc.properties`.

   The directory in which the `emgc.properties` file is located is the "instance home" of the OMS. In the following example, `/u01/app/oracle/product/gc_inst/em/EMGC_OMS1` is the instance home of the OMS:

   ```
   EMGC_OMS1=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1/emgc.properties
   ```

2. Set the environment variable `ORACLE_CONFIG_HOME` to the directory of this `emgc.properties` file.

   Example:

   ```
   $export ORACLE_CONFIG_HOME=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1
   ```

3. If My Oracle Support credentials were not provided during the Enterprise Manager installation, run the following command to set them:

   ```
   setupCCR
   ```

   Provide the My Oracle Support credentials when prompted.

For more information about the Oracle Configuration Manager (OCM), see the *Oracle® Configuration Manager Installation and Administration Guide*:

http://docs.oracle.com/cd/E49269_01/doc.12/e48361/toc.htm

Or visit the OCM documentation library:

http://docs.oracle.com/cd/E49269_01/index.htm

### F.1.3 Support For Enterprise Manager Release 12.1

By default, all targets are uploaded using the credentials used to register Oracle Configuration Manager in the OMS Home. In Enterprise Manager release 12.1, you have the option of assigning a Customer Support Identifier (CSI) to each target home.

The Oracle Harvester supports uploading configuration data to different CSIs for each different Oracle Home.

The steps include:

1. Ensuring that the Oracle Harvester has run. This job runs automatically. The status of the run can be monitored from the Support Identifier Assignment page. To access this page from the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. From the menu, select **Support Identifier Assignment.**
2. Setting My Oracle Support preferred credentials. From the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. From the menu, select **Set credentials** and supply any valid My Oracle Support credentials.
3. Assigning the Support Identifier.
   a. From the Enterprise Manager home page, select **Setup**, then select **My Oracle Support**. Select **Support Identifier Assignment** and provide the correct user name and password. Select Set credentials.
   b. Select **Home**. Click **Assign** button. Select CSI and click **OK**.
4. Ensuring the message displays indicating the assignment was successful. The message reads:

   ```
   Support Identifier has been assigned for 1 Oracle homes. The changes in the
   Customer Support Identifiers will be reflected in My Oracle Support after the
   next Harvester run.
   ```

### F.1.4 Viewing CSIs in Enterprise Manager

You can see the CSI associated with a target by viewing the target property or by doing a configuration search with CSI set as the search criteria. Any user with operator privilege on all targets for a given Oracle Home can assign a CSI for that Oracle Home.

Refer to the help in the Enterprise Manager interface on how to access this information.

### F.1.5 Harvester Target Lifecycle Properties from Enterprise Manager

Oracle Harvester provides the target lifecycle property to enable you to identify the purpose of a target, for example, development, testing, and so on.

Once defined, the Oracle Harvester collects the target lifecycle property for all the targets and uploads the property to Oracle Configuration Manager server.

You can assign target lifecycle property to any target from either the Enterprise Manager UI or the My Oracle Support UI.

The possible values of a target's lifecycle property are:

- Mission Critical
- Production
- Stage
- Test
- Development

### F.1.6 Harvester Job Status Metric

From Enterprise Manager Cloud Control 12*c* Release 12.1.0.3 and OCM 10.3.8.1.0, a *Harvester Job Status* metric has been added to the OMS and Repository target. This metric will provide information related to the Harvester Job. The following information is collected as part of this metric:

- **Harvester Status**: Provides the status of the last harvester job run. Possible values include:
  - SUCCESS: indicates the job ran successfully.
  - ERROR: returned if job failed.
  - NOT CONFIGURED: indicates that OCM is not configured.
  - NOT AUTHENTICATE: shows that OCM is configured, but it is not in Authenticated mode.
- **Harvester Error**: Shows an error message in case the harvester job fails to run.
- **Last Harvester Job Run**: Shows the time the last harvester job ran.
- **Next Harvester Job Run**: Shows the time of the next harvester job run.
- **Total Targets Processed**: Shows the number of targets processed by the harvester job during its last run.
- **Total Targets Successful**: Total number of targets successfully uploaded to MOS from Total Targets Processed.
- **Total Targets Failed**: Shows the total number of target that failed to upload to MOS out of the Total Targets Processed in the Last Harvester Job Run.
- **OCM Version**: Shows the version of OCM configured with Enterprise Manager.

The Harvester Job Status metric data is available from the OMS and Repository target metrics page. An ERROR threshold has been defined for the Harvester Status field. If the value of this field shows ERROR, then an incident will be created, which will appear on both the OMS and Repository home page and the Incident Manager Page.

### F.1.7 Supported Targets in Oracle Harvester

Depending on the release of Enterprise Manager that Oracle Harvester is running on, Oracle collects the configuration data from a different set of target types. Only configuration data from the target types shown in Table F–1 are collected by Oracle Harvester.

***Table F–1 Supported Targets in Enterprise Manager 12.1 Releases***

| | | Enterprise Manager Release | | |
|---|---|---|---|---|
| **Target** | **Plug-in Release** | **12.1.0.1** | **12.1.0.2** | **12.1.0.3** |
| BI | 12.1.0.3 | No | Yes | Yes |
| Host | not applicable | Yes | Yes | Yes |
| Management Agent | not applicable | Yes | Yes | Yes |
| Management Repository | not applicable | Yes | Yes | Yes |
| Oracle Application Server | all versions | Yes | Yes | Yes |
| Oracle Database | all versions | Yes | Yes | Yes |
| Oracle Database Machine | all versions | Yes | Yes | Yes |
| Oracle Exadata Storage Server | all versions | Yes | Yes | Yes |
| Oracle Exalogic | 12.1.0.2 | No | Yes | Yes |
| | 12.1.0.3 | No | No | Yes |
| Oracle Fusion Applications | all versions | Yes | Yes | Yes |
| Oracle Fusion Middleware | all versions | Yes | Yes | Yes |
| Oracle Home | not applicable | Yes | Yes | Yes |
| Oracle Identity Manager for configurations: OIF, OID, OVD and DIP | | No | Yes | Yes |
| Oracle Identity Manager for configurations: OIM, OAM and OAAM | all versions | Yes | Yes | Yes |
| Oracle Management Service | not applicable | Yes | Yes | Yes |
| Oracle SOA Suite | all versions | Yes | Yes | Yes |
| Oracle Virtual Manager | all versions | Yes | Yes | Yes |
| Oracle WebLogic Server | all versions | Yes | Yes | Yes |
| Siebel | 12.1.0.3 | No | No | Yes |

### F.1.8 Configuration Data Not Available in My Oracle Support

In previous versions of Enterprise Manager, Oracle Harvester configuration data was only uploaded to My Oracle Support when 30 days had passed since the last upload of data by a standalone OCM Collector if such data already existed in My Oracle Support.

This restriction has been lifted in Enterprise Manager 12*c*. Configuration data for targets collected from Oracle Harvester running in Enterprise Manager release 12*c* displays in My Oracle Support immediately, regardless of how recently data was uploaded by a standalone OCM Collector.

## F.2 Oracle Configuration Manager

Oracle Configuration Manager is installed and configured automatically when you install an Oracle product. It is installed in the product Home and collects configuration data for all targets installed in that Home.

The OCM setup requires specifying the My Oracle Support account and password, or My Oracle Support account and Customer Support Identifier (CSI). Configuration data will be uploaded using this information and can be viewed by logging in to My Oracle Support using the same credentials.

OCM must be installed in every Oracle Home from which you want to upload configuration data to Oracle. In addition to being part of the product installation, OCM can also be downloaded from My Oracle Support. The Mass Deployment tool is available to help with deploying OCM across data centers. The OCM kit is available from the Collector tab on My Oracle Support.

Once OCM is installed, no additional work is required. By default, automatic updates are enabled and you are encouraged to use this feature to ensure you are always running the latest version of OCM. This feature can be disabled if required, for example, for security reasons. If you disable the feature, you can turn it on by executing the following command:

```
<ocm_install_root>/ccr/bin/emCCR automatic_update on
```

**Note:** If you use Enterprise Manager or Ops Center to manage your applications, we recommend that you use Oracle Harvester or Ops Center Harvester respectively to upload your configurations to Oracle. Otherwise, use OCM.

## F.3 Additional Information About MOS and OCM

To find additional information about My Oracle Support, see:

`https://support.oracle.com`

To find more information about OCM, perform the following steps:

1. Log into My Oracle Support at `https://support.oracle.com`
2. To access the **Collector** tab, click **More** and select **Collector** from the drop-down menu. The Collector page contains useful information.

## F.4 Troubleshooting Configuration Data Collection Tools

In Enterprise Manager release 12.1.0.2, ensure that collection data is uploaded to Oracle by using the `emccr status` command. Look at the last uploaded date and time.

**Note:** This `emccr status` command shows that collected data was uploaded, but does not ensure the Oracle Harvester collections were successful and uploaded.

Location of error logs:

- Oracle Harvester error logs:
  - For Harvester Job errors, look at:

    ```
    INSTANCE_HOME/sysman/log/emoms_pbs.trc
    ```

  - UI errors, for example CSI Assignment errors, look at:

    ```
    INSTANCE_HOME/sysman/log/emoms.trc
    ```

    For example:

    ```
    /gc_inst/user_projects/domains/GCDomain/servers/EMGC_
    OMS1/sysman/log/emoms.trc
    ```

- Oracle Configuration Manager log is located at:

```
ccr/hosts/<hostname>/log/collector.log
```

The following sections describe how to resolve issues with the configuration data collections:

- Oracle Harvester Collection Fails If the state/upload/external Directory Is Missing
- Oracle Configuration Manager Is Not Running
- Configuration Data Not Available in My Oracle Support
- Only a Subset of the Targets Is Collected by the Oracle Harvester

## F.4.1 Oracle Harvester Collection Fails If the state/upload/external Directory Is Missing

If the Oracle Harvester collection fails with the following error, the required directory named *external* is missing.

```
[JobWorker 75210:Thread-61] ERROR gcharvester.GcCollectionMgr initOcm.? - GC OCM
Harvester: Caught GC Harvester exception from GCInit.init(): The installed version
of Oracle Configuration Manager in the ORACLE_HOME
(/scratch/aime/work/midlwre8937/oms11g) is prior to 10.3.1. The Grid Control
Configuration harvesting requires at a minimum, 10.3.1
```

To resolve this issue, create the *external* directory:

```
$ORACLE_INSTANCE_HOME/ccr/state/upload/external
```

(Bug 12795503)

## F.4.2 Oracle Configuration Manager Is Not Running

When OCM is not running, you may see the following error:

```
2012-08-29 16:34:20,709 [JobWorker 97285:Thread-60] WARN
gcharvester.HarvesterJobUtils performOCMCollections.? - GC OCM Harvester: OCM was
stopped and is not running
```

To resolve this issue, verify that the OCM was installed and configured in the appropriate directories (execute `emCCR` status).

In particular, OCM must be installed in the OMS Oracle Home and configured (and running in connected mode) in the OMS Instance Home.

## F.4.3 Configuration Data Not Available in My Oracle Support

When you look at My Oracle Support and do not find configuration data, it could be that the Oracle Harvester collection did not run.

To resolve this issue, verify that the OCM was installed and configured in the appropriate directories (execute `emCCR status`). In particular, OCM must be installed in the OMS Oracle Home and configured (and running in connected mode) in the OMS Instance Home.

To verify that OCM is running, perform the following steps:

1. Set `ORACLE_CONFIG_HOME` to the INSTANCE HOME
2. Execute `$ORACLE_HOME/ccr/bin/emCCR status`

## F.4.4 Only a Subset of the Targets Is Collected by the Oracle Harvester

If many targets are uploaded to the Management Repository but only a subset of the targets is collected by the Oracle Harvester, it could be because the same error was encountered 10 times during a collection, causing the Oracle Harvester to stop collecting. Look at the appropriate log file to verify that this error has occurred.

Resolve the issue by running the following SQL script against the Management Repository. This script forces the Oracle Harvester to ignore this collection error and continue collecting the remaining target information.

```
sql> insert into mgmt_ocm_upl_props (name,str_value) values('ignore_
errors','true');
sql> commit;
```

Bounce the OMS after executing the SQL script.

(Bug 11734389)

# G

# Enabling the Enterprise Manager Accessibility Features

As part of the effort to make Oracle products, services, and supporting documentation accessible and usable to the disabled community, Enterprise Manager offers several features that make management data available to users of assistive technology. Enterprise Manager provides the following accessibility features:

- Support for Screen Reader
- Support for High Contrast
- Support for Large Fonts

This appendix consists of the following configuration settings you must modify to enable Screen Reader support:

- Enabling Enterprise Manager Accessibility Mode
- Setting uix-config.xml Flag
- Configuring web.xml File
- Verifying That Screen Reader Support Is Enabled

> **Note:** If Screen Reader support is enabled, then all pages related to *Refresh Process Status* are not refreshed automatically because PPR is turned off. This is an expected behavior.

## G.1 Enabling Enterprise Manager Accessibility Mode

To enable screen reader mode, do the following:

1. On the Cloud Control home page, from the **<user_name>** menu, select **My Preferences** and then select **Accessibility**.
2. In the Accessibility Preference page, select **I use a screen reader**. Click **Apply**.

   ADF accessibility mode is a session based setting which takes place immediately and does not require you to restart the Enterprise Manager Management Service.

   For ADF pages, you will see an Accessibility Preferences dialog after logging into Cloud Control for the first time. The settings in this dialog are the same as those in the Accessibility Preference page mentioned above.

## G.2 Setting uix-config.xml Flag

To enable screen reader mode for UIX pages, do the following:

1. Locate the `uix-config.xml` configuration file.

   To locate the `uix-config.xml` file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

   ```
   ./oms/sysman/archives/emgc/deployments/EMGC_
   DOMAIN/emgc.ear/em.war/WEB-INF/uix-config.xml
   ```

2. Open the `uix-config.xml` file using a text editor and set the following entry:

   ```
   <!-- An alternate configuration that disables accessibility features  -->
   <default-configuration>
   <accessibility-mode>screenReader</accessibility-mode>
   </default-configuration>
   ```

3. Save and close the file.
4. Restart the Oracle Management Service.

> **Note:** UIX accessibility mode is a product-wide setting. You will have to restart the Enterprise Manager Management Service for this setting to take effect.

> **Note:** In the `uix-config.xml` file, `enable-auto-table-ctrl-labels` is set to `true`. This enables tool tip boxes containing labels to appear when you hover your cursor over UI elements such as checkboxes and radio buttons in tables. To disable this function, change the setting to `false.`

## G.3 Configuring web.xml File

To configure web.xml file, follow these steps:

1. Locate the `web.xml` configuration file.

   To locate the `web.xml` file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

   ```
   ./oms/sysman/archives/emgc/deployments/EMGC_
   DOMAIN/emgc.ear/em.war/WEB-INF/web.xml
   ```

2. Open the `web.xml` file with your favorite text editor and locate the following six lines of the file:

   ```
   <!-- Uncomment this to enable textual chart descriptions
   <context-param>
   <param-name>enableChartDescription</param-name>
   <param-value>true</param-value>
   </context-param>
   -->
   ```

3. Remove comments from this section by deleting the first line and the last line of this section so that the section consists of only these 4 lines:

   ```
   <context-param>
   ```

```
<param-name>enableChartDescription</param-name>
<param-value>true</param-value>
</context-param>
```

4. Save and exit the file.
5. Restart the Oracle Management Service.

## G.4 Verifying That Screen Reader Support Is Enabled

Throughout Enterprise Manager, charts are used to display performance data. For most users, these charts provide a valuable graphical view of the data that can reveal trends and help identify minimum and maximum values for performance metrics.

However, charts do not convey information in a manner that can be read by a screen reader. To remedy this problem, you can configure Enterprise Manager to provide a complete textual representation of each performance chart. By default, support for the textual representation of charts is disabled. When textual description for charts is enabled, Enterprise Manager displays a small icon for each chart that can be used as a drill-down link to the textual representation.

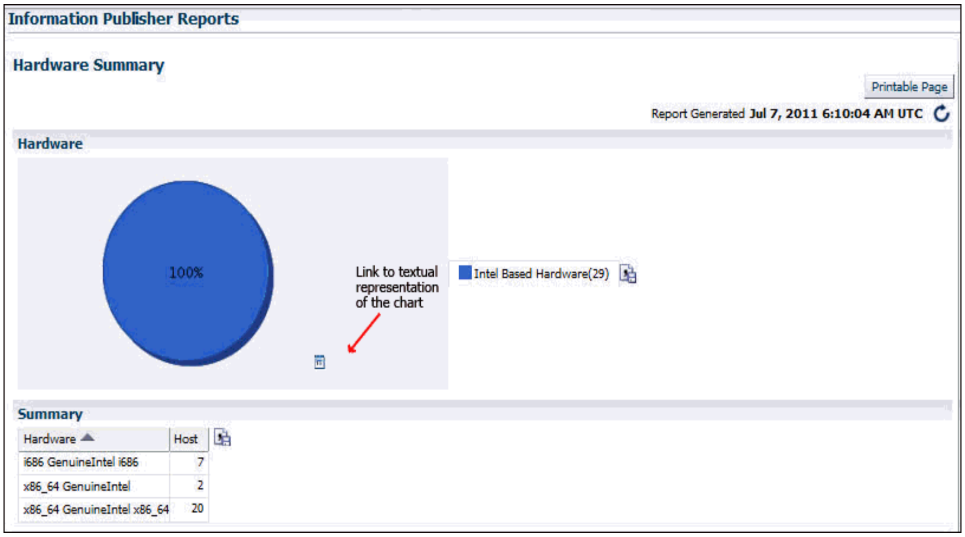
To verify whether Screen Reader support has been enabled for ADF pages, follow these steps:

1. On the Cloud Control home page, click **Help** and then select **About Enterprise Manager**.
2. In the About Enterprise Manager dialog box, ensure that **Accessibility Preference - Screen Reader Support** is set to **Enabled**.
3. If **Accessibility Preference - Screen Reader Support** is set to **Disabled**, follow the steps listed in Enabling the Enterprise Manager Accessibility Features.

To verify whether Screen Reader support has been enabled for UIX pages, follow these steps:

1. On the Cloud Control home page, from the **Enterprise** menu, select **Reports** and then select **Information Publisher Reports**.
2. In the Information Publisher Reports page, click **Hardware Summary**. The Hardware Summary page is displayed. If accessibility setting has been enabled, you will see the icon shown in Figure G–1:

***Figure G–1 Icon Representing Textual Representation of Charts***



Information Publisher Reports

Hardware Summary

Printable Page

Report Generated **Jul 7, 2011 6:10:04 AM UTC**

Hardware

100%
Link to textual representation of the chart
🟦 Intel Based Hardware(29)

Summary

| Hardware ▲ | Host |
|---|---|
| i686 GenuineIntel i686 | 7 |
| x86_64 GenuineIntel | 2 |
| x86_64 GenuineIntel x86_64 | 20 |

# H

# Configuring Targets for Failover in Active/Passive Environments

This section provides a general reference for Cloud Control administrators who want to relocate Cold Failover Cluster (CFC) targets from one existing Management Agent to another. Although the targets are capable of running on multiple nodes, these targets run only on the active node in a CFC environment.

CFC environments commonly use a combination of cluster software to provide a virtual host name and IP address along with interconnected host and storage systems to share information and provide high availability (HA) for applications. Automating failover of the virtual host name and IP, in combination with relocating the Enterprise Manager targets and restarting the applications on the passive node, requires the use of the Oracle Enterprise Manager command-line interface (EM CLI) and Oracle or third-party cluster software. Several Oracle partner vendors offer clusterware solutions in this area.

This chapter covers the following topics:

- Target Relocation in Active/Passive Environments
- Installation and Configuration
- Failover Procedure
- Failback Procedure
- EM CLI relocate_targets Parameters
- Relocation Script

## H.1 Target Relocation in Active/Passive Environments

With Oracle Enterprise Manager 12*c*, a single Oracle Management Agent running on each node in the cluster can monitor targets configured for active/passive high availability. Only one Management Agent is required on each of the physical nodes of the CFC cluster because, in case of a failover to the passive node, Enterprise Manager can move the HA monitored targets from the Management Agent on the failed node to another Management Agent on the newly activated node using a series of EMCLI commands. See the *Oracle® Enterprise Manager Command Line Interface* manual for more information.

If your application is running in an active/passive environment, the clusterware brings up the applications on the passive node in the event that the active node fails. For Enterprise Manager to continue monitoring the targets in this type of configuration, the existing Management Agent needs additional configuration.

The following sections describe how to prepare the environment to automate and restart targets on the new active node. Failover and failback procedures are also provided.

## H.2 Installation and Configuration

The following sections describe how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents communicating with the Oracle Management Service processes:

- Prerequisites
- Configuration Steps

### H.2.1 Prerequisites

The following steps assume that the monitored targets have already been installed and configured for failover in a CFC.

Prepare the Active/Passive environments as follows:

- Ensure the operating system clock is synchronized across all nodes of the cluster. (Consider using Network Time Protocol (NTP) or another network synchronization method.)
- Install management agents on each node in the cluster using the physical hostname. Install the Management Agent on a local disk volume on each node in the cluster. Once installed, the Management Agents are visible in the Cloud Control console.
- Install and configure EMCLI on each node in the CFC cluster. See the *Oracle® Enterprise Manager Command Line Interface Guide* for more information.
- When a target is being relocated, ensure that the plug-in version and plug-in revision are the same on both the Management Agent of the failed node and the Management Agent of the newly activated node.

### H.2.2 Configuration Steps

The following steps show how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents that are communicating with the OMS processes. The example that follows is based on a configuration with a two-node cluster that has one failover group.

Configuration involves two steps:

- Discovering Targets
- Deploying Plug-ins

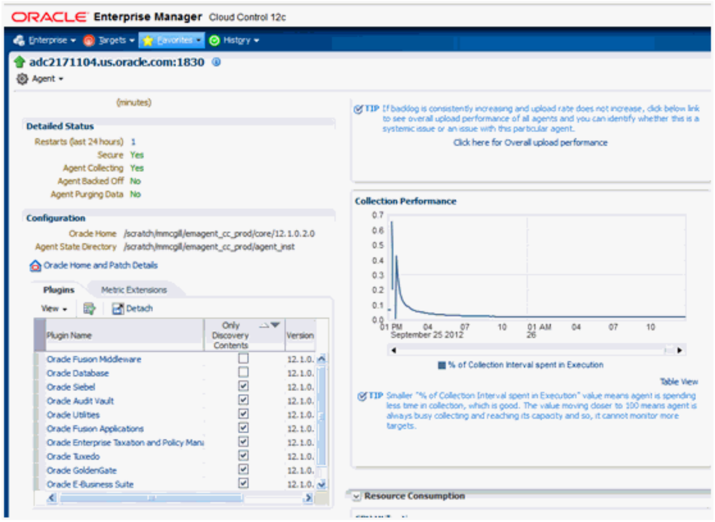
#### H.2.2.1 Discovering Targets

After the Active / Passive targets have been configured, use the Add Targets Manually screens in the Cloud Control console to add the targets (such as database, listener, application server, and so on). This screen can be accessed by navigating to Setup | Add Target | Add Targets Manually. You should perform this step specifying the active node (the node that is currently hosting the target to be added).

### H.2.2.2 Deploying Plug-ins

After the target has been added determine which plug-ins have been deployed on the agent for the active host. This can be found by navigating to the agent homepage and viewing the plug-ins tab in the Configuration region.

***Figure H–1 Agent Home Page***



adc2171104.us.oracle.com:1830

**Detailed Status**

Restarts (last 24 hours) 1
Secure Yes
Agent Collecting Yes
Agent Backed Off No
Agent Purging Data No

**Configuration**

Oracle Home /scratch/mmcgill/emagent_cc_prod/core/12.1.0.2.0
Agent State Directory /scratch/mmcgill/emagent_cc_prod/agent_inst

Oracle Home and Patch Details

| Plugin Name | Only Discovery Contents | Version |
|---|---|---|
| Oracle Fusion Middleware | □ | 12.1.0. |
| Oracle Database | □ | 12.1.0. |
| Oracle Siebel | ☑ | 12.1.0. |
| Oracle Audit Vault | ☑ | 12.1.0. |
| Oracle Utilities | ☑ | 12.1.0. |
| Oracle Fusion Applications | ☑ | 12.1.0. |
| Oracle Enterprise Taxation and Policy Manı | ☑ | 12.1.0. |
| Oracle Tuxedo | ☑ | 12.1.0. |
| Oracle GoldenGate | ☑ | 12.1.0. |
| Oracle E-Business Suite | ☑ | 12.1.0. |

TIP If backlog is consistently increasing and upload rate does not increase, click below link to see overall upload performance of all agents and you can identify whether this is a systemic issue or an issue with this particular agent.

Click here for Overall upload performance

TIP Smaller "% of Collection Interval spent in Execution" value means agent is spending less time in collection, which is good. The value moving closer to 100 means agent is always busy collecting and reaching its capacity and so, it cannot monitor more targets.

Make a note of the Plug-ins that do not have the Only Discovery Contents box checked. These plug-ins need to be deployed on the agent of the passive node.

After determining which plug-ins are missing by looking at the Agent homepage of the passive node, deploy any missing plug-ins by navigating to Setup | Extensibility | Plug-ins, selecting the relevant plug-in and using the Deploy on Management Agent menu to deploy the plug-in.

## H.3 Failover Procedure

To speed relocation of targets after a node failover, configure the following steps using a script that contains the commands necessary to automatically initiate a failover of a target. Typically, the clusterware software has a mechanism with which you can automatically execute the script to relocate the targets in Enterprise Manager. Also, see "Relocation Script" on page H-5 for a sample script.

1. Shut down the target services on the failed active node.

   On the active node where the targets are running, shut down the target services running on the virtual IP.

2. If required, disconnect the storage for this target on the active node.

   Shut down all the applications running on the virtual IP and shared storage.

3. Enable the target's IP address on the new active node.

4. If required, connect storage for the target on the currently active node.

5. Relocate the targets in Cloud Control using EM CLI.

   To relocate the targets to the Management Agent on the new active node, run the EM CLI *relocate_targets* verb for each target type (such as a listener or application servers) that you must relocate after the failover operation.

Example:

```
emcli relocate_targets
-src_agent=<node 1>:3872
-dest_agent=<node 2>:3872
-target_name=<database_name>
-target_type=oracle_database
-copy_from_src
-force=yes
```

In this example, port 3872 is the default port for the Management Agent. To find the appropriate port number for your configuration, use the value for the Agent URL parameter. You can determine this parameter by running the following command for the Management Agent:

```
emctl status agent
```

**Note:** In case of a failover event, the source Agent may not be running. However, there is no need to have the source Management Agent running to accomplish the relocate operation. EM CLI is an OMS client that performs its relocate operations directly against the Management Repository.

6. Bring up all targets on the new active node.
7. From the Enterprise Manager console, ensure all relocated targets are up and running .

## H.4 Failback Procedure

To return the HA targets to the original active node, or to any other cluster member node:

1. Repeat the steps in "Failover Procedure" on page H-3 to return the HA targets to the active node.
2. Verify the target status in the Enterprise Manager console.

## H.5 EM CLI relocate_targets Parameters

As shown in Section H.3, "Failover Procedure", you run the EM CLI `relocate_targets` verb for each target type that will be failed over to (or be switched over) during relocation operations. Table H–1, " relocate_targets Verb Parameters" documents the verb parameters associated with this EM CLI verb.

*Table H–1 relocate_targets Verb Parameters*

| EM CLI Parameter | Description |
|---|---|
| -src_agent | Management Agent on which the target was running before the failover occurred. |
| -dest_agent | Management Agent that will be monitoring the target after the failover. |
| -target_name | Name of the target to be failed over. |

*Table H–1 (Cont.) relocate_targets Verb Parameters*

| EM CLI Parameter | Description |
|---|---|
| -target_type | Type of target to be failed over (internal Enterprise Manager target type). For example, the Oracle database (for a standalone database or an Oracle RAC instance), the Oracle listener for a database listener, and so on. |
| -copy_from_src | Use the same type of properties from the source Management Agent to identify the target. This is a **MANDATORY** parameter. Not supplying this parameter may result in the corruption of the target definition. |
| -force | Force dependencies (if needed) to failover as well. |

## H.6 Relocation Script

The following example shows a relocation script that can executed from a clusterware configuration when a failover operation occurs.

Before running the script:

- Set up the *Default Normal Host Credential* with *Normal Host Credential*.
- Set up the *Target Preferred Credential* of the database instance with the *Normal Database Credential*, *SYSDBA Database Credential*, and *Database Host Credential*.

### H.6.1 Relocation Script Example

```
#! /bin/ksh
#get the status of the targets

emcli get_targets
 -targets="db1:oracle_database;listener_db1:oracle_listener"
 -noheader

  if [[ $? != 0 ]]; then exit 1; fi

# blackout the targets to stop false errors.  This blackout is set to expire in 30
minutes.

emcli create_blackout
 -name="relocating active passive test targets"
 -add_targets="db1:oracle_database;listener_db1:oracle_listener"
 -reason="testing failover"
 -schedule="frequency:once;duration:0:30"

  if [[ $? != 0 ]]; then exit 1; fi

# relocate the targets to the new host

emcli relocate_targets
 -src_agent=host1.example.com:3872
 -dest_agent=host2.example.com:3872
 -target_name=db1 -target_type=oracle_database
 -copy_from_src -force=yes

  if [[ $? != 0 ]]; then exit 1; fi

emcli relocate_targets
 -src_agent=host1.example.com:3872
 -dest_agent=host2.example.com:3872
 -target_name=listener_db1
 -target_type=oracle_listener
 -copy_from_src -force=yes

  if [[ $? != 0 ]]; then exit 1; fi


# End the blackout and let the targets become visible

emcli stop_blackout
 -name="relocating active passive test targets"

  if [[ $? != 0 ]]; then exit 1; fi

# Recheck the status of the targets

emcli get_targets
 -targets="db1:oracle_database;listener_db1:oracle_listener"
 -noheader

  if [[ $? != 0 ]]; then exit 1; fi
```

# I

# Standby OMSs Using Standby WebLogic Domain

The following standby OMS implementation is used for Enterprise Manager Release 12.1.0.2 and earlier installations. For Enterprise Manager Release 12.1.0.3 and later, see Chapter 18, "Enterprise Manager Disaster Recovery."

> **IMPORTANT:** Standby OMSs using Standby WebLogic Domain are still supported but have been deprecated and may be de-supported in a future release (see My Oracle Support Note 1563541.1 for details).
>
> BI Publisher server configuration is not supported on standby OMSs using Standby Weblogic Domain for Cloud Control 12.1.0.4 and later.

## I.1 Configuring Standby Management Services on a Standby Site

Consider the following before installing the standby Management Services.

Oracle recommends that this activity be done during a lean period or during a planned maintenance window. When new Oracle Management Service instances are installed on the standby site, they are initially configured to connect to the Management Repository database on the primary site. Some workload will be taken up by the new Management Service. This could result in temporary loss in performance if the standby site Management Services are located far away from the primary site Management Repository database. However there would be no data loss and the performance would recover once the standby Management Services are shutdown post configuration.

### Prerequisites

- The primary site must be configured as per Cloud Control MAA guidelines described in previous sections. This includes Management Services fronted by an SLB and all Management Agents configured to upload to Management Services by the SLB.
- The standby site must be similar to the primary site in terms of hardware and network resources to ensure there is no loss of performance when failover happens.
- Configure storage used by the software library to be replicated at the primary and standby site. In the event of a site outage, the contents of this storage must be made available on the standby site using hardware vendor disk level replication technologies.

- The shared storage used for the software library must be made available on the standby site using the same paths as the primary site.
- For complete redundancy in a disaster recovery environment, a second load balancer must be installed at the standby site. The secondary SLB must be configured in the same fashion as the primary. Some SLB vendors (such as F5 Networks) offer additional services that can be used to pass control of the Virtual IP presented by the SLB on the primary site to the SLB on the standby site in the event of a site outage. This can be used to facilitate automatic switching of Management Agent traffic from the primary site to the standby site.
- Oracle Platform Security Services (OPSS) is the underlying security platform that provides security to Oracle Fusion Middleware including products like WebLogic Server, SOA, and WebCenter and serves as the single security framework for both Oracle and third-party environments. After upgrading Enterprise Manager, you many encounter configuration problems when attempting to set up a standby site if the Weblogic domain name and the OPSS farm name do not match. Specifically, you will run into this issue after switching over from primary to standby, upgrading the new primary site, and then attempting to create new standby sites. The name used for the primary domain is the original name and can be found in the jps-config.xml file of the original primary site.

### I.1.1 Installing the First Standby Management Service

Install the first standby Management Service using the following steps:

1. Copy the emkey to the Management Repository by running the following command on the first Management Service on the primary site:

   ```
   emctl config emkey -copy_to_repos
   ```

2. Export the configuration from the first Management Service on the primary site using:

   ```
   emctl exportconfig oms -dir <location for the export file>
   ```

   After the configuration is exported, do not make any configuration changes to the primary site till the standby management service is configured.

3. Install a Management Agent on the standby host if one does not already exist.
4. Perform a software-only install of the Enterprise Manager software using a modified version of the “Add Management Service” Deployment Procedure.
   1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
   2. Select **Add Oracle Management Service** procedure and click **Create Like**.
   3. Go to the **Procedure Steps** tab and select and disable the steps - “Configure Oracle Management Service”, “Targets Discovery” and “Post Configuration Tasks”.
   4. Save the modified deployment procedure and use it to install the Enterprise Manager software on the standby OMS host.
   5. After the Deployment Procedure completes, delete the file emInstanceMapping.properties from <OMS Oracle Home>/sysman/config on the standby OMS host.
5. Configure the Management Service by running `omsca` in standby mode. Choose a different domain name for the standby. For example, if the primary WebLogic domain is GCDomain, choose GCDomainStby.

```
omsca standby -EM_PRIMARY_DOMAIN_NAME GCDomain -EM_DOMAIN_NAME
GCDomainStby -NM_USER nodemanager -AS_USERNAME weblogic -nostart
```

When prompted for the Administration Server host and EM Instance host, enter the standby OMS hostname (or accept the default).

When prompted for the passwords, provide the same passwords as the primary site.

When prompted for Management Repository details, provide the primary database details.

> **Important:** When running `omsca standby`, if the OMS Oracle Home has been installed in software-only mode, then you must first copy the *ORACLE_HOME/sysman/config/farmkey* from the primary OMS machine to this new Oracle Home at the same location (ORACLE_HOME/sysman/config).

6. Configure the required plug-ins by running the following command:

   ```
   pluginca -action deploy -isFirstOMS true -plugins <plugin-list>
   -oracleHome <oms oracle home> -middlewareHome <wls middleware home>
   ```

   where plugin-list is the list of plug-ins returned by the SQL query

   ```
   SELECT epv.plugin_id, epv.version FROM em_plugin_version epv, em_
   current_deployed_plugin ecp WHERE epv.plugin_type NOT IN ( 'BUILT_IN_
   TARGET_TYPE' , 'INSTALL_HOME') AND ecp.dest_type='2' AND epv.plugin_
   version_id = ecp.plugin_version_id;
   ```

   and is a comma separated list in the following format:
   `<plugin-id>=<plugin-version>,<plugin-id>=<plugin-version>,…`

   **Example**:
   ```
   oracle.sysman.empa=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.sysma
   n.emas=12.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.db=12.1.0
   .1.0,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.s
   ysman.ssa=12.1.0.1.0
   ```

7. Copy over the configuration exported from the primary Management Service in step 2 above to the standby Management Service host. Import the exported configuration on the standby Management Service using:

   ```
   emctl importconfig oms -file <full path of the export file>
   ```

   Note this command will start the Management Service.

8. Stop the Management Service but leave the Administration Server running using:

   ```
   emctl stop oms
   ```

9. Add the standby Weblogic Domain and associated targets:

   The standby Weblogic Domain and associated targets can be added using the Guided Discovery process.

   1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**.
   2. Select **Add Targets Using Guided Process**.

3. Select **Oracle Fusion Middleware/WebLogic Domain** from the **Target Types** menu.
4. Use the secure port (typically 7101) and, under Advanced, set the JMX Protocol to t3s.

> **Note:** The WebLogic targets, except the Administration Server, will be shown as down as the standby OMS is down at this stage.

10. If you have Single Sign On configured on the primary site, follow the same steps to configure SSO on the standby OMS.
11. If you have Real User Experience Insight, AD4J Manager or BI Publisher configured on the primary site, follow the same steps to configure them on the standby OMS.

### I.1.2 Installing the First Standby Management Service (Oracle Installer, Software Only Mode)

1. Copy the emkey to the Management Repository by running the following command on the first OMS on the primary site:

   ```
   emctl config emkey -copy_to_repos
   ```

2. Export the configuration from the first OMS on the primary site.

   ```
   emctl exportconfig oms -dir <location for the export file>
   ```

   After the configuration is exported, do not make any configuration changes to the primary site until the standby OMS is configured.

3. On the remote host, perform a software-only installation of the standby OMS as described in the Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide chapter "Installing Enterprise Manager Software Now and Configuring Later" (Installing in Graphical Mode). Ensure that you install the software binaries in the same middleware location as that of the primary OMS.

   > **Note:** Make sure you select same set of plug-ins as the primary OMS.

   If you have installed extra plug-ins which are not part of the installation, then complete the following steps.

   1. Connect to repository and execute the following query to obtain the list of installed plug-ins:

      ```
      SELECT epv.plugin_id "plugin id", epv.version "version", epv.rev_version
      "revision", epv.su_entity_id "update id"
      FROM em_plugin_version epv, em_current_deployed_plugin ecp
      WHERE epv.plugin_type NOT IN ('BUILT_IN_TARGET_TYPE', 'INSTALL_HOME')
      AND ecp.dest_type='2'
      AND epv.plugin_version_id = ecp.plugin_version_id;
      ```

      Write down the returned list of plug-ins installed.

   2. Extract the plug-in archives from the primary site.

      ```
      emcli export_update -id=<update id> -host=<standby OMS host>
      ```

```
-dir=<directory to export archives> <host credential options>
```

where <update id> is the value returned by the four column of query above.

Note that this command generates a file with a .zip extension. Rename the file from *<file_name>.zip* to *<file_name>.opar* .

Repeat above steps for all plugins. In standby OMS host, place all .opar files in one directory *<plugin dir >*.

3. Invoke runInstaller and choose software-only install. This will install only the middleware home and OMS Oracle homes.
4. To install the required plug-ins, run the plug-in install script.

```
<OMS_HOME>/sysman/install/PluginInstall.sh -pluginLocation <plugin dir>
```

where <plugin dir> is the directory where you placed extra plug-ins in step two above. Running this command displays a screen that will let you select the plug-ins to install. Verify that all the plug-ins listed in step 1 appear and that you select them. If there is a mismatch, OMS configuration may fail at a later step.

4. On the software-only installation, apply all the patches you applied on the primary OMS so that both the primary and standby OMSs are identical and are in sync.
5. Configure the OMS by running *omsca* in standby mode. Choose a different domain name for the standby. For example, if the primary WebLogic domain is GCDomain, choose GCDomainStby.

```
omsca standby -EM_DOMAIN_NAME GCDomainStby -NM_USER nodemanager -AS_USERNAME
weblogic -nostart
```

When prompted for the Administration Server host and Enterprise Manager Instance host, enter the standby OMS hostname (or accept the default).

When prompted for the passwords, provide the same passwords as the primary site.

When prompted for Management Repository details, provide the primary database details.

6. Configure the required plug-ins by running the following command:

```
pluginca -action deploy -isFirstOMS true -plugins <plug-in list> -oracleHome
<oms oracle home> -middlewareHome <wls middleware home>
```

where *plug-in list* is the list of plug-ins returned by the SQL query.

```
SELECT epv.plugin_id, epv.version FROM em_plugin_version epv, em_current_
deployed_plugin ecp WHERE epv.plugin_type NOT IN ( 'BUILT_IN_TARGET_TYPE' ,
'INSTALL_HOME') AND ecp.dest_type='2' AND epv.plugin_version_id = ecp.plugin_
version_id;
```

The plug-in list must be a comma separate list in the following format:

<plugin-id>=<plugin-version>,<plugin-id>=<plugin-version>,…

**Example:**

```
oracle.sysman.empa=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.sysman.emas=1
2.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.db=12.1.0.1.0,oracle.sysm
an.emct=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.sysman.ssa=12.1.0.1.0
```

7. Copy over the configuration exported from the primary OMS in step 2 above to the standby OMS host. Import the exported configuration on the standby OMS:

   ```
   emctl importconfig oms -file <full path of the export file>
   ```

   Note that this command generates a warning about a failed export and prompts for confirmation in order to proceed. The warning can be ignored by entering "y" to proceed.

   This command will automatically start the OMS.

8. Stop the Management Service but leave the Administration Server running using:

   ```
   emctl stop oms
   ```

9. Configure the Management Agent on the second OMS host by running the following command from the OMS home:

   ```
   $<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<middleware_
   home>/agent OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_port> AGENT_
   REGISTRATION_PASSWORD=<password> -configOnly
   ```

   Note: If you have an SLB configured, then directly specify the host and port of the primary load balancer.

   If no SLB is configured, then use the secure upload port of primary OMS.

   Example:

   ```
   ./agentDeploy.sh AGENT_BASE_DIR=$MIDDLEWARE_BASE/agent OMS_HOST=prim_oms_
   hhost.domain.com EM_UPLOAD_PORT=4900 AGENT_REGISTRATION_PASSWORD=password
   -configOnly
   ```

10. Deploy the required plug-ins on the Management Agent.

    For information about deploying plug-ins, refer to the chapter on *Managing Plug-Ins* in the of the Enterprise Manager Cloud Control Administrator's Guide.

11. Add the standby WebLogic Domain and associated targets:

    The standby WebLogic Domain and associated targets can be added using the Guided Discovery process.

    From the **Setup** menu, select **Add Target** , then select **Add Targets Manually.** Select **Oracle Fusion Middleware** from the **Target Types** menu. Use the secure port (typically 7101) and, under **Advanced**, set the JMX Protocol to *t3s*.

    Note that the WebLogic targets, except the Administration Server, will be shown as "down" since the standby OMS is down at this stage.

12. If you have Single Sign-On configured on the primary site, follow the same steps to configure SSO on the standby OMS.

13. If you have Real User Experience Insight, AD4J Manager or BI Publisher configured on the primary site, follow the same steps to configure them on the standby OMS.

### I.1.3 Installing Additional Standby Management Services

It is recommended that your standby site be similar in configuration as your primary site. This means configuring multiple OMS on your standby site, similar to your primary site.

1. Start the standby Administration Server by running the following command on the first standby Management Service:

   ```
   emctl start oms -admin_only
   ```

2. Export the configuration from the first Management Service on the primary site using:

   ```
   emctl exportconfig oms -dir <location for the export file>
   ```

   After the configuration is exported, do not make any configuration changes to the primary site until the standby management service is configured.

3. Install a Management Agent on the standby host.
4. Perform a software-only install of the Enterprise Manager software using a modified version of “Add Oracle Management Service” Deployment Procedure.
   1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
   2. Select **Add Oracle Management Service** procedure and then click **Create Like**.
   3. Go to the Procedure Steps tab and select and disable the steps - “Configure Management Service”, “Targets Discovery” and “Post Configuration Tasks”.
   4. Save the modified deployment procedure and use it to install the Enterprise Manager software on the standby OMS host.
   5. After the Deployment Procedure completes, delete the file emInstanceMapping.properties from <OMS Oracle Home>/sysman/config on the standby OMS host.
5. Configure the Management Service by running omsca.

   ```
   omsca add -nostart
   ```

   When prompted for Management Repository details, provide the primary database details.

   When prompted for Administration Server details, provide the standby administration server details.

6. Configure the required plug-ins by running the following command:

   ```
   pluginca -action deploy -isFirstOMS false -plugins <plugin-list>
   -oracleHome <oms oracle home> -middlewareHome <wls middleware home>
   ```

   where *plugin-list* is the list of plug-ins returned by the SQL query

   ```
   SELECT epv.plugin_id, epv.version FROM em_plugin_version epv, em_
   current_deployed_plugin ecp WHERE epv.plugin_type NOT IN ( 'BUILT_IN_
   TARGET_TYPE' , 'INSTALL_HOME') AND ecp.dest_type='2' AND epv.plugin_
   version_id = ecp.plugin_version_id;
   ```

   and is a comma separated list in the following format:
   `<plugin-id>=<plugin-version>,<plugin-id>=<plugin-version>,…`

   **Example**

   ```
   oracle.sysman.empa=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.sysma
   n.emas=12.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.db=12.1.0
   .1.0,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.s
   ysman.ssa=12.1.0.1.0
   ```

7. Copy over the configuration exported from the primary Management Service in step 1 above to the standby Management Service host. Import the exported configuration on the standby Management Service using:

   ```
   emctl importconfig oms -file <full path of the export file>
   ```

   Note this command will start the Management Service.

8. Stop the Management Service using:

   ```
   emctl stop oms
   ```

9. Refresh the standby domain target from the console. This will present a guided workflow to discover and add the new managed server and associated targets.
10. If you have Single Sign On configured on the primary site, follow the same steps to configure SSO on the standby OMS.
11. If you have Real User Experience Insight, AD4J Manager or BI Publisher configured on the primary site, follow the same steps to configure them on the standby OMS.

## I.1.4 Installing Additional Standby Management Services (Oracle Installer, Software Only Mode)

1. Start the standby Administration Server by running the following command on the first standby Management Service:

   ```
   emctl start oms -admin_only
   ```

2. Export the configuration from the first Management Service on the primary site using:

   ```
   emctl exportconfig oms -dir <location for the export file>
   ```

   After the configuration is exported, do not make any configuration changes to the primary site still the standby management service is configured.

3. On the remote host, perform a software-only installation of the standby OMS as described in the Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide chapter "Installing Enterprise Manager Software Now and Configuring Later" (Installing in Graphical Mode). Ensure that you install the software binaries in the same middleware location as that of the primary OMS.

   **Note:** Make sure you select same set of plug-ins as the primary OMS.

   If you have installed extra plug-ins which are not part of the installation, then complete the following steps.

   1. Connect to repository and execute the following query to obtain the list of installed plug-ins:

      ```
      SELECT epv.plugin_id "plugin id", epv.version "version", epv.rev_version
      "revision", epv.su_entity_id "update id"
      FROM em_plugin_version epv, em_current_deployed_plugin ecp
      WHERE epv.plugin_type NOT IN ('BUILT_IN_TARGET_TYPE', 'INSTALL_HOME')
      AND ecp.dest_type='2'
      AND epv.plugin_version_id = ecp.plugin_version_id;
      ```

Write down the returned list of plug-ins installed.

2. Extract the plug-in archives from the primary site.

   ```
   emcli export_update -id=<update id> -host=<standby OMS host>
   -dir=<directory to export archives> <host credential options>
   ```

   where `<update id>` is the value returned by the four column of query above.

   Note that this command generates a file with a .zip extension. Rename the file from *<file_name>.zip* to *<file_name>.opar* .

   Repeat above steps for all plugins. In standby OMS host, place all .opar files in one directory *<plugin dir* >.

3. Invoke runInstaller and choose software-only install. This will install only the middleware home and OMS Oracle homes.

4. To install the required plug-ins, run the plug-in install script.

   ```
   <OMS_HOME>/sysman/install/PluginInstall.sh -pluginLocation <plugin dir>
   ```

   where `<plugin dir>` is the directory where you placed extra plug-ins in step two above. Running this command displays a screen that will let you select the plug-ins to install. Verify that all the plug-ins listed in step 1 appear and that you select them. If there is a mismatch, OMS configuration may fail at a later step.

4. On the software-only installation, apply all the patches you applied on the primary OMS so that both the primary and standby OMSs are identical and are in sync.

5. Configure the Management Service by running omsca.

   ```
   omsca add -nostart
   ```

   When prompted for Management Repository details, provide the primary database details. When prompted for Administration Server details, provide the standby Administration Server details.

   To keep the ports consistent with your primary site, provide all the ports on the command line itself. For example:

   ```
   omsca add -MSPORT 7202 -MS_HTTPS_PORT 7301 -EM_NODEMGR_PORT 7403 -EM_UPLOAD_
   PORT 4889 -EM_UPLOAD_HTTPS_PORT 4900 -EM_CONSOLE_PORT 7788 -EM_CONSOLE_HTTPS_
   PORT 7799 -nostart
   ```

6. Configure the required plug-ins by running the following command:

   ```
   pluginca -action deploy -isFirstOMS false -plugins <plugin-list>
   -oracleHome <oms oracle home> -middlewareHome <wls middleware home>
   ```

   where the plugin-list is the list of plug-ins returned by the SQL query above and is a comma separated list in the following format:
   `<plugin-id>=<plugin-version>,<plugin-id>=<plugin-version>,…`

   **Example**

   ```
   oracle.sysman.empa=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.sysma
   n.emas=12.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.db=12.1.0
   .1.0,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.s
   ysman.ssa=12.1.0.1.0
   ```

7. Copy over the configuration exported from the primary Management Service in step 1 above to the standby Management Service host. Import the exported configuration on the standby Management Service using:

   ```
   emctl importconfig oms -file <full path of the export file>
   ```

   Note this command emits a warning about a failed export and prompts for confirmation to proceed. The warning can be ignored by entering "y" to proceed.

   Note this command will automatically start the OMS.

8. Stop the OMS using:

   ```
   emctl stop oms
   ```

9. Configure the Management Agent on the second OMS host by running the following command from the OMS home:

   ```
   $<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<middleware_
   home>/agent OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_port> AGENT_
   REGISTRATION_PASSWORD=<password> -configOnly
   ```

   **Note:** If you have an SLB configured, then directly specify the host and port of the primary load balancer.

10. Deploy the required plug-ins on the Management Agent.

    For information about deploying plug-ins, refer to the *Updating Cloud Control* chapter of the Enterprise Manager Cloud Control Administrator's Guide.

11. Refresh the standby domain target from the console. This will present a guided workflow to discover and add the new managed server and associated targets.

12. If you have Single Sign On configured on the primary site, follow the same steps to configure SSO on the standby OMS.

13. If you have Real User Experience Insight, AD4J Manager or BI Publisher configured on the primary site, follow the same steps to configure them on the standby OMS.

## I.1.5 Validating Your Installation and Complete the Setup

Update the standby SLB configuration by adding the standby Management Service(s) to the different pools on the SLB. Setup monitors for the new Management Service.

### I.1.5.1 Keeping the Standby Site in Sync

After the initial setup of the standby site, the standby site has to be kept in sync with the changes done on primary site. Transactions on the primary Management Repository get propagated to the Standby Management Repository automatically through Data Guard but the OMS side changes have to be redone manually on the standby site. The following sections describe this procedure for typical activities.

#### Applying patches

When patches are applied on the primary site Management Services, they have to be applied on the standby site Management Services too. Note that patches typically update the Oracle Homes (via the OPatch apply command) and optionally might require scripts to be run against the Management Repository. On the standby site, it is sufficient to update the Oracle Homes (via the OPatch apply command) and skip the running of scripts on the Management Repository because database changes are automatically propagated to the standby site using Data Guard.

### Managing Plug-ins

When new plug-ins are deployed on the primary site or existing plug-ins upgraded or un-deployed on the primary site, the following procedures needs to be run on the standby site too to keep the Standby Management Services in sync. Note if the Standby Management Services are not kept in sync, they would fail to start when a switchover or failover operation is attempted.

The procedure below assumes that the standby site was setup as per the documented process and the standby management services are currently down and point to the primary repository. The plug-in(s) deployment on the primary site has been completed successfully.

### Deploying a New Plug-in or Upgrading a Plug-in on a Standby Site

1. Extract the plug-in archives from the primary site

   Go to the Self Update Home, click on Plug-ins, select the required plug-in and select export from the Action table menu. Note the EM CLI command from the popup that gets displayed.

   ```
   emcli export_update -id=<update id> -deep -host=<standby OMS host>
   -dir=<directory to export archives> <host credential options>
   ```

   Note that an additional option "-deep" is required. This command would create 4 files on the destination directory specified. The filename <version>_OMS_<platform>_<revision>.zip is the one to be used in next step.

2. Start the Standby Administration Server, if it is down.

   ```
   emctl start oms -admin_only
   ```

3. Run prerequisite checks for the plug-in and apply the required patch reported by after running the following command.

   ```
   ./emctl plugin deploy -action prereqcheck -isFirstOMS false -archives
   <exported_plugin_archive>
   ```

   where `<exported_plugin_archive>` is the zip file that was exported in Step 1: *<version>_OMS_<platform>_<revision>.zip*

**Important: Deploying Plug-in Revisions**

If the plug-ins you are attempting to deploy have revision versions, you must add the `-revisions <list_of_revisions>` option when executing the `emctl plugin deploy` command. Without the `-revisions` option, the plug-in CA attempts to copy the plug-in XML for the base revision over the existing correct plug-in XML, thus overwriting revision information.

For example, the commands to check prerequisites and deploy 12.1.0.3.0 DB plug-in revision 20130402 on a stand-by OMS are as follows:

```
./emctl plugin deploy -action prereqcheck -isFirstOMS false
-archives 12.1.0.3.0_OMS_2000_20130402.zip -revisions 20130402

./emctl plugin deploy -action deploy -isFirstOMS false
-archives 12.1.0.3.0_OMS_2000_20130402.zip -revisions 20130402
```

4. Configure the plug-in on the first standby OMS Oracle Home.

   ```
   ./emctl plugin deploy -action deploy -isFirstOMS false -archives <exported_
   plugin_archive>
   ```

   where `exported_plugin_archive` represents the zip file *<version>_OMS_<platform>_<revision>.zip*

5. Repeat steps 3 and 4 for each standby additional OMS/

   ```
   ./emctl plugin deploy -action prereqcheck -isFirstOMS true -archives <exported_
   plugin_archive>

   ./emctl plugin deploy -action deploy -isFirstOMS true -archives <exported_
   plugin_archive>
   ```

   This completes the plug-in deployment on the standby site.

### Sync Up Sysman Credentials

When administrators modify sysman credentials on the primary site, the following procedure must be run on the standby site in order to keep the standby management service in sync with respect to sysman credentials.

If the sysman credentials for the primary and standby sites are not kept in sync, they will fail to start when switchover or failover operations are attempted. In addition, the administrator will not be able to log into the standby OMS once the switchover operation is complete.

The procedure below assumes that the standby site was set up according to the documented process and the standby management services are currently down and point to the primary repository. The plug-in(s) deployment on the primary site has been completed successfully.

Perform following steps on the standby management service:

1. Stop all Enterprise Manager processes.

   ```
   emctl stop oms -all &
   ```

2. Stop any remaining Enterprise Manager processes using the "kill" command on UNIX platforms or by using the Process Explorer or similar process monitoring tool on Windows platforms.
3. Change the datasource password by running the following command:

   ```
   emctl config oms -update_ds_pwd -ds_name sysman-opss-ds [-ds_pwd <new_
   pwd>]
   ```

4. Start the AdminServer by itself by running the following command:

   ```
   emctl start oms -admin_only
   ```

5. Change the SYSMAN password:

   ```
   emctl config oms -change_repos_pwd [-use_sys_pwd]
   ```

6. Restart all Enterprise Manager processes:

   ```
   emctl stop oms -all &
   ```

   ```
   emctl start oms
   ```

## I.2 Managing Switchover and Failover Operations

Outages can be planned as might be the case when performing upgrades or periodic maintenance, or unplanned as can happen in the event of hardware/software failure, or perhaps some environmental catastrophe. Regardless of the type of outage, you want to ensure that your IT infrastructure can be restored and running as soon as possible.

This section covers:

- Switchover
- Failover

### I.2.1 Switchover

> **Warning:** The following switchover instructions are only for use with the Standby OMSs using Standby WebLogic Domain disaster recovery approach as originally used in Enterprise Manager Release 12.1.0.2 and earlier installations as detailed in this appendix.
>
> For switchover instructions for the Standby OMSs using Storage Replication disaster recovery approach used in Enterprise Manager Release 12.1.0.3 and later, see Chapter 18, "Enterprise Manager Disaster Recovery."

Switchover is a planned activity where operations are transferred from the Primary site to a Standby site. This is usually done for testing and validation of Disaster Recovery (DR) scenarios and for planned maintenance activities on the primary infrastructure.

This section describes the steps to switchover to the standby site. The same procedure is applied to switchover in either direction.

Enterprise Manager Console cannot be used to perform switchover of the Management Repository database. Use the Data Guard Broker command line tool DGMGRL instead.

1. Prepare the Standby Database

   Verify that recovery is up-to-date. Using the Enterprise Manager Console, you can view the value of the ApplyLag column for the standby database in the Standby Databases section of the Data Guard Overview Page.

2. Shut down the Primary Enterprise Manager Application Tier.

   Shutdown all the Management Service instances in the primary site by running the following command on each Management Service:

   ```
   emctl stop oms -all
   ```

3. Verify Software Library Availability

   Ensure all files from the primary site are available on the standby site.

4. Switch over to the Standby Database

   Use DGMGRL to perform a switchover to the standby database. The command can be run on the primary site or the standby site. The switchover command verifies the states of the primary database and the standby database, affects switchover of roles, restarts the old primary database, and sets it up as the new standby database.

   ```
   SWITCHOVER TO <standby database name>;
   ```

   Verify the post switchover states. To monitor a standby database completely, the user monitoring the database must have SYSDBA privileges. This privilege is required because the standby database is in a mounted-only state. A best practice is to ensure that the users monitoring the primary and standby databases have SYSDBA privileges for both databases.

   ```
   SHOW CONFIGURATION;
   ```

   ```
   SHOW DATABASE <primary database name>;
   ```

   ```
   SHOW DATABASE <standby database name>;
   ```

5. Start the AdminServer if it is not already running on the standby site.

   ```
   emctl start oms -admin_only
   ```

6. Make the standby Management Services point to the Standby Database which is now the new Primary by running the following on each standby Management Service.

   ```
   emctl config oms -store_repos_details -repos_conndesc <connect
   descriptor of new primary database> -repos_user sysman
   ```

7. Startup the Enterprise Manager Application Tier.

   Startup all the Management Services on the standby site:

   ```
   emctl start oms
   ```

8. Relocate Management Services and Management Repository target

   The Management Services and Management Repository target is monitored by a Management Agent on one of the Management Services on the primary site. To ensure that the target is monitored after switchover/failover, relocate the target to a Management Agent on the standby site by running the following command on one of the Management Service standby sites.

   ```
   emctl config emrep -agent <agent name> -conn_desc <connect descriptor
   of new primary database>
   ```

9. Switch over to the Standby SLB.

   Make appropriate network changes to failover your primary SLB to standby SLB that is, all requests should now be served by the standby SLB without requiring any changes on the clients (browser and Management Agents).

10. Establish the old primary Management Services as the new standby Management Services to complete the switchover process.

    Start the Administration Server on old primary site

    ```
    emctl start oms -admin_only
    ```

This completes the switchover operation. Access and test the application to ensure that the site is fully operational and functionally equivalent to the primary site. Repeat the same procedure to switchover in the other direction.

### I.2.2 Failover

> **Warning:** The following failover instructions are only for use with the Standby OMSs using Standby WebLogic Domain disaster recovery approach as originally used in Enterprise Manager Release 12.1.0.2 and earlier installations as detailed in this appendix.
>
> For failover instructions for the Standby OMSs using Storage Replication disaster recovery approach used in Enterprise Manager Release 12.1.0.3 and later, see Chapter 18, "Enterprise Manager Disaster Recovery."

This section describes the steps to failover to a standby database, recover the Enterprise Manager application state by re-synchronizing the Management Repository database with all Management Agents, and enabling the original primary database as a standby using flashback database.

1. Shut down all OMS components at the primary site if running.

2. Verify Software Library Availability.

   Ensure all files from the primary site are available on the standby site.

3. Failover to Standby Database.

   Shutdown the database on the primary site. Use DGMGRL to connect to the standby database and execute the FAILOVER command:

   ```
   FAILOVER TO <standby database name>;
   ```

   Verify the post-failover states:

   ```
   SHOW CONFIGURATION;
   ```

   ```
   SHOW DATABASE <primary database name>;
   ```

   ```
   SHOW DATABASE <standby database name>;
   ```

   Note that after the failover completes, the original primary database cannot be used as a standby database of the new primary database unless it is re-enabled.

4. Start the AdminServer on the standby site if it is not already running.

   ```
   emctl start oms -admin_only
   ```

5. Make the standby Management Services point to the Standby Database which is now the new Primary by running the following on each standby Management Service.

   ```
   emctl config oms -store_repos_details -repos_conndesc <connect
   descriptor of new primary database> -repos_user sysman
   ```

6. Resync the New Primary Database with Management Agents.

   Skip this step if you are running in Data Guard Maximum Protection or Maximum Availability level as there is no data loss on failover. However, if there is data loss, synchronize the new primary database with all Management Agents.

   On any one Management Service on the standby site, run the following command:

   ```
   emctl resync repos -full -name "<name for recovery action>"
   ```

   This command submits a resync job that would be executed on each Management Agent when the Management Services on the standby site are brought up.

   Repository re-synchronization is a resource intensive operation. A well tuned Management Repository will help significantly to complete the operation as quickly as possible. Specifically if you are not routinely coalescing the IOT/indexes associated with Advanced Queueing tables as described in My Oracle Support note 271855.1, running the procedure before re-synchronization will significantly speed up the re-synchronization process.

7. Start up the Enterprise Manager Application Tier

   Start up all the Management Services on the standby site by running the following command on each Management Service.

   ```
   emctl start oms
   ```

8. Relocate Management Services and Management Repository target.

   The Management Services and Management Repository target is monitored by a Management Agent on one of the Management Services on the primary site. To ensure that target is monitored after switchover/failover, relocate the target to a Management Agent on the standby site by running the following command on one of the standby site Management Service.

   ```
   emctl config emrep -agent <agent name> -conn_desc <connect descriptor
   of new primary database>
   ```

9. Switchover to the Standby SLB.

   Make appropriate network changes to failover your primary SLB to the standby SLB, that is, all requests should now be served by the standby SLB without requiring any changes on the clients (browser and Management Agents).

10. Establish Original Primary Database as Standby Database Using Flashback.

    Once access to the failed site is restored, and if you had flashback database enabled, you can reinstate the original primary database as a physical standby of the new primary database using the following procedure.

    1. Shut down all the Management Services in the original primary site.

       ```
       emctl stop oms -all
       ```

    2. Restart the original primary database in mount state:

       ```
       shutdown immediate;
       ```

       ```
       startup mount;
       ```

3. Reinstate the Original Primary Database

   Use DGMGRL to connect to the old primary database and execute the REINSTATE command

   ```
   REINSTATE DATABASE <old primary database name>;
   ```

4. The newly reinstated standby database will begin serving as standby database to the new primary database.

5. Verify the post-reinstate states.

   ```
   SHOW CONFIGURATION;
   ```

   ```
   SHOW DATABASE <primary database name>;
   ```

   ```
   SHOW DATABASE <standby database name>;
   ```

11. Establish Original Primary Management Service as the standby Management Service.

    Start the Administration Server on old primary site:

    ```
    emctl start oms -admin_only
    ```

12. Monitor and complete Repository Re-synchronization

    Navigate to the Management Services and Repository Overview page of Cloud Control Console. Under Related Links, click Repository Synchronization. This page shows the progress of the re-synchronization operation on a per Management Agent basis. Monitor the progress.

    Operations that fail should be resubmitted manually from this page after fixing the error mentioned. Typically, communication related errors are caused by Management Agents being down and can be fixed by resubmitting the operation from this page after restarting the Management Agent.

    For Management Agents that cannot be started due to some reason, for example, old decommissioned Management Agents, the operation should be stopped manually from this page. Re-synchronization is deemed complete when all the jobs have a completed or stopped status.

This completes the failover operation. Access and test the application to ensure that the site is fully operational and functionally equivalent to the primary site.

Perform a switchover procedure if the site operations have to be moved back to the original primary site.

# J Troubleshooting

This appendix describes how to troubleshoot issues that you might encounter while working with Enterprise Manager Cloud Control.

- Troubleshooting Configuration Assistant Failures
- Troubleshooting ADP and JVMD Failures
- Troubleshooting Package-Related Issues
- Troubleshooting Deinstallation Failures
- Troubleshooting Management Agent Installation Failures

## J.1 Troubleshooting Configuration Assistant Failures

This section describes the log files you must review and the actions you must take when the following configuration assistants fail:

- Plugins Prerequisite Check Configuration Assistant
- Repository Configuration Assistant
- Repository Out Of Box Configuration Assistant
- MDS Schema Configuration Assistant
- OMS Configuration Assistant
- Plugins Deployment and Configuration Configuration Assistant
- Start Oracle Management Service Configuration Assistant
- Plugins Inventory Migration Configuration Assistant
- Oracle Configuration Manager Repeater Configuration Assistant
- OCM Configuration for OMS Configuration Assistant
- Agent Configuration Assistant
- Agent Upgrade Configuration Assistant
- Repository Upgrade Configuration Assistant
- Stopping APM Engines Configuration Assistant
- Stop Admin Server Configuration Assistant

### J.1.1 Plugins Prerequisite Check Configuration Assistant

Review the log files and perform the suggested workaround steps.

#### J.1.1.1 Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/cfgtoollogs/pluginca/configplugin_prereq_check_<timestamp>.log`

#### J.1.1.2 Workaround Steps

1. Run the plug-ins prerequisite check configuration assistant:

```
$<OMS_HOME>/oms/bin/pluginca -action prereqCheck -oracleHome <oms_home_
path> -middlewareHome <middleware_home_path> -plugins <plugin_
id>=<plugin_version>
```

> **Note:** For multiple plug-ins, separate the plug-in details with a comma. For example, `-plugins <plugin_id>=<plugin_version>, <plugin_id>=<plugin_version>`

2. Complete the installation:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

### J.1.2 Repository Configuration Assistant

Review the log files and perform the suggested workaround steps.

#### J.1.2.1 Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/`

> **Note:** `<ACTION>` refers to any of the schema actions, for example, CREATE, TRANSX, MY_ORACLE_SUPPORT, and so on.

#### J.1.2.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Clean up the Management Repository by running the following command:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_
host> <repository_database_port> <repository_database_sid> -action drop
-dbUser <repository_database_user> -dbPassword <repository_database_
password> -dbRole <repository_database_user_role> -mwHome <middleware_
home> -mwOraHome <oms_oracle_home> -oracleHome <oms_oracle_home>
```

> **Note:**
>
> - For Microsoft Windows, invoke `RepManager.bat`.
> - For information on the support for `-action drop` and `-action dropall`, see Table 2–3.

3. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

> **Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.3 Repository Out Of Box Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.3.1 Log Files

Review the following log file:

```
$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/
```

### J.1.3.2 Workaround Steps

1. Resolve the cause of the issue.

> **Caution:** Do NOT clean up or drop the Management Repository.

2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.4 MDS Schema Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.4.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

For more information, review the following log files:

- `<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/mds.log`
- `$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/rcu.log`

### J.1.4.2 Workaround Steps

Follow these steps:

1. Drop the MDS schema by running the following command from the OMS home:

   ```
   $<OMS_HOME>/sysman/admin/emdrep/bin/mdsschemamanager.pl
   -action=-dropRepository -connectString=<database_connect_string>
   -dbUser= <database_user> -dbPassword=<database_password>
   -oracleHome=<OMS_oracle_home> -mwHome=<middleware_home>
   ```

   Where `<database_connect_string>` must be in the following format:`<database_host>:<database_port>:<database_sid>`

2. Rerun the Configuration Assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.5 OMS Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.5.1 Log Files

Review the following log files:

- If the installer fails BEFORE the OMS configuration assistant starts running, then review the following log file:

  ```
  $<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
  ```

- If the installer fails AFTER the OMS configuration assistant starts running, then review the following log file:

  ```
  $<OMS_HOME>/cfgtoollogs/omsca/omsca_<timestamp>.log
  ```

### J.1.5.2 Workaround Steps

Follow these steps:

1. Check whether any Java processes are running from the Middleware home. To do so, run the following command from the host where the OMS is running:

   ```
   ps -ef | grep java | grep <Oracle_Middleware_Home>
   ```

2. Kill all the running processes, except for installer-related Java processes, by running the following command. The installer-related Java processes run from the temp directory, so you can ignore the processes from that directory.

   ```
   kill -9 <process_id>
   ```

3. Remove the Oracle Management Service Instance Base by running the following command:

   ```
   rm -rf <OMS_Instance_Home>
   ```

4. Rerun the Configuration Assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.6 Plugins Deployment and Configuration Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.6.1 Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/cfgtoollogs/pluginca/configplugin_deploy_<timestamp>.log`

### J.1.6.2 Workaround Steps

Complete the plug-ins deployment and configuration, and the installation:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path> MODE=perform
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

## J.1.7 Start Oracle Management Service Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.7.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.7.2 Workaround Steps

Run the following command:

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

**Note:** For additional troubleshooting tips on OMS, see the My Oracle Support note 1495519.1.

## J.1.8 Plugins Inventory Migration Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.8.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.8.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.9 Oracle Configuration Manager Repeater Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.9.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.9.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

   **Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.10 OCM Configuration for OMS Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.10.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.10.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.11 Agent Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.11.1 Log Files

Review the following log files:

- `$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- If secure fails, then review the following log file:

  `$<AGENT_INSTANCE_HOME>/sysman/log/secure.log`
- In the log file, search for the following statement:

  `SEVERE:Plugin configuration has failed.`

  If you find this statement, then review the following log file:

  `$<AGENT_INSTANCE_HOME>/install/logs/agentplugindeploy_<timestamp>.log`

### J.1.11.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
```

If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

**Note:** For Microsoft Windows, run `runConfig.bat`.

If you are installing in silent mode, then run the following command from the Management Agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<agent_base
dir_path> OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_upload_https_
port> AGENT_REGISTRATION_PASSWORD=<agent_reg_password> -configOnly
```

**Note:** Enter the HTTPS port (secure port) for the `EM_UPLOAD_PORT` argument.

## J.1.12 Agent Upgrade Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.12.1 Log Files

If the agent upgrade configuration assistant fails, then review the following log file:

```
$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.12.2 Workaround Steps

Resolve the cause of the issue, and rerun the configuration assistant from the Jobs page of the Enterprise Manager Cloud Control console.

**Note:** The Jobs page referred to here is the page within the earlier release of the Enterprise Manager Cloud Control console.

## J.1.13 Repository Upgrade Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.13.1 Log Files

Review the following log files:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

```
$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/
```

**Note:** (`<ACTION>` refers to any of the schema actions, for example, PREUPGRADE, UPGRADE, TRANSX, and so on.)

### J.1.13.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.

2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

   **Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.14 Stopping APM Engines Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.14.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.14.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

   **Note:** For Microsoft Windows, run `runConfig.bat`.

## J.1.15 Stop Admin Server Configuration Assistant

Review the log files and perform the suggested workaround steps.

### J.1.15.1 Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

### J.1.15.2 Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   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 (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script (`runConfig.bat` on Microsoft Windows) from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the `runConfig.sh` script fails, then clean up your environment and redo the installation.

   **Note:** For Microsoft Windows, run `runConfig.bat`.

# J.2 Troubleshooting ADP and JVMD Failures

This section describes how to troubleshoot the errors encountered while deploying ADP/JVMD Engines, and ADP/JVMD Agents:

- ADP Engine Name Conflict
- ADP Agent Deployment Failure
- ADP Agent Deployment Failure on WebLogic Server 12.1.2
- JVMD Agent Deployment Failure
- SSL Handshake Failure During Agent Deployment
- Copying ADP Agent Zip or Javadiagnosticagent.ear Failure
- JVM Pool Creation Failure

## J.2.1 ADP Engine Name Conflict

Confirm the error and perform the workaround steps.

#### J.2.1.1 Error

When you deploy ADP Engine to an existing managed server whose instance (for example: `EMGC_ADPENGINE2`) has not been completely removed, then the new deployment of ADP Engine with the same name fails on the unzip step with the following error:

```
@ Are you sure you haven't deployed adp engine to a managed server with name
@ <ADP_managed_server> already?
```

#### J.2.1.2 Workaround Steps

To remove the existing managed server completely, perform the following steps:

1. Follow the steps listed in Chapter 23 to remove the ADP Engine application and the managed server to which the ADP application is deployed.
2. Connect to the host machine where the managed server was present, and navigate to the following location to manually delete the managed server (`EMGC_ENGINE2`):

   ```
   $DOMAIN_HOME/<ADP_managed_server>

   Where, $DOMAIN_HOME is the location of the Cloud Control domain
   ```

### J.2.2 ADP Agent Deployment Failure

Confirm the error and perform the workaround steps.

#### J.2.2.1 Error

While deploying the ADP Agent, the deployment job may fail on the Deploy ADP Agent On Target step, with the following error:

```
Failed to connect to
https://<host>:<port>/HttpDeployer/HttpDeployerServlet
```

Also, if you check the output of the Deploy HttpDeployer OnTarget (the previous step), then you will see a message as follows:

```
Operation is pending and will be activated or cancelled when the ongoing
edit session is activated or cancelled.
```

#### J.2.2.2 Workaround Steps

To correct this error, perform the following steps:

1. Log into WebLogic Administration Console of the domain where the ADP Agent was to be deployed.
2. On the Administration home page, click **Save Changes** or **Discard Changes**, and start deploying the ADP Agent afresh.

### J.2.3 ADP Agent Deployment Failure on WebLogic Server 12.1.2

Confirm the error and perform the workaround steps.

#### J.2.3.1 Error

ADP Agent deployment fails on a 12.1.2 WebLogic Server target.

#### J.2.3.2 Workaround Steps

Build `wlfullclient.jar` on the WebLogic Server target where you want to deploy the ADP Agent, and retry the ADP Agent deployment.

For information on how to build `wlfullclient.jar,` see *Oracle Fusion Middleware Developing Stand-alone Clients for Oracle WebLogic Server.*

### J.2.4 JVMD Agent Deployment Failure

Confirm the error and perform the workaround steps.

#### J.2.4.1 Error

While deploying a JVMD Agent on a target, the *Deploy HTTPDeployer On Target* job step fails due to an SSL handshake failure. This error may occur if the appropriate patch is not applied on the WebLogic Server software.

#### J.2.4.2 Workaround Steps

Apply the appropriate patch on your Oracle WebLogic Server software, then retry the deployment. The appropriate patches for different versions of Oracle WebLogic Server are mentioned in Table J–1. Note that if you are deploying a JVMD Agent on Oracle WebLogic Server 9.2.4 or higher, or Oracle WebLogic Server 10.3.2 or higher, you do not need to apply a patch, as the fix is already present in these versions.

***Table J–1 Oracle WebLogic Server Patches to be Applied***

| Oracle WebLogic Server Version | Patch to be Applied |
|---|---|
| 9.1.0 | Patch 8422724 |
| 9.2.0 | Patch 9384535 |
| 9.2.1 | Patch 9032735 |
| 9.2.2 | Patch 9309512 |
| 9.2.3 | Patch 8849418 |
| 10.0.0 | Patch 8422724 |
| 10.0.1 | Patch 8895699 |
| 10.0.2 | Patch 8896127 |
| 10.3.0 | Patch 8715553 |
| 10.3.1 | Patch 9003716 |

### J.2.5 SSL Handshake Failure During Agent Deployment

Confirm the error and perform the workaround steps.

#### J.2.5.1 Error

If the WebLogic Domain is SSL enabled using a demo certificate, then the agent deployment may fail due to an SSL Handshake Failure. The following error normally occurs because the demo certificate is not present in `AgentTrust.jks`:

```
Certificate chain received from myhost.acme.com - 123.34.11.11 was not
trusted causing SSL handshake failure. Check the certificate chain to
determine if it should be trusted or not. If it should be trusted, then
update the client trusted CA configuration to trust the CA certificate
```

```
that signed the peer certificate chain. If you are connecting to a WLS
server that is using demo certificates (the default WLS server behavior),
and you want this client to trust demo certificates, then specify
-Dweblogic.security.TrustKeyStore=DemoTrust on the command line for this
client.
```

**Note:** If the WebLogic Domain is using a production certificate, then this issue will not occur as `AgentTrust.jks` has trusted certificates from all well known CA's.

### J.2.5.2 Workaround Steps

To correct the error, import WebLogic demo certificate to Management Agent keystore as follows:

1. Export WebLogic Demo certificate from `cacerts` file. This file is present under the WebLogic home of the Middleware installation at the following location:

   ```
   keytool -export -keystore $WEBLOGIC_HOME/server/lib/cacerts -alias
   certgencab -file mycert.cer
   ```

   Press **Enter** when prompted for a password.

2. Import WebLogic Demo certificate to TrustStore of Oracle Management Agent as follows:

   ```
   keytool -import -keystore $ORACLE_
   HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.jks -alias
   wlscertgencab -file mycert.cer
   ```

   Enter the password **welcome** when prompted, and press **Enter.**

To check if the certificate has been imported correctly, run the following command:

```
keytool -list -keystore $ORACLE_
HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.jks
```

Where, `$ORACLE_HOME` is Oracle Management Agent home.

Press **Enter** when prompted for password, a certificate with the name `wlscertgencab` is generated with the current date.

## J.2.6 Copying ADP Agent Zip or Javadiagnosticagent.ear Failure

Confirm the error and perform the workaround steps.

### J.2.6.1 Error

If the users who installed the OMS, and the Management Agent are not in the same group, then the job fail on Copying ADP Agent Zip step for an ADP agent, and Copy Javadiagnosticagent Ear step for a JVMD agent, with the following error:

```
oracle.sysman.emSDK.emd.comm.RemoteOperationException: Error while streaming
JobReader:java.io.IOException: Broken pipe
```

### J.2.6.2 Workaround Steps

To correct the error, either install the Enterprise Manager Agent using OMS host user credentials.

OR

Enable `sudo` or `Powerbroker` settings for the agent host, so that the job runs as if run by an OMS host user.

To set the sudo, or Powerbroker settings, do the following:

1. In Cloud Control, from the **Setup** menu, select **Security,** and then click **Privilege Deligation.**
2. On the Manage Privilege Delegation Settings page, do the following:
   a. Select the **Sudo** or **PowerBroker** from the type menu.
   b. Enter the host name, or alternatively select the name from the list of host targets. Ensure that the host selected corresponds to the Management Agent; this agent must be the one monitoring the WebLogic Domain where the ADP/JVMD agents have to be deployed.
   c. Click **Go**.

## J.2.7 JVM Pool Creation Failure

Confirm the error and perform the troubleshooting tips steps.

### J.2.7.1 Error

No JVM target or pool is created even though the JVMD Agent deployment was successful.

### J.2.7.2 Troubleshooting Tips

The causes of this error may be the following:

- The JVMD Engine, to which the JVMD Agent connects is down.

  Restart the JVMD Engine and refresh the Application Performance Management pages to check if the target or pool has been created.

- The user that submitted the job may not have write permissions in the temporary directory of the WebLogic installation.

  Grant the user write permissions for the temporary directory and retry the deployment, or retry the deployment using a different user account.

- The JVMD Engine host and port are not reachable from the host where the JVMD Agent is deployed.

  Contact the network administrator to resolve the network issue. If a firewall is configured, ensure that the JVMD Engine port is open over the configured firewall.

- The status of the JVMD Agent deployment is falsely marked as `Successful.`

  Carefully examine each of the job steps of the JVMD Agent deployment to ensure that there are no unidentified errors or exceptions that led to a false status.

# J.3 Troubleshooting Package-Related Issues

While installing Enterprise Manager Cloud Control, you might see the following error message:

```
Lin.X64 SUSE 10 : Backup fails with the given below error
install_driver(Oracle) failed: Attempt to reload DBD/Oracle.pm aborted.
Compilation failed in require at (eval 15) line 3.
```

If you see this error, then install the following packages, and try again.

- `libaio-32bit-0.3.104-14.2`

- `libaio-devel-32bit-0.3.104-14.2`

## J.4 Troubleshooting Deinstallation Failures

While deinstalling the *Shared Agent* as described in Section 22.1.2.4, you might see the following error:

```
SEVERE:The home <AGENT_HOME> cannot be deinstalled. Please deinstall all
referenced home(s) <REFERENCE_HOME>
```

For example,

```
SEVERE:The home /tmp/agt_install/core/12.1.0.1.0 cannot be deinstalled. Please
deinstall all referenced home(s) /tmp/agt_install/plugins
```

If you see the error, then deinstall the *Shared Agent* following these steps:

1. Identify the dependent plug-ins and the sbin home to be detached from the Central Inventory:

   a. On the host where the *Shared Agent* is installed, open the following file from the Central Inventory:

      ```
      <absolute_path>/oraInventory/ContentsXML/inventory.xml
      ```

   b. Make a note of the dependent plug-ins listed within the `<REFHOMELIST>` and `</REFHOMELIST>` tags.

      For example,

      ```
      <HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
      TYPE="O" IDX="1">
      <REFHOMELIST>
      <REFHOME
      LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.discovery.pl
      ugin_12.1.0.0.0"/>
      <REFHOME
      LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.db.discovery.pl
      ugin_12.1.0.0.0"/>
      <REFHOME
      LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.emas.discovery.
      plugin_12.1.0.0.0"/>
      <REFHOME
      LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.agent.plugin
      _12.1.0.0.0"/>
      </REFHOMELIST>
      </HOME>
      ```

   c. Make a note of the sbin directory listed within the `<REFHOMELIST>` and `</REFHOMELIST>` tags.

      For example,

      ```
      <HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
      TYPE="O" IDX="1">
      <REFHOMELIST>
      <REFHOME LOC="home/john/software/oracle/agent/sbin"/>
      </REFHOMELIST>
      ```

   d. Detach the dependent plug-ins you identified in Step 1 (b) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc  ORACLE_
HOME=<plug-in_home>  -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/oui/bin/runInstall
er -detachHome -silent -waitForCompletion -invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.3.0/oraInst.loc
ORACLE_
HOME=/home/john/software/oracle/agent/plugins/oracle.sysman.emas.di
scovery.plugin_12.1.0.3.0  -nogenerateGUID
```

**Note:** This step detaches only one plug-in at a time. Therefore, if you have multiple plug-ins, repeat this step to detach every other dependent plug-in.

e. Detach the sbin home you identified in Step 1 (c) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc  ORACLE_
HOME=<sbin_home>  -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/oui/bin/runInstall
er -detachHome -silent -waitForCompletion -invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.3.0/oraInst.loc
ORACLE_HOME=/home/john/software/oracle/agent/sbin  -nogenerateGUID
```

2. Deinstall the *Shared Agent*. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/perl/bin/perl  <AGENT_
HOME>/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_
HOME=<absolute_path_to_agent_instance_home> ORACLE_HOME=<absolute_path_
to_agent_home>
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.3.0/perl/bin/perl
/home/john/software/oracle/agent/core/12.1.0.3.0/sysman/install/NFSAgen
tDeInstall.pl AGENT_INSTANCE_
HOME=/home/john/software/oracle/agent/agent_inst ORACLE_
HOME=/home/john/software/oracle/agent/core/12.1.0.3.0
```

## J.5 Troubleshooting Management Agent Installation Failures

While deploying a Management Agent, you may encounter the following failures:

- If the Management Agent installation fails, and the Management Agent deployment logs available at `<ORACLE_HOME>/cfgtoollogs/agentDeploy/agentDeploy<TIMESTAMP>.log` mention that the port check failed, then run the `agentDeploy.sh` script again, using the `-ignorePrereqs` option.

Also, if the port check failed for a host that has an IPv6 address listed as part of the host DNS setup, then ensure that the IPv6 address is enabled on the host.

- If the Management Agent installation fails on a Microsoft Windows host, with an error message mentioning that `setup.exe` cannot be executed, then log in using an administrator account and retry the Management Agent installation on the host.

# Index