Oracle® Enterprise Manager

Advanced Installation and Configuration Guide

24ai Release 1
F97192-01
December 2024

ORACLE

Oracle Enterprise Manager Advanced Installation and Configuration Guide, 24ai Release 1

F97192-01

Primary Author: Oracle Corporation

Contributors: Enterprise Manager Development Teams, Quality Assurance Teams, Customer Support Teams, and Product Management Teams.

Contents

7 Cloning Oracle Management Agents

13 Managing the Lifecycle of Agent Gold Images

14 Configuring Enterprise Manager for Firewalls

15 Sizing Your Enterprise Manager Deployment

16 Configuring Proxies for OMS and Management Agent Communication

17 Installing JVMD Agents with Advanced Install Options

18 Configuring Enterprise Manager Federation

19 Using Oracle Analytics Server with Enterprise Manager

20 Configuring Oracle Enterprise Manager App for Grafana

25 Enterprise Manager Disaster Recovery

26 Backing Up and Recovering Enterprise Manager

Part IX Appendixes

A Overview of the Installation and Configuration Log Files

B Redirecting Oracle Management Agent to Another Oracle Management Service

C Using the RepManager Utility

D Collecting OCM Data Using Oracle Harvester

E Enabling the Enterprise Manager Accessibility Features

F Configuring Targets for Failover in Active/Passive Environments

G Updating Demonstration Keystores to Reflect Alias Hostnames

Preface

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

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

This preface contains the following topics:

Audience

Oracle Enterprise Manager Advanced Installation and Configuration Guide is intended for systems administrators who want to install Enterprise Manager components in complex environments.

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 Resources

For more information about Enterprise Manager documentation, see the following books:

- Oracle Enterprise Manager Basic Installation Guide
- Oracle Enterprise Manager Upgrade Guide

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

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

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
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.

Part I
Getting Started

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

- Procuring the Software
- Understanding the Basics

1

Procuring the Software

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

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

Releases Available for Enterprise Manager

Table 1-1 describes the releases Enterprise Manager has had so far.

Table 1-1 Enterprise Manager Releases

Release Numbers	Release Type	Release Date	Implementation Method	Description
Oracle Enterprise Manager 24ai Release 1	Major Release	December 2024	• New installation of 24ai Release 1 • Upgrade from 13*c* Release 5	The first 24ai release.
Oracle Enterprise Manager Cloud Control 13c Release 5	Major Release	March 2021	• New installation of 13*c* Release 5 • Upgrade from 13*c* Release 4, 13*c* Release 3	The fifth 13c release.
Oracle Enterprise Manager Cloud Control 13c Release 4	Major Release	January 2020	• New installation of 13*c* Release 4 • Upgrade from 13*c* Release 3, 13*c* Release 2	The forth 13c release.
Oracle Enterprise Manager Cloud Control 13c Release 3	Major Release	May 2018	• New installation of 13*c* Release 3 • Upgrade from 13*c* Release 2, 12*c* Release 5 (12.1.0.5, 12)*c* Release 4 (12.1.0.4)	The third 13c release.
Oracle Enterprise Manager Cloud Control 13c Release 2	Major Release	June 2016	• New installation of 13*c* Release 2 • Upgrade from 13*c* Release 1, 12*c* Release 5 (12.1.0.5, 12)*c* Release 4 (12.1.0.4)	The second 13c release.

Table 1-1 (Cont.) Enterprise Manager Releases

Release Numbers	Release Type	Release Date	Implementation Method	Description
Oracle Enterprise Manager Cloud Control 13c Release 1	Base Release	December 2015	• New installation of 13*c* Release 1 • Upgrade from 12*c* Release 5 (12.1.0.5), 12*c* Release 4 (12.1.0.4), 12*c* Release 3 (12.1.0.3)	First ever 13c release.

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

Procuring the Enterprise Manager Software

You can procure the Enterprise Manager software from either the product DVD or Oracle Software Downloads site. This section describes these sources and covers the following:

- How Do You Access the Enterprise Manager Software from a DVD?
- How Do You Procure the Enterprise Manager Software from Oracle?

How Do You Access the Enterprise Manager Software from a DVD?

You can obtain the Enterprise Manager 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 multiple DVDs depending on the operating system.

This section covers the following:

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

Accessing the Software from a DVD

If the software is available on a single DVD, then insert the DVD into the DVD drive, and run the `.bin` file.

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. Then, run the `.bin` file. No need to extract the archived (ZIP) files. Retain them as `.bin` and `.zip` files.

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`

How Do You Procure the Enterprise Manager Software from Oracle?

You can procure the Enterprise Manager software from *Oracle Software Downloads* site. The software available 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 Software

To download the Enterprise Manager software, follow these steps:

1. As the install user who will be installing the product, create a directory where you can download and store the Enterprise Manager software files.
2. Access `Enterprise Manager Download` from *Oracle Software Downloads* site.
3. Download the following files:
   - For UNIX platforms:
     - `em24100_<platform>.bin`
     - `em24100_<platform>-2.zip`
     - `em24100_<platform>-3.zip`
     - `em24100_<platform>-4.zip`
     - `em24100_<platform>-5.zip`
   - For Microsoft Windows platforms:
     - `setup_em24100_win64.exe`
     - `setup_em24100_win64-2.zip`
     - `setup_em24100_win64-3.zip`
     - `setup_em24100_win64-4.zip`
     - `setup_em24100_win64-5.zip`

   > **WARNING:**
   >
   > Do not extract the contents of the downloaded archived (ZIP) files like you did for the previous releases of Enterprise Manager. Retain them as `.bin` and `.zip` files.

4. As the install user who will be installing the product, set the *execute* permission for the `.bin` or the `.exe` file.

   For example, on UNIX platforms, set the *execute* permission for the `em24100_linux64.bin` file.

   ```
   chmod +x em24100_linux64.bin
   ```

5. Verify that the *execute* permission has been correctly set for the `.bin` or the `.exe` file.

   For example, on UNIX platforms, run the following command:

   ```
   ls -ltr
   ```

   You should see a similar output that lists the file permissions:

   ```
   -r-xr-xr-x 1 user1 group1 2032373759 Jul 14 03:57 em24100_linux64.bin
   -r--r--r-- 1 user1 group1 2022925751 Jul 14 03:57 em24100_linux64-2.zip
   -r--r--r-- 1 user1 group1 2046336073 Jul 14 03:57 em24100_linux64-3.zip
   -r--r--r-- 1 user1 group1 653990632 Jul 14 03:57 em24100_linux64-4.zip
   -r--r--r-- 1 user1 group1 653990632 Jul 14 03:57 em24100_linux64-5.zip
   ```

Verifying the File Size of Enterprise Manager Zip Files

After downloading the ZIP files, 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 *Oracle Software Downloads* site.

The following is the format of the ZIP files released for 24ai Release 1 for UNIX platforms. Here, *<platform>* refers to the operating system and *N* refers to the ZIP file number. For example, `em24100_linux64-2.zip, em24100_linux64-3.zip, em24100_linux64-4.zip` and `em24100_linux64-5.zip`.

em24100_<platform>-N.zip (<value> bytes) (cksum - <value>)

Similarly, the following is the format of the ZIP files released for 24ai Release 1 for Microsoft Windows platforms. Here, *N* refers to the ZIP file number. For example, `setup_em24100_win64-2.zip, setup_em24100_win64-3.zip, setup_em24100_win64-4.zip` and `setup_em24100_win64-5.zip`.

setup_em24100_win64-N.zip (<value> bytes) (cksum - <value>)

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 em24100_<platform>-N.zip
```

For example,

```
$ cksum em24100_linux64-2.zip
```

Procuring the Oracle Management Agent Software

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager, and therefore, its software is part of the Enterprise Manager software. When you install Enterprise Manager, 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 Console (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 24ai Release 1 and it is running on Linux platform, then the Oracle Management Agent software available there is also for that release and for that 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 Enterprise Manager Console.

For information on Self Update, see *Oracle Enterprise Manager Administrator's Guide*.

2

Understanding the Basics

This chapter introduces you to some key concepts of Enterprise Manager, 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 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
- Understanding the Limitations of Enterprise Manager
- Understanding the Startup Scripts
- Understanding Other Miscellaneous Concepts

Understanding the Basics of Enterprise Manager 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?
- What Is an Enterprise Manager Installation Wizard?
- What Installation Types Are Offered by the Enterprise Manager Installation Wizard?
- What Is Oracle Configuration Manager?
- What Are the Enterprise Manager Software Updates?
- What Is a Deployment Size for Enterprise Manager in an Advanced Configuration?
- What Is an Agent Gold Image?
- What Is an Agent Gold Image Console?
- 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

What Are the Different Installation Modes Offered by Enterprise Manager?

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

Installation Modes	Description
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 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 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.

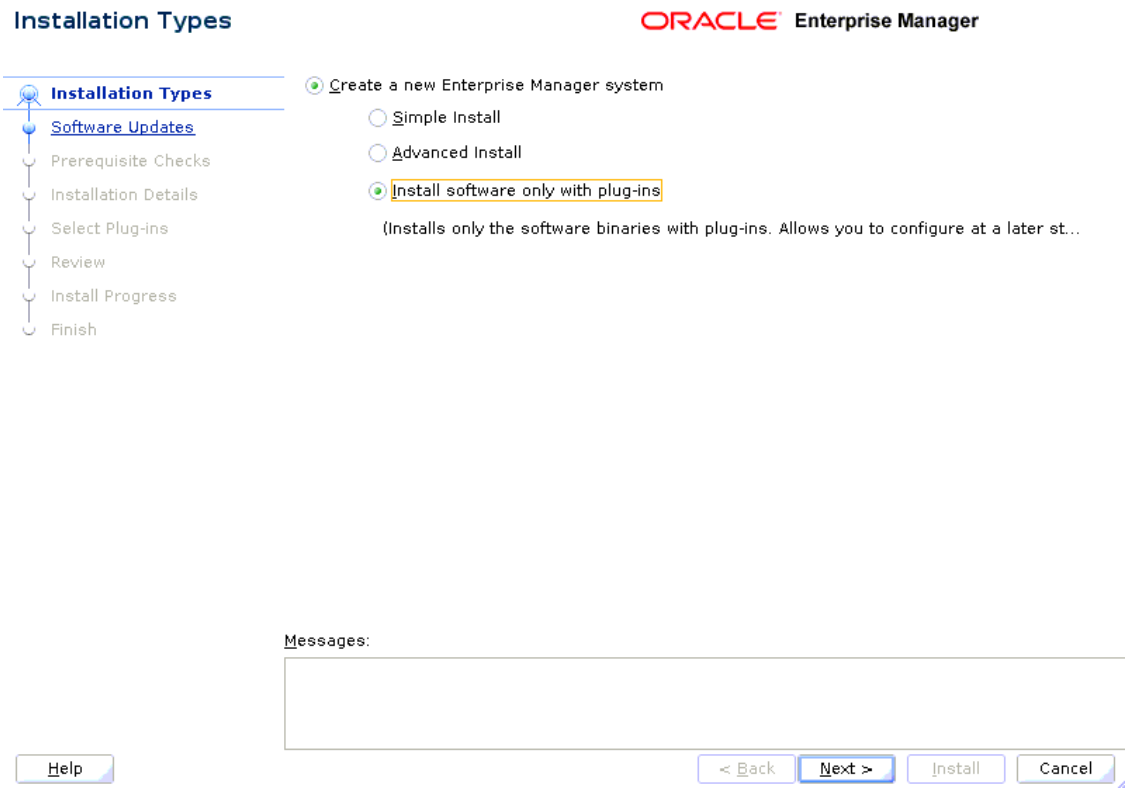
What Is an Enterprise Manager Installation Wizard?

Enterprise Manager Installation Wizard is a Java-based wizard that helps you install or upgrade to Enterprise Manager in graphical mode. If you are installing Enterprise Manager 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 `em24100_<platform>.bin`.
> To invoke on Microsoft Windows platforms, run `setup_em24100_win64.exe`.

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

Figure 2-1 Enterprise Manager Installation Wizard



What Installation Types Are Offered by the Enterprise Manager Installation Wizard?

The Enterprise Manager Installation Wizard offers the following installation types:

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

Create a New Enterprise Manager System

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

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

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

Upgrade an Existing Enterprise Manager System

This installation type enables you to upgrade the following to Enterprise Manager 24ai Release 1:

- Enterprise Manager Cloud Control 13*c* Release 5

Both are the only upgrade paths supported.

For upgrade, you can select *Upgrade End-to-End* or *Upgrade software only with plug-ins and Configure Later*. The upgrade process enables you to upgrade on the same host where your earlier release of Enterprise Manager is running. It also upgrades the Management Repository in the existing database. Since the upgrade happens on the same host, there is a reasonable downtime involved.

Install Only the Software With Plug-ins

This installation type enables you to install the software binaries of Enterprise Manager with plug-ins 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 software binaries.

For information about what is installed during the installation phase and what is configured during the configuration phase, refer to Introduction to Installing Enterprise Manager Using the Software Only with Plug-ins Method.

What Is Oracle Configuration Manager?

While installing Enterprise Manager, you can choose to enable Oracle Configuration Manager.

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.

In addition, Oracle Configuration Manager enables the Harvester feature, which automatically collects configuration information about the targets monitored by Enterprise Manager and uploads it to Oracle repository at regular Intervals. This eliminates the need to install and configure Oracle Configuration Manager collector in each and every Oracle home of the targets that are managed by Enterprise Manager. For more information about Oracle Configuration Manager and the Harvester feature, see the *Oracle Configuration Manager Installation and Configuration Guide*..

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 an Internet connection, 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.

If the host from where you are running the installation wizard does not have an Internet connection, then enter only the e-mail address and leave the other fields blank. After you complete the installation, at a later point when you are ready to configure Oracle Configuration Manager, run the following command from the Oracle home of the OMS host:

On UNIX Platforms:

```
$<OMS_HOME>/oracle_common/ccr/bin/configCCR
```

On Microsoft Windows Platforms:

```
$<OMS_HOME>\oracle_common\ccr\bin\configCCR.exe
```

What Are the Enterprise Manager Software Updates?

This section describes the following:

What Is a Software Update?

Software Update is a feature built in to the Enterprise Manager 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.

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.

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.

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. This enables OUI to always run the latest 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.

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.

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 Installation Wizard with the `DOWNLOAD_UPDATES=true` 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 24ai Release 1 software location, and NOT from the existing OMS home or database home.**

     ```
     <Software_Extracted_Location>./em24100_<platform>.bin
     DOWNLOAD_UPDATES=true
     ```

     > **Note:**
     >
     > – On Microsoft Windows, run `setup_em24100_win64.exe DOWNLOAD_UPDATES=true`
     >
     > – 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.

  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 `/OraInstall<timestamp>/updates`. Click **Next.**

     After the download is complete, close the Software Updates screen.

  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 `SHOW_PROXY=true` argument. For example, if you are invoking in graphical mode, then invoke in the following way:
>
> ```
> <Software_Location>/em24100_<platform>.bin SHOW_PROXY=true
> ```

- **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 Installation Wizard.

  On a host that has Internet connectivity, invoke the Enterprise Manager 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.

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.

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
```

What Is a Deployment Size for Enterprise Manager in an Advanced Configuration?

When you install Enterprise Manager 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 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 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 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 Sizing Your Enterprise Manager Deployment .

After installing Enterprise Manager 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 Sizing Your Enterprise Manager Deployment .

What Is an Agent Gold Image?

In the past, Enterprise Manager has offered several approaches for installing Management Agents, including the Add Host Targets Wizard, EM CLI, and response files to silently perform the installation. Starting with 13*c* Release 1, Enterprise Manager offers *Agent Gold Images* that can be used for mass-deployment and upgrade of Management Agents in your environment.

An Agent Gold Image represents the ideal state of a Management Agent in a data center managed by Enterprise Manager, having a customized configuration of the desired versions of the Management Agent software, the desired versions of the monitoring plug-ins, and the desired patches.

An Agent Gold Image version is created by an Enterprise Manager user, using a live reference Management Agent that is thoroughly tested and tuned. An Agent Gold Image version can be used to provision new Management Agents or update existing Management Agents on a large number of hosts.

For more information on Agent Gold Images, see Managing the Lifecycle of Agent Gold Images .

What Is an Agent Gold Image Console?

The Agent Gold Image Console is a GUI-rich application accessible from within the Enterprise Manager Console, and used for managing the lifecycle of Agent Gold Images. For information about Agent Gold Image, see What Is an Agent Gold Image?.

Using the Agent Gold Image Console, you can create or delete a gold image; you can create, delete, or stage a gold image version; you can set a gold image version as current or restricted version; you can subscribe or unsubscribe Management Agents to a gold image; and most importantly, you can provision new Management Agents or upgrade existing ones.

For more information on the Agent Gold Image Console, see Understanding the Agent Gold Image Console.

What Is an Add Host Target Wizard?

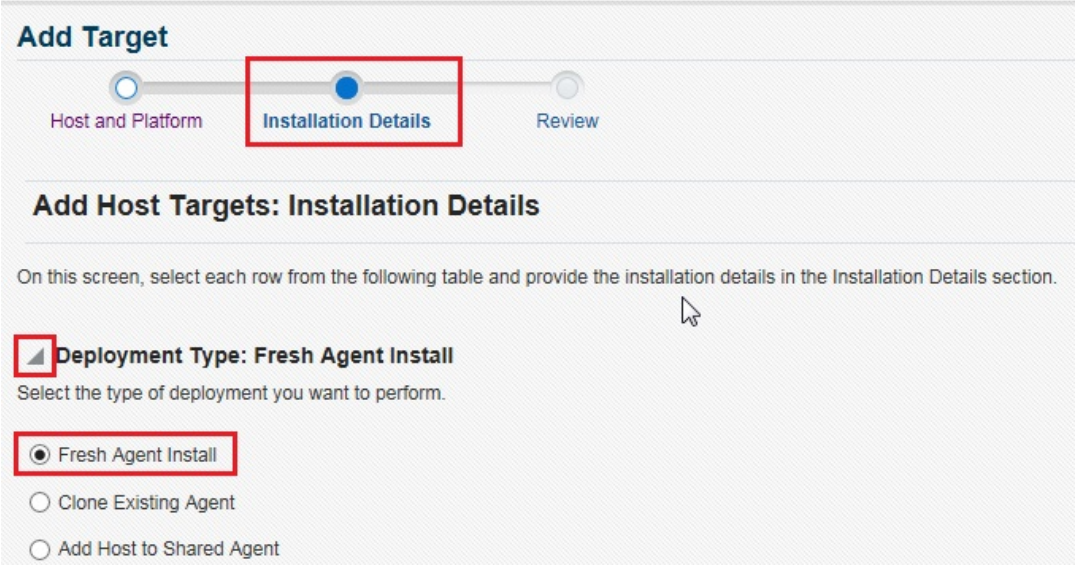
The Add Host Targets Wizard is a GUI-rich application accessible from within the Enterprise Manager Console, and used for installing Management Agents on unmanaged hosts and converting them to managed hosts in the Enterprise Manager system.

To access the Add Host Targets Wizard, do one of the following:

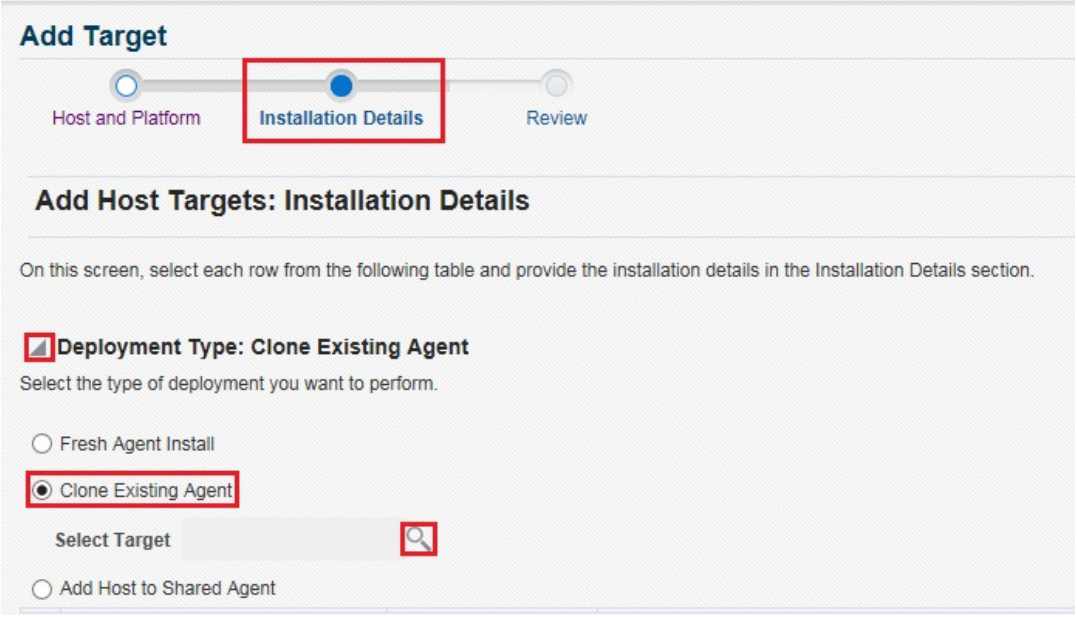
- From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**. On the Add Targets Manually page, click **Install Agent on Host.**
- From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**. On the Auto Discovery Results page, under the Servers, Storage and Network tab, select a host that you want to monitor from the displayed list, then click **Promote**.

The wizard enables you to do the following on multiple hosts across platforms with options to run preinstall and postinstall scripts:

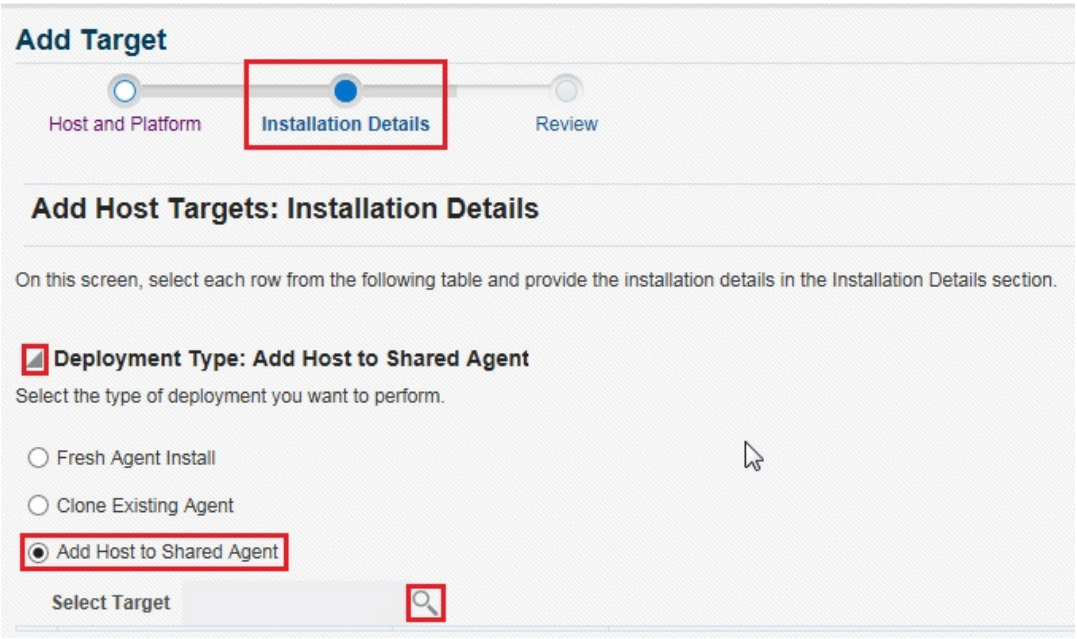
- Deploy a fresh Management Agent



- Clone an existing well-tested and patched Management Agent



- Install a Management Agent (called *Shared Agent*) using an existing, centrally shared Management Agent (called *Master Agent*)



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.

What Is an Add Remote Host Target Wizard?

The Add Remote Host Targets Wizard is a GUI-rich application accessible from within the Enterprise Manager Console, and used for installing remote Management Agents on unmanaged hosts and converting them to managed hosts in the Enterprise Manager system.

To access the Add Remote Host Targets Wizard, do the following:

- From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**. On the Add Targets Manually page, go to **Add Remote Host Targets** and click **Install Remote Agent on Host.**

The wizard gives you the flexibility to select hosts on which you want to install a remote Management Agent. This helps you when you want to install the Management Agent on several hosts.

For information about remote agents, see Installing Oracle Remote Management Agentsin *Enterprise Manager Basic Installation Guide*.

What Is a Plug-in?

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

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

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

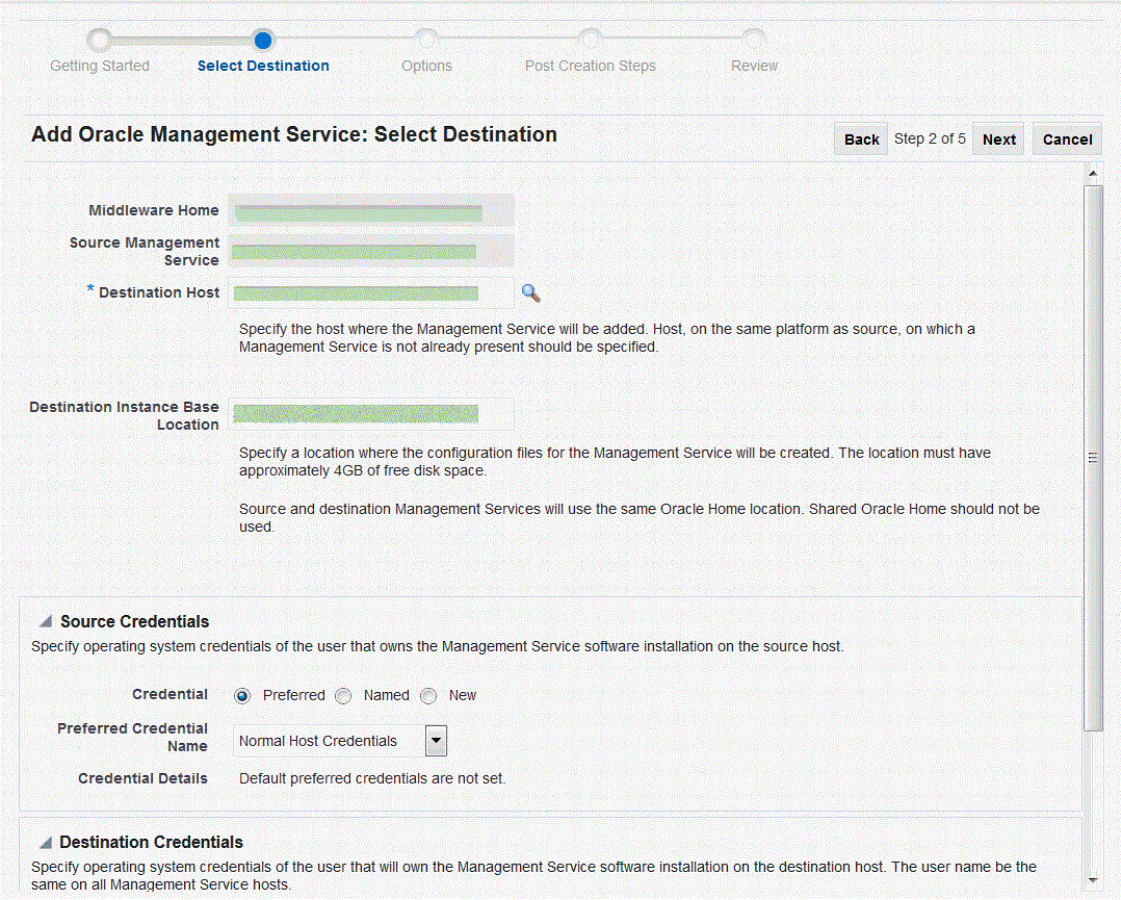
What Is an Add Management Service Deployment Procedure?

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

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

Figure 2-2 Add Management Service Deployment Procedure



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 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 Basic Installation Guide*.

What Ports Are Used for Installation?

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

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

What Default Ports Are Used for Enterprise Manager Installation?

The following are the default ports used for installation:

- **Enterprise Manager**

  Table 2-2 Default Port for Enterprise Manager

	Upload Port	Console Port
HTTP Port	The first available free port from the range 4889 to 4898 is selected.	The first available free port from the range 7788 to 7798 is selected.
HTTPS Port	1159 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 to 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 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.

- **Managed Server**

  The default HTTP port is the first available free port from the range 7201 to 7300.

  The default HTTPS port is the first available free port from the range 7301 to 7400.

- **Node Manager**

  The default HTTPS port is the first available free port from the range 7401 to 7500.

- **JVM Diagnostics Managed Server**

  If SLB is not configured, then the aforementioned HTTP and HTTPS upload ports of Enterprise Manager are used.

  If SLB is configured, then the ports configured for JVM Diagnostics on the SLB are used. Alternatively, in addition to the SLB configuration, if the HTTP upload port is enabled for Enterprise Manager, then the HTTP upload port also can be used by the JVM Diagnostics Agents for communicating with the JVM Diagnostics Engine.

- **Java Object Cache (JOC)**

  The default JOC port is 23456.

  If 23456 is not available, no alternate port is used. You need to ensure that port 23456 is free.

- **API Gateway Admin**

  The default HTTP port is 9802. If 9802 is not available, then the first available free port from the range 9801 to 9850 is selected.

The default HTTPS port is 9899. If 9899 is not available, then the first available free port from the range 9851 to 9900 is selected.

- **Extended Domain Admin Server**

  The default HTTP port is the first available free port from the range 7051 to 7100.

  The default HTTPS port is the first available free port from the range 7002 to 7050.

- **Extended Domain Managed Server**

  The default HTTP port is the first available free port from the range 7601 to 7650.

  The default HTTPS port is the first available free port from the range 7651 to 7700.

- **Extended Domain Node Manager**

  The default HTTP port is the first available free port from the range 7501 to 7600.

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>
  ```

How Can You Customize the Ports During and After Installing Enterprise Manager?

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

Customizing the Ports While Installing Enterprise Manager

For information on how to start a Oracle HTTP server instances, see Starting Oracle HTTP Server Instances on a Privileged Port (UNIX Only) in the *Oracle® Fusion Middleware Administering Oracle HTTP Server.*

- If you are installing Enterprise Manager (advanced installation) in graphical mode, that is, using the Enterprise Manager 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.
- If you are installing Enterprise Manager in silent mode, that is, using the installation procedures described in Installing Enterprise Manager System - Advanced Installation Modes, 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

For information on how to start a Oracle HTTP server instances, see Starting Oracle HTTP Server Instances on a Privileged Port (UNIX Only) in the *Oracle® Fusion Middleware Administering Oracle HTTP Server.*

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

1. Stop the OMS. To do so, run the following command from the Oracle home of the OMS host.

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

2. Update the emoms properties with HTTP and HTTPS ports as described in Table 2-3. Specify the values for parameters <http_upload_new>, <https_upload_new>, <http_console_new>, and <https_console_new>):

   Table 2-3 Updating EMOMS Properties with HTTP and HTTPS Ports

Port/Property Type	Command to Run
HTTP Upload Port	<ORACLE_HOME>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerPort -value <http_upload_new>
HTTPS Upload Port	<ORACLE_HOME>/bin/emctl set property -name oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort -value <https_upload_new>
HTTP Console Port	<ORACLE_HOME>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerPort -value <http_console_new>
HTTPS Console Port	<ORACLE_HOME>/bin/emctl set property -name oracle.sysman.emSDK.svlt.EMConsoleServerHTTPSPort -value <https_console_new>

3. Back up the following file that is present in the OMS instance base directory (typically, gc_inst).

   ```
   $<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. To do so, run the following command from the Oracle home of the OMS host.

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

   ```
   $<ORACLE_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 that is present in the agent instance home (typically, `agent_inst`).

   `$<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.**

What Precautions You Must Take While Customizing the Enterprise Manager 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.

What Data Files Are Created While Configuring Oracle Management Repository?

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

Table 2-4 Data Files Created While Configuring Oracle Management Repository

Data Files	Description
`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).

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 Oracle home of the OMS host.

```
$<ORACLE_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
<middleware_home> -oracleHome <ORACLE_HOME>
```

> **Note:**
>
> For Microsoft Windows, invoke `RepManager.bat`.

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 2-5 describes the `-action` options that are supported by the different versions of RepManager.

Table 2-5 RepManager Support for -action dropall and -action drop Commands

RepManager Version	Command Supported
24ai Release 1	`-action drop` The command drops SYSMAN, SYSMAN_MDS, SYSMAN122140_OPSS, and SYSMAN_RO.
13*c* Release 5	`-action drop` The command drops SYSMAN, SYSMAN_MDS, SYSMAN122140_OPSS, and SYSMAN_RO.
13*c* Release 4	`-action drop` The command drops SYSMAN, SYSMAN_MDS, SYSMAN122130_OPSS, SYSMAN_RO, and SYSMAN_BIPLATFORM. Starting with 13*c* Release 4, SYSMAN_OPSS user no longer exists. It has been changed to SYSMAN122130_OPSS user for this release.
13*c* Release 3, 13*c* Release 2, 13*c* Release 1	`-action drop` The command drops SYSMAN, SYSMAN_MDS, SYSMAN_OPSS, SYSMAN_RO, and SYSMAN_BIPLATFORM.

Globalization Support for Enterprise Manager

Enterprise Manager 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 Console.

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

Understanding the Oracle WebLogic Server Requirement for an Enterprise Manager Installation

Enterprise Manager 24ai requires Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0) and Java Development Kit 1.8.0_431. The Enterprise Manager installation wizard automatically installs them for you while installing a new Enterprise Manager system.

> **Note:**
>
> Enterprise Manager 24ai does not support preinstalled Oracle WebLogic Server and Java Development Kit. You need to let the installation wizard get Enterprise Manager installed for you.

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

In particular, this section covers the following:

- How Many Oracle WebLogic Server Domains Are Created?
- 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?

How Many Oracle WebLogic Server Domains Are Created?

During the installation or upgrade to Enterprise Manager 24ai, there are two Oracle WebLogic Server domains created: `GCDomain` and `EMExtDomain1`.

`GCDomain` is the primary domain and used for the Enterprise Manager installation or upgrade.

`EMExtDomain1` is an internal domain and maintained by the `GCDomain` domain.

The WebLogic domains directories are created under the Oracle Management Service (OMS) instance base directory, typically called `gc_inst`.

Example:

```
/u01/software/em24/gc_inst/user_projects/domains
```

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

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

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

When and Why Do You Need the Node Manager Credentials?

While installing or upgrading to Enterprise Manager, 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.

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.

Example:

```
/u01/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

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
```

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

Example:

```
/u01/oracle/gc_inst/em/EMGC_OMS1/emgc.properties
```

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 -admin_only
```

Understanding the Installation Directories

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

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

What Is an Oracle Inventory Directory?

If Enterprise Manager is the first Oracle product that you are installing, then the Enterprise Manager 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 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 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

  ```
  ./em24100_<platform>.bin -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 What Are Oracle Middleware Home, Oracle Management Service Home and Extended Oracle Management Service Home?.

What Are Oracle Middleware Home, Oracle Management Service Home and Extended Oracle Management Service Home?

While installing or upgrading to Enterprise Manager, 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 Oracle Management Service (OMS), the extended Oracle Management Service, the Web tier instance files, and other relevant directories and files. This is where the OMS, extended OMS and the plug-ins are deployed.

Example: `/u01/software/em24/middleware`

> **Caution:**
>
> Starting with Enterprise Manager 24ai Release 1, the Middleware home and the OMS home are separate homes. The OMS home is a subdirectory within the Middleware home. In previous Enterprise Manager releases, the Middleware home and the OMS home were viewed as the same home, also known as Oracle home.

By default, the installation wizard installs Java Development Kit (JDK) 1.8.0_431 and Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0) in the Middleware home you specify. You need to 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:\sw\em24\mwhome` containing less than 25 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\mwh` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

Oracle Management Service Home

It's the home of the Oracle Management Service, also called Oracle home. It's created during the Enterprise Manager installation under the middleware home.

Example: `/u01/software/em24/middleware/oms_home`

Extended Oracle Management Service Home

Starting with Enterprise Manager 24ai Release 1, there's a new extended Oracle Management Service (OMS) home. It's created during the Enterprise Manager installation under the middleware home.

Example: `/u01/software/em24/middleware/ext_oms_home`

The extended OMS home allows performing administrative tasks without interrupting the Enterprise Manager operations. For example, no need of downtime when performing Enterprise Manager upgrades or updates.

What Is an Oracle Management Service Instance Base Location?

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

Oracle Management Service Instance Base Location is a directory outside the Middleware home where the configuration files of the OMS are stored. By default, `gc_inst` is the Oracle Management Service Base Location. However, you can choose to use a custom name if you want.

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/software/em24/middleware`, then by default, the following is the Oracle Management Service Instance Base Location:

```
/u01/software/em24/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 What Are Oracle Middleware Home, Oracle Management Service Home and Extended Oracle Management Service Home?.

What Is an Agent Base Directory?

While installing Enterprise Manager and a standalone Management Agent, 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 (or Oracle home), where the Management Agent home is created.

For example,

```
/u01/software/em24/agentbasedir
```

Ensure that the number of characters in the agent base directory path does not exceed 25 characters for Microsoft Windows platforms. For example, the agent base directory path `C:\sw\em24\agntbsedir` containing only 22 characters is acceptable. However, `C:\Oracle\ManagementAgent\241\new` containing more than 25 characters is not acceptable.

What Is an Agent Home?

Agent Home is the subdirectory within the Agent Base Directory where the Management Agent installed.

For example, if the agent base directory is `/u01/software/em24/agentbasedir`, then by default, the following is the agent home:

```
/u01/software/em24/agentbasedir/agent_24.1.0.0.0
```

What Is an Agent Instance Directory?

Agent Instance Directory is a subdirectory (`agent_inst`) within the Agent Base Directory that is created for storing all Management Agent-related configuration files.

For example, if the agent base directory is `/u01/software/em24/agentbasedir`, then by default, the following is the agent instance directory:

```
/u01/software/em24/agentbasedir/agent_inst
```

What Is a Plug-in Home?

Plug-in home is a subdirectory either within the Middleware home or within the Agent Base Directory where the plug-ins related to the OMS and the Management Agent are deployed, respectively.

Table 2-6 lists the default *Plug-ins homes* are created.

Table 2-6 Plug-in Homes

Component	Default Oracle Home	Sample Location
Plug-In (OMS-specific plug-ins)	`$<ORACLE_HOME>/plugins/<pluginID_Version>`	`/u01/software/em24/oms_home/plugins/oracle.sysman.db.agent.plugin_24.1.0.0.0`
Plug-In (agent-specific plug-ins)	`$<AGENT_BASE_DIR>/agent_24.1.0.0.0/plugins`	`/u01/software/em24/agentbasedir/agent_24.1.0.0.0/plugins`

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

When you invoke the Enterprise Manager 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 Installation Wizard. (For UNIX operating systems, you invoke `em24100_<platform>.bin`, and for Microsoft Windows, you invoke `setup_em24100_win64.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.

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?

What Are Configuration Assistants?

While installing or upgrading to Enterprise Manager 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.)

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

Configuration Assistants Run While Installing a New Enterprise Manager

The following are the configuration assistants that are run while installing a new OMS:

- Plug-ins 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 *MDS Schema Configuration* is not run.

- OMS Configuration

- Plug-ins Deployment and Configuration
- Start Oracle Management Service
- Agent Configuration Assistant

Configuration Assistants Run While Upgrading an Existing Enterprise Manager

The following are the configuration assistants that are run while upgrading an OMS:

- Upgrade Prerequisite
- Plug-ins Prerequisites
- Repository Upgrade
- MDS Schema Configuration
- OMS Configuration
- Plug-ins Deployment and Configuration
- Start Oracle Management Service
- Agent Upgrade And Configuration

Configuration Assistants Run While Upgrading an Additional Oracle Management Service

The following are the configuration assistants that are run while upgrading an additional OMS.

- Upgrade Prerequisite
- Plug-ins Prerequisites
- OMS Configuration
- Plug-ins Deployment and Configuration
- Start Oracle Management Service
- Agent Upgrade And Configuration

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.

Understanding the Prerequisite Checks before Installing Enterprise Manager

Every time you install Enterprise Manager 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?

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 `/bin/bash` file exists with write permission.
- Prerequisite check for verifying that the environment variable `EMCLI_STATE_DIR` is not set.
- 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.
- Prerequisite check for verifying whether there is sufficient disk space in the `temp` directory.
- 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.
- 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.
- Prerequisite check for verifying the host name.
- Prerequisite check for verifying whether the `LD_ASSUME_KERNEL` environment variable is set.
- Prerequisite check for verifying whether proper timezone is set.
- Prerequisite check for verifying whether there is 4 GB of swap space.
- Prerequisite check for verifying whether the `http_proxy` environment variable is set. Ideally, it must not be set.

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 2-7 shows the commands you need to run to run the prerequisite checks in standalone mode:

Table 2-7 Running Prerequisite Checks in Standalone Mode

Installation Type	Command
• Create a New Enterprise Manager System • Upgrade an Existing Enterprise Manager System • Install Software Only	`<Software_Location>/em24100_<platform>.bin -prereqchecker -entryPoint "oracle.sysman.top.oms_Core" -silent`

> **Note:**
>
> On Microsoft Windows, run `setup_em24100_win64.exe`. Also, `<Software_Location>` mentioned in the commands in Table 2-7 refer to the location where the Enterprise Manager software is available. For example, DVD. If you have downloaded the software from *Oracle Software Downloads* site, then enter the absolute path to that downloaded location.

Understanding the Limitations of Enterprise Manager

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

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

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`

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 components to function properly.

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

`https://support.oracle.com/`

Understanding the Startup Scripts

By default, Enterprise Manager 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.

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
```

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:

```
$<ORACLE_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
```

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`.

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.

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 the *Oracle Enterprise Manager 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 6-4.

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 `$<AGENT_HOME>/install/unix/scripts/gcroot.sh` file.

   For more information about these parameters, see Table 6-4.

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

   ```
   $<AGENT_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 `<AGENT_HOME>/install/unix/scripts/gcroot.sh` file, and then run `root.sh`.

Understanding Other Miscellaneous Concepts

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

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

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
```

What Scripts Are Run During the Installation Process?

At least once during or after the installation of Enterprise Manager 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 Oracle home of the OMS host:

  ```
  <ORACLE_HOME>/allroot.sh
  ```

Part II

Installing Enterprise Manager System - Advanced Installation Modes

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

- Installing Enterprise Manager in Silent Mode
- Installing Enterprise Manager Using the Software Only with Plug-ins Method

3

Installing Enterprise Manager in Silent Mode

This chapter describes how you can install Enterprise Manager 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, are acceptable for storing Enterprise Manager 24ai Release 1 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 24ai Release 1 on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.

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 Basic Installation Guide*.

Before You Begin Installing Enterprise Manager in Silent Mode

Before you begin installing an Enterprise Manager system in silent mode, familiarize yourself with the key aspects of installation described in the *Oracle Enterprise Manager Basic Installation Guide*.

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 Basic Installation Guide*.

Installing Enterprise Manager in Silent Mode

This section covers the following:

Installing Enterprise Manager in Silent Mode

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

> **Note:**
>
> Oracle recommends running 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 installer and generate the response file you need to use for performing a silent installation.

   ```
   ./em24100_<platform>.bin -getResponseFileTemplates -outputLoc
   <absolute_path_to_a_directory_to_store_the_generated_response_file>
   ```

> **Note:**
>
> The command generates multiple response files. You must use only the `new_install.rsp` file for this silent installation.

2. Edit the `new_install.rsp` file and enter appropriate values for the parameters described in Table 3-2.
3. Invoke the installer in silent mode and pass the updated response file.

   (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 Basic Installation Guide*.)

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

     ```
     ./em24100_<platform>.bin -silent -responseFile
     <absolute_path_to_the_directory_where_the_generated_and_updated_response_f
     ile_is_stored>/new_install.rsp [-invPtrLoc <absolute_path_to_oraInst.loc>]
     ```

   - Otherwise, run the following command:

     ```
     ./em24100_<platform>.bin -silent -responseFile
     <absolute_path_to_the_directory_where_the_generated_and_updated_response_f
     ile_is_stored>/new_install.rsp
     ```

Note:

- To invoke the installation wizard on UNIX platforms, run `em24100_<platform>.bin`. To invoke on Microsoft Windows platforms, run `setup_em24100_win64.exe`.
- The installer requires about 14 GB of hard disk space in the temporary directory. If your temporary directory does not have this space, then pass the `-J-Djava.io.tmpdir` parameter and provide an alternative directory where there is 14 GB of space.

  The directory specified by this parameter will also be used as the location for the Provisioning Advisor Framework (PAF) staging directory, which is used for copying the Software Library entities related to the deployment procedures. The PAF staging directory is used only for provisioning activities — entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.

  For example,

  ```
  ./em24100_linux64.bin -J-Djava.io.tmpdir=/u01/software/em24/stage/
  ```
- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager 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.
- 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 Advanced Installer Options Supported for Installing an Enterprise Manager System in Silent Mode.

> **Note:**
>
> If a Server Load Balancer (SLB) is configured in your environment, and the upload port is locked, then configure the SLB for JVMD Engines, and then secure the OMS.
>
> If an SLB is configured in your environment, but the upload port is unlocked, then decide whether you want to route the JVMD traffic through the SLB. If you do, then configure the SLB for JVMD Engines, and then secure the OMS.
>
> To secure the OMS, run the following command from the Oracle home of the OMS host:
>
> ```
> <ORACLE_HOME>/bin/emctl secure oms -host <SLB host>-
> slb_jvmd_http_port <JVMD_SLB_HTTP_Port> -slb_jvmd_https_port
> <JVMD_SLB_HTTPS_Port> -sysman_pwd <system_password> -reg_pwd
> <agent_registration_password>
> ```

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 `-J-Djava.io.tmpdir` option, and enter a unique custom location.

  For example,

  ```
  ./em24100_linux64.bin -J-Djava.io.tmpdir=/u00/install/em/STAGE/ -silent -
  responseFile /u01/software/em/response/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 `START_AGENT` 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:

  ```
  ./em24100_<platform>.bin START_OMS=true START_AGENT=false -silent -
  responseFile <absolute_path>/new_install.rsp
  ```

  To understand the limitations involved with this advanced option, see Limitations with the Advanced 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

When you use `START_OMS` and `START_AGENT` 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 Enterprise Manager Console.

Table 3-1 lists the different combinations of these advanced options, and describes the workaround to be followed for each combination:

Table 3-1 Advanced Options and Workarounds

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

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

Table 3-2 describes what variables you must edit and how you must edit them in the new_install.rsp response file for installing Enterprise Manager in silent mode.

Table 3-2 Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

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. For example, "dba" **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
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. For example, "/scratch/oracle/oraInventory". **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
INSTALL_UPDATES_SELECTION	String	Yes	By default, this variable is set to skip indicating that the software updates will not be installed during installation. Enter skip if you want to skip the software updates. Enter staged if you have already downloaded the software updates and you want to install the software updates from a staged location.
STAGE_LOCATION	String	Yes	(Required only if INSTALL_UPDATES_SELECTION=staged) Enter the absolute path of the stage location where the software updates are available.
MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES	String	Yes	Enter the username of the My Oracle Support account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES and MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES, and set INSTALL_UPDATES_SELECTION="download".
MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES	String	Yes	Enter the password of the My Oracle Support account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES and MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES, and set INSTALL_UPDATES_SELECTION="download".
PROXY_USER	String	Yes	Enter the user name that can be used to access the proxy server. **Note:** Applies only if you have set 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. **Note:** Applies only if you have set 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. **Note:** Applies only if you have set the INSTALL_UPDATES_SELECTION parameter to "download", and only if your connection to the Internet requires you to connect through a proxy.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
PROXY_PORT	String	Yes	Enter the port used by the proxy server. **Note:** Applies only if you have set the `INSTALL_UPDATES_SELECTION` parameter to `"download"`, and only if your connection to the Internet requires you to connect through a proxy.
ORACLE_MIDDLEWARE_HOME_LOCATION	String	Yes	Enter the location where you want the installer to install Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0) and Java Development Kit (JDK) 1.8.0_431. Ensure that the middleware location has *write* permission. Note that the middleware location is essentially the one and only Oracle home in 24ai release. For example, `"/u01/software/em24/middleware"` **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:\sw\em24\middlwhome` containing only 22 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. 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. If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host.
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. For example, `"/u01/software/em24/agentbasedir".` Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home. **Note:** *(Only for Microsoft Windows)* Ensure that the number of characters in the agent base directory path does not exceed 25 characters. For example, the agent base directory path `C:\sw\em24\agntbsedir` containing only 22 characters is acceptable. However, `C:\Oracle\ManagementAgent\em24\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.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
WLS_ADMIN_SERVER_PASSWORD	String	Yes	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	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. 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. For more information about this location, see What Is an Oracle Management Service Instance Base Location?. **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 Performing Postinstallation Tasks After Installing an Enterprise Manager System in Silent Mode.
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`. 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 Console. Oracle recommends toconfigure it at the time of installation therefore it's automatically configured by the installer which saves time and effort. For example, `CONFIGURE_ORACLE_SOFTWARE_LIBRARY=true`
SOFTWARE_LIBRARY_LOCATION	String	Yes	Required if you set `CONFIGURE_ORACLE_SOFTWARE_LIBRARY=true` 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 shared location on the OMS host. This helps when you install additional OMS instances that can use the same shared Software Library location.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System 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. For example, `"example.com"`. 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. 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. 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. However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command: `$<ORACLE_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` If your Oracle RAC database is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener. **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 SYSMAN122140_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. For example, `"1521"`.
SERVICENAME_OR_SID	String	Yes	Enter the service name or the system ID (SID) of the existing database. For example, `"orcl"`. If you are providing the details of a pluggable database (PDB), then use the full service name instead of the alias. For example, pdb.example.com. If you are providing the details of a lone-pluggable database (Lone-PDB), then use the full service name. For example, pdb.example.com. If you are providing the details of a non-container database (Non-CDB), then use the SID.
SYS_PASSWORD	String	Yes	Enter the SYS database user account's password.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
dbUser	String	Yes	Enter the non-SYS (admin) username. This is the non-SYS database user (a database user other than the SYS database user) that creates the repository schema during the install process. The `dbUser` parameter value cannot be `SYS`. Naming convention: User name should start with the `SYSMAN_` prefix. For example: `dbUser=SYSMAN_ADMIN` If the user doesn't exist, the install process creates the new user in the Repository database. This parameter is only required if `INSTALL_WITH_NON_SYS_USER = true`
dbPassword	String	Yes	Enter the non-SYS (admin) user password. This is the non-SYS database user password that creates the repository schema. This parameter is only required if `INSTALL_WITH_NON_SYS_USER = true`
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. The SYSMAN account password must begin with a letter, and can only contain uppercase or lowercase letters, numbers and the following characters: $, # , _ Examples of invalid passwords: Welcome!, 123oracle, #Oracle 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 SYSMAN122140_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 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System 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. • **SMALL,** to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions • **MEDIUM,** to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions • **LARGE,** to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions For example, `"MEDIUM"`. 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. 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 What Is a Deployment Size for Enterprise Manager in an Advanced Configuration?. **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 set here matches with the deployment size you selected on the 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: • 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 Basic Installation Guide*. • 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 Basic Installation Guide*.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System 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 (`mgmt.dbf`) for management tablespace can be stored. Ensure that the specified path leads up to the file name. For example: • If the database is on a file system, then the path must look like "`/u01/oracle/prod/oradata/mgmt.dbf`". • 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). • 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. Enterprise Manager 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. For example, "`/home/john/oradata/mgmt_ecm_depot1.dbf`". Enterprise Manager 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. For example, "`/home/john/oradata/mgmt_deepdive.dbf`". Enterprise Manager requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).
EMPREREQ_AUTO_CORRECTION=false	Boolean	No	It specifies whether prereqs can be auto corrected.
INSTALL_WITH_NON_SYS_USER	Boolean	No	It specifies if the install is being performed using a database user different than SYS. This user is also known as non-SYS user. For example: `INSTALL_WITH_NON_SYS_USER=true` If this parameter is set to `true`, you also need to provide the `dbUser` and `dbPassword` parameters (the user name and password of the non-SYS user). The `dbUser` parameter value cannot be `SYS` and should always start with `SYSMAN_`.
Is_oneWaySSL	Boolean	No	Applicable for one-way SSL configuration. Set it to `true` if the repository database is configured with one-way SSL. Example: `Is_oneWaySSL=true` If `Is_oneWaySSL=true` is set, then the `TRUSTSTORE_LOCATION` and `TRUSTSTORE_PASSWORD` parameters are required.

Table 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
TRUSTSTORE_LOCATION	String	Yes	(Required only if `Is_oneWaySSL=true`) Applicable for one-way SSL configuration. Enter the absolute location of TrustStore Wallet file.
TRUSTSTORE_PASSWORD	String	Yes	(Required only if `Is_oneWaySSL=true`) Applicable for one-way SSL configuration. Enter the TrustStore Wallet password.
Is_twoWaySSL	Boolean	No	Applicable for two-way SSL configuration. Set it to `true` if the repository database is configured with two-way SSL. Example: `Is_twoWaySSL=true`
KEYSTORE_LOCATION	String	Yes	(Required only if `Is_twoWaySSL=true`) Enter the location of the keystore (location where the SSL key will get stored).
KEYSTORE_PASSWORD	String	Yes	(Required only if `Is_twoWaySSL=true`) Enter the password of the keystore.
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 What Ports Are Used for Installation? are honored. If you want to accept the default ports, then leave this field blank. 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 3-2 (Cont.) Editing the new_install.rsp Response File for Installing Enterprise Manager System in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description

PLUGIN_SELECTION	String List	Yes
		(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 Plug-in, Oracle Fusion Middleware Plug-in, and Oracle Exadata Plug-in, Oracle Cloud Framework Plug-in, and Oracle System Infrastructure Plug-in are automatically installed with the Enterprise Manager system.
			In addition to the default ones, if you want to deploy any addition plug-in, then list those plug-in names in a comma-separated list. Ensure that the plug-in names are in double quotes.
			If you want to deploy a deprecated plug-in that is supported only in the current release, but not in any of the future releases, then evaluate your selection and decide whether or not you want to proceed with the deployment of such plug-ins.
			For example,
			`PLUGIN_SELECTION={"oracle.sysman.empa"}`
			If you want to install some plug-ins that are not in the software kit (DVD, downloaded software), then do the following:
			1. Manually download the required plug-ins from `Plug-in Update`.
			Plug-ins produced by partners and customers are available for download from the Enterprise Manager Extensibility Exchange.
			2. Invoke the installer with the following option and pass the location where the additional plug-ins have been downloaded:
			`./em24100_<platform>.bin PLUGIN_LOCATION=<absolute_path_to_plugin_software_location>`

b_upgrade	Boolean	No	For this case, set it to `b_upgrade=false`
EM_INSTALL_TYPE	String	No	For this case, set it to `EM_INSTALL_TYPE=NOSEED`
CONFIGURATION_TYPE	String	No	For this case, set it to `ADVANCED` `CONFIGURATION_TYPE=ADVANCED`

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 Basic Installation Guide*.

4

Installing Enterprise Manager Using the Software Only with Plug-ins Method

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

Note:

- To install Enterprise Manager in a production environment, use the *Advanced Install* or *Install software only with plug-ins* installation type. The *install software only with plug-ins* installation type offers custom and advanced configuration options that enable you to customize your installation to suit your needs.
- **Non-SYS user**: You can configure Oracle Enterprise Manager with a non-SYS admin user during the installation, upgrade, patching and plug-ins deployment. Using a non-SYS user allows Enterprise Manager administrators to use another user, an admin user, for these tasks since organizations continue to lock privileges credentials like the SYS database user to perform those activities.
- **SSL Support**: SSL configuration is supported. If the repository database is configured with one-way or two-way SSL authentication, you can configure the Enterprise Manager against the SSL-enabled repository database when configuring the Enterprise Manager software only in graphical or silent mode. PKCS12 is the wallet file format supported for SSL configuration.
- All general purpose file systems, including OCFS2, are acceptable for storing Enterprise Manager 24ai 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 24ai on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.

Introduction to Installing Enterprise Manager Using the Software Only with Plug-ins Method

You can choose to install only the software binaries of Enterprise Manager 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:

- Installs Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0).
- Installs Oracle JRF 12*c* Release 2 (12.2.1.4.0).
- Installs Java Development Kit (JDK) 1.8.0_431.
- Installs Oracle Management Service 24ai Release 1 which includes the following:
  - WebLogic container.
  - Zero Downtime (ZDT) WebLogic container.
  - API Gateway.
- Installs Oracle Management Agent 24ai Release 1 in the agent base directory.

  It's located outside the Middleware home and specified during the installation process.

During the configuration phase, you invoke a configuration script to do the following:

- Creates an Oracle WebLogic domain called `GCDomain` in the WebLogic container. For this WebLogic domain, a default user account `weblogic` is used as the administrative user. This domain is one across all OMSs.
- Creates an Oracle WebLogic domain called `EMExtDomain1` in the Zero Downtime (ZDT) WebLogic container. It's also called extended domain. This domain is one per OMS instance.
- 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 24ai including the two WebLogic domains `GCDomain` and `EMExtDomain1`.

  For example, if the Middleware home is `/u01/software/em24/middleware`, then the instance base location is `/u01/software/em24/gc_inst`.

- Configures Oracle Management Repository in the existing, certified Oracle Database. If the database instance is created using the database template offered by Oracle, then this step is skipped.

  > **Note:**
  >
  > – The existing, certified Oracle Database must be one of the certified databases listed in the Enterprise Manager certification matrix available on *My Oracle Support,* or a database instance created with a preconfigured Oracle Management Repository (Management Repository) using the database templates offered by Oracle. To access the Enterprise Manager certification matrix, see Accessing the Enterprise Manager Certification Matrix.
  >
  > For information about creating a database instance with a preconfigured Management Repository using the database templates offered by Oracle, see Creating a Database Instance with Preconfigured Repository Using Database Templates in the *Enterprise Manager Basic Installation Guide*.
  >
  > The database can be on a local or remote host, and if it is on a remote host, it must be monitored by Oracle Management Agent. However, Oracle Real Application Clusters (Oracle RAC) databases must only be on a shared disk.
  >
  > – SSL configuration is supported. If the repository database is configured with one-way or two-way SSL authentication, you can configure the Enterprise Manager against the SSL-enabled repository database when configuring the Enterprise Manager software only in graphical or silent mode. PKCS12 is the wallet file format supported for SSL configuration.

- Creates a plug-in directory and installs the following default plug-ins.
  – Oracle Database Plug-in
  – Oracle Fusion Middleware Plug-in

  > **Note:**
  >
  > Starting with 13*c* Release 1, as part of the Oracle Fusion Middleware Plug-in deployment, one Java Virtual Machine Diagnostics (JVMD) Engine is installed by default on the OMS. For every additional OMS you deploy, you receive one JVMD Engine by default with that OMS.
  > JVMD 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.
  >
  > While JVMD Engine is installed by default on the OMS host, you will still need JVMD Agents to be manually deployed on the targeted JVMs. For instructions to deploy the JVMD Agent, see Installing JVMD Agents with Advanced Install Options for installing with advanced install options.

  – Oracle Exadata Plug-in
  – Oracle Cloud Framework Plug-in
  – Oracle System Infrastructure Plug-in

  - Any other additional plug-ins you choose to deploy
- Runs the following configuration assistants to configure the installed components for simple as well as advanced installation:
  - Plug-ins 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 *MDS Schema Configuration* is not run.

  - OMS Configuration
  - Plug-ins Deployment and Configuration
  - Start Oracle Management Service
  - Agent Configuration Assistant

Before You Begin Installing Enterprise Manager Using the Software Only with Plug-ins Method

Before you begin installing an Enterprise Manager system using software only mode, familiarize yourself with the key aspects of installation described in the *Enterprise Manager Basic Installation Guide*.

Prerequisites for Installing Enterprise Manager Using the Software Only with Plug-ins Method

Meet the prerequisites described under the Prerequisites for Installing an Enterprise Manager System in the *Enterprise Manager Basic Installation Guide*.

Installing the Enterprise Manager Using the Software Only with Plug-ins Method

This section describes the following:

- Install Software Only With Plug-ins and Configure Later in Graphical Mode
- Install Software Only With Plug-ins and Configure Later in Silent Mode

> **Note:**
>
> - The above software only methods are only applicable for a new fresh installation of Enterprise Manager. Do not use if you are doing an Enterprise Manager upgrade using the software only method.

Install Software Only With Plug-ins and Configure Later in Graphical Mode

This section explains how you can install only the software binaries of Enterprise Manager with plug-ins at one point and configure the installation at a later point all in graphical mode.

This installation type provides the following benefits:

- Deploys the mandatory plug-ins such as Oracle Database plug-in, Oracle Fusion Middleware plug-in, Oracle Exadata plug-in, Oracle Cloud Framework plug-in, and Oracle System Infrastructure plug-in. In addition, enables you to select and deploy other optional plug-ins of your choice. This installation type allows you to install software only OMS bits, along with selected plug-ins.

  > **Note:**
  >
  > You may choose to manually download the required plug-ins from `Plug-in Update`.
  >
  > In addition, plug-ins produced by partners or customers are available for download from the `Enterprise Manager Extensibility Exchange`.

- You may choose to apply release update patches available post-release, once you have completed installing the Enterprise Manager System Using Software Only Install With Plug-ins and Configuring Later in Graphical Mode option.
- Offers an option to select the deployment size (small, medium, or large) of your choice, and depending on the deployment size you select, configures with the required memory. 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.
- Allows you to use a database where the Management Repository is preconfigured using the database templates offered by Oracle.
- Allows you to change the name of the default WebLogic user account for the WebLogic domain GCDomain.
- Prompts for separate, distinct passwords for WebLogic Server administration, Node Manager, SYSMAN user account, and Management Agent registration.
- Allows you to change the name of the default OMS instance base directory (gc_inst) to a name of your choice, and creates that directory outside the Middleware home.
- Allows you to change the locations of the tablespaces for management, configuration data, and JVM diagnostics data.

- Allows you to customize the ports according to your environment.
- **SSL Support:** You can enable one-way or two-way Secure Sockets Layer (SSL) mode during the Configuring the Enterprise Manager Software Only in Graphical Mode step when running the `ConfigureGC` script.

> **Note:**
>
> PKCS12 is the wallet file format supported for SSL configuration.

- **Non-SYS User**: You can configure Oracle Enterprise Manager with a non-SYS admin user during the Configuring the Enterprise Manager Software Only in Graphical Mode step when running the `ConfigureGC` script. Using a non-SYS user allows Enterprise Manager administrators to use another user, an admin user, for these tasks since organizations continue to lock privileges credentials like the SYS database user to perform those activities.

Workflow for Installing Software Only With Plug-ins and Configure Later in Graphical Mode

General workflow for installing the software binaries of Enterprise Manager with plug-ins first, and then configuring the installation at a later point in graphical mode.

1. Installing the Enterprise Manager Software Only With Plug-ins in Graphical Mode
2. Running the Root Script
3. Evaluate Non-SYS User Creation
4. Apply Release Update
5. Configuring the Enterprise Manager Software Only in Graphical Mode
6. Performing Postconfiguration Tasks After Configuring the Enterprise Manager Software Only in Graphical Mode

Installing the Enterprise Manager Software Only With Plug-ins in Graphical Mode

This section explains how you can install only the software binaries of Enterprise Manager with Plug-ins at one point in graphical mode, and configure the installation at a later point.

To install Enterprise Manager for a production site, 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 *Overview of the EM Prerequisite Kit* in the *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 Installation Wizard.**

   Invoke the installation wizard as a user who belongs to the `oinstall` group you created following the instructions in *Creating Operating System Groups and Users for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.*

   `./em24100_<platform>.bin [-invPtrLoc <absolute_path_to_oraInst.loc>]`

   For example, for Linux platform, run `/u1/software/em/em24100_linux64.bin [-invPtrLoc <absolute_path_to_oraInst.loc>]`

Note:

- To invoke the installation wizard on UNIX platforms, run `em24100_<platform>.bin`. To invoke on Microsoft Windows platforms, run `setup_em24100_win64.exe`.
- The installer requires about 14 GB of hard disk space in the temporary directory. If your temporary directory does not have this space, then pass the `-J-Djava.io.tmpdir` parameter and provide an alternative directory where there is 14 GB of space.

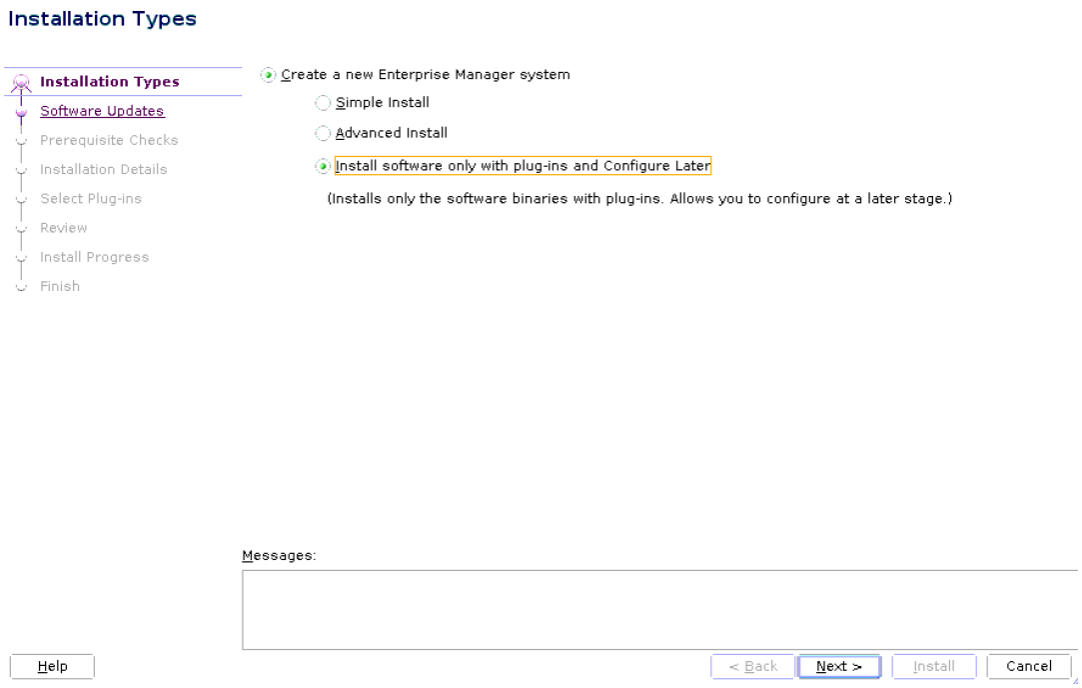
  The directory specified by this parameter will also be used as the location for the Provisioning Advisor Framework (PAF) staging directory, which is used for copying the Software Library entities related to the deployment procedures. The PAF staging directory is used only for provisioning activities — entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.

  For example,

  ```
  ./em24100_linux64.bin -J-Djava.io.tmpdir=/u01/software/em24/stage/
  ```
- Ensure that there are no white spaces in the name of the directory where you download and run the Enterprise Manager 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.
- The `INSTALL_SWONLY_WITH_PLUGINS` parameter is not supported starting with Enterprise Manager 13c Release 5. If you execute the `./em24100_<platform>.bin` script using the `INSTALL_SWONLY_WITH_PLUGINS` parameter, you will receive an invalid parameter error message since the parameter is no longer supported.

2. Click **Next.**
3. **Select Installation Type.**

   On the Installation Types screen, select **Create a new Enterprise Manager system,** then select **Install software only with plug-ins**



4. Click **Next.**
5. **(Recommended) Install Software Updates.**

   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 the *Enterprise Manager Advanced Installation and Configuration Guide*.

> **Note:**
>
> The Software Updates screen uses the built-in feature *Auto Update* to automatically download and deploy the latest recommended patches while installing or upgrading Enterprise Manager. 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.

> **Note:**
>
> During installation, you will be 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 software updates selected on this screen cannot be automatically applied. In such a case, you must manually download and apply these software updates after the installation.

> **Note:**
>
> Despite providing the My Oracle Support credentials, if you are unable to download the software updates, then exit the installer, and invoke the installer again passing the `-showProxy` parameter in the following way:
>
> ```
> <Software_Location>/em24100_<platform>.bin SHOW_PROXY=true
> ```

6. Click **Next.**

   If Enterprise Manager 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 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
   ```

7. **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>/em24100_<platform>.bin
  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.

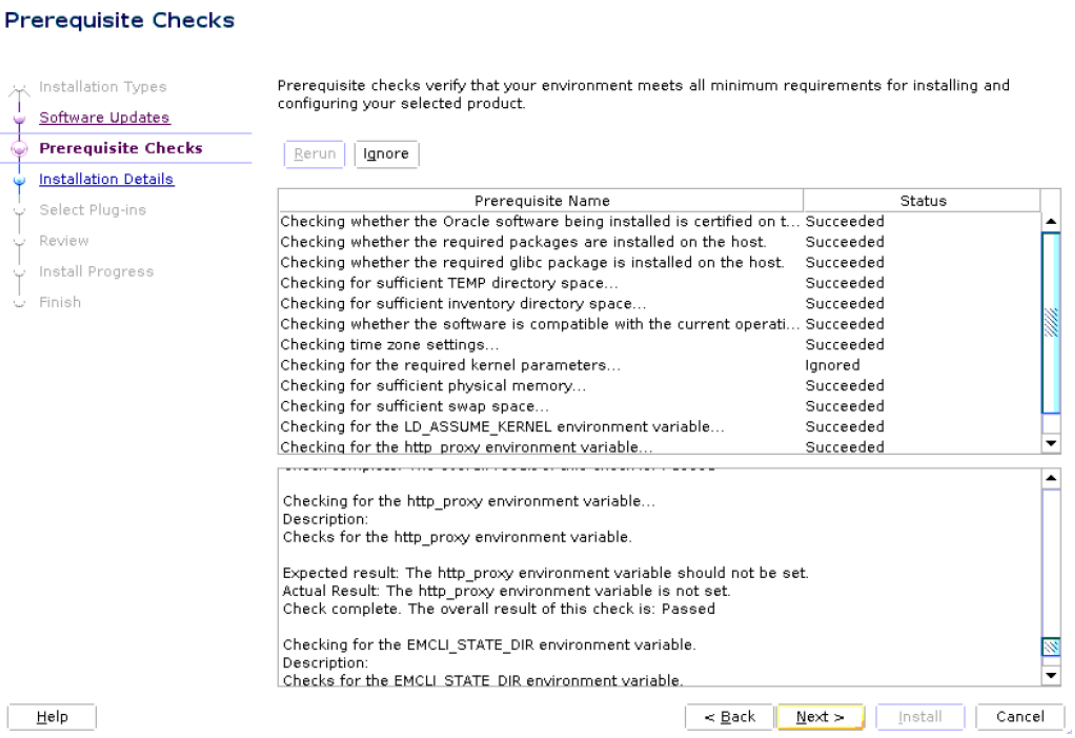
  For example,

  ```
  <Software_Location>/em24100_<platform>.bin -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.

8. Click **Next.**
9. **Check Prerequisites.**



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. For example, it checks for the required operating system patches and operating system packages.

The status of the prerequisite check can be either **Warning, Failed, Succeeded, Not Executed, In Progress,** or **Pending.**

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.

> **Note:**
>
> You can choose to ignore the checks with **Warning** status by clicking **Ignore.** However, all package requirements must be met or fixed before proceeding any further.

10. 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, see *Package Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.

11. **Enter Installation Details.**

On the Installation Details screen, do the following:

a. Enter the Middleware home where you want to install the OMS and other core components. This is essentially the Oracle home.

> **Note:**
>
> - The Enterprise Manager Installation Wizard installs Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0) and JDK 1.8.0_431 by default in this middleware home directory you enter here. A preinstalled JDK or Oracle WebLogic Server is *not* supported from 13*c* Release 1 onwards.
> - 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 middleware home where the Management Agent can be installed. For example, if the middleware home is `/u01/software/em24/middleware`, then you can specify the agent base directory as `/u01/software/em24/agentbasedir`.

   Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle 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 or virtual 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.

12. Click **Next.**
13. **Select Plug-Ins.**

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

    Plug-Ins are pluggable entities that offer special management capabilities customized to suit specific target types or solution areas.

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

    > **Note:**
    >
    > If you select a deprecated plug-in that is supported only in the current release, but not in any of the future releases, then you are prompted to evaluate your selection and decide whether or not you want to proceed with the deployment of such plug-ins.

    > **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.
    >
    > For details, see Using Advanced Script Options While Configuring the Enterprise Manager Software Using the Install Software Only Method in Graphical Mode.

14. Click **Next.**

Note:

- If you are connecting to an Oracle RAC database, and if you have specified the virtual IP address of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connection string with information about the other nodes that are part of the cluster. Update the connection string and click **OK.** If you want to test the connection, click **Test Connection.**
- If your Oracle RAC database is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener.
- If you are connecting to an Oracle Database that is configured with CDB or PDB, then make sure you open the PDB before you provide the PDB details on this screen.
- If you see an error stating that the connection to the database failed with ORA-01017 invalid user name/password, then follow these steps to resolve the issue:

  (1) Verify that SYS password provided is valid.

  (2) Verify that the database initialization parameter `REMOTE_LOGIN_PASSWORDFILE` is set to Shared or Exclusive.

  (3) Verify that password file with the file name `orapw<SID>` exists in the `<ORACLE_HOME>/dbs` directory of the database home. If it does not, create a password file using the `ORAPWD` command.
- 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, see *Installing Oracle Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.

15. **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 software only installation process.

16. **Track the Progress.**

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

17. **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.

18. **Run Scripts.**

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

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

    The install software only with plug-ins has been completed. Now you can proceed with the next step, the configuration process.

Using Advanced Installer Options While Installing the Enterprise Manager Software Using the Software-Only Method in Graphical Mode

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

- For Oracle Enterprise Manager 13c and higher, `GCDomain` is the only supported domain name for creating the WebLogic domain. Customized WebLogic domain names are not supported.
- 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,

  ```
  ./em24100_<platform>.bin -invPtrLoc /scratch/OracleHomes/oraInst.loc
  ```
- 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 `START_AGENT` options, and set them to `true` or `false` depending on what you want to control.

> **Note:**
>
> Ensure that the `START_OMS` and `START_AGENT` options are used even when the ConfigureGC.sh is invoked to configure the software binaries as described in Configuring the Enterprise Manager Software Only in Graphical Mode .

Running the Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager, 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 Oracle home of the OMS host:

  ```
  $<ORACLE_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 $<ORACLE_HOME>/allroot.sh`

Evaluate Non-SYS User Creation

Review the creation and usage of a non-SYS user and evaluate if it fits the security needs of your organization.

Since security is a growing concern, Oracle provides the option to perform the installation, configuration and patching of the OMS using a non-privileged administrator user, also known as non-SYS user.

After the user is created, the non-SYS database user performs the Enterprise Manager installation, configuration and patching process, eliminating the requirement to use the SYS user for those operations.

> **Note:**
>
> Once you create and start using the non-SYS admin user for the installation, configuration and patching of the OMS, you cannot switch back to use SYS as an admin user to perform any of those operations.

Using Non-SYS user

- Less-privileged database administrator user. Also known as admin user.
- Performs Enterprise Manager installation, configuration and patching operations. (The SYS database user is no longer required during the installation, configuration and patching).
- User is created during the execution of the `ConfigureGC` script (Enterprise Manager configuration).
- Naming convention: `SYSMAN_` is the username prefix.

Using SYS user (Default option)

- Privileged database administrator user.
- Performs the Enterprise Manager installation, configuration and patching operations.

You are prompted to make the selection of creating and performing the installation using SYS or non-SYS user during the **Database User Details** step from Configuring the Enterprise Manager Software Only in Graphical Mode .

Apply Release Update

If there's a Release Update available, Oracle recommends to apply the latest Release Update after installing the Enterprise Manager software binaries.

A Release Update, previously known as Bundle Patch, is an official Oracle patch that can be applied on top of Enterprise Manager 24ai Release 1 main release on an Oracle Home using the `omspatcher apply -bitonly` command. For more information about patching and the

`omspatcher` utility, see Patching Oracle Management Service and the Repository in the *Enterprise Manager Administrator's Guide*.

> **Note:**
>
> You can patch the OMS using a non-SYS user (admin user).
> Oracle provides the option to perform the configuration and patching process using a non-privileged user, eliminating the requirement to use the SYS database user and password for the patching process. For information, see Evaluate Non-SYS User Creation.

To apply the Release Update, do the following:

- Obtain the latest Release Update by logging in to My Oracle Support: https://support.oracle.com/.
- Review the `Readme` file that comes with the Release Update.
- Use the latest version of the `omspatcher` as suggested in the Release Update `Readme` file, and keep a backup of the previous `omspatcher`.
- **Non-SYS user**: If you decide to create and use non-SYS user in your environment, you must confirm that the non-SYS user has already been created before applying the release update. For information about creating the user, see Evaluate Non-SYS User Creation.

To apply a Release Update, perform the following steps:

1. Before proceeding, ensure that `$ORACLE_HOME/OMSPatcher` directory is included in the path since `omspatcher` is located in that directory.
2. Execute omspatcher in bitonly mode for the Release Update.

   ```
   omspatcher apply -bitonly
   ```

3. Run `omspatcher lspatches` command to list all the sub-patches applied in Step 1.

   Syntax: omspatcher lspatches | grep "<RU Number / Id >"

Configuring the Enterprise Manager Software Only in Graphical Mode

To configure Enterprise Manager, follow these steps:

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

   Invoke the installation wizard in graphical mode. (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, *Creating Operating System Groups and Users for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.*

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

   For Microsoft Windows platforms, invoke `ConfigureGC.bat` script.

   Optional Parameter:

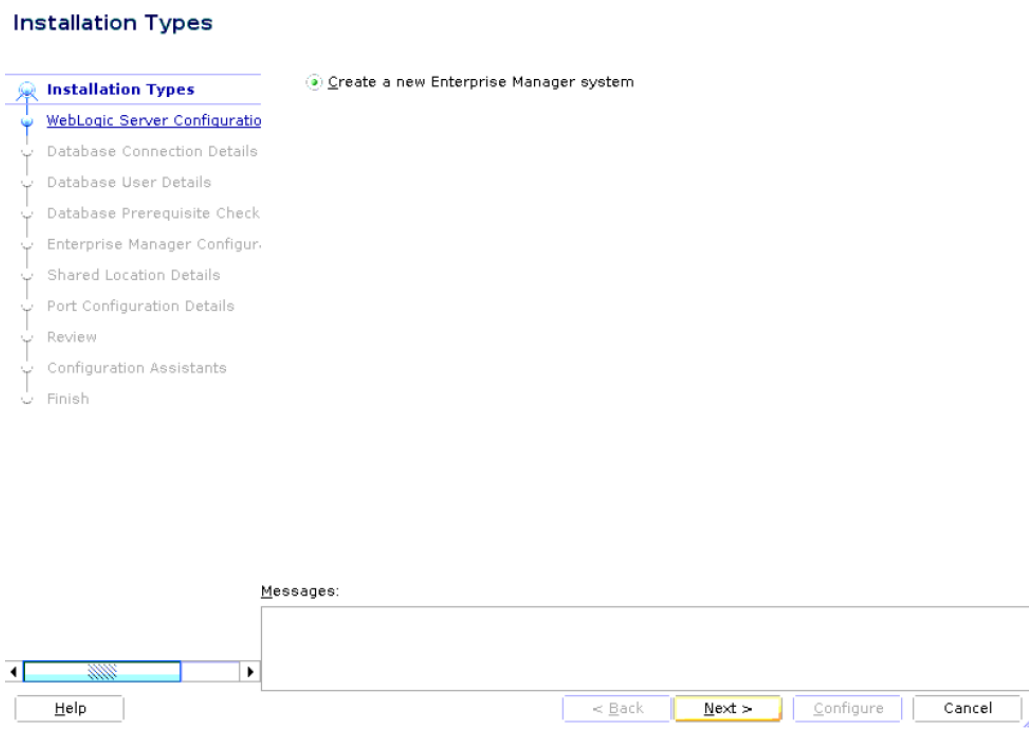
   - The `-invPtrLoc` parameter is supported only on UNIX platforms. Do not use it on Microsoft Windows platforms.

For more information additional advanced options you can pass while invoking the `ConfigureGC` script, see Using Advanced Script Options While Configuring the Enterprise Manager Software Using the Install Software Only Method in Graphical Mode.

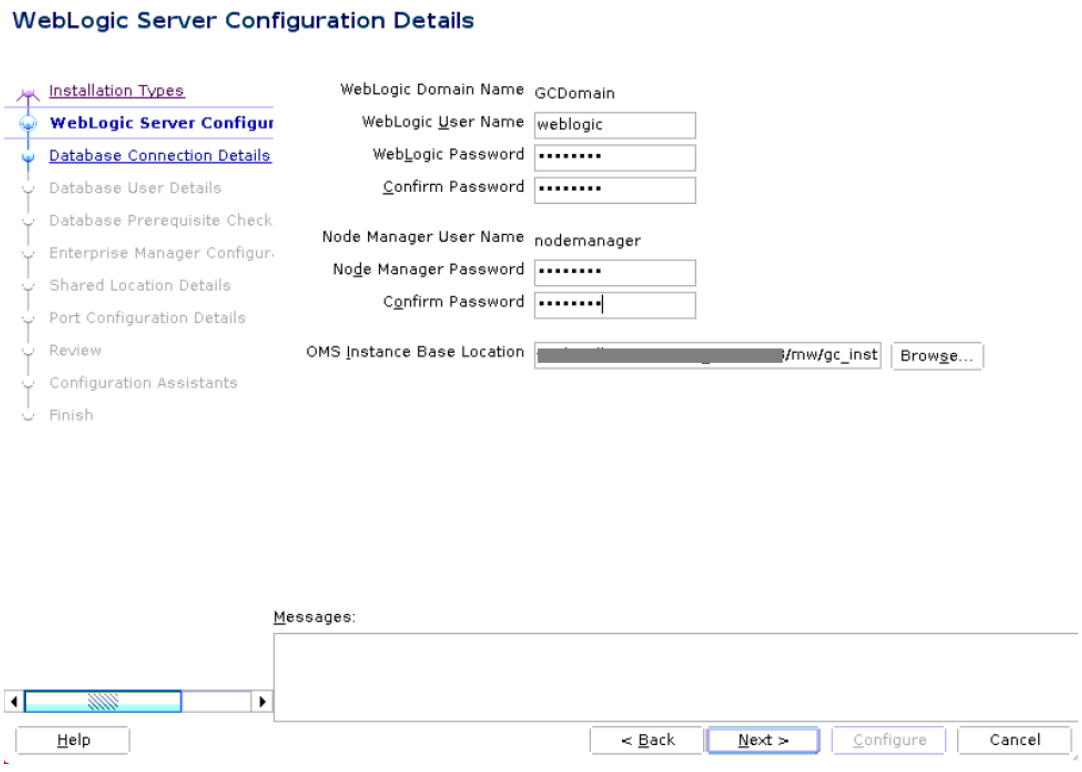
> **Note:**
>
> - While installing the software binaries as described in Installing the Enterprise Manager Software Only With Plug-ins in Graphical Mode, if you had passed the argument `-invPtrLoc`, then you need to pass the same argument in this step as well.
> - The only way to configure the software 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.
> - If you accidentally exit the installer before clicking **Retry,** then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.pl` script from the Oracle home to rerun the Configuration Assistant in silent mode. For Microsoft Windows platforms, invoke `runConfig.pl` script.
>
>   ```
>   $<ORACLE_HOME>/oui/bin/runConfig.pl
>   <absolute_path_to_Middleware_home>
>   ```
>
>   If the `runConfig.pl` script fails, then clean up your environment and redo the installation.

2. **Select Installation Type**

   On the Installation Types screen, select **Create a new Enterprise Manager system**.



3. Click **Next**.
4. **Enter WebLogic Server Configuration Details**



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

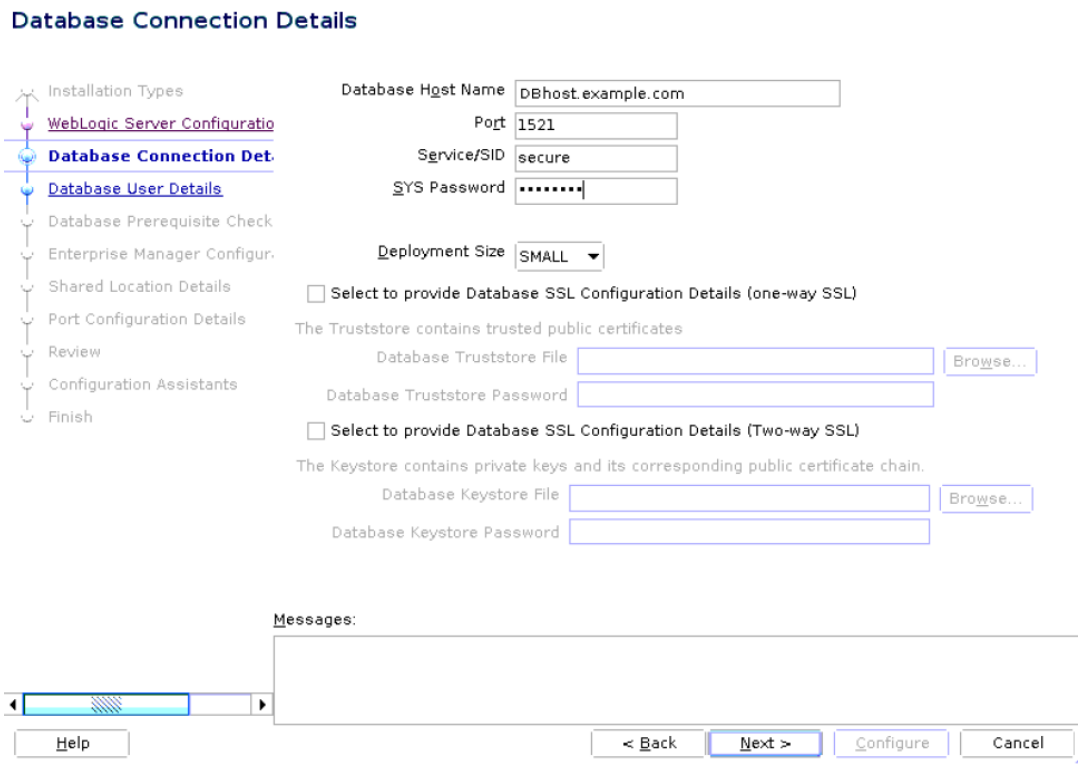
By default, the WebLogic Domain name is `GCDomain`, and the Node Manager name is `nodemanager`. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager.

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.

5. Click **Next**.
6. **Enter Database Connection Details**



On the Database Connection Details screen, do the following:

a. Enter the Database connection details.

   Provide the following details of the existing certified database where the Management Repository needs to get created:

   - Database host name.
   - Port (Database listener port).
   - Service/SID (Database service id).
   - SYS Password (Password of the SYS database user).

   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 *Enterprise Manager 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 SYSMAN122140_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on the Repository Configuration Details screen).
- The PDB name will always be `empdbrepos` irrespective of the CDB name if the PDB is created with the above listed templates. However, if the CDB is created with `<domain name>` then the PDB will be `empdbrepos.<domain name>`. For more information see, *Creating a Database Instance with Preconfigured Repository Using Database Templates* in the *Oracle Enterprise Manager Basic Installation Guide.*
- If you are providing the details of a pluggable database (PDB), then use the full service name instead of the alias. For example, pdb.example.com. If you are providing the details of a lone-pluggable database (Lone-PDB), then use the full service name. For example, pdb.example.com. If you are providing the details of a non-container database (Non-CDB), then use the SID.
- To identify whether your database is a certified database listed in the certification matrix, access the certification matrix as described in *Accessing the Enterprise Manager Certification Matrix* in the *Oracle Enterprise Manager Basic Installation Guide.*
- 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, see *Overview of the EM Prerequisite Kit* in the *Oracle Enterprise Manager Basic Installation 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 What Is a Deployment Size for Enterprise Manager in an Advanced Configuration?.

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

Table 4-1 (Cont.) Deployment Size

Deployment Size	Targets Count	Management Agents Count	Concurrent User Session Count
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

c. (Optional) Check the **Select to provide Database SSL Configuration Details (one-way SSL)** checkbox if the database is one-way SSL configured. The truststore details are required for one-way SSL configuration.

   Provide the database truststore file and password.

d. (Optional) Check the **Select to provide Database SSL Configuration Details (two-way SSL)** checkbox if the database is two-way SSL configured. The keystore details are required for two-way SSL configuration.

   Provide the database keystore file and password.

   PKCS12 wallet file format is supported.

7. 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 in the 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 the *Enterprise Manager 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 the *Enterprise Manager Basic Installation Guide*.

8. **Enter Database User Details**

On the **Database User Details** screen, select if you want to perform the installation using SYS or non-SYS database user.

> **Note:**
>
> Starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher, you can perform the configuration using the SYS admin user (default option) or a different user, known as a non-SYS admin user.

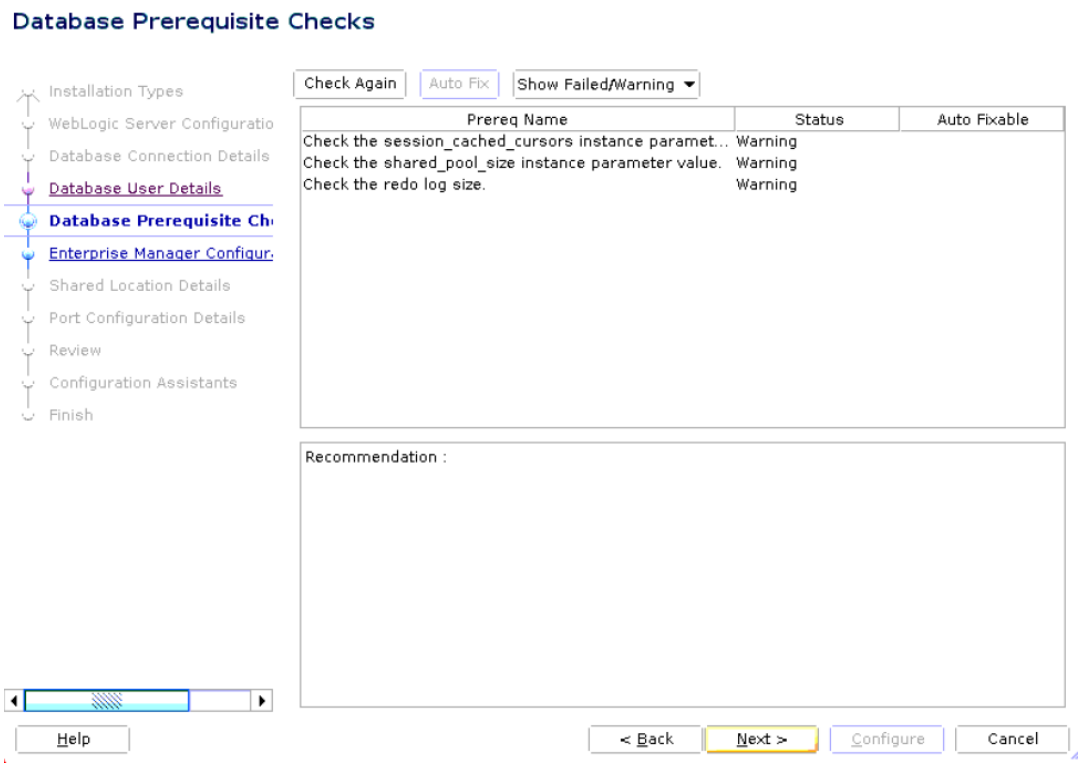
SYS is the default user in the Repository database.

A non-SYS user is a less privileged administrator user of the Repository database that still allows you to perform Enterprise Manager administration tasks.

If the **Perform Installation using non-SYS user** is selected, you need to provide the database user name and password for the non-SYS user. The non-SYS user name should have the `SYSMAN_` prefix as part of user name. For example, you can enter `SYSMAN_ADMIN` under **DB Username**. If the user doesn't exist, the Enterprise Manager installer creates the new user in the Repository database.

Click **Next**.

9. **Check the Database Prerequisites.**



On the Database Prerequisite Checks screen, check the status of the database prerequisites performed by the installation wizard, and verify whether your environment meets all the minimum requirements for a successful installation. Then click **Next**.

The installation wizard runs the database prerequisite checks automatically when you come to this screen. 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 **Check Again** to check the database prerequisites again.

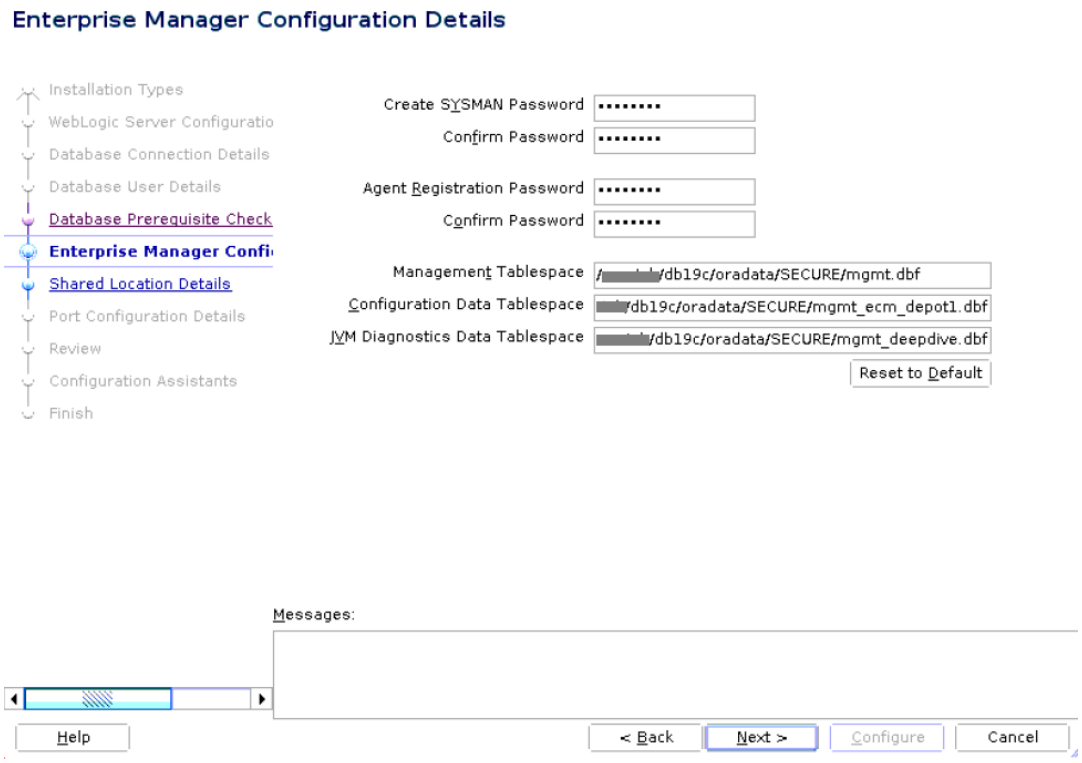
- If the Auto Fixable column is `Yes`, you can click on **Auto Fix** and the installer will fix the issue automatically.
- If the recommendation indicates that the Correction Type is `Manual`, you need to fix the issue manually.

After you complete reviewing and fixing the prerequisites results, click **Next**.

The **Information** pop-up window is displayed.

Review the important information provided and then click **OK**.

10. Click **Next**.
11. **Enter Enterprise Manager Configuration Details**



On the Repository Configuration Details screen, do the following:

a. For **SYSMAN Password**, enter and confirm 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. SYSMAN is also the super administrator for Enterprise Manager.

> **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 SYSMAN122140_OPSS, which were created while preconfiguring the Management Repository, are automatically reset with the SYSMAN password you enter on this screen.

b. For **Agent Registration Password**, enter and confirm 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 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`

12. Click **Next**.

13. **Configure Shared Locations**.

    On the Enterprise Manager Shared Location Details screen, do the following:

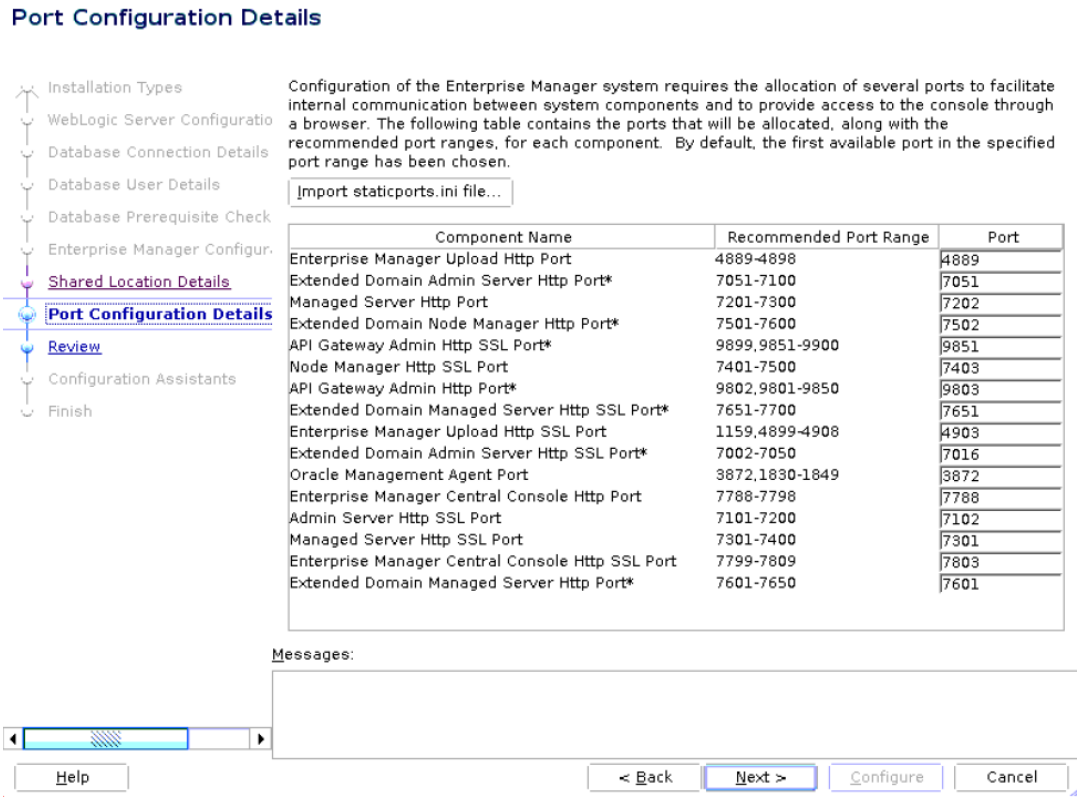
    a. Configure Oracle Software Library. Oracle Software Library (Software Library) is a feature within Enterprise Manager that acts as a repository to store software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. You require the Software Library for operations such as provisioning and patching.

       When checking **Configure Oracle Software Library** check box, enter the absolute path leading up to a unique directory name. By default, the storage location that is configured is the *OMS Shared File System* location, Oracle strongly recommends that the location you enter is a mounted location on the OMS host. This helps when you install additional OMS instances that can use the same mounted Software Library location.

> **Note:**
>
> Software Library supports two types of storage locations, mainly *OMS Shared File System* location and *OMS Agent File System* location. To understand these storage locations, see *Upload File Locations* in the *Oracle Enterprise Manager Administrator's Guide.*.
>
> For some reason, if you are unable to configure an *OMS Shared File System* location, then configure an *OMS Agent Storage* location. For instructions, see *Configuring an OMS Agent File system Location* in the *Oracle Enterprise Manager Administrator's Guide.*

> **Note:**
>
> - 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 using the *Initial Setup Console* or the *Software Library Administration Console* (available within the Enterprise Manager 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. This saves time and effort, and enables you to install an additional OMS, immediately after the first OMS, and configure it to use the same Software Library location.
> - Once the Software Library is configured, you can view the location details in the *Software Library Administration Console*. To access this console, from the **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**

14. Click **Next**.
15. **Review Port Configuration Details**



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

You can enter an available 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>
  ```

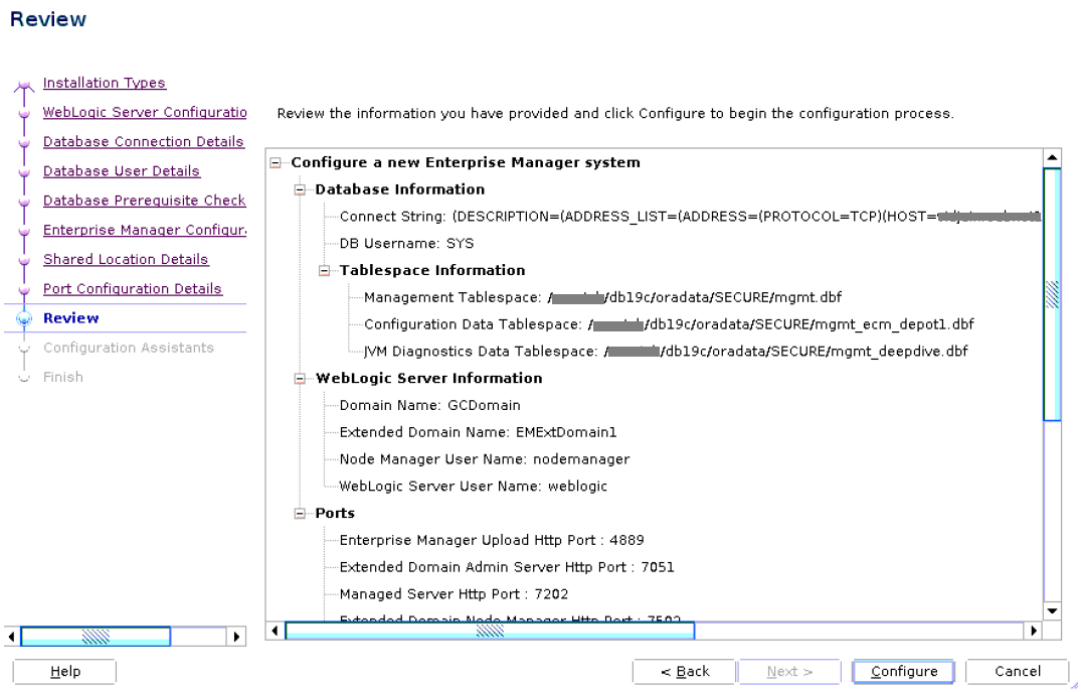
- On Microsoft Windows:

  ```
  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`

16. Click **Next**.
17. **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, click **Configure** to begin the configuration process.

18. **Track the Configuration Progress**

On the Configuration Details screen, view the overall progress (in percentage) of the configuration.

> **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.
> - If you accidentally exit the installer before clicking **Retry,** then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.pl` script from the Oracle home of the OMS host to rerun the configuration assistant in silent mode. For Microsoft Windows platforms, invoke the `runConfig.pl` script.
>
>   ```
>   $<ORACLE_HOME>/oui/bin/runConfig.pl
>   <absolute_path_to_Middleware_home>
>   ```
>
>   If the `runConfig.pl` script fails, then clean up your environment and redo the installation.

19. **End the Installation**

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

> **Note:**
>
> If a Server Load Balancer (SLB) is configured in your environment, and the upload port is locked, then configure the SLB for JVMD Engines, and then secure the OMS.
>
> If an SLB is configured in your environment, but the upload port is unlocked, then decide whether you want to route the JVMD traffic through the SLB. If you do, then configure the SLB for JVMD Engines, and then secure the OMS.
>
> To secure the OMS, run the following command from the `bin` directory of the Oracle home of the OMS host:
>
> ```
> <ORACLE_HOME>/bin/emctl secure oms -host <SLB host>-
> slb_jvmd_http_port <JVMD_SLB_HTTP_Port> -slb_jvmd_https_port
> <JVMD_SLB_HTTPS_Port> -sysman_pwd <system_password> -reg_pwd
> <agent_registration_password>
> ```

Using Advanced Script Options While Configuring the Enterprise Manager Software Using the Install Software Only Method in Graphical Mode

The following are some additional advanced options you can pass while invoking the `ConfigureGC` script (`ConfigureGC.sh` on UNIX/Linux or `ConfigureGC.bat` on Microsoft Windows):

- For Oracle Enterprise Manager 13c and higher, `GCDomain` is the only supported domain name for creating the WebLogic domain. Customized WebLogic domain names are not supported.
- **SSL configuration support**: Starting with Enterprise Manager 13c Release 5 Update 8 (13.5.0.8) or higher, SSL configuration is supported. If the repository database is configured with one-way or two-way SSL authentication, you can configure the Enterprise Manager against the SSL-enabled repository database when configuring the Enterprise Manager software only in graphical mode.
  The graphical configuration installer has multiple steps. During the **Database Connection Details** step, enter the SSL information applicable to your environment. For details, see Configuring the Enterprise Manager Software Only in Graphical Mode .
- 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 `START_AGENT` options, and set them to `true` or `false` depending on what you want to control.

> **Note:**
>
> Ensure that the `START_OMS` and `START_AGENT` options are used even when the installation wizard was invoked to install the software binaries as described in Install Software Only With Plug-ins and Configure Later in Graphical Mode.

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

```
$<ORACLE_HOME>/sysman/install/ConfigureGC.sh START_OMS=true START_AGENT=false
```

To understand the limitations involved with this advanced option, see Limitations with the Advanced Options Supported for Installing an Enterprise Manager System in Silent Mode.

Performing Postconfiguration Tasks After Configuring the Enterprise Manager Software Only in Graphical Mode

Perform the post-install steps as described in Performing Postinstallation Tasks After Installing an Enterprise Manager System chapter from the *Enterprise Manager Basic Installation Guide*.

Install Software Only With Plug-ins and Configure Later in Silent Mode

This section explains how you can install only the software binaries of Enterprise Manager at one point in silent mode, and configure the Enterprise Manager installation at a later point.

SSL Support: You can enable one-way or two-way Secure Sockets Layer (SSL) mode during the Configuring the Enterprise Manager Software Only in Silent Mode step when running the `ConfigureGC` script.

> **Note:**
>
> PKCS12 wallet file format is supported.

Non-SYS User: You can configure Oracle Enterprise Manager with a non-SYS admin user during the Configuring the Enterprise Manager Software Only in Silent Mode step when running the `ConfigureGC` script. Using a non-SYS user allows Enterprise Manager administrators to use another user, an admin user, for these tasks since organizations continue to lock privileges credentials like the SYS database user to perform those activities.

Workflow for Installing Software Only With Plug-ins and Configure Later in Silent Mode

General Worklfow for installing the software binaries of Enterprise Manager with plug-ins first, and then configuring the installation at a later point in graphical mode.

1. Installing the Enterprise Manager Software Only with Plug-ins in Silent Mode
2. Running the Root Script
3. Evaluate Non-SYS User Creation
4. Apply Release Update
5. Configuring the Enterprise Manager Software Only in Silent Mode
6. Performing Postconfiguration Tasks After Configuring the Enterprise Manager Software Only in Silent Mode

Installing the Enterprise Manager Software Only with Plug-ins in Silent Mode

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

> **Note:**
>
> Oracle recommends running 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 the *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 installer and generate the response file you need to use for performing a silent software-only installation.

   ```
   ./em24100_<platform>.bin -getResponseFileTemplates -outputLoc
   <absolute_path_to_a_directory_to_store_the_generated_response_file>
   ```

   > **Note:**
   >
   > The command generates multiple response files. You must use only the **`softwareOnlyWithPlugins_install.rsp`** file for this silent software-only installation.

2. Edit the `softwareOnlyWithPlugins_install.rsp` file and enter appropriate values for the variables described in Table 4-2.
3. Invoke the installer in silent mode and pass the updated response file.

   (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 *Enterprise Manager Basic Installation Guide*.)

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

     ```
     ./em24100_<platform>.bin -silent -responseFile
     <absolute_path_to_the_directory_where_the_generated_and_updated_response_f
     ile_is_stored>/softwareOnlyWithPlugins_install.rsp [-invPtrLoc
     <absolute_path_to_oraInst.loc>]
     ```

   - Otherwise, run the following command:

     ```
     ./em24100_<platform>.bin -silent -responseFile
     <absolute_path_to_the_directory_where_the_generated_and_updated_response_f
     ile_is_stored>/softwareOnlyWithPlugins_install.rsp
     ```

Note:

- To invoke the installation wizard on UNIX platforms, run `em24100_<platform>.bin`. To invoke on Microsoft Windows platforms, run `setup_em24100_win64.exe`.
- The installer requires about 14 GB of hard disk space in the temporary directory. If your temporary directory does not have this space, then pass the `-J-Djava.io.tmpdir` parameter and provide an alternative directory where there is 14 GB of space.

  The directory specified by this parameter will also be used as the location for the Provisioning Advisor Framework (PAF) staging directory, which is used for copying the Software Library entities related to the deployment procedures. The PAF staging directory is used only for provisioning activities — entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.

  For example,

  ```
  ./em24100_linux64.bin -J-Djava.io.tmpdir=/u01/software/em24/stage/
  ```

- For information about the additional, advanced options you can pass while invoking the installer, refer to Advanced Installer Options Supported for Installing an Enterprise Manager System in Silent Mode.

Editing the softwareOnlyWithPlugins_install.rsp Response File for Installing the Enterprise Manager Using the Software Only Method in Silent Mode

Table 4-2 describes what variables you must edit and how you must edit them in the `softwareOnlyWithPlugins_install.rsp` response file for installing the software binaries.

Table 4-2 Editing the softwareOnlyWithPlugins_install.rsp Response File for Installing the Enterprise Manager 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. For example, `"dba"`. **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
INSTALL_UPDATES_SELECTION	String	No	By default, this variable is set to `skip` indicating that the software updates will not be installed during installation. Enter `skip` if you want to skip the software updates. Enter `staged` if you have already downloaded the software updates and you want to install the software updates from a staged location. For example, `INSTALL_UPDATES_SELECTION=skip`

Table 4-2 (Cont.) Editing the softwareOnlyWithPlugins_install.rsp Response File for Installing the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quote Required for Values?	Description
STAGE_LOCATION	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION=staged`) Enter the absolute path of the stage location for the software updates.
MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION=download`) Enter the username of the My Oracle Support account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES` and set `INSTALL_UPDATES_SELECTION="download"`.
MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION=download`) Enter the password of the My Oracle Support user account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES` and set `INSTALL_UPDATES_SELECTION="download"`.
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. For example, `"/u01/oracle/oraInventory"`. **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

Table 4-2 (Cont.) Editing the softwareOnlyWithPlugins_install.rsp Response File for Installing the Enterprise Manager 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 and Java Development Kit (JDK). Ensure that the middleware location has *write* permission. For example, "`/u01/software/em24/middleware`". **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:\sw\em24\middlwhome` containing only 22 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.
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. For example, "`/u01/software/em24/agentbasedir`". Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home. **Note:** *(Only for Microsoft Windows)* Ensure that the number of characters in the agent base directory path does not exceed 25 characters. For example, the agent base directory path `C:\sw\em24\agntbsedir` containing only 22 characters is acceptable. However, `C:\Oracle\ManagementAgent\em24\new` containing more than 25 characters is not acceptable.

Table 4-2 (Cont.) Editing the softwareOnlyWithPlugins_install.rsp Response File for Installing the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quote Required for Values?	Description
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. 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. If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host.
PLUGIN_SELECTION={}	String List	Yes	Enter the list of new plug-ins to be deployed during installation. It contains a list of strings and each string is the PLUGIN_ID of that plugin. For example, `PLUGIN_SELECTION={'oracle.sysman.empa'}`
b_upgrade	Boolean	No	For install software only, set it to `false` `b_upgrade=false`
EM_INSTALL_TYPE	String	No	For install software only, set it to `NOSEED` `EM_INSTALL_TYPE=NOSEED`
CONFIGURATION_TYPE	String	No	For install software only, set it to `LATER` `CONFIGURATION_TYPE=LATER`

Running the Root Script

(For UNIX Only) After you install the software binaries of Enterprise Manager, 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:

  `$<ORACLE_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 $<ORACLE_HOME>/allroot.sh`

Evaluate Non-SYS User Creation

Review the creation and usage of a non-SYS user and evaluate if it fits the security needs of your organization.

Since security is a growing concern, Oracle provides the option to perform the installation, configuration and patching of the OMS using a non-privileged administrator user, also known as non-SYS user.

After the user is created, the non-SYS database user performs the Enterprise Manager installation, configuration and patching process, eliminating the requirement to use the SYS user for those operations.

> **Note:**
>
> Once you create and start using the non-SYS admin user for the installation, configuration and patching of the OMS, you cannot switch back to use SYS as an admin user to perform any of those operations.

Using Non-SYS user

- Less-privileged database administrator user. Also known as admin user.
- Performs Enterprise Manager installation, configuration and patching operations. (The SYS database user is no longer required during the installation, configuration and patching).
- User is created during the execution of the `ConfigureGC` script (Enterprise Manager configuration).
- Naming convention: `SYSMAN_` is the username prefix.

Using SYS user (Default option)

- Privileged database administrator user.
- Performs the Enterprise Manager installation, configuration and patching operations.

You are prompted to make the selection of creating and performing the installation using SYS or non-SYS user during the **Database User Details** step from Configuring the Enterprise Manager Software Only in Graphical Mode .

Apply Release Update

If there's a Release Update available, Oracle recommends to apply the latest Release Update after installing the Enterprise Manager software binaries.

A Release Update, previously known as Bundle Patch, is an official Oracle patch that can be applied on top of Enterprise Manager 24ai Release 1 main release on an Oracle Home using the `omspatcher apply -bitonly` command. For more information about patching and the `omspatcher` utility, see Patching Oracle Management Service and the Repository in the *Enterprise Manager Administrator's Guide*.

> **Note:**
>
> You can patch the OMS using a non-SYS user (admin user).
> Oracle provides the option to perform the configuration and patching process using a non-privileged user, eliminating the requirement to use the SYS database user and password for the patching process. For information, see Evaluate Non-SYS User Creation.

To apply the Release Update, do the following:

- Obtain the latest Release Update by logging in to My Oracle Support: https://support.oracle.com/.
- Review the `Readme` file that comes with the Release Update.
- Use the latest version of the `omspatcher` as suggested in the Release Update `Readme` file, and keep a backup of the previous `omspatcher`.
- **Non-SYS user**: If you decide to create and use non-SYS user in your environment, you must confirm that the non-SYS user has already been created before applying the release update. For information about creating the user, see Evaluate Non-SYS User Creation.

To apply a Release Update, perform the following steps:

1. Before proceeding, ensure that `$ORACLE_HOME/OMSPatcher` directory is included in the path since `omspatcher` is located in that directory.
2. Execute omspatcher in bitonly mode for the Release Update.

   ```
   omspatcher apply -bitonly
   ```

3. Run `omspatcher lspatches` command to list all the sub-patches applied in Step 1.

   Syntax: omspatcher lspatches | grep "<RU Number / Id >"

Configuring the Enterprise Manager Software Only in Silent Mode

> **Note:**
>
> Starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher, you can configure and patch the OMS using the SYS admin user (default option) or a different user, known as a non-SYS admin user. Oracle provides the option to perform the configuration and patching process using a non-privileged user, eliminating the requirement to use the SYS database user and password for the configuration and patching process. Before proceeding, ensure to review Evaluate Non-SYS User Creation.

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

1. Access the `new_install.rsp` file that you generated in Step (1) of Installing the Enterprise Manager Software Only with Plug-ins in Silent Mode. Edit that file and enter appropriate values for the variables described in Table 4-3.
2. Configure the software binaries by invoking the `ConfigureGC.sh` script (or `ConfigureGC.bat` on Microsoft Windows) passing the response file you edited in the previous step:

   ```
   $<ORACLE_HOME>/sysman/install/ConfigureGC.sh -silent -responseFile
   <absolute_path_to_the_directory_where_the_generated_and_updated_response_file_
   is_stored>/new_install.rsp [-invPtrLoc <absolute_path_to_oraInst.loc>]
   ```

   Optional Parameter:

   - The `-invPtrLoc` parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

     For more information about additional advanced options you can pass while invoking the `ConfigureGC.sh` script, see Using Advanced Script Options While Configuring the Enterprise Manager Software Using the Install Software Only Method in Silent Mode.

> **Note:**
>
> - While installing the software binaries as described in Installing the Enterprise Manager Software Only with Plug-ins in Silent Mode, if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
> - 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.

Server Load Balancer Considerations:

If a Server Load Balancer (SLB) is configured in your environment, and the upload port is locked, then configure the SLB for JVMD Engines, and then secure the OMS.

If an SLB is configured in your environment, but the upload port is unlocked, then decide whether you want to route the JVMD traffic through the SLB. If you do, then configure the SLB for JVMD Engines, and then secure the OMS.

To secure the OMS, run the following command from the `bin` directory of the Oracle home of the OMS host:

```
<ORACLE_HOME>/bin/emctl secure oms -host <SLB host>-slb_jvmd_http_port
<JVMD_SLB_HTTP_Port> -slb_jvmd_https_port <JVMD_SLB_HTTPS_Port> -sysman_pwd
<system_password> -reg_pwd <agent_registration_password>
```

```
<ORACLE_HOME>/bin/emctl secure oms -host <SLB host>-slb_jvmd_http_port
<JVMD_SLB_HTTP_Port> -slb_jvmd_https_port <JVMD_SLB_HTTPS_Port> -sysman_pwd
<system_password> -reg_pwd <agent_registration_password>
```

Other Considerations:

- 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 minimum version of the packages mentioned in the *Enterprise Manager Basic Installation Guide*. To understand the logic the installer uses to verify these packages, see the *Enterprise Manager 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 *Enterprise Manager 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.

Editing the new_install.rsp Response File for Configuring the Enterprise Manager 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.

> **Note:**
>
> Starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher, you can configure and patch the OMS using a non-SYS user (admin user). Oracle provides the option to perform the configuration and patching process using a non-privileged user, eliminating the requirement to use the SYS database user and password for the patching process. Before proceeding, ensure to review Evaluate Non-SYS User Creation.

Table 4-3 Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

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. For example, `"dba"` **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
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. For example, `"/u01/oracle/oraInventory"`. **Note:** This parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.
INSTALL_UPDATES_SELECTION	String	Yes	By default, this variable is set to `skip` indicating that the software updates will not be installed during installation. Enter `skip` if you want to skip the software updates. Enter `staged` if you have already downloaded the software updates and you want to install the software updates from a staged location.
STAGE_LOCATION	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION=staged`) Enter the absolute path of the stage location for the software updates.

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION="download"`) Enter the username of the My Oracle Support user account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES`, and set `INSTALL_UPDATES_SELECTION="download"`.
MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES	String	Yes	(Required only if `INSTALL_UPDATES_SELECTION="download"`) Enter the password of the My Oracle Support user account to download the updates during the installation. If you want to download the updates during the installation, make sure you provide `MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES` and `MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES`, and set `INSTALL_UPDATES_SELECTION="download"`.
PROXY_USER	String	Yes	Enter the user name that can be used to access the proxy server.
PROXY_PWD	String	Yes	Enter the password that can be used to access the proxy server.
PROXY_HOST	String	Yes	Enter the name of the proxy host.
PROXY_PORT	String	Yes	Enter the port used by the proxy server.
ORACLE_MIDDLEWARE_HOME_LOCATION	String	Yes	Enter the location where you want the installer to install Oracle WebLogic Server 12*c* Release 2 (12.2.1.4.0) and Java Development Kit (JDK) 1.8.0_431. Ensure that the middleware location has *write* permission. Note that the middleware location is essentially the one and only Oracle home in 24ai release. For example, `"/u01/software/em24/middleware"` **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:\sw\em24\middlwhome` containing only 22 characters is acceptable. However, `C:\OracleSoftware\OracleMiddleware\OracleEnterpriseManager\OMS\newrelease\oms` containing more than 25 characters is not acceptable for Microsoft Windows platforms.

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
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. 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. If you do not mention the host name, the installation wizard will proceed further, honoring the host name it automatically detects for that host.
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. For example, `"/u01/software/em24/agentbasedir"`. Ensure that this location is empty and has write permission. Also ensure that it is always maintained outside the Oracle Middleware home. **Note:** *(Only for Microsoft Windows)* Ensure that the number of characters in the agent base directory path does not exceed 25 characters. For example, the agent base directory path `C:\sw\em24\agntbsedir` containing only 22 characters is acceptable. However, `C:\Oracle\ManagementAgent\em24\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 leave the field 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. 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. 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 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

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. For more information about this location, see What Is an Oracle Management Service Instance Base Location?. **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 Performing Postconfiguration Tasks After Configuring the Enterprise Manager Software Only in Silent Mode.
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`. 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 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	(Required only if `CONFIGURE_ORACLE_SOFTWARE_LIBRARY=TRUE`) 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 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. For example, `"example.com"`. 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. 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. 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. However, if you want to update the connect string with other nodes of the cluster, then after the installation, run the following command: `$<ORACLE_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` If your Oracle RAC database is configured with Single Client Access Name (SCAN) listener, then you can enter a connection string using the SCAN listener. **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 SYSMAN122140_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. For example, `"1521"`.
SERVICENAME_OR_SID	String	Yes	Enter the service name or the system ID (SID) of the existing database. For example, `"orcl"`. If you are providing the details of a pluggable database (PDB), then use the full service name instead of the alias. For example, pdb.example.com. If you are providing the details of a lone-pluggable database (Lone-PDB), then use the full service name. For example, pdb.example.com. If you are providing the details of a non-container database (Non-CDB), then use the SID.
SYS_PASSWORD	String	Yes	*(Required only if using SYS as the admin user)* Enter the password of the SYS user.

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
dbUser	String	Yes	Enter the non-SYS (admin) username. If using the default option, enter 'SYS' as a user. The database user name that creates the repository schema during the install process. This is the non-SYS database user (a database admin user other than the SYS user). Naming convention: User name should start with the `SYSMAN_` prefix. For example: `dbUser=SYSMAN_ADMIN` If the user doesn't exist, the install process creates the new user in the Repository database. This parameter is only required if `INSTALL_WITH_NON_SYS_USER = true`
dbPassword	String	Yes	Enter the non-SYS (admin) user password. If using the default option, enter the password of the 'SYS' user. The password of the database user that creates the repository schema. This is the non-SYS database user password. This parameter is only required if `INSTALL_WITH_NON_SYS_USER = true`
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. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value. **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 SYSMAN122140_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 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. • **SMALL,** to monitor up to 999 targets, with up to 99 Management Agents and up to 10 concurrent user sessions • **MEDIUM,** to monitor about 1000 to 9999 targets, with about 100 to 999 Management Agents and about 10 to 24 concurrent user sessions • **LARGE,** to monitor 10,000 or more targets, with 1000 or more Management Agents, and with about 25 to 50 concurrent user sessions. For example, `"MEDIUM"`. 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 same deployment size you selected on the 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: • 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 Basic Installation Guide*. • 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 Basic Installation Guide Enterprise Manager Basic Installation Guide*.
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. For example: • If the database is on a file system, then the path must look like `"/u01/oracle/prod/oradata/mgmt.dbf"`. • 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). • 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. Enterprise Manager 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.

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
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. For example, `"/home/john/oradata/mgmt_ecm_depot1.dbf"`. Enterprise Manager 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 for JVM Diagnostics data tablespace (`mgmt_deepdive.dbf`) can be stored. Ensure that the specified path leads up to the file name. For example, `"/home/john/oradata/mgmt_deepdive.dbf"`. Enterprise Manager requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).
EMPREREQ_AUTO_CORRECTION=false	Boolean	No	It specifies whether prereqs can be auto corrected.
INSTALL_WITH_NON_SYS_USER	Boolean	No	It specifies if the install is being performed using a database user different than SYS. This user is also known as non-SYS user. For example: `INSTALL_WITH_NON_SYS_USER=true` If this parameter is set to `true`, you also need to provide the `dbUser` and `dbPassword` parameters (the user name and password of the non-SYS user).
Is_oneWaySSL	Boolean	No	Applicable for one-way SSL configuration. Set it to `true` if the repository database is configured with one-way SSL. Example: `Is_oneWaySSL=true` If `Is_oneWaySSL=true` is set, `TRUSTSTORE_LOCATION` and `TRUSTSTORE_PASSWORD` parameters are required.
TRUSTSTORE_LOCATION	String	Yes	(Required only if `Is_oneWaySSL=true` or `Is_twoWaySSL=true`) Applicable for one-way SSL configuration. Enter the absolute location of the Truststore Wallet file.
TRUSTSTORE_PASSWORD	String	Yes	(Required only if `Is_oneWaySSL=true` or `Is_twoWaySSL=true`) Applicable for one-way SSL configuration. Enter the the TrustStore Wallet password.
Is_twoWaySSL	Boolean	No	Applicable for two-way SSL configuration. Set it to `true` if the repository database is configured with two-way SSL. Example: `Is_twoWaySSL=true` If `Is_twoWaySSL=true` is set, `TRUSTSTORE_LOCATION`, `TRUSTSTORE_PASSWORD`, `KEYSTORE_LOCATION` and `KEYSTORE_PASSWORD` parameters are required.
KEYSTORE_LOCATION	String	Yes	(Required only if `Is_twoWaySSL=true`) Enter the location of the keystore (location where the SSL key will get stored).

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
KEYSTORE_PASSWORD	String	Yes	(Required only if `Is_twoWaySSL=true`) Enter the password of the keystore.
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 What Ports Are Used for Installation? are honored. If you want to accept the default ports, then leave this field blank. 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			By default, mandatory plug-ins such as Oracle Database Plug-in, Oracle Fusion Middleware Plug-in, and Oracle Exadata Plug-in, Oracle Cloud Framework Plug-in, and Oracle System Infrastructure Plug-in are automatically installed with the Enterprise Manager system.
			In addition to the default ones, if you want to deploy any addition plug-in, then list those plug-in names in a comma-separated list. Ensure that the plug-in names are in double quotes.
			If you want to deploy a deprecated plug-in that is supported only in the current release, but it's not in any of the future releases, then evaluate your selection and decide whether or not you want to proceed with the deployment of such plug-ins.
			For example,
			`PLUGIN_SELECTION={"oracle.sysman.empa"}`
			If you want to install some plug-ins that are not in the software kit (DVD, downloaded software), then do the following:
			1. Manually download the required plug-ins from `Plug-in Update`.
			In addition, plug-ins produced by partners or customers are available on the `Enterprise Manager Extensibility Exchange`.
			2. Invoke the installer with the following option and pass the location where the additional plug-ins have been downloaded:
			`./em24100_<platform>.bin PLUGIN_LOCATION=<absolute_path_to_plugin_software_location>`

b_upgrade	Boolean	No	For this case, set it to `false` `b_upgrade=false`
EM_INSTALL_TYPE	String	No	For this case, set it to `NOSEED` `EM_INSTALL_TYPE=NOSEED`

Table 4-3 (Cont.) Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode

Parameter	Data Type	Double Quotes Required for Value?	Description
CONFIGURATION_TYPE	String	No	For this case, set it to `ADVANCED` `CONFIGURATION_TYPE=ADVANCED`

Using Advanced Script Options While Configuring the Enterprise Manager Software Using the Install Software Only Method in Silent Mode

The following are some additional advanced options you can pass while invoking the `ConfigureGC` script (`ConfigureGC.sh` on UNIX/Linux or `ConfigureGC.bat` on Microsoft Windows):

- For Oracle Enterprise Manager 13c and later, `GCDomain` is the only supported domain name for creating the WebLogic domain. Customized WebLogic domain names are not supported.
- **SSL configuration support**: Starting with Enterprise Manager 13c Release 5 Update 8 (13.5.0.8) or higher, SSL configuration is supported. If the repository database is configured with one-way or two-way SSL authentication, you can configure the Enterprise Manager against the SSL-enabled repository database when configuring the Enterprise Manager software only in silent mode.

  > **Note:**
  >
  > PKCS12 is the wallet file format supported for SSL configuration.

  To enable SSL configuration in Enterprise Manager using configuring the Enterprise Manager software only in silent mode, prepare a response file and then run the `ConfigureGC` script using a response file: Review the SSL configuration, edit the `new_install.rsp` response file and update the appropriate SSL parameters and values applicable to your environment. The SSL parameters available are:

  - `Is_oneWaySSL`
  - `Is_twoWaySSL`
  - `TRUSTSTORE_LOCATION`
  - `TRUSTSTORE_PASSWORD`
  - `KEYSTORE_LOCATION`
  - `KEYSTORE_PASSWORD`

  For more details about the SSL parameters from the response file, see Editing the new_install.rsp Response File for Configuring the Enterprise Manager Software Using the Software Only Method in Silent Mode.
- 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 `START_AGENT` options, and set them to `true` or `false` depending on what you want to control.

> **Note:**
>
> Ensure that the `START_OMS` and `START_AGENT` options are used even when the installation wizard was invoked to install the software binaries as described inInstall Software Only With Plug-ins and Configure Later in Graphical Mode.

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

```
$<ORACLE_HOME>/sysman/install/ConfigureGC.sh START_OMS=true START_AGENT=false
```

To understand the limitations involved with this advanced option, see Limitations with the Advanced Options Supported for Installing an Enterprise Manager System in Silent Mode.

Performing Postconfiguration Tasks After Configuring the Enterprise Manager Software Only in Silent Mode

Perform the post-install steps as described in Performing Postinstallation Tasks After Installing an Enterprise Manager System section that is available in the *Enterprise Manager Basic Installation Guide*.

Part III

Installing Additional Oracle Management Services

This part contains the following chapters:

- Installing Additional Oracle Management Services in Silent Mode

5

Installing Additional Oracle Management Services in Silent Mode

Oracle recommends that you install additional Oracle Management Services (OMS) in your environment to ensure high availability of your Enterprise Manager system. This chapter describes how you can install an additional OMS in silent mode. In particular, this chapter covers the following:

About Installing Additional Oracle Management Services in Silent Mode

Oracle recommends that you install additional OMS instances in your environment to ensure high availability of your Enterprise Manager system. To install an additional OMS, you can use the Add Management Service deployment procedure. The Add Management Service deployment procedure offers a GUI-rich, interactive way of installing an additional OMS. For instructions, see *Adding Additional Oracle Management Services* in the *Oracle Enterprise Manager 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 you can install in silent, non-interactive mode. Before you start the silent installation, meet all the prerequisites listed in *Adding Additional Oracle Management Services* in the *Oracle Enterprise Manager Basic Installation Guide.*

> **WARNING:**
>
> Do not install Enterprise Manager 24ai on servers of SPARC series: T1000, T2000, T5xx0, and T3-*. For more information, see My Oracle Support note 1590556.1.

Installing Additional Oracle Management Services in Silent Mode

To install an additional OMS in silent mode, follow these steps:

1. If Oracle Software Library (Software Library) is configured on the main OMS, which comes with Enterprise Manager, then do the following:
   - **On Unix Platforms:**
     - Ensure that the 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 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 Install Software Only With Plug-ins and Configure Later in Graphical Mode

Install Software Only With Plug-ins and Configure Later in Graphical Mode.

> **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.
> - If the installation of an additional OMS is happening after the Primary OMS upgrade and the installation is by using the installation software only and configure later in silent mode method, then do the following:
>
> a. Make sure during the software only installation to select all the same plug-ins which were installed on the Primary OMS.
>
> b. If there are some plug-ins which got migrated during the Primary OMS upgrade and they are not available in Enterprise Manager 24ai, make sure that after adding the OMS using the software only install method to run the `plugins.sh` script by passing the old opar location. Therefore that additional OMS home will have the same plug-ins as the Primary OMS.

3. Deploy the plug-ins.

   a. Graphical Mode
   Invoke the `PluginInstall.sh` script from the following location:

   ```
   <ORACLE_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.

   b. Silent Mode

Invoke the `PluginInstall.sh` script from the following location:

```
<ORACLE_HOME>/sysman/install/PluginInstall.sh -silent
PLUGIN_SELECTION="{PLUGIN_ID1,PLUGIN_ID2}"
```

For example:

```
/u01/software/em/oraclehome/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:

  a. 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}}
  ```

  b. 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:

  a. Manually download the required plug-ins from http://www.oracle.com/technetwork/oem/extensions/index.html.
  In addition, if you want to download any partner or customer plug-ins, then download from https://apex.oracle.com/pls/apex/f?p=53891:1.

  b. Invoke the script and pass the location where the additional plug-ins have been downloaded.

  – Graphical Mode:

  ```
  <ORACLE_HOME>/sysman/install/PluginInstall.sh
  PLUGIN_LOCATION=<absolute_path_to_plugin_software_locatio
  n>
  ```

  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.

  – Silent Mode:

  ```
  {{<ORACLE_HOME>/sysman/install/PluginInstall.sh  -silent
  PLUGIN_SELECTION="{PLUGIN_ID1,PLUGIN_ID2}"
  PLUGIN_LOCATION=<absolute_path_to_plugin_software_locatio
  n>}}
  ```

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:

```
mw_home/OMSPatcher/omspatcher 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/OMSPatcher/omspatcher apply <patch location> -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 host, and pass the location where the configuration details can be exported as a file.

   ```
   $<ORACLE_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. *(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 agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh AGENT_BASE_DIR=<agent_base_dir>
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.

9. Deploy the required plug-ins on the Management Agent.

   For information about deploying plug-ins, see *Managing Plug-Ins* in the *Oracle Enterprise Manager Administrator's Guide.*

10. Recover the configuration details onto the additional OMS. To do so, run the following command from the Oracle home of the additional OMS host:

    ```
    $<ORACLE_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>]
    ```

    For example,

    ```
    /u01/software/em24/oraclehome2/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_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.

11. Import the trusted certificate on the additional OMS host, where you configured the Management Agent as described in Step (9). When prompted for a password, enter `welcome`.

    ```
    $<AGENT_HOME>/bin/emctl secure add_trust_cert_to_jks
    ```

12. Review and perform the applicable postinstallation steps. See *Performing Postinstallation Tasks After Adding an Additional Oracle Management Service* in the *Oracle Enterprise Manager 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 Enterprise Manager 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 refreshes the WebLogic Domain and discovers the second managed server on the additional OMS host.

    For information about discovering the other targets and adding targets, see *Overview of Discovering and Adding Targets* in the *Oracle Enterprise Manager Administrator's Guide.*

    For configuring the shared Oracle Software Library location and the Server Load Balancer, see *Configuring a Software Library* in the *Oracle Enterprise Manager Administrator's Guide.*

14. Discover Coherence Cache of EMGC_GC Domain.

    When EMGC_GC Domain target is auto discovered, Coherence Cache targets from EMGC_GC Domain will not get discovered. If you want to discover it, you need to do the following steps:

    a. In the Enterprise Manager Console, from the Targets menu, select **All Targets**.
    b. On **All Targets** page, search and click **/EMGC_GCDomain/GCDomain/**.
    c. On the **EMGC_GCDomain** home page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.
    d. On the **Refresh WebLogic Domain** page, click **Add / Update Targets**.
    e. Click **Close** from the Confirmation dialog.
    f. Expand the **Advanced** node from the **Refresh WebLogic Domain: Assign Agents** page.
    g. Select **Oracle Coherence Cache** from the **Selected Target Types** box under the **Disabled Target Types** section and click **<** to proceed.
    h. Click first **Refresh Targets** and then **Add Targets** to complete the discovery.

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:

- Installing Oracle Management Agent in Silent Mode
- Cloning Oracle Management Agents
- Installing Shared Agents
- Installing the Oracle Management Agent Software Now and Configuring It Later

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:

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 x86-64 platform.
> - For Enterprise Manager 24ai Release 1 (24.1.0.x), installing a Management Agent by downloading the Management Agent `.rpm` file from *Oracle Software Downloads* site is not supported.

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
    |_____agent_24.1.0.0.0
          |_____sbin
          |_____OPatch
          |_____agent.rsp
          |_____bin
          |_____cfgtoollogs
          |_____config
          |_____install
          |_____instalclient
          |_____.
          |_____.
          |_____.
    |_____agent_inst
    |_____agentInstall.rsp
    |_____agentimage.properties
```

> **Note:**
>
> - You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For instructions, see Redirecting Oracle Management Agent to Another Oracle Management Service.
>
> 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 24.1.0.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 Response File Parameters for Installing a Management Agent in Silent Mode Using the agentDeploy Script.

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 *Acquiring the Management Agent Software in Online Mode* in the *Oracle Enterprise Manager Basic Installation Guide*.
- Starting with Enterprise Manager 13*c* Release 3, 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.

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 *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager 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*. To access the Enterprise Manager certification matrix, follow the steps outlined in *Accessing the Enterprise Manager Certification Matrix* in the *Oracle Enterprise Manager Basic Installation Guide.*
File System Requirements	Ensure that the file system mounted on the destination host does not permit buffered writes.

Table 6-1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description

File Descriptor Requirements	• Ensure that the maximum user process limit is set to 13312 or greater.
	To verify the current value set, run the following command:
	`ulimit -u`
	If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.
	• Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.
	To verify the current value set, run the following commands:
	For Soft Limit:
	`/bin/sh -c "ulimit -n"`
	For Hard Limit:
	`/bin/sh -c "ulimit -Hn"`
	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:
	`<UID> soft nofile 4096`
	`<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 *Package, Kernel Parameter, and Library Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.* 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: `rpm -qa | grep rpm-build`
CURL Utility Requirements (For installing using the `AgentPull` script only)	Ensure that you install the CURL utility on the destination host. You can download the CURL utility from the following URL: `http://curl.haxx.se/dlwiz/?type=bin` **Note:** For destination hosts running on Microsoft Windows, Oracle recommends that you install CURL in `c:\`.
ZIP and UNZIP Utility Requirements	Ensure that the ZIP and the UNZIP utilities are present on the destination host. The ZIP utility must be of version 3.0 2008 build or higher. 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. For more information, see the chapter on creating operating system groups and users in the *Creating Operating System Groups and Users for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.* **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: `172.16.0.0 example.com mypc` *(Only for Microsoft Windows)* Ensure that the entry for local host in the `etc/hosts` file is always against 127.0.0.1 and against any other address.

Table 6-1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description

Time Zone Requirements	Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:
	`echo $TZ`
	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:
	• For Korn shell:
	`TZ=<value>`
	`export TZ`
	• For Bourne shell or Bash shell:
	`export TZ=<value>`
	• For C shell:
	`setenv TZ <value>`
	For example, in the Bash shell, run the following command to set the time zone to America/New_York:
	`export TZ='America/New_York'`
	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.
	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).
	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 After Installing a Management Agent in Silent Mode.

PATH Environment Variable Requirements (For installing using the `AgentPull` script only)	Ensure that the location of `zip` and `unzip` is part of the `PATH` environment variable. 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 *Validating Command Locations* in the *Oracle Enterprise Manager 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 What Default Ports Are Used for Enterprise Manager Installation? are free.
Temporary Directory Space Requirements	Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied. 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 (For installing using the `.rpm` file only)	Ensure that the `/var/tmp` directory has at least 700 MB of free space.

Table 6-1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
/usr/lib/oracle Requirements (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: • The agent base directory is empty and has at least 1 GB of free space. • The directory name does not contain any spaces. • 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. 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. • If the agent base directory is mounted, it is mounted with the `setuid` option turned on.
Agent Instance Home Requirements (For installing using the `agentDeploy` script only)	Ensure that the agent instance home location you specify in the response file is empty.
Permission Requirements	• Ensure that you have *write* permission in the agent instance home. • 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. 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. • 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 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 6-7. Note that these parameters are supported only on UNIX platforms, and not on Microsoft Windows platforms.

Table 6-1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Agent User Account Permissions and Rights (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: • Act as part of the operating system. • Adjust memory quotas for a process. • Replace process level token. • Log on as a batch job. To verify whether the agent user has these rights, follow these steps: 1. Launch the Local Security Policy. 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**. 2. In the Local Security Policy window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**.
Permissions for cmd.exe (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. For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site: `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`.

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
- Contents of the Downloaded Management Agent Software

> **Note:**
>
> 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 `ORACLE_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`

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 a Management Agent Using the AgentPull Script
3. Installing a Management Agent Using an Agent Gold Image, Using the AgentPull Script

> **Note:**
>
> **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.**

Acquiring the Management Agent Software

1. If the destination host runs on UNIX, access the following URL from the host, and save the file as `AgentPull.sh` (`AgentPull.bat` for Microsoft Windows) to a temporary directory. For example, `/tmp` (`c:\temp` for Microsoft Windows).

   ```
   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
   ```

   > **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. To do so, run the `AgentPull.sh` script (`AgentPull.bat` for Microsoft Windows) passing the `-showPlatforms` option.

   ```
   <absolute_path_to_AgentPull.sh> -showPlatforms
   ```

   The following is a sample output of the command:

   ```
   Platforms Version
   Linux x86-64 24.1.0.0.0
   Microsoft Windows x64 (64-bit) 24.1.0.0.0
   IBM AIX on POWER Systems (64-bit) 24.1.0.0.0
   ```

   If the output lists the platform on which you want to install the Management Agent, then proceed to Installing a Management Agent Using the AgentPull Script. 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 Basic Installation Guide.*

Installing a 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 6-3. 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 for Unix and `AgentPull.bat` for Microsoft Windows specifying the `AGENT_BASE_DIR` and RSPFILE_LOC parameters:

   ```
   AgentPull.sh LOGIN_USER=<value> LOGIN_PASSWORD=<value> CURL_PATH=<value>
   PLATFORM=<value> [VERSION=<value> AGENT_BASE_DIR=<value> RSPFILE_LOC=<value>
   AGENT_REGISTRATION_PASSWORD=<value> -download_only -showPlatforms -
   ignoreDiscoveryPlugin]
   ```

   ```
   AgentPull.bat AGENT_BASE_DIR=<value> RSPFILE_LOC=<value> CURL_PATH=<value>
   [AGENT_REGISTRATION_PASSWORD=<value> VERSION=<value> -download_only -
   showPlatforms -ignoreDiscoveryPlugin -help]
   ```

   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 6-6.

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 Manual Management Agent Installation Logs.

Installing a Management Agent Using an Agent Gold Image, Using the AgentPull Script

To install a Management Agent using the `AgentPull` script, follow these steps:

1. Meeting the Prerequisites for Installing a Management Agent Using an Agent Gold Image, Using the AgentPull Script
2. Installing a Management Agent Using an Agent Gold Image Using the AgentPull Script

Meeting the Prerequisites for Installing a Management Agent Using an Agent Gold Image, Using the AgentPull Script

1. Ensure that there is at least one standalone 24ai Management Agent installed in your environment.
2. Create an Agent Gold Image. See Creating an Agent Gold Image.
3. Create an Agent Gold Image version. See Creating an Agent Gold Image Version.
4. Set a particular Agent Gold Image version as the current version that can be used for deployment. Setting a Particular Agent Gold Image Version as the Current Version.
5. To acquire the Management Agent software, follow the instructions outlined in Acquiring the Management Agent Software.

Installing a Management Agent Using an Agent Gold Image Using the AgentPull Script

To install a Management Agent using an Agent Gold Image, using the AgentPull script, follow these steps:

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 6-3. 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) in the following way. Table 6-2 describes the parameters passed to this command.

```
<absolute_path_to_AgentPull.sh> LOGIN_USER=<username>
LOGIN_PASSWORD=<password> CURL_PATH=/usr/curl VERSION_NAME=<value>|
IMAGE_NAME=<value> [ AGENT_BASE_DIR=<value> RSPFILE_LOC=<value>
AGENT_REGISTRATION_PASSWORD=<password> -download_only -showGoldImages -
showGoldImageVersions -ignoreAuthentication]
```

For example, the following command downloads the latest revision of the Agent Gold Image available in the production system, and uses it to deploy the Management Agent:

```
AgentPull.sh LOGIN_USER=username LOGIN_PASSWORD=password CURL_PATH=/usr/curl
IMAGE_NAME=DB_MONITORING AGENT_BASE_DIR=/tmp/agentpull
```

Table 6-2 Parameters Passed to the AgentPull.sh Script While Installing a Management Agent Using an Agent Gold Image

Parameter	Description
`LOGIN_USER`	Enterprise Manager Console login user name.
`CURL_PATH`	Absolute path to the curl software.
`LOGIN_PASSWORD`	Enterprise Manager Console login password.
`VERSION_NAME`	Agent Gold Image version name to be used for deployment.
`IMAGE_NAME`	Agent Gold Image name from which the Agent Gold Image version should be used for deployment.
`AGENT_BASE_DIR`	Directory where the Agent Gold Image should be downloaded and where the Management Agent should be installed.
`AGENT_REGISTRATION_PASSWORD`	Agent registration password to secure the Management Agent.
`RSPFILE_LOC`	Absolute path to the response file location.
`-download_only`	Downloads the Agent Gold Image, but does not deploy the Management Agent using that image.
`-showGoldImages`	Lists the Agent Gold Images.
`-showGoldImageVersions IMAGE_NAME=<value>`	Lists the Agent Gold Image versions available for a particular Agent Gold Image.
`-ignoreAuthentication`	Bypasses the Enterprise Manager credentials.

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 Manual Management Agent Installation Logs.

If the source Management Agent was installed using the Add Host Targets Wizard, ensure that you specify the `START_AGENT=true` and the `b_secureAgent=true` parameters while invoking the deployment script.

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

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.**

   a. 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, see *EM CLI Overview and Concepts* in the *Oracle Enterprise Manager Command Line Interface Guide.*

   b. 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.

   c. Synchronize EM CLI:

   ```
   <emcli_install_location>/emcli sync
   ```

   d. 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 = 24.1.0.0.0
   Platform Name = Linux x86-64
   ----------------------------------------------
   Version = 24.1.0.0.0
   Platform Name = Oracle Solaris on x86-64 (64-bit)
   ----------------------------------------------
   Version = 24.1.0.0.0
   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 *Acquiring the Management Agent Software in Online Mode* in the *Oracle Enterprise Manager Basic Installation Guide.*

e. Download the Management Agent software from Software Library to a temporary directory on the destination host. 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 `24.1.0.0.0_AgentCore_226.zip`. For information on the contents of this core software, see Contents of the Downloaded Management Agent Software.

```
<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=24.1.0.0.0
```

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.

> **Note:**
>
> 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 meet the following requirements:
>
> - Ensure the ZIP utility is of version 3.0 2008 build or higher, and the UNZIP utility is of version 6.0 or higher.
> - Set the `ZIP_LOC` environment variable to the subdirectory where the ZIP utility is present. For example, if the ZIP utility is present in `/usr/bin/zip`, then set `ZIP_LOC=usr/bin/zip`.
> - Set the `UNZIP_LOC=usr/bin/unzip` environment variable to the parent directory of the subdirectory where the UNZIP utility is present. For example, if the UNZIP utility is present in the subdirectory `/usr/bin/unzip`, then set `UNZIP_LOC=usr/bin/`, where `usr/bin` is the parent directory.
>
> Similarly, 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 meet the following requirements:
>
> - Ensure the ZIP utility is of version 3.0 2008 build or higher, and the UNZIP utility is of version 6.0 or higher.
> - Set the `ZIP_LOC` environment variable to `$OMS_HOME/bin/zip`, that is, the subdirectory where the ZIP utility is present on the OMS host.
> - Set the `UNZIP_LOC=<ORACLE_HOME>/bin/unzip` environment variable to `<ORACLE_HOME>/bin/`, that is, the parent directory of the subdirectory where the UNZIP utility is present in the Oracle home of the OMS host.

2. **Installing the Management Agent Using the agentDeploy Script.**

   a. 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/24.1.0.0.0_AgentCore_226.zip -d /tmp/agtImg
   ```

   b. Edit the response file `agent.rsp` as described in Table 6-4.

   ```
   <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`.

   c. 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/agent24 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=/u01/software/em24/
  agentbasedir 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 `START_AGENT`).
- 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 Options Supported by the agentDeploy Script.
- 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.

d. Run the root scripts after the install. For more information, see After Installing a Management Agent in Silent Mode.

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 Manual Management Agent Installation Logs.

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.**

   a. On the OMS host, from the Oracle 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.

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<username>
   ```

   For example,

   ```
   /u01/software/em24/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`

   b. Synchronize EM CLI:

   ```
   $<ORACLE_HOME>/bin/emcli sync
   ```

   c. Identify the platforms for which the Management Agent software is available in Software Library:

   ```
   $<ORACLE_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 = 24.1.0.0.0
   Platform Name = Linux x86-64
   ----------------------------------------------
   Version = 24.1.0.0.0
   Platform Name = Oracle Solaris on x86-64 (64-bit)
   ----------------------------------------------
   ```

```
Version = 24.1.0.0.0
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 *Acquiring the Management Agent Software in Online Mode* in the *Oracle Enterprise Manager Basic Installation Guide.*

d. Download the Management Agent software from the Software Library to a temporary directory on the OMS host:

```
$<ORACLE_HOME>/bin/emcli get_agentimage -destination=<download_directory>
-platform="<platform>" -version=<version>
```

For example,

```
./emcli get_agentimage -destination=/tmp -platform="Linux x86-64" -
version=24.1.0.0.0
```

> **Note:**
>
> 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 `24.1.0.0.0_AgentCore_226.zip`. For information on the contents of this core software, see Contents of the Downloaded Management Agent Software.

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 Using EM CLI from the Remote Destination Host to install the Management Agent.

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.

Acquiring the Management Agent Software and Downloading the RPM File onto the OMS Host

1. On the OMS host, from the Oracle 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.

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<username>
   ```

   For example,

```
/u01/software/em24/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:

```
$<ORACLE_HOME>/bin/emcli sync
```

3. Identify the platforms for which the Management Agent software is available in Software Library:

```
$<ORACLE_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 = 24.1.0.0.0
Platform Name = Linux x86-64
----------------------------------------------------
Version = 24.1.0.0.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
----------------------------------------------------
Version = 24.1.0.0.0
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 *Acquiring the Management Agent Software in Online Mode* in the *Oracle Enterprise Manager Basic Installation Guide.*

4. Download the `.rpm` file of the Management Agent from Software Library to a temporary directory on the OMS host:

```
$<ORACLE_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=24.1.0.0.0
```

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-24.1.0.0.0-1.0.i386.rpm`

> **Note:**
>
> Creating an agent rpm file for Linux is not supported when OMS is running on AIX.

Transferring the RPM File to the Destination Host

- 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.

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-24.1.0.0.0-1.0.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-24.1.0.0.0-1.0.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 6-5. 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 Manual Management Agent Installation Logs.

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 Using EM CLI from the Remote Destination Host or Using EM CLI from the OMS Host. 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 6-4.

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`

Response File Parameters for Installing a Management Agent in Silent Mode Using the AgentPull 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 `AgentPull` script.

Table 6-3 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. For example, `LOGIN_USER=sysman`
LOGIN_PASSWORD	*(Mandatory)* Enter the Enterprise Manager console login password. For example, `LOGIN_PASSWORD=myuserpassword`
PLATFORM	*(Mandatory)* Enter the platform for which you want to download the Management Agent software. For example, `PLATFORM="Linux x86-64"` **Note:** The value of this parameter must be in " ".

Table 6-3 (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. 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. For example, `AGENT_REGISTRATION_PASSWORD=Wel456come`
VERSION	*(Optional)* Enter the version of the Management Agent software you want to download. For example, `VERSION=24.1.0.0.0` If you do not specify this parameter, it is assigned the OMS version.
CURL_PATH (For Microsoft Windows hosts only)	*(Optional)* Enter the absolute path of the installed CURL utility. For example, `CURL_PATH=c:\Program Files\curl` If you do not include this parameter, it is assigned the value `c:\.`
OMS_HOST	*(Optional)* Enter the OMS host name. For example, `OMS_HOST=example.com`
EM_UPLOAD_PORT	*(Optional)* Enter the upload port (HTTP or HTTPS) for communicating with the OMS. 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: • Leave it blank. In this case, by default, an instance directory titled `agent_inst` is created in the agent installation base directory. For example, if the installation base directory is `/john/oracle/`, then the instance directory is defaulted to `/john/oracle/agent_inst` • Enter the absolute path to a custom directory. Although you can enter any location as a custom location, Oracle recommends you to maintain the instance directory inside the installation base directory. For example, `AGENT_INSTANCE_HOME=/u01/software/em24/agentbasedir/agent_inst`
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. For example, `AGENT_PORT=1832` If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored.
START_AGENT	*(Optional)* Enter `TRUE` if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter `FALSE`. For example, `START_AGENT=TRUE` 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. For example, `ORACLE_HOSTNAME=example.com` If you do not include this parameter, it defaults to the physical host name.

Table 6-3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using AgentPull Script

Parameter	Description
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. For example, `ALLOW_IPADDRESS=TRUE` If you do not include this parameter, it defaults to `FALSE`.
INVENTORY_LOCATION	*(Optional)* Enter the custom inventory location.

PROPERTIES_FILE	*(Optional)* Use this parameter to specify the absolute location of the properties file.
	For example, `PROPERTIES_FILE=/tmp/agent.properties`
	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 `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:
	`REPOSITORY_PROXYHOST=abc.example.com`
	`REPOSITORY_PROXYPORT=1532`
	The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:
	`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>`

s_agentSrvcName (Only for Microsoft Windows hosts)	*(Optional)* Enter the customized Management Agent service name. For example, `s_agentSrvcName=agentsrvc1` If you do not include this parameter, it defaults to *Oracle*+<oracle_home_name>+*Agent*. **Note:** *(For Microsoft Windows hosts)* If you upgrade a 24.1.0.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.
Access Permission	Add write permission to the agent.rsp file

Response File Parameters for Installing a Management Agent in Silent Mode Using the agentDeploy Script

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 the `agentDeploy` script.

Table 6-4 Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
OMS_HOST	*(Mandatory)* Enter the OMS host name. For example, `OMS_HOST=example.com`
EM_UPLOAD_PORT	*(Mandatory)* Enter the upload port (HTTP or HTTPS) for communicating with the OMS. For example, `EM_UPLOAD_PORT=14511`

Table 6-4 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description
AGENT_REGISTRATION_PASSWORD	*(Mandatory)* Enter a password for registering new Management Agents that join the Enterprise Manager system. 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. For example, `AGENT_REGISTRATION_PASSWORD=Wel456come`
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: • Leave it blank. In this case, by default, an instance directory titled `agent_inst` is created in the agent installation base directory. For example, if the installation base directory is `/john/oracle/`, then the instance directory is defaulted to `/john/oracle/agent_inst` • Enter the absolute path to a custom directory. Although you can enter any location as a custom location, Oracle recommends you to maintain the instance directory inside the installation base directory. For example, `AGENT_INSTANCE_HOME=/u01/software/em24/agentbasedir/agent_inst`
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. For example, `AGENT_PORT=1832` If you do not enter any value, then either 3872 or any free port between 1830 and 1849 is honored.
START_AGENT	*(Optional)* Enter `TRUE` if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter `FALSE`. For example, `START_AGENT=TRUE` 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. For example, `ORACLE_HOSTNAME=example.com` 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. For example, `ALLOW_IPADDRESS=TRUE` If you do not include this parameter, it defaults to `FALSE`.
INVENTORY_LOCATION	*(Optional)* Enter the custom inventory location.

Table 6-4 (Cont.) Creating a Response File for Installing Oracle Management Agent Using agentDeploy Script

Parameter	Description

PROPERTIES_FILE	*(Optional)* Use this parameter to specify the absolute location of the properties file.
	For example, `PROPERTIES_FILE=/tmp/agent.properties`
	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 `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:
	`REPOSITORY_PROXYHOST=abc.example.com`
	`REPOSITORY_PROXYPORT=1532`
	The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:
	`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>`

s_agentSrvcName (Only for Microsoft Windows hosts)	*(Optional)* Enter the customized Management Agent service name. For example, `s_agentSrvcName=agentsrvc1` If you do not include this parameter, it defaults to *Oracle*+<oracle_home_name>+*Agent*. **Note:** *(For Microsoft Windows hosts)* If you upgrade a 24.1.0.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.

Response File Parameters for Installing a Management Agent in Silent Mode Using an RPM File

Table 6-5 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 6-5 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. For example, `OMS_HOST=example.com`
OMS_PORT	*(Mandatory)* Enter the upload port (HTTP or HTTPS) to communicate with the OMS. For example, `OMS_PORT=1835`
AGENT_REGISTRATION_PASSWORD	*(Mandatory)* Enter a password for registering new Management Agents that join the Enterprise Manager system. 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. For example, `AGENT_REGISTRATION_PASSWORD=Wel456come`

Table 6-5 (Cont.) Creating a Response File for Installing Oracle Management Agent Using an RPM File

Parameter	Description
AGENT_USERNAME	*(Mandatory)* Enter the user name with which you want to install the Management Agent. For example, `AGENT_USERNAME=oracle`
AGENT_GROUP	*(Mandatory)* Enter the group to which the Management Agent user should belong. For example, `AGENT_GROUP=dba`
AGENT_PORT	*(Optional)* Enter the port used for the Management Agent process. For example, `AGENT_PORT=1832` 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. For example, `ORACLE_HOSTNAME=example.com`

Options Supported by the AgentPull Script

Table 6-6 lists the options supported by the `AgentPull.sh` script. On Microsoft Windows, these options apply to the `AgentPull.bat` file.

Table 6-6 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.
-ignoreDiscoveryPlugin	Ignores all the discovery plug-ins and allows only Oracle home plug-in.
-invPtrLoc	Enter the absolute path to the inventory file that has the location of the Central Inventory (oraInventory). For example, `-invPtrLoc /tmp/oraInst.loc` **Important:** • This option is supported only on Unix platforms, and not on Microsoft Windows platforms. • 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. • If you use this option, ensure that you do not use the `INVENTORY_LOCATION` option.

Options Supported by the agentDeploy Script

Table 6-7 lists the options supported by the `agentDeploy.sh` script. On Microsoft Windows, these options apply to the `agentDeploy.bat` file.

Table 6-7 Understanding the Options Supported by agentDeploy.sh/agentDeploy.bat

Option	Description
-prereqOnly	Runs only the prerequisite checks. Does NOT actually install the Management Agent. 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). For example, `INVENTORY_LOCATION=$HOME/oraInventory` **Important:** • This option is supported only on Unix platforms, and not on Microsoft Windows platforms. • 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. • 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). For example, `-invPtrLoc /tmp/oraInst.loc` **Important:** • This option is supported only on Unix platforms, and not on Microsoft Windows platforms. • 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. • 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.
-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 Installing the Oracle Management Agent Software Now and Configuring It Later. **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 Installing the Oracle Management Agent Software Now and Configuring It Later. **Note:** This option does not apply if you are cloning using a ZIP file.

Table 6-7 (Cont.) Understanding the Options Supported by agentDeploy.sh/agentDeploy.bat

Option	Description
-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. If you pass this option, then do not pass -configOnly, -softwareOnly, and -prereqOnly. **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. When you install the agent using the response file and -forceConfigure option, use the option as follows: • b_forceConfigure=true

Contents of the Downloaded Management Agent Software

Table 6-8 describes the contents of the core Management Agent software you download before installing the Management Agent using the `agentDeploy` script.

Table 6-8 Contents of the Downloaded Management Agent Software

Files	Description
Plugins	Plug-in directory containing all the discovering plug-ins, which were installed with the OMS, Oracle Home discovery plug-in, and Oracle Home monitoring plug-in.
agentcore.bin	Binary 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.

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 6-9 describes the contents of this agent base directory:

Table 6-9 Contents of the Agent Base Directory Present in RPM File

Element	Description
agent_24.1.0.0.0	Contains the Management Agent software.
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.

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 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 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 and adding targets in Enterprise Manager, see *Overview of Discovering and Adding Targets* in the *Oracle Enterprise Manager Administrator's Guide.*

Note:

- 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="agent24"`. 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:\agent24r1\24.1.0.0.0` denotes the Management Agent Oracle home:

  ```
  <HOME NAME="agent24" LOC="D:\agent24r1\24.1.0.0.0" 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 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 Enterprise Manager Console, or in silent mode. In particular, this chapter covers the following:

Overview of Cloning Management Agents

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager 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 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 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 and adding targets in Enterprise Manager, see *Overview of Discovering and Adding Target* in the *Oracle Enterprise Manager Administrator's Guide.*

Once the installation is complete, you will see the following default contents in the agent base directory:

```
<agent_base_directory>
    |_____agent_24.1.0.0.0
          |_____sbin
          |_____OPatch
          |_____agent.rsp
          |_____bin
          |_____cfgtoollogs
          |_____config
          |_____install
          |_____instalclient
          |_____.
          |_____.
          |_____.
    |_____agent_inst
    |_____agentInstall.rsp
    |_____agentimage.properties
```

> **Note:**
>
> You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For instructions, see Redirecting Oracle Management Agent to Another Oracle Management Service.
>
> 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.

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.
- For more information on the compatibility between a particular version of Oracle Management Agent 24ai and a particular version of Oracle Management Service 24ai, see *Before You Begin Installing an Enterprise Manager System* in the *Oracle Enterprise Manager 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 Installing Shared Agents.

- 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 4 of the following procedure.

1. Navigate to the following location in the Oracle home of the OMS host:

   ```
   $<ORACLE_HOME>/oui/prov/resources/scripts
   ```

   For example,

   ```
   /home/software/em/middleware/oms_home/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 install 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 Basic Installation Guide*), then run the following script on the OMS host as the OMS install 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.

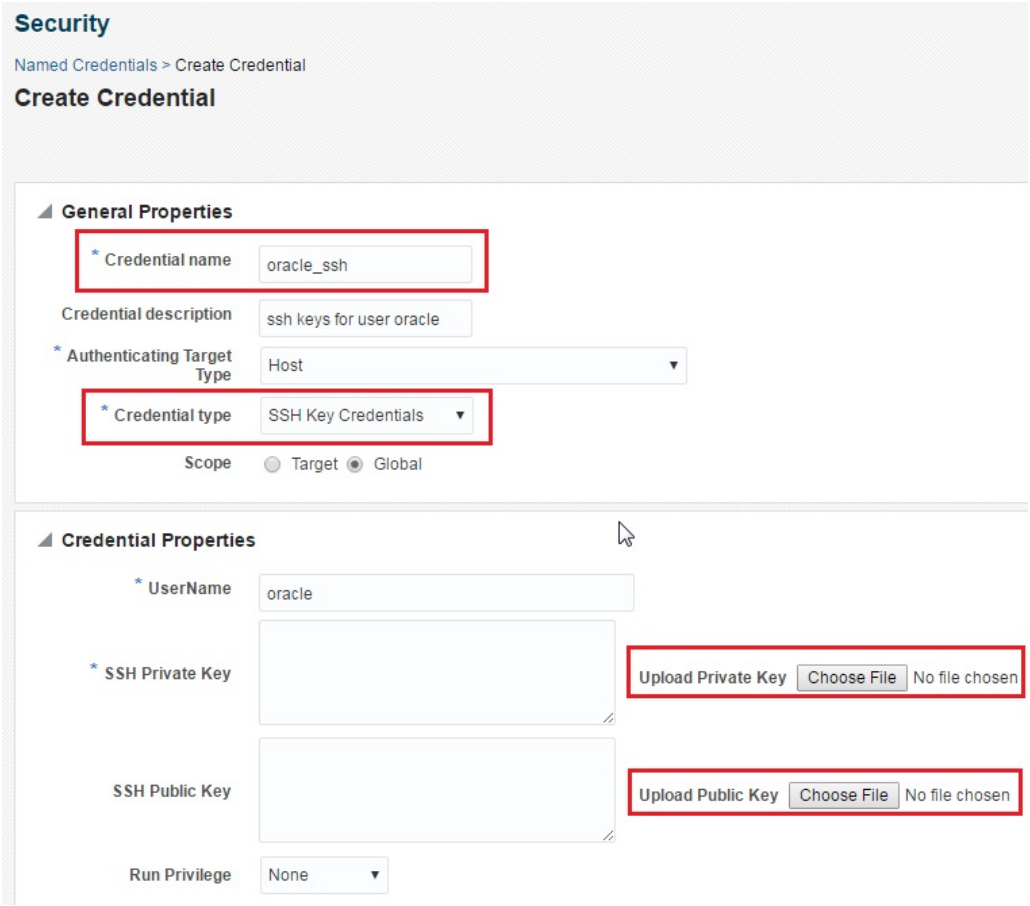
   From the **Setup** menu, select **Security,** then select **Named Credentials.** Click **Create.** For **Credential Name,** specify the name of the credential, for **Credential Type,** select **SSH Key Credentials,** and for **Scope,** select **Global.** If you do not select the **Global** option, you 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



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.

You can also use the Add host Targets Wizard to set up SSH public key authentication for a named credential.

- 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.
- Oracle Management Agent 24ai Release 1 was built, tested, and certified on Solaris. For version details, see Package Requirements for Oracle Management Agent in the *Oracle Enterprise Manager Basic Installation Guide*.
- Changes done to the `emd.properties` file on the source host before cloning are not carried over to the destination host after cloning.

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 *Hardware Requirements for Enterprise Manager*in the *Oracle Enterprise Manager Basic Installation Guide.*
Software Requirements *(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 *Installing Cygwin* in the *Oracle Enterprise Manager Basic Installation Guide.* **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*. To access the Enterprise Manager certification matrix, follow the steps outlined in *Accessing the Enterprise Manager Certification Matrix* in the *Oracle Enterprise Manager Basic Installation Guide.* 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.
	To verify the current value set, run the following command:
	`ulimit -u`
	If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.
	• Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.
	To verify the current value set, run the following commands:
	For Soft Limit:
	`/bin/sh -c "ulimit -n"`
	For Hard Limit:
	`/bin/sh -c "ulimit -Hn"`
	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:
	`<UID> soft nofile 4096`
	`<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 *Package, Kernel Parameter, and Library Requirements for Enterprise Manager* in the *Oracle Enterprise Manager 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. For more information, see the chapter on creating operating system groups and users in the *Creating Operating System Groups and Users for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.* **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.

Table 7-1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
/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: `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. 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. 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: `172.16.0.0 example.com mypc`
Destination Host Credential Requirements *(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. 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
(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:
	`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`
	If the time zone displayed is incorrect, log in to the destination host, and follow these steps:
	1. Run the following commands to set the time zone on the destination host:
	• For Korn shell:
	`TZ=<value>`
	`export TZ`
	• For Bourne shell or Bash shell:
	`export TZ=<value>`
	• For C shell:
	`setenv TZ <value>`
	For example, in the Bash shell, run the following command to set the time zone to America/New_York:
	`export TZ='America/New_York'`
	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.
	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).
	2. Restart the SSH daemon.
	If the destination host runs on a UNIX based operating system, run the following command:
	`sudo /etc/init.d/sshd restart`
	If the destination host runs on a Microsoft Windows operating system, run the following commands:
	`cygrunsrv -E sshd`
	`cygrunsrv -S sshd`
	3. Verify whether the SSH server can access the `TZ` environment variable by logging in to the OMS host, and running the following command:
	`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`
	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 After Cloning a Management Agent.

Table 7-1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description

Time Zone Requirements
(Only for Silent Mode)
	Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:
	`echo $TZ`
	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:
	• For Korn shell:
	`TZ=<value>`
	`export TZ`
	• For Bourne shell or Bash shell:
	`export TZ=<value>`
	• For C shell:
	`setenv TZ <value>`
	For example, in the Bash shell, run the following command to set the time zone to America/New_York:
	`export TZ='America/New_York'`
	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.
	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).
	Note:
	• 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.
	• 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 After Cloning a Management Agent.
	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 After Cloning a Management Agent.

sudo/pbrun/sesu/su SSH Requirements *(Only for Graphical Mode)*	*(Only for UNIX)* Ensure that you set the `oracle.sysman.prov.agentpush.enablePty` property to `true` in the `$<ORACLE_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. **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: • 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. For information on how to access the Installation Details page, see Cloning a Management Agent in Graphical Mode. • Comment out `Defaults requiretty` in the `/etc/sudoers` file.

Table 7-1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description

sudo/pbrun/sesu/su Requirements (for *Root* User)
(Only for Graphical Mode)
	(Only for UNIX)
	• 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.
	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:
	`<install_user> ALL=(root) /usr/bin/id, <agent_home>/*/agentdeployroot.sh`
	For example, `oracle ALL=(root) /usr/bin/id, /home/oracle/agentibd/*/agentdeployroot.sh`
	Here, `oracle` is the installing user, and `/home/oracle/agentibd` is the Management Agent home, that is, the agent base directory.
	• 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.
	In Enterprise Manager Cloud Control 13c Release 3 , 13c Release 4, 13c Release 5 and 24ai Release 1:
	`(root) /<AGENT_ORACLE_HOME>/sbin/nmosudo`

sudo/pbrun/sesu/su Requirements (for Locked Account User) *(Only for Graphical Mode)*	*(Only for UNIX)* 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. 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: `login_user1 ALL=(oracle) /bin/sh` Here, `login_user1` is the SSH log in user, and `oracle` is the locked account and install user. 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, em24100_<platform>.bin,` and `unzip` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool. 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: `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/agent_24.1.0.0.0/oui/bin/em24100_<platform>.bin, /home/oracle/agentibd/*/unzip, /home/oracle/agentibd/*/unzipTmp/unzip, /home/oracle/agentibd/*/agentcore.bin` 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.

Table 7-1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Permission Requirements	• Ensure that the agent base directory you specify is empty and has *write* permission. • Ensure that the instance directory is empty and has *write* permission.
PATH Environment Variable Requirements *(Only for Graphical Mode)*	On the destination host, ensure the following: • *(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). • (*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 *Validating Command Locations* in the *Oracle Enterprise Manager 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.
Temporary Directory Space Requirements	Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied. 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. Ensure that the directory name does not contain any spaces. 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. 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. If the agent base directory is mounted, then ensure that it is mounted with the `setuid` turned on.

Default SSH Port Requirements
(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:
	`netstat -anp | grep -i sshd`
	For example, the output of this command may be the following:
	`tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 3188/sshd`
	The above output indicates that the SSH daemon is running on port 22.
	Also, on a Unix host, you can run the following command to verify the SSH port:
	`cat /etc/ssh/sshd_config`
	For a Microsoft Windows host, the SSH port value is mentioned in the `C:\cygwin\etc\sshd_config` file.
	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:
	`$<ORACLE_HOME>/oui/prov/resources/Paths.properties`

Table 7-1 (Cont.) Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Software Availability Requirements *(Only for Graphical Mode)*	**For Cloning an Existing Management Agent** Ensure that you already have Oracle Management Agent 24ai 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. **For Installing a Management Agent Using Shared Oracle Home** Ensure that you already have Oracle Management Agent 24ai installed as a *Master Agent* in a shared, mounted location.
Installation Base Directory Requirements *(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. Also ensure that the inventory owner and the group to which the owner belongs have *read* and *write* permissions on the inventory directory. 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.
	• 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.
	`INVENTORY_LOCATION=<absolute_path_to_inventory_directory>`
	`-invPtrLoc <absolute_path_to_oraInst.loc>`

Port Requirements	Ensure that the default ports described in What Default Ports Are Used for Enterprise Manager Installation? are free.
Agent User Account Permissions and Rights *(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: • Act as part of the operating system. • Adjust memory quotas for a process. • Replace process level token. • Log on as a batch job. To verify whether the agent user has these rights, follow these steps: 1. Launch the Local Security Policy. 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**. 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. For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site: `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 *(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.

Cloning a Management Agent

This section describes the following:

- Cloning a Management Agent in Graphical Mode
- Cloning a Management Agent in Silent Mode

> **Note:**
>
> 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`

Cloning a Management Agent in Graphical Mode

This section describes how to clone a Management Agent using the Enterprise Manager 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

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 Enterprise Manager Console, 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, and click **Promote**.

  Enterprise Manager 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, click **Install Agent on Host.**

  Enterprise Manager 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 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 Format of Host List File .

      > **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 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:
>
> i. 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.
>
> ii. 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.)

b. From the table, select the first row that indicates the hosts grouped by their common platform name.

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.

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 After Cloning a Management Agent.

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 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 Oracle home of the OMS host:
>
> `$<ORACLE_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.

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.

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). For example, `INVENTORY_LOCATION=$HOME/oraInventory` **Important:** • This parameter is supported only on Unix platforms, and not on Microsoft Windows platforms. • 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. • 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). For example, `-invPtrLoc /tmp/oraInst.loc` **Important:** • This parameter is supported only on Unix platforms, and not on Microsoft Windows platforms. • 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. • If you use this parameter, ensure that you do not use the `INVENTORY_LOCATION` parameter.
s_agentSrvcName	*(Only for Microsoft Windows)* Enter a custom name for the Management Agent service. 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. For example, `s_agentSrvcName=agentsrvc1` **Note:** If you upgrade a 13c Release 5 Management Agent installed on a Microsoft Windows host to 24ai Release 1, 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.
START_AGENT=false	Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured. 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. If you specify this parameter, ensure that you also specify the OMS HTTP port, using the `EM_UPLOAD_PORT` parameter. For example, `b_secureAgent=false EM_UPLOAD_PORT=4899` If you do not specify this parameter, the Management Agent is secured automatically after the install.

Cloning a Management Agent in Silent Mode

To clone a Management Agent manually, follow these steps:

> **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.

1. Set the required environment variables as described in Table 7-3.

Table 7-3 Setting Environment Variables for Cloning in Silent Mode

Variable	What to Set?	How to Set?

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:
		`export AGENT_BASE_DIR=<absolute_path_to_agent_install_base_dir>`
		For example,
		`export AGENT_BASE_DIR=/u01/software/em24/agentbasedir`
		• In other terminals, run the following command:
		`setenv AGENT_BASE_DIR <absolute_path_to_agent_install_base_dir>`
		For example,
		`setenv AGENT_BASE_DIR /u01/software/em24/agentbasedir`

AGENT_HOME	Set it to the Oracle home of the Management Agent.
	For example,
	`/u01/software/em24/agentbasedir/agent_24.1.0.0.0`
		• In bash terminal, run the following command:
		`export AGENT_HOME=<absolute_path_to_agent_home>`
		For example,
		`export AGENT_HOME=/u01/software/em24/agentbasedir/agent_24.1.0.0.0`
		• In other terminals, run the following command:
		`setenv AGENT_HOME <absolute_path_to_agent_home>`
		For example,
		`setenv AGENT_HOME /u01/software/em24/agentbasedir/agent_24.1.0.0.0`

T_WORK	Set it to `/tmp/clone_work`.	• In bash terminal, run the following command:
		`export T_WORK=/tmp/clone_work`
		• In other terminals, run the following command:
		`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 agent_24.1.0.0.0 plugins.txt
   ```

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_HOME/sysman/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 6-4.

> **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> -clone
    ```

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 Options Supported by the agentDeploy Script.
- If the source Management Agent was installed using the Add Host Targets Wizard, ensure that you specify the `START_AGENT=true` and the `b_secureAgent=true` parameters while invoking the deployment script.

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, click **Install Agent 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 Oracle home of the OMS host:
>
> `$<ORACLE_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 After Installing a Management Agent in Silent Mode.

> **Note:**
>
> - You can repoint your existing Management Agents to a new Oracle Management Service (OMS). For instructions, see Redirecting Oracle Management Agent to Another Oracle Management Service.
>
> 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.

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 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.

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 Oracle home of the OMS:

   ```
   $<ORACLE_HOME>/oui/prov/resources/scripts
   ```

   For example,

   ```
   /u01/software/em24/oms_home/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 install 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 (see *Installing Cygwin* in the *Oracle Enterprise Manager Basic Installation Guide*), then run the following script on the OMS host as the OMS install 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.

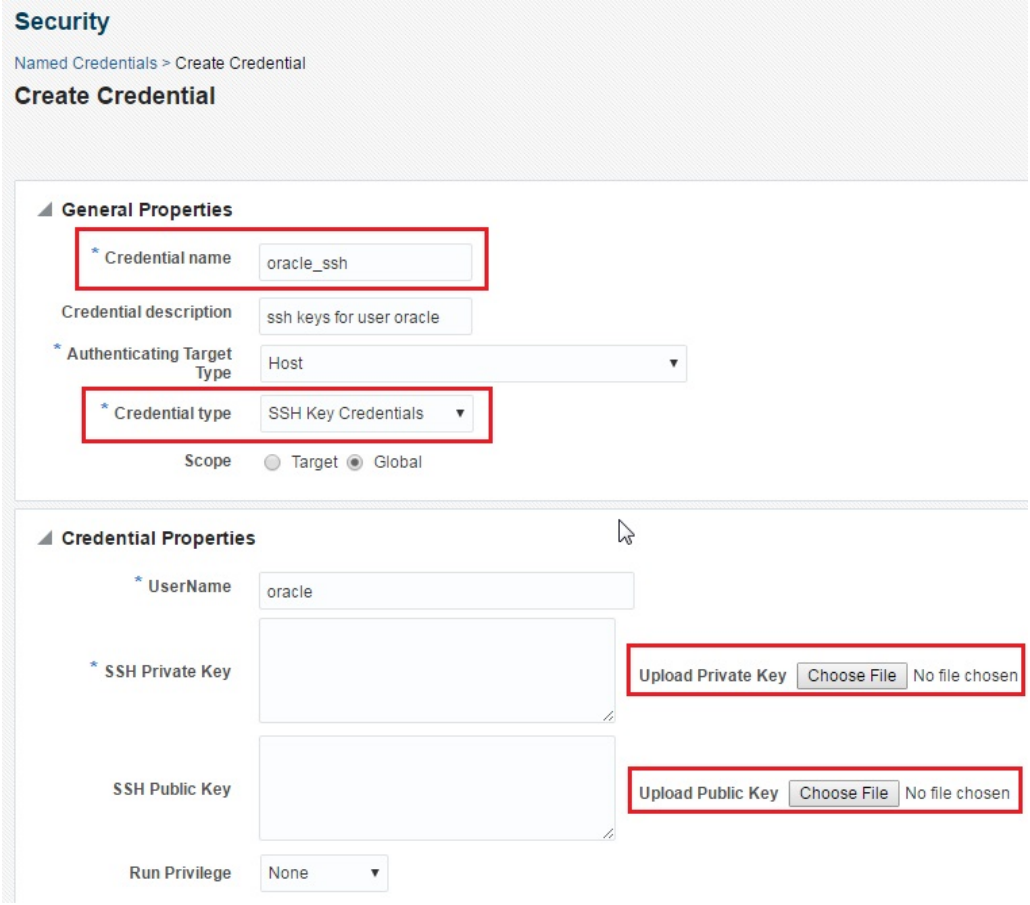
   From the **Setup** menu, select **Security,** then select **Named Credentials.** Click **Create.** For **Credential Name,** specify the name of the credential, for **Credential Type,** select **SSH Key Credentials,** and for **Scope,** select **Global.** If you do not select the **Global** option, you 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



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*
- Oracle Management Agent 24ai Release 1 was built, tested, and certified on Solaris. For version details, see Package Requirements for Oracle Management Agent.

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 *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager 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*. 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. To access the Enterprise Manager certification matrix, see *Accessing the Enterprise Manager Certification Matrix* in the *Oracle Enterprise Manager Basic Installation Guide.* 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.
	To verify the current value set, run the following command:
	`ulimit -u`
	If the current value is not 13312 or greater, then contact your system administrator to set it to at least 13312.
	• Ensure that you set the soft limit of file descriptor to a minimum of 4096 and hard limit less then or equal to 16384.
	To verify the current value set, run the following commands:
	For Soft Limit:
	`/bin/sh -c "ulimit -n"`
	For Hard Limit:
	`/bin/sh -c "ulimit -Hn"`
	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:
	`<UID> soft nofile 4096`
	`<UID> hard nofile 16384`

Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see *Package, Kernel Parameter, and Library Requirements for Enterprise Manager* in the *Oracle Enterprise Manager 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. For more information, see *Creating Operating System Groups and Users for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.* **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 24ai installed as a *Master Agent* in a shared, mounted location. For information on how to install a Management Agent, see *Installing Oracle Management Agents* in the *Oracle Enterprise Manager Basic Installation Guide.*

Table 8-1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description

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:
	`mount -t nfs -o rw <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent>`
	For example, run the following command:
	`mount -t nfs -o rw abc.oracle.com:/scratch/agent /scratch/agent`
	To mount the Management Agent software on the *Shared Agent* host with read only permissions, run the following command:
	`mount -t nfs -o ro <master_agent_host_name>:<agent_base_dir_of_master_agent> <agent_base_dir_of_shared_agent>`
	For example, run the following command:
	`mount -t nfs -o ro abc.oracle.com:/scratch/agent /scratch/agent`
	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: `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. 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. 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: `172.16.0.0 example.com mypc`
Destination Host Credential Requirements *(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. 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
(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:
	`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`
	If the time zone displayed is incorrect, log in to the destination host, and follow these steps:
	1. Run the following commands to set the time zone on the destination host:
	• For Korn shell:
	`TZ=<value>`
	`export TZ`
	• For Bourne shell or Bash shell:
	`export TZ=<value>`
	• For C shell:
	`setenv TZ <value>`
	For example, in the Bash shell, run the following command to set the time zone to America/New_York:
	`export TZ='America/New_York'`
	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).
	2. Restart the SSH daemon.
	If the destination host runs on a UNIX based operating system, run the following command:
	`sudo /etc/init.d/sshd restart`
	If the destination host runs on a Microsoft Windows operating system, run the following commands:
	`cygrunsrv -E sshd`
	`cygrunsrv -S sshd`
	3. Verify whether the SSH server can access the `TZ` environment variable by logging in to the OMS host, and running the following command:
	`ssh -l <install_user> <destination_host_name> /bin/sh -c 'echo $TZ'`
	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 After Installing Shared Agents.

Table 8-1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description

Time Zone Requirements
(Only for Silent Mode)
	Ensure that the host time zone has been set correctly. To verify the host time zone, run the following command:
	`echo $TZ`
	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:
	• For Korn shell:
	`TZ=<value>`
	`export TZ`
	• For Bourne shell or Bash shell:
	`export TZ=<value>`
	• For C shell:
	`setenv TZ <value>`
	For example, in the Bash shell, run the following command to set the time zone to America/New_York:
	`export TZ='America/New_York'`
	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).
	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 After Installing Shared Agents.

sudo/pbrun/sesu/su SSH Requirements *(Only for Graphical Mode)*	Ensure that you set the `oracle.sysman.prov.agentpush.enablePty` property to `true` in the `$<ORACLE_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. **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: • 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. For information on how to access the Installation Details page, see Installing Shared Agents Using Add Host Targets Wizard. • 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)
(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.
	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:
	`<install_user> ALL=(root) /usr/bin/id, <agent_home>/*/agentdeployroot.sh`
	For example, `oracle ALL=(root) /usr/bin/id, /u01/app/oracle/admin/shared/agent_home/*/agentdeployroot.sh`
	Here, `oracle` is the installing user, and `/u01/app/oracle/admin/shared/agent_home` is the *Shared Agent* home.
	• 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.
	In Enterprise Manager Cloud Control 13c Release 3, 13c Release 4, 13c Release 5 and 24ai Release 1:
	`(root) /<AGENT_ORACLE_HOME>/sbin/nmosudo`

sudo/pbrun/sesu/su Requirements (for Locked Account User) *(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. 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: `login_user1 ALL=(oracle) /bin/sh` Here, `login_user1` is the SSH log in user, and `oracle` is the locked account and install user. 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, em24100_<platform>.bin,` and `unzip` as the locked account user. Grant the privileges in the configuration file of your privilege delegation tool. 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: `login_user1 ALL=(oracle) /usr/bin/id, /bin/chmod, /bin/cp, /bin/mkdir, /bin/rm, /bin/tar, /home/oracle/agentinst/bin/emctl, /home/oracle/agentibd/agent_24.1.0.0.0/perl/bin/perl, /home/oracle/agentibd/agent_24.1.0.0.0/oui/bin/em24100_<platform>.bin, /home/oracle/agentibd/agent_24.1.0.0.0/bin/unzip, /home/oracle/agentibd/*/agentcore.bin` 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.

Table 8-1 (Cont.) Prerequisites for Installing Shared 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. 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 *(Only for Graphical Mode)*	Validate the path to all command locations. For more information, see *Validating Command Locations* in the *Oracle Enterprise Manager 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.

Default SSH Port Requirements
(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:
	`netstat -anp | grep -i sshd`
	For example, the output of this command may be the following:
	`tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 3188/sshd`
	The above output indicates that the SSH daemon is running on port 22.
	Also, on a Unix host, you can run the following command to verify the SSH port:
	`cat /etc/ssh/sshd_config`
	For a Microsoft Windows host, the SSH port value is mentioned in the `C:\cygwin\etc\sshd_config` file.
	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:
	`$<ORACLE_HOME>/oui/prov/resources/Paths.properties`

Port Requirements	Ensure that the default ports described in What Default Ports Are Used for Enterprise Manager Installation? are free.
Installing User Requirements	• The *Master Agent* and the *Shared Agent* must be installed with the same user account. • If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group. • Ensure that the inventory owner and the group to which the owner belongs have *read* and *write* permissions on the inventory directory. 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. • The *Shared Agent* uses the inventory location mentioned in the `oraInst.loc` file, which is present in the `<MASTER_AGENT_BASE DIR>/24.1.0.0.0/` directory. Ensure that the *Shared Agent* user has read and write permissions on this directory.

Table 8-1 (Cont.) Prerequisites for Installing Shared Agent

Requirement	Description
Preinstallation/Postinstallation Scripts Requirements *(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.

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

> **Note:**
>
> 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`

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 Enterprise Manager, 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, and click **Promote**.
   - From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, click **Install Agent on 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 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 Format of Host List File

> **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 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.

   b. From the table, select the first row that indicates the hosts grouped by their common platform name.

   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.

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 After Installing Shared Agents.

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 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.

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
START_AGENT=false	Specify this parameter if you do not want the Management Agent to start automatically once it is installed and configured. If you do not specify this parameter, the Management Agent starts automatically once it is installed and configured.

Table 8-2 (Cont.) Supported Additional Parameters

Parameter	Description
b_secureAgent=false	Specify this parameter if you do not want the Management Agent to be secured after the install. If you specify this parameter, ensure that you also specify the OMS HTTP port, using the `EM_UPLOAD_PORT` parameter. For example, `b_secureAgent=false EM_UPLOAD_PORT=4899` If you do not specify this parameter, the Management Agent is secured automatically after the install.

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,

   ```
   /shared/app/agentbasedir/agent_24.1.0.0.0/perl/bin/perl /shared/app/agentbasedir/agent_24.1.0.0.0/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,

  ```
  /shared/app/agentbasedir/agent_24.1.0.0.0/perl/bin/perl /
  shared/app/agentbasedir/agent_24.1.0.0.0/sysman/install/
  AgentNFS.pl AGENT_INSTANCE_HOME=/<local_location>/agent_inst
  ORACLE_HOME=/shared/app/agentbasedir/agent_24.1.0.0.0
  AGENT_PORT=1832 AGENT_REGISTRATION_PASSWORD=welcome
  b_secureAgent=TRUE START_AGENT=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>
  ```

  ```
  START_AGENT=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 /shared/app/agentbasedir/agent_inst/root.sh
   ```

4. Repeat Step (2) to Step (4) on the remaining hosts where you want to install the *Shared Agent*.

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. For example, /shared/app/agentbasedir/agent_24.1.0.0.0
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. 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. For example, `/<local_location>/agent_inst` 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. 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. For example, `Wel456come` **Note:** If the *Master Agent* was installed using the Add Host Targets Wizard, then you must pass this parameter.
b_secureAgent=TRUE	Set it to `TRUE` so that the *Shared Agent* is secured.
START_AGENT	Set it to `TRUE` so that the *Shared Agent* is started automatically once it is installed and configured. **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. For example, `ALLOW_IPADDRESS=TRUE` If you do not include this parameter, it defaults to `FALSE`.
START_PRIORITY_LEVEL (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. For example, `START_PRIORITY_LEVEL=95` If you do not include this parameter, it defaults to `98`.
SHUT_PRIORITY_LEVEL (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`. For example, `SHUT_PRIORITY_LEVEL=25` If you do not include this parameter, it defaults to `19`.

Table 8-3 (Cont.) Creating a Response File for Installing Oracle Management Agent Using the AgentNFS.pl Script

Parameter	Description

PROPERTIES_FILE	*(Optional)* Use this parameter to specify the absolute location of the properties file.
	For example, `PROPERTIES_FILE=/tmp/agent.properties`
	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 `$<AGENT_INSTANCE_HOME>/sysman/config/emd.properties`. In the properties file, you must specify the parameters in name value pairs, for example:
	`REPOSITORY_PROXYHOST=abc.example.com`
	`REPOSITORY_PROXYPORT=1532`
	The properties file does not support parameter values that have spaces. If the value of a particular parameter contains a space, then run the following command after deploying the Management Agent:
	`$<AGENT_INSTANCE_HOME>/bin/emctl setproperty agent -name <parameter_name> -value <parameter_value>`

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, click **Install Agent 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 13*c* Release 4, 13*c* Release 5 and 24ai Release 1 , `nmosudo` is located in the `sbin` directory, which is in the agent base directory. For example, `<AGENT_BASE_DIRECTORY>/sbin/nmosudo`.

   Therefore, when you install a 24ai Release 1 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 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 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, see *Discovering and Adding Host and Non-Host Targets* in the *Oracle Enterprise Manager Administrator's Guide*

9

Converting Shared Agents to Standalone Agents

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

With the first Oracle Management Service (OMS) you install, by default you receive a Management Agent called the *Central Agent.* The *Central Agent* is used for monitoring only the first OMS host, the first OMS, and the other targets running on the first OMS host. To monitor other hosts and the targets running on those hosts, you must install a separate *Standalone Management Agent* on each of those hosts.

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 chapter describes how to convert Shared Agents to Standalone Agents. In particular, this chapter covers the following:

Converting NFS or Shared Agents to Standalone Agents

> **Note:**
>
> You must carry out this procedure for every Shared Agent that you want to convert to a standalone Agent.

To convert NFS or Shared Agents to Standalone agents, follow these steps:

1. In the Master Agent host, navigate to the agent base directory and compress the directory excluding the following files:
   - agent_inst directory
   - root owned files in the sbin directory

   To do so, execute the following command:

   ```
   cd <agent base directory>
   zip -rq agentcoreimage.zip  * -x sbin/nmb sbin/nmgsshe sbin/nmhs sbin/nmo sbin/
   nmopdpx sbin/nmosudo agent_inst
   For example,
   cd /u01/app/oracle/agent_nfs/agentbasedir
   zip -rq agentcoreimage.zip * -x sbin/nmb sbin/nmgsshe sbin/nmhs sbin/nmo sbin/
   nmopdpx sbin/nmosudo agent_inst
   ```

Perform the following steps in each of the Shared agents.

2. Stop the agent by executing the following command:

```
<sharedagent_inst>/bin/emctl stop agent
For example,
/u01/app/emstate/agent_inst/bin/emctl stop agent
```

3. Copy the compressed file to a local folder in the Shared Agent host by executing the following command:

```
cp <agent base directory>/agentcoreimage.zip <local directory>
For example,
cp /u01/app/oracle/agent_nfs/agentbasedir/agentcoreimage.zip /u01/stage
```

4. Unmount the agent base directory by executing the following command:

```
umount <path to the agent base directory>
For example,
umount /u01/app/oracle/agent_nfs/agentbasedir
```

> **Note:**
>
> You cannot run this command if you are not a root user.

5. Extract the compressed file from the local directory in the agent base directory by executing the following command:

```
unzip agentcoreimage.zip -d <agent base directory>
For example,
unzip /u01/stage/agentcoreimage.zip -d /u01/app/oracle/agent_nfs/agentbasedir
```

6. Run the <path to the agent home>/root.sh script as a root user.

7. Copy the instance home in the agent base directory and rename it to agent_inst to match the structure in the Master Agent, by executing the following command:

```
cp -r <local instance home> <agent base directory>/
For example,
cp -r /u01/app/emstate/agent_inst/* /u01/app/oracle/agent_nfs/agentbasedir/
agent_inst/
```

8. Start the Agent from the path <agent base directory>/agent_inst, by executing the following command:

```
<agent base directory>/agent_inst/bin/emctl start agent
For example,
/u01/app/oracle/agent_nfs/agentbasedir/agent_inst/bin/emctl start agent
```

9. Execute the following command to create an entry in the inventory by executing the following command:

```
$ORACLE_HOME/oui/bin/attachHome.sh -silent ORACLE_HOME=<$ORACLE_HOME> -force
```

10. Refresh the Oracle home collection by executing the following command:

```
<Agent Instance Home>/bin/emctl control agent runCollection
<ORACLEHOME_TARGET_NAME>: oracle_home oracle_home_config

For example,

./u01/app/oracle/agent_nfs/agentbasedir/agent_inst/emctl control agent
runCollection example.com:oracle_home oracle_home_config
```

> **Note:**
>
> <ORACLEHOME_TARGET_NAME> is present in the <Agent Instance Home>/sysman/emd/targets.xml file.

To refresh the Oracle home collection using the graphical interface, follow these steps:

a. On the Home page of the Management Agent, in the Summary section, click **Oracle Home and Patch Details.**

b. On the following page, click **Refresh Configuration.**

> **Note:**
>
> Perform this step for both Shared and Master Agents.

10

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:

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 system in a test environment to an Enterprise Manager 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.

Before You Begin Installing a Management Agent

Before you begin installing a Management Agent, review the points outlined in Before You Begin Installing a Management Agent in Silent Mode.

Prerequisites for Installing a Management Agent

Before installing the Management Agent, ensure that you meet the prerequisites described in Prerequisites for Installing a Management Agent in Silent Mode.

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 Installing a Management Agent Using the agentDeploy Script. 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=/u01/software/em24/agentbasedir 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`.

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, `/u01/software/em24/agentbasedir/agent_24.1.0.0.0/sysman/install/agentDeploy.sh AGENT_BASE_DIR=/u01/software/em24/agentbasedir 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 Installing Only the Management Agent Software Binaries.
> - Do not pass the option `-forceConfigure`.

After Installing a Management Agent

After you install the Management Agent, follow the steps outlined in After Installing a Management Agent in Silent Mode.

Part V
Hybrid Cloud Management

This part describes the Hybrid Cloud Management feature in Enterprise Manager. It consists of the following chapters:

- Enabling Hybrid Cloud Management
- Deploying JVMD for Hybrid Cloud

11

Enabling Hybrid Cloud Management

With Oracle Hybrid Cloud, you can use the Enterprise Manager Console to administer both your on-premises and Oracle Cloud deployments. Oracle Hybrid Cloud lets on-premises Enterprise Manager administrators monitor and manage cloud services using the same Oracle Enterprise Manager tools they use to monitor, provision, and maintain Oracle Databases, Engineered Systems, Oracle Applications, Oracle Middleware, and a variety of third-party systems.

This chapter consists of the following sections:

What is Oracle Hybrid Cloud?

Your IT infrastructure may consist of a mix of on-premises and cloud-based targets. For example, you may have instances of Oracle Database Cloud Services and Java Cloud Services to manage along with various on-premises software. No matter where your IT assets reside, Enterprise Manager allows you to manage this *Hybrid Cloud* environment through a single pane of glass.

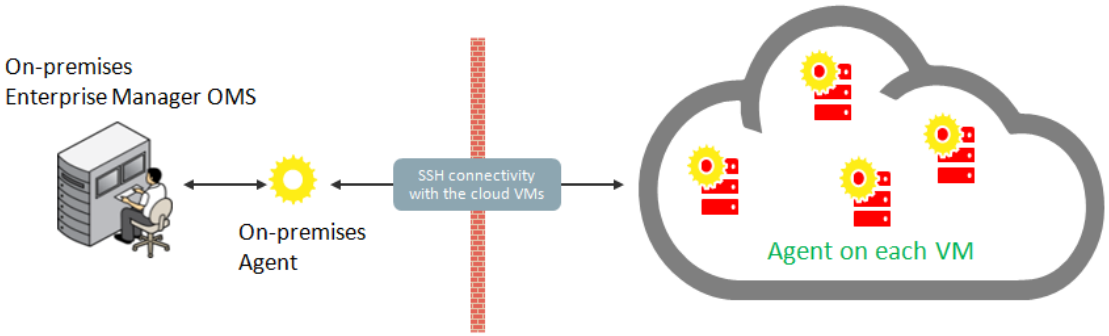
Configuring Enterprise Manager to manage a Hybrid Cloud environment involves deploying Management Agents throughout your Hybrid Cloud environment to allow your cloud services to communicate with Enterprise Manager. By deploying Agents on the Oracle Cloud virtual hosts running your Oracle Cloud services, you are able to manage these services just as you would any other monitored target from the Enterprise Manager Console.

You can monitor four service types with Oracle Hybrid Cloud:

- Database Cloud
- Java Cloud
- Compute Cloud
- Cloud Machine

Communication between your cloud services and the OMS is secure from external interference. As shown in the following graphic, the on-premises OMS communicates via

HTTPS, SQL*Net and JMX over SSH (if VPN is not available) with Agents installed on the VMs running your cloud services.



How do I set up Oracle Hybrid Cloud Monitoring?

Setting up your Oracle Hybrid Cloud environment is straightforward. The following table provides a quick how-to reference.

Step	What you need to do:
1. Make sure the on-premises host running an Agent can communicate with the Oracle Cloud VMs. **This step is IMPORTANT!** All subsequent setup tasks will fail without an open communication channel between the on-premises Agent and the Oracle Cloud.	Ensure there is network connectivity between the OMS and Oracle Cloud. SSH must work between the host that the Gateway is installed on and VMs in the Oracle Cloud. For more information about Oracle Hybrid Cloud prerequisites, see Hybrid Cloud Management Prerequisites and Basic Setup, Prerequisites for Configuring a Management Agent as a Gatewayand Prerequisites for Installing Agents on Oracle Cloud VMs. Make sure you have supported cloud services to monitor. Oracle Hybrid Cloud supports the following services: • Oracle Database Cloud Services See Creating a Service Instance (Oracle Database Cloud-Database as a Service Quick Start. • Oracle Java Cloud Services See Oracle Java Cloud Service. • Oracle Compute Cloud Services See Creating an Oracle Linux Instance Using the Oracle Compute Cloud Service Web Console.
2. Configure an Enterprise Manager Agent as a Gateway.	See Configuring a Management Agent as a Gateway **Important**: Ensure environment requirements have been met before deploying a Management Agent as a Gateway. For more information, see Prerequisites for Configuring a Management Agent as a Gateway
3. **(Optional)** Set up an external proxy.	Configure an external proxy between the Oracle Cloud and the Gateway to enhance security. See Configuring an External Proxy to Enable Gateways to Communicate with the Oracle Cloud.

Step	What you need to do:
4. Deploy Agents to the VMs running your Oracle Cloud services.	See Installing an Agent on an Oracle Cloud VM. **Important**: Ensure resource and network requirements have been met before installing the Agent. For more information, see Prerequisites for Installing Agents on Oracle Cloud VMs.

Setting Up Hybrid Cloud Management in Three Steps

Now that you understand the Hybrid Cloud management setup flow shown in What is Oracle Hybrid Cloud?, you now know that setting up Hybrid Cloud management is fairly straightforward. Setting up your on-premises Enterprise Manager system to manage and monitor an Oracle Cloud can be done in as little as three steps:

Step 1 Make sure an on-premises Agent can communicate with the Oracle Cloud via SSH.

From the on-premises side: Make sure that an on-premises host running a Management Agent (version 24ai or higher) can connect via SSH with the Oracle Cloud VM you want to monitor.

From the Oracle Cloud side:

- Make sure the default port is set to 1748, or that one port in the range 1830 to 1848 is free on the Oracle Cloud VM.
- Make sure the user installing the Enterprise Manager Agent on the Oracle Cloud VM has SUDO privileges in order to run the *root.sh* script.

Step 2: Configure an on-premises Agent to serve as a Gateway.

Use the EM CLI `register_hybridgateway_agent` verb to designate an Agent as a Gateway.

```
emcli register_hybridgateway_agent -hybridgateway_agent_list="<On-premises
target name for the Agent chosen in Step 1>"
     -named_credential="named_credential"
     -named_credential_owner="named_credential_owner"
     -cloud_hostname="cloud_hostname"
```

Step 3: Deploy Agents on Oracle Cloud VMs to communicate with the on-premises Gateway.

Before starting the Agent deployment process, make sure you have the following information:

- IP Address of the Oracle Cloud VM.
- SSH public keys mapped as Enterprise Manager Named Credentials.

  You can create a Named Credential either through the Enterprise Manager console (**Setup** –> **Security** –> **Named Credentials**) or by using the EM CLI `create_named_credential` verb.
- Details about the Gateway you configured in **Step 2**.

You can deploy the Agent to the Cloud VM using Agent Push functionality from the Enterprise Manager console, or by using the EM CLI `submit_add_host` verb shown below:

```
emcli submit_add_host
   -host_names=<IP addresses of Oracle Cloud VM>
   -installation_base_directory=<Path for installing the Agent on the Oracle
Cloud VM>
   -credential_name=<Enterprise Manager Credential for the SSH Key>
   -configure_hybrid_cloud_agent -hybrid_could_gateway_agent=<Target Name of
the Gateway Agent>
   -hybrid_cloud_gateway_proxy_port=<Port on the Gateway host used for
outbound SSH communication>
```

Hybrid Cloud Management Prerequisites and Basic Setup

Setting up Hybrid Cloud management consists of the following steps:

1. Ensure that your on-premises OMS is version 24ai, and that at least one 24ai Management Agent exists in your on-premises environment.

   If your on-premises OMS is an earlier version, ensure that you upgrade the OMS to version 24ai. For information on how to do so, see the *Oracle Enterprise Manager Upgrade Guide.*

   To ensure that at least one 24ai Management Agent exists in your on-premises environment, either deploy a new 24ai Management Agent, or upgrade an existing Management Agent of an earlier version to version 24ai.

   For information on how to deploy a new 24ai Management Agent, see *Oracle Enterprise Manager Basic Installation Guide.* For information on how to upgrade an existing Management Agent of an earlier version to version 24ai, see the *Oracle Enterprise Manager Upgrade Guide.*

   > **Note:**
   >
   > Oracle strongly recommends that you first upgrade the earlier version of the Management Agent to 24ai and then configure that Agent to serve as a Gateway. This way, your entire stack will be at 24ai. However, if you do not want to upgrade the earlier version, you can continue to use it and configure it to act as a Gateway. However, only the earlier version 13*c* Release 5 is supported in this case. All earlier Agent versions must be upgraded to either 13*c* Release 5 or 24ai Release 1.

2. Configure one or more 24ai Management Agents within your on-premises environment to serve as a Gateway. A Gateway provides an SSH-based communication channel between the Oracle Cloud virtual hosts and the on-premises OMS. For more information on configuring an external proxy to enable Hybrid Cloud Gateways, see Configuring an External Proxy to Enable Hybrid Cloud Gateway Agents to Communicate with Oracle Cloud

   To ensure high availability, Oracle recommends that you configure multiple 24ai Management Agents to act as Gateways.

3. Ensure that the on-premises OMS can communicate with the Oracle Cloud targets via the Gateway.

If the Gateway is unable to communicate with the Oracle Cloud targets directly, configure an external proxy for the communication. For information on how to do so, see Configuring an External Proxy to Enable Gateways to Communicate with the Oracle Cloud.

To communicate with Oracle Cloud targets, the on-premises OMS uses the My Oracle Support (MOS) proxy by default. You can also configure an Agent Proxy instead of the default proxy. Ensure that the proxy configured in your enterprise supports SSH tunneling, or configure a new MOS proxy that supports SSH tunneling.

4. Deploy Management Agents to the Oracle Cloud virtual hosts using the *Add Host Targets Wizard* or EM CLI. and configure them in Hybrid mode. Management Agents configured in Hybrid mode enable Enterprise Manager to manage the Oracle Cloud targets. As part of the Hybrid Cloud Agent deployment process, you will associate each with the Gateway that it will use to communicate with the on-premises OMS.

Prerequisites for Configuring a Management Agent as a Gateway

Before configuring a Management Agent to act as a Gateway, ensure the following prerequisites are met:

- Ensure there is network connectivity between the OMS and Oracle Cloud. SSH must work between the host that the Gateway is installed on and VMs in the Oracle Cloud.
- Ensure that the CPU, RAM, and hard disk space requirements are met.

  The CPU, RAM, and hard disk space requirements for a Hybrid Cloud Gateway are described in *Oracle Enterprise Manager Basic Installation Guide.*

  Note that the hardware requirements for the Hybrid Cloud Gateway and regular Management Agents are the same.
- *(Recommendation)* You should install a new Agent on a dedicated host to serve as the Hybrid Cloud Gateway. This ensures high Gateway performance.

> **Note:**
>
> Oracle recommends that you do not designate the central Agent as a Hybrid Cloud Gateway. In an enterprise with a large number of targets, the designated central Agent may compete with the OMS for resources.

In general, any prerequisites required for deploying Management Agents also apply to Gateways. For more information, see *Oracle Enterprise Manager Basic Installation Guide.*

Configuring a Management Agent as a Gateway

To configure an existing Management Agent version 24ai as a Gateway, follow these three steps:

> **Note:**
>
> You can use an existing Management Agent of an earlier version and configure that to act as a Gateway. However, Oracle strongly recommends that you first upgrade that Management Agent of the earlier version to 24ai version and then configure that to act as a Gateway. This way, your entire stack will be at 24ai version.

1. As SYSMAN user, log in to EM CLI. You can log in from the default EM CLI installation that is available in the OMS home, or from the EM CLI installation that is set up on any other host.

   ```
   $<emcli_install_location>/bin/emcli login -username=sysman
   ```

   EM CLI is set up by default on the on-premises OMS host (the EM CLI install location is the OMS home). Hence, if you choose to run EM CLI from the on-premises OMS host, no additional steps are required. This is the recommended option.

   For example, if you are logging in from the EM CLI installation that is available in the OMS home, then run the following command:

   ```
   /em24/oms_home/bin/emcli login -username=sysman
   ```

   If you choose to run EM CLI from a custom location on a host that is not running the on-premises OMS, you must first set up EM CLI on the required host..

2. Designate the selected Management Agent to act as a Hybrid Cloud Gateway. To do so, run the `register_hybridgateway_agent` EM CLI verb from the OMS home or from any other host where EM CLI is set up. The verb can be executed from a command line or from a script.

   The verb takes a list of Management Agents and marks each Agent as a *hybridgateway*.

   Command Line Mode

   ```
       $<emcli_install_location>/bin/emcli register_hybridgateway_agent -
   hybridgateway_agent_list="<list_of_hybrid_cloud_gateway_agents>"
            [-named_credential="named_credential"]
            [-named_credential_owner="named_credential_owner"]
            [-cloud_hostname="cloud_hostname"]
            [-ignore_central_agent_check]
            [-ignore_network_check]
            [-ssh_port="ssh_port"]
            [-timeout="timeout"]
   ```

   Script/Interactive Mode

   ```
       $<emcli_install_location>/bin/emcli
   register_hybridgateway_agent(hybridgateway_agent_list="<list_of_hybrid_clou
   d_gateway_agents>"
            [,named_credential="named_credential"]
            [,named_credential_owner="named_credential_owner"]
            [,cloud_hostname="cloud_hostname"]
            [,ignore_central_agent_check=True/False]
            [,ignore_network_check=True/False]
            [,ssh_port="ssh_port"]
            [,timeout="timeout"]
           )
   ```

   For more information about the `register_hybridgateway_agent` verb, see the *Enterprise Manager Command Line Interface Guide*.

   Options:

   - *hybridgateway_agent_list*

     List of Management Agents that need to be registered as Gateways. You can specify more than one Management Agent (host name and port combination). Ensure that you

specify the fully qualified name for the Management Agents, and separate the Management Agent names using a space.

Multiple Gateways are only needed for failover and load balancing and are not mandatory. Multiple Gateways can be added at initial Hybrid Cloud setup or can be added at a later point in time. See Configuring Cloud-based Agents for High Availabilityfor more information.

- *named_credential*

  Named credential used to make SSH connection to the cloud host. This is used for the network check.

  *Optional only if '-ignore_network_check' is present..

- *named_credential_owner*

  Owner of named credential.

  *Optional only if '-ignore_network_check' is present.

- *cloud_hostname*

  Cloud hostname where you want to install hybrid agent.

  *Optional only if '-ignore_network_check' is present.

- *ignore_central_agent_check*

  Flag used to skip the central Agent check for the specified list of Agents. We recommend not registering the Agent on the OMS host as a Gateway. However, you can use this flag to ignore that check.

- *ignore_network_check*

  Flag used to skip the network check for the specified list of Agents. Use this flag only if you are sure that the network connection works from Gateway to the cloud host.

- *ssh_port*

  Specifies the SSH port used to check network. 22 is used as the default.

- *timeout*

  Specifies the amount of time (in seconds) the network check process will wait for a connection. 5 seconds is the default.

Example 1: Basic Command Usage

Standard Mode

```
emcli register_hybridgateway_agent -hybridgateway_agent_list="agent1:port
agent2:port..."
     -named_credential="named_credential"
     -named_credential_owner="named_credential_owner"
         -cloud_hostname="cloud_hostname"
```

Interactive or Script Mode

```
register_hybridgateway_agent(hybridgateway_agent_list="agent1:port
agent2:port...",
             named_credential="named_credential",
             named_credential_owner="named_credential_owner",
             cloud_hostname="cloud_hostname"           )
```

Example 2: If the '-ignore_network_check' flag is present, the parameters '-named_credential', '-named_credential_owner' and '-cloud_hostname' are not required.

Standard Mode

```
emcli register_hybridgateway_agent -hybridgateway_agent_list="agent1:port
agent2:port..." -ignore_network_check -ignore_central_agent_check
```

Interactive or Script Mode

```
register_hybridgateway_agent(hybridgateway_agent_list="agent1:port
agent2:port...",
             ignore_network_check=True,
             ignore_central_agent_check=True
           )
```

Example 3: . If the '-ignore_central_agent_check' flag is present, but the '-ignore_network_check' flag is missing, the parameters '-named_credential', '-named_credential_owner' and '-cloud_hostname' are required.

Standard Mode

```
emcli register_hybridgateway_agent -hybridgateway_agent_list="agent1:port
agent2:port..." -named_credential="named_credential" -
named_credential_owner="named_credential_owner" -
cloud_hostname="cloud_hostname" -ignore_central_agent_check
```

Interactive or Script Mode

```
register_hybridgateway_agent(hybridgateway_agent_list="agent1:port
agent2:port...",
             named_credential="named_credential",
             named_credential_owner="named_credential_owner",
             cloud_hostname="cloud_hostname",
             ignore_central_agent_check=True
           )
```

3. Verify that the Management Agent has been configured as a Gateway. You can do this only while installing an Agent on an Oracle Cloud VM as described in Installing an Agent on an Oracle Cloud VM Using the Add Host Targets Wizard.

Prerequisites for Installing Agents on Oracle Cloud VMs

Before deploying Agents on your Oracle Cloud VMs, ensure that the following prerequisites have been met:

- Ensure that the CPU, RAM, and hard disk space requirements are met.

  The CPU, RAM, and hard disk space requirements for a Hybrid Cloud Agent are described in *Oracle Enterprise Manager Basic Installation Guide.*

- Ensure that you configure at least one Management Agent to act as a Gateway. A Gateway provides a communication channel between the Oracle Cloud VMs and the on-premises OMS.

For information on how to configure Management Agent version 24ai to act as a Gateway, see Configuring a Management Agent as a Gateway.

- Ensure that port 22 is open on the destination Oracle Cloud virtual host (the virtual host on which you want to install an Agent), and the SSH daemon process must be running on it. To verify whether the SSH Daemon process is running on the destination virtual host, run the following command from the virtual host:

  ```
  ps -ef | grep sshd
  ```

  > **Note:**
  >
  > If the SSH daemon is configured and running other than on the default port 22, then make sure the SSH port number is updated in the `$MW_HOME/oui/prov/resources/Paths.properties` file. For example, if the SSH daemon is running on port 23, then update the parameter `SSH_PORT` in the Paths.properties file and proceed with deployment.

- Ensure that port 1748, or at least one port in the range 1830 - 1848 is free on every destination Oracle Cloud virtual host.

  By default, Enterprise Manager uses port 1748 as the Gateway Proxy port. If port 1748 is not free, the application uses a free port in the range 1830 - 1848.

- Ensure that the user installing the Agent on the Cloud VM er has the *root* privileges to run the `root.sh` script. If the user installing this Agent does not have the *root* privileges, ensure that you run the `root.sh` script manually on all the destination virtual hosts, after the deployment operation. Make sure to have a write permission on the directory.
- Meet the prerequisites required for deploying on-premises Management Agents, as described in *Oracle Enterprise Manager Basic Installation Guide*.
- Ensure that the Cloud-based Agent is deployed only on an Oracle Linux x86-64 operating system. It is supported only on Oracle Linux x86-64 operating system.
- To install an Agent on a Cloud-based virtual host, it is recommended to install it on the local file system of the virtual host. Optionally, you can create a mount using an external storage device and install the Agent on it. Otherwise, you will lose all the data that is stored in the boot volume every time you stop, start, or restart the virtual host.
- Ensure that you do not modify the domain name in the Virtual Machine (VM) network or host configuration settings. The Agent must be used only for Oracle Cloud-hosted VMs, so if you change the VM domain name to reflect a non-Oracle Cloud-hosted VM, then the Agent deployment will fail.

  To verify this, log in to the VM and run the `hostname -d` command, and ensure that the output contains `oracle.com`, `oraclecloud.com`, or `oraclecloud.internal`. If you see any other domain name, remove it from the list.

  Also run the following commands, and ensure that the output contains either `oracle.com` or `oraclecloud.internal`. If you see any other domain name, remove it from the list.

  ```
  cat /etc/sysconfig/network
  ```

  ```
  cat /etc/resolv.conf
  ```

  ```
  cat /etc/hosts
  ```

Installing an Agent on an Oracle Cloud VM

This section covers the following methods to install an Agent on an Oracle Cloud VM:

- Installing an Agent on an Oracle Cloud VM Using EM CLI
- Installing an Agent on an Oracle Cloud VM Using the Add Host Targets Wizard

> **Note:**
>
> Since an Agent connects to the on-premises OMS through an SSH bridge, manual deployment such as Silent Agent Installation is not supported for Cloud-based Agents. You can only deploy Agents using the Add Host Targets Wizard, or EM CLI.
>
> You can deploy a Cloud-based Agent only on an Oracle Linux x86-64 operating system. An Agent configured as a Gateway is supported on all operating systems.

Installing an Agent on an Oracle Cloud VM Using EM CLI

Follow these steps to install a Cloud-based Agent using EM CLI:

1. Log in to EM CLI from the `/bin` directory present within the EM CLI install location:

   ```
   $<emcli_install_location>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

   EM CLI is set up by default on the on-premises OMS host (the EM CLI install location is the OMS home). Hence, if you choose to run EM CLI from the on-premises OMS host, no additional steps are required. This is the recommended option.

   If you choose to run EM CLI from a custom location on a host that is not running the on-premises OMS, you must first set up EM CLI on the required host. For information on how to do so, see *Oracle Enterprise Manager Command Line Interface Guide.*

2. Run the `list_add_host_platforms` verb to obtain a list of the platforms for which the Hybrid Cloud Agent software is available in Self Update:

   ```
   $<emcli_install_location>/bin/emcli list_add_host_platforms
                        [-all]
                        [-noheader]
                        [-script | -format]
   ```

   Note that the parameters mentioned in `[ ]` are optional.

   For example, `$<emcli_install_location>/bin/emcli list_add_host_platforms -all`

   If the Management Agent software for a particular platform is not available, download and apply it using Self Update. For information on how to download and apply the Management Agent software for a platform, see *Enterprise Manager Basic Installation Guide.*

   To view more information on the syntax and the usage of the `list_add_host_platforms` verb, run the following command:

   ```
   $<emcli_install_location>/bin/emcli help list_add_host_platforms
   ```

3. If you want to deploy Agents on the selected Oracle Cloud virtual hosts in a rolling manner, such that the deployment proceeds continuously from one deployment phase to another, ignoring the failed hosts in each deployment phase, specify the following in the `$OMS_HOME/sysman/prov/agentpush/agentpush.properties` file:

   ```
   oracle.sysman.prov.agentpush.continueIgnoringFailedHost=true
   ```

4. Run the `submit_add_host` verb, specifying the `-configure_hybrid_cloud_agent`, `-hybrid_cloud_gateway_agent`, and `-hybrid_cloud_gateway_proxy_port` options to submit the Add Host session and install the Cloud-based Agents:

   ```
   $<emcli_install_location>/bin/emcli submit_add_host
                        -host_names=<list_of_hosts>
                        -platform=<platform_ID>
                        -installation_base_directory=<install_directory_of_agent>
                        -credential_name=<named_credential_for_agent_install>
                        -configure_hybrid_cloud_agent
                        -hybrid_cloud_gateway_agent=<hybrid_cloud_gateway_agent_name>
                        [-
   hybrid_cloud_gateway_proxy_port=<hybrid_cloud_gateway_proxy_port>]
                        [-credential_owner=<named_credential_owner>]
                        [-instance_directory=<agent_instance_directory>]
                        [-port=<agent_port>]
                        [-session_name=<add_host_session_name>]
                        [-deployment_type=<type_of_agent_deployment>]
                        [-privilege_delegation_setting=<privilege_delegation>]
                        [-additional_parameters=<additional_params_for_install>]
                        [-source_agent=<source_agent_for_cloned_agent_install>]
                        [-master_agent=<master_agent_for_shared_agent_install>]
                        [-properties_file=<properties_file_having_inputs>]
                        [-preinstallation_script=<pre_install_script>]
                        [-preinstallation_script_on_oms]
                        [-preinstallation_script_run_as_root]
                        [-postinstallation_script=<post_install_script>]
                        [-postinstallation_script_on_oms]
                        [-postinstallation_script_run_as_root]
                        [-wait_for_completion]
   ```

   Note that the parameters mentioned in `[ ]` are optional.

   For example, `$<emcli_install_location>/bin/emcli submit_add_host -host_names=oc1.example.com -platform=226 -installation_base_directory=/opt/agent -credential_name=oracle -configure_hybrid_cloud_agent -hybrid_cloud_gateway_agent=abc.example.com -hybrid_cloud_gateway_proxy_port=1748`

   This example installs an Agent on the Oracle Cloud virtual host `oc1.example.com` having the platform ID `226`, in the directory `/opt/agent`, using the named credential `oracle`. The deployed Agent will use `abc.example.com` as the Gateway, and use port `1748` to communicate with the Gateway Proxy.

   To view more information on the syntax and the usage of the `submit_add_host` verb, run the following command:

   ```
   $<emcli_install_location>/bin/emcli help submit_add_host
   ```

> **Note:**
>
> Can I deploy more than one Agent on the same Oracle Cloud virtual host?

Installing an Agent on an Oracle Cloud VM Using the Add Host Targets Wizard

Follow these steps to install an Agent on an Oracle Cloud VM using the Add Host Targets Wizard:

1. In Enterprise Manager, from the **Setup** menu, select **Add Target**, then click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets**, then 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_hybrid_cloud_operation_1`
   b. Click **Add** to enter the fully qualified host name (preferred) or IP address and select the platform of the Oracle Cloud virtual host on which you want to install the Agent. The IP address for the virtual host running each of your Oracle Cloud services would have been provided to you by Oracle.

      > **Note:**
      >
      > - Cloud-based Agent deployment is supported for the Linux x86-64 platform only.
      > - You must enter only one IP address per row. Entering multiple addresses separated by a comma is not supported.

      Alternatively, you can click **Load from File** to add the IP addresses that are stored in a file.

      Specify the platform as Linux x86-64 for all the virtual hosts. To do so, you can specify the platform as Linux x86-64 for the first virtual host, then from the **Platform** list, you can select **Same for All Hosts**.
   c. Click **Next**.
3. On the Installation Details page, do the following:
   a. In the Deployment Type section, select **Fresh Agent Install**.
   b. From the table, select the first row that indicates the virtual hosts grouped by their common platform name.
   c. In the Installation Details section, provide the installation details common to the virtual hosts selected in Step 3 (b). For **Installation Base Directory**, enter the absolute path to the base directory on the Oracle Cloud virtual host where you want the software binaries, security files, and inventory files of the Hybrid Cloud Agent to be copied.

      For example, `/u01/app/Oracle/`.

      If the path you enter does not exist, the application creates a directory at the specified path, and copies the Agent software binaries, security files, and inventory files there.
   d. For **Instance Directory**, accept the default instance directory location or enter the absolute path to a directory of your choice where all Agent-related configuration files can be stored.

For example, `/u01/app/Oracle/agent_inst`.

If you are entering a custom location, then ensure that the directory has *write* permissions. Oracle recommends that you 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 Agent-related configuration files there.

e. For **Named Credential,** select the named credential that you want to use to set up SSH connectivity between the on-premises OMS and the destination Oracle Cloud virtual hosts, and to install a Agent on each of the Oracle Cloud virtual hosts. Starting with Enterprise Manager 13c Release 2, you can create SSH key named credentials directly from the wizard so there's no need to pre-create the credentials.

   Ensure that you only specify a named credential that uses SSH public key authentication. Password based authentication is not supported. Also, note that deploying Cloud-based Agents using a locked user account (by switching to the locked user account using a privilege delegation provider) is not supported.

   For information on how to create a named credential that uses SSH public key authentication, see Prerequisites for Installing Agents on Oracle Cloud VMs.

f. For **Privileged Delegation Setting**, use the default value. Privilege delegation providers and locked accounts are not supported for Agent deployment.

   If the Agent install user has *root* privileges, then `root.sh` is run automatically on the destination virtual hosts post deployment. Else, you must manually run `root.sh` on every destination virtual host post deployment.

g. For **Port**, accept the default port (3872) that is assigned for the 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 automatically assigns the first available free port within the range of 1830 - 1849.

h. If you want to run certain scripts before or after deploying the Agents, in the Optional Details section, enter the absolute path to the locations where the scripts that you want to run are available. Note that only shell scripts are supported, and only one pre-installation or one post-installation 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 the on-premises OMS is running and is not on the virtual host where you want to install the Agent, then select **Script on OMS**. In this case, the script will be copied from the on-premises OMS host to the destination virtual hosts, and then run on the destination virtual hosts.

i. If you want to specify certain additional parameters for the deployment, in the Optional Details section, for **Additional Parameters**, enter a white space-separated list of the additional parameters.

   For example, provide the following path:

   ```
   INVENTORY_LOCATION=/u01/app/oracle/oraInventory
   ```

   However, note that this parameter is supported only on UNIX platforms, and not on Microsoft Windows platforms.

j. Select **Configure Hybrid Cloud Agent** to specify the details for the Gateway that the Cloud-based Agent must communicate with.

   For **Hybrid Cloud Gateway,** specify the Management Agent within your enterprise that you want to use as a Gateway for the Cloud-based Agent to communicate with. Click

the magnifying glass icon, and select a Hybrid Cloud Gateway from the displayed list (only those Gateways that are up and running are displayed).

Note that for this field, you can only select a Management Agent that has already been designated as a Gateway. For information on how to designate a particular Management Agent as a Gateway, see Configuring a Management Agent as a Gateway.

For **Hybrid Cloud Gateway Proxy Port,** specify the port for communication between the Cloud-based Agent and the Gateway Proxy. If you do not specify a value, port 1748 is used, and if port 1748 is not free, then a free port between 1830 and 1848 is used.

k. Click **Next**.

4. On the Review page, review the details you have provided for the installation and if you are satisfied with the details, then click **Deploy Agent** to install the 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 Agent Deployment Details page that enables you to monitor the progress of the deployment session. To understand the tasks you can perform on this page, click **Help**.

5. To verify that the Agent was deployed on Oracle Cloud, from the **Setup** menu, select **Manage Enterprise Manager,** then select **Agents.** Search for, then click the name of the Cloud-based Agent to access its home page. Beside the Agent target name, *Running in Oracle Cloud,* and a cloud icon must be displayed.

> **Note:**
>
> The following features are not supported, or are partially supported for Cloud-based Agents:
>
> - Buddy Agent
> - Management Agent to Management Agent communication
> - Distributed Software Library
> - Target Relocation
> - Support for third party Management Agent certificates
> - Support Workbench

> **Note:**
>
> Can I deploy more than one Agent on the same Oracle Cloud virtual host?

Advanced Topics

Topics

- Discovering and Monitoring Oracle Cloud Targets

Discovering and Monitoring Oracle Cloud Targets

Once the Hybrid Cloud is deployed in the on-premises environment and the Agent is deployed in the Oracle Cloud environment, the Oracle Cloud virtual hosts become manageable targets in Enterprise Manager. To discover and monitor the targets running on these manageable virtual hosts, you should follow the instructions outlined in Oracle Enterprise Manager Administrator's Guide. The procedure to discover and promote the targets running on an Oracle Cloud virtual host is the same as the procedure to discover and promote targets running on any normal host in the on-premises environment.

However, for discovering Fusion Middleware domains running on Oracle Cloud virtual hosts, such as WebLogic JCS domains, you should use the public IP address and port 9001 (representing the custom t3 channel that is configured by default on these Admin Servers).

To find out more about cloning in Hybrid Cloud, see the chapter on cloning solutions in the *Enterprise Manager Lifecycle Management Administrator's Guide*.

Patching Cloud-based Agents and Gateways

You can patch Agents installed on Oracle Cloud VMs and Gateways using patch plans. Patch plans are consolidated plans that include one or more patches to be rolled out as a group. The patching procedure remains the same for normal Management Agents, Agents installed on Oracle Cloud VMs, and Gateways.

> **Caution:**
>
> The database instance created on Oracle Cloud before the first week of June 2015 is typically based on the database patchset update released in January 2015 (Jan DB PSU). If you want to patch such a database instance with the database patchset update released in April 2015 (Apr DB PSU), then as a prerequisite, before you apply the patchset update, create the following file and add the absolute path to the directory where the Cloud-based Agent is available.
>
> `/var/opt/oracle/patch/files_to_save.ora`
>
> If you do not follow the aforementioned instruction, you will notice that the Cloud-based Agent in /u01/app/oracle is automatically moved to /u01/app.ORG/oracle as part of the database patching process. You will then have to manually copy the directory back to its original location. To circumvent this issue and avoid any manual effort from your end, Oracle recommends that you follow the aforementioned instruction to create a file as described and add the Cloud-based Agent location to it.

To patch Agents on the Oracle Cloud virtual hosts, follow these steps:

1. If the patch you are applying accesses the `sbin` directory of the agent home, then first follow the instructions outlined in the ReadMe file of the patch.

2. For scalability and performance, use Gold Image based patching to patch Hybrid Agents. For more information on upgrading agents using Gold Image, see the *Oracle Enterprise Manager Upgrade Guide*.
3. Patch the Agents by following the instructions outlined in Patch Management from the *Oracle Enterprise Manager Lifecycle Management Guide*. The patching procedure remains the same for normal Management Agents and Hybrid Cloud Agents.

To patch Agents configured as Gateways, follow the instructions outlined in *Oracle Enterprise Manager Lifecycle Management Guide*.

> **Note:**
>
> Once the first Gateway is up after being patched, will it monitor the Cloud-based Agents?

Configuring an External Proxy to Enable Gateways to Communicate with the Oracle Cloud

For security, you can optionally configure external proxies between the Cloud-based Agents and the Gateway. However, only proxies that support tunneling (for example, SOCK4, SOCK5, HTTP) are supported.

To configure an external proxy between a Cloud-based Agent and a Gateway, follow these steps:

1. Set up a proxy server. HTTP, SOCKS4, and SOCKS5 proxy servers are supported. Ensure that the proxy server supports tunneling.
2. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Agents.**
3. Search for and click the name of the Gateway for which you want to configure an external proxy. You should select an Agent from the list for which the 'register' command has been executed.
4. From the **Agent** menu, select **Properties.**
5. From the **Show** menu, select **Basic Properties.** For **externalProxyPort,** specify the communication port that must be used to connect to Oracle Cloud.

   Click **Apply.**
6. From the **Show** menu, select **Advanced Properties.** Expand the Runtime Settings section. For **externalProxyHost,** specify the host name of the proxy. For **externalProxyType,** select whether the proxy uses **HTTP, SOCKS4,** or **SOCKS5** for communication.

   If the proxy server that you set up requires user name and password authentication, specify values for **externalProxyUsername** and **externalProxyPassword.**
7. Click **Apply.**
8. Verify the external proxy without authentication. To do so, run the following command:

   ```
   ssh -l <user> -i <path_to_private_key> -o "ProxyCommand /usr/bin/nc -X connect
   -x <proxy host>:<proxy port> %h %p" <oracle_cloud_host> "<test command>"
   ```

Performing Additional Hybrid Cloud Management Tasks

This section describes the additional Hybrid Cloud Management tasks that you can perform. It consists of the following:

- Configuring Cloud-based Agents for High Availability
- Disabling Gateways
- Disassociating Gateways from a Cloud-based Agent
- Decommissioning Cloud-based Agents

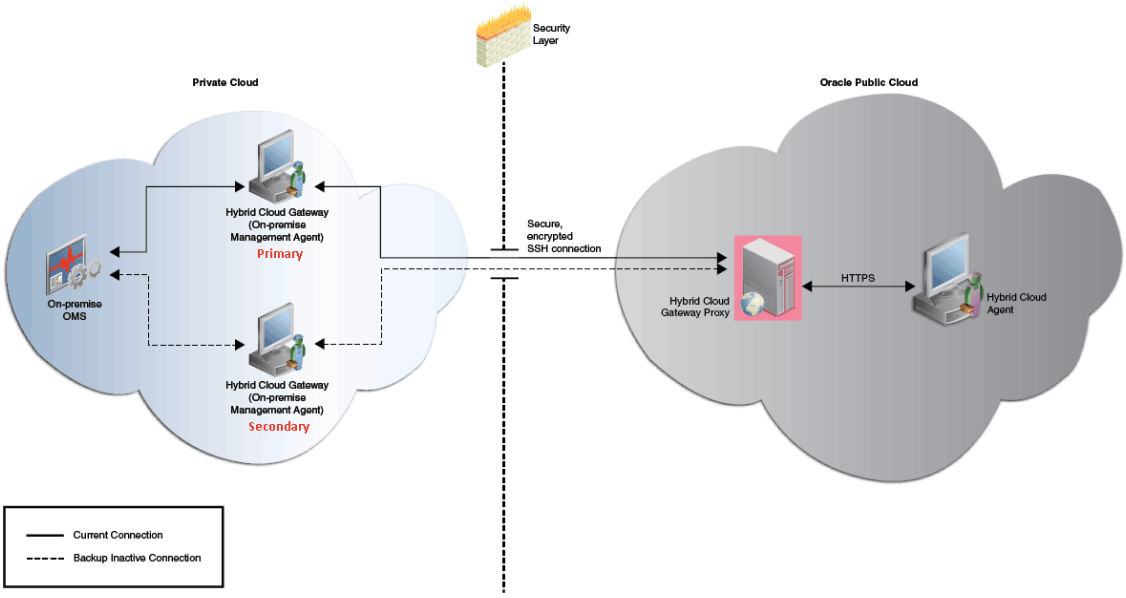
Configuring Cloud-based Agents for High Availability

When you deploy an Agent on an Oracle Cloud VM, you associate it with a single Gateway by default. Throughout the lifecycle of the Cloud-based Agent, the Agent is dependent on the Gateway to forward the collected monitoring data to the on-premises OMS. Hence, if the Gateway is down or is not reachable, the Cloud-basedAgent monitoring data will not reach the on-premises OMS. Thus, Oracle recommends that you enable every Cloud-based Agent to use multiple Gateways to decrease the probability of a loss in monitoring data.

While deploying an Agent to the Oracle Cloud, the first Gateway that you select is designated as the *primary Hybrid Cloud Gateway.* If you enable the deployed Agent to use additional Gateways, then the additional Gateways are designated as *secondary Hybrid Cloud Gateways.* This way, if the *primary Hybrid Cloud Gateway* for a Cloud-based Agent is down or is unreachable, then one of the *secondary Hybrid Cloud Gateways* takes over. If the *secondary Hybrid Cloud Gateway* that took over also goes down or becomes unreachable at some point of time, then the next available *secondary Hybrid Cloud Gateway* takes over.

Figure 11-1 depicts the communication from the Hybrid Cloud Agents to the on-premises OMS through multiple Hybrid Cloud Gateways.

Figure 11-1 Communication from the Hybrid Cloud Agents to the On-Premise OMS Using Multiple Hybrid Cloud Gateways for High Availability



To configure a Cloud-based Agent for high availability, you must associate one or more *secondary Hybrid Cloud Gateways* with the Cloud-based Agents. To do so, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the EM CLI install location:

   ```
   $<emcli_install_location>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

   EM CLI is set up by default on the on-premises OMS host (the EM CLI install location is the OMS home). Hence, if you choose to run EM CLI from the on-premises OMS host, no additional steps are required. This is the recommended option.

   If you choose to run EM CLI from a custom location on a host that is not running the on-premises OMS, you must first set up EM CLI on the required host. For information on how to do so, see *Oracle Enterprise Manager Command Line Interface Guide.*

2. Associate *secondary Hybrid Cloud Gateway(s)* with a Hybrid Cloud Agent.

   ```
   $<emcli_install_location>/bin/emcli add_hybridgateway_for_hybrid_agent
   -hybrid_agent_name="<hybrid_cloud_agent>:<port>" -
   hybridgateway_agent_list="<secondary1_hybrid_cloud_gateway_agent>:<port>
   <secondary2_hybrid_cloud_gateway_agent>:<port>
   <secondaryN_hybrid_cloud_gateway_agent>:<port>"
   ```

   For example, `emcli add_hybridgateway_for_hybrid_agent -hybrid_agent_name="abc.example.com:1831" –hybridgateway_agent_list="secondary1.example.com:1831 secondary2.example.com:1831"`

   > **Note:**
   >
   > In the `–hybridgateway_agent_list`, you can specify more than one Gateway. Ensure that you specify the fully qualified name for each Gateway, and separate the Gateway names using a space.

> **Note:**
>
> Once the first Gateway is up after being patched, will it monitor the Cloud-based Agents?
>
> How can I redistribute my connections once I have added the Gateways? Does it need reconfiguration?

Disabling Gateways

To disable the gateway functionality of a Gateway, that is, to ensure that a Gateway functions like a regular Management Agent again and does not forward communication from the Cloud-based Agents to the on-premises OMS, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the EM CLI install location:

   ```
   $<emcli_install_location>/bin/emcli login -username=<user_name>
   ```

Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

EM CLI is set up by default on the on-premises OMS host (the EM CLI install location is the OMS home). Hence, if you choose to run EM CLI from the on-premises OMS host, no additional steps are required. This is the recommended option.

If you choose to run EM CLI from a custom location on a host that is not running the on-premises OMS, you must first set up EM CLI on the required host. For information on how to do so, see *Oracle Enterprise Manager Command Line Interface Guide.*

2. Disable the Gateway functionality of a set of Gateways.

```
$<emcli_install_location>/bin/emcli deregister_hybridgateway_agent -
hybridgateway_agent_list="<hybrid_cloud_gateway_agent1>:<port>
<hybrid_cloud_gateway_agent2>:<port> <hybrid_cloud_gateway_agentN>:<port>"
```

For example, `emcli deregister_hybridgateway_agent -hybridgateway_agent_list="abc.example.com:3873 def.example.com:3873"`

Note that for `-hybridgateway_agent_list`, you can specify more than one Hybrid Cloud Gateway. Ensure that you specify the fully qualified name for each Gateway, and separate the Gateway names using a space.

Disassociating Gateways from a Cloud-based Agent

To disassociate Gateways from a Cloud-based Agent, such that the specified Agent does not communicate with the Gateway and the on-premises OMS anymore, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the EM CLI install location:

```
$<emcli_install_location>/bin/emcli login -username=<user_name>
```

Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

EM CLI is set up by default on the on-premises OMS host (the EM CLI install location is the OMS home). Hence, if you choose to run EM CLI from the on-premises OMS host, no additional steps are required. This is the recommended option.

If you choose to run EM CLI from a custom location on a host that is not running the on-premises OMS, you must first set up EM CLI on the required host. For information on how to do so, see *Oracle Enterprise Manager Command Line Interface Guide.*

2. Disassociate Gateways from a Cloud-based Agent.

```
$<emcli_install_location>/bin/emcli delete_hybridgateway_for_hybrid_agent
-hybrid_agent_name="<hybrid_cloud_agent>:<port>" -
hybridgateway_agent_list="<hybrid_cloud_gateway1_agent_to_disassociate>:<port>
<hybrid_cloud_gateway2_agent_to_disassociate>:<port>
<hybrid_cloud_gatewayN_agent_to_disassociate>:<port>"
```

For example, `emcli delete_hybridgateway_for_hybrid_agent -hybrid_agent_name="abc.example.com:1831" -hybridgateway_agent_list="gateway1.example.com:1831 gateway2.example.com:1831"`

> **Note:**
>
> Can I deinstall or deconfigure a Gateway without deinstalling an associated Cloud-based Agent?

Decommissioning Cloud-based Agents

To decommission an Agent installed on an Oracle Cloud VM, follow these steps:

1. Stop the Agent running on the Oracle Cloud VM.
2. On the Agent Home page of the Agent, from the **Agent** menu, select **Target Setup,** then select **Agent Decommission.**

> **Note:**
>
> Can I deinstall or deconfigure a Gateway without deinstalling an associated Cloud-based Agent?

Troubleshooting Cloud-based Management Agents

This section provides tips to issues that you might encounter when installing or working with Management Agents installed on Oracle VMs.

Table 11-1describes the error messages that you might encounter, along with its causes and suggestions.

Table 11-1 Troubleshooting Cloud-based Management Agents

Warnings/Error Messages	Cause or Possible Causes	Solution
`The host names specified include IP addresses or short names. It is advised to provide Fully Qualified Host Names, such as myhost.myco.com, that are persistent over the life of the targets. It is recommended for ease of maintenance and overall security. However, you can choose to ignore this warning and proceed by clicking Next.`	IP address is used in place of fully qualified name.	Click **Continue all hosts.**

Table 11-1 (Cont.) Troubleshooting Cloud-based Management Agents

Warnings/Error Messages	Cause or Possible Causes	Solution
`The requiretty flag is set in the sudoers file on the remote host, and as a result the user will not be able to run sudo over ssh.`	Agent push failure.	Either set the `oracle.sysman.prov.agentpush.enablePty` property to `true` in the `/scratch/aime/mw_41005/oms/sysman/prov/agentpush/agentpush.properties` file, which is present on the OMS host, or disable the `requiretty` flag in the sudoers file. You can also ignore this warning and continue in which case the root.sh, any preinstallation or postinstallation scripts specified with run as root enabled will not be run and you have to run them manually after installation. The other option is click **Continue all hosts.**
`Execution of command/scratch/passagt6/ADATMP_2024-04-06_04-10-01-AM/prereq_stage/core/24.1.0.0.0/oui/bin/runInstaller -prereqchecker -silent -ignoreSysPrereqs -waitForCompletion -prereqlogloc /scratch/passagt6/ADATMP_2024-04-06_04-10-01-AM/prereqlogs -entryPoint oracle.sysman.top.agent_Complete PREREQ_CONFIG_LOCATION=/scratch/passagt6/ADATMP_2024-04-06_04-10-01-AM/prereq_stage/core/24.1.0.0.0/prereqs -J-DFORWARDER_PROXY_PORT=-1 -J-DAGENT_PORT=-1 -J-DALLOW_IPADDRESS=true -J-DAGENT_BASE_DIR=/scratch/passagt6 -J-DSTAGE_LOCATION=/scratch/passagt6/ADATMP_2024-04-06_04-10-01-AM/prereq_stage on host 129.152.134.156 Failed.`	Agent push failure.	1. Check the .bashrc or.cshrc file in the installation user home directory. 2. Comment on the following two lines • export TMP=$TMPDIR • export TEMP=$TMPDIR OR Provide Read/Write/Execute permission to the temd directory.

Table 11-1 (Cont.) Troubleshooting Cloud-based Management Agents

Warnings/Error Messages	Cause or Possible Causes	Solution
`Execution of command /u01/app/oracle/agent/ADATMP_2024-04-25_05-56-23-AM/agentDeploy.sh AGENT_BASE_DIR=/u01/app/oracle/agent -softwareOnly AGENT_MODE=PAAS on host 129.191.1.207 Failed`	Agent push failure.	Include `ignorePrereqs` to additional parameters during the agent deployment.
`When VM is created on Oracle Cloud and user is deploying agent to Oracle Cloud VM. See this error - Port not free [ see this error for range of ports which are actually free ].`	Agent push failure.	Check security rules. Enable compute instance security rule to accept connections on the desired port. Check port connectivity using nc utility to confirm if host:port is accessible from the OMS host.

Frequently Asked Questions About Hybrid Cloud Management

This section provides answers to the following frequently asked questions about Hybrid Cloud Management.

- Can I deploy more than one Agent on the same Oracle Cloud virtual host?
- Can I deinstall or deconfigure a Gateway without deinstalling an associated Cloud-based Agent?
- How do I relocate the Gateway to another host without deinstalling anything else?
- How can I redistribute my connections once I have added the Gateways? Does it need reconfiguration?
- After an Oracle PaaS instance is decommissioned, what happens to the Cloud-based Agent and the related targets?
- If I change my SSH keys on Oracle Cloud, what should I do in Enterprise Manager?
- What are the guidelines for sizing the number of Gateways? What is the indication that my gateway Agent is overloaded?
- Once the first Gateway is up after being patched, will it monitor the Cloud-based Agents?
- What are the user restrictions on Cloud-based Agents and the targets on Oracle Cloud?
- On what operating system can I deploy a Cloud-based Agent and a Gateway?

Can I deploy more than one Agent on the same Oracle Cloud virtual host?

Yes, you can. However, make sure you first decommission the Cloud-based Agent that is already present on the Oracle Cloud virtual host, and then deploy another one.

To decommission the Agent that is already present on the Oracle Cloud virtual host, follow these steps:

1. On the Agent Home page of the Hybrid Cloud Agent, from the **Agent** menu, select **Target Setup,** then select **Agent Decommission.**
2. Deploy a new Agent as described in Installing an Agent on an Oracle Cloud VM.

Can I deinstall or deconfigure a Gateway without deinstalling an associated Cloud-based Agent?

No, you can't. You must first decommission the Agent that is present on the Oracle Cloud virtual host. When you decommission the Agent, the Gateway with which it is associated is automatically removed.

If you have a single Gateway, and if you want to deinstall it, then follow these steps:

1. Stop the Agent running on the Oracle Cloud VM.
2. On the Agent Home page of this Cloud-based Agent, from the **Agent** menu, select **Target Setup,** then select **Agent Decommission.**

If you have multiple Gateways, and if you want to deinstall the *primary Hybrid Cloud Gateway,* then follow these steps:

1. Shut down the *primary Hybrid Cloud Gateway.* This will automatically redirect the communication from the Cloud-based Agent to the *secondary Hybrid Cloud Gateway.*
2. Deinstall the *primary Hybrid Cloud Gateway.*

> **Note:**
>
> No need to decommission the Agent that is associated with the *primary Hybrid Cloud Gateway.* You only have to shut down the *primary Hybrid Cloud Gateway* as described in Step (1).
>
> After Step (2), the *secondary Hybrid Cloud Gateway* will act as the *primary Hybrid Cloud Gateway.*
>
> When you bring back the Hybrid Cloud Gateway that you deinstalled in Step (2), it will come back only as a *secondary Hybrid Cloud Gateway.*

> **Note:**
>
> How do I relocate the Gateway to another host without deinstalling anything else?

How do I relocate the Gateway to another host without deinstalling anything else?

You can't relocate the Gateway from one host to another host because the *relocate* logic is only for targets monitored **by** the Gateway and not for the Gateway.

How can I redistribute my connections once I have added the Gateways? Does it need reconfiguration?

Yes, you can redistribute the connections once you have added additional Gateways. However, there is no automated way to do this. You must manually redistribute the connections.

For example, if you have one Gateway and multiple Cloud-based Agents associated with it, and if you now deploy another Gateway, then you can redistribute the connections between the two gateways.

To do so, follow these steps:

1. Remove the *primary Gateway* from serving the Cloud-based Agent. To do so, run the following command. This command causes the OMS to switch the primary gateway to the secondary gateway.

   ```
   emcli delete_hybridgateway_for_hybrid_agent -
   hybrid_agent_name="<hybrid_agent_name>:<port>" -
   hybridgateway_agent_list="<primary_gateway_agent>:<port>"
   ```

2. Add back the old primary gateway to the Cloud-based Agent. To do so, run the following command. This command restores the old primary gateway as a secondary gateway to the Cloud-based Agent.

   ```
   emcli add_hybridgateway_for_hybrid_agent -
   hybrid_agent_name="<hybrid_agent_name>:<port>" -
   hybridgateway_agent_list="<old_primary_gateway_agent>:<port>"
   ```

After an Oracle PaaS instance is decommissioned, what happens to the Cloud-based Agent and the related targets?

After an Oracle PaaS instance is decommissioned from Oracle Cloud, the associated Agent will be in a *unreachable* state. To clean up the Agent from the Enterprise Manager Console, follow these steps:

1. In the Enterprise Manager Console, from the **Setup** menu, select **Manage Enterprise Manager,** then select **Agents.**
2. Click the name of the Cloud-based Agent you want to clean up from the console.
3. On the Agent Home page, from the **Agent** menu, select **Target Setup,** then click **Agent Decommission.**
4. Select the targets you want to remove, and click **Submit.**

If I change my SSH keys on Oracle Cloud, what should I do in Enterprise Manager?

Update the monitoring credentials with the new SSH keys so that all Cloud-based Agents can automatically honor them for new deployments. Once the new keys are saved, the SSH tunnelling uses the new keys to communicate with the Cloud-based Agents.

To update the monitoring credentials, follow these steps:

1. In the Enterprise Manager Console, from the **Setup** menu, select **Security,** then select **Monitoring Credentials.**
2. On the Monitoring Credentials page, in the table click **Hybrid Cloud Connection.**
3. On the Hybrid Cloud Connection Monitoring Credentials page, select the target name where you want to update the new SSH keys, and click **Set Credentials.**
4. In the Enter monitoring credentials dialog, enter the new SSH private key and the SSH public key, and click **Save.**

What are the guidelines for sizing the number of Gateways? What is the indication that my gateway Agent is overloaded?

Currently, there are no statistics available. You can continue to use utilities such as EM Diag Kit to assess the load on the Hybrid Cloud Gateway.

Once the first Gateway is up after being patched, will it monitor the Cloud-based Agents?

No. The only time there is a switch of a *primary Gateway* is when the *primary Gateway* goes down.

To list the Gateways for a given Cloud-based Agent, run the following query:

```
SELECT emd_url FROM MGMT_TARGETS

WHERE target_name LIKE '%PAAS_AGENT_NAME%' AND

target_type='oracle_hybridcloud_connection'
```

What are the user restrictions on Cloud-based Agents and the targets on Oracle Cloud?

No restrictions as such for users. The Cloud-based Agent install user can be different from the Oracle Cloud target install user, but both users must belong to the same primary operating system group. Otherwise, the discovery might fail.

For example, the Cloud-based Agent install user can be `oci`, and the Oracle Cloud target install user can be `oracle`. However, both these users must belong to the `oinstall` operating system group.

In addition, the user must have sudo access. Otherwise, the root.sh script will have to be run as a manual step during agent deployment.

On what operating system can I deploy a Cloud-based Agent and a Gateway?

You can deploy a Gateway on any operating system, but you must deploy a Cloud-based Agent only on an Oracle Linux x86-64 operating system.

List of Unsupported Features

Table 11-2 lists the features that Hybrid Cloud Management does not currently support.

Table 11-2 Features Not Supported by Hybrid Cloud Management

Targets	Features Not Supported
Database	**Automatic Workload Repository Warehouse** Collection from Oracle Cloud databases. **SQL Performance Analyzer** • Remote trials to Database Cloud Service instances. • Copy of workload artifacts *(capture files/STS)* to Oracle Cloud using deployment procedures. Workaround is to manually copy. • Active Data Guard support for Database Cloud Service instances *(needs a database link)*. **Database Replay** Disabled for database PaaS targets. **Reorganized Objects** Reorganized objects. **Change Management** Data Synchronization. **Database Cloning** **Data Guard** Management of standby databases on Oracle Cloud.
Oracle Exadata Cloud	• Oracle Exadata hardware and hypervisor monitoring, configuration settings. • Patching and upgrade. • Backup and restore. • Provisioning database services in Oracle Cloud.
Enterprise Manager	• Agent: - Manual deployment. - Buddy Agents. Sudo and Run As Different User • Target Relocation. • Software Library on Oracle Cloud. • Third-party certificates. • Support workbench of Oracle Cloud targets.

12

Deploying JVMD for Hybrid Cloud

This chapter describes how to deploy Java Virtual Machine Diagnostics (JVMD) Agents in a Hybrid Cloud setup. It consists of the following sections:

Overview of Deploying JVMD for Hybrid Cloud

Enterprise Manager offers Hybrid Cloud Management that enables you to monitor certain Oracle Cloud targets using an on-premise Enterprise Manager instance. Leveraging this feature, Enterprise Manager enables you to deploy JVMD Agents on your Oracle Cloud virtual hosts, which can report to a JVMD Engine deployed on-premise. Thus, you can monitor your Oracle Cloud JVM targets and diagnose performance problems in Java applications that are deployed in Oracle Cloud, using an on-premise Enterprise Manager instance.

For more information on the Hybrid Cloud feature, see Enabling Hybrid Cloud Management .

The deployed JVMD Agent (on the Oracle Cloud virtual host) uses the Hybrid Cloud Gateway Proxy and a Hybrid Cloud Gateway Agent to communicate with the on-premise JVMD Engine. The Hybrid Cloud Gateway Proxy forwards communication from the JVMD Agent to the on-premise Hybrid Cloud Gateway Agent, which in turn forwards the message to the JVMD Engine and from the JVMD Engine back to the JVMD Agent. Reverse communication follows the same flow, that is, the Hybrid Cloud Gateway Agent forwards communication from the JVMD Engine to the Hybrid Cloud Gateway Proxy, which in turn forwards the message to the JVMD Agent.

Note that except cross-tier functions, all JVMD features are supported for a Hybrid Cloud setup.

Prerequisites for Deploying JVMD Agents on Oracle Cloud Virtual Hosts

Before deploying JVMD Agents on Oracle Cloud virtual hosts, ensure that you meet the following prerequisites:

- Deploy a Hybrid Cloud Agent on the Oracle Cloud virtual host on which you want to deploy a JVMD Agent.

  For information on how to deploy a Hybrid Cloud Agent on an Oracle Cloud target, see Enabling Hybrid Cloud Management .
- Meet the prerequisites for deploying an on-premise JVMD Agent. These prerequisites are described in *Oracle Enterprise Manager Basic Installation Guide.*

Deploying JVMD Agents on Oracle Cloud Virtual Hosts

To deploy JVMD Agents on Oracle Cloud virtual hosts, follow these 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.**
3. For **Operation,** ensure that **Deploy** is selected.

   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 discovered WebLogic Administration Servers and Managed Servers (part of all discovered WebLogic domains).

   Select the WebLogic Managed Servers on which you want to deploy JVMD Agents. 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.**

   Click **Next.**
5. To deploy JVMD Agents on Oracle Cloud virtual hosts, select **Configure Hybrid Mode,** and specify the Hybrid Cloud Gateway Proxy host and port that you want to use. When you select **Configure Hybrid Mode,** the value for **Available JVMD Engine** is automatically set to **Other,** as the JVMD Agent connects to the Hybrid Cloud Gateway Proxy, which in turn connects to the JVMD Engine (via the Hybrid Cloud Gateway Agent).

   By default, all JVMD Agents deployed on Oracle Cloud virtual hosts will effectively report to the JVMD Engine marked as the default end point.

   To view the default JVMD end point for all the Hybrid Cloud Gateway Agents deployed in your enterprise, on the Application Performance Management page, select **JVM Diagnostics Engines,** then click **Configure.** Select the Hybrid Gateways Configuration tab. The default JVMD end point is displayed. For information on how to change the default JVMD end point for the Hybrid Cloud Gateway Agents deployed in your enterprise, see Changing the Default JVMD End Point for Hybrid Cloud Gateway Agents.

   Click **Next.**
6. On the Review page, review all the information, then click **Deploy.**

   Once the JVMD Agent deployment is successful, you can verify the deployment by navigating to the Application Performance Management page, and viewing the Application Performance Management Agents section.

Changing the Default JVMD End Point for Hybrid Cloud Gateway Agents

The deployed Hybrid Cloud JVMD Agents use the Hybrid Cloud Gateway Agents to communicate with an on-premise JVMD Engine. The JVMD Engine that is deployed by default with the OMS version 24ai is marked as the default end point for all the Hybrid Cloud Gateway Agents deployed in your enterprise. This means that, effectively, all the deployed Hybrid Cloud JVMD Agents will report to the JVMD Engine that is marked as the default end point. To change the default end point to a different JVMD Engine, or to a load balancer that is configured in your enterprise, follow these steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Application Performance Management.**
2. Select **JVM Diagnostics Engines,** then click **Configure.**
3. Select the Hybrid Gateways Configuration tab. Click the edit icon displayed against **JVMD default end point URL.**
4. If you want to set the default end point to a load balancer that is configured in your environment, select **Load Balancer URL,** then specify the required value. If you want to set the default end point to a different JVMD Engine (that is, different from the default end point), select **JVMD Engine,** then select the required JVMD Engine from the drop down list.

> **Note:**
>
> Typically, all the Hybrid Cloud Gateway Agents deployed in your enterprise are configured for JVMD and are marked with the default JVMD end point. In case a particular Hybrid Cloud Gateway Agent is not marked with the default JVMD end point, select it from the list displayed in the Hybrid Gateways section, then click **Update.**

After Deploying JVMD Agents on Oracle Cloud Virtual Hosts

After deploying JVMD Agents to your Oracle Cloud virtual hosts, verify the deployment as described in *Oracle Enterprise Manager Basic Installation Guide.*

Part VI
Advanced Configuration Tasks

This part describes the advanced configuration tasks you can perform after you have installed Enterprise Manager and have started using the product.

In particular, this part contains the following chapters:

13

Managing the Lifecycle of Agent Gold Images

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager 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, at any point in time, if you want to monitor a target running on a host, you must first convert that unmanaged host to a managed host by installing a Management Agent.

In the past, Enterprise Manager has offered several approaches for installing Management Agents, including the Add Host Targets Wizard, EM CLI, and response files to silently perform the installation. Starting with 13c, Enterprise Manager offers *Agent Gold Images* that can be used for mass-deployment and upgrade of Management Agents in your environment.

An Agent Gold Image represents the ideal state of a Management Agent in a data center managed by Enterprise Manager, having a customized configuration of the desired versions of the Management Agent software, the desired versions of the monitoring plug-ins, and the desired patches.

An Agent Gold Image version is created by an Enterprise Manager user, using a live reference Management Agent that is thoroughly tested and tuned. An Agent Gold Image version can be used to provision new Management Agents or update existing Management Agents on a large number of hosts.

This chapter describes how you can manage the lifecycle of an Agent Gold Image. In particular, this chapter covers the following:

Agent Gold Image Terminology

The following terminologies are commonly used while discussing Agent Gold Images:

- **Agent Gold Image and Agent Gold Image version:** An Agent Gold Image represents the ideal state of a Management Agent in a data center, having customized configurations of

the desired versions of the Management Agent software, the desired versions of the monitoring plug-ins, and the desired patches.

An Agent Gold Image is expected to undergo revisions whenever you plan to upgrade your Management Agents, upgrade the plug-ins deployed on your Management Agents, deploy new plug-ins on your Management Agents, or deploy new patches on your Management Agents or plug-ins. Each of these sequential revisions of an Agent Gold Image is termed as an Agent Gold Image version.

- **Updating a Management Agent:** This can refer to upgrading a Management Agent (that is, upgrading the Management Agent software), deploying new plug-ins on a Management Agent, upgrading the existing plug-ins on a Management Agent, applying Management Agent and plug-in patches, and any combination of these. You can perform any combination of these tasks using Agent Gold Image versions.
- **Current version of an Agent Gold Image:** The up-to-date version of an Agent Gold Image that you want to use to standardize the Management Agents in your enterprise.
- **Restricted version of an Agent Gold Image:** An Agent Gold Image version that must be used only for limited deployment, perhaps for testing purposes, and not for mass deployment. By default, you can deploy or update a maximum of 10 Management Agents using a restricted version of a particular Agent Gold Image. It is recommended that administrators seek the permission of the super administrator before using this gold image version to deploy or update Management Agents. At any given point, for a Management Agent gold image, you can have only one restricted version.
- **Subscribing a Management Agent to an Agent Gold Image:** Associating a Management Agent with a particular Agent Gold Image. This is a prerequisite for updating Management Agents using a particular Agent Gold Image version.
- **Unsubscribing a Management Agent from an Agent Gold Image:** Disassociating a Management Agent from the Agent Gold Image that it subscribes to. Perform this task if you do not want to manage the update operations of a particular Management Agent using an Agent Gold Image anymore.
- **Agent Gold Image compliance:** Out of all the Management Agents subscribed to a particular gold image, the percentage of Management Agents that are on the current version of the Agent Gold Image.

Operations You Can Perform Using an Agent Gold Image

Using an Agent Gold Image, you can perform the following tasks:

- Provision new Management Agents.
- Update any existing Management Agents.
  - Upgrade your Management Agents (that is, upgrading the Management Agent software).
  - Deploy new plug-ins on your Management Agents.
  - Upgrade the existing plug-ins that are deployed on your Management Agents.
  - Deploy patches on your Management Agents.
  - Deploy patches on the plug-ins that are deployed on your Management Agents.
- Check the Agent Gold Image compliance level to identify what percentage of Management Agents in your environment are already associated with an Agent Gold Image, and what percentage are not.

- Track the Agent Gold Image activities, such as the gold image jobs submitted, their status, the start and end time of the activity, and so on.

> **Note:**
>
> You cannot install, update, or upgrade a Shared Agent (NFS Agent) using an Agent Gold Image. For information about Shared Agents, see Overview of Installing Shared Agents.
>
> In addition, you cannot use an unsecure Management Agent to create an Agent Gold Image version. Therefore, always use only a secure Management Agent as the source for creating an Agent Gold Image version.
>
> You cannot subscribe the following Management Agents to an Agent Gold Image:
>
> - Central Agent.
> - Already subscribed Management Agents.
> - Shared Agents (NFS Agents).
> - Unsecure Management Agents.
> - Management Agents on platforms that are different from the platforms on which the Agent Gold Image is available.
>
> The platform is identified by the Oracle home collection, so make sure the Oracle home target is discovered and collected. To do so, On the Home page of the Management Agent, in the Summary section, click **Oracle Home and Patch Details,** and on the following page, click **Refresh Configuration.**

Understanding the Agent Gold Image Console

To access the Agent Gold Image console, from the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**

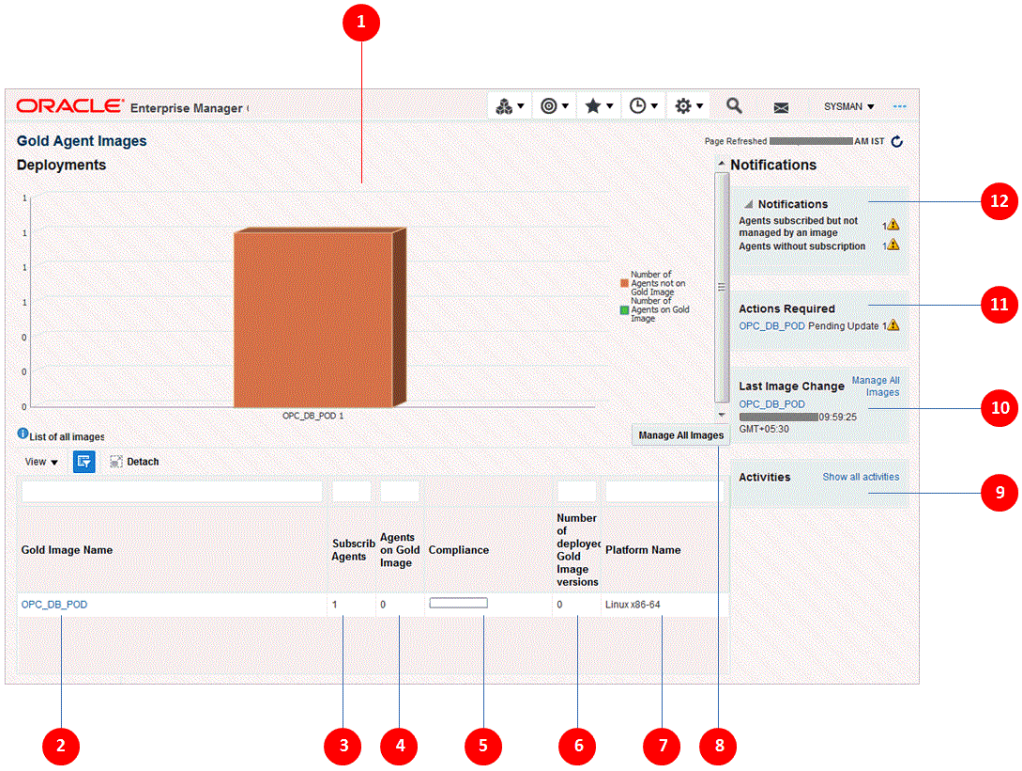


Table 13-1 describes the various parts of the Gold Agent Image Console.

Table 13-1 Description of the Gold Agent Image Console

Number	Description
1	A pictorial representation of the compliance level - out of all the Management Agents that are subscribed to an Agent Gold Image, how many are deployed or updated with a gold image and how many are yet to be deployed or updated with a gold image. Hover your mouse over the graph to see the exact number of Management Agents.
2	Name of the Agent Gold Image. To view more details about an Agent Gold Image, click the gold image. On the Gold Image page, view details of the image versions created for that gold image. Also, for each gold image version, view general details, the associated instance properties, the plug-ins and patches deployed, the activities performed on it, and the stage locations configured for it. **Note:** The Gold Image page lists only those gold image versions that have been set to current (active) or restricted version status. It does not list gold image versions of any other status. If you want to view all the gold image versions of a particular gold image, regardless of their status, then on the Agent Gold Images page, click **Manage Image Versions and Subscriptions.** And on the Manage Image page, click the **Versions And Drafts** tab.
3	Number of Management Agents associated or subscribed to the Agent Gold Image. This includes the Management Agents that are not only updated with the gold image but also the ones that are not updated but subscribed to the gold image. Subscribing Management Agents to a gold image is a prerequisite for updating Management Agents with a particular gold image version.
4	Number of Management Agents subscribed to a gold image and also updated with that gold image.
5	Percentage of Management Agent on the latest gold image version.

Table 13-1 (Cont.) Description of the Gold Agent Image Console

Number	Description
6	Number of gold image versions subscribed to by the Management Agents. This includes all gold image versions, including the latest version that Management Agents are subscribed to.
7	Platform for which the Agent Gold Image is created.
8	Enables you to manage the Agent Gold Images. You can create, edit, or remove a gold image. You can also view details of the gold images created so far.
9	List of the Agent Gold Image activities, such as the jobs submitted to the Enterprise Manager job system, their status, the time at which the activity began, the time at which the activity ended, and so on.
10	Name of the Agent Gold Image and the date and time when they were last changed.
11	List of Agent Gold Images that have pending updates.
12	List of notifications related to Agent Gold Images.

Understanding the Management Agent Base Directory Structure

This section illustrates the base directory structure of a Management Agent that is provisioned, upgraded, or updated using a gold image. It consists of the following:

- Agent Base Directory Structure After a Management Agent Is Provisioned Using a Gold Image
- Agent Base Directory Structure After Upgrade or Update to 24ai Using a Gold Image

Agent Base Directory Structure After a Management Agent Is Provisioned Using a Gold Image

The following is the agent base directory structure of a Management Agent that is provisioned using a gold image.

```
<agent_base_directory>
    |_____agent_24.1.0.0.0
          |_____bin
          |_____sysman
          |_____root.sh
          |_____agent.rsp
          |_____oraInst.loc
          |_____plugins
          |_____OPatch
          |_____oracle_common
          |_____cfgtoollogs
          |_____perl
          |_____stage
          |_____ocm
          |_____lib
          |_____inventory
          |_____install
          |_____config
          |_____EMStage
          |_____.
          |_____.
          |_____.
```

```
|_____oraInventory
|_____agent_inst
|_____sbin
|_____plugins.txt
|_____plugins.txt.status
|_____agentimage.properties
```

Agent Base Directory Structure After Upgrade or Update to 24ai Using a Gold Image

The following is the agent base directory structure of a Management Agent that is upgraded or updated using a gold image.

```
<agent_base_directory>
    |_____GoldImage_<gold_image_name>
         |_____agentInstall.rsp
         |_____agent_24.1.0.0.0
         |_____agentimage.properties
         |_____backup_agtup
         |_____plugins.txt
         |_____plugins.txt.status
    |_____agent_inst
    |_____agentimage.properties
    |_____core
    |_____plugins
    |_____plugins.txt
    |_____plugins.txt.status
    |_____sbin
         |_____cfgtoollogs
         |_____install
         |_____inventory
         |_____oraInst.loc
         |_____.
         |_____.
         |_____.
```

Managing the Lifecycle of an Agent Gold Image

> **Note:**
>
> To view a visual demonstration on Agent Gold Image console and its operations, access the following URL and click **Begin Video.**
>
> `https://apexapps.oracle.com/pls/apex/f?p=44785:24:0:::24:P24_CONTENT_ID,P24_PREV_PAGE:12891,1`

You can perform the following lifecycle management operations for an Agent Gold Image:

- Creating an Agent Gold Image
- Editing an Agent Gold Image
- Deleting an Agent Gold Image
- Creating an Agent Gold Image Version
- Deleting an Agent Gold Image Version

- Staging an Agent Gold Image Version
- Setting a Particular Agent Gold Image Version as the Current Version
- Setting a Particular Agent Gold Image Version as the Restricted Version
- Subscribing Management Agents to an Agent Gold Image
- Unsubscribing Management Agents from an Agent Gold Image
- Provisioning Management Agents Using an Agent Gold Image
- Updating Management Agents Using an Agent Gold Image Version

Creating an Agent Gold Image

To create an Agent Gold Image, use either of the following methods:

- Creating an Agent Gold Image Using the Gold Agent Images Home Page
- Creating an Agent Gold Image Using EM CLI

Creating an Agent Gold Image Using the Gold Agent Images Home Page

To create an Agent Gold Image, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click **Manage All Images.**
3. Click **Create.**
4. Specify the gold image name, a description (optional), and the platform of the source Management Agent that you want to use to create the Agent Gold Image versions. Ensure that you use only a standalone Management Agent as the source, and not a central agent.
5. Click **Submit.**

Creating an Agent Gold Image Using EM CLI

When you create an Agent Gold Image version using EM CLI, the Agent Gold Image gets automatically created.

To create an Agent Gold Image by creating an Agent Gold Image version using EM CLI, see Creating an Agent Gold Image Version Using EM CLI

Editing an Agent Gold Image

> **Note:**
>
> You can only edit an Agent Gold Image if you haven't created any Agent Gold Image versions.

To edit an Agent Gold Image, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**

2. Click **Manage All Images.**
3. Select the gold image that you want to edit, then click **Edit.**
4. Edit the gold image name, description, and platform details.
5. Click **Submit.**

Deleting an Agent Gold Image

> **Note:**
>
> You can only delete an Agent Gold Image if you have not created any Agent Gold Image versions.

To delete an Agent Gold Image, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click **Manage All Images.**
3. Select the gold image that you want to delete, then click **Remove.**

Creating an Agent Gold Image Version

To create an Agent Gold Image version, use either of the following methods:

- Creating an Agent Gold Image Version Using the Gold Agent Images Home Page
- Creating an Agent Gold Image Version Using EM CLI

Creating an Agent Gold Image Version Using the Gold Agent Images Home Page

To create an Agent Gold Image version, follow these steps:

> **Note:**
>
> You cannot use unsecure Management Agents to create an Agent Gold Image version. Therefore, always use only secure Management Agents. Before creating an Agent Gold Image version, meet the hardware requirements. See*Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.
>
> If the configuration properties of the source Management Agent were changed for some reason in the emd.properties file, then before creating an agent gold image version using that source Management Agent, reload the configuration properties of that Management Agent. To do so, run the following command:
>
> ```
> emctl reload agent
> ```

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**

2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Versions and Drafts** tab, then from the **Actions** menu, select **Create.**
5. Specify an image version name, and a description for the image version, if required.

   When you create an image version and update a Management Agent with it, Enterprise Manager uses the image version name you provide here to create a subdirectory in the agent base directory for the Management Agent being updated.

   For example, if the agent base directory of the Management Agent being updated is `/u01/software/em24/agentbasedir`, and the agent home is `/u01/software/em24/agentbasedir/agent_24.1.0.0.0`, and if you provide `OPB_BP1` as the image version name, then when you update the Management Agent with the image version, a new subdirectory `/u01/software/em24/agentbasedir/GoldImage_OPB_BP1/agent_24.1.0.0.0` is created. The word limit for the image version name is 20 characters.
6. If you want to create the gold image version using a source Management Agent, for **Create image by,** select **Selecting a source agent,** then specify the source Management Agent that you want to use. In this case, you can also specify the following:

   - Work Directory: The working directory that must be used to create the Agent Gold Image. The default working directory is `$AGENT_INSTANCE_HOME/install`. Ensure that you have minimum 750MB space in this location.
   - Configuration Properties: The Management Agent configuration properties separated by a semicolon (;) that must be captured while creating the Agent Gold Image. The names of these properties can be found in the `$AGENT_INSTANCE_HOME/sysman/config/emd.properties` file.
   - Exclude Files: The list of files that you want to exclude from the Agent Base Directory of the source agent while creating the Agent Gold Image. Ensure that you provide the complete file path. If there are two or more files, then separated them by a semicolon (;).

   However, if you want to create the gold image version by importing an existing gold image version, for **Create image by,** select **Importing an image,** then specify the location of the gold image version that you want to import. In order to be able to import an image, the image should already be staged. If you have not already staged the image for this purpose, then stage it as described in Staging an Agent Gold Image Version Using Gold Agent Images Home Page.
7. Click **OK.**

   A job that creates the Agent Gold Image version is submitted to the Enterprise Manager job system. You can view the status of this job on the Gold Agent Image Activities page, in the Image Activities tab.

Creating an Agent Gold Image Version Using EM CLI

To create an Agent Gold Image version using EM CLI, follow these steps:

> **Note:**
>
> You cannot use unsecure Management Agents to create an Agent Gold Image version. Therefore, always use only secure Management Agents. Before creating an Agent Gold Image version, meet the hardware requirements. See *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.
>
> If the configuration properties of the source Management Agent were changed for some reason in the emd.properties file, then before creating an agent gold image version using that source Management Agent, reload the configuration properties of that Management Agent. To do so, run the following command:
>
> ```
> emctl reload agent
> ```

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `create_gold_agent_image` verb to create an Agent Gold Image using the specified source Management Agent or by importing an already created image from another Enterprise Management System:

   ```
   $<OMS_HOME>/bin/emcli create_gold_agent_image
           -image_name="gold_image_name"
           -version_name="gold_image_version_name"
           -source_agent|-import_location="source_agent|import_location"
           [-gold_image_description="gold_image_description"]
           [-working_directory="working_directory_location"]
           [-config_properties= " agent_configuration_properties"]
           [-exclude_files= "list_of_files_directories_to_exclude"]
   ```

   Note that the parameters mentioned in `[ ]` are optional.

   Table 13-2 lists and describes the parameters supported for creating an Agent Gold Image version using EM CLI.

Table 13-2 Supported Parameters for Creating an Agent Gold Image Version

Parameter	Description
`-image_name`	Agent Gold Image name to which the created Agent Gold Image must be added.

Table 13-2 (Cont.) Supported Parameters for Creating an Agent Gold Image Version

Parameter	Description
-version_name	Version name of the Agent Gold Image. When you create an image version and update a Management Agent with it, Enterprise Manager uses the image version name you provide here to create a subdirectory in the agent base directory for the Management Agent being updated. For example, if the agent base directory of the Management Agent being updated is /u01/software/em24/agentbasedir, and the agent home is /u01/software/em24/agentbasedir/agent_24.1.0.0.0, and if you provide OPB_BP1 as the image version name, then when you update the Management Agent with the image version, a new subdirectory /u01/software/em24/agentbasedir/GoldImage_OPB_BP1/agent_24.1.0.0.0 is created. The word limit for the image version name is 20 characters.
-source_agent	Management Agent to be used as the source to create the Agent Gold Image. To view a list of the Management Agents that can be used as a source to create a gold image, run emcli get_targets -target="oracle_emd".
-import_location	Location where the Agent Gold Image is staged for creating the gold agent image version. This location is accessible from all the OMS instances.
-gold_image_description	Description of the Agent Gold Image.
-working_directory	Working directory to be used to create the Agent Gold Image. The default working directory is $AGENT_INSTANCE_HOME/install. Minimum free space required is 1 GB.
-config_properties	Management Agent configuration properties separated by \";\" that must be captured while creating the Agent Gold Image. For example, MaxThread;GracefulShutdown.
-exclude_files	List of files or directories separated by \";\" that must be excluded from the gold agent image version. For example, agent_24.1.0.0.0/cfgtoollogs/agentDeploy;agent_24.1.0.0.0/oui. Ensure that you provide only the relative path to the files and directories and not the absolute path.

Examples:

- The following example creates an Agent Gold Image OPC_AGI_DB_JUL_13, using example.com:3872 as the source Management Agent, and adds the gold image version to the gold image OPC_DB_MONITORING:

```
$<OMS_HOME>/bin/emcli create_gold_agent_image -source_agent=example.com:3872 -
version_name=OPC_AGI_DB_JUL_13 -image_name=OPC_DB_MONITORING
```

- The following example creates an Agent Gold Image OPC_AGI_DB_JUL_13, using example.com:3872 as the source Management Agent, /tmp as the working directory, and adds the gold image version to the gold image OPC_DB_MONITORING:

```
$<OMS_HOME>/bin/emcli create_gold_agent_image -source_agent=example.com:3872 -
version_name=OPC_AGI_DB_JUL_13 -image_name=OPC_DB_MONITORING -
working_directory=/tmp
```

- The following example creates an Agent Gold Image OPC_AGI_DB_JUL_13 using gold image software staged at import location /abc/stage:

```
$<OMS_HOME>/bin/emcli create_gold_agent_image -import_location=/abc/stage -
version_name=OPC_AGI_DB_JUL_13 -image_name=OPC_DB_MONITORING
```

Deleting an Agent Gold Image Version

To delete an Agent Gold Image version, use either of the following methods:

- Deleting an Agent Gold Image Version Using Gold Agent Images Home Page
- Deleting an Agent Gold Image Version Using EM CLI

Deleting an Agent Gold Image Version Using Gold Agent Images Home Page

To delete an Agent Gold Image version, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager**, then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Versions and Drafts** tab.

> **Note:**
>
> An active (current) image cannot be deleted.

5. Select the gold image version that you want to delete, then from the **Actions** menu, select **Delete.**

Deleting an Agent Gold Image Version Using EM CLI

To delete an Agent Gold Image version using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `delete_gold_agent_image` verb:

   ```
   $<OMS_HOME>/bin/emcli delete_gold_agent_image        -
   version_name="gold_image_version_name_to_delete"
   ```

   Use the `-version_name` parameter to specify the Agent Gold Image version that you want to delete.

   For example, to delete the Agent Gold Image OPC_AGI_DB_JUL_13, run the following:

   ```
   $<OMS_HOME>/bin/emcli delete_gold_agent_image -version_name=OPC_AGI_DB_JUL_13
   ```

Staging an Agent Gold Image Version

To stage a functional Agent Gold Image version on a host, use either of the following methods:

- Staging an Agent Gold Image Version Using Gold Agent Images Home Page
- Staging an Agent Gold Image Version Using EM CLI

Staging an Agent Gold Image Version Using Gold Agent Images Home Page

To stage an Agent Gold Image version on a host, follow these steps:

> **Note:**
>
> Before staging an Agent Gold Image version, meet the hardware requirements. See *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Versions and Drafts** tab. Select the gold image version that you want to stage, then from the **Actions** menu, select **Stage.**
5. Specify the host, and the location on the host where you want to stage the Agent Gold Image version. Click **OK.**

   A job that stages the Agent Gold Image version is submitted to the Enterprise Manager job system. You can view the status of this job on the Gold Agent Image Activities page, in the Image Activities tab.

Staging an Agent Gold Image Version Using EM CLI

To stage an Agent Gold Image version using EM CLI, follow these steps:

> **Note:**
>
> Before staging an Agent Gold Image version, meet the hardware requirements. See *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.*

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.
2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```
3. Run the `stage_gold_agent_image` verb to stage an Agent Gold Image on a destination host:

   ```
   $<OMS_HOME>/bin/emcli stage_gold_agent_image -
   version_name="gold_image_version_to_stage" -image_name="gold_image_name" -
   host_name="staging_destination_host" -
   ```

```
stage_location="stage_location_on_destination_host"
```

Table 13-3 lists and describes the parameters supported for staging an Agent Gold Image version using EM CLI.

Table 13-3 Supported Parameters for Staging an Agent Gold Image Version

Parameter	Description
`-version_name`	Agent Gold Image version that should be staged.
`-image_name`	Agent Gold Image that should be staged.
`-host_name`	Destination host where the Agent Gold Image should be staged. As a prerequisite, a Management Agent should be running on this host.
`-stage_location`	Location on the destination host where the Agent Gold Image should be staged. The location should be a shared location and should be accessible by the Management Agents being updated by that Agent Gold Image. Otherwise, the location should be accessible from the OMS that is used to import the Agent Gold Image from this location. In addition, the minimum free space required is 1 GB.

For example, to stage the Agent Gold Image OPC_AGI_DB_JUL_13 of gold image OPC_AGI_DB, at the stage location `/net/stage/agent` on the host `example.com`, run the following:

```
$<OMS_HOME>/bin/emcli stage_gold_agent_image -version_name=OPC_AGI_DB_JUL_13 -
stage_location=/net/stage/agent -host_name=example.com
```

Setting a Particular Agent Gold Image Version as the Current Version

The up-to-date version of an Agent Gold Image that you want to use to standardize the Management Agents in your enterprise is termed as the *current version* of the Agent Gold Image.

When an Agent Gold Image version is created, it is marked as a draft version. Setting a draft version of an Agent Gold Image as the current version indicates that the gold image version is ready to be used to mass deploy or mass update Management Agents. Once an image is set to Active (Current), you cannot revert it to a draft or a restricted version.

To set a draft version of an Agent Gold Image as the current version, use either of the following methods:

- Setting a Particular Agent Gold Image Version as the Current Version Using Gold Agent Images Home Page
- Setting a Particular Agent Gold Image Version as the Current Version Using EM CLI

Setting a Particular Agent Gold Image Version as the Current Version Using Gold Agent Images Home Page

To set a draft version of an Agent Gold Image as the current version, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**

4. Select the **Versions and Drafts** tab. Select the gold image version that you want to set as the current version, then click **Set Current Version.**

   A job that promotes the Agent Gold Image draft version to the current version is submitted to the Enterprise Manager job system. You can view the status of this job on the Gold Agent Image Activities page, in the Image Activities tab.

Setting a Particular Agent Gold Image Version as the Current Version Using EM CLI

To set a particular Agent Gold Image version as the current version using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `promote_gold_agent_image` verb to promote the Agent Gold Image version to the Current maturity level:

   ```
   $<OMS_HOME>/bin/emcli promote_gold_agent_image -
   version_name="gold_image_version_name" -maturity="Current/Restricted/Draft"
   ```

   The `-version_name` parameter defines the Agent Gold Image that you want to promote.

   The `-maturity` parameter defines the gold image maturity level.

   For example, to promote the Agent Gold Image OPC_AGI_DB_JUL_13 to the Current maturity level, run the following:

   ```
   $<OMS_HOME>/bin/emcli promote_gold_agent_image -version_name=OPC_AGI_DB_JUL_13 -
   maturity=Current
   ```

Setting a Particular Agent Gold Image Version as the Restricted Version

To set a draft or active version of an Agent Gold Image as the restricted version, use either of the following methods:

- Setting a Particular Agent Gold Image Version as the Restricted Version Using Gold Agent Images Home Page
- Setting a Particular Agent Gold Image Version as the Restricted Version Using EM CLI

Setting a Particular Agent Gold Image Version as the Restricted Version Using Gold Agent Images Home Page

To set a draft or active version of an Agent Gold Image as the restricted version, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**

4. Select the **Versions and Drafts** tab. Select the gold image version that you want to set as the restricted version, then click **Set Restricted Version.**

Setting a Particular Agent Gold Image Version as the Restricted Version Using EM CLI

To set a draft or active version of an Agent Gold Image version as the restricted version using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `promote_gold_agent_image` verb to promote the Agent Gold Image version to the Restricted maturity level:

   ```
   $<OMS_HOME>/bin/emcli promote_gold_agent_image -
   version_name="gold_image_version_name" -maturity="Current/Restricted/Draft"
   ```

   The `-version_name` parameter defines the Agent Gold Image that you want to promote.

   The `-maturity` parameter defines the gold image maturity level.

   For example, to promote the Agent Gold Image OPC_AGI_DB_JUL_13 to the Restricted maturity level, run the following:

   ```
   $<OMS_HOME>/bin/emcli promote_gold_agent_image -version_name=OPC_AGI_DB_JUL_13 -
   maturity=Restricted
   ```

Subscribing Management Agents to an Agent Gold Image

To subscribe a set of Management Agents to an Agent Gold Image, use either of the following methods:

- Subscribing Management Agents to an Agent Gold Image Using Gold Agent Images Home Page
- Subscribing Management Agents to an Agent Gold Image Using EM CLI

Subscribing Management Agents to an Agent Gold Image Using Gold Agent Images Home Page

> **Note:**
>
> You cannot install, update, or upgrade a Shared Agent (NFS Agent) using an Agent Gold Image.
>
> You cannot subscribe the following Management Agents to an Agent Gold Image:
>
> - Central Agent.
> - Already subscribed Management Agents.
> - Shared Agents (NFS Agents).
> - Unsecure Management Agents.
> - Management Agents on platforms that are different from the platforms on which the Agent Gold Image is available.
>
>   The platform is identified by the Oracle home collection, so make sure the Oracle home target is discovered and collected. To do so, On the Home page of the Management Agent, in the Summary section, click **Oracle Home and Patch Details,** and on the following page, click **Refresh Configuration.**

To subscribe a set of Management Agents to an Agent Gold Image, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Subscriptions** tab. Click **Subscribe.**
5. Search for and select the required Management Agents, then click **Select.**

Subscribing Management Agents to an Agent Gold Image Using EM CLI

> **Note:**
>
> You cannot install, update, or upgrade a Shared Agent (NFS Agent) using an Agent Gold Image.
>
> You cannot subscribe the following Management Agents to an Agent Gold Image:
>
> - Central Agent.
> - Already subscribed Management Agents.
> - Shared Agents (NFS Agents).
> - Unsecure Management Agents.
> - Management Agents on platforms that are different from the platforms on which the Agent Gold Image is available.
>
>   The platform is identified by the Oracle home collection, so make sure the Oracle home target is discovered and collected. To do so, On the Home page of the Management Agent, in the Summary section, click **Oracle Home and Patch Details,** and on the following page, click **Refresh Configuration.**

To subscribe a Management Agent to an Agent Gold Image using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `subscribe_agents` verb to subscribe the specified Management Agent to a specific Agent Gold Image:

   ```
   $<OMS_HOME>/bin/emcli subscribe_agents
            -image_name="Image Name"
            [-agents="agent_name_pattern"]
            [-groups="group_name"]
   ```

   Note that the parameters mentioned in `[ ]` are optional.

   The `-image_name` parameter subscribes the Management Agents to the specified Agent Gold Image.

   The `-agents` parameter subscribes only the Management Agents that match the specified name pattern.

   The `-groups` parameter subscribes only the Management Agents that belong to the specified groups.

   Examples:

- The following example subscribes the Management Agents that match the name pattern `abc%` or `xyz.example.com:1243` to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli subscribe_agents -image_name="OPC_AGT_ADC_POD" -
  agents="abc%,xyz.example.com:1243"
  ```

- The following example subscribes all the Management Agents to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli subscribe_agents -image_name="OPC_AGT_ADC_POD"
  ```

- The following example subscribes all the Management Agents that belong to the group GROUP1 or GRP2 to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli subscribe_agents -image_name="OPC_AGT_ADC_POD" -
  groups="GROUP1,GRP2"
  ```

Unsubscribing Management Agents from an Agent Gold Image

To unsubscribe Management Agents from an Agent Gold Image, use either of the following methods:

- Unsubscribing Management Agents to an Agent Gold Image Using Gold Agent Images Home Page
- Unsubscribing Management Agents to an Agent Gold Image Using EM CLI

Unsubscribing Management Agents to an Agent Gold Image Using Gold Agent Images Home Page

To unsubscribe Management Agents from an Agent Gold Image, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Subscriptions** tab. Select the Management Agents that you want to unsubscribe from the Agent Gold Image. Click **Unsubscribe.** Select **OK.**

Unsubscribing Management Agents to an Agent Gold Image Using EM CLI

To unsubscribe a Management Agent from an Agent Gold Image using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `unsubscribe_agents` verb to unsubscribe the specified Management Agent from a specific Agent Gold Image:

```
$<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="Image Name" [-agents="Full
Agent Name"] [-groups="List of group names"] [-closure_related="true/false"] [-
closure_nfs="true/false"]
```

Note that the parameters mentioned in `[ ]` are optional.

Table 13-4 lists and describes the supported parameters for unsubscribing Management Agents from an Agent Gold Image.

Table 13-4 Supported Parameters for Unsubscribing Management Agents

Parameter	Description
`-image_name`	Unsubscribes the Management Agents that subscribe to the specified Agent Gold Image.
`-agents`	Unsubscribes the Management Agents that match the specified name pattern.
`-groups`	Unsubscribes the Management Agents that belong to the specified groups.
`-closure_related`	Does not unsubscribe the related Management Agents if the value specified for this parameter is 'false'.
`-closure_shared`	Does not unsubscribe the related shared agents if the value specified for this parameter is 'false'.

Examples:

- The following example unsubscribes the Management Agents that subscribe to the Agent Gold Image OPC_AGT_ADC_POD, and match the name pattern `abc%` or `xyz.example.com:1243`:

  ```
  $<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="OPC_AGT_ADC_POD" -
  agents="abc%,xyz.example.com:1243"
  ```

- The following example unsubscribes all the Management Agents that subscribe to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="OPC_AGT_ADC_POD"
  ```

- The following example unsubscribes the Management Agents that subscribe to the Agent Gold Image OPC_AGT_ADC_POD, and belong to the group GROUP1 or GRP2:

  ```
  $<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="OPC_AGT_ADC_POD" -
  groups="GROUP1,GRP2"
  ```

- The following example unsubscribes `xyz.example.com:1243` and all its related shared agents that subscribe to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -closure_shared="true"
  ```

- The following example unsubscribes `xyz.example.com:1243` and all its related Management Agents that subscribe to the Agent Gold Image OPC_AGT_ADC_POD:

  ```
  $<OMS_HOME>/bin/emcli unsubscribe_agents -image_name="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -closure_related="true"
  ```

Provisioning Management Agents Using an Agent Gold Image

See *Advantages of Provisioning, Upgrading, and Updating Management Agents Using a Gold Image Version* in the *Oracle Enterprise Manager Basic Installation Guide.*

> **Note:**
>
> You cannot install, update, or upgrade a Shared Agent (NFS Agent) using an Agent Gold Image. For information about Shared Agents, see Overview of Installing Shared Agents.

Updating Management Agents Using an Agent Gold Image Version

To update a Management Agent using an Agent Gold Image version, follow these steps:

1. Create an Agent Gold Image. To do this, see Creating an Agent Gold Image.
2. Create an Agent Gold Image version. To do this, see Creating an Agent Gold Image Version.
3. Set a particular Agent Gold Image version as the current version. To do this, see Setting a Particular Agent Gold Image Version as the Current Version.
4. Subscribe Management Agents to an Agent Gold Image. To do this, see Subscribing Management Agents to an Agent Gold Image.
5. Update Management Agents. To update your Management Agents using an Agent Gold Image version, use either of the following procedures:
   - Updating Management Agents with an Agent Gold Image
   - Updating Management Agents Using Agent Gold Image Version Using EM CLI

> **Note:**
>
> Before updating a standalone Management Agent using an Agent Gold Image version, meet the hardware requirements. See *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide.*

> **Note:**
>
> When you have to update a set of related Management Agents to an Agent Gold Image, it is mandatory to update all the related agents. However, there is an option to override this in case if you want to update only a selected few Agents to the Agent Gold Image. To achieve this, you have to set the parameter `closureRelated` to `false` in the `EM_GI_MASTER_INFO` table.

> **Note:**
>
> You cannot install, update, or upgrade a Shared Agent (NFS Agent) using an Agent Gold Image.

Updating Management Agents with an Agent Gold Image

To update a Management Agent using an Agent Gold Image version, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. Click the name of the required Agent Gold Image.
3. Click **Manage Image Versions and Subscriptions.**
4. Select the **Subscriptions** tab. Select the Management Agents that you want to update, select **Update,** then select **To Current Version,** or **To Restricted Version.**
5. Accept the default job name for the Management Agent update job. You can change this, if required.

   If you have not included certain Management Agents in the previous step and want to include them in the update operation now, select **Add,** then specify the additional Management Agents.

   If there is any change to the sbin directory, particularly for a complete agent upgrade or when there is an sbin-specific patch, after updating the Management Agent, the preferred privileged credentials of the Management Agent host are used for running the root.sh script on the Management Agent.

   If these credentials are not already set, then click **Override Preferred Credentials** and enter the credentials you want to use instead.

   Click **Next.**
6. By default, Image Version Pre Staged is not selected, in this case provide a stage location that is local to the destination host. However, if you select the **Image version Pre Staged**, provide a shared, NFS-mounted stage location that is accessible by all the Management Agents.

   Also, specify a method for Management Agent deployment. If you select the default option **Push,** the OMS transfers the Management Agent software to all the hosts that are selected for the update operation. However, if you want the Management Agent present on each destination host to retrieve the Management Agent software from the OMS instead, select **Pull.**
7. In the Additional Inputs section, specify any scripts that you want to run before the update operation and after the update operation. Ensure that you select **Script on OMS Host** if the script exists on the OMS host. Also, specify any additional parameters that you want to use for the update operation. Table 13-5 provides the additional parameters that you can use while updating Management Agents.

Table 13-5 List of Additional Parameters for Management Agent Update

Parameter	Description
-ignorePrereqs	Skips running the prerequisite checks. Specify this parameter when you have already verified the prerequisites, and only want to perform the rest of the upgrade process.
-debug	Logs debug messages useful for debugging and resolving errors.

8. In the Schedule section, specify values for the following:

9.
   - **Batch Size:** A Management Agent update activity runs in a way that the Management Agents are updated in batches. The batch size represents the number of Management Agents present in a batch.
   - **Job Frequency:** The time (in minutes) after which the application checks whether the current batch is complete or not.
   - **Success Rate:** The percentage of the total number of Management Agents (that is, the Management Agents that are a part of the current update batch and the Management Agents that were a part of the previous update batches) that must have been updated once a batch is complete, before the next batch is allowed to begin.

     For example, if there are 1000 Agents deployed in your enterprise and the batch size is set to 100, the batch success rate is set to 90, and the Agents are updated in batches of 100. In this case, once a batch is complete, the application moves to the next batch only if 90 per cent of the total number of Management Agents are updated successfully.
   - **Start:** The time when you want to start the update operation, and the time when you want the update operation to end. By default, the time set is **Immediately**. In this context, it is the OMS time that is considered.
   - **Duration:** The duration until which you want the update operation to run.
10. In the Notify section, specify the email addresses to which you want the notifications about the update job progress to be sent.
11. In the Shell Profile section, select Update Shell Profile, and specify the location of your shell profile, if you want your shell profile to be updated with the new Management Agent Oracle home location.

    By default, this is not selected, and is optional.
12. In the Cleanup options section, select:
    - **Pre-Cleanup** to clean up the old or inactive agent homes prior to updating the Management Agents.
    - **Post-Cleanup** to clean up the old or inactive agent homes after updating the Management Agents.

    > **Note:**
    >
    > If the cleanup operation is not performed at this point, it can be done at a later time using the Agent Upgrade Console. For more information, see *Oracle Enterprise Manager Upgrade Guide.*

    A job that updates the Management Agents is submitted to the Enterprise Manager job system. You can view the status of this job on the Gold Agent Image Activities page, in the Update Activities tab.
13. Click **Update.**

    A job that updates the Management Agents is submitted to the Enterprise Manager job system. You can view the status of this job on the Gold Agent Image Activities page, in the Update Activities tab.

Updating Management Agents Using Agent Gold Image Version Using EM CLI

To update Management Agents using an Agent Gold Image version, using EM CLI, follow these steps:

> **Note:**
>
> Before updating a standalone Management Agent using an Agent Gold Image version, meet the hardware requirements. See *Hardware Requirements for Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.

1. Log in to EM CLI from the `/bin` directory present within the Oracle home of the OMS:

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<ORACLE_HOME>/bin/emcli sync
   ```

3. Run the `get_updatable_agents` verb to display the Management Agents that can be updated using a particular Agent Gold Image version or Agent Gold Image:

   ```
   $<ORACLE_HOME>/bin/emcli get_updatable_agents -version_name | -image_name
   [-agents="Full Agent Name"] [-versions="List of Versions"]
   [-groups="List of group names"] [-output_file="Location of the output
   file"]
   ```

   Note that the parameters mentioned in `[ ]` are optional.

   > **Note:**
   >
   > It is mandatory to specify the `-version_name` parameter or the `-image_name` parameter. If you specify both, a union of the outputs (when each of these parameters is specified individually) is displayed.

   > **Note:**
   >
   > To view a list of Management Agents that cannot be updated, run the `get_not_updatable_agents` verb:
   >
   > ```
   > emcli get_not_updatable_agents [-version_name | -image_name]
   > ```
   >
   > The parameters mentioned in `[ ]` are optional.

Table 13-6 lists and describes the supporting parameters for displaying the Management Agents that can be updated using a particular Management Agent image version.

Table 13-6 Supported Parameters for Displaying Management Agents That Can Be Updated

Parameter	Description
`-version_name`	Specify this option to display the Management Agents that can be updated using the specified Agent Gold Image version.
`-image_name`	Specify this option to display the Management Agents that can be updated using the specified Agent Gold Image.
`-versions`	Specify this option to display the Management Agents that can be updated, and are of the specified versions.
`-agents`	Specify this option to display the Management Agents that can be updated, and whose name matches the specified name pattern.
`-groups`	Specify this option to display the Management Agents that can be updated, and are a part of those groups whose name matches the specified name pattern.
`-output_file`	Specify this option to add the displayed list of Management Agents that can be updated to an output file.

Examples:

- The following example lists the Management Agents that can be updated using the latest Agent Gold Image OPC_AGT_ADC_POD:

```
<ORACLE_HOME>/bin/emcli get_updatable_agents -image_name="OPC_AGT_ADC_POD"
```

- The following example lists the Management Agents that can be updated using the Agent Gold Image version OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli get_updatable_agents -version_name="OPC_AGT_ADC_POD_JUNE"
```

- The following example lists the Management Agents that are of version 12.1.0.1.0 or 12.1.0.2.0, and can be updated using the Agent Gold Image version OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli get_updatable_agents -
version_name="OPC_AGT_ADC_POD_JUNE" -versions="12.1.0.1.0,12.1.0.2.0"
```

- The following example lists the Management Agents that belong to GROUP1 or GRP2, and can be updated using the Agent Gold Image version OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli get_updatable_agents -
version_name="OPC_AGT_ADC_POD_JUNE" -groups="GROUP1,GRP2"
```

- The following example lists the Management Agents that can updated using the Agent Gold Image OPC_AGT_ADC_POD_JUNE, and adds the list to the output file `/scratch/agents_file.txt`:

```
<ORACLE_HOME>/bin/emcli get_updatable_agents -image_name="OPC_AGT_ADC_POD_JUNE" -
output_file="/scratch/agents_file.txt"
```

4. Run the `update_agents` verbs to prepare the environment for updating your Management Agents and to submit the Management Agent update job:

```
<ORACLE_HOME>/bin/emcli update_agents
        -version_name | -image_name
        -agents="agent_names" | -input_file="agents_file:input_file_location"
        [-pre_script_loc="location_of_pre_script"]
        [-pre_script_on_oms]
        [-post_script_loc="location_of_post_script"]
        [-post_script_on_oms]
        [-op_name="custom_operation_name"]
```

```
[-override_credential="named_credential"]
[-additional_parameters]
[-stage_location="custom_stage_location"]
[-is_staged="true|false"]
[-stage_action="push|pull"]
[-batch_size]
[-start_time]
[-end_time]
[-frequency]<
[-success_rate]
[-runPrecleanup]
{-runPostcleanup]
[-email]
[-update_profile]
[-profile_path]
```

Note that the parameters mentioned in `[ ]` are optional.

> **Note:**
>
> It is mandatory to specify the `-version_name` parameter or the `-image_name` parameter. Also, it is mandatory to specify the `-agents` parameter or the `-input_file` parameter. If you specify both `-agents` and `-input_file`, a union of the outputs (when each of these parameters is specified individually) is displayed.
>
> All parameters can be passed in a response file, using the -input_file parameter. For example, `-input_file="response_file:/scratch/response_file.txt"`.
>
> In the response file, each parameter must be specified on a new line, and in name value pairs. For example, `op_name=UPDATE_AGT_121020`
>
> If the same parameter is passed both on the command line and in the response file, the value of the command line parameter is given precedence.

Table 13-7 lists and describes the supporting parameters for updating Management Agents using an Agent Gold Image version.

Table 13-7 Supported Parameters for Updating Management Agents Using Agent Gold Image Version

Parameter	Description
`-version_name`	Agent Gold Image version to which the Management Agents should be updated.
`-image_name`	Agent Gold Image to which the Management Agents should be updated.
`-agents`	Names of all the Management Agents that should be updated.
`-input_file`	Absolute path to the file that lists the Management Agents to be updated.
`-pre_script_loc`	Absolute path to a script that should be run before updating the Management Agents.
`-pre_script_on_oms`	Indicates that the pre-script is present on the OMS host.
`-post_script_loc`	Absolute path to a script that should be run after updating the Management Agents.
`-post_script_on_oms`	Indicates that the post-script is present on the OMS host.
`-op_name`	Custom operation name for the Management Agent update.

Table 13-7 (Cont.) Supported Parameters for Updating Management Agents Using Agent Gold Image Version

Parameter	Description
-override_credential	Overrides the preferred credentials with different named credentials. Typically, the preferred credentials of the Oracle home of the Management Agent are used to run root.sh on certain Management Agents after the update. But passing this option overrides those preferred credentials.
-additional_parameters	Additional parameters to be passed for the Management Agent update.
-stage_location	Custom stage location for the Management Agent update. Minimum free space required is 1 GB if image is not already staged. Ensure that this location is accessible from all the Management Agents being updated if image is prestaged.
-is_staged	Set to 'true' if you have already staged the Agent Gold Image.
-stage_action	Set to 'pull' if you want the Management Agents to be updated to pull the Agent Gold Image. Typically, If the Agent Gold Image has not already been staged, by default the Agent Gold Image is pushed to the Management Agents to be updated. Setting to 'pull' pulls the Agent Gold Image instead.
-batch_size	Number of Management Agents present in an update batch. Default value is 100.
-start_time	Start time for the update job. Specify in \" yyyy-mm-dd hh:mm:ss\" format.
-end_time	End time for the update job. Specify in \" yyyy-mm-dd hh:mm:ss\" format.
-frequency	Time (in minutes) after which the application should check whether or not the current batch is complete, and should schedule the next batch for update. Default value is.
-success_rate	Percentage of the total number of Management Agents that must have been successfully updated in previous batches, before the next batch is allowed to begin. Default value is 90.
-runPrecleanup	Cleans up the old agent homes before updating the Management Agents.
-runPostcleanup	Cleans up the old agent homes after updating the Management Agents.
-email	Email IDs separated by a comma (,) to which notifications should be sent once the batch completes.
-update_profile	Indicates that a profile is set with agent Oracle home.
-profile_path	Absolute path to user profiles separated by a comma (,) if the update profile option is selected.

Examples:

- The following example updates `xyz.example.com:1243` using the latest Agent Gold Image in the series OPC_AGT_ADC_POD:

```
<ORACLE_HOME>/bin/emcli update_agents -gold_image_series="OPC_AGT_ADC_POD" -
agents="xyz.example.com:1243"
```

- The following example updates `xyz.example.com:1243` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
agents="xyz.example.com:1243"
```

- The following example updates all the Management Agents present in the input file `/scratch/agents_file.txt` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
input_file="agents_file:/scratch/agents_file.txt"
```

- The following example runs `/scratch/pre_script`, then updates `xyz.example.com:1243` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
  agents="xyz.example.com:1243" -pre_script_loc="/scratch/pre_script"
  ```

- The following example updates `xyz.example.com:1243` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE, then runs `/scratch/post_script`:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
  agents="xyz.example.com:1243" -post_script_loc="/scratch/post_script"
  ```

- The following example updates `xyz.example.com:1243` (creates an update job UPDATE_JOB123) using the Agent Gold Image OPC_AGT_ADC_POD_JUNE:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
  agents="xyz.example.com:1243" -op_name="UPDATE_JOB123"
  ```

- The following example updates `xyz.example.com:1243` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE, and uses `NAMED_CRED123` to run root.sh after the update:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
  agents="xyz.example.com:1243" -override_credential="NAMED_CRED123"
  ```

- The following example updates `xyz.example.com:1243` using the Agent Gold Image OPC_AGT_ADC_POD_JUNE, passing two additional parameters:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_name="OPC_AGT_ADC_POD_JUNE" -
  agents="xyz.example.com:1243" -additional_parameters="-ignorePrereqs -
  newParameter"
  ```

- The following example updates `xyz.example.com:1243` using the latest Agent Gold Image in the series OPC_AGT_ADC_POD, passing two additional parameters:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_series="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -additional_parameters="-ignorePrereqs -
  newParameter"
  ```

- The following example updates `xyz.example.com:1243` using the latest Agent Gold Image in the series OPC_AGT_ADC_POD, without staging the gold image:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_series="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -is_staged="true"
  ```

- The following example updates `xyz.example.com:1243` using the latest Agent Gold Image in the series OPC_AGT_ADC_POD, and the gold image is pulled by `xyz.example.com:1243`:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -gold_image_series="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -stage_action="pull"
  ```

- The following example runs the Management Agent update with maximum of 150 Management Agents getting updated in each batch:

  ```
  <ORACLE_HOME>/bin/emcli update_agents -image_name="OPC_AGT_ADC_POD" -
  agents="xyz.example.com:1243" -batch_size=150
  ```

- The following example runs the Management Agent update with maximum of 150 Management Agents getting updated in each batch:

> **Note:**
>
> The next batch gets scheduled only if 80% of the Management Agents are successfully updated in the previous batches.

```
<ORACLE_HOME>/bin/emcli update_agents -image_name="OPC_AGT_ADC_POD" -
agents="xyz.example.com:1243" -batch_size=150 success_rate=80
```

- The following example schedules the agent update job starting at May 7, 10:00:00 AM and ending at May 8, 10:00:00 AM:

```
<ORACLE_HOME>/bin/emcli update_agents -image_name="OPC_AGT_ADC_POD" -
agents="xyz.example.com:1243" -start_time="2019-05-07 10:00:00" -
end_time="2019-05-08 10:00:00"
```

5. Run the `get_agent_update_status` verb to displays the update results of the Management Agent:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status
        -version_name | -op_name
        [-agent="agent_name_pattern"]
        [-severity="ERROR|WARNING"]
        [-severity_id="severity_id"]
        [-status="PendingUpdateInprogress|Updatable|NotUpdatable|NotExecuted|Success|
Inprogress|Failed"]
```

Note that the parameters mentioned in `[ ]` are optional.

> **Note:**
>
> It is mandatory to specify the `-op_name` parameter or the `-version_name` parameter. If you have specified `-severity` or `-severity_id`, ensure that you do not specify `-version_name` or -status.

Table 13-8 lists and describes the supporting parameters for displaying the update status of the Management Agent.

Table 13-8 Supported Parameters for Displaying Update Status of the Management Agent

Parameter	Description
`-version_name`	Displays the details of the update operation submitted for the specified Agent Gold Image version name.
`-op_name`	Displays the details of the specified update operation.
`-agent`	Displays the details of the operations submitted for Management Agents that have the specified name pattern.
`-status`	Displays the details of the update operations that have the specified status.
`-severity`	Displays the details of the update operations that have the specified severity level.
`-severity_id`	Displays the details of the update operations that have the specified severity ID

Examples:

- The following example displays the details of the update operations submitted for the Agent Gold Image version OPC_AGT_ADC_POD_JUNE:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -
version_name="OPC_AGT_ADC_POD_JUNE"
```

- The following example displays the details of the update operations submitted for the Agent Gold Image OPC_AGT_ADC_POD_JUNE, for the Management Agent `xyz.example.com:1243`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -
version_name="OPC_AGT_ADC_POD_JUNE" -agent="xyz.example.com:1243"
```

- The following example displays the details of the update operations submitted for the Agent Gold Image OPC_AGT_ADC_POD_JUNE, for the Management Agent `xyz.example.com:1243`, that have their status as `Failed`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -
version_name="OPC_AGT_ADC_POD_JUNE" -agent="xyz.example.com:1243" -
status="Failed"
```

- The following example displays the details of the update operation `UPDATE_JOB123`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123"
```

- The following example displays the details of the update operation `UPDATE_JOB123`, for the Management Agent `xyz.example.com:1243`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -op_name="UPDATE_JOB123" -
agent="xyz.example.com:1243"
```

- The following example displays the details of the update operation `UPDATE_JOB123`, for Management Agents having the status `Failed`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -op_name="UPDATE_JOB123" -
status="Failed"
```

- The following example displays the details of the update operation `UPDATE_JOB123` for the Management Agent `xyz.example.com:1243`, having the status `Failed`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status -op_name="UPDATE_JOB123" -
status="Failed" -agent="xyz.example.com:1243"
```

- The following example displays the Management Agents of the update operation `UPDATE_JOB123`, for which severity is `ERROR`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
severity="ERROR"
```

- The following example displays the Management Agents of the update operation `UPDATE_JOB123`, for which severity is `WARNING`, and severity ID is `ROOT_RUN_CHECK`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
severity="WARNING" -severity_id="ROOT_RUN_CHECK"
```

- The following example displays the Management Agents of the update operation `UPDATE_JOB123`, for which severity ID is `ROOT_RUN_CHECK`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
severity_id="ROOT_RUN_CHECK"
```

- The following example displays the details of the update operation `UPDATE_JOB123` for the Management Agent `xyz.example.com:1243`, with severity as `ERROR`:

```
<ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
severity="ERROR"  -agent="xyz.example.com:1243"
```

- The following example displays the details of the update operation `UPDATE_JOB123` for the Management Agent `xyz.example.com:1243`, with severity ID as `ROOT_RUN_CHECK`:

  ```
  <ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
  severity_id="ROOT_RUN_CHECK"  -agent="xyz.example.com:1243"
  ```

- The following example displays the details of the update operation `UPDATE_JOB123` for the Management Agent `xyz.example.com:1243`, with severity as `WARNING` and severity ID as `ROOT_RUN_CHECK`:

  ```
  <ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
  severity="WARNING" -severity_id="ROOT_RUN_CHECK"  -agent="xyz.example.com:1243"
  ```

- The following example displays the Management Agents of the update operation `UPDATE_JOB123`, for which severity is `ERROR`:

  ```
  <ORACLE_HOME>/bin/emcli get_agent_update_status  -op_name="UPDATE_JOB123" -
  severity="ERROR"
  ```

Viewing Agent Gold Image Activity Details

To view a list of the Agent Gold Image activities (that is, the jobs that are submitted to the Enterprise Manager job system) and details such as their status, the time at which the activity begun, the time at which the activity ended, and so on, use either of the following methods:

- Viewing Agent Gold Image Activity Details Using Gold Agent Image Home Page
- Viewing Agent Gold Image Activity Details Using EM CLI

Viewing Agent Gold Image Activity Details Using Gold Agent Image Home Page

To view a list of the Agent Gold Image activities, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. In the Activities section, click **Show all activities.**
3. To view the status details of Agent Gold Image activities, Management Agent update activities, or Management Agent unsubscribe activities, select the **Image Activities, Update Activities,** or **Unsubscribe Activities** tab, respectively.
4. To view the execution details of a particular Agent Gold Image activity, Management Agent update activity, or Management Agent unsubscribe activity, click the job name.

Viewing Agent Gold Image Activity Details Using EM CLI

To view the activity details of an Agent Gold Image using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `list_gold_agent_image_activities` verb to list the activities that the specified Agent Gold Image is a part of:

```
$<OMS_HOME>/bin/emcli list_gold_agent_image_activities -
version_name="gold_image_version_name" [-noheader]
[-script | -format= [name:<pretty|script|csv>];
[column_separator:"column_sep_string"]; [row_separator:"row_sep_string"]; ]
```

Note that the parameters mentioned in `[ ]` are optional.

Table 13-9 lists and describes the supported parameters for viewing details about the Agent Gold Image.

Table 13-9 Supported Parameters for Viewing Details about the Agent Gold Image

Parameter	Description
`-version_name`	Agent Gold Image version whose activities you want to view.
`-no_header`	Displays a tabular form of the output without column headers.
`-script`	This parameter is equivalent to `-format="name:script"`.
`-format`	This parameter defines the type of the output format. The default value of this parameter is `-format="name:pretty"`. `-format="name:pretty"` displays the output table in a readable format that cannot be parsed by scripts. `-format="name:script"` sets the default column separator to a tab character and the default row separator to a newline character. You can specify the `column_separator` and `row_separator` strings to change these default characters. `-format="name:csv"` sets the column separator to a comma and the row separator to a newline character.

For example, to view activity details for the Agent Gold Image OPC_AGI_DB_JUL_13, run the following command:

```
$<OMS_HOME>/bin/emcli list_gold_agent_image_activities -
version_name=OPC_AGI_DB_JUL_13
```

4. You can also run the `get_gold_agent_image_activity_status` to check the activity status of the Agent Gold Image:

```
$<OMS_HOME>/bin/emcli get_gold_agent_image_activity_status
        -operation_name="gold_image_operation_name"
        [-noheader]
        [-script | -format=
                        [name:<pretty|script|csv>];
                        [column_separator:"column_sep_string"];
                        [row_separator:"row_sep_string"];
        ]
```

Table 13-10 lists and describes the supported parameters for viewing the activity status of the Agent Gold Image.

Table 13-10 Supported Parameters for Viewing Activity Status of the Agent Gold Image

Parameter	Description
`-operation_name`	Displays the status of a particular Agent Gold Image activity.
`-no_header`	Displays a tabular form of the output without column headers.

Table 13-10 (Cont.) Supported Parameters for Viewing Activity Status of the Agent Gold Image

Parameter	Description
`-script`	This parameter is equivalent to `-format="name:script"`.
`-format`	This parameter defines the type of the output format. The default value of this parameter is `-format="name:pretty"`. `-format="name:pretty"` displays the output table in a readable format that cannot be parsed by scripts. `-format="name:script"` sets the default column separator to a tab character and the default row separator to a newline character. You can specify the `column_separator` and the `row_separator` strings to change these default characters. `-format="name:csv"` sets the column separator to a comma and the row separator to a newline character.

For example, to display the activity status of the Agent Gold Image operation GOLDAGENTIMAGE_CREATE_12_22_12_12_52_535, run the following command:

```
$<OMS_HOME>/bin/emcli get_gold_agent_image_activity_status  -
operation_name=GOLDAGENTIMAGE_CREATE_12_22_12_12_52_535
```

Checking the Agent Gold Image Compliance Level

To check the compliance level for all the Agent Gold Images, from the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**

You can view a pictorial representation (a vertical bar graph) of the number of Management Agents that are on gold image and not on gold image. Hover your mouse over the vertical bars to see the exact number of Management Agents that are in question.

In the table below the vertical bar graph, you can view details about the gold images created so far. To check the compliance level, see the **Compliance** column.

Viewing Details about the Agent Gold Images

You can view details about the Agent Gold Images, using either of the following methods:

- Viewing Details about the Agent Gold Images and Gold Image Versions Using the Gold Agent Images Home Page
- Viewing Details about the Agent Gold Images Using EM CLI

Viewing Details about the Agent Gold Images and Gold Image Versions Using the Gold Agent Images Home Page

To view details about the Agent Gold Images and gold image versions using the Gold Agent Images Home page, from the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**

You can view a pictorial representation (a vertical bar graph) of the number of Management Agents that are on gold image and not on gold image. Hover your mouse over the vertical bars to see the exact number of Management Agents that are in question.

In the table below the vertical bar graph, you can view details about the gold images created so far. Table 13-11 describes these details.

Table 13-11 Gold Agent Image Details

Column Name	Description
Gold Image Name	Name of the Agent Gold Image. To view more details about an Agent Gold Image and its versions, click the gold image. On the Gold Agent Images page, view details about the deployments and the image versions created for that gold image. Also, for each gold image version, view general details, the associated instance properties, the plug-ins and patches deployed, the activities performed on it, and the stage locations configured for it. **Note:** The Gold Image page lists only those gold image versions that have been set to current (active) or restricted version status. It does not list gold image versions of any other status. If you want to view all the gold image versions of a particular gold image, regardless of their status, then on the Agent Gold Images page, click **Manage Image Versions and Subscriptions.** And on the Manage Image page, click the **Versions And Drafts** tab.
Subscribed Agents	Number of Management Agents associated or subscribed to the Agent Gold Image. This includes the Management Agents that are not only updated with the gold image but also the ones that are not updated but subscribed to the gold image. Subscribing Management Agents to a gold image is a prerequisite for updating Management Agents with a particular gold image version.
Agents on Gold Image	Number of Management Agents subscribed to a gold image and also updated with that gold image.
Compliance	Percentage of Management Agent on the latest gold image version.
Number of Deployed Gold Image Versions	Number of gold image versions subscribed to by the Management Agents. This includes all gold image versions, including the latest version that Management Agents are subscribed to.
Platform Name	Platform for which the Agent Gold Image is created.

Viewing Details about the Agent Gold Images Using EM CLI

To view details about an Agent Gold Image using EM CLI, follow these steps:

1. Log in to EM CLI from the `/bin` directory present within the OMS home:

   ```
   $<OMS_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<OMS_HOME>/bin/emcli sync
   ```

3. Run the `list_gold_agent_images` verb to list the various Agent Gold Images that have been created.:

   ```
   $<OMS_HOME>/bin/emcli list_gold_agent_images
   [-noheader]
   [-script | -format=
   [name:<pretty|script|csv>];
   [column_separator:"column_sep_string"];
   [row_separator:"row_sep_string"];
   ]
   ```

Note that the parameters mentioned in `[ ]` are optional.

Table 13-12 lists and describes the supported parameters for displaying the list of Agent Gold Images.

Table 13-12 Supported Parameters for Displaying the List of Agent Gold Images

Parameter	Description
`-no_header`	Displays a tabular form of the output without column headers.
`-script`	This parameter is equivalent to `-format="name:script"`.
`-format`	This parameter defines the type of the output format. The default value of this parameter is `-format="name:pretty"`. `-format="name:pretty"` displays the output table in a readable format that cannot be parsed by scripts. `-format="name:script"` sets the default column separator to a tab character and the default row separator to a newline character. You can specify the `column_separator` and `row_separator` strings to change these default characters. `-format="name:csv"` sets the column separator to a comma and the row separator to a newline character.

4. Run the `list_gold_agent_imageversions` verb to list the Agent Gold Image versions:

```
$<OMS_HOME>/bin/emcli list_gold_agent_imageversions
[-image_name="gold_image_name"]
[-all]
[-noheader]
[-script | -format=
 [name:<pretty|script|csv>]; [column_separator:"column_sep_string"];
[row_separator:"row_sep_string"];
]
```

Note that the parameters mentioned in `[ ]` are optional.

Table 13-13 lists and describes the supported parameters for displaying the list of Agent Gold Image versions.

Table 13-13 Supported Parameters for Displaying the List of Agent Gold Image Versions

Parameter	Description
`-image_name`	A parameter to view the Agent Gold Image versions that are part of a particular Agent Gold Image.
`-all`	A parameter to view all the Agent Gold Images.
`-no_header`	A parameter to display a tabular form of the output without column headers.
`-script`	This parameter is equivalent to `-format="name:script"`.

Table 13-13 (Cont.) Supported Parameters for Displaying the List of Agent Gold Image Versions

Parameter	Description
`-format`	This parameter defines the type of the output format. The default value of this parameter is `-format="name:pretty"`. `-format="name:pretty"` displays the output table in a readable format that cannot be parsed by scripts. `-format="name:script"` sets the default column separator to a tab character and the default row separator to a newline character. You can specify the `column_separator` and the `row_separator` strings to change these default characters. `-format="name:csv"` sets the column separator to a comma and the row separator to a newline character.

For example, to display the Agent Gold Image versions that are promoted to Current, run the following command:

```
$<OMS_HOME>/bin/emcli list_gold_agent_imageversions
```

To display the Agent Gold Image versions that are part of the OPC_DB_MONITORING and promoted to Current, run the following command:

```
$<OMS_HOME>/bin/emcli list_gold_agent_imageversions -
image_name=OPC_DB_MONITORING
```

5. Run the `get_gold_agent_image_details` verb to display a list of the platform, plug-in, patch, configuration properties, and Management Agent details of an Agent Gold Image:

```
$<OMS_HOME>/bin/emcli get_gold_agent_image_details
-version_name="gold_image_version_name"
[-platform]
[-plugin]
[-patch]
[-config_properties]
[-agent]
[-noheader]
[-script | -format=
[name:<pretty|script|csv>]; [column_separator:"column_sep_string"];
[row_separator:"row_sep_string"];
]
```

Note that the parameters mentioned in `[ ]` are optional.

Table 13-14 lists and describes the supported parameters for displaying the platform, plug-in, patch, configuration properties, and Management Agent details of the Agent Gold Image.

Table 13-14 Supported Parameters for Displaying the Details of the Agent Gold Image

Parameter	Description
`-version_name`	The name of the Agent Gold Image version whose details you want to view.
`-platform`	The platform details of the Agent Gold Image.
`-plugin`	The plug-in details of the Agent Gold Image.
`-patch`	The patch details of the Agent Gold Image.

Table 13-14 (Cont.) Supported Parameters for Displaying the Details of the Agent Gold Image

Parameter	Description
-config_properties	The configuration properties of the Agent Gold Image.
-agent	The Management Agent details of the Agent Gold Image.
-no_header	A tabular form of the output without column headers.
-script	This parameter is equivalent to -format="name:script".
-format	This parameter defines the type of the output format. The default value of this parameter is -format="name:pretty". -format="name:pretty" displays the output table in a readable format that cannot be parsed by scripts. -format="name:script" sets the default column separator to a tab character and the default row separator to a newline character. You can specify the column_separator and row_separator strings to change these default characters. -format="name:csv" sets the column separator to a comma and the row separator to a newline character.

For example, to display the platform, plug-in, and patch details of the Agent Gold Image OPC_AGI_DB_JUL_13, run the following command:

```
$<OMS_HOME>/bin/emcli get_gold_agent_image_details -version_name=OPC_AGI_DB_JUL_13
```

6. You can also run the list_agents_on_gold_image verb to list the Management Agents that were deployed or updated using a particular Agent Gold Image version or overall agent deployment report for Agent Gold Image:

```
$<OMS_HOME>/bin/emcli list_agents_on_gold_image -version_name|-
image_name="gold_image_version_name|gold_image_name" [-
agent_name="agent_name_pattern"]
```

Note that the parameters mentioned in [ ] are optional.

Specify the -version_name parameter to view the Management Agents that were deployed or updated using a particular Agent Gold Image version.

Specify the -image_name parameter to view the number of Management Agents deployed for given Agent Gold Image.

Specify the -agent_name parameter to view only the Management Agents that match the specified name pattern.

For example, to display the Management Agents that were deployed or updated using the Agent Gold Image OPC_AGI_DB_JUL_13, run the following command:

```
$<OMS_HOME>/bin/emcli list_agents_on_gold_image -version_name=OPC_AGI_DB_JUL_13
```

To display the number of Management Agents that were deployed or updated using any of the Agent Gold Image versions that are part of the gold image OPC_DB_MONITORING, run the following command:

```
$<OMS_HOME>/bin/emcli list_agents_on_gold_image -image_name=OPC_DB_MONITORING
```

Viewing Notifications Related to Agent Gold Images

To view notifications related to Agent Gold Images, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. On the Gold Agent Images page, in the Notifications section that is on the right, view the notifications pertaining to gold images.

Viewing Agent Gold Images with Pending Updates

To view the Agent Gold Images with pending updates, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. On the Gold Agent Images page, in the Actions Required section that is on the right, view the pending updates against the gold images.
3. To drill down further and update the Management Agents with the latest gold image version, click the gold image name.

Viewing the Last Agent Gold Image That Was Changed

To view the last Agent Gold Image that was changed, follow these steps:

1. From the **Setup** menu, select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. On the Gold Agent Images page, in the Last Image Change section that is on the right, view the date and time stamp of the gold image that was last changed.

Viewing the Log Files Related to Agent Gold Image

To view the log files related to Agent Gold Image, see Overview of the Installation and Configuration Log Files .

Viewing the Status of Unsubscribed Operations Using EM CLI

To view the status of unsubscribed operations, follow these steps:

1. Log in to EM CLI from the /bin directory present within the Oracle home:

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.
2. Synchronize EM CLI:

   ```
   $<ORACLE_HOME>/bin/emcli sync
   ```
3. Run the `emcli get_agent_unsubscribe_status` verb to view the status of unsubscribed operations:

   ```
   <ORACLE_HOME>/bin/emcli get_agent_unsubscribe_status
      -version_name | -op_name
      [-agent="agent_name_pattern"]
      [-severity="ERROR|WARNING"]
      [-severity_id="severity_id"]
   [-status="PendingUpdateInprogress|Updatable|NotUpdatable|NotExecuted|Success|
   Inprogress|Failed"]
   ```

Note the parameters mentioned in [ ] are optional.

Table 13-15 lists and describes the parameters supported for viewing the status of unsubscribed operations using EM CLI.

> **Note:**
>
> It is mandatory to specify the -op_name parameter or the -version_name parameter. If you have specified -severity or -severity_id, then ensure that you do not specify -version_name or -status.

Table 13-15 Supported Parameters for Viewing the Status of Unsubscribed Operations

Parameters	Description
-version_name	Version name of the unsubscribed Agent Gold Image.
--op_name	Operation name of the unsubscribed Agent Gold Image.
-agent	Agent name of the unsubscribed Agent Gold Image.
-severity	Severity status of the Agent Gold Image.
-severity_id	Severity ID of the Agent Gold Image.
-status	Status of the unsubscribed Agent Gold Image.

Examples:

- The following example displays the details of the unsubscribe operations submitted for the Agent Gold Image version 'OPC_AGT_ADC_POD_JUNE':

```
emcli get_agent_unsubscribe_status -version_name="OPC_AGT_ADC_POD_JUNE"
```

- The following example displays the details of the unsubscribe operations submitted for the Agent Gold Image 'OPC_AGT_ADC_POD_JUNE', for the Management Agent xyz.example.com:1243:

```
emcli get_agent_unsubscribe_status -version_name="OPC_AGT_ADC_POD_JUNE" -
agent="xyz.example.com:1243"
```

- The following example displays the details of the unsubscribe operations submitted for the Agent Gold Image 'OPC_AGT_ADC_POD_JUNE', for the Management Agent xyz.example.com:1243, that have their status as 'Failed':

```
emcli get_agent_unsubscribe_status -version_name="OPC_AGT_ADC_POD_JUNE" -
agent="xyz.example.com:1243" -status="Failed"
```

- The following example displays the details of the unsubscribe operation 'UNSUBSCRIBE_JOB123':

```
emcli get_agent_unsubscribe_status  -op_name="UNSUBSCRIBE_JOB123"
```

- The following example displays the details of the unsubscribe operation 'UNSUBSCRIBE_JOB123' for the Management Agent xyz.example.com:1243, having the status 'Failed':

```
emcli get_agent_unsubscribe_status -op_name="UNSUBSCRIBE_JOB123" -
status="Failed" -agent="xyz.example.com:1243"
```

Viewing a List of Management Agents Subscribed to a Given Agent Gold Image Using EM CLI

To view a list of Management Agents subscribed to a given Agent Gold Image, follow these steps:

1. Log in to EM CLI from the /bin directory present within the Oracle home:

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<ORACLE_HOME>/bin/emcli sync
   ```

3. Run the emcli list_gold_image_subscribed_agent verb to view the status of unsubscribed operations:

   ```
   <ORACLE_HOME>/bin/emcli list_gold_image_subscribed_agent
       -image_name="gold_image_name"
       [-noheader]
       [-script | -format=
       [name:<pretty|script|csv>];
       [column_separator:"column_sep_string"];
       [row_separator:"row_sep_string"];
   ]
   ```

   Note the parameters mentioned in [ ] are optional.

   Table 13-16 lists and describes the parameters supported to view the list of all agents subscribed to a given Management Gold image.

Table 13-16 Supported Parameters for Viewing the List of Management Agents Subscribed to a Given Agent Gold Image

Parameters	Description
-image_name	Image name of a particular Management Agent that is subscribed to an Agent Gold Image.
-noheader	A tabular form of the output without column headers.
-script	This is equivalent to -format="name:script".
-format	Defines the format of a particular Management Agent that is subscribed to an Agent Gold Image.

Example:

The following example displays all the agents subscribed to OPC_DB_MONITORING image:

```
emcli list_gold_image_subscribed_agent -image_name=OPC_DB_MONITORING
```

Creating an Agent Gold Image Update Policy and Defining the Default Values To Be Set for Management Agent Upgrade

To create an Agent Gold Image Update Policy and to define default values for Management Agent Upgrade, use either of the following methods:

- Creating an Agent Gold Image Update Policy and Defining the Default Values to be Set for Management Agent Update Using the Gold Agent Images Home Page
- Creating an Agent Gold Image Update Policy and Defining the Default Values To Be Set for Management Agent Upgrade Using EM CLI

Creating an Agent Gold Image Update Policy and Defining the Default Values to be Set for Management Agent Update Using the Gold Agent Images Home Page

To create an Agent gold image update policy and define the default values for agent update, follow these steps:

1. From the **Setup** menu , select **Manage Enterprise Manager,** then select **Gold Agent Images.**
2. On the Gold Agent Images page, in the Policy Settings section that is on the right, click the **Policy Setting** icon.
3. In the Property Description table, select a row, then click **Edit** and set the value.

Creating an Agent Gold Image Update Policy and Defining the Default Values To Be Set for Management Agent Upgrade Using EM CLI

To create an Agent Gold Image Update Policy and to define default values for Management Agent Upgrade using EM CLI, follow these steps:

1. Log in to EM CLI from the /bin directory present within the Oracle home:

   ```
   $<ORACLE_HOME>/bin/emcli login -username=<user_name>
   ```

   Once you run this command, EM CLI will prompt you for a password. Enter the password for the user name you specified.

2. Synchronize EM CLI:

   ```
   $<ORACLE_HOME>/bin/emcli sync
   ```

3. Run the emcli set_gold_agent_update_policy verb to define default values for Management Agent Upgrade:

   ```
   <ORACLE_HOME>/bin/emcli set_gold_agent_update_policy
           [-additional_parameters="Additional_parameters seperated by space"]
           [-pre_script_loc="Absolute path of Prescript location"]
           [-post_script_loc="Absolute path of Postscript location"]
           [-is_pre_script_on_oms="true/false"]
           [-is_post_script_on_oms="true/false"]
           [-stage_location="Absolute path of stage location]
           [-is_staged="true/false"]
           [-stage_action="Stage action]
   ```

```
[-batch_size="Batch size"]
[-frequency="Frequency"]
[-success_rate="Success rate"]
[-update_profile="true/false"]
[-profile_path="Profile path"]
[-email="Email IDs separated by comma"]
[-run_preCleanup="true/false"]
[-run_postCleanup="true/false"]
```

Note the parameters mentioned in [ ] are optional.

Table 13-17 lists and describes the parameters supported to upgrade and define default values for Management Agents.

Table 13-17 Supported Parameters for Upgrading Agents and Defining Default Values

Parameters	Description
-additional_parameters	Additional parameters set in the repository to create an Agent Gold Image Policy.
-pre_script_loc	Prescript location set in the repository to create an Agent Gold Image Policy.
-post_script_loc	Postscript location set in the repository to create an Agent Gold Image Policy.
-is_pre_script_on_oms	Value set in the repository for this parameter to create an Agent Gold Image Policy.
-is_post_script_on_oms	Value set in the repository for this parameter to create an Agent Gold Image Policy.
-stage_location	Stage location value set in the repository to create an Agent Gold Image Policy.
-is_staged	Value set for this parameter in the repository to create an Agent Gold Image Policy.
-stage_action	Value set for stage action in the repository to create an Agent Gold Image Policy.
-batch_size	Value set for batch size in the repository to create an Agent Gold Image Policy.
-frequency	Value set for frequency in the repository to create an Agent Gold Image Policy.
-success_rate	Value set for success rate in the repository to create an Agent Gold Image Policy.
-update_profile	Value set for update profile in the repository to create an Agent Gold Image Policy.
-profile_path	Value set for profile path in the repository to create an Agent Gold Image Policy.
-email	Email set in the repository to create an Agent Gold Image Policy.
-run_preCleanup	Value set for this parameter to create an Agent Gold Image Policy.
-run_postCleanup	Value set for this parameter to create an Agent Gold Image Policy.

Examples:

- The following example sets additional parameters in the repository:

  ```
  emcli set_gold_agent_update_policy -additional_parameters=-ignorePrereqs
  ```

- The following example sets prescript location in the repository:

  ```
  emcli set_gold_agent_update_policy -pre_script_loc=/home/john/pretscript
  ```

- The following example sets stage location in the repository:

  ```
  emcli set_gold_agent_update_policy -stage_location=/scratch/tmp
  ```

- The following example sets batch size in the repository:

  ```
  emcli set_gold_agent_update_policy -batch_size=100
  ```

- The following example sets the success rate in the repository:

```
emcli set_gold_agent_update_policy -success_rate=90
```

14

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 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 various Enterprise Manager components.

This chapter contains the following sections:

Planning to Configure a Firewall for the Enterprise Manager System

Firewall configuration should be the last phase of Enterprise Manager deployment. Before you configure your firewalls, verify that 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. After you verify, configure the firewall for the default ports described in What Ports Are Used for Installation?. The default ports are typically assigned while installing the Enterprise Manager system. However, while installing the Enterprise Manager system, if you had used any custom ports instead of the default ones, then make sure you configure the firewall for the custom ports.

If you are deploying the Enterprise Manager system in an environment where firewalls are already available, then make sure you open the default ports, or the custom ports that you want to use, 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.

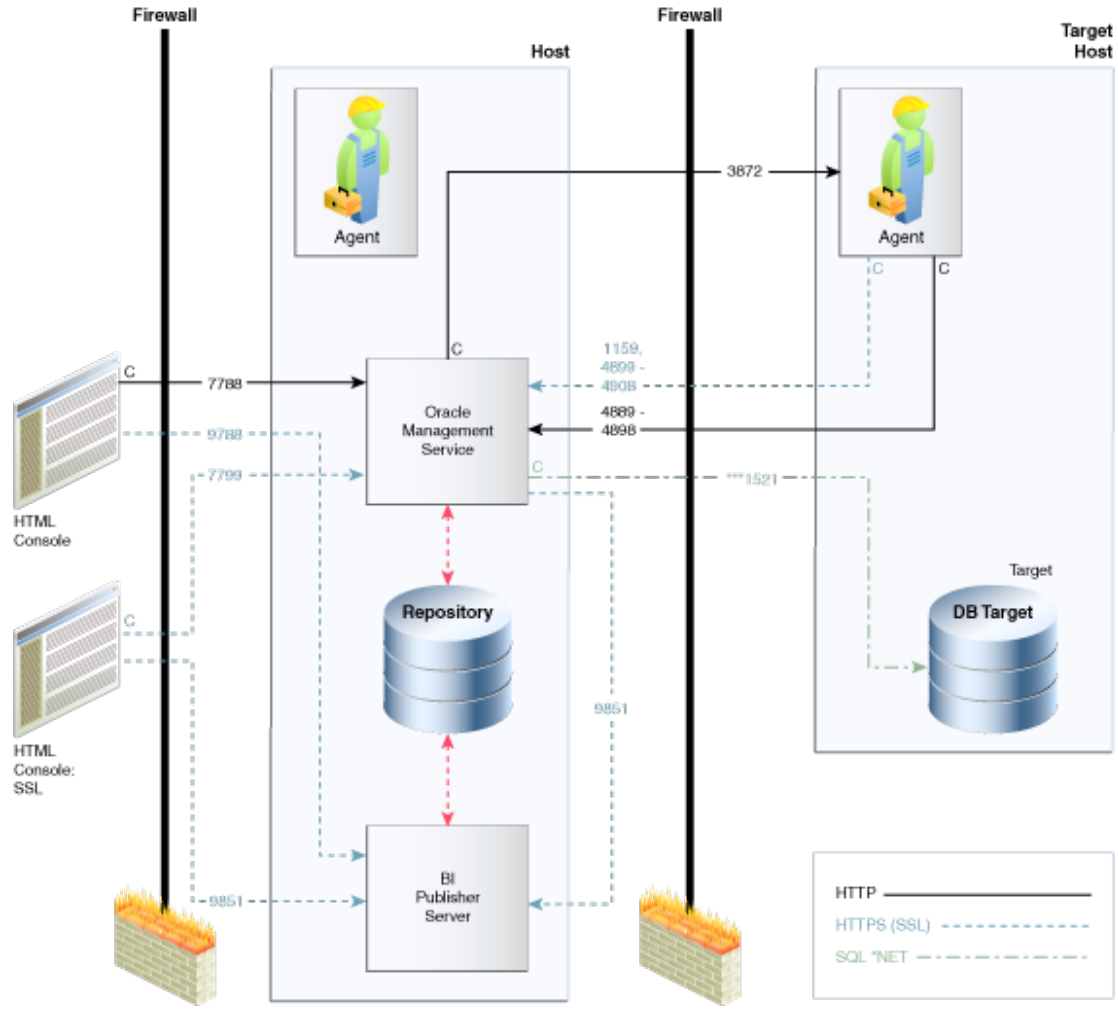
If you are enabling Enterprise Manager Framework Security for the Oracle Management Service (OMS), the final step in that configuration process is to restrict uploads from the Management Agents to secure channels only. Before completing that step, configure your firewalls to allow both HTTP and HTTPS 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.

Typical Firewall Configurations for the Enterprise Manager System

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 14-1 provides a topology of an Enterprise Manager environment that is using a firewall, and also illustrates the default ports that can be used.

Figure 14-1 Firewall Port Requirements (Default)



The conventions used in the preceding illustration are as follows:

Table 14-1 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.

> **Note:**
>
> - 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.

Configuring a Firewall Between the Web Browser and the Enterprise Manager System

Connections from your web browser to the Enterprise Manager system are performed over the default port used for the Oracle HTTP Server.

The default, non-secure port for the Oracle HTTP Server is 7788. If 7788 is not available, then the first available free port from the range 7788 - 7798 is selected. 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
```

If you have enabled security for your Oracle HTTP Server, then the secure port for the Oracle HTTP Server is 7799. If 7799 is not available, then the first available free port from the range 7799 - 7809 is selected. 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
```

Configuring an 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:

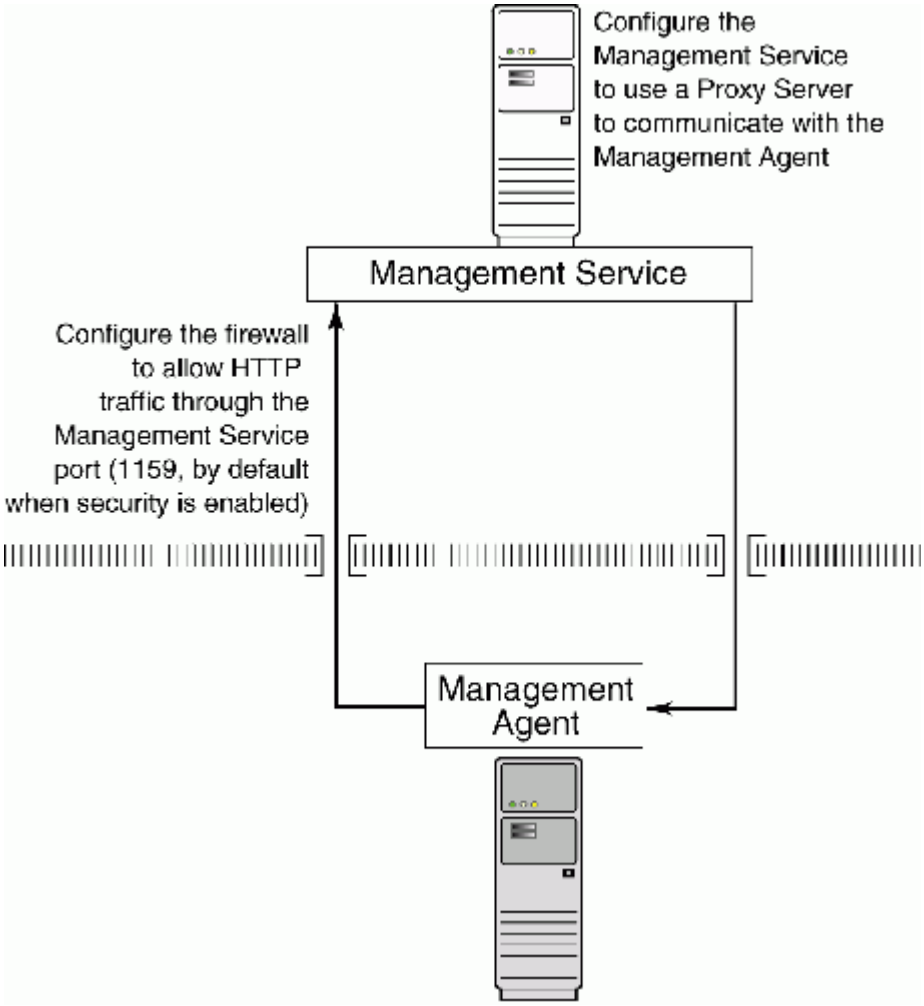
- Configure the OMS to use a proxy server for its communication with the Management Agents, as described in Configuring the OMS to Use a Proxy Server to Communicate with Management Agents.
- Configure the firewall to allow incoming HTTP and HTTPS traffic from the Management Agents on the Management Repository upload port.

  The default, non-secure upload port is 4889. If 4889 is not available, then the first available port in the range 4889 - 4897 is selected.

  If you have enabled Enterprise Manager Framework Security, then the secure upload port is 1159. If 1159 is not available, then the first available free port from the range 4899 to 4908 is selected.

Figure 14-2 illustrates the connections the Management Agent must make when it is protected by a firewall.

Figure 14-2 Configuration Tasks When the Management Service Is Behind a Firewall



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.

> **Note:**
>
> You can also configure the OMS to use multiple proxies for its communication with Management Agents. For information about configuring OMS and Management Agent, see Configuring Proxies for OMS and Management Agent Communication .

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:

   ```
   <ORACLE_HOME>/bin/emctl stop oms
   <ORACLE_HOME>/bin/emctl start oms
   ```

   To restart an OMS that runs on a Microsoft Windows platform, follow these steps:

   a. Right-click **My Computer,** then select **Manage.**
   b. In the Computer Management window, in the left pane, expand **Services and Applications,** then select **Services.**
   c. Select the `OracleManagementServer_EMGC_OMS*` service, then click the restart button.

Configuring a Management Agent on a Host Protected by a Firewall

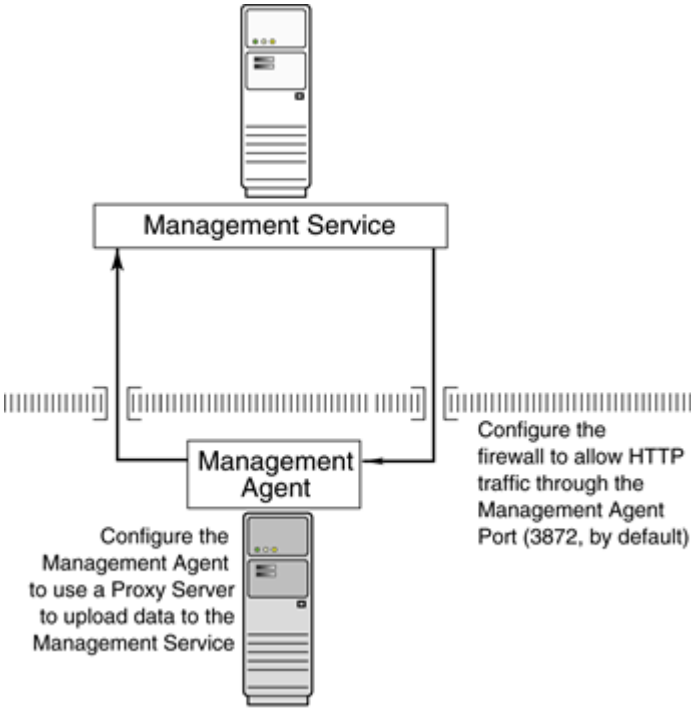
If a Management Agent is installed on a host that is protected by a firewall and the OMS is on the other side of the firewall, you must perform the following tasks:

- Configure the Management Agent to use a proxy server for its uploads to the OMS, as described in Configuring a Management Agent to Use a Proxy Server.
- Configure the firewall to allow incoming HTTP and HTTPS traffic from the OMS on the Management Agent port.

  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.

Figure 14-3 illustrates the connections the Management Agent must make when it is protected by a firewall.

Figure 14-3 Configuration Tasks When the Management Agent Is Behind a Firewall



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.

Configuring 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.

Configuring Firewalls Between the Enterprise Manager Console 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.

Configuring Firewalls for 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:**
  >
  > Configuring a Management Agent on a Host Protected by a Firewall
  >
  > Configuring an 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.

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`
- `login-ext.identity.oraclecloud.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.

Configuring 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
```

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 features of Enterprise Manager.

> **See Also:**
>
> "About " 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.

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.

15

Sizing Your Enterprise Manager Deployment

This section 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.
Oracle Enterprise Manager has the ability to scale for hundreds of users and thousands of systems and services on a single Enterprise Manager implementation.

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 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 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 Enterprise Manager Introduction . 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.

Overview of Sizing Guidelines

The following sections provide an overview of the sizing guidelines.

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 X4-2
- Hypervisor -- 64 bit Linux Oracle Virtual Server
- Operating System of Virtual Machines -- 64 bit Oracle 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 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.

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 15-1.

Table 15-1 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*
Extra Large	>= 5000	>=50,000	>=50, <=100

For larger user loads see Large Concurrent UI Load.

The Eval configuration is not meant for production environments. It is only to be used for trial and testing environments.

Extra Large is not an option while installing Enterprise Manager. You can configure your environment with the Extra Large settings if it matches the sizing criteria.

Sizing for Upgraded Installs

If upgrading from a previous release of Enterprise Manager to Enterprise Manager 24ai, 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'

Minimum Hardware Requirements

Table 15-2 lists the minimum hardware requirements for the four configurations.

Table 15-2 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	10	24	-	-	-
Small	1	4	10	24	1	4	7
Medium	2	6	12	24	2 (Oracle RAC)	6	10
Large	2 4	12 6	24 12	24 24	2 (Oracle RAC) 2 (Oracle RAC)	12 12	18 18
Extra Large	4	24	32	24	2 (Oracle RAC)	48	96

Table 15-3 Oracle Enterprise Manager Minimum Storage Requirements

Size	MGMT_TABLESPACE (GB)	MGMT_AD4J_TS (GB)	MGMT_ECM_DEPOT_TS (GB)	TEMP	ARCHIVE LOG AREA (GB
Eval	15	3	1	3	Archive log off
Small	100	10	1	12	25
Medium	300	30	4	20	100
Large	400	50	8	40	150
Extra Large	600	80	16	80	250

Network Topology Considerations

A critical consideration when deploying Enterprise Manager is network performance between tiers. Enterprise Manager 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 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 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.

Software Configurations

The following sections provide information about Eval, small, medium and large configurations.

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 1 GB.

Minimum Repository Database Settings

Table 15-4 below lists the minimum repository database settings that are recommended for an Eval configuration.

Table 15-4 Eval Configuration Minimum Database Settings

Parameter	Minimum Value
Processes	300
memory_target	1000 MB
redo log file size	50 MB
shared_pool_size	450 MB
session_cached_cursors	remove

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 15-5 lists the minimum recommended database settings.

Table 15-5 Small Site Minimum Database Settings

Parameter	Minimum Value
processes	300
pga_aggregate_target*	1024 MB
sga_target*	3 GB
redo log file size	300 MB
shared_pool_size	600 MB

> **Note:**
>
> *memory_target of 4 GB can be used in place of sga_target and pga_aggregate_target

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 15-6 lists the minimum repository database settings that are recommended for a Medium configuration.

Table 15-6 Medium Site Minimum Database Settings

Parameter	Minimum Value
processes	600
pga_aggregate_target*	1280 MB
sga_target*	5 GB
redo log file size	600 MB
shared_pool_size	600 MB

> **Note:**
>
> *memory_target of 6.25 GB can be used in place of sga_target and pga_aggregate_target

> **Note:**
>
> Processes count should be adjusted based on OMS nodes *300.

Large Configuration

The Large configuration modifies several out-of-box Oracle Enterprise Manager settings.

Minimum OMS Settings

Table 15-7 lists the minimum OMS settings that are recommended for Large configurations.

Table 15-7 Large Site Minimum OMS Settings

OMS Count	Heap Size Minimum Value
2	8192 MB
4	4096 MB

Minimum Repository Database Settings

Table 15-8 lists the minimum repository database settings that are recommended for a Large configuration.

Table 15-8 Large Site Minimum Database Settings

Parameter	Minimum Value
processes	1000
pga_aggregate_target*	1536 MB
sga_target*	8 GB
redo log file size	1000 MB
shared_pool_size	600 MB

> **Note:**
>
> *memory_target of 9.5 GB can be used in place of sga_target and pga_aggregate_target

Extra Large Configuration

The Extra Large configuration requires the following settings:

Minimum OMS Settings

Table 15-9 lists the minimum OMS settings that are recommended for Extra Large configurations.

Table 15-9 Extra Large Site Minimum OMS Settings

OMS Count	Heap Size Minimum Value
4	16384 MB

Minimum Repository Database Settings

Table 15-10 lists the minimum repository database settings that are recommended for a Extra Large configuration.

Table 15-10 Extra Large Site Minimum Database Settings

Parameter	Minimum Value
processes	2000
pga_aggregate_target*	6 GB
sga_target*	40 GB
redo log file size	2 GB
shared_pool_size	600 MB

> **Note:**
>
> It is recommended to set RAC services for ping alerts, jobs, rollup, events, and Config Metric Post Load Callbacks. For more information, see Step 4: Eliminating Bottlenecks Through Tuning.

Repository Tablespace Sizing

Table 15-11 lists the required minimum storage requirements for the Management Repository.

Table 15-11 Total Management Repository Storage

-	Minimum Tablespace Sizes*				
Development Size	**SYSTEM****	**MGMT_TABLESPACE**	**MGMT_ECM_DEPOT_TS**	**MGMT_AD4J_TS**	**TEMP**
Small	600 MB	100 GB	1 GB	10 GB	12 GB
Medium	600 MB	300 GB	4 GB	30 GB	20 GB
Large	600 MB	400 GB	Greater than 8 GB	50 GB	40 GB
Extra Large	600 MB	600 GB	16 GB	80 GB	80 GB

Additional Configurations

Some Enterprise Manager installations may need additional tuning settings based on larger individual system loads. Additional settings are listed below.

Large Concurrent UI Load

If more than 50 concurrent users are expected per OMS, the following settings should be altered as seen in Table 15-12.

Table 15-12 Large Concurrent UI Load Additional Settings

Process	Parameter	Value	Where To Set
OMS	-Djbo.recyclethreshold	Number of concurrent users / number of OMS	Per OMS

Table 15-12 (Cont.) Large Concurrent UI Load Additional Settings

Process	Parameter	Value	Where To Set
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 15-13 (based on a LARGE 2 OMS configuration).

Table 15-13 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	10 GB	8GB (standard large setting) + (150 users - 50 default large user load) * (1GB / 50 users)

Minimum Additional Hardware required is listed in Table 15-14.

Table 15-14 Large Concurrent UI Load Minimum Additional Hardware Example For 2 OMS Configuration

Tier	Parameter	Value	Calculation
OMS	CPU cores	32 (total between all OMS hosts)	12 cores * 2 OMS (default large core count) + (150 users - 50 default large user load) *(2 cores * 2 OMS)/ 50 users)
Database	CPU cores	32 (total between all Database hosts)	12 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 details about changing *Changing Djbo.ampool.maxavailablesize and Djbo.recyclethreshold (JAVA_EM_ARGS)*, see Changing OMS Properties.

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.

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 15-15 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*

> **Note:**
>
> *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.

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 - Small: 256M Medium: 256M Large: 256M For IBM JVM, irrespective of the app size, use the following settings: 32-bit: 1024M 64-bit: 1740M	Same as mentioned in the Default section. 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 – Small/Medium/Large: 1524M 64 bit - Small: 1740M Medium: 4096M Large: 8192M For IBM JVM, irrespective of the app size, there are no limits on the heap size.	Same as mentioned in the Default section. 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 - Small: 128M Medium: 128M Large: 128M For IBM JVM, irrespective of the app size, use the following settings: 32-bit: 128M 64-bit: 128M	Same as mentioned in the Default section. 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 – Small/Medium/Large: 612M 64 bit - Small: 612M Medium: 768M Large: 768M For IBM JVM, irrespective of the app size, use the following settings: 32-bit: 612M 64-bit: 612M	Same as mentioned in the Default section. 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 - Defines 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"
```

After changing the property, the default value is 25.

> **Note:**
>
> Starting from Enterprise Manager 13.5 Release Update 2, the `shortPoolSize` parameter update is made hot deployable on OMS and does not require any OMS restart.

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"
```

After changing the property, the default value is 12.

> **Note:**
>
> Starting from Enterprise Manager 13.5 Release Update 2, the `longPoolSize` parameter update is made hot deployable on OMS and does not require any OMS restart.

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"
```

After changing the property, the default value is 10.

> **Note:**
>
> Starting from Enterprise Manager 13.5 Release Update 2, the `longSystemPoolSize` parameter update is made hot deployable on OMS and does not require any OMS restart.

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"
```

After changing the property, the default value is 25.

> **Note:**
>
> Starting from Enterprise Manager 13.5 Release Update 2, the `systemPoolSize` parameter update is made hot deployable on OMS and does not require any OMS restart.

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.

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:

Table 15-16 Scripts for Deployment Sizes for DB 19c

Size	Script
Small	`<DB_HOME>/assistance/dbca/templates/set_repo_param_<Database Version>_Database_SQL_for_<EM Version>_Small_deployment.sql`
Medium	`<DB_HOME>/assistance/dbca/templates/set_repo_param_<Database Version>_Database_SQL_for_<EM Version>_Medium_deployment.sql`
Large	`<DB_HOME>/assistance/dbca/templates/set_repo_param_<Database Version>_Database_SQL_for_<EM Version>_Large_deployment.sql`

> **Note:**
>
> The above scripts do not adjust MEMORY_TARGET/ SGA_TARGET/ PGA_AGGREGATE_TARGET so these parameters must be modified manually.

Enterprise Manager Performance Methodology

An accurate predictor of capacity at scale is the actual metric trend information from each individual Enterprise Manager 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 deployment. It also assists in keeping your deployment performing at an optimal level.

Here are the steps to follow to enact the Enterprise Manager sizing methodology:

1. If you have not already installed Enterprise Manager, choose a rough starting host configuration as listed in Table 15-1.
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 site, for the life of the deployment on a regular basis. These steps are essential to an efficient Enterprise Manager 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.

Step 1: Choosing a Starting Platform Enterprise Manager Deployment

For information about choosing a starting platform Enterprise Manager deployment, see Overview of Sizing Guidelines.

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 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 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 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)
-	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

Module	Metrics	EM Site 1	EM Site 2
-	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 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 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.

Another crucial vital sign to monitor on the Enterprise Manager console is the self-monitoring Managing the Manager Repository pages which provide visibility into the inflow of metrics and events. Fine tuning incoming metric and events data is crucial for maintaining overall Enterprise Manager health and performance.

The next step provides guidance of what to do when the vital sign values are not within established baseline thresholds, though the inflow trend of Metrics and Events data in the self-monitoring pages does not show any abnormality. Also, it explains how to maintain your site's performance through routine housekeeping.

Step 3: Using DBA and Enterprise Manager Tasks To Eliminate Bottlenecks

It is critical to note that routine housekeeping helps keep your Enterprise Manager site running well. The following are lists of housekeeping tasks and the interval on which they should be done.

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.

Step 4: Eliminating Bottlenecks Through Tuning

The most common causes of performance bottlenecks in the Enterprise Manager 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 application. The vital signs listed in the previous table reflect key points of resource utilization and throughput in Enterprise Manager. 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.

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. Check out Top Wait Events metrics for the Enterprise Manager Repository.
    b. 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.

c. Check the Database Locks on the Management Repository's Database Performance page looking for any contention issues.

d. 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 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 steps 3.a, 3b, 3c, and 3.d listed above. CPU should be always be the topmost wait event. Log File Sync wait event indicating slow I/O performance should not appear in the top 5 waits ideally. To identify the root cause, start at the Management Repository Performance page and work your way down to the SQL that is consuming the most CPU in its processing. Correlate your findings with the AWR report. 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 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.

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.

Ensure that back-off requests are spread uniformly across OMS in a multi-OMS environment. If the back-off requests pertain to a specific OMS and does not show uniform trend across OMS, verify that the load-balancing algorithm set at Server Load Balancer is round-robin. Add loader threads only if there are backoffs on important channels in the range of hundreds an hour consistently and there are sufficient free resources on the database.

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.

Rollup Vital Signs

The rollup process is the aggregation mechanism for Enterprise Manager. 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 performance is struggling because of it. There will be times when increasing buffer cache will not help improve performance for Enterprise Manager. 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. Enterprise Manager 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 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 Enterprise Manager 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.

Rollup Process

If rollup % of hour run is trending up (or is higher than your baseline) and buffer cache is already set to optimal but there is still many cluster Wait events reported in the AWR report, configure the Rollup database service and set affinity to run the Rollup Service only on a single-instance RAC node. Ensure that single-instance RAC node is sized to handle large I/O volume.

Use the following configuration steps for Rollup database service:

1. Create database service "rollup" and set one of the RAC instances as the primary instance in "-r".
   - srvctl add service -d <dbname>-s rollup -r <primary instance> -a <the other instances> -y automatic
   - srvctl start service -d <dbname>-s rollup

     srvctl status service -d <dbname>
2. As sys user, execute DBMS_SCHEDULER.create_job_class(job_class_name => 'ROLLUP', service => 'rollup')
3. GRANT EXECUTE ON sys.ROLLUP TO sysman;
4. As sysman user, execute DBMS_SCHEDULER.SET_ATTRIBUTE (name => 'EM_ROLLUP_SCHED_JOB', attribute => 'job_class', value => 'ROLLUP')
5. As sysman user, execute GC_SCHED_JOB_REGISTRAR.SET_JOB_CLASS('EM_ROLLUP_SCHED_JOB', 'ROLLUP')

In addition to configuration of Rollup database service, add Rollup worker threads if the database can handle the increased load from these threads. Configure additional rollup worker threads using configure option in Metric Rollup Performance Chart available in self- monitoring "Managing the Manager" Repository page.

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 site.

Jobs

A growing backlog in Jobs Steps Scheduled at the repository indicates there are not enough resources available at the repository. High Job Dispatcher processing time (%) indicates a repository bottleneck. Low throughput with High Job Dispatcher processing time (%) indicates a processing bottleneck. The Jobs subsystem uses the locks to maintain sequence internally, so you can see application locks wait events, and transaction locking wait events in the AWR report in repository. It is normal to observe the Job system consuming 5-8% of waiting time, but if that value crosses 20-30%, it is quite abnormal and should be triaged. If there are significant amounts of cluster waits for Job SQLs in AWR, you could potentially optimize the Job system by introducing RAC services. Create a database service for Jobs and then set affinity to run on a two-node RAC instance for better optimal performance.

Use the following configuration steps to set up the Rollup database service:

1. Create the database service emjob and set two of the RAC instances as primary instance in "-r".

   ```
   srvctl add service -d <dbname> -s emjob -r <primary instances> -a <the other instances> -y automatic
   ```

   After creating the database service, you need to restart the service using the `srvctl start service` command.
2. Execute the following DBMS_SCHEDULER jobs:
   - As a sys user, execute DBMS_SCHEDULER.create_job_class(job_class_name => 'EMJOB', service => 'emjob ')
   - GRANT EXECUTE ON sys.EMJOB TO sysman;

- As a sysman user, execute DBMS_SCHEDULER.SET_ATTRIBUTE (name => ' EM_JOBS_STEP_SCHED ', attribute => 'job_class', value => 'EMJOB')
- As a sysman user, execute DBMS_SCHEDULER.SET_ATTRIBUTE (name => ' EM_JOB_PURGE_POLICIES ', attribute => 'job_class', value => 'EMJOB')
- As a sysman user, execute GC_SCHED_JOB_REGISTRAR.SET_JOB_CLASS('EM_JOBS_STEP_SCHED', 'EMJOB')
- As a sysman user, run GC_SCHED_JOB_REGISTRAR.SET_JOB_CLASS('EM_JOB_PURGE_POLICIES', 'EMJOB')
- INSERT INTO MGMT_PARAMETERS(parameter_name, parameter_value) VALUES ('EM_jobs_step_sched_job_class', 'EMJOB')

3. Set the connect string with *ping* service name to the emctl property

   oracle.sysman.core.omsAgentComm.ping.connectionService.connectDescriptor

   - **Sample**: `emctl set property -name "company.sysman.core.jobs.conn.service" -value "\(DESCRIPTION=\(ADDRESS_LIST=\(ADDRESS=\(PROTOCOL=TCP\)\(HOST=xxx.example.com\)\(PORT=1521\)\)\)\(CONNECT_DATA=\(SERVICE_NAME=emjob\)\)\)"`

Events and Notifications

If the vital sign has crossed the baseline threshold, look for vital signs in self-monitoring Managing the Manager pages. Monitor charts for consistent drastic increase in Metric alerts backlog, Metric Collection errors backlog, and Notification backlog. Key Metrics to check event backlogs are Total Events Pending and Total Events Processed (Last Hour). If Total Events Pending remains high but Total Events Processed (Last Hour) is making good progress, it could be a temporary spike which can be ignored, but if there is a consistent increase in both metrics, the Events subsystem will benefit by introducing a database service and setting affinity to only run on a single-instance RAC node.

Use these configuration steps for an Events database service:

1. Create a database service *event* and set one of the RAC instances as the primary instance in "-r"

   ```
   srvctl add service -d <dbname>-s event -r <primary instance> -a <the the other instances> -y automatic
   ```

2. Set the connect string with the 'ping' service name to the emctl property *oracle.sysman.core.events.connectDescriptor*

   Sample `emctl set property -name "oracle.sysman.core.events.connectDescriptor" -value "\(DESCRIPTION=\(ADDRESS_LIST=\(ADDRESS=\(PROTOCOL=TCP\)\(HOST=xxx.example.com\)\(PORT=1521\)\)\)\(CONNECT_DATA=\(SERVICE_NAME=event\)\)\)"`

Ping Alerts

Ping Alerts performance is crucial for determining target availability. If the vital signs have crossed a baseline threshold and there are many cluster waits in the AWR report, there is a measurable benefit by introducing a database service for Ping and setting affinity to run only on a single instance RAC node.

Use these configuration steps for defining a Pings database service:

1. Create database service *ping* and set one of RAC instance as primary instance in "-r"

```
srvctl add service -d <dbname>-s ping -r <primary instance> -a <the the other
instances> -y automatic
```

2. Execute the following DBMS_SCHEDULER jobs
   - As a sys user, execute DBMS_SCHEDULER.create_job_class(job_class_name => 'PING', service => 'ping')
   - GRANT EXECUTE ON sys.PING TO sysman;
   - As a sysman user, execute DBMS_SCHEDULER.SET_ATTRIBUTE (name => 'EM_PING_MARK_NODE_STATUS', attribute => 'job_class', value => 'PING')
   - As a sysman user, execute DBMS_SCHEDULER.SET_ATTRIBUTE (name => 'EM_REPOS_SEV_EVAL', attribute => 'job_class', value => 'PING')
   - As a sysman user, execute GC_SCHED_JOB_REGISTRAR.SET_JOB_CLASS('EM_REPOS_SEV_EVAL', 'PING')
   - As a sysman user, execute GC_SCHED_JOB_REGISTRAR.SET_JOB_CLASS('EM_PING_MARK_NODE_STATUS', 'PING')
3. Set the connect string with *ping* service name to emctl property *oracle.sysman.core.omsAgentComm.ping.connectionService.connectDescriptor*

   Sample

```
emctl set property -name
oracle.sysman.core.omsAgentComm.ping.connectionService.connectDescriptor" -
value "\(DESCRIPTION=\(ADDRESS_LIST=\(ADDRESS=\(PROTOCOL=TCP\)\
(HOST=xxx.example.com\)\(PORT=1521\)\)\)\(CONNECT_DATA=\(SERVICE_NAME=ping\)\)
\)
```

Config Metric Post Load Callbacks

The Config Metrics upload to OMS from Agents is a two step process:

1. Agents upload the Config Metric collections to OMS, OMS registers the upload in the Enterprise Manager Repository, generates a snapshot and then, feeds the uploaded payload (or data) into a queue, called as the Loader-Job Queue, for processing later. This allows the Loader module at OMS off-load the additional processing required with Config Metric Upload, and free up resources to process more uploads from Agents.
2. There is a separate module responsible for pulling the entries out of this queue, and then calling the callbacks responsible to work on the data and then assimilate the data in the repository in order of their insertion into the Loader-Job Queue. This module is referred to as the Config Metric Post Upload Callback Executor (or loader-job) module. This module allows the end user to configure the number of threads that will process the data, number of SQL connections to the Enterprise Manager Repository that these threads have access to, and whether to use a dedicated DB service pinned on one of the RAC nodes which hosts the Enterprise Manager Repository.

The default values of the settings on Eval, Small, and Medium Enterprise Manager site sizes works fine. You might need to override the default values for Large and Extra Large configurations.

To configure a DB Service and pin it to a Repository node

```
srvctl add service -d <dbname>-s loaderjob -r <primary instance> -a <the the
otherinstances> -y automatic
```

To configure a DB service as the connection source

```
emctl set property -name "oracle.sysman.core.pbs.gcloader.connectDescriptor" -value
"\(DESCRIPTION=\(ADDRESS_LIST=\(ADDRESS=\(PROTOCOL=TCP\)\(HOST=xxx.example.com\)\
(PORT=1521\)\)\)\(CONNECT_DATA=\(SERVICE_NAME=loaderjob\)\)\)"
```

Large

To configure the number of threads to be created for this module

```
emctl set property -name "oracle.sysman.core.pbs.gcloader.numThreads" -value 5
```

To configure the number of SQL connection available to the threads of this module

```
emctl set property -name "oracle.sysman.core.gcloader.loaderjob.maxConnections" -value 5
```

Extra Large

To configure the number of threads to be created for this module

```
emctl set property -name "oracle.sysman.core.pbs.gcloader.numThreads" -value 10
```

To configure the number of SQL connection available to the threads of this module

```
emctl set property -name "oracle.sysman.core.gcloader.loaderjob.maxConnections" -value 10
```

I/O Vital Signs

Monitoring the I/O throughput of the different channels in your Enterprise Manager 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 Enteprise Manager. You will then be notified automatically if you approach these thresholds on your site. Some site administrators can be unaware or mistaken about what these I/O channels can handle on their sites. This can lead to Enterprise Manager 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 Enterprise Manager 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 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 Enterprise Manager 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

Enterprise Manager 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 Enterprise Manager 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 repository database storage.

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.

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. This end-to-end (or E2E) monitoring functionality in Enterprise Manager 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 Enterprise Manager 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 Step 3: Using DBA and Enterprise Manager Tasks To Eliminate Bottlenecks. 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* guide.

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.

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 Enterprise Manager 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 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 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.

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.

Overview of 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 Enterprise Manager version 24ai, both ADP and JVMD use the Enterprise Manager repository as their repository. Their data are stored in the MGMT_AD4J_TS tablespace.

16

Configuring Proxies for OMS and Management Agent Communication

Oracle Management Service (OMS) and Oracle Management Agent (Management Agent) are core components of Enterprise Manager. While the Management Agents discover and monitor targets in your environment, the OMS orchestrates with the Management Agents to manage the discovered targets and to store the collected information in a repository for future reference and analysis.

For this purpose, OMS and Management Agents constantly communicate with each other. To manage the HTTP and HTTPS requests more efficiently and to add an additional layer of security, you can choose to secure this communication by configuring an HTTP or HTTPS-based proxy between the OMS and the Management Agents.

This chapter describes how you can configure an HTTP proxy to secure the communication between the OMS and the Management Agents. In particular, this chapter covers the following:

About Using Proxies for OMS and Management Agent Communication

Oracle Management Service (OMS) and Oracle Management Agent (Management Agent) are core components of Enterprise Manager. While the Management Agents discover and monitor targets in your environment, the OMS orchestrates with the Management Agents to manage the discovered targets and store the collected information in a repository for future reference and analysis. For this purpose, OMS and Management Agents constantly communicate with each other. To manage the HTTP and HTTPS requests more efficiently and to add an

additional layer of security, you can choose to secure this communication by configuring an HTTP or HTTPS-based proxy between the OMS and the Management Agents.

A proxy is an application external to Enterprise Manager that acts as an intermediary for managing HTTP as well as HTTPS requests across network boundaries or firewalls. By using a proxy, you can expose only certain ports for communication between two or more components, thus making the communication more secure and reliable.

In the earlier releases of Enterprise Manager, you had the option of configuring only one proxy for an OMS to communicate with its Management Agents. However, starting with Enterprise Manager 13*c* Release 1, you have the following proxy configuration options:

- No proxy at all.
- One proxy for all the Management Agents.
- One proxy for a few Management Agents and no proxy for the rest.
- Different proxies for the same group of Management Agents (redundant proxies).
- Different proxies for different groups of Management Agents.

A proxy is modeled and added as a manageable entity in Enterprise Manager, and is monitored much like other target type for its availability. Therefore, even a non-administrator can view the details of a proxy in Enterprise Manager. However, only administrators with full privileges on targets are permitted to modify the proxy configuration settings.

However, the proxies configured for Management Agent-to-OMS communication and for OMS-to-My Oracle Support communication are not modeled as target types and are not monitored in Enterprise Manager. Also, you cannot configure redundant proxies for them in any way.

In addition, starting with Enterprise Manager 13*c* Release 1, you can configure multiple proxies for the same group of Management Agents, as *redundant proxies,* to support high availability of the proxies configured for the OMS. In this case, since the OMS has multiple proxies configured to communicate with its Management Agents, the proxy that is up and running is selected for communication, regardless of the status of the other proxies.

> **Note:**
>
> - NTLM-based Microsoft proxies are not supported. To enable access through such proxies, add all the available agent hosts to the *Unauthenticated Sites Properties* of the NTLM-based Microsoft proxy.
> - Local addresses of each OMS automatically bypass the proxy.

Configuring Proxies for OMS-to-Management Agent Communication

You can secure the communication between Oracle Management Service (OMS) and Oracle Management Agents (Management Agents) by configuring a proxy. A proxy is an application external to Enterprise Manager that acts as an intermediary for managing HTTP as well as HTTPS requests across network boundaries or firewalls. By using a proxy, you can expose only certain ports for communication, and thereby have a more secure and reliable communication between the OMS and the Management Agents.

You can configure one proxy for all Management Agents, one proxy for a set of Management Agents and none for the rest, or different proxies for different sets of Management Agents.

In addition, you can configure two or more proxies as *redundant proxies* to support high availability of the proxies configured for OMS and Management Agent communication. Under such circumstances, by default, the proxy that is up and running is selected for communication, regardless of the status of the other proxies. Before starting to communicate if a proxy is found to be inactive or down, then an alternate proxy configured for that Management Agent is selected. However, note that after the communication begins through a particular proxy, if that proxy turns inactive or shuts down, then no fallback mechanism is currently available to select an alternate proxy that is up and running.

> **Note:**
>
> - NTLM-based Microsoft proxies are not supported. To enable access through such proxies, add all the available agent hosts to the *Unauthenticated Sites Properties* of the NTLM-based Microsoft proxy.
> - Local addresses of each OMS automatically bypass the proxy.

To configure proxies for OMS and Management Agent communication, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, click **Create.**
3. On the Create a Proxy page, do the following:
   a. In the **Name** field, enter a unique name for the proxy you are configuring. This is the name with which the proxy is modeled as a target type and monitored in Enterprise Manager. For example, `oms-agent_proxy1`.
   b. In the **Host** field, enter the name of the host on which the proxy resides. For example, `www-proxy.example.com`.
   c. In the **Port** field, enter the port used by the proxy.
   d. From the **Protocol** options, select an appropriate protocol, either **HTTP** or **HTTPS.**
   e. To verify if the OMS is able to successfully connect to the proxy you have specified, click **Test Proxy.**
4. If the proxy you are configuring is set up using a realm, or login credentials, or both, then select **Associate a Named Credential,** and in the Named Credential section, select the registered named credential you want to use.

   > **Note:**
   >
   > If a named credential is not available for selection, then create a new one. To do so, from the **Setup** menu, select **Security,** then select **Named Credentials.** On the Named Credentials page, click **Create.** On the Create Credential page, in the General Properties section, enter a unique name for the credential, set **Authenticating Target Type** to **Host, Credential Type** to **Host Credentials,** and **Scope** to **Global.** In the Credential Properties section, enter the user name and password. Click **Save.**

5. In the Associated Agents section, select the Management Agents that should communicate with the OMS using the proxy you are configuring. Select the Management Agents in one of the following ways. After selecting, if you want to verify if the Management Agents are able to successfully communicate with the proxy, click **Test.**

   - Click **Select Agents,** and in the Select Targets dialog, select one or more Management Agents.

     This option is particularly useful when you have a short list of Management Agents, each with unique names, to select. For example, `agent1.example.com, agent2.example.com, agent3.example.com.`

   - In the **Agent Patterns** field, enter the agent patterns of the Management Agents. Use comma (,) to separate individual patterns. Use asterisk (*) to represent zero or more characters, and a question mark (?) to represent a single character.

     This option is particularly useful when you have a short list of Management Agents, all with common prefixes to their unique names, to select. For example, to select all Management Agents running in Australia that start with the prefix `aus_agent,` such as `aus_agent1.example, aus_agent2.example, aus_agent3.example.com`. In this case, enter `aus_agent*`.

     > **Note:**
     >
     > If a backslash (\) character precedes either a star (*), a question mark (?), a comma (,) or a backslash (\) itself in the pattern, it hides the special meaning associated with the following character. For example, while the pattern abc* matches with any string prefixed by the string: abc, the pattern abc* matches with just one string: abc* .

   - In the **Excluded Agent Patterns** field, enter the agent patterns of the Management Agents that you want to exclude from associating with the proxy you are configuring, and include all the other Management Agents. Use comma (,) to separate individual patterns. Use asterisk (*) to represent zero or more characters, and a question mark (?) to represent a single character.

     This option is particularly useful when you have a long list of Management Agents you want to exclude, each with either fully unique names or with common prefixes to their unique names. For example, to exclude all the Management Agents running in Hong Kong that start with the prefix `hkg_agent,` such as `hkg_agent1.example.com, hkg_agent2.example.com, hkg_agent3.example.com.`

     > **Note:**
     >
     > Excluded Agent Patterns do not exclude the Management Agents from the list of Management Agents selected by their names. They exclude only those Management Agents that are derived from the agent patterns you have entered in the **Agent Patterns** field.

6. Click **Submit.**

Configuring Proxies for Management Agent-to-OMS Communication After the Management Agent Is Deployed

You can secure the communication between the Management Agents and the OMS by configuring a proxy. A proxy is an application external to Enterprise Manager that acts as an intermediary for managing HTTP as well as HTTPS requests across network boundaries or firewalls. By using a proxy, you can expose only certain ports for communication, and thereby have a more secure and reliable communication between the Management Agents and the OMS.

You can configure a proxy between the Management Agent and the OMS, after deploying the Management Agent, either using the Enterprise Manager Console or using the command-line interface *(EMCTL commands)*.

To configure a proxy between the Management Agent and the OMS, after deploying the Management Agent, using the Enterprise Manager Console, follow these steps:

1. From the **Targets** menu, select **All Targets.**
2. On the All Targets page, in the Refine Search pane, under the heading **Target Type,** scroll down and expand the subheading **Internal.** Then click **Agent.**
3. From the list of Management Agents, click the Management Agent for which you want to configure the proxy.
4. On the Agent Home page, from the **Agent** menu, select **Properties.**
5. On the Properties page, from the **Show** drop down list, select **Advanced Properties.**
6. Expand **Runtime Settings.**
7. Set the following properties:

   `REPOSITORY_PROXYHOST`

   `REPOSITORY_PROXYPORT`

   `REPOSITORY_PROXYPWD`

   `REPOSITORY_PROXYREALM`

   `REPOSITORY_PROXYUSER`
8. Click **Apply.**

To configure a proxy between the Management Agent and the OMS, after deploying the Management Agent, using the command-line interface (EMCTL), follow these steps:

1. Set the proxy properties in the `<AGENT_HOME>/sysman/config/emd.properties` file. To do so, run the following EMCTL commands from the Management Agent home:

   ```
   emctl setproperty agent -name REPOSITORY_PROXYHOST -value <proxy_host>

   emctl setproperty agent -name REPOSITORY_PROXYPORT -value <proxy_port>

   emctl setproperty agent -name REPOSITORY_PROXYREALM –value <proxy_realm>

   emctl setproperty agent -name REPOSITORY_PROXYUSER –value <proxy_user>

   emctl setproperty agent -name REPOSITORY_PROXYPWD –value <proxy_password>
   ```

   For example,

   ```
   emctl setproperty agent -name REPOSITORY_PROXYHOST -value www-proxy.example.com
   emctl setproperty agent -name REPOSITORY_PROXYPORT -value 80
   ```

```
emctl setproperty agent -name REPOSITORY_PROXYREALM -value realm1
emctl setproperty agent -name REPOSITORY_PROXYUSER -value u01
emctl setproperty agent -name REPOSITORY_PROXYPWD -value password
```

2. Restart the Management Agent.

Configuring Proxies for Management Agent-to-OMS Communication While Deploying the Management Agent

You can secure the communication between the Management Agents and the OMS by configuring a proxy. A proxy is an application external to Enterprise Manager that acts as an intermediary for managing HTTP as well as HTTPS requests across network boundaries or firewalls. By using a proxy, you can expose only certain ports for communication, and thereby have a more secure and reliable communication between the Management Agents and the OMS.

To configure a proxy between the Management Agent and the OMS while deploying the Management Agent, follow the steps outlined in *Installing Management Agents Using an Agent Gold Image Using Add Host Targets Wizard* or *Provisioning Management Agents Using An Agent Gold Image*, and deploy the Management Agent. While providing the details for Management Agent deployment, on the Installation Details page of the Add Target Wizard, expand the Optional Details section, and in the **Additional Parameters** field, enter the following parameters with the appropriate proxy settings. Separate the parameters with a comma (,).

`REPORSITORY_PROXYHOST=<proxy_host_name>, REPORSITORY_PROXYPORT=<proxy_host_port>`

For example,

`REPORSITORY_PROXYHOST=www-proxy.example.com, REPORSITORY_PROXYPORT=1523`

Configuring Proxies for OMS-to-My Oracle Support Communication

Oracle Management Service (OMS) uses the Internet connectivity on its host to connect to My Oracle Support periodically to download patches, patch sets, patch recommendations, and Automated Release Updates (ARU) seed data. To secure this communication, you can add a proxy between the OMS and My Oracle Support.

To configure a proxy between the OMS and My Oracle Support, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **My Oracle Support.**
2. On the Proxy Settings for My Oracle Support page, select **Manual Proxy Configuration.**
3. In the **HTTPS** field, enter the name of the host where the proxy resides. For example, `www-proxy.example.com`.
4. In the **Port** field, enter the port used by the proxy.
5. If the specified proxy is configured using a security realm, login credentials, or both, then select **Password/Advanced Setup** and enter the realm and the credentials.
6. To verify if the OMS can successfully connect to My Oracle Support using the specified proxy details, click **Test.**
7. If the connection is successful, click **Apply.**

Note:

- The proxy you configure applies to all OMS instances in a multi-OMS environment.
- If you are using a proxy in your setup, ensure that it allows connectivity to `aru-akam.oracle.com`, `ccr.oracle.com`, `login.oracle.com`, `support.oracle.com`, and `updates.oracle.com`.

  NTLM or NT LAN Manager-based Microsoft proxies are not supported. If you are using an NTLM-based Microsoft proxy to enable access to the aforementioned sites, then add the aforementioned URLs to the *Unauthenticated Sites Properties* of the proxy.

Updating Proxies Configured for OMS-to-Management Agent Communication

You can modify the proxy you have configured for secure communication between Oracle Management Service (OMS) and Oracle Management Agents (Management Agent). You might want to modify the proxy port, the protocol, the credentials, or a more common requirement—you might want to add more or remove some Management Agents that are associated with the proxy.

Note:

You cannot modify the proxy name with which the proxy is monitored in Enterprise Manager, and you cannot map a different proxy to the proxy name.

To update or modify the proxy configured for OMS and Management Agent communication, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, select the proxy (the row in the table) you want to update, and click **Modify.**
3. On the Modify a Proxy page, edit the port, the protocol, the named credentials, or the Management Agents associated with the proxy.

   For instructions to update the port, the protocol, and the proxy credentials, see Configuring Proxies for OMS-to-Management Agent Communication.

   For instructions to associate additional Management Agents to an existing proxy, see Associating Additional Management Agents to an Existing Proxy to Communicate with the OMS. For instructions to exclude Management Agents from using an existing proxy, see Excluding Management Agents from Using Proxies to Communicate with the OMS.

Associating Additional Management Agents to an Existing Proxy to Communicate with the OMS

You can secure the communication between Oracle Management Service (OMS) and Oracle Management Agents (Management Agent) by configuring a proxy and associating a set of Management Agents to communicate with the OMS only through that proxy. Under certain circumstances, after configuring a proxy, you might have to modify the proxy to include additional Management Agents to communicate using that proxy.

To associate additional Management Agents to an existing proxy, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, select the proxy (the row in the table) you want to modify to exclude the Management Agents, and click **Modify.**
3. On the Modify Proxy page, do one of the following:
   - In the Associated Agents section, click **Select Agents,** and in the Select Targets dialog, select one or more Management Agents.

     This option is particularly useful when you have a short list of Management Agents, each with unique names, to select. For example, `agent1.example.com, agent2.example.com, agent3.example.com`.
   - In the Associated Agents section, in the **Agent Patterns** field, enter the agent patterns of the Management Agents. Use comma (,) to separate individual patterns. Use asterisk (*) to represent zero or more characters, and a question mark (?) to represent a single character.

     This option is particularly useful when you have a short list of Management Agents, all with common prefixes to their unique names, to select. For example, to select all Management Agents running in Australia that start with the prefix `aus_agent`, such as `aus_agent1.example, aus_agent2.example, aus_agent3.example.com`. In this case, enter `aus_agent*`.

     > **Note:**
     >
     > If a backslash (\) character precedes either a star (*), a question mark (?), a comma (,) or a backslash (\) itself in the pattern, it hides the special meaning associated with the following character. For example, while the pattern abc* matches with any string prefixed by the string: abc, the pattern abc* matches with just one string: abc* .

     You can also use the **Agent Patterns** field in combination with the **Excluded Agent Patterns** field to add any additional Management Agents to the list. For example, if you have 100 Management Agents in Australia that start with the prefix `aus_agent`, and if you want to exclude `aus_agent98.example, aus_agent99.example.com`, and `aus_agent100.example.com`, then you can enter `aus_agent*` in the **Agent Patterns** field, and enter `aus_agent98.example, aus_agent99.example.com`, and `aus_agent100.example.com` in the **Excluded Agent Patterns** field.

Excluding Management Agents from Using Proxies to Communicate with the OMS

You can secure the communication between Oracle Management Service (OMS) and Oracle Management Agents (Management Agent) by configuring a proxy and associating a set of Management Agents to communicate with the OMS only through that proxy. However, under certain circumstances, after configuring a proxy, you might have to modify it to exclude some Management Agents from using that proxy, and have only the remaining Management Agents use that proxy.

To exclude Management Agents from using a proxy to communicate with the OMS, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, select the proxy (the row in the table) you want to modify to exclude the Management Agents, and click **Modify.**
3. On the Modify Proxy page, do one of the following:
   - In the Associated Agents section, select the Management Agents you want to exclude, and click **Remove Agents.**
   - In the Associated Agents section, in the **Excluded Agent Patterns** field, enter the agent patterns of the Management Agents that you want to exclude. Use comma (,) to separate individual patterns. Use asterisk (*) to represent zero or more characters, and a question mark (?) to represent a single character.

     This option is particularly useful when you have a long list of Management Agents you want to exclude, each with either fully unique names or with common prefixes to their unique names. For example, to exclude all the Management Agents running in Hong Kong that start with the prefix `hkg_agent`, such as `hkg_agent1.example.com`, `hkg_agent2.example.com`, `hkg_agent3.example.com`, enter `hkg_agent*` in the **Excluded Agent Patterns** field.

> **Note:**
>
> Excluded Agent Patterns do not exclude the Management Agents from the list of Management Agents selected by their names. They exclude only those Management Agents that are derived from the agent patterns you have entered in the **Agent Patterns** field.

Viewing a List of Proxies by Proxy Names or Management Agents

To view a list of proxies configured for OMS and Management Agent communication, from the **Setup** menu, select **Proxy Settings,** then select **Agents.**

By default, the proxies are sorted by proxy names.

- To search for a particular proxy, in the **Search Proxy** section, enter the proxy name and click the search icon. You can enter the full proxy name, a few characters of the proxy

name, or the percentage (%) wildcard character. The table filters itself to list the proxy you searched for.

- To drill down and view more details about a proxy, in the **Proxy Name** column, click the proxy name.
- To view a list of Management Agents that are associated with a proxy, select a proxy name row in the table and view the details in the **Associated Agents** table.
- To drill down further and view more details about a Management Agent that is associated with a particular proxy, in the **Agent Name** column of the **Associated Agents** section, click the Management Agent name.

To sort the proxies by Management Agent names, from the **View by** options, select **Agents.**

- To drill down and view more details about the Management Agent, in the **Agent Name** column, click the Management Agent name.
- To drill down and view more details about the proxy, in the **Associated Proxy Targets** column, click the proxy name.

Monitoring Proxies Configured for OMS-to-Management Agent Communication

All proxies configured for OMS to Management Agent communication are modeled as targets in Enterprise Manager. To monitor a proxy, you must access its Home page from either the Proxy page or from the All Targets page.

To access the Home page of a particular proxy from the Proxy page, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, in the **Proxy Name** column, click the proxy name.

To access the Home page of a particular proxy from the All Targets page, follow these steps:

1. From the **Targets** menu, select **All Targets.**
2. On the All Targets page, in the Refine Search pane, expand **Others,** then click **Proxy.** The resultant table lists all the proxies configured. Click the proxy name to access its Home page.
3. On the Proxy Home page, click Help for more information.

Removing Proxies Configured for OMS-to-Management Agent Communication

To remove a proxy that is configured for OMS and Management Agent communication, follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **Agents.**
2. On the Proxy page, in the **Proxy Name** column, select the proxy you want to remove, and click **Remove.**

EM CLI Verbs for Configuring Proxies for OMS and Management Agent Communication

Table 16-1 lists the EM CLI verbs for configuring proxies for OMS and Management Agent communication. For more information about these verbs, see the *Oracle Enterprise Manager Command Line Interface Guide*.

Table 16-1 EM CLI Verbs for Configuring Proxies for OMS and Management Agent Communication

EM CLI Verb	Description
`add_proxy`	Adds a proxy that mediates the HTTP or HTTPS traffic from the OMS to the Management Agent. This proxy is modeled as `oracle_em_proxy` target type in Enterprise Manager.
`delete_proxy`	Deletes an HTTP or HTTPS proxy that is configured for the OMS and Management Agent communication.
`list_proxies`	Lists all HTTP and HTTPS proxies that are configured for the OMS and Management Agent communication. By default, the output is in tabular format, listing the proxy name, the protocol, the host name (with its port), and the status.
`modify_proxy`	Modifies an HTTP or HTTPS proxy that is configured for the OMS and Management Agent communication.
`show_proxy`	Shows the details of an HTTP or HTTPS proxy that is configured for the OMS and Management Agent communication.
`test_proxy`	Tests whether or not an HTTP or HTTPS proxy, which is configured for the OMS and Management Agent communication, is reachable.

17

Installing JVMD Agents with Advanced Install Options

This chapter describes how you can install JVM Diagnostics (JVMD) Agents manually in the Enterprise Manager environment.

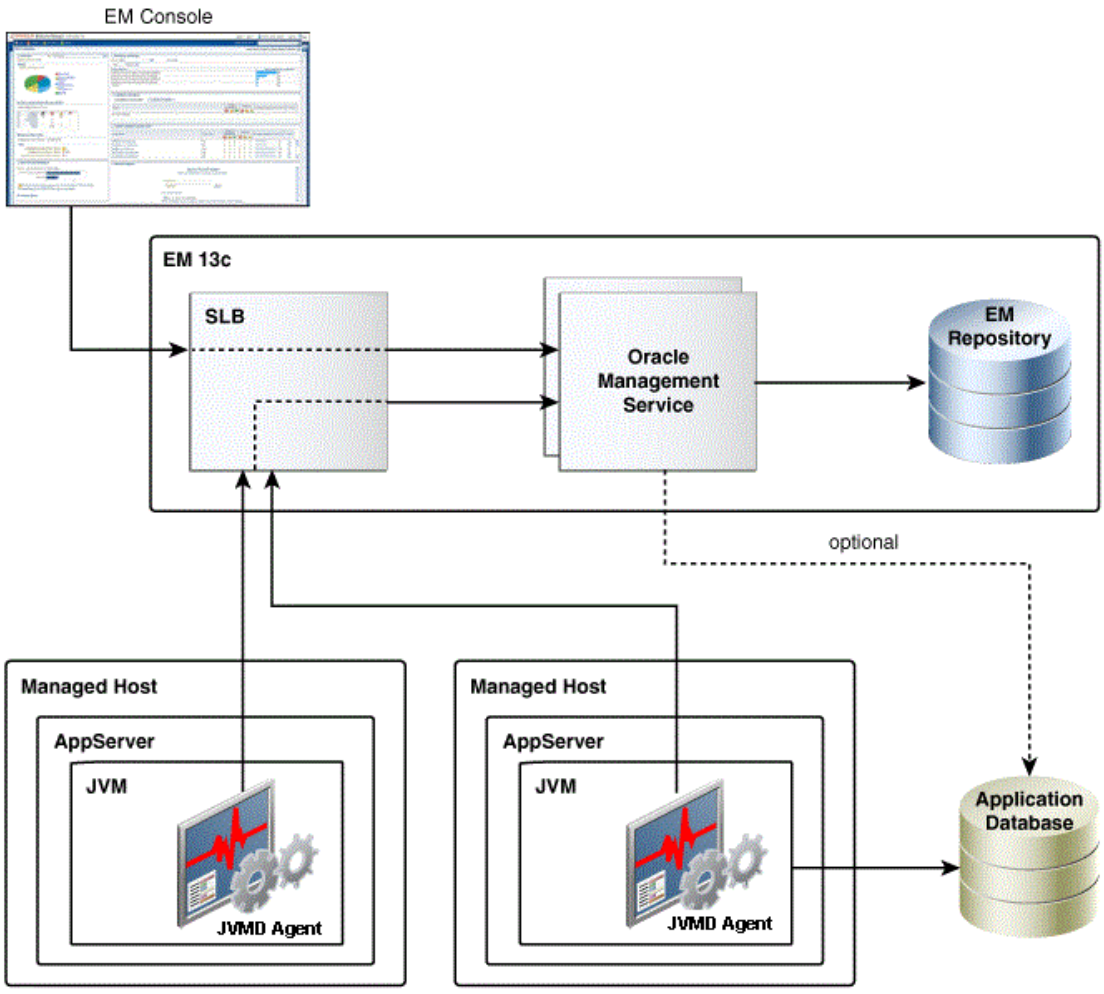
In particular, this chapter covers the following:

Overview of JVMD Architecture

JVM Diagnostics is integrated with Oracle Enterprise Manager . 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 17-1 JVMD Architecture



JVMD Engine is the core analytical engine of the JVMD monitoring system. Starting with Enterprise Manager 13c, JVMD Engine is deployed as an Enterprise Application Deployment (ear file) on the EMGC domain out-of-the-box. JVMD Engine runs as an Enterprise JavaBeans (EJB) technology in the OMS server. 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 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 Console for monitoring purposes. The communication between JVMD Engine and JVMD Agent can be secure (SSL), or non-secure.

JVMD communication between clients (also known as agents) and server (also known as manager servers or engines) is HTTPS based. The JVMD manager server hosts and ports can be found on the Engines and Agents page, under the Middleware Management option of the Enterprise Manager Setup menu. Please refer the SLB user guide to set up a pool for the

corresponding JVMD manager hosts and ports. The JVMD agent deployment and download should specify the SLB host and port to achieve HA.

Most SLBs ensure source address (that is, client host) based affinity. JVMD communication inserts header field `FROM-AGENT-ID`, which can be used for this purpose. Please refer the SLB user guide for configuration instructions.

Starting with Enterprise Manager 13c Release 2, if the load balancer is configured to terminate at the OMS managed servers and you have defined the custom certificates, then ensure the following:

- Custom certificates file(s) are placed in `<EMAS plugin home>/archives/jvmd/certificates` directory
- Custom certificates file(s) have a `.crt` extension
- Custom certificates file(s) do not have a `WLSDemo_` prefix
- Custom certificates file(s) are provided in above location on each OMS

> **Note:**
>
> A `README.txt` file is available at `<EMAS plugin home>/archives/jvmd/certificates` directory.

Before you Begin Installing JVMD Agent

Before installing a JVMD Agent, review the points outlined in *Oracle Enterprise Manager Basic Installation Guide*.

Prerequisites for Installing JVMD Agent

Before installing a JVMD Agent, ensure that you meet the prerequisites described in *Oracle Enterprise Manager Basic Installation Guide.*

Deploying JVMD Agents Using Advanced Installation Options

This section describes how to deploy JVMD Agents manually.

> **Note:**
>
> If you have removed an agent and you want to deploy it again, you must restart JVM before deploying it.

This section consists of the following:

Deploying JVMD Agents Manually by Downloading and Deploying jamagent.war

To deploy JVMD Agents manually, follow these steps:

> **Note:**
>
> - The preferred method of manual deployment of JVMD Agents is using step 1. Download jamagent.war.
> - Step 2. Deploy JVMD Agent manually section is applicable only if the Download jamagent.war fails.

1. **Download jamagent.war.**

   To download `jamagent.war` using Enterprise Manager, follow these steps:

   a. In Enterprise Manager, from the **Setup** menu, select **Middleware Management,** then select **Engines And Agents**.

   b. On the Engines And Agents page, click **Download JVMD Agent**. The Download JVM Diagnostics Components dialog box is displayed.

   c. From the **JVMD Component** menu, select **JVMD Agent** to download `jamagent.war` and then click **OK.** The JVM Diagnostics Agent web.xml Parameters dialog box is displayed.

   d. From the **Available Engines** menu, select an option from the list:

      Select the HTTP URL if you want the JVMD Agent to connect to the JVMD Engine using a non-secure connection.

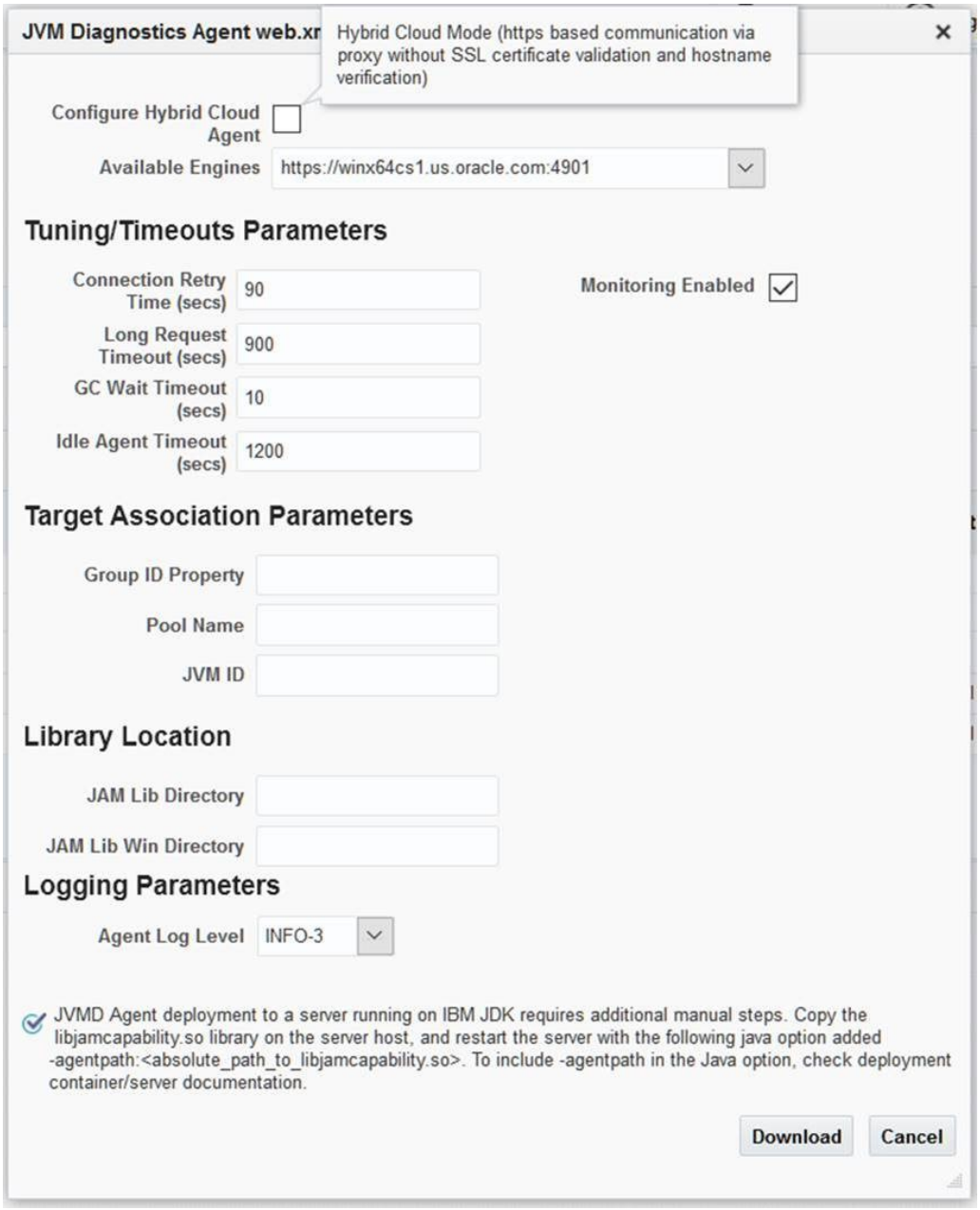
      Select the HTTPS URL if you want the JVMD Agent to connect to the JVMD Engine using a secure connection.

      Select **Custom** if you want the JVMD Agent to connect to a JVMD Engine through a Load Balancer or a firewall. Specify the host name and the port that the JVMD Agent must connect to.

      For example:

      HTTP: `http://sl1.us.example.com:3800`

      HTTPS: `https://sl1.us.example.com:3801 (secure communication)`



e. Select **Enable Monitoring** to deploy an agent in monitoring disabled mode, uncheck the checkbox. You can enable or disable the monitoring using **Configure JVM Target** button on **JVM Target** home page.

   Library Location: Default location where jvmd agent library would be copied during deployment.

f. Click **Download** to download `jamagent.war`.

2. **Deploy JVMD Agent manually.**

   Deploying JVMD Agent on WebLogic Server: using the WebLogic Server Administration Console

   To deploy JVMD Agent on a WebLogic Managed Server manually, follow these steps:

   a. Login to the WebLogic Server Administration console.

   b. In the Change Center, click **Lock & Edit** if that button is enabled.

c. Under Domain Structure, select **Deployments.**

d. On the Deployments page, click **Install.**

e. Click **Install.**

f. Delete old javadiagnosticagent.ear or jamagent.war if there are any.

g. Follow wizard instruction to install the agent as an application , target it to all or some of the servers in the domain, leave all other options in their default setting.

h. Start jamagent app if not started already.

   Server restart is not required (unless it is an agent upgrade).

i. Go to EM CC and verify if ServerName_jvm target is created.

Deploying JVMD Agent on WebLogic Server

To deploy JVMD Agent on a WebLogic Managed Server manually, follow these steps:

a. 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.

b. 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:

a. Log in to the Glassfish Administration console.

b. In the Common Tasks section, click **Applications.**

c. In the Deployed Applications section, click **Deploy.**

d. For **Location,** select **Packaged File to Be Uploaded to the Server,** then specify the location on your local host where `jamagent.war` is present.

e. For **Selected Targets,** add the server on which you want to deploy `jamagent.war`.

f. Click **OK.**

Deploying JVMD Agent on JBoss

To deploy JVMD Agent on JBoss manually, follow these steps:

a. Log in to the JBoss Administration console.

b. Under **Applications,** click **Web Application (WAR)s.**

c. Click **Add a new resource.**

d. Enter the absolute path to `jamagent.war` present on your local host.

e. For both **Deploy Exploded** and **Deploy Farmed,** select **No.**

f. Click **Continue.**

To deploy JVMD Agent on JBoss manually, you can also do the following:

a. Transfer `jamagent.war` to the following location:

```
<JBOSS_HOME>/server/all/deploy
```

b. Restart the application server.

Deploying JVMD Agent on Tomcat

To deploy JVMD Agent on Tomcat manually, follow these steps:

a. Transfer `jamagent.war` to the following location:

```
$CATALINA_BASE/webapps
```

b. 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:

a. Log in to the Websphere Administration console.

b. Expand **Applications,** then click **New Application.**

c. Click **New Enterprise Application.**

d. For **Path to the new application,** select **Local file system,** then specify the location on your local host where `jamagent.war` is present.

e. Provide the context root for `jamagent.war`.

f. Save the configuration.

g. Start the application**.**

Deploying JVMD Agent on OC4J

To deploy JVMD Agent on OC4J manually, follow these steps:

a. Log in to the OC4J Administration console.

b. Click **Applications.**

c. Click **Deploy.**

d. Select **Archive is present on local host.** For **Archive Location,** specify the location on your local host where `jamagent.war` is present. Click **Next.**

e. For **Application Name,** enter `jamagent`. For **Context Root,** enter `/jamagent`.

f. 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
```

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 `jamagent.war` has been downloaded.

   For information on how to download `jamagent.war`, see Step 1 in Deploying JVMD Agents Manually by Downloading and Deploying jamagent.war.

2. Navigate to the following location on the OMS host:

   ```
   $<MIDDLEWARE_HOME>/plugins/oracle.sysman.emas.oms.plugin_24.1.0.0.0/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

defines 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 defines 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`.

Deploying JVMD Agents for High Availability

If you have multiple JVMD Engines 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. For more information on configuring multiple OMS High Availability behind a SLB, refer to `Oracle Maximum Availability Architecture Best Practices for Enterprise Manager`.

You can deploy JVMD Agents for high availability using the Engines And Agents page, or manually.

Deploying JVMD Agents for High Availability Using the Engines And Agents Page

To deploy JVMD Agents for high availability using the Engines And Agents page, follow these steps:

1. Follow the steps mentioned in *Oracle Enterprise Manager Basic Installation Guide* to deploy a JVMD Agent.

   > **Note:**
   >
   > By default, the JVMD Agent connects to the load balancer using HTTPS.

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.**

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 Deploying JVMD Agents Manually by Downloading and Deploying jamagent.war to download `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 Deploying JVMD Agents Manually by Downloading and Deploying jamagent.war.

After Installing JVMD Agents

After installing a JVMD Agent, follow the steps outlined in *Oracle Enterprise Manager Basic Installation Guide*.

18

Configuring Enterprise Manager Federation

Enterprise Manager Federation allows customers to have a consolidated view of all Enterprise Manager sites providing a summary of all Enterprise Manager sites deployed across the enterprise.

This chapter contains the following sections:

For troubleshooting, see Enterprise Manager Federation Troubleshooting.

Overview

Enterprise Manager Federation allows customers to have a consolidated view of all Enterprise Manager sites providing a summary of all Enterprise Manager sites deployed across the enterprise.

The Enterprise Manager Federation user interface offers federated summary and also, links to specific Enterprise Manager sites summary pages for in depth analysis. The Federation Overview page offers federated summary for the following areas: Targets summary, Incidents summary, Problems summary and Jobs summary.

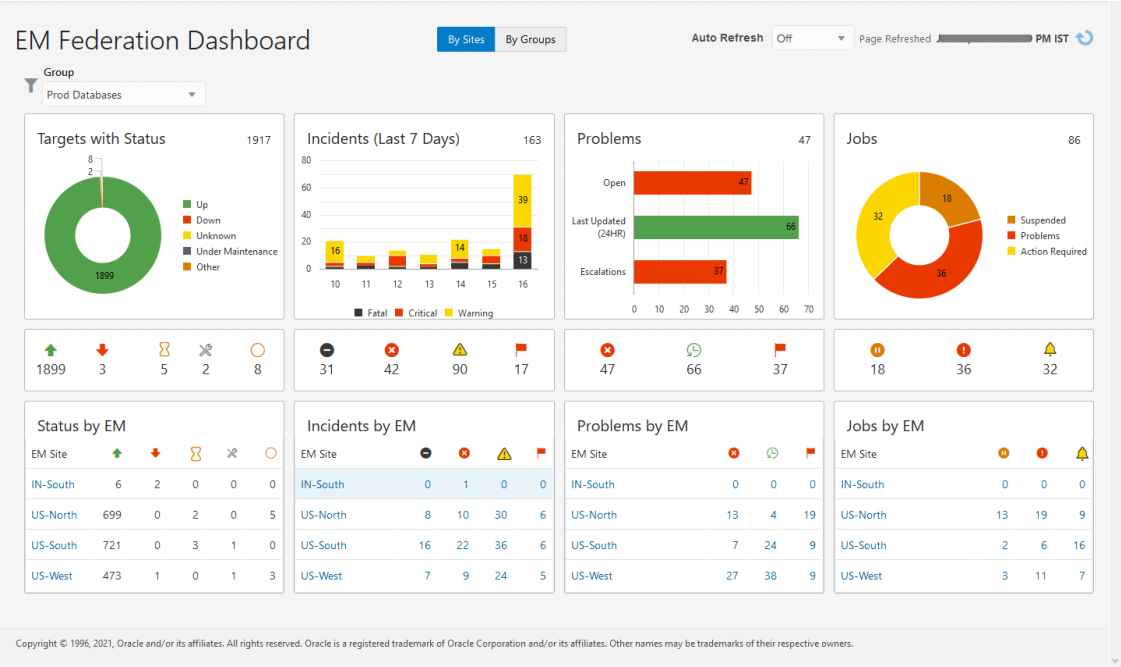
The Enterprise Manager Federation supports the use of `cURL` commands and `REST API`.

Enterprise Manager Federation Dashboard

The federated Enterprise Manager sites data is accessible from a single interface. The Enterprise Manager Federation Dashboard summarizes:

- Targets
- Incidents
- Problems
- Jobs

You can also drill down from any of the summary options described above. For example, you can drill down into an individual Enterprise Manager's *All Targets* page, *Job* activity page or *Incident* overview page for details.



Enterprise Manager Federation Set Up and Configuration

The following steps are required to be executed only once by any EM Super Administrator user to set up the Enterprise Manager Federation:

- Step 1: Specify name of AuthN Provider for Enterprise Manager Federation
- Step 2: Create AuthN Provider on Primary Enterprise Manager site
- Step 3: Add list of Enterprise Manager sites to be federated
- Step 4: Import Certificates into Primary Enterprise Manager site's trust store

Step 1: Specify name of AuthN Provider for Enterprise Manager Federation

The Enterprise Manager administrator needs to select a Primary Enterprise Manager site from the entire enterprise.

To set up the Primary Enterprise Manager site, you need to enable the Enterprise Manager Federation and implicitly make the site the Primary Enterprise Manager site for Federation by running the following:

```
emctl set property \
   -name oracle.sysman.federation.masterEMAuthNProducerName \
   -value EMFederation
Oracle Enterprise Manager ...
Copyright (c) ...
Enter Enterprise Manager Root (SYSMAN) Password : *****
Property oracle.sysman.federation.masterEMAuthNProducerName has
been set to value EMFederation for all Management Servers
OMS restart is not required to reflect the new property value
```

The above command specifies the required name of the AuthN provider, **EMFederation**, which will be used in step 2.

Step 2: Create AuthN Provider on Primary Enterprise Manager site

To create an AuthN Provider on the Primary Enterprise Manager site, run the following:

```
emctl config apiauth \
  -create_provider \
  -name EMFederation \
  -useDefaults \
  -out EMFederation.json
Oracle Enterprise Manager ...
Copyright (c) ...
Enter Enterprise Manager Root (SYSMAN) Password : *****
Creating Provider named 'EMFederation' with Defaults ...
Successfully created a token provider named 'EMFederation'
The Contents of the provider are:
{"kty" : "oct" ,"kid" : "....-....", "k" : "W20_....."}
The provider details are in the file named 'EMFederation.json'
Commiting the changes ...
Done commiting the changes.
Provider created successfully.
Exit Code: SUCCESS
```

The above command generates a small JSON file named: `EMFederation.json`.

After the JSON file is generated, you need to establish trust between the primary Enterprise Manager site and the Enterprise Manager sites to be federated.

Do the following on each secondary Enterprise Manager site to be federated to establish the trust relationship between the primary Enterprise Manager site and the respective secondary site:

- Copy the generated JSON file from the primary site to each secondary site.
  This operation is designed to be performed out-of-band from Enterprise Manager.

  Typically, the file is copied using a secure copy command like the following:

  ```
  scp <generated_json_file> <em_secondary_site>
  ```

  Example:

  ```
  scp EMFederation.json em_site1.example.com:.
  ```

- Login to each secondary site and create an AuthN Asserter using the JSON file transferred to the respective secondary EM site by running the following:

  ```
  emctl config apiauth \
    -create_asserter  \
    -name EMFederation  \
    -in EMFederation.json
  Oracle Enterprise Manager...
  Copyright (c) ...
  Enter Enterprise Manager Root (SYSMAN) Password :  *****
  Registering Asserter Named 'EMFederation' using file
  'EMFederation.json' ...
  Commiting the changes ...
  ```

```
Done commiting the changes.
Asserter named 'EMFederation' created successfully.
Exit Code: SUCCESS
```

The above two commands are repeated each time an additional secondary site becomes part of the primary Enterprise Manager federated dashboard.

Step 3: Add list of Enterprise Manager sites to be federated

The Enterprise Manager administrator needs to add a list of the Enterprise Manager sites that will be part of the federation and their respective URLs to the Primary Enterprise Manager site using `cURL` command line tool. Any Enterprise Manager 13c Release 4 Update 4 (13.4.0.4) or higher can be a federated site.

To add a list of Enterprise Manager sites, you can use `cURL` command line tool and run the following:

```
curl -X POST <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites -u '<EM_user_from_Primary_EM_host>' -H 'content-type:
application/json' -d '{"siteURL":
"<EM_site1_URL>:EM_site1_port>", "name": "host"}'
```

Example using cURL

```
curl -X POST https://primary_em.sample.com:5416/em/websvcs/restful/fed/
emSites -u 'user1' -H 'content-type: application/json' -d '{"siteURL":
"https://em_site1.sample.com:5416", "name": "host"}'
```

Response

The response from this command returns the following:

- Successful operation: It returns the newly generated `EM Site GUID` for a successful response. This value will be used in the following step. For example, it will return "422cf85c13354336874a1971c1d57a70" as the `EM Site GUID` for em_site1.sample.com site.
- Invalid input: It returns an error code and a message for a failed response.

The `cURL` command supports one Enterprise Manager site at a time. Repeat this step to add more Enterprise Manager sites as federated sites. The maximum number of federated Enterprise Manager sites supported is 10.

Step 4: Import Certificates into Primary Enterprise Manager site's trust store

To allow `https` connectivity to other Enterprise Manager sites, the Enterprise Manager administrator imports the federated Enterprise Manager sites certificates into the Primary Enterprise Manager site's trust store.

The administrator needs to ensure the certificates provided are `PEM` encoded (`DER` encoded certificates are not supported).

The customer will provide other Enterprise Manager's certificate by using `cURL` command line tool

```
curl -X POST <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites/<EM Site GUID>/certificates -u
```

```
'<EM_user_from_Primary_EM_host>' -H 'content-type: multipart/form-data' -F
file=@<certificate file>
```

Example using cURL

```
curl -X POST https://primary_em.sample.com:5416/em/websvcs/restful/fed/
emSites/422cf85c13354336874a1971c1d57a70/certificates -u 'user1' -H 'content-
type: multipart/form-data' -F file=@em_site1.pem
```

Response

The response from this command returns the following:

- Successful operation: It returns the `Certificate GUID` and the `PEM` content of the file uploaded for a successful response.
- Invalid input: It returns an error code and a message for a failed response.

The certificate is stored in Enterprise Manager credential framework.

For information about how to secure Enterprise Manager, including configuring custom certificates, see Custom Configurations in the *Enterprise Manager Security Guide*.

Enterprise Manager Federation Post Configuration Tasks

The following post configuration tasks are required to be performed by any individual user who wants to have access to the Enterprise Manager Federation Dashboard which resides in the Primary Enterprise Manager site. Users will need to create credentials and link it to the federated Enterprise Manager site. The credentials are private to that user and not shared.

1. **(Optional) Configure groups to view federated Enterprise Manager sites by groups**

   Starting with Enterprise Manager 13 Release 5 Update 1 (13.5.0.0.1), group based filtering is supported by configuring groups to view information specific to selected group(s) across federated Enterprise Manager sites.

   Groups are used to logically organize, manage and monitor the targets in individual Enterprise Manager sites or federated Enterprise Manger sites. Creating a federation group in the primary Enterprise Manager enables the federation dashboard to get data specific to the configured groups from the federated Enterprise Manager sites. For example, the super administrator can create groups for specific applications or business units: One group for Customer Service applications and other group for Finance applications. The groups created by the super administrator user are available to all users.

   Requirement:

   - The Primary Enterprise Manager site must have installed Enterprise Manager 13c Release 5 Update 1 (13.5.0.0.1) or higher.
   - The federated Enterprise Manager sites must have installed Enterprise Manager 13c Release 4 Update 9 (13.4.0.0.9) or higher.

   To add a group, you can use the following `cURL` command:

   ```
   curl -X POST https://<Primary_EM_host_name>.<Primary_EM_host_domain>/em/
   websvcs/restful/fed/composites -u '<EM_user_from_Primary_EM_host>' -H
   'content-type: application/json' -d '{ "targetName":"<Group_Name>",
   "targetType":"composite"}'
   ```

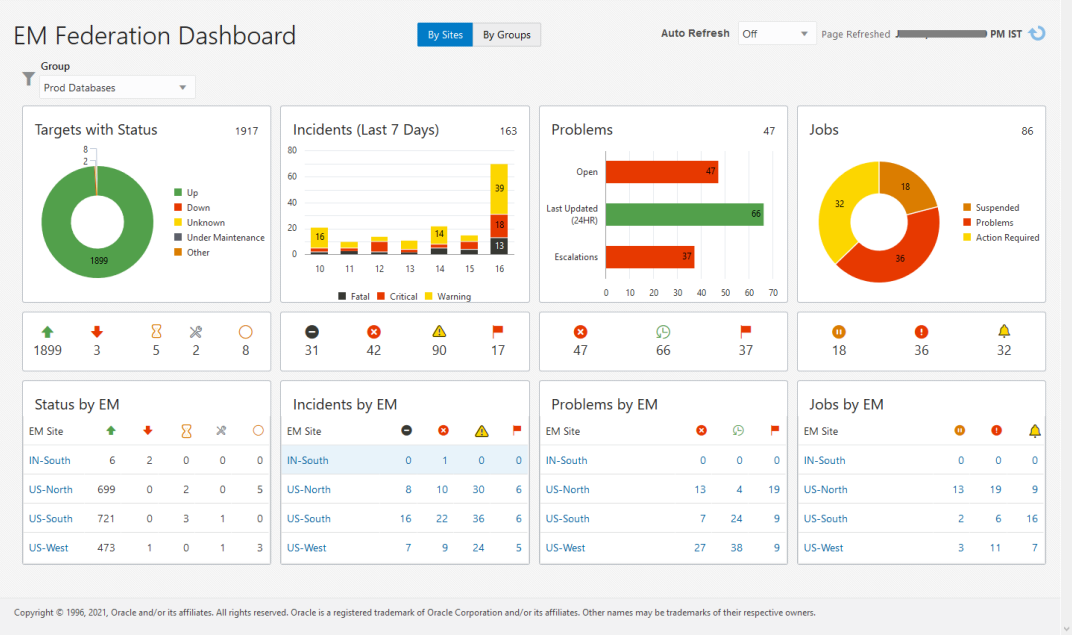
For example, to add a group called "Finance DB", use the following command:

```
curl -X POST https://primary_em.sample.com/em/websvcs/restful/fed/
composites -u 'superadmin' -H 'content-type: application/json' -d
'{ "targetName":"Finance DB", "targetType":"composite"}'
```

After the groups are configured, Enterprise Manager Federation will have two dashboard types available:

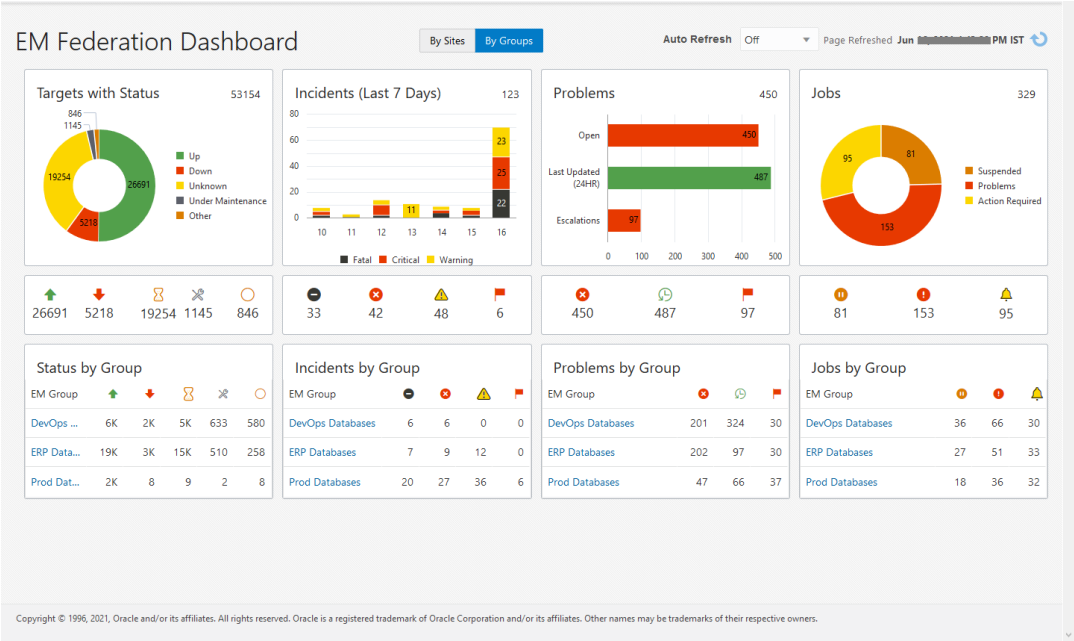
- **By Sites**

  It allows filtering down data to specific federated group across all federated Enterprise Manager.



- **By Groups**

  It consolidates data for all federated groups across all federated Enterprise Manager sites. This dashboard is useful for users interested to see data only related to the federated groups, and not the whole enterprise.



Enterprise Manager Federation Troubleshooting

This section covers common troubleshooting tasks for Enterprise Manager Federation using `cURL` command line tool for the following EM Federation resources:

- EM Site Management
- EM Certificate Management
- EM Credentials Management
- EM Credentials Mapping

EM Site Management

- **Get EM site**

```
curl -X GET <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites -u '<EM_user_from_Primary_EM_host>'
```

For example:

```
curl -X GET https://primary_em.sample.com:5416/em/websvcs/restful/fed/
emSites -u 'user1'
```

Display existing trust relationship

For an existing secondary Enterprise Manager site, display the existing trust relationship established from the primary Enterprise Manager site.

```
emctl config apiauth -list_asserters -name EMFederation
Oracle Enterprise Manager 24ai Release 1
Copyright (c) 1996, 2024 ...
Enter Enterprise Manager Root (SYSMAN) Password :
Listing asserter with name = EMFederation
```

```
TokenAsserter [id=xxx, name= EMFederation, tokenType=JWS]
Done listing Asserter(s).
Exit Code: SUCCESS
```

- **Update EM site**

```
curl -X PUT <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites/<EM-SITE_GUID> -u '<EM_user_from_Primary_EM_host>' -H
'content-type: application/json' -d ' {"siteURL":
"<EM_site1_URL>:EM_site1_port>", "name": "ProdHost"} '
```

For example:

```
curl -X PUT https://primary_em.sample.com/em/websvcs/restful/fed/emSites/
422cf85c13354336874a1971c1d57a70 -u 'user1' -H 'content-type: application/
json' -d ' {"siteURL": "https://em_site1.sample.com:5416", "name":
"ProdHost"} '
```

- **Delete a secondary EM site**

```
emctl config apiauth -delete_asserter -name EMFederation
```

```
curl -X DELETE <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites/<EM-SITE_GUID> -u '<EM_user_from_Primary_EM_host>'
```

For example:

```
curl -X DELETE https://primary_em.sample.com/em/websvcs/restful/fed/
emSites/422cf85c13354336874a1971c1d57a70 -u 'user'
```

> **Note:**
>
> The `<EM-SITE_GUID>` value is returned when creating an EM Site. You can also obtain it using the `GET` API.

EM Certificate Management

- **Get certificate**

```
curl -X GET <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites/<EM-SITE_GUID>/certificates -u
'<EM_user_from_Primary_EM_host>'
```

For example:

```
curl -X GET https://primary_em.sample.com/em/websvcs/restful/fed/emSites/
422cf85c13354336874a1971c1d57a70/certificates -u 'user1'
```

- **Delete certificate**

```
curl -X DELETE <Primary_EM_host_URL>:<Primary_EM_host_port>/em/websvcs/
restful/fed/emSites/<EM-SITE_GUID>/certificates -u
'<EM_user_from_Primary_EM_host>'
```

For example:

```
curl -X DELETE https://primary_em.sample.com/em/websvcs/restful/fed/
emSites/422cf85c13354336874a1971c1d57a70/certificates -u 'user1'
```

> **Note:**
>
> The `<EM-SITE_GUID>` value is returned when creating an EM Site. You can also obtain it using the `GET` API.

19

Using Oracle Analytics Server with Enterprise Manager

Starting with Enterprise Manager Cloud Control 13c Release 5 (13.5.0.0.0), Oracle Analytics Publisher (formerly BI Publisher) must be accessed from a standalone Oracle Analytics Server. If you want to use reporting functionality, you will need to install or access a standalone instance of Oracle Analytics Server (OAS), previously called Enterprise Edition (OBIEE). Similarly, BI Publisher, which is part of OBIEE, has been renamed Oracle Analytics Publisher (OAP). See *Standalone Oracle Analytics Service* for more information.

20

Configuring Oracle Enterprise Manager App for Grafana

The Oracle Enterprise Manager App for Grafana allows you to integrate and display EM Metrics data in Grafana. EM collects extensive metric data from various managed targets, and this app allows you to leverage this data for your use cases. You can create custom EM-based Grafana dashboards by browsing and selecting the EM metrics of interest, or for advanced use cases running SQL queries against the EM Repository's SDK views or Target Databases. The App is an extension to EM's data visualization capabilities for added dashboard customization supported by Grafana.

Starting with Enterprise Manager 13c Release 4 Update 3 (13.4.0.3) or higher, the Oracle Enterprise Manager App for Grafana is available for download. For more information about installing, enabling and using this app, see Oracle Enterprise Manager App for Grafana User's Guide.

21

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. This chapter describes how you can run the OMS in console-only mode. In particular, this chapter covers the following:

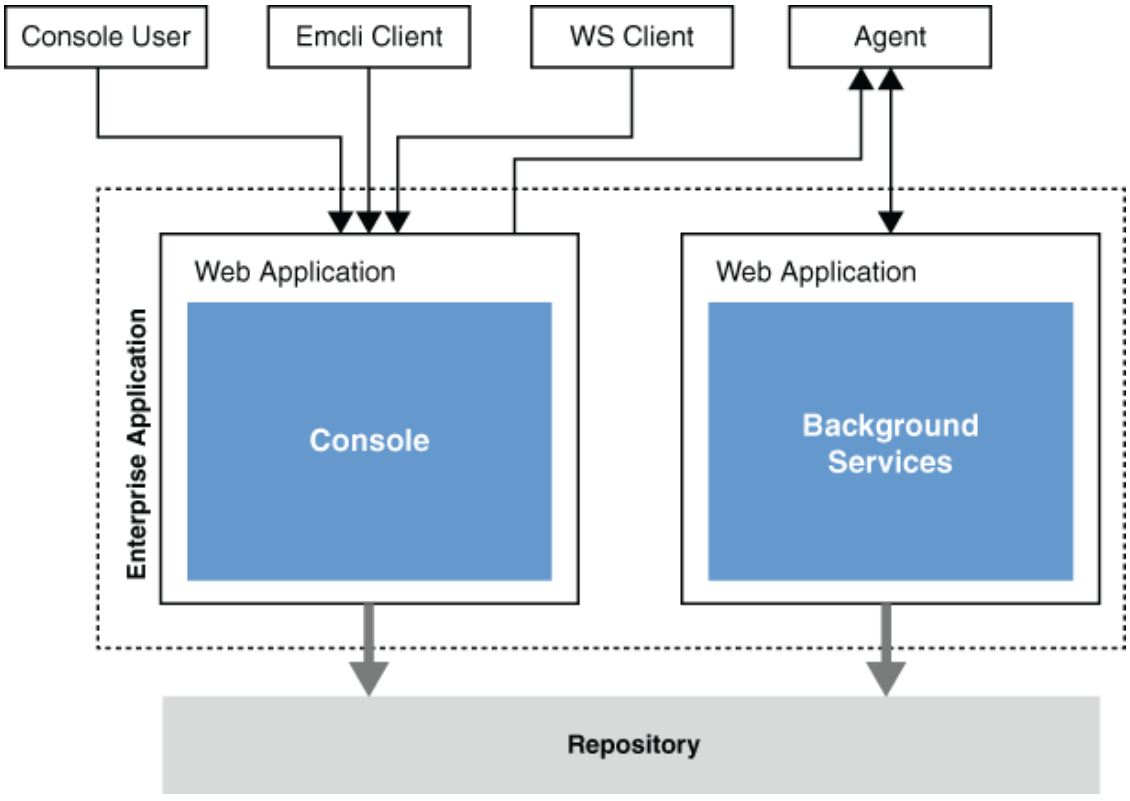
- About Running the OMS in Console-Only Mode
- Running the OMS in Console-Only Mode

About 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 21-1 illustrates the functioning of an OMS where both console services and background services are running.

Figure 21-1 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.

Running the OMS in Console-Only Mode

To run the OMS in console-only mode, follow these steps:

1. Stop the OMS using the following command.

   ```
   $<ORACLE_HOME>/bin/emctl stop oms
   ```

2. Set the start up mode to console-only, using the following command.

   ```
   $<ORACLE_HOME>/bin/emctl config oms -set_startup_mode console_only
   ```

3. Start the OMS using the following command.

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

To revert the OMS instances to Normal mode, run the following command, and restart the OMS.

```
$<ORACLE_HOME>/bin/emctl config oms -set_startup_mode normal
```

22

Support for Customization of Enterprise Manager Login Page

Enterprise Manager allows customization of the login page in order to accommodate corporate policies and standards.

This chapter covers the following topics:

Logo on Enterprise Manager Login Page

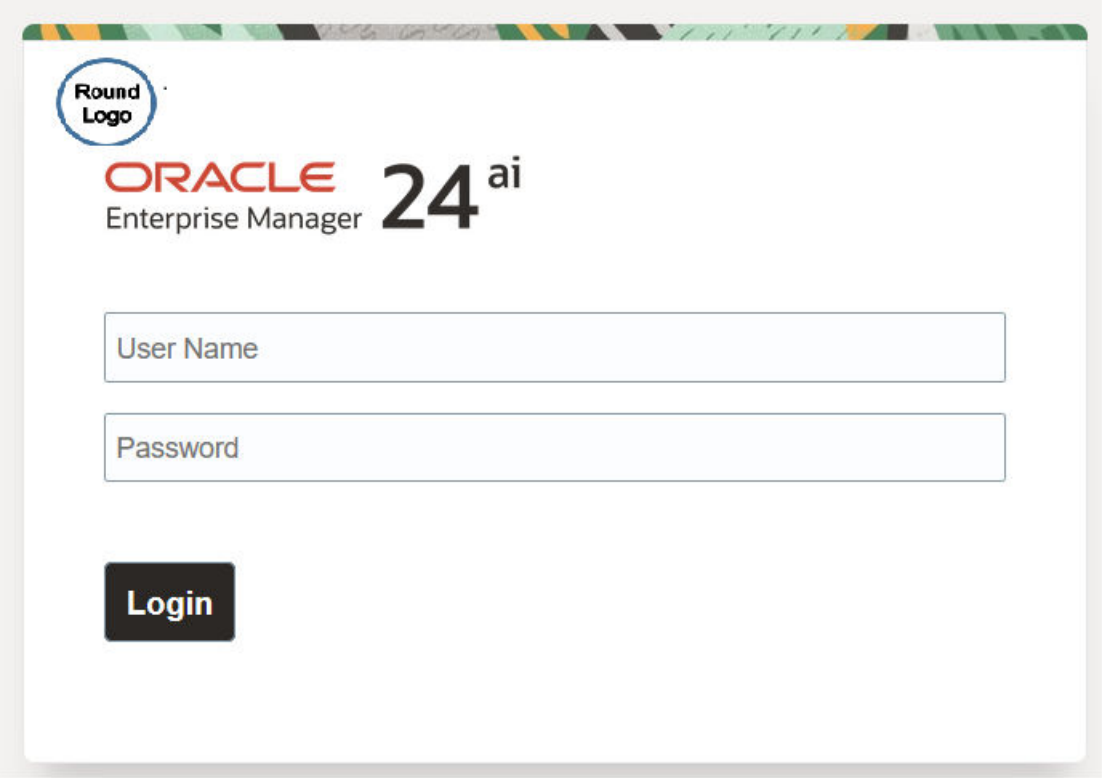
Starting with Enterprise Manager 13*c* Release 3, a logo can be placed on the upper left corner of the Enterprise Manager login page. The supported image formats are jpeg, jpg, png, and gif. The logo ratio of the image file is adjusted according to the allocated space.

The current size of the space provided is “width:200px;height:70px”.

It is recommended to modify the logo image to ensure it fits properly in the space provided.

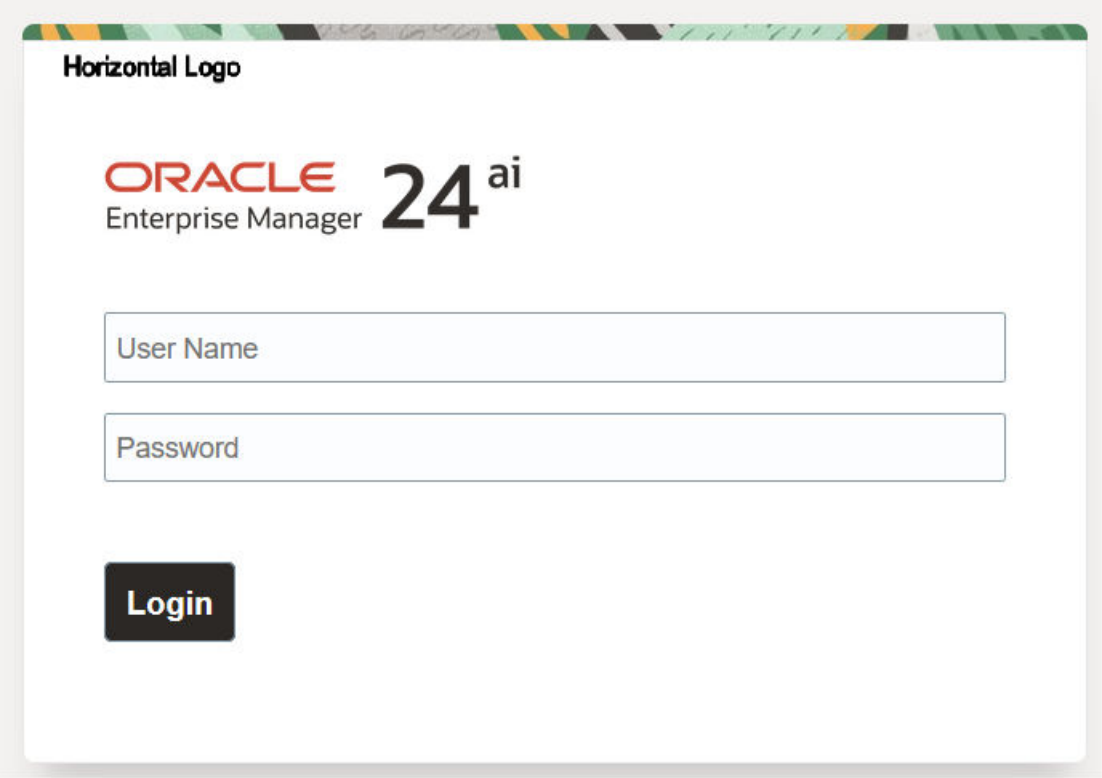
Round Logo:

Figure 22-1 Modify the round logo image to accomodate the allocate space



Horizontal Logo:

Figure 22-2 Modify the horizontal logo image to accommodate the allocated space



The image file can be hosted on any web server including Weblogic server. For an example on how to set it up on Weblogic server, see Setup Weblogic Server to Host Images.

Setup Weblogic Server to Host Images

In order to load a custom logo image file on the Enterprise Manager login page, a web application containing the static image file needs to be deployed to the Weblogic domain on the Admin Server. For instructions on how to install a Web application, see https://docs.oracle.com/middleware/1213/wls/WLACH/taskhelp/web_applications/InstallWebApplications.html

To deploy the custom logo image file, perform the following steps:

1. On the OMS host, create a directory to store the logo image file to be used on the EM login page. For example, `/u01/oracle/gc_inst/em/EMGC_OMS1/temp`
2. Copy the logo image file to the newly created directory. For example, `/u01/oracle/gc_inst/em/EMGC_OMS1/temp/custom_logo.png`
3. In the newly created directory, create a WEB-INF directory. For example, `/u01/oracle/gc_inst/em/EMGC_OMS1/temp/WEB-INF`
4. In the WEB-INF directory create a file called web.xml with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE web-app PUBLIC
"-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
"http://java.sun.com/j2ee/dtds/web-app_2_3.dtd">
```

```
<web-app>
</web-app>
```

5. Login to the Weblogic console. Username by default is weblogic and password is the sysman password.

   URL: `https://hostname:port/console`

   Example: `https://<fully_qualified_host_name>:7102/console`

   > **Note:**
   >
   > The Weblogic console URL (Admin Server URL) is not the same URL as the Enterprise Manager console. The host and the port are values specified in the AS_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, `/u01/oracle/gc_inst/em/EMGC_OMS1/emgc.properties`. The Admin Server URL can also be found in the `<EM Home Dir>/install/setupinfo.txt` file.

6. Enable 'http' port for the Admin Server. This can be done from the Admin Server settings.

   a. From the tree view, expand **Environment** and then select **Servers.** Find and click **EMGC_ADMINSERVER (admin)** in the table.

      > **Note:**
      >
      > For multi-OMS deployments, the custom logo image can be hosted on each OMS server. In case an OMS server is not available due to patching or upgrade, the running OMS server can still access the logo image hosted by its own OMS tier. To configure the logo image in this method, deploy the image to each OMS tier, for example, EMGC_OMS1, EMGC_OMS2, EMGC_OMS3 and so on, instead of EMGC_ADMINSERVER.

   b. Settings for EMGC_ADMINSERVER page opens. Go to the **General Tab,** if not opened already. Select the **Listen Port Enabled** check box.

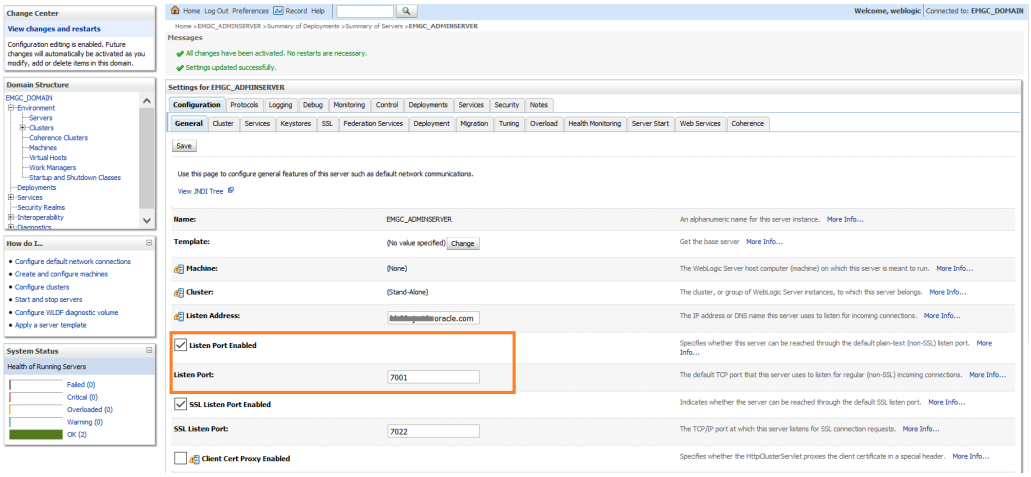
   c. Edit the port number as required. The default port number is **7001**. **The value of Listen Port will be the http port which will be used later to run the emctl command to set the image file.**

   d. Click **Save.** The following message appears at the top of the screen:

      All changes have been activated. No restarts are necessary.

      Settings updated successfully.

Figure 22-3 Setting http listen port on the Weblogic Server Administration Console



7. Click **Deployments** menu at the left. The **Install** button is disabled by default.
8. Click **Lock & Edit** to enable the **Install** button.
9. In the **Deployments** screen, click the **Install** button.
10. Set the path to the directory created from Step 1 (`/u01/oracle/gc_inst/em/EMGC_OMS1/temp`) **.**
11. Click **Next.**
12. In the next screen, accept the default values for the selected options. By default **Install this deployment as an application** option will be selected.
13. Click **Next.**
14. In the next screen, select **EMGC_ADMINSERVER** as the target.
15. Click **Next.**
16. In the next screen, accept the default values.
17. Click **Finish.**

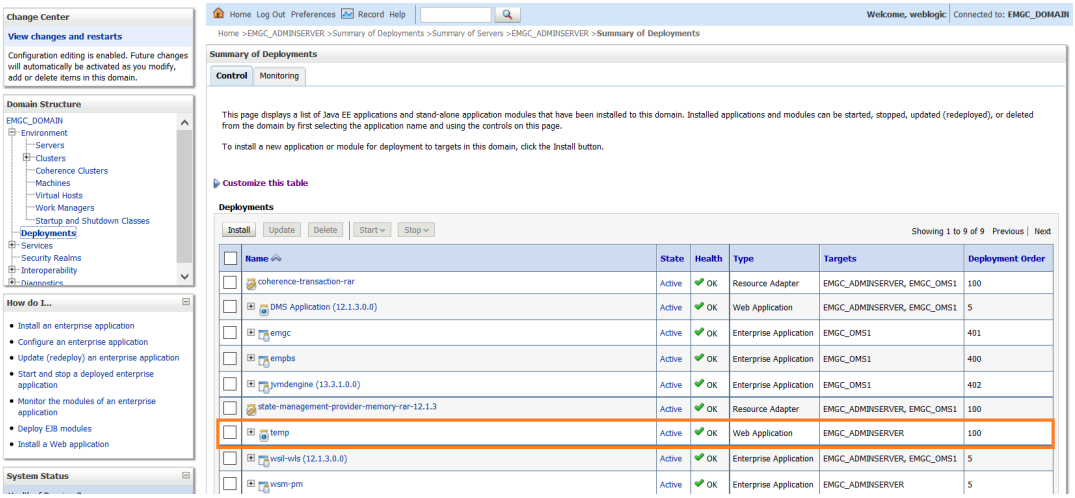
    If the application is successfully deployed, the following message appears:

    All changes have been activated. No restarts are necessary.

    The deployment has been successfully installed.
18. Ensure that the status of the web application 'temp' deployed above is in 'Active' state. If not, click **Activate Changes** on the upper left corner to activate.
19. If the status of ‘temp’ appears as **Prepared** even after Step 18, select ‘temp’ from the table and click **Start.**

> **Note:**
>
> Ensure that the status of ‘temp’ appears ‘Active’ in the **Deployments** table.

Figure 22-4 Deploying a Web Application on the Weblogic Server Administration Console



20. Access the file path to ensure the image appears on the browser screen.

    URL: `http://hostname:port/console/<newly created directory>/<logo image filename>`

    Example: `http://<fully_qualified_host_name>:7001/temp/custom_logo.png`

    Both http and https based image location are supported.

Run EMCTL Command to set the Logo Image

The login page logo can be set by using EMCTL commands. For more information, see Executing EMCTL Commands. OMS restart is not required to reflect the new property value.

The EMCTL command to set the logo image is:

```
emctl set property -name oracle.sysman.core.uifwk.loginPageLogo -value '<HTTP URL to the image file>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.loginPageLogo -value 'http://page.example.com:7001/temp/custom_logo.png' -sysman_pwd password
```

Below is a sample output after running the EMCTL command to set the logo image:

```
bash-4.2$ ./emctl set property -name oracle.sysman.core.uifwk.loginPageLogo -value 'http://page.example.com:7001/temp/custom_logo.png' -sysman_pwd password

Oracle Enterprise Manager  24 Release 1
Copyright (c) 1996, 2024 Oracle Corporation.  All rights reserved.
Property oracle.sysman.core.uifwk.loginPageLogo has been set to value http://page.example.com:7001/temp/custom_logo.png for all Management Servers
OMS restart is not required to reflect the new property value
```

The EMCTL command to unset the logo image is:

```
emctl set property -name oracle.sysman.core.uifwk.loginPageLogo -value null -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.loginPageLogo -value null -sysman_pwd
password
```

Access EM Login Page to see the Logo

From the browser, go to `https://<hostname>:<port>/em/faces/logon/core-uifwk-console-login`

> **Note:**
>
> You must clear the browser cache if you do not see the custom logo on the Enterprise Manager login page.

License Agreement Popup

A License Agreement popup can be configured to appear after the user clicks on the Login button from the Enterprise Manager login page. On pressing **Login,** a License Agreement popup message appears confirming the user whether they 'Agree' or 'Disagree'. On pressing **Agree** the user will be able to successfully login. On pressing **Disagree** or **Close,** the user will stay in the login page. By default, the popup title is **Terms of Service Agreement** and the button labels are **Agree** and **Disagree**. The License Agreement popup title, message, and the button labels are customizable using EMCTL commands. OMS restart is not required to reflect the new property value.

The EMCTL command to set the License Agreement popup title is:

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessagePopupTitle -
value '<popup title>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessagePopupTitle -
value 'ABC Company License Agreement' -sysman_pwd password
```

The EMCTL command to set the License Agreement popup message is:

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessage -value '<popup
message>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessage -value 'Do you
agree to the License Agreement?' -sysman_pwd password
```

The popup message supports HTML tags. For a list of supported HTML tags, see https://docs.oracle.com/html/E12419_09/tagdoc/af_outputFormatted.html

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessage -value '<H2
align=center>ABC Company </H2>
Warning: You are accessing a system operated by ABC Company. Unauthorized access or use
of this system is prohibited and may constitute an offense under the Computer Misuse Act
1990.
</b> <br><br> ABC Company will take appropriate actions if information is disclosed
without prior authorization. This may include legal proceedings, prosecution and
disciplinary action up to and including dismissal.
<br><br> <b>Click &amp;quot;Agree&amp;quot; if you are authorized to access this application and
```

```
agree to the stated Terms of Service Agreement.
</b>' -sysman_pwd password
```

The EMCTL command to unset the License Agreement popup message is:

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessage -value null -
sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessage -value null -
sysman_pwd password
```

The EMCTL command to set the License Agreement popup's agree button label is:

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessageAgreeButton -
value '<Agree button label>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessageAgreeButton -
value 'Yes' -sysman_pwd password
```

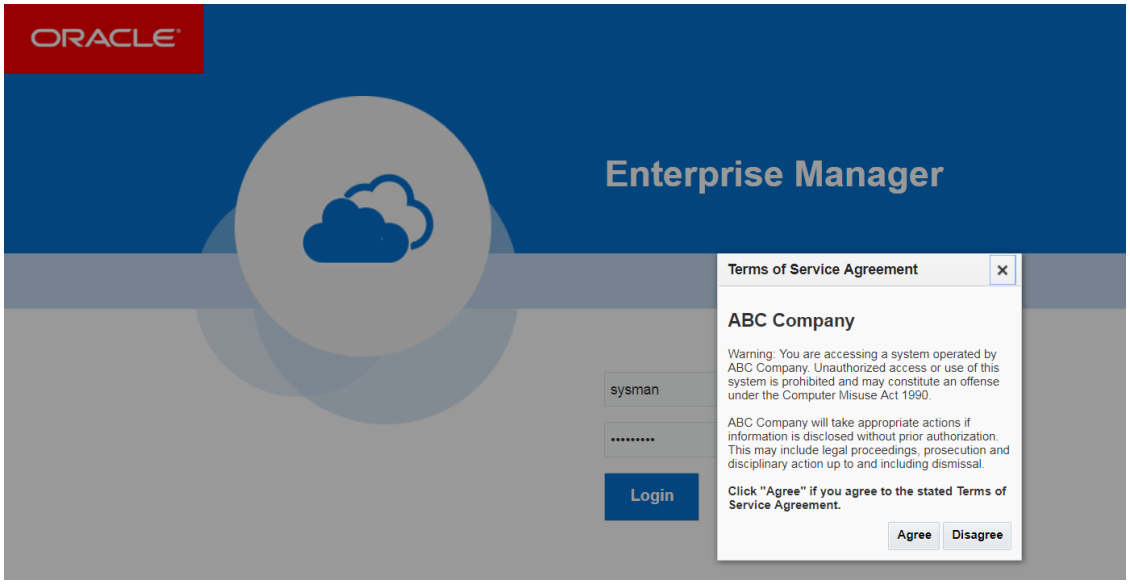
The EMCTL command to set the License Agreement popup's disagree button label is:

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessageDisagreeButton -
value '<Disagree button label>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.licenseAgreementMessageDisagreeButton -
value 'No' -sysman_pwd password
```

Figure 22-5 Enterprise Manager License Agreement Popup



Informational Text on Enterprise Manager Login Page

An informational text can be placed to the left of the Enterprise Manager login fields. The Informational text can be used to provide contextual help with using the site. Some examples

of usage include instructions to apply for access, password reset policy, and instructions for assistance. Similar to the License Agreement popup message, informational text also supports HTML tags. OMS restart is not required to reflect the new property value.

The EMCTL command to set the informational text is:

```
emctl set property -name oracle.sysman.core.uifwk.loginPageInformationText -value
'<informational text>' -sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.loginPageInformationText -value '<b>
Please use your IUSER credentials to log into OEM </b> <br><br> For lost/forgotten
passwords, please use the reset facility: http://page.example.com <br><br> To apply for
access please complete this application form: http://page.example.com <br>' -sysman_pwd
password
```

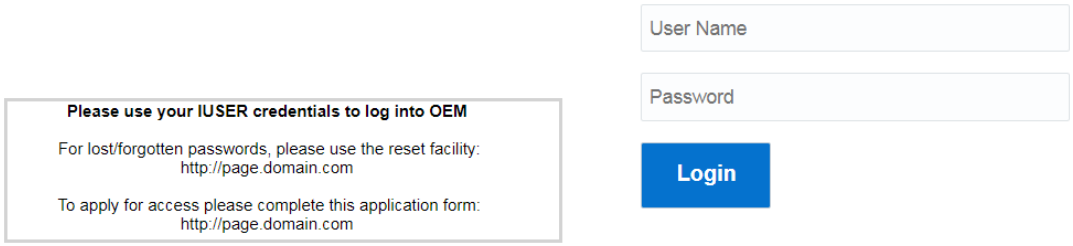
The EMCTL command to unset the informational text is:

```
emctl set property -name oracle.sysman.core.uifwk.loginPageInformationText -value null -
sysman_pwd <sysman password>
```

For example,

```
emctl set property -name oracle.sysman.core.uifwk.loginPageInformationText -value null -
sysman_pwd password
```

Figure 22-6 Enterprise Manager Login Page Informational Text



Part VII

Configuring Enterprise Manager for High Availability and Migrating Oracle Management Service

This section covers Enterprise Manager high availability best practices and strategies that allow you to safeguard your Oracle Enterprise Manager installation.

23

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 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 Enterprise Manager 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.

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 Framework and Infrastructure Web site

  HTTP://www.oracle.com/technetwork/oem/frmwrk-infra-496656.html

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.

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 23-1 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
Level 4	OMS on the primary site in Active/ Active Configuration. Repository deployed using Oracle RAC. Duplicate hardware deployed at the standby site. DR for OMS and Software Library using Storage Replication between primary and standby sites. Database DR using Oracle Data Guard. **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. **Optional**: Global Load Balancer

Comparing Availability Levels

The following tables compare the protection levels and recovery times for the various HA levels.

Table 23-2 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 23-3 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.

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	Where to find information
Level 2	*Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide* PLUS • Configuring the Enterprise Manager OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names • 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* PLUS • Oracle Management Service High Availability • Configuring a Load Balancer • Configuring the Software Library • Installing Additional Management Services • 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* PLUS • Configuring a Standby Database for the Management Repository • Management Service Disaster Recovery

24

Enterprise Manager High Availability

This chapter discusses best practices for installation and configuration of each Enterprise Manager component and covers the following topics:

- Agent High Availability
- Repository High Availability
- Oracle Management Service High Availability

Agent High Availability

The following sections discuss best practices for installation and configuration of the Management Agent.

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.

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.

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 Enterprise Manager Console.

Repository High Availability

The following sections document best practices for repository configuration.

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 Overview of High Availability for more information on these and other best practices to ensure the database that hosts the Management Repository is configured to provide required availability.

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

```
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=primary-cluster-scan.example.com)(PORT=1521))
(CONNECT_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>
```

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 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 Enterprise Manager OMS to be Compatible with Disaster Recovery using Alias Host Names and Storage Replication" 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.

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 Enterprise Manager OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names" 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". Once you've added additional OMS(s), see "Configuring Multiple Management Services Behind a Server Load Balancer (SLB) " for information on how to configure multiple OMSs behind a SLB.

Best Practices for Configuring the Enterprise Manager OMS to be Compatible with Disaster Recovery using Alias Host Names and Storage Replication

This section provides best practices for Enterprise Manager administrators who want to install the Enterprise Manager 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.

Overview and Requirements

The following installation conditions must be met in order for a Enterprise Manager 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.

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.

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." 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 installation wizard command line:

```
ORACLE_HOSTNAME=oms1.example.com
```

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 installation wizard 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.

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)
```

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.

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 for additional important NFS-related requirements. See *Prerequisites for Installing an Enterprise Manager System* in the *Oracle Enterprise Manager Basic Installation Guide.*

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 Oracle Enterprise Manager*" in the Enterprise Manager Basic Installation Guide, specifying the following information as part of the installation process:
   a. Ensure that the Middleware Home, OMS Instance Base, and Agent Base are located under the OMS installation base directory.
   b. 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:

      ```
      $ <Software_Location>/em_<platform>.bin -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 *installation wizard* UI.
6. Continue the remainder of the installation.

Configuring the Enterprise Manager OMS in an Active/Passive Environment for HA Failover Using Virtual Host Names

This section provides a general reference for Enterprise Manager administrators who want to configure Enterprise Manager in Cold Failover Cluster (CFC) environments.

Overview and Requirements

The following conditions must be met for Enterprise Manager 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).

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.

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.

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.

Setting Up the Environment

Some operating system versions require specific operating system patches be applied prior to installing Enterprise Manager 24ai. The user installing and using the Enterprise Manager 24ai 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

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)
```

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
   ```

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:

   ```
   $ <Software_Location>/em_<platform>.bin -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 installation wizard 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, ...)

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 Enterprise Manager using `emctl start oms`
5. Test functionality.

In case of failover, refer to Performing Switchover and Failover Operations.

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 *Adding Additional Oracle Management Services* in the *Oracle Enterprise Manager 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 Advanced Installation and Configuration Guide*.

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.

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 **Provisioning and Patching**, and then select **Software Library**.
2. On the Software Library: Administration page, select **OMS Shared File system**.
3. To add a new OMS Shared File System, click **+Add**.
4. In the **Add OMS Shared File System location** dialog box, provide a unique name for the location and set the location to the shared storage that can be accessed by any Management Service hosts.

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 have configured public-facing ports that provide access to the various services provided by the OMS's that are part of the SLB load balancer configuration.

  Depending on your configuration, you may require up to 4 ports on the SLB (Secure Upload, Agent Registration, Secure Console, Unsecure Console)
- Support for persistence.

  HTTP and HTTPS traffic between the user-interactive browser and the OMS requires persistence settings to ensure that navigation between OMS pages occur to the same pool member throughout the interactive session.

- 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.

- Understand the SSL configuration for your SLB environment.
  The following are the SSL configurations available:

  – **Layer 3 Load Balancing:** The load balancer tunnels incoming SSL connections to your OMS servers on the back end. This SSL configuration is also known as SSL Tunneling.

  – **SSL Proxy:** The load balancer terminates the client SSL connection and acts as a proxy to initiate an SSL connection to the backend OMS servers. This permits the Load Balancer to utilize Layer 7 inspection which enables modifications to the session, such as applying rules, perform virtual server authentication, or cookie/session persistence. This SSL configuration is also known as SSL End-To-End.

  – **SSL Termination:** The client browser session to the Load Balancer is encrypted using SSL, decrypted at the Load Balancer, then the traffic is sent unencrypted to the back end OMS. This SSL configuration is not supported for OMS.

SLB configuration is a two-step process:

1. Configure the SLB.
2. Make requisite changes on the Management Services.

SLB Side Setup

Use the following table as reference for setting up the SLB with Enterprise Manager Management Services.

Various configuration items listed in the below table will be described in subsequent sections of this document.

Table 24-1 Management Service Ports

Enterprise Manager Service	OMS TCP Port	Monitor Name	TCP Profile Name	Persistence Profile	Pool Name	Virtual Server Name	SLB Virtual Server Port
Secure Console	7799	mon_ccsc	tcp_ccsc	sourceip_ccsc	pool_ccsc	vs_ccsc443	443
Unsecure Console	7788	mon_ccuc	tcp_ccuc	sourceip_ccuc	pool_ccuc	vs_ccuc80	80
Secure Upload	4900	mon_ccsu	tcp_ccsu	None	pool_ccsu	vs_ccsu4900	4900
Agent Registration	4889	mon_ccar	tcp_ccar	cookie_ccar	pool_ccar	vs_ccar4889	4889
Always-On Monitoring Secure Upload	8081	mon_ccaom	tcp_ccaom	None	pool_ccaom	vs_ccaom8081	8081
Secure JVMD	7301	mon_ccsjvmd	tcp_ccsjvmd	sourceip_ccsjvmd	pool_ccsjvmd	vs_ccsjvmd7301	7301
Unsecure JVMD	7202	mon_ccujvmd	tcp_ccujvmd	sourceip_ccujvmd	pool_ccujvmd	vs_ccujvmd7202	7202

Cipher profiles are used to define the security, compatibility and speed of the HTTPS traffic. Ciphers are supported by Enterprise Manager and they are used by the SLB administrator to determine which ciphers may be used or which must be excluded to connect to the Enterprise Manager.

> **Note:**
>
> If the Always-On Monitoring service is installed on a host other than the OMS host in the HA configuration, you need to specify the host on which the Always-On Monitoring service is installed instead of the OMS host

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 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 24-2 Monitors

Enterprise Manager Service	OMS TCP Port	Monitor Name	Type	Interval	Timeout	Send String	Receive String
Secure Console (when not using SSL)	7799	mon_ccsc	HTTPS	5	16	`GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	Enterprise Manager Console is UP
Unsecure Console (when not using SSL)	7788	mon_ccuc	HTTP	5	16	`GET /em/consoleStatus.jsp HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	Enterprise Manager Console is UP

Table 24-2 (Cont.) Monitors

Enterprise Manager Service	OMS TCP Port	Monitor Name	Type	Interval	Timeout	Send String	Receive String
Secure Upload	4900	mon_ccsu	HTTPS	60	181	`GET /empbs/upload HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	Http Receiver Servlet active!
Agent Registration	4889	mon_ccar	HTTP	60	181	`GET /empbs/genwallet HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	GenWallet Servlet activated
Always-On Monitoring Secure Upload	8081	mon_ccaom	HTTPS	60	181	`GET /upload HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	Always On Monitoring is active
Secure JVMD	7301	mon_ccsjvmd	HTTPS	60	181	`GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Reply to empty request`
Unsecure JVMD	7202	mon_ccujvmd	HTTPS	60	181	`GET /jamservlet/comm HTTP/1.1\r\nHost: slb.example.com\r\nConnection: Close`	`Reply to empty request`

> **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.

2. Create Pools

   A *pool* is a set of servers configured behind the Load Balancer and grouped together to receive traffic over a specific TCP port for each OMS service.

   Load balancing methods vary depending on the SLB vendor; with several of most common methods being round-robin, least connection, and source-IP hashing. Refer to your specific SLB documentation for available methods and to determine the most suitable for your SLB and operating environment.

   Each pool can have its own unique characteristic for a persistence definition and the load-balancing algorithm used.

Table 24-3 Pools

Enterprise Manager Services	Pool Name	Associated Health Monitor	Load Balancing	OMS Host:OMS Service Port
Secure Console	pool_ccsc	mon_ccsc	Least Connections (member)	OMS Host A:7799 OMS Host B:7799
Unsecure Console	pool_ccuc	mon_ccuc	Least Connections (member)	OMS Host A:7788 OMS Host B:7788
Secure Upload	pool_ccsu	mon_ccsu	Least Connections (member)	OMS Host A:4900 OMS Host B:4900
Agent Registration	pool_ccar	mon_ccar	Least Connections (member)	OMS Host A:4889 OMS Host B:4889
Always-On Monitoring Secure Upload	pool_ccaom	mon_ccaom	Least Connections (member)	OMS Host A:8081 OMS Host B:8081
Secure JVMD	pool_ccsjvmd	mon_ccsjvmd	Least Connections (member)	OMS Host A:7301 OMS Host B:7301
Unsecure JVMD	pool_ccujvmd	mon_ccujvmd	Least Connections (member)	OMS Host A:7202 OMS Host B:7202

3. Create TCP Profiles

   TCP profiles are collections of TCP settings that are configurable settings for controlling the behavior of a particular type (e.g. TCP, HTTP) of network traffic. These profiles enhance control over network traffic and allow the user to control different characteristics for specific clients or applications (e.g. differing browsers).

   Separate TCP profiles can then be associated with different services or virtual servers as required for your operating environment.

   TCP profile values can have serious impacts on the network performance and should be used carefully and with careful consideration of your network and operational requirements.

TCP profile settings are site and SLB-specific therefore there are no specific OMS requirements for TCP profile settings. Refer to your SLB documentation and network administrator for required TCP profile configuration settings.

Table 24-4 TCP Profiles

Enterprise Manager Service	TCP Profile Name
Secure Console	tcp_ccsc
Unsecure Console	tcp_ccuc
Secure Upload	tcp_ccsu
Agent Registration	tcp_ccar
Always-On Monitoring Secure Upload	tcp_ccaom
Secure JVMD	tcp_ccsjvmd
Unsecure JVMD	tcp_ccujvmd

4. Create Persistence Profiles

   Certain types of applications may require the same client returning to the same pool member, this is called persistence or “stickiness". It can be configured using a persistence profile, and applied to the virtual server. For Oracle Enterprise Manager services, persistence needs to be configured for every service, except for the Secure Upload service.

   Some products offer session persistence support without cookies. These products depend on the IP address of the incoming request. In some circumstances, the originating IP address can change, resulting in session persistence being lost or the request redirected to the wrong backend server. If these cases occur, the service would be better defined to use cookies for persistence instead of source address affinity. Cookie persistence is only applicable when implementing SSL proxying architecture. For Layer 3 Load Balancing (formerly known as SSL Tunneling) the only Persistence Type alternative is Source Address Affinity.

Table 24-5 Persistence Profiles

Enterprise Manager Service	Persistence Profile Name	Type	Timeout	Expiration
Secure Console	sourceip_ccsc	Source Address Affinity or Cookie	3600	Not Applicable
Unsecure Console	sourceip_ccuc	Source Address Affinity or Cookie	3600	Not Applicable
Agent Registration	cookie_ccar	Cookie	Not Applicable	3600
Secure JVMD	sourceip_ccsjvmd	Source Address Affinity	3600	Not Applicable
Unsecure JVMD	sourceip_ccujvmd	Source Address Affinity or Cookie	3600	Not Applicable

5. Create Rules

   Rules are scripts that run against network traffic passing through your load balancer device. Rules give you the ability to influence network traffic in a variety of ways according to your functional needs.

   Some of the following are types of rules that may be configured, depending on your local Load Balancer:

- Access control rules which provide access to application resources based upon the source of the request.
- Access method rules which specify the permitted HTTP methods.
- URL redirect rules which route incoming HTTP requests to a different destination URL.
- Request and response header rules which add, alter or remove HTTP request or response headers.
- HTTP header rules which specify the size of the HTTP header and whether period and underscore characters are permitted within the headers.

Rule capabilities and rule definition syntax vary according to your Load Balancer vendor. Refer to the vendor documentation for information about these capabilities and syntactic guidance.

In the examples provided within this document, our virtual servers for Unsecure Console and Unsecure BI Publisher use notional rules for the purpose of redirecting requests to the Unsecure Console service (port 80) and Unsecure BI Publisher (port 8080) and sending them to the secure Console Service (port 443) and Secure BI Publisher (Port 5443) on the Load Balancer.

6. 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 24-6 Required Virtual Servers

Enterprise Manager Service	Virtual Server Name	Virtual IP and Port	Protocol Profile (Client)	Rule Name	Defaut Pool	Default Persistence Profile
Secure Console	vs_ccsc443	VIP:443	tcp_ccsc	None	pool_ccsc	sourceip_ccsc
Unsecure Console *	vs_ccuc80	VIP:80	tcp_ccuc	ccuc_httptohttps	pool_ccuc	sourceip_ccuc
Secure Upload	vs_ccsu4900	VIP:4900	tcp_ccsu	None	pool_ccsu	None
Agent Registration	vs_ccar4889	VIP:4889	tcp_ccar	None	pool_ccar	cookie_ccar
Always-On Monitoring Secure Upload	vs_ccaom8081	VIP:8081	tcp_ccaom	None	pool_ccaom	sourceip_aom
Secure JVMD	vs_ccsjvmd7301	VIP:7301	tcp_ccsjvmd	None	pool_ccsjvmd	sourceip_ccsjvmd
Unsecure JVMD	vs_ccujvmd7202	VIP:7202	tcp_ccujvmd	None	pool_ccujvmd	sourceip_ccujvmd

** These entries are not considered best practice and are not recommended as they provide unsecured and unencrypted access to Enterprise Manager.*

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
  -slb_jvmd_https_port 7301
  -lock_consle
  -lock_upload
  Oracle Enterprise Manager 24 Release 1
  Copyright (c) 1996, 2024 Oracle Corporation. All rights reserved.
  Securing OMS... Started
  Enter Enterprise Manager Root (SYSMAN) Password :
  Enter Agent Registration Password :
  (c) 1996, 2024 Oracle Corporation. All rights reserved.
  Securing OMS... Started.
  Securing OMS... Successful
  Restart OMS
```

The slb_console_port corresponds to the Virtual Server port that is used to access Enterprise Manager. This is defined above (in the Virtual Server Name - vs_gcsc443) with a Virtual Server Port of 443.

Restart the OMS after resecuring the Oracle Management Service. Repeat this step for each OMS supported by the Load Balancer.

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
   ```

3. Configure Always-On Monitoring

   Refer to the chapter “Alway-On Monitoring” in the Enterprise Manager Administrator's Guide for details on configuring the Always-on Monitoring application using the emsca utility.

   The following command must be run only once against any specific OMS after it is secured.

   ```
   emctl set property -name "oracle.sysman.core.events.emsURL" -value "https://
   slb.example.com:8081/upload"

   Enter Enterprise Manager Root (SYSMAN) Password :

   Oracle Enterprise Manager 24 Release 1

   Copyright (c) 1996, 2024 Oracle Corporation.  All rights reserved.

   Property oracle.sysman.core.events.emsURL has been set to value

   https://slb.example.com:8081/upload for all Management Servers

   OMS restart is not required to reflect the new property value
   ```

No Enterprise Manager components must be restarted for this command to take effect.

Adding a Second/Subsequent Always-On Monitoring Instance

Download the latest Always-On Monitoring (AOM) release from Self-Update. Copy the ems.zip file to a location where you want AOM to be installed and unzip the file.

The *emsca* tool can be rerun to add additional Always-On Monitoring instances to the same/different host as shown in the following example:

```
cd ems/scripts

./emsca add_ems
Oracle Enterprise Manager 24 Release 1
Copyright (c) 1996, 2024 Oracle Corporation.  All rights reserved.
-----------------------------------------------------------------
Event Monitoring Service Repository Connection String : emshost:25059:emssid
Event Monitoring Service Repository Username : ems
Event Monitoring Service Repository Password :
Enterprise Manager Repository Connection String : emhost:25059:emsid
Enterprise Manager Repository Username : sysman
Enterprise Manager Repository Password :
Enter Enterprise Manager Middleware Home : /mylocation/omsOracleHome
Connecting to EMS repository.
Registering EMS instance
Event Monitoring Service Upload URL: https://myemshost:1830/upload
Oracle PKI Tool : Version 12.1.3.0.0
Copyright (c) 2004, 2024, Oracle and/or its affiliates. All rights reserved.
Certificate was added to keystore
```

4. Configure EMCLI

   Configure the EMCLI client installations to use the SLB hostname and port for the EM console. This reconfiguration can be expected to run for approximately 15-20 minutes.

   ```
    emcli setup -url="https://slb.example.com:443/em" -username=sysman -
   trustall
   ```

Configuring SSL on Enterprise Manager and the SLB

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 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) 2024 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) 2024 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>
```

For more information about configuring multiple OMS High Availability behind a SLB, refer to Oracle Maximum Availability Architecture Best Practices for Enterprise Manager.

25

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:**
>
> Enterprise Manager 24ai supports a single approach to OMS Disaster Recovery. The Standby OMSs using Standby WebLogic Domain approach that was previously deprecated as of Enterprise Manager 12.1.0.3 is now desupported. Standby OMSs using Storage Replication is the supported approach and is discussed in this chapter.

Standby OMSs using Storage Replication is the disaster recovery approach in Enterprise Manager. 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.

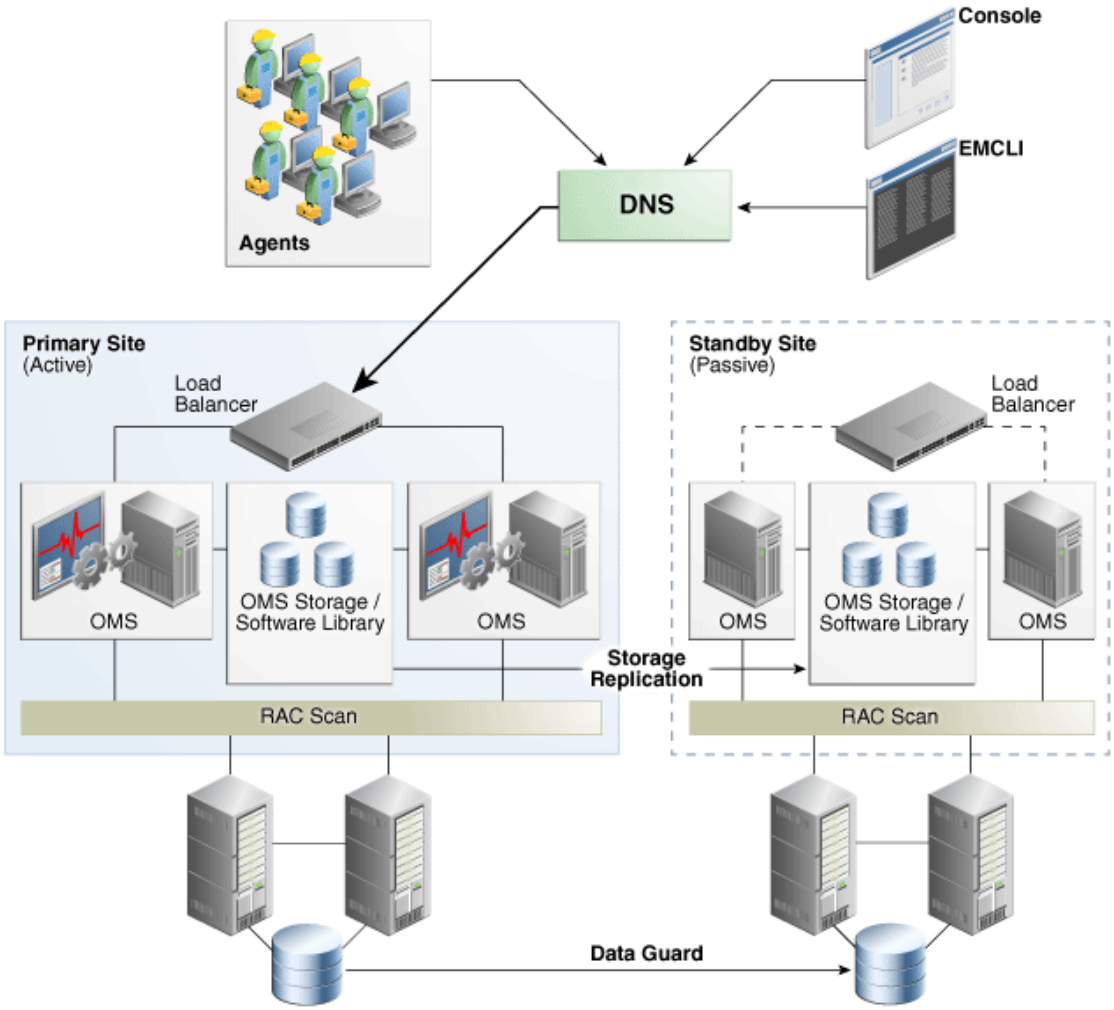
This chapter covers the following topics:

Disaster Recovery Overview and Topology

The Disaster Recovery solution for a Enteprise Manager 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 Enterprise Manager.

A complete implementation of the Enterprise Manager 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 25-1 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.

> **Note:**
>
> **3-Site DR Architecture Support**
> By default, Enterprise Manager out-of-the-box provides two sites: Primary Site and Standby Site with DR capabilities where the second site failover can take place.
>
> In some cases you have to abide by industry and/or regulatory requirements where all critical IT systems on which the institution relies for its business should not or cannot be down. If you want to expand the default DR architecture, you can include an additional site (a third site) which can be available for failover when the Primary and Standby sites are unavailable. To configure the 3-Site DR architecture, add the second Standby Site to your existing first Standby Site following the same steps updated in this document.

Design Considerations

This section discusses design considerations for a Enterprise Manager Disaster Recovery solution for an enterprise deployment.

The following topics are covered:

Network Considerations

The following sections discuss network considerations that must be taken into account when implementing standby Management Services using storage replication

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 Enterprise Manager 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 Enterprise Manager installation and start with alias host names or you have an existing Enterprise Manager 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 em_<platform>.bin 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
```

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.

Application Virtual Host Name Consideration

A hostname through which the Enterprise Manager clients (agents and users) should access Enterprise Manager 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 Enterprise Manager application hostname when using multiple OMSs with an SLB at each site is shown in the table below:

Table 25-1 DNS Configuration

DNS NAME	DNS RECORD TYPE	VALUE	COMMENTS
em.example.com	CNAME	slb_primary.example.com	Virtual Hostname used by Enterprise Manager 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 Enterprise Manager 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.

Storage Considerations

The Disaster Recovery solution for an Enterprise Manager 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`.
- Decide on appropriate replication frequency for the OMS file systems and software library 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 25-2 Storage Configuration

Volume	Mounted on Host	Mount Point	Comments
VOLOMS1	oms1-p.example.com (*Host 1*)	/u01/app/oracle/OMS	Installation of Enterprise Manager on Primary Site OMS1
VOLOMS2	oms2-p.example.com (*Host 2*)	/u01/app/oracle/OMS	Installation of Enterprise Manager on Primary Site OMS2
VOLSWLIB	oms1-p.example.com and oms2-p.example.com (*Host 1 + Host 2*)	/swlib	Software library on Primary Site OMS1 and OMS2
VOLAOM1	aom1.example.com / AOM (*Host 3*)	/u01/app/oracle /AOM	Always-On Monitoring installed on Host 3.
VOLAOM2	aom2.example.com / AOM (*Host 4*)	/u01/app/oracle/AOM	Always-On Monitoring installed on Host 4.

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.
- Logical standby Management Repository databases are not supported for disaster recovery.
- 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 Connect Descriptor Considerations, 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 Connect Descriptor Considerations.

  ```
  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
  ```

Connect Descriptor Considerations

Two technologies that together dramatically improve the simplicity of connection string management for Repository databases for Disaster Recovery are 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, see *Oracle Clusterware Administration and Deployment*.

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, 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 12, 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))))
```

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 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

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.

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 and Setting Up the OMS and Software Library Disaster Recovery to complete the DR setup.

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.
2. Use the procedure documented in The primary site is already created, standby site is being planned.

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 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 and Software Library Disaster Recovery

Setting Up Management Repository Disaster Recovery

The Management Repository should use Data Guard as a Disaster Recovery solution.

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.

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.

Setting Up the OMS and Software Library Disaster Recovery

The Disaster Recovery solution for a Enterprise Manager deployment involves installing the Software Library, OMS installation, Agent installation and Oracle inventory on replicated filesystem.

The recommended method for creating Standby OMSs is to use storage replication as documented in this chapter.

> **Note:**
>
> Enterprise Manager 24ai supports a single approach to OMS Disaster Recovery. The Standby OMSs using Standby WebLogic Domain approach that was previously deprecated as of Enterprise Manager 12.1.0.3 is now de-supported. Standby OMSs using Storage Replication is the supported approach and is discussed in this chapter.

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

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 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 Advanced Installation and Configuration Guide* for more information.

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 the chapter on EMCTL Commands for Management Agent in the *Enterprise Manager Administrator's Guide* for details on changing the agent time zone.

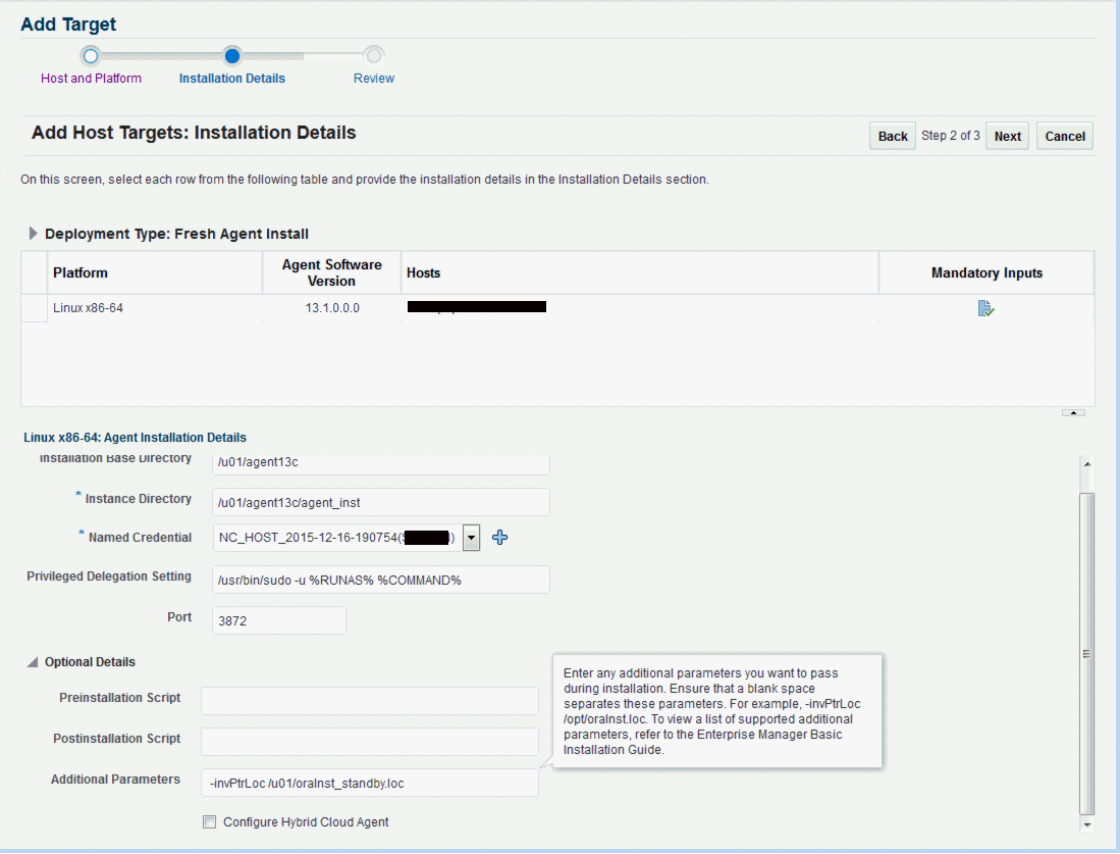
To specify an inventory location for Agent installation, an inventory pointer file can be created and the `-invPtrLoc` flag can be used during installation.

The following example shows an inventory pointer file that defines 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.



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 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).

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 Enterprise Manager.
- Use the process documented in the *Enterprise Manager Administrator's Guide* to move the software library to shared storage.

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.`

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. Shut down the Always-On Monitoring service for each of the OMSs:

   `<AOM location>/scripts/emsctl stop`
4. Unmount the OMS filesystem and the software library filesystems from OMS hosts at the primary site.

   If configured, unmount the BIP shared storage and AOM storage filesystems.
5. 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.
6. Update DNS entry for the application virtual hostname.
7. 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>;
```

8. Perform role reversal of the Software Library and OMS storage (refer to your storage documentation for instructions).
9. Re-enable replication schedules for SWLIB and OMS storage.

   If AOM hase been configured, re-enable replication schedules for the AOM storage location.
10. Mount OMS, AOM (if configured), and Software Library filesystems on OMS hosts at Standby site.
11. 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 Database Considerations.

12. Point the OMS to the 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 Database Considerations.

This step should be repeated on each OMS.

13. Point AOM to the new Primary Repository Database using the following command:

```
emsctl set_ems_repos_conn -username=<repository username> -password=<repository
password> -connect_string=<repository connect descriptor>
```

Note: Changing the AOM connect information applies only to the local AOM instance.This command must be executed on each AOM instance in order for it to take affect.

14. Start the OMSs and AOMs (if configured) at the standby site.
15. Start the Management Agents at the standby site using the following command:

```
emctl start agent
```

16. 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.

17. Update the URI for the WebLogic Admin Console from within Enteprise Manager.

    Navigate to the target homepage for *GCDomain*. From the **WebLogic Domain** menu, select **Target Setup**, and then **Monitoring Configuration**.

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. Shut down all AOM instances (if configured).
4. 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.

   If AOM has been configured, unmount the AOM storage filesystem.
5. 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, perform an on-demand replication of the BI Publisher shared storage filesystem. If AOM has been configured, perform an on-demand replication of the AOM storage filesystem.

> **Note:**
>
> Refer to your storage documentation for steps required to perform an on-demand replication.

6. Update the DNS entry for the application virtual hostname.
7. Failover Oracle Database using Data Guard failover.
8. Perform role reversal of Software Library and OMS storage.
9. Re-enable replication schedules for SWLIB and OMS storage
10. Mount the OMS and Software Library filesystems on OMS hosts at the standby site
11. Start the first OMS Admin Server.

> **Note:**
>
> This step is not required if the following two conditions are met:
>
> a. Using a Repository Connect Descriptor that works from both primary and standby sites, such as by using SCAN addresses and Role-Based Database Services.
>
> b. Running in Data Guard Maximum Protection or Maximum Availability level as there is no data loss on failover.

12. 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.

13. Modify the AOM connect descriptor to point to the new Primary Repository Database:

```
emsctl set_ems_repos_conn -username=<repository username> -password=<repository
password> -connect_string=<repository connect descriptor>
```

Changing the AOM connect information applies only to the local AOM instance

This command must be executed on each AOM instance in order for it to take affect.

14. 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.

15. Start the Agents at the standby site.
16. Start the OMSs at the standby site.
17. Start the AOM instances at the standby site.
18. Modify Management Services and Repository target connect descriptor.

    From the **Setup** menu, select **Manage Enterprise Manager** 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

19. Update the URI for the WebLogic Admin Console from within Enteprise Manager.

    Navigate to the target homepage for *GCDomain*. From the **WebLogic Domain** menu, select **Target Setup**, and then **Monitoring Configuration**.

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

> **Note:**
>
> Refer to your storage documentation for steps required to perform an on-demand replication.

26

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:

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, see *Installation of Enterprise Manager* in the *Oracle Enterprise Manager Basic Installation Guide*.

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.

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 Enterprise Manager console.

Management Repository 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 Enterprise Manager 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 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.

For a thorough summary of how to configure backups using Enterprise Manager, see *Configuring Your Database for Basic Backup and Recovery* in the *Oracle Database 2 Day DBA*. For additional information on Database high availability, see *Overview of High Availability*.

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 Enterprise Manager 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 Enterprise Manager 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).

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 Enterprise Manager console to install and maintain reference Agent installs.

If a Management Agent is lost, it should be reinstalled by cloning from a reference install.

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

Repository Recovery

Recovery of the Repository database must be performed using RMAN since Enterprise Manager 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 Enterprise Manager console unless the repository is synchronized with the latest state available on the Agents.

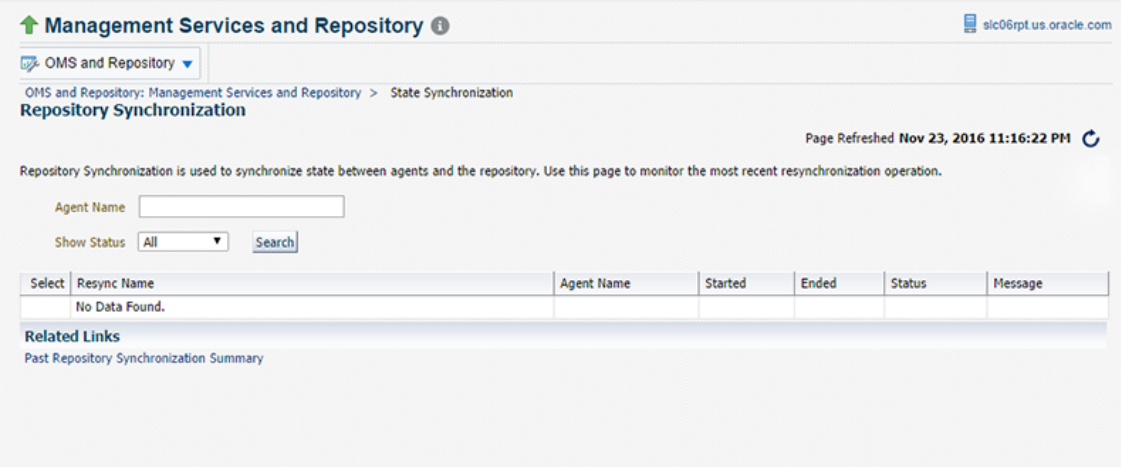
A repository resync feature allows you to automate the process of synchronizing the Enterprise Manager repository with the latest state available on the Management Agents.

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 26-1 Repository Synchronization Page



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

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.

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.

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 Enterprise Manager. From the Setup menu, select **Manage Enterprise Manager**, and then **Health Overview**. The Management Services and Repository page displays.
6. From the **OMS and Repository** menu, select **Repository Synchronization**.
7. Verify that the site is fully operational.

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.

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 Enterprise Manager. From the Setup menu, select **Manage Enterprise Manager**, 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.

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.

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 Enterprise Manager 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 PLUGIN_LOCATION=<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.

To apply the patches in bitonly mode, use the following command:

- `$omspatcher apply -analyze -bitonly`
- `$omspatcher apply -bitonly`

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.

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.

OMS Recovery Scenarios

The following scenarios illustrate various OMS recovery situations along with the recovery steps.

> **Note:**
>
> 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.

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 Enterprise Manager 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 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, the Management Agent instance directory should be recreated to ensure consistency between the Management Agent and OMS.

   a. Remove the agent_inst directory if it was restored from backup.
   b. Use `agentDeploy.sh` to configure the agent:

      ```
      <AGENT_BASE_DIR>/core/24.1.0.0.0/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 the Management Agent configuration fails, see `<AGENT_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent_<time_stamp>.log`
   c. 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.

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".

   Note: If configured, all BIP shared locations (sharedLoc) should also accessible.

2. Restore the software homes on “Host B". See 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>/agent_24.1.0.0.0/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 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>
```

After running the above, point all targets to the new OMS Agent: Go to **EM Console** > **Middleware** > **GCDomain** > **target Setup** > **Modify Agents**, enter "new Agent name", click **Assign** and click **Modify Targets**.

> **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 Enterprise Manager console, locate the 'WebLogic Domain' target for the Enterprise Manager 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 Enterprise Manager 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.

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 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/24.1.0.0.0/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.

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 Enterprise Manager 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 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.

   a. Remove the agent_inst directory if it was restored from backup.
   b. Use agentDeploy.sh to configure the Management Agent:

      ```
      <AGENT_HOME>/core/24.1.0.0.0/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>
      ```
   c. 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.

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 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_BASE_DIR>/agent_24.1.0.0.0/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>
   ```

   - **Custom Certificates**: If the OMS is secured with custom certificates, run the following:

     ```
     emcli relocate_targets -dest_agent="emc123.example.com:3872" -
     src_agent="emcc456.example.com:3872" -copy_from_src -force=yes -
     ```

```
target_name="Management Services and Repository" -
target_type=oracle_emrep
```

- **Non-default plug-ins:** 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 Enterprise Manager console, locate the 'WebLogic Domain' target for the Enterprise Manager 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 Enterprise Manager 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.

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 Enterprise Manager 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 Installing Additional Oracle Management Services in Silent Mode.
5. Verify that the site is fully operational.

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.

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.

If agent is not reinstalled by using clone option, patches should be reapplied after new agent is installed.

> **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.

> **Note:**
>
> 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.

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.

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.

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.

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.

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 Single OMS, No Server Load Balancer (SLB), OMS Restored on the same Host.
3. Verify that the site is fully operational.

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 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 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 Multiple OMS, Server Load Balancer Configured, Primary OMS Recovered on a Different Host.

3. Follow the OMS recovery procedure shown in Multiple OMS, SLB configured, additional OMS recovered on same or different host.
4. Verify that the site is fully operational.

27

Oracle Management Service Migration

Starting with Enterprise Manager 13c Release 5 Update 24 (13.5.0.24), the Oracle Management Service (OMS) migration has been automated. This process allows you to perform the OMS migration to a different host in an easier and simpler way.

OMS migration is supported on all the platforms that the OMS is certified. For certification information, see My Oracle Support.

Prerequisites Check

Before performing the OMS migration, complete the following prerequisites:

1. Check the operating system of the hosts.
   The source and destination hosts must have the same operating system.

   > **Note:**
   >
   > Cross platform OMS migration are not supported.

2. The Management Agent needs to get installed and running on the destination host (host where the OMS is going to get migrated) prior to starting the OMS migration process. Once completed, verify the agent status on the destination host by running the following:

   ```
   <AGENT_HOME>/bin> ./emctl status agent
   ```

3. Confirm the disk space available.
   The minimum disk space available is 25 Gb in the destination host.
4. The software library location must be the same on both hosts. It must accessible and empty on the destination host.
   As part of the migration process, files are copied over to the same location from the source to the destination host.

Perform Oracle Management Service Migration

After completing the prerequisites check, perform the following steps to migrate the OMS:

- Step 1: Launch the Migrating OMS Deployment Procedure
- Step 2: Run ConfigureGC Wizard

Step 1: Launch the Migrating OMS Deployment Procedure

A deployment procedure is a sequence of provisioning steps and phases where each phase can contain sequence of steps. The **Migrating the OMS to another host** deployment procedure is provided by Oracle to be used to perform OMS migrations.

During this step, the OMS files are being copied over from the source to the destination host.

To launch the **Migrating the OMS to another host** deployment procedure, do the following:

- From the Enterprise Manager Console, click **Enterprise**.
- Under **Enterprise**, click **Provisioning and Patching** and then **Procedure Library**.

  The **Deployment Procedure Manager** page is displayed.
- Under **Search Text Field**, enter **Migrating the OMS to another host** and click **Go**.

  From the results, select the **Migrating the OMS to another host** deployment procedure and click **Launch**.

  The **OMS Migration Service** wizard is displayed.

  1. On the **OMS Migration Service: Getting Started** page, confirm that you completed the prerequisites by selecting the appropriate checkboxes and click **Next**.
     For details about the OMS migration prerequisites, see Prerequisites Check.
  2. On the **OMS Migration Service: Select Destination** page, provide the following:
     - **Destination Host**: Host name where the OMS is getting migrated to.
     - **Destination Instance Base Location**: Location where the configuration files of the OMS migration service process are created. The location must be same on the source and destination hosts.

     Under **Source Credentials**, provide the credentials details of the user that owns the OMS software installation in the source host.

     Under **Destination Credentials**, provide the credentials details of the user that owns the OMS software installation in the destination host.

     Click **Next**.
  3. On the **OMS Migration Service: Options** page, do the following:
     - Under **File Transfer Options**, provide the preferred transferred mode to copy files over from the source to the destination host to complete the deployment procedure process.
     - Under **Staging Locations**, provide the locations in the source and destination hosts to store the temporary files during the deployment procedure process. They will be cleaned up once deployment procedure is completed.
  4. On the **OMS Migration Service: Post Creation Steps** page, review the information provided and click **Next**.
  5. On the **OMS Migration Service: Review** page, review the details provided and click **Finish** to run the deployment procedure.

Once the deployment procedure is completed, connect to the destination host and perform Step 2: Run ConfigureGC Wizard.

Step 2: Run ConfigureGC Wizard

During this step, the OMS files are being configured in the destination host.

Prerequisite:

Confirm that all the OMSs are down: The source OMS and if applicable, its additional OMSs.

Configure the Migration

Connect to the destination host, go to the `<OMS_HOME>sysman/install` directory and execute the following:

```
./ConfigureGc.sh -omsmigration
```

The **ConfigureGC** wizard is displayed.

- Select **Migrate Enterprise Manager system** and click **Next**.
- Under **Installation Details**, review the destination host information.
  The **Host Name** and **Backup file location** get populated automatically and cannot be edited.

  Click **Next**.
- Under **Configuration Details**, provide the database and WebLogic credentials information.
  - The database connector details.
  - The SYSMAN password.
  - The WebLogic Server Administrator password.
  - The Node Manager password.
  - The Agent Registration password.

  Click **Next**.
- Review and click **Configure**.

Run ConfigureGC in Silent Mode

Alternatively, you can run `ConfigureGC` script in silent mode by doing the following:

```
cd <oms_home>/sysman/install
./ConfigureGC.sh -omsmigration -silent -responseFile <response_file>
```

See below an example of the response file:

```
# oms migration response file for silent install
SYS_PASSWORD=pwdwelcome9
SYSMAN_PASSWORD=pwdwelcome9
SYSMAN_CONFIRM_PASSWORD=pwdwelcome9
WLS_ADMIN_SERVER_PASSWORD=pwdwelcome9
WLS_ADMIN_SERVER_CONFIRM_PASSWORD=pwdwelcome9
NODE_MANAGER_PASSWORD=pwdwelcome9
NODE_MANAGER_CONFIRM_PASSWORD=pwdwelcome9
AGENT_REGISTRATION_PASSWORD=pwdwelcome9
```

Post Migration Tasks

The following steps should be performed to ensure that the Oracle Management Service (OMS) migration was successful:

1. Start the OMS.

Run the following:

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

The output looks similar to the following:

```
Oracle Enterprise Manager 24 Release 1
Copyright (c) 1996, 2024 Oracle Corporation. All rights reserved.
Starting Oracle Management Server...
WebTier Successfully Started
Oracle Management Server Successfully Started
Oracle Management Server is Up
JVMD Engine is Up
```

Verify the OMS status by running the following:

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

2. Secure the source OMS agent with the new OMS.
   Confirm that the source OMS agent is up and running, then secure it with new OMS to relocate the targets.

   Run the following command in the source OMS Agent server:

   ```
   <Source_AGENT_HOME>/bin/emctl secure agent -emdWalletSrcUrl https://
   <NEW_OMS HOST_NAME. DOMAIN NAME>:<HTTPS UPLOAD_PORT>/em
   ```

3. Refresh Weblogic Domain to reconfigure the domain with the new hostname.
   In the Enterprise Manager Console, do the following:
   - Navigate to **Targets**, **Middleware** and locate the **WebLogic Domain(GCDomain)** target.
   - Right click on the GCDomain, select **Target Setup** and then, **Monitoring Credentials**.
   - Update the Administration Server Host to the new OMS hostname and click **Ok**.
   - Return to **Targets** and **Middleware**, right click on the GCDomain target and select **Refresh Weblogic Domain**.
   - Click on **Add/Update Targets** and wait for the domain to refresh.
4. Relocate the source OMS Agent targets to the target OMS Agent.
   To point all targets to new the agent, do the following:
   - Navigate to **Targets** and **All Targets**
   - Click **GCDomain**, select **Target Setup** and **Modify Agents**. Then, click **Continue**.
   - Under **Monitor All Targets Using This Agent**, enter "`<new Agent Hostname.domain name>:<port>`" and then click **Assign**.
   - The list is populated with `<new Agent Hostname.domain name>:<port>` under **New Agent**.
   - Click **Modify Agents**.
5. Relocate the `oracle_emrep` target to the Management Agent of the new OMS host.

Run the following:

```
<OMS_HOME>/bin/emcli login -username=sysman
<OMS_HOME>/bin/emcli sync
<OMS_HOME>/bin/emctl config emrep -agent <new oms hostname.domain
name>:<agent port>
```

For example:

```
<OMS_HOME>/bin>./emctl config emrep -agent <new oms hostname.domain
name>:<agent port>
Oracle Enterprise Manager 24 Release x
Copyright (c) 1996, 2024 Oracle Corporation. All rights reserved.
Please enter repoEnter password : Login successful
Moved all targets from <old oms hostname.domain name>:<port> to <old oms
hostname.domain name>:<agent port>
Command completedEnter password : Login successful
Moved all targets from <old oms hostname.domain name>:<port> to <new oms
hostname.domain name>:<agent port>
Command completed successfully!
<OMS_HOME>/bin>
```

6. Resecure Management Agents.
   Resecure all management agents point to this OMS using new OMS hostname .

   ```
   <AGENT_INST>/bin/emctl secure agent -emdWalletSrcUrl https://<NEW_OMS
   HOST_NAME.DOMAIN NAME>:<UPLOAD_PORT>/em
   ```

7. Remove stale OMS entries.
   The repository will be having the old OMS information which should be cleaned up.

   To get the stale OMS entries cleaned, follow the My Oracle Support Doc Id 2764682.1 - **How To Cleanup the Old OMS Entries in the Repository DB That are Leftover After OMS Migration Activity**.

8. Migrate additional OMSs.

   If you want to migrate additional OMSs then decommission additional OMSs once the primary OMS migration was successful.

   It's recommended to reinstall/reconfigure the additional OMSs using the regular Add OMS deployment procedure or the Silent method to install additional OMS.

> **Note:**
>
> For more details, see Doc ID : 2913963.1 from My Oracle Support.

Part VIII
Deinstallation

In particular, this part contains the following chapters:

- Deinstalling Enterprise Manager (Single and Multi-OMS Environments)
- Decommissioning and Deinstalling Oracle Management Agents
- Deinstalling JVMD Agents
- Removing Standby Oracle Management Services

28

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:

Deinstallation Scope

The following describes the scope of deinstalling the components of an Enterprise Manager system.

Table 28-1 Deinstallation Scope

Environment Type	OMS Type	Installation Type	Components Deinstalled	Components Not Deinstalled
Single OMS, Multi-OMS	First OMS	Fresh Installation	• First OMS *(including the instance home)* • Central Agent • Management Repository	Not Applicable
Single OMS, Multi-OMS	First OMS	Upgrade	• First OMS *(including the instance home)* • Management Repository	Central Agent. To deinstall the central agent, see Decommissioning and Deinstalling Oracle Management Agents.
Multi-OMS	Additional OMS	Fresh Installation	Additional OMS	• Management Repository • Standalone Management Agent running on the additional OMS host. To deinstall the central agent, see Decommissioning and Deinstalling Oracle Management Agents.

Table 28-1 (Cont.) Deinstallation Scope

Environment Type	OMS Type	Installation Type	Components Deinstalled	Components Not Deinstalled
Multi-OMS	Additional OMS	Upgrade	Additional OMS	• Management Repository • Standalone Management Agent running on the additional OMS host. To deinstall the central agent, see Decommissioning and Deinstalling Oracle Management Agents.

Deinstalling the Enterprise Manager System

To deinstall an Enterprise Manager system in a single OMS environment or multi-OMS environment, follow these steps:

> **Note:**
>
> - Before you begin, understand the scope of deinstallation as described in Deinstallation Scope.
> - For a multi-OMS environment, first deinstall the additional OMS instances, and then deinstall the first OMS.
> - The steps outlined in this section not only deinstall the OMS instances but also deinstall the Management Repository.
> - Once the Management Repository is deinstalled from the database, you can reuse the empty database for any other purpose. Only the Enterprise Manager schema is removed from the database, but the physical files or the software binaries of the database software will continue to remain on the host.
> - The steps outlined in this section do not deinstall, remove, or roll back any of the patches applied on the database.
> - For a fresh OMS installation, either the first OMS or an additional OMS, the steps outlined in this section automatically remove the middleware, the OMS, the OMS instance home, and the Management Agent directories.
> - For an upgraded OMS, either the first OMS or an additional OMS, the steps outlined in this section automatically remove the middleware, the OMS, and the OMS instance home directories, but not the Management Agent directory. You must deinstall the Management Agent as described in Decommissioning and Deinstalling Oracle Management Agents.

1. Copy the deinstallation script from the Oracle home of the OMS host to a temporary or stage location.

   ```
   cp <ORACLE_HOME>/sysman/install/EMDeinstall.pl <temporary_location>
   ```

   For example,

```
cp /u01/software/em24/oms_home/sysman/install/EMDeinstall.pl /u01/
tmp_deinstall
```

2. Deinstall the OMS.

   ```
   <ORACLE_HOME>/perl/bin/perl <temporary_location>/EMDeinstall.pl -mwHome
   <Middleware_Home> -stageLoc <temporary_location>
   ```

   You will be prompted for database credentials (SYS and SYSMAN) and the WebLogic Domain credentials. Enter the credentials and proceed with the deinstallation.

   The Middleware_Home is the parent directory of both the `oms_home` and `ext_oms_home`.

   For example,

   ```
   /u01/software/em24/oms_home/perl/bin/perl /u01/tmp_deinstall/EMDeinstall.pl -
   mwHome /u01/software/em24/ -stageLoc /u01/tmp_deinstall
   ```

> **Note:**
>
> 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 symlinks associated with it because when you install Enterprise Manager again on the same host, the installer automatically overwrites the script and re-create the symlinks.
>
> However, if you want to clear the host of any Oracle products, then Oracle recommends that you manually delete this script and the symlinks 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`.

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 Console. For instructions, see the *Oracle Enterprise Manager Administrator's Guide*. **Do NOT use this chapter to undeploy only the plug-ins.**

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:

- Run the following command from the Primary OMS 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_oms_apigateway and oracle_oms_svcapp.

  ```
  $ORACLE_HOME/bin/omsca delete -OMSNAME <oms name>
  ```

  Example: For cleaning up entries of a second OMS, the command will be `$ORACLE_HOME/bin/omsca delete -OMSNAME "EMGC_OMS2"`

This task will remove all references to the deleted OMS in the Management Repository database.

Now Enterprise Manager will not have any reference of the deleted additional OMS.

29

Decommissioning and Deinstalling Oracle Management Agents

This chapter describes how to decommission and deinstall standalone Oracle Management Agents (Management Agent). In particular, this chapter covers the following:

- Decommissioning Oracle Management Agents
- Deinstalling Oracle Management Agents
- Deinstalling or Undeploying Only Plug-ins from the Oracle Management Agent

Decommissioning Oracle Management Agents

This section describes the various ways of decommissioning Oracle Management Agents. In particular, this section covers using the **Agent Decommission** feature from the Enterprise Manager console user interface and from command line using `emcli` commands. They both allow to decommission a single or multiple agents at the same time.

- Decommissioning Management Agents Using Enterprise Manager Console
- Decommissioning Management Agents Using emcli

Decommissioning Management Agents Using Enterprise Manager Console

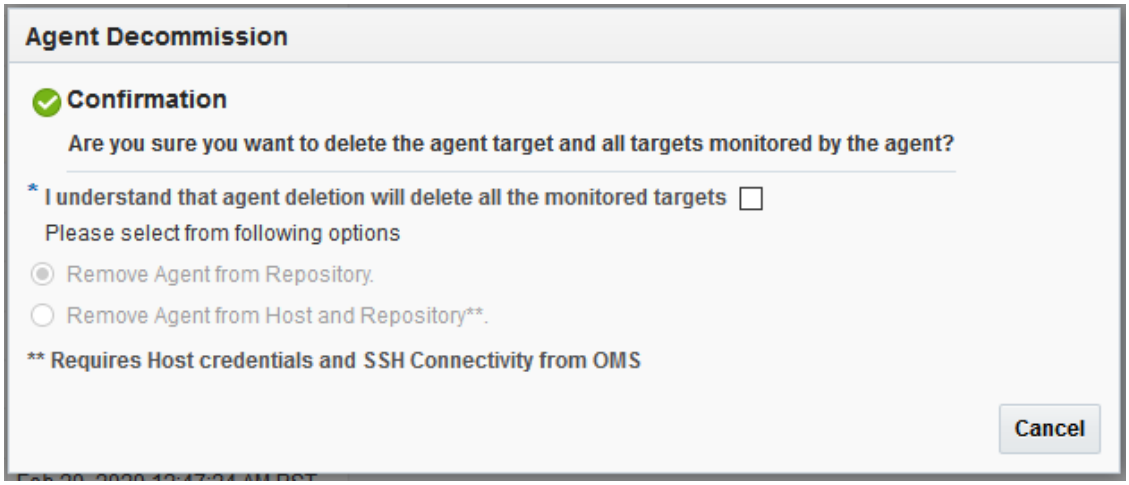
To decommission Management Agents using the Enterprise Manager console, you can use the **Agent Decommission** button under **Setup** > **Manage Enterprise Manager**>**Agents** page.

If you want to decommission a single agent, you can also use the **Agent Decommission** option from Agent Home page by going to **Targets**> **Select Agent** > **Agent** > **Target Setup** > **Agent Decommission**.

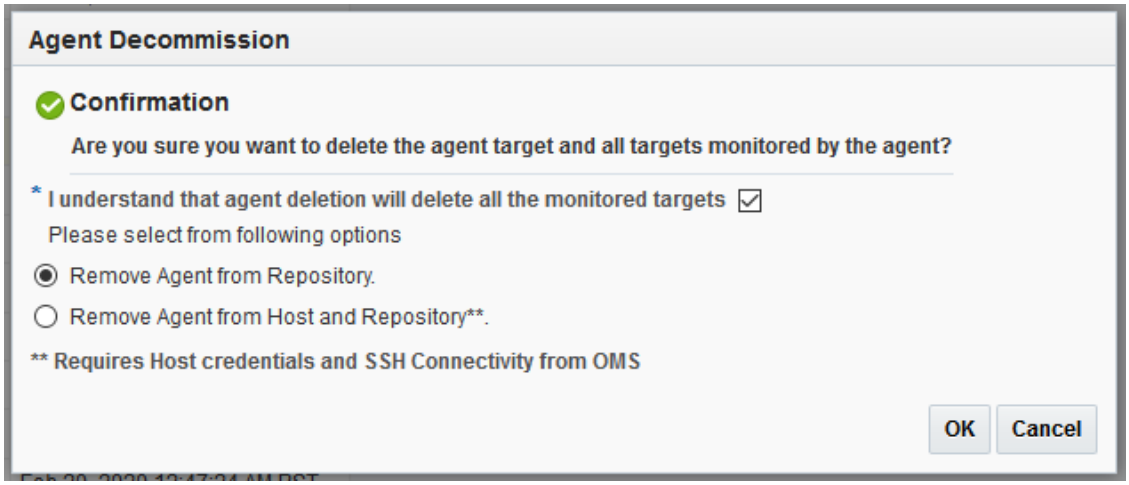
The **Agent Decommission** provides the following two options:

- **Remove Agent from Repository**: It removes the agent(s) selected and its targets from the repository. It doesn't require agent host credentials. Only super user credentials are sufficient.
- **Remove Agent from Host and Repository**: It removes the agent(s) selected and its targets from the repository. It also performs an agent software deinstallation from the host and it requires agent install user host credentials. If you select this option, there's no need to cleanup any directories or to do any agent deinstallation manually afterward.

After you select the desired option, the Agent Decommission confirmation window will be displayed:



Check "*I understand that agent deletion will delete all the monitored targets*" checkbox. Then, select your option and press **OK**.



After confirmation, the Enterprise Manager Jobs page will open. You need to enter the required details information and click **Submit**. The **Successful Job Submission** window will be displayed with the link to the Agent Decommission job. In some cases, user may not see the complete job details since the targets and agents are already removed from repository.

Decommissioning Management Agents Using emcli

To decommission Management Agents using `emcli` commands, you can use the command line to create scripts and manage the agent decommission process by running the scripts manually.

Decommissioning agents using `emcli` provides the following two options:

- **Remove Agent from Repository**: It removes the desired agent(s) and its targets from the repository. This option doesn't require agent host credentials. Only super user credentials are sufficient. This option type is called `"Multiple Agents Decommission"`.
- **Remove Agent from Host and Repository**: It removes the desired agent(s) and its targets from the repository. It also performs an agent software deinstallation from the host and it requires agent install user host credentials. There's no need to cleanup any directories or to do any agent deinstallation manually afterward. This option type is called `"Multiple Agents Cleanup"`.

Follow the instructions below:

1. Create an input property file using a text editor with the following required parameters:

   name is any job name you would like to use.

   type is the agent decommission option type name. It can be `type=Multiple Agents Decommission` or `type=Multiple Agents Cleanup`.

   target_list specifies the list of targets using the fully qualified host name and port number. For example, `target_list=host1.example.com:1834:oracle_emd`.

   schedule.frequency specifies the frequency. The supported value is `IMMEDIATE`.

   cred.agent_creds.<all_targets>:oracle_emd specifies the agent credentials. This is a mandatory parameter only when using `type=Multiple Agents Cleanup`. For example, `cred.agent_creds.<all_targets>:oracle_emd=NAMED:agentinst`

   - Sample input property file for `type=Multiple Agents Cleanup`

     ```
     name=Multi Agent Full Cleanup Job
     type=Multiple Agents Cleanup
     target_list=<FQDN_Host_Name1>:<port>:oracle_emd
     target_list=<FQDN_Host_Name2>:<port>:oracle_emd
     target_list=<FQDN_Host_Name3>:<port>:oracle_emd
     schedule.frequency=IMMEDIATE
     cred.agent_creds.<all_targets>:oracle_emd=NAMED:<Agent_Install_User>
     ```

     If `type=Multiple Agents Cleanup`, all agents targets should have been installed with the same agent credentials. If there are agents targets installed with different credentials, the input property file with different credentials should be created.

   - Sample input property file for `type=Multiple Agents Decommission`

     ```
     name=Multi Agent Decommission Repo only
     type=Multiple Agents Decommission
     target_list=<FQDN_Host_Name1>:<port>:oracle_emd
     target_list=<FQDN_Host_Name2>:<port>:oracle_emd
     target_list=<FQDN_Host_Name3>:<port>:oracle_emd
     schedule.frequency=IMMEDIATE
     ```

   After creating the appropriate input property file, it can be saved as a text file. For example, it can be named `"decom_agent_multi.txt"`.

2. Run `emcli` command to create the job using the text file created in Step 1.

   ```
   ./emcli create_job -input_file=property_file:"decom_agent_multi.txt"
   Creation of job "MULTI AGENT FULL CLEANUP JOB" was successful.
   ```

3. Check status of the agent decommission job.

   ```
   ./emcli get_jobs -name="MULTI AGENT FULL CLEANUP JOB"
   Name    Type
   Job ID                              Execution ID
   Scheduled
   Completed        TZ Offset    Status    Status ID  Owner    Target Type
   Target Name
   MULTI AGENT FULL CLEANUP JOB  Multiple Agents Decommission
   90AF4B4FBAD35BAEE053BD70F00A8249  90AF4B4FBADC5BAEE053BD70F00A8249
   2019-08-21 22:52:25
   ```

```
none             GMT-07:00  Running  2           SYSMAN  oracle_emd
<Host_Name1>:<port>
MULTI AGENT  FULL CLEANUP JOB  Multiple Agents Decommission
90AF4B4FBAD35BAEE053BD70F00A8249  90AF4B4FBAD55BAEE053BD70F00A8249
2019-08-21 22:52:25
none             GMT-07:00  Running  2           SYSMAN  oracle_emd
<Host_Name2>:<port>
MULTI AGENT  FULL CLEANUP JOB  Multiple Agents Decommission
90AF4B4FBAD35BAEE053BD70F00A8249  90AF4B4FBAD95BAEE053BD70F00A8249
2019-08-21 22:52:25
none             GMT-07:00  Running  2           SYSMAN  oracle_emd
<Host_Name3>:<port>
```

Deinstalling Oracle Management Agents

This section lists the deinstallation prerequisites and describes the various ways of deinstalling a standalone Oracle Management Agent. In particular, this section covers the following:

- Deinstalling Standalone Management Agents
- After Deinstalling Standalone Management Agents

> **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 standalone Management Agent and install a new standalone 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 standalone Management Agent, then run the `emcli relocate_targets` command to hand over the targets from the old standalone Management Agent to the new standalone Management Agent, and then deinstall the old standalone Management Agent.
>
> For information about the `emcli relocate_targets` command, see *relocate_targets* in the *Oracle Enterprise Manager Command Line Interface Guide.*

Deinstalling Standalone Management Agents

This section describes the following:

- Deinstalling Standalone Management Agents Using the AgentDeinstall.pl Script
- Deinstalling Shared Agents
- Deinstalling Standalone Management Agents Installed Using an RPM File

Deinstalling Standalone Management Agents Using the AgentDeinstall.pl Script

To deinstall a standalone Management Agent using the `AgentDeinstall.pl` script, follow these steps:

1. Invoke the `AgentDeinstall.pl` script to delete the standalone Management Agent and also remove the agent base directory.

   ```
   $<AGENT_HOME>/perl/bin/perl <AGENT_HOME>/sysman/install/AgentDeinstall.pl -
   agentHome <AGENT_HOME>
   ```

   For example,

   ```
   /u01/software/em24/agentbasedir/agent_24.1.0.0.0/perl/bin/perl /u01/software/
   em24/agentbasedir/agent_24.1.0.0.0/sysman/install/AgentDeinstall.pl -
   agentHome /u01/software/em24/agentbasedir/agent_24.1.0.0.0
   ```

2. Manually remove the targets, which were being monitored by the standalone Management Agent you deinstalled, from the Enterprise Manager Console. To do so, run the following EM CTL command from any host where EM CLI is installed.

   ```
   emcli delete_target

   -name="<host_name>:<agent_port>"

   -type="oracle_emd"

   -delete_monitored_targets
   ```

   For example,

   ```
   emcli delete_target

   -name="example.com:1836"

   -type="oracle_emd"

   -delete_monitored_targets
   ```

3. Manually delete the agent base directory. For information on agent base directory, see What Is an Agent Base Directory?.

   For UNIX platforms:

   ```
   rm -rf <absolute_path_to_install_base_dir>
   ```

   For Microsoft Windows platforms:

   ```
   rmdir /s /q <absolute_path_to_install_base_dir>
   ```

> **Note:**
>
> While deinstalling the standalone Management Agent, the Management Agent service is removed automatically. If the service is not removed automatically, you can remove it manually after the deinstall, by running the following command:
>
> ```
> sc delete <service_name>
> ```

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,

```
/shared/app/agentbasedir/agent_24.1.0.0.0/perl/bin/perl /shared/app/agentbasedir/
agent_24.1.0.0.0/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_HOME=/
shared/app/agentbasedir/agent_inst ORACLE_HOME=/shared/app/agentbasedir/
agent_24.1.0.0.0
```

Deinstalling Standalone Management Agents Installed Using an RPM File

To deinstall a standalone 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.

After Deinstalling Standalone Management Agents

After you deinstall a standalone Management Agent, follow these steps:

1. Verify that 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` that will be present under `/etc/init.d` directory.

   > **Note:**
   >
   > These auto-start scripts are not available on Microsoft Windows.

2. If you deinstalled on a Microsoft Windows platform, then follow these steps to remove the entries from the Microsoft Windows registry. Ensure that you are logged in as a user with Administrator privileges on that host.

   a. Expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Oracle**, and then **Sysman**. Under the **Sysman** directory, delete the Management Agent service. For example, `Oracleagent13cAgent`.

   b. Close the registry editor.

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 to deinstall the Management Agent itself, then use the Plug-ins page within the Enterprise Manager Console. For instructions, see *Undeploying Plug-Ins from Oracle Management Agent* in the *Oracle Enterprise Manager Administrator's Guide.***Do NOT use the installer to undeploy only the plug-ins.**

30
Deinstalling JVMD Agents

This chapter describes how you can deinstall Java Virtual Machine Diagnostics (JVMD) Agents in the Enterprise Manager environment.

Deinstalling JVMD Agents

This section describes the methods to remove JVMD Agents. It consists of the following:

- Removing JVMD Agents Using Engines And Agents Page
- Removing JVMD Agents Manually

Removing JVMD Agents Using Engines And Agents Page

To remove the JVMD Agents (that are deployed on monitored WebLogic domains) using the Engines And Agents page, perform the following steps:

1. From the **Setup** menu, select **Middleware Management,** then select **Engines And Agents.**
2. On the Engines And Agents page, click **Manage JVMD Agents.**

   > **Note:**
   >
   > If no active JVMD Engines are present and no JVMD Agents are deployed, the **Manage JVMD 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, and so on of all the Managed Servers on which JVMD 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 EMAgent Target Host Credentials** and **Oracle WebLogic Domain Credentials** (corresponding to the Admin server target), and then click **Apply.**

   > **Note:**
   >
   > In case host and domain preferred credentials are already set for the Admin server target, they are automatically applied to the domain, and it is not required to click **Apply**.

   Oracle EMAgent Target Host Credentials are the login credentials for the host on which the Management Agent, that is used to discover the WebLogic domain's Admin Server, is

running. Oracle WebLogic Domain Credentials are the credentials for the Administration Server of the selected WebLogic domain.

To set the preferred credentials for a WebLogic domain's Admin server (that is, the preferred EMAgent target host credentials and the preferred Oracle WebLogic Domain credentials), from the **Setup** menu, select **Security,** then select **Preferred Credentials.** Select the **Oracle Admin Server** target type, then click **Manage Preferred Credentials.** In the Target Preferred Credentials section, set the preferred host credentials and the preferred WebLogic administrator credentials for the required WebLogic Admin server.

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, if 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 information. In this case, you may need to provide additional information in the Advanced Domain 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 must provide the virtual host IP address for **Administration server host.**

   Click **Next.**

6. On the Review page, review all the information, and then click **Remove.**

> **Note:**
>
> To deploy an agent after you have removed it, you must restart JVM before deploying the agent.

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 relevant JVMD Agent application `(javadiagnosticagent)`.

> **Note:**
>
> The JVMD agent can be deployed in 2 ways:
>
> - Using bulk deployment job on Weblogic domain manager servers. In this case, the application is referred as javadiagnosticagent.
> - Manually downloading agent and deploying to a server. In this case, the application is referred as jamagent.

4. From the **Stop** menu, select **Force Stop Now.**
5. After the applications are stopped, select the same applications, then click **Delete.**
6. Log in to Enterprise Manager.

7. From the **Targets** menu, select **Middleware**.
8. 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.**

> **Note:**
>
> To deploy an agent after you have removed it, you must restart JVM before deploying the agent.

31

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

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:

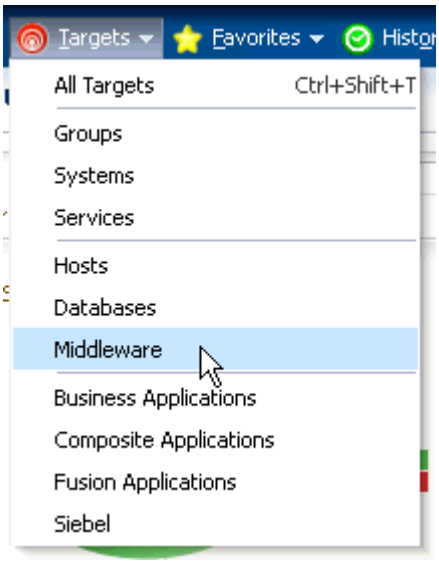
   ```
   $<OMS_HOME>/bin/omsca delete -OMSNAME <oms_name>
   ```

   When prompted, enter the repository login credentials.

   > **Note:**
   >
   > Run this command on each of the additional standby OMS instances.

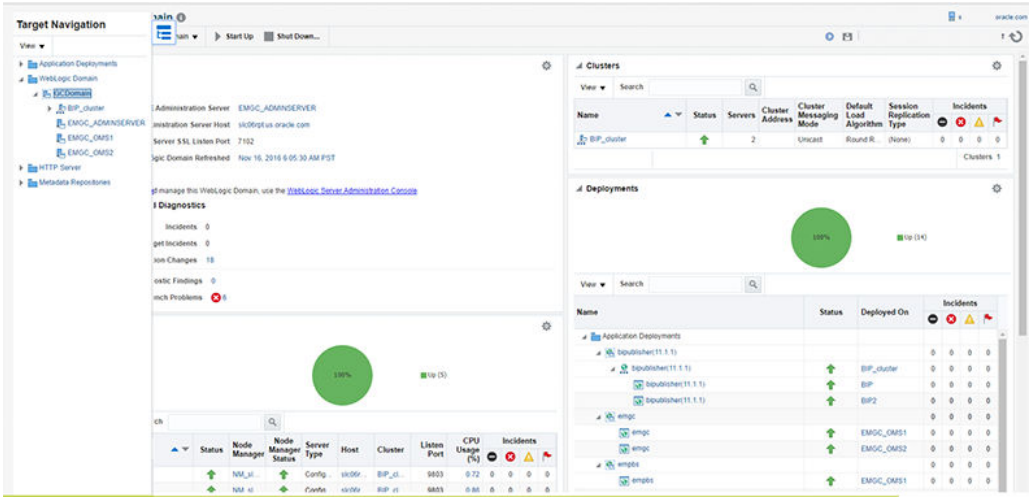
2. From the Enterprise Manager console, refresh the Weblogic domain.
   a. From the **Targets** menu, select **Middleware**.

Figure 31-1 Middleware Menu



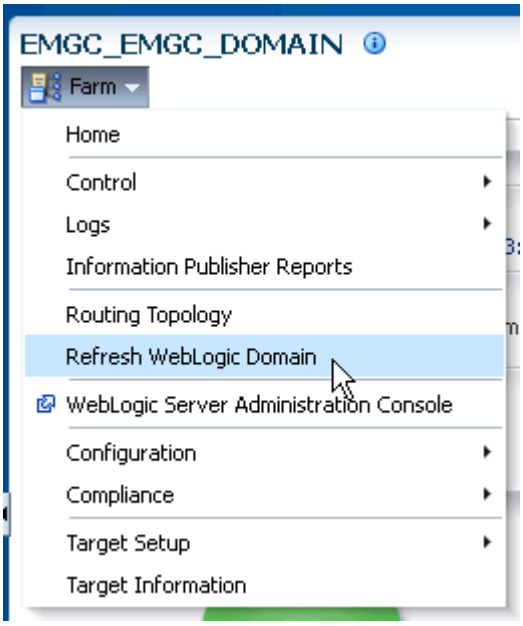
b. Click the **WebLogic Domain** you want to refresh. The domain home page displays.

Figure 31-2 Domain Home Page



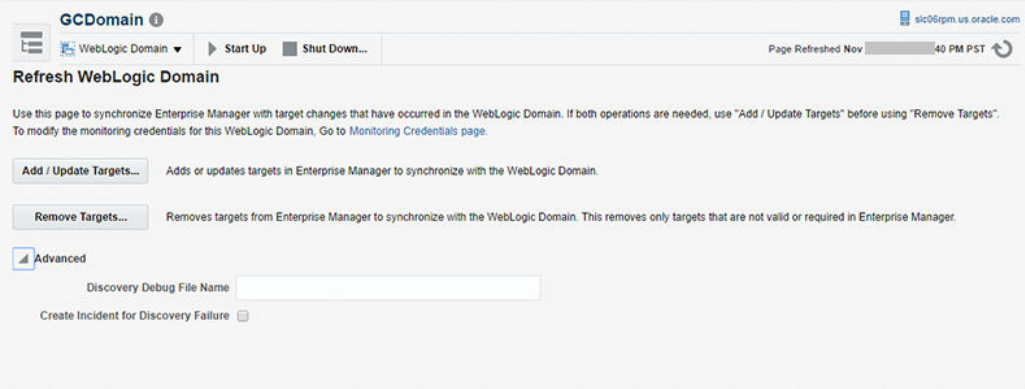
c. From either the **Farm** or **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

Figure 31-3 Refresh WebLogic Domain



Enterprise Manager displays available **Refresh WebLogic Domain** options.

Figure 31-4 Refresh WebLogic Domain



d. Click **Add/Update Targets** on the **Refresh Weblogic Domain** page. 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. Enterprise Manager will search the domain for new and modified targets.

3. Delete the OMS target associated with the OMS.

   a. From the **Target Navigation** area, click the target associated with the additional standby OMS you deconfigured earlier.

   b. 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.

Removing the First Standby OMS

To remove the first standby OMS, follow these steps:

> **Note:**
>
> 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" 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.
   a. From the **Target Navigation** area, click the target associated with the first standby OMS you deconfigured earlier.
   b. 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 IX
Appendixes

This part contains the following appendixes:

A

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 components.

In particular, this appendix covers the following:

- Enterprise Manager Installation Logs
- Add Host Log Files
- Manual Management Agent Installation Logs
- Agent Gold Image Log Files
- Additional OMS Installation Logs

Enterprise Manager Installation Logs

This section describes the following log files that are created while installing Enterprise Manager:

- Installation Logs
- Configuration Logs

Installation Logs

The following are the installation logs, which provide complete information on the installation status:

- `<ORACLE_INVENTORY_HOME>/logs/install<timestamp>.log`
- `<ORACLE_HOME>/cfgtoollogs/oui/install<timestamp>.log`

> **Note:**
>
> The `install` 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.

Configuration Logs

This section describes the following configuration logs:

- General Configuration Logs
- Repository Configuration Logs
- Secure Logs

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 A-1 lists the configuration logs for different installation types.

Table A-1 General Configuration Logs

Installation Type	Location
Install a new or Upgrade Enterprise Manager system	• `<ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger<timestamp>.log` • `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log` **Note:** `<ORACLE_HOME>` refers to the Oracle home of the OMS.
Add an additional Management Service	• `<ORACLE_HOME>/cfgtoollogs/omsca/logs/omsca<timestamp.log>` • `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.oms.<timestamp>.log` **Note:** `<ORACLE_HOME>` refers to the Oracle home of the OMS.
Install Oracle Management Agent	• `<ORACLE_HOME>/cfgtoollogs/cfgfw/CfmLogger` • `<ORACLE_HOME>/cfgtoollogs/cfgfw/oracle.sysman.top.agent.<timestamp>.log` **Note:** `<ORACLE_HOME>` refers to the Oracle home of the Management Agent.

Repository Configuration Logs

This section describes the following repository configuration logs:

- SYSMAN Schema Operation Logs
- MDS Schema Operation Logs

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 09/29/2023 12:50PM, then the following subdirectory is created.

```
$<ORACLE_HOME>/sysman/log/schemananager/m_092923_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 09/29/2023 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_092923_1250_PM/m_092923_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_030223_0349_AM
            m_030223_0325_AM.TRANSX
                emrep_config.log
                emschema.log.TRANSX
        m_030223_0438_AM
            m_030223_0438_AM.DROP (Same structure for Drop and Dropall actions)
                rcu.log
                emschema.log.DROP
                em_repos_drop.log
        m_030223_0450_AM
            m_030223_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_030223_1006_PM
            m_030223_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_030223_1021_PM
            m_030223_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_030223_1100_PM
                m_030223_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_030223_1125_PM
                m_030223_1125_PM.MY_ORACLE_SUPPORT
                    emschema.log.MY_ORACLE_SUPPORTm_030223_1135_PM
m_030223_1135_PM.PLUGINPURGE                emschema.log.PLUGINPURGE
em_repos_pluginpurge.logrcu.log
```

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`

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/oms24/mds.log` and `/scratch/OracleHomes/oms24/emmdsdrop_<timestamp>.log`.

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
```

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
```

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

Initialization Logs

Table A-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 A-2 Initialization Logs

Log File	Location
<hostname>_deploy.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/applogs

Application Prerequisite Logs

Table A-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 A-4.

Table A-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 A-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

System Prerequisite Logs

Table A-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 A-5 System Prerequisite Logs

Log File	Location
prereqchecker<time_stamp>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
launcher<time_stamp>.log	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
oraInstall<time_stamp>.out	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/

Table A-5 (Cont.) System Prerequisite Logs

Log File	Location
oraInstall<time_stamp>.err	<OMS_INSTANCE_HOME>/sysman/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/

Agent Installation Logs

Table A-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 A-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

Other Add Host Logs

Table A-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 A-7 Other Add Host Logs

Logs	Location	Description
EMAgentPushLogger<TIMESTAMP>.log.0	<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.

Manual Management Agent Installation Logs

Table A-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>/24.1.0.0.0/.

Table A-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
cloneActions<TIMESTAMP>.log	<ORACLE_HOME>/cfgtoollogs/agentDeploy/	Clone action logs

Agent Gold Image Log Files

Table A-9 lists the log files that need to be scrutinised for a failure of Gold Image creation process.

Table A-9 Agent Gold Image Creation Failure Logs

Logs	Location	Description
Output log.	From the Enterprise Manger home page click **Setup** and select **Manage Enterprise Manager** and then click **Agent Gold Images.** On the Agent Gold Images page click on **Show all activities** link to see all the jobs. Click on the job name to see the job result and the output logs.	Output logs for the agent gold image job run.
GoldAgentImageLogger<timestamp>.log	<OMS_INSTANCE_HOME>/EMGC_OMS1/sysman/goldagentimage/logs/	OMS side logs.
goldimagecreate<timestamp>.log	<AGENT_INSTANCE_HOME>/install/<TIMESTAMP>/	Agent side logs.

Table A-10 lists the log files that need to be scrutinised for Agent update failure.

Table A-10 Agent Update Failure Logs

Logs	Location	Description
agentDeploy<timestamp>.log	<New oracle home>/cfgtoollogs/agentDeploy/ **Note:** If the <New oracle home>/cfgtoollogs/agentDeploy/ location is not editable, the logs are created in <AGENT_INSTANCE_HOME>/install/logs/ folder.	Agent deploy logs.
All log files.	<AGENT_INSTANCE_HOME>/sysman/logs	Additional information logs.
All log files.	<OMS_INSTANCE_HOME>/EMGC_OMS1/sysman/logs	OMS side exception logs.

Table A-10 (Cont.) Agent Update Failure Logs

Logs	Location	Description
All log files.	`user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/logs/`	Server side logs.

Additional OMS Installation Logs

Table A-11 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 A-11 Additional OMS Installation Logs

Logs	Location
omsca failure	`$ORACLE_HOME/cfgtoollogs/omsca`
Plug-in failure	`$ORACLE_HOME/cfgtoollogs/pluginca`
Managed server logs • emLogs (emoms logs) • msLogs (Managed server logs, if server fails to start) • nmLogs	`$ORACLE_HOME/cfgtoollogs/omsca/log_<timestamp>/`
Admin logs	`$INSTANCE_HOME/user_projects/domains/GCDomain/servers/EMGC_ADMINSERVER/logs` (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`

B

Redirecting Oracle Management Agent to Another Oracle Management Service

This appendix explains how to redirect or repoint your Oracle Management Agent (Management Agent), which 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 deployment.

> **Note:**
>
> - Redirecting Management Agents to a different OMS that is part of a different Enterprise Manager deployment is supported only for Management Agents that were deployed afresh, 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 Enterprise Manager 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

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 Enterprise Manager,** 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 Enterprise Manager,** 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 *Accessing the Enterprise Manager Certification Matrix* in the *Oracle Enterprise Manager 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, see*Patching Oracle Management Service and the Repository* in the *Oracle Enterprise Manager 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.

Redirecting a Management Agent to Another OMS

To redirect or repoint a Management Agent, follow these steps:

1. Stop the Management Agent:

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

2. Delete the Management Agent target on the old OMS:

   ```
   $<ORACLE_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, see *delete_target* in the *Oracle Enterprise Manager Command Line Interface Guide.*

3. 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. Create a new instance home for the Management Agent and redirect it to the new OMS. To do so, run the `agentDeploy.sh` script (`agentDeploy.bat` for Microsoft Windows hosts) with the `-configOnly` option:

   ```
   $<AGENT_BASE_DIR>/agent_24.1.0.0.0/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>
   -configOnly
   ```

   For example,

   ```
   /scratch/emga/agt4agi/agent_24.1.0.0.0/sysman/install/agentDeploy.sh
   AGENT_BASE_DIR=/u01/software/em24/agentbasedir AGENT_INSTANCE_HOME=/u01/
   software/em24/agentbasedir/agent_inst AGENT_PORT=3880
   OMS_HOST=newoms.example.com EM_UPLOAD_PORT=4900
   AGENT_REGISTRATION_PASSWORD=<password> -configOnly
   ```

   For more information about the parameters you can specify while running `agentDeploy.sh` or `agentDeploy.bat`, refer Table 6-4. For more information about the `-configOnly` option, refer Table 6-7.

> **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.

C

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

Overview of the RepManager Utility

RepManager is a utility that enables you to upgrade and drop Oracle Management Repository (Management Repository), selectively purge plug-ins, and load dlf messages to Oracle Management Repository. This utility is available in the Oracle home of the Oracle Management Service (OMS) host.

For UNIX operating systems:

```
$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager
```

For Microsoft Windows operating systems:

```
$<ORACLE_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.

> **Note:**
>
> If you want to drop the Enterprise Manager schema completely, then use the RepManager available in the Oracle home of the OMS host. Do not use the one in the database home because it cannot remove the Enterprise Manager schema completely.

Actions and Commands Supported by the RepManager Utility

Table C-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 C-1 Actions and Commands Supported by RepManager

Action	Command	Description	Example

preupgrade	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action preupgrade <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"`	Use this action with the following parameters to perform the preupgrade steps before upgrading a Management Repository.
		• Specify the host, port, and SID to connect to the database where the Management Repository has to be upgraded.
		• Specify the database user (SYS) and password, the database role (SYSDBA), the repository name (SYSMAN) and password, and the Middleware home to upgrade the Management Repository. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured.
		• Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the `-pluginDepList` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list:
		`$<ORACLE_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList`
		• 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.
		• Specify a comma-separated locations for DLF files from platform/plug-ins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plug-ins. 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:
		`$<ORACLE_HOME>/sysman/admin/emdrep/plugininfo/dlfSources`
		If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.
			`$<ORACLE_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 C-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example

upgrade	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action upgrade <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>]-pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -runAsReposUser <TRUE/FALSE> -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"`
	Note: Run preupgrade before performing upgrade action.
		Use this action with the following parameters to upgrade a Management Repository.
		• Specify the host, port, and SID to connect to the database where the Management Repository has to be upgraded.
		• Specify the database user (SYS) and password, the database role (SYSDBA), the repository name (SYSMAN) and password, and the Middleware home to upgrade the Management Repository. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured.
		• Specify a comma-separated list of plug-ins to be deployed according to the dependency. You can pass a file with this option, the contents being a comma-separated list of plug-in IDs. If the `-pluginDepList` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the plug-in dependency list:
		`$<ORACLE_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList`
		• 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
		• Specify a comma-separated locations for DLF files from platform/plug-ins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plug-ins. 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:
		`$<ORACLE_HOME>/sysman/admin/emdrep/plugininfo/dlfSources`
		If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.
			`$<RACLE_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 C-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
transX	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action transx <repository_database_host> <repository_database_port> <repository_database_sid> -reposName sysman [-mwHome <Middleware home>] -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"` **Note:** You can also run `-doTransX`. By default, it is set to true. If you set the value to false, no translation bundles are loaded. This is applicable for `-dlfSources` for preupgrade and upgrade actions.	Use this action with the following parameters to load the translation resources to the Management Repository. • Specify the host, port, and SID to connect to the database and load the translation resources to the Management Repository. • Specify the repository name (SYSMAN) and password, and the Middleware home to load translation resources to Oracle Management Repository. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured. • Specify a comma-separated locations for DLF files from platform/plug-ins. You can pass a file with this option, the contents being comma-separated locations for DLF files from platform/plug-ins. If the `-dlfSources` parameter is not set, or is left with an empty list (for example, "{}"), then the following is read, by default, to retrieve the dlf resource locations: `$<ORACLE_HOME>/sysman/admin/emdrep/plugininfo/dlfSources` 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.	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action transx example.com 1521 db3 -reposName sysman -mwHome /scratch/WLS/middleware`

Table C-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
resume	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -resume retry <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] -checkpointLocation <directory where schemamanager stores checkpoints>`	Use this action with the following parameters to resume the last failed action, for example, the upgrade action. • Specify the host, port, and SID to connect to the database where the action has to be resumed. • Specify the database user (SYS) and password, the database role (SYSDBA), the repository name (SYSMAN) and password for the SYSMAN user, and the Middleware home where the action has to be resumed. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured. • Specify the location at which to resume the step. The checkpoint location is `$<ORACLE_HOME>/sysman/log/schemamanager`.	`$<ORACLE_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 C-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example

drop	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action drop <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman [-mwHome <Middleware home>] [-mwOraHome <Oracle Home>]`
	OR
	`$<ORACLE_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>]`
	Ensure that there are no active sessions, scheduler jobs, and dbms_jobs running for SYSMAN, SYSMAN_MDS SYSMAN122130_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.
		Use this action with the following parameters to remove all the Enterprise Manager repository schemas.
		• Specify the host, port, and SID to connect to the database in which all the schemas have to be dropped.
		• Specify the database user (SYS) and password, the database role (SYSDBA), the repository name (SYSMAN) and password, and the Middleware home. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured.
		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.
		For example,
		`SYSMAN_OPSS schema is not cleaned. EM_X synonyms are not dropped.`
			`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action drop -mwHome /scratch/weblogic/middleware`
			OR
			`$<ORACLE_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 C-1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
`plugin purge`	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager -action pluginpurge <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -pluginPurgeList "<plugin_name>=<plugin_location>" [-mwHome <Middleware home>] -mwOraHome <Oracle Home>` **Note:** To purge multiple plug-ins, for the `-pluginPurgeList` argument, enter the plug-ins separated by a command. For example, `<pluginid1>=<pluginid1 home>, <pluginid2>=<pluginid2 home>`	Use this action with the following parameters to deinstall a plug-in from the Management Repository. • Specify the host, port, and SID to connect to the database from which the plug-in has to be deinstalled. • Specify the database user (SYS) and password, the database role (SYSDBA), the repository name (SYSMAN) and password, and the Middleware home. Here, Middleware home is the Oracle home where the WebLogic Server, OMS, and other components are configured • Specify a comma-separated list of plug-ins to be purged from Enterprise Manager Repository with EM-EXT model.	`$<ORACLE_HOME>/sysman/admin/emdrep/bin/RepManager example.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action pluginpurge -pluginPurgeList "oracle.sysman.myyempwpax.oms.plugin_24.1.0.0.0=/scratch/weblogic/middleware/plugins/oracle.sysman.myyempwpax.oms.plugin_24.1.0.0.0" -mwHome /scratch/weblogic/middleware`

Note:

For information on the support for `-action drop` and `-action dropall` commands, see Table 2-5.

Note:

If you do not specify passwords during RepManager actions, you will be prompted to do so.

D

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 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

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, 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

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.
   - For Oracle Enterprise Manager Cloud Control 13*c* and later, OCM is located in the following directory:

     ```
     OMS_HOME/oracle_common
     ```

   - For Oracle Enterprise Manager Cloud Control 12*c* and earlier:

     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
     ```

     Set the environment variable `ORACLE_CONFIG_HOME` to the directory of this `emgc.properties` file. (**Note:** this setting is not required for Cloud Control 13*c*.)

     For example:

```
$export ORACLE_CONFIG_HOME=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1
```

2. 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*.

Or visit the OCM documentation library:

http://docs.oracle.com/cd/E49269_01/index.htm

Support For Enterprise Manager

By default, all targets are uploaded using the credentials used to register Oracle Configuration Manager in the OMS Home. In Enterprise Manager, 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.
   ```

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.

> **Note:**
>
> A Super Administrator can assign a CSI for any Oracle Home. Administrators can assign CSIs to Oracle Homes for which they have operator privilege on all the targets.

Refer to the help in the Enterprise Manager interface on how to access this information.

There are a number of areas in the Enterprise Manager UI where you can view CSIs.

- Oracle Home target home page.
  1. From the Enterprise Manager home page, select **Targets**, then select a target.
  2. In the Refine Search area, select **Other**, then select the Oracle Home of choice.
  3. On the Oracle Home target page, select Target Information in the target's drop down menu.
- Another way is by adding a CSI to a search.
  1. From the Enterprise Manager home page, select Targets, then select Add CSI to Configuration Search criteria; Add Properties

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

Harvester Job Status Metric

Starting 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.

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 D-1 are collected by Oracle Harvester.

Table D-1 Supported Targets in Enterprise Manager 12.1 Releases

Target	Plug-in Release	Enterprise Manager 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

Table D-1 (Cont.) Supported Targets in Enterprise Manager 12.1 Releases

Target	Plug-in Release	Enterprise Manager Release		
		12.1.0.1	12.1.0.2	12.1.0.3
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

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 beginning with Enterprise Manager 12*c*. Configuration data for targets collected from Oracle Harvester running in Enterprise Manager release 12*c* and later displays in My Oracle Support immediately, regardless of how recently data was uploaded by a standalone OCM Collector.

Leveraging the Enterprise Manager Infrastructure

A full deployment of Enterprise Manager includes the following components:

1. One or more Oracle Management Service (OMS) instances
2. An Oracle database used as the Management Repository
3. Management Agents deployed onto each host containing targets to be managed by Enterprise Manager

On a regular basis, configuration data is collected by Management Agents for targets managed by Enterprise Manager and uploaded to the OMS; the data is stored in the Enterprise Manager Repository.

Enterprise Manager extracts, or harvests, the collected configuration data from the Enterprise Manager repository for the purpose of conveying that data to Oracle. Once harvested, the configuration data is automatically uploaded to My Oracle Support by way a recurring Enterprise Manager job, generating system configuration information in My Oracle Support just as if it were uploaded from OCM instances.

Note that this also carries the advantage of simpler software deployment. The pure OCM model requires one instance of the OCM software in every Oracle Home. The Enterprise Manager infrastructure, on the other hand, requires one Management Agent on each host, thus potentially requiring many fewer deployments.

Configuring Enterprise Manager to Upload Configuration Data to Oracle

The only prerequisites for using Enterprise Manager to collect and upload configuration data to Oracle Support are that the Enterprise Manager OMS must be at least version 10.2.0.5, and there must be an OCM instance configured (and running in connected mode) in the Oracle Home of the OMS.

If multiple OMS instances are used for the Enterprise Manager infrastructure, then each OMS must have OCM configured and running. OCM is easily set up as part of the 10.2.0.5 patchset installation; alternatively OCM can be configured later from the command line. For more information, see the *Oracle Configuration Manager Installation and Administration Guide.* Once OCM is configured in the OMS home, Enterprise Manager-collected configuration upload to Oracle is enabled.

> **Note:**
>
> The Oracle Home of the OMS is the only place in which an OCM instance is needed (not on any managed targets).

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.

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.

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`
- Ops Center Harvester error log is located at:

  `/var/opt/sun/xvm/logs/ocharvester.log`
- 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

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)

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.

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`

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)

E

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 and individuals with disabilities in general.

Enterprise Manager provides support for Screen Reader. Also, you can navigate through the Enterprise Manager console with a keyboard alone – using common keyboard commands.

This appendix covers the following topics:

- Enabling Screen Reader Mode
- Verifying Screen Reader Support Is Enabled
- Enterprise Manager Keyboard Navigation

> **Note:**
>
> If Screen Reader support is enabled, then all pages related to *Refresh Process Status* are not refreshed automatically because Partial Page Rendering (PPR) is turned off. This is an expected behavior.

Enabling Screen Reader Mode

There are numerous pages of monitoring and management data in the Enterprise Manager console. Different technologies are used for implementing these pages – for example, many pages rely upon Oracle Application Development Framework (ADF), while others depend upon User Interface XML (UIX). These underlying technologies require different setup for enabling screen reader mode. Pages implemented with ADF work in screen reader by default. No further action is required. However, pages implemented with UIX require additional steps to be screen reader enabled.

Enabling Screen Reader Mode for UIX Pages

UI implemented in UIX needs additional manual configuration for screen reader mode.

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 an Enterprise Manager 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
   ```

> **Note:**
>
> If you have multiple OMS, you need to perform the steps individually for each OMS.

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>
```

> **Note:**
>
> <accessibility-mode>- The accessibility-mode element defines what level of accessibility support should be generated. Acceptable values are default and inaccessible, which turns off accessibility features. This improves the page size and screenReader, which enhances the accessibility to optimize usability with screen readers, but might degrade the appearance in standard browsers.

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`.

Enabling Text Descriptions for Charts for UIX Pages

Throughout the Enterprise Manager console, 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 configure web.xml file, follow these steps:

1. Locate the `web.xml` configuration file.

To locate the `web.xml` file in an Enterprise Manager 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
```

> **Note:**
>
> If you have multiple OMS, you need to perform the steps individually for each OMS.

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.

Verifying Screen Reader Support Is Enabled

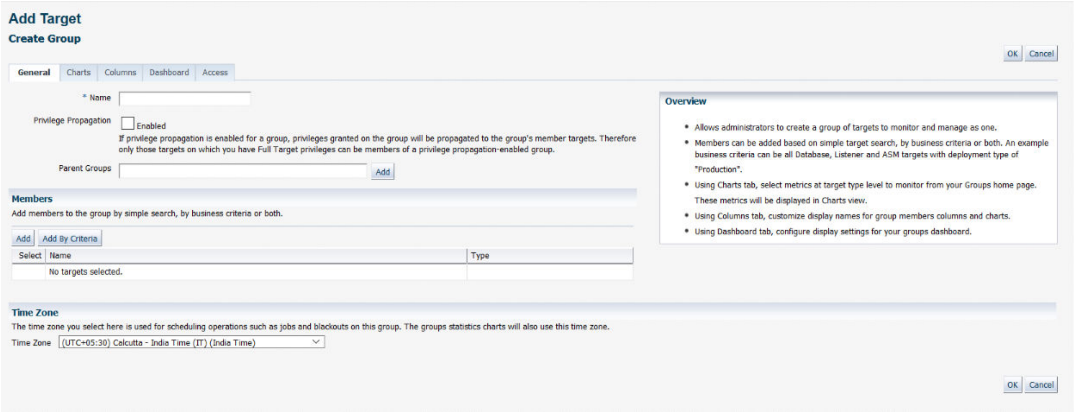
To verify if the Screen Reader support is enabled for ADF pages, follow these steps:

1. On the Enterprise Manager home page, from the **<user_name>** menu, 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:

- On the Enterprise Manager home page, from the **Setup** menu, select **Add Target** and then select **Groups**.

  The **Add Target** page is displayed.



Enterprise Manager Keyboard Navigation

You can navigate the Enterprise Manager console without a mouse and access all relevant functionality using only the keyboard. You don't need screen reader mode or any other assistive technology to use keyboard-only navigation, which is available to all users.

Generally, you use the following keys to navigate:

- Tab key: Move to the next control, such as a dynamic target menu, navigation tree, content pane, or tab in a page. Tab traverses the page left to right, top to bottom. Use Shift +Tab to move to the previous control.
- Up and Down Arrow keys: Move to the previous or next item in the navigation tree, menu, or table. Down Arrow also opens a menu.
- Left and Right Arrow keys: Collapse and expand an item in the navigation tree or a submenu.
- Esc: Close a menu.
- Spacebar: Activate a control. For example, in a check box, spacebar toggles the state, checking or unchecking the box. On a link, spacebar navigates to the target of the link.
- Enter: Activate a button.

Table E-1 shows some common tasks and the keyboard navigation used.

Table E-1 Keyboard Navigation for Common Tasks

Task	Navigation
Move to next control, such as navigation tree or menu	Tab
Move to previous control, such as navigation tree or menu	Shift+Tab
Move to navigation pane	Tab until navigation tree has input focus
Move down the navigation tree	Down Arrow
Move up the navigation tree	Up Arrow
Expand a folder	Right Arrow
Collapse a folder	Left Arrow
Open a menu	Down Arrow
Move to the next item in a menu	Down Arrow

Table E-1 (Cont.) Keyboard Navigation for Common Tasks

Task	Navigation
Move to the previous item in a menu	Up Arrow
Select a menu item	Enter
Open a submenu	Right Arrow
Close a submenu	Left Arrow
Move out of a menu	Esc
Activate a button	Enter
Open a tab in a content pane	Tab to the content pane, Tab to the tab to get input focus, then Enter to select the tab
Select an item, such as Message type in Log Messages screen	Spacebar
Select a row in a table	Tab to the header of the table, then Down Arrow to move to a row
Select a cell in a table	Tab to the header of the table, then Tab until you reach the cell you want to select, then Enter

Keyboard Shortcuts

Keyboard shortcuts enable you to perform user interface actions without using a mouse. Keyboard shortcuts for specific UI elements come from the Oracle Application Development Framework components that they are based on. You might also find keyboard shortcuts that are specific to a particular feature or product.

Keyboard Shortcuts for Oracle Application Development Framework Components

Enterprise Manager is based on some Oracle Application Development Framework (ADF) components which come with standard keyboard shortcuts. In some cases, you might find different keyboard shortcuts specific to the page, feature or product that you are using. Oracle ADF keyboard shortcuts are described in the Oracle Fusion Middleware Developing Web User Interfaces with Oracle Application Development Framework Faces.

Default Mode

- Refer to the following sections in the guide for the corresponding keyboard shortcuts.

  See: Keyboard Shortcuts

  - Shortcut Keys for Common Components
  - Shortcut Keys for Widgets
  - Shortcut Keys for Rich Text Editor Component
  - Shortcut Keys for Table, Tree, and Tree Table Components
  - Shortcut Keys for ADF Data Visualization Components
  - Shortcut Keys for Calendar Component

Screen Reader Mode

The keyboard shortcuts for some components in screen reader mode are different from the shortcuts in default mode.

- Refer to the following sections in the guide for the corresponding keyboard shortcuts.

  See: Keyboard Shortcuts

  - Shortcut Keys for Table, Tree, and Tree Table Components in Screen Reader Mode
  - Shortcut Keys for ADF Data Visualization Components in Screen Reader Mode
  - Shortcut Keys for Calendar Component in Screen Reader Mode

Keyboard Shortcuts for Oracle JavaScript Extension Toolkit (JET) Components

Enterprise Manager is based on some Oracle Java Script Extension Toolkit (JET) components which come with standard keyboard shortcuts. Oracle JET keyboard shortcuts are described in the Oracle JavaScript Extension Toolkit (JET) Keyboard and Touch Reference.

Enterprise Manager Performance Hub uses the following Oracle JET components:

- oj-accordion
- oj-button
- oj-buttonset-many
- oj-buttonset-one
- oj-chart
- oj-checkboxset
- oj-collapsible
- oj-data-grid
- oj-diagram
- oj-dialog
- oj-input-date
- oj-input-date-time
- oj-input-number
- oj-input-text
- oj-input-time
- oj-label
- oj-legend
- oj-list-view
- oj-masonry-layout
- oj-menu
- oj-menu-button
- oj-navigation-list
- oj-paging-control
- oj-popup

- oj-progress
- oj-radioset
- oj-row-expander
- oj-slider
- oj-status-meter-gauge
- oj-tab-bar
- oj-table
- oj-text-area
- oj-toolbar
- oj-treemap

F

Configuring Targets for Failover in Active/Passive Environments

This section provides a general reference for Enterprise Manager 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

With Oracle Enterprise Manager 24ai, 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 Guide* 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.

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

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 Enterprise Manager 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.

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

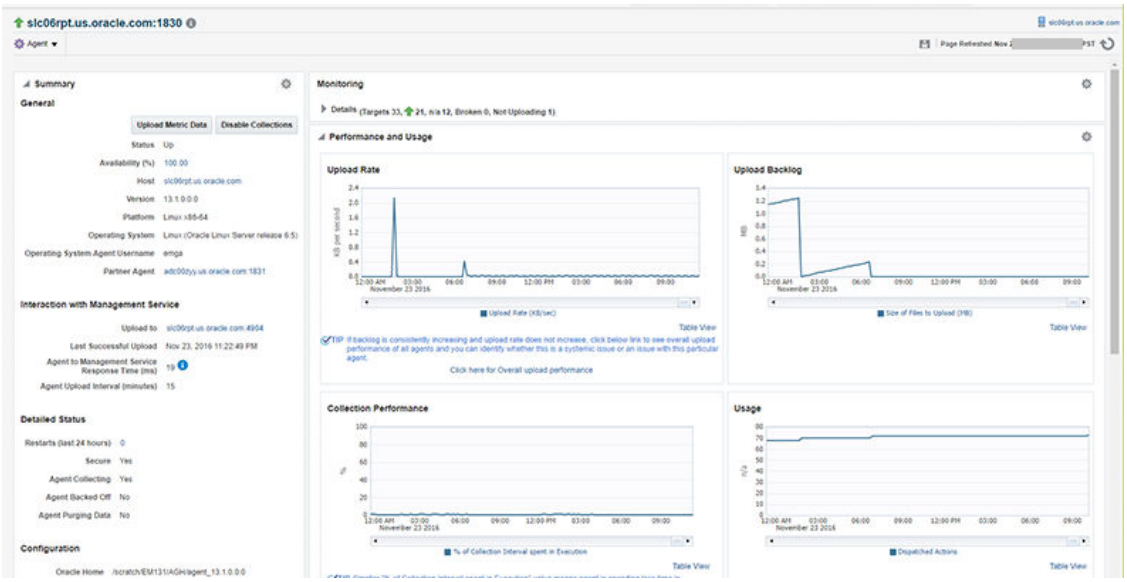
Discovering Targets

After the Active / Passive targets have been configured, use the Add Targets Manually screens in the Enterprise Manager 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).

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 F-1 Agent Home Page



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.

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" 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 Enterprise Manager 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 .

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" to return the HA targets to the active node.
2. Verify the target status in the Enterprise Manager console.

EM CLI relocate_targets Parameters

As shown in 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 F-1 documents the verb parameters associated with this EM CLI verb.

Table F-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 F-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.

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*.

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
```

G

Updating Demonstration Keystores to Reflect Alias Hostnames

If you are using demonstration WebLogic certificates, and if you have implemented alias hostnames as part of preparation for implementing Standby OMSs using the Storage Replication DR architecture, the demonstration identity certificates configured for WebLogic Server need to be recreated on each OMS to have the alias hostname for the OMS, instead of the physical hostname of the server. These steps need to be implemented after installations and upgrades. These steps involve downtime as the OMS must be restarted. To maintain availability, these steps should be performed serially, first on OMS1 and then one by one on additional OMSs so that other OMSs remain online while only one OMS is being updated at a time.

Perform the following steps serially, first on OMS1 and then on each additional OMS:

1. Backup existing `DemoIdentity.jks` file.

   ```
   cp -p <NEW_INSTANCE_BASE>/user_projects/domains/GCDomain/security/
   DemoIdentity.jks <NEW_INSTANCE_BASE>/user_projects/domains/GCDomain/security/
   DemoIdentity.jks.before_regen_YYYYMMDD
   ```

   For example:

   ```
   cp -p /u01/app/oracle/OMS/gc_inst/user_projects/domains/GCDomain/security/
   DemoIdentity.jks /u01/app/oracle/OMS/gc_inst/user_projects/domains/GCDomain/
   security/DemoIdentity.jks.before_regen_20160402
   ```

2. Backup existing `DemoTrust.jks` file.

   ```
   cp -p <NEW_MIDDLEWARE_HOME>/oms_home/wlserver/server/lib/DemoTrust.jks
   <NEW_MIDDLEWARE_HOME>/oms_home/wlserver/server/lib/
   DemoTrust.jks.before_regen_YYYYMMDD
   ```

   For example:

   ```
   cp -p /u01/app/oracle/OMS/MWare24/oms_home/wlserver/server/lib/
   DemoTrust.jks /u01/app/oracle/OMS/MWare24/oms_home/wlserver/server/lib/
   DemoTrust.jks.before_regen_20160402
   ```

3. Run the following commands in a separate session to prevent the environment variable settings required to run these steps from affecting other commands. These environment variable settings can cause issues to the standard OMS operations and the other instructions in this upgrade and transition process.

   a. Open a new shell session as the Oracle Software Owner User.

   b. Set the necessary environment variables.

      i. Change directory to the bin directory for the domain.

         ```
         cd <NEW_INSTANCE_BASE>/user_projects/domains/GCDomain/bin
         ```

         For example:

         ```
         cd /u01/app/oracle/OMS/gc_inst/user_projects/domains/GCDomain/bin
         ```

ii. Source the script to set environment variables. Make sure you source the contents of the script using the exact syntax below including the leading dot and space. `. ./setDomainEnv.sh`

c. Create a new keystores directory to use while generating these files.

```
mkdir -p <NEW_MIDDLEWARE_HOME>/oms_home/keystores
```

For example:

```
mkdir -p /u01/app/oracle/OMS/MWare24/oms_home/keystores
```

d. Change directory to the new keystores directory.

```
cd <NEW_MIDDLEWARE_HOME>/oms_home/keystores
```

For example:

```
cd /u01/app/oracle/OMS/MWare24/oms_home/keystores
```

e. Generate the new certificate with the alias hostname for the OMS server. In the following command, replace `<OMS_ALIAS_HOSTNAME_FQDN>` with the value for `<OMS1_ALIAS_HOSTNAME_FQDN>` when running these commands on OMS1 and with the value for `<OMS<#>_ALIAS_HOSTNAME_FQDN>` when running these commands on OMS<#>.

```
java utils.CertGen -cn <OMS_ALIAS_HOSTNAME_FQDN> -keyfilepass
DemoIdentityPassPhrase -certfile democert -keyfile demokey
```

For example:

```
java utils.CertGen -cn emoms1.example.com -keyfilepass
DemoIdentityPassPhrase -certfile democert -keyfile demokey
```

f. Import the new certificate into a new `DemoIdentity.jks` file.

```
java utils.ImportPrivateKey -keystore DemoIdentity.jks -storepass
DemoIdentityKeyStorePassPhrase -keyfilepass DemoIdentityPassPhrase -
certfile democert.pem -keyfile demokey.pem -alias demoidentity
```

g. Confirm that the newly generated certificate in the keystore references the alias hostname FQDN of the OMS. When prompted for a password, hit enter as a password is not required to view contents of the keystore. Examine the value after `CN=` on the line that starts `Owner:` `keytool -list -v -keystore DemoIdentity.jks`

h. Delete the four interim files that are no longer needed, leaving just the new `DemoIdentity.jks` file in the current directory:

```
rm democert.*

rm demokey.*
```

i. Exit the separate shell session that was started to execute these commands.

4. Stop the OMS.

```
<NEW_MIDDLEWARE_HOME>/oms_home/bin/emctl stop oms -all
```

For example:

```
/u01/app/oracle/OMS/MWare24/oms_home/bin/emctl stop oms -all
```

5. Change directory to the new keystores directory.

```
cd <NEW_MIDDLEWARE_HOME>/oms_home/keystores
```

For example:

```
cd /u01/app/oracle/OMS/MWare24/oms_home/keystores
```

6. Replace the old DemoIdentity.jks file with the newly generated file. Note that we are explicitly NOT passing the -p parameter to cp here so that the target file retains its original permissions. Specifying -p here will cause the wrong permissions to be set on the target file.

   ```
   cp DemoIdentity.jks <NEW_INSTANCE_BASE>/user_projects/domains/GCDomain/
   security/
   ```

   For example:

   ```
   cp DemoIdentity.jks /u01/app/oracle/OMS/gc_inst/user_projects/domains/
   GCDomain/security/
   ```

7. Confirm that the `DemoIdentity.jks` file has been copied successfully.

   ```
   ls -alF <NEW_INSTANCE_BASE>/user_projects/domains/GCDomain/security/Demo*
   ```

   For example:

   ```
   ls -alF /u01/app/oracle/OMS/gc_inst/user_projects/domains/GCDomain/security/
   Demo*
   ```

8. Start the OMS.

   ```
   <NEW_MIDDLEWARE_HOME>/oms_home/bin/emctl start oms
   ```

   For example:

   ```
   /u01/app/oracle/OMS/MWare24/oms_home/bin/emctl start oms
   ```

9. Run the following commands in a separate session to prevent the environment variable settings required to run these steps from affecting other commands. These environment variable settings can cause issues to the standard OMS operations and the other instructions in this upgrade and transition process.

   a. Open a new shell session as the Oracle Software Owner User.

   b. Set necessary environment variables

      i. Change directory to the bin directory for WebLogic Home.

         ```
         cd <NEW_MIDDLEWARE_HOME>/oms_home/wlserver/server/bin
         ```

         For example:

         ```
         cd /u01/app/oracle/OMS/MWare24/oms_home/wlserver/server/bin
         ```

      ii. Source script to set the environment needed to run wlst. Make sure you source the contents of the script using the exact syntax below including the leading dot and space.

         ```
         . ./setWLSEnv.sh
         ```

   c. Change directory to prepare to run wlst.

      ```
      cd <NEW_MIDDLEWARE_HOME>/oms_home/oracle_common/common/bin
      ```

      For example:

      ```
      cd /u01/app/oracle/OMS/MWare24/oms_home/oracle_common/common/bin
      ```

   d. Launch wlst.

      ```
      java -Dweblogic.security.TrustKeyStore=DemoTrust -
      Dweblogic.security.SSL.minimumProtocolVersion=TLSv1 weblogic.WLST
      ```

   e. At this point you should be able to successfully connect to this OMS server via wlst specifying the alias hostname for this OMS server, and if you have already completed

these steps on the other OMS server(s) you should also be able to connect to the other OMS server(s).

f. Attempt to connect to the Admin server:

```
connect('<ADMIN_SERVER_USER>','<ADMIN_SERVER_PASSWORD>','t3s://
<OMS1_ALIAS_HOSTNAME_FQDN>:<ADMIN_SERVER_HTTPS_PORT>')
```

For example:

```
connect('weblogic','myadminpassword','t3s://emoms1.example.com:7101')
```

g. Attempt to connect to the OMS1 Managed Server.

```
connect('<ADMIN_SERVER_USER>','<ADMIN_SERVER_PASSWORD>','t3s://
<OMS1_ALIAS_HOSTNAME_FQDN>:<OMS_SERVER_HTTPS_PORT>')
```

For example:

```
connect('weblogic','myadminpassword','t3s://emoms1.example.com:7301')
```

h. Attempt to connect to the OMS<#> Managed Server (will fail until these steps are completed on OMS<#>. These connection tests can be repeated again once the process is complete on all OMS servers.

```
connect('<ADMIN_SERVER_USER>','<ADMIN_SERVER_PASSWORD>','t3s://
<OMS<#>_ALIAS_HOSTNAME_FQDN>:<OMS_SERVER_HTTPS_PORT>')
```

For example:

```
connect('weblogic','myadminpassword','t3s://emoms2.example.com:7301')
```

i. Exit wlst.

```
exit()
```

j. Exit the separate shell session that was started to execute these commands.

H

Postinstalltion Task to Configure TLS for Oracle Management Repository Database

To configure Oracle Management Repository (OMR) Database in Transport Layer Security that is, TLS 1.2, follow the steps in Configuring TLSv1.2 for Communication with the Enterprise Manager Repository in the *Enterprise Manager Security Guide.*

Index

Symbols

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V