Oracle® Enterprise Manager

Cloud Control Advanced Installation and Configuration Guide

12*c* Release 1 (12.1.0.1)

E24089-01

October 2011

ORACLE®

Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide, 12*c* Release 1 (12.1.0.1)

E24089-01

Primary Author: Aravind Jayaraaman

Contributing Author: Dan Hynes, Dennis Lee, Aparna Kamath, Namrata Bhakthavatsalam, Leo Cloutier, Jacqueline Gosselin,

Contributor: Anu Vale, Smitha Vishwanathan, Abhishek Suresh Kumar, Srilatha Uravakonda, Shilpa Thergaonkar, Palem Naga Maheshwara Reddy, Smitha Nath, Prakash Jaganathan, Ariram Kandasamy, Raj Aggarwal, Daniel Tsao, Maria Kaval, James Emmond, Anand Kurumbur, Leslie Gloyd, Raj Aggarwal, Ravi Pinnamaneni, Amitava Raha, Rajiv Kuriakose, Ashish Goel, Atif Jamil, Karthik Somasundaram, Devanand Patil, Sushma Vale, Abhishek Vaidya, Venkatesh BGS, Atif Jamil, Ashish Goel, Jing Ning, Akanksha Sheron, Bhavin Desai, David Eschliman, Glen Hawkins, James Kao, Andrew Gregory, Bhavin Desai, David Eschliman, Farouk Abushaban, Neelima Bawa, Courtney Llamas, Alvin Chyan, Suman Kumar Pramanik, Long Yang, Prasad Chebrolu, Bala Kuchibhotla, Daniel Tsao, Sanjay Ediga, Amitabh Khare, Mohammed Nazim, Rajesh Parasuraman, Maria Teresa Gil Lucientes.

Contents

11 Performing Additional Configuration Tasks

12 Configuring Enterprise Manager for Firewalls

13 Installing ADP with Advanced Installation Options

C Collecting OCM Data in Enterprise Manager and Ops Center Environments

D Troubleshooting

Index

Preface

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

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

This preface contains the following topics:

Intended Audience

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

Purpose of the Document

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

- Installing the following in graphical mode:
  - Enterprise Manager Cloud Control software only so that you can configure it later
  - Oracle Management Agent using a shared Oracle home
- Installing the following in silent mode:
  - Enterprise Manager Cloud Control
  - Enterprise Manager Cloud Control software only so that you can configure it later
  - Oracle Management Agent
  - Oracle Management Agent software only so that you can configure it later
  - Oracle Management Agent using a shared Oracle home
- Cloning Oracle Management Agent in graphical and silent mode
- Deinstalling Enterprise Manager Cloud Control and Oracle Management Agent in graphical and silent mode

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

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

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

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

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

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

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

Conventions

The following text conventions are used in this document:

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

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

1 Procuring Software

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

- Procuring Enterprise Manager Cloud Control Software
- Procuring Oracle Management Agent Software

1.1 Procuring Enterprise Manager Cloud Control Software

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

- How Do You Access the Software from DVD?
- How Do You Procure the Software from Oracle Technology Network?

1.1.1 How Do You Access the Software from DVD?

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

This section covers the following:

- Accessing Software from DVD
- Setting Mount Point for DVD

1.1.1.1 Accessing Software from DVD

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

If the software is available on multiple DVDs, then follow these steps:

1. Insert the first DVD into the DVD drive.
2. Copy the ZIP file from the DVD to a location on your local disk.
3. Insert the second DVD into the DVD drive.
4. Copy the ZIP file from the DVD to the same location on your local disk.
5. Extract the contents of both the ZIP files in the same location.
6. Run the Enterprise Manager Cloud Control Installation Wizard.

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

1.1.1.2 Setting Mount Point for 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 verify whether the disk mounts automatically and to manually mount the disk if it does not mount itself automatically, follow these steps:

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

   ```
   $ su -root
   ```

2. Insert the disk into the drive.

   Note: If required, enter the following command to eject the currently mounted disk and to remove it from the drive:

   ```
   # /usr/sbin/umount /<SD_DVD>
   ```

3. Enter the following command:

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

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

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

1.1.2 How Do You Procure the Software from Oracle Technology Network?

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

This section covers the following:

- Downloading Software
- Verifying File Size
- Extracting Contents
- Verifying Platform Information

1.1.2.1 Downloading Software

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

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

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

1.1.2.2 Verifying File Size

After downloading the ZIP files, run the `cksum` command against the files and check if the file checksum of the downloaded software is the same as the file checksum displayed on OTN.

The following is the format of the ZIP files:

em12_<platform>_diskNofM.zip (<value> bytes) (cksum - <value>)

Here, *<platform>* refers to the operating system, *N* refers to the ZIP file number, and *M* refers to the total number of ZIP files available for download. For example, em12_linux_disk1of2.zip, em12_linux_disk2of2.zip, em12_linux64_disk1of2.zip, or em12_linux64_disk2of2.zip.

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

```
$ cksum em12_<platform>_diskNofM.zip
```

For example,

```
$ cksum em12_linux_disk1of2.zip
```

1.1.2.3 Extracting Contents

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

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

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

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

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

1.1.2.4 Verifying Platform Information

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

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

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

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

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

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

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

Table 1–1 Verifying Platform Information

Platform Name	Platform Specified in ARU_ID_DESCRIPTION	32-bit / 64-bit
Linux x86	Linux x86	32-bit
Microsoft Windows (32-bit)	Win 32	32-bit
Microsoft Windows (64-bit AMD64)	win 64	64-bit
Microsoft Windows (64-bit IA)	Windows Itanium	64-bit
Solaris Operating System (SPARC 64-bit)	Solaris	64-bit

Table 1–1 (Cont.) Verifying Platform Information

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

1.2 Procuring Oracle Management Agent Software

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

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

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

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

For information on Self Update and how you can use it to download the software, see the chapter on Self Update in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

2

Understanding the Basics

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

In particular, this chapter covers the following:

- Understanding Installation Basics
- Understanding Oracle WebLogic Server Requirement
- Understanding Installation Directories
- Understanding Additional Components Installed
- Understanding Configuration Assistants
- Understanding Prerequisite Checks
- Understanding Limitations of Enterprise Manager Cloud Control
- Understanding Other Miscellaneous Concepts

2.1 Understanding Installation Basics

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

- What Different Installation Modes Can You Use?
- What Is Enterprise Manager Cloud Control Installation Wizard?
- What Installation Types Are Offered by the Installation Wizard?
- What Is Add Host Target Wizard?
- What Is 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 Data Files?

2.1.1 What Different Installation Modes Can You Use?

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

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

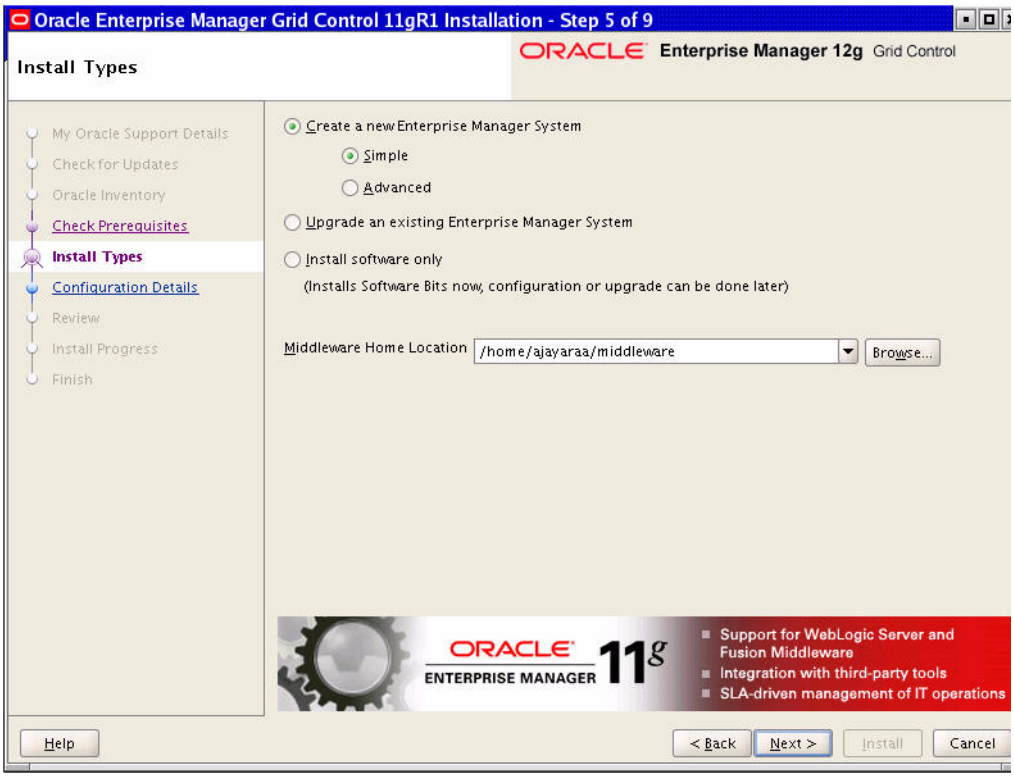
In both these modes, you can perform a *software-only* installation. A *Software-Only* installation is an approach that enables you to install only the software binaries of Enterprise Manager Cloud Control or a Management Agent, that is, without any configuration to the installation. This is best suited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

2.1.2 What Is Enterprise Manager Cloud Control Installation Wizard?

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

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

Figure 2–1 Enterprise Manager Cloud Control Installation Wizard



2.1.3 What Installation Types Are Offered by the Installation Wizard?

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

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

2.1.3.1 Create a New Enterprise Manager System

This installation type enables you to install a new Enterprise Manager Cloud Control system in one of the following ways:

- **Simple,** installs a new Enterprise Manager Cloud Control system quickly *with default configuration settings*, using an existing, certified Oracle Database to house the Management Repository.
- **Advanced,** installs a new Enterprise Manager Cloud Control system *with custom configuration settings*, using an existing, certified Oracle Database to house the Management Repository.

For both simple and advanced installation types, the installation wizard does the following:

- Installs Java Development Kit (JDK) 1.6 v24, Oracle WebLogic Server 11g Release 1 (10.3.5) if they do not already exist
- Installs Oracle JRF 11g Release (11.1.1.4.0), which includes `oracle_common` directory
- Installs Oracle Web Tier 11g Release (11.1.1.4.0), which includes `Oracle_WT` directory
- Installs Oracle Management Service 12*c* and Oracle Management Agent 12*c*
- Installs Oracle Management Plug-Ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In
- Creates an Oracle WebLogic domain called `GCDomain`, and a Node Manager user account called `nodemanager`
- Configures an Oracle Management Service Instance Base directory for storing all configuration details related to the OMS
- Configures the Management Repository (in the existing Oracle Database), the OMS, and the Management Agent

2.1.3.2 Upgrade an Existing Enterprise Manager System

This installation type enables you to upgrade an existing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) or Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0) to Enterprise Manager Cloud Control.

This installation type offers the following approaches:

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

- **Two System Upgrade,** enables you to install Enterprise Manager Cloud Control on a host that is different from the host where your existing Enterprise Manager system is running. This approach does not upgrade the Management Repository in the existing Oracle Database, but upgrades the one in the backed up database, thus offering the scope for two Enterprise Manager systems to exist. Since a new Enterprise Manager system coexists with the old one, there is *no* or *near zero* downtime involved.

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

2.1.3.3 Install Software Only

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

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

During the installation phase, the installation wizard does the following:

- Installs Java Development Kit (JDK) 1.6 v24, Oracle WebLogic Server 11g Release 1 (10.3.5) if they do not already exist.
- Installs Oracle JRF 11g Release (11.1.1.4.0), which includes `oracle_common` directory.
- Installs Oracle Web Tier 11g Release (11.1.1.4.0), which includes `Oracle_WT` directory.
- Installs Oracle Management Service 12*c* and Oracle Management Agent 12*c*.
- Installs Oracle Management Plug-Ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In.

During the configuration phase, the installation wizard does the following:

- Creates an Oracle WebLogic domain called `GCDomain`, and a Node Manager user account called `nodemanager`.
- Configures an Oracle Management Service Instance Base directory for storing all configuration details related to the OMS.
- Configures the Management Repository (in the existing Oracle Database), the OMS, and the Management Agent.

2.1.4 What Is Add Host Target Wizard?

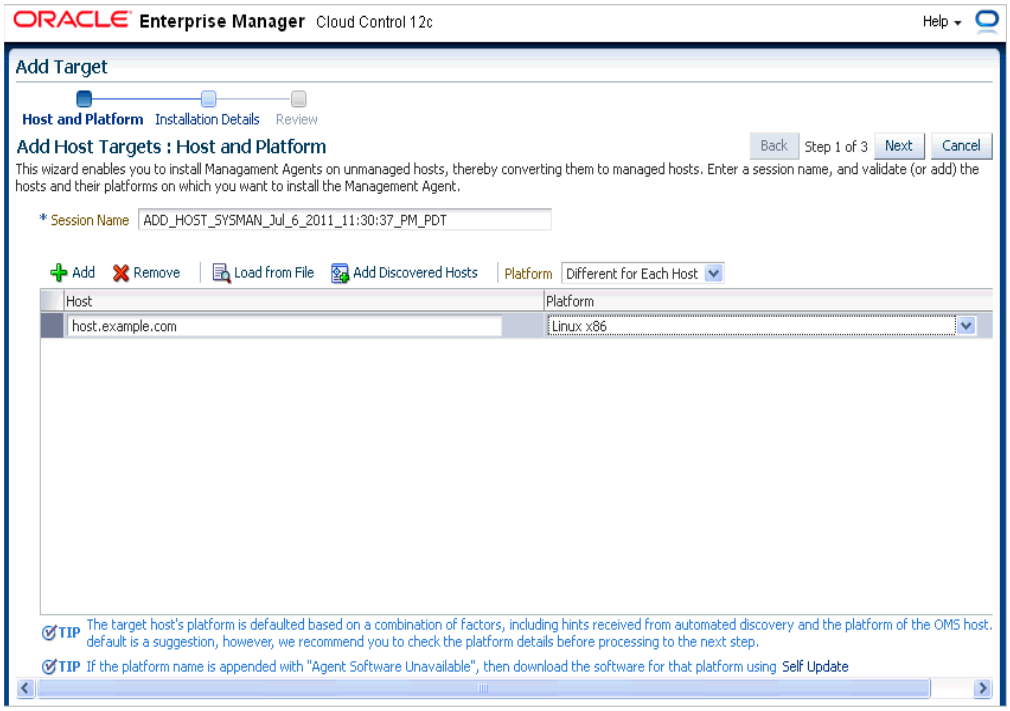
The Add Host Targets Wizard (Figure 2–2) is a GUI-rich application accessible from within the Cloud Control console, and used for installing Management Agents on unmanaged hosts and converting them to managed hosts in the Enterprise Manager system.

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

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

- Install a Management Agent from an existing, centrally shared Management Agent

Figure 2–2 Add Host Target Wizard



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 multiple hosts on which you want to install a Management Agent. This helps you when you want to install the Management Agent on several hosts, in one attempt.

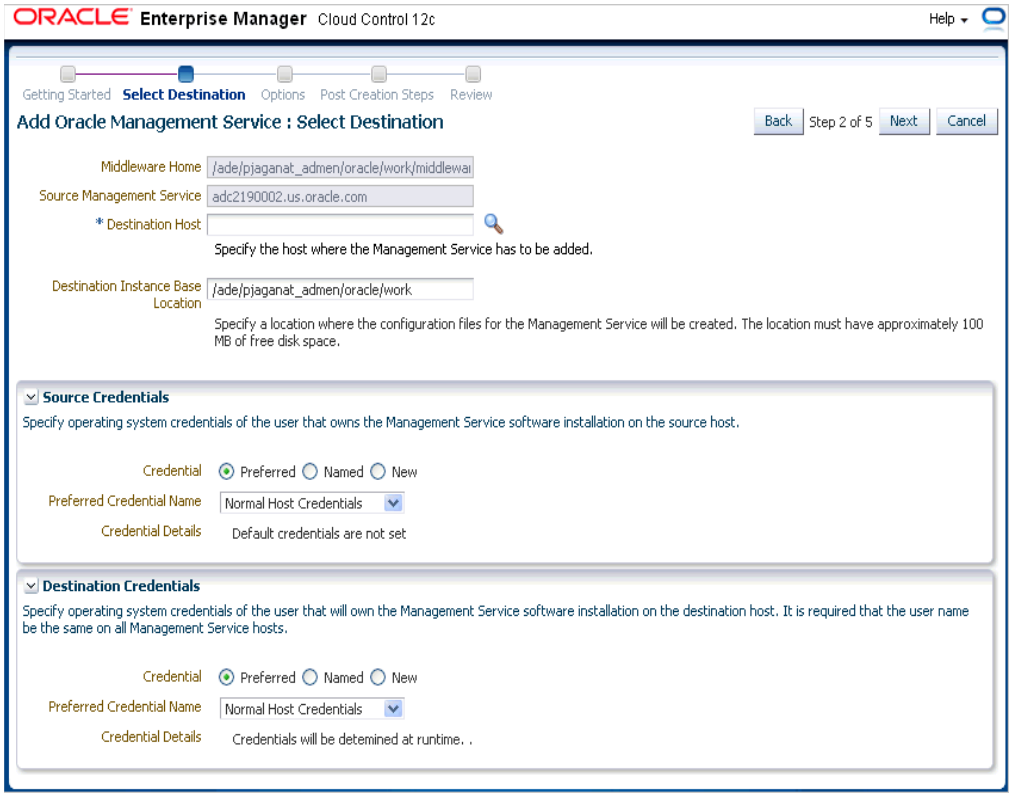
2.1.5 What Is Add Management Service Deployment Procedure?

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

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

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

Figure 2–3 Add Management Service Deployment Procedure



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

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

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

2.1.6 What Ports Are Used for Installation?

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

- What Default Ports Are Used?
- How Can You Customize Ports?
- What Precautions You Must Take While Customizing Port Numbers?

2.1.6.1 What Default Ports Are Used?

The following are the default ports used for installation:

- **Enterprise Manager Cloud Control**

Upload Port	Console Port

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

- **Oracle Management Agent**

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

- **Admin 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.

- **Node Manager**

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

- **Managed Server**

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

  The default HTTPS port for Managed Server is 7301. If 7310 is not available, then the first available free port from the range 7301 to 7400 is selected.

2.1.6.2 How Can You Customize Ports?

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

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

  The `staticports.ini` file is available at the following location of the software kit (DVD, downloaded software, and so on):

  ```
  <software_kit>/response/staticports.ini
  ```

2.1.6.3 What Precautions You Must Take While Customizing Port Numbers?

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:

- Always enter port numbers that are greater than 1024 and less than 65536.

- If a port is already being used by a component or any other application, do not enter that port (used port) in the `staticports.ini` file. If you do, then the related configuration assistant also fails.
- If you have entered the same port for more than one component, then the installation displays an error after the prerequisite checks phase. You must rectify this error before proceeding with the installation.
- If you have syntax errors in the `staticports.ini` file (for example, if you omitted the equal (=) character for a line), then the installation wizard ignores the line. For the components specified on such lines, the installation wizard assigns the default ports. The installation wizard does not display a warning for lines with syntax errors.
- If you misspell a component name, then the installation wizard assigns the default port for the component. Names of components in the file are case-sensitive. The installation wizard does not display a warning for lines with unrecognized names.
- If you enter a nonnumeric value for the port number, then the installation wizard ignores the line and assigns the default port number for the component. It does this without displaying any warning.
- If you misspell the parameter on the command line, then the installation wizard does not display a warning. It continues and assigns default ports to all components.
- If you enter a relative path to the `staticports.ini` file (for example, `./staticports.ini`) in the command line, then the installation wizard does not find the file. It continues without displaying a warning and it assigns default ports to all components. You must enter a full path to the `staticports.ini` file.

2.1.7 What Data Files Are Created While Configuring Oracle Management Repository?

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

`mgmt.dbf`	Stores information about the monitored targets, their metrics, and so on.
`mgmt_ecm_depot1.dbf`	Stores configuration information collected from the monitored targets.
`mgmt_ad4j.dbf`	Stores monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

2.1.8 How Do You Delete Data Files?

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

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_
database_host> <repository_database_port> <repository_database_
sid> -action dropall -dbUser <repository_database_user>
-dbPassword <repository_database_password> -dbRole <repository_
database_user_role> -mwHome <middleware_home> -mwOraHome <oms_
home> -oracleHome <oms_home>
```

Note:

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

  ```
  -mwHome <middleware_home> -mwOraHome <middleware_
  ora_home> -oracleHome <OMS_HOME>
  ```

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

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

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

Table 2–1 describes the `-action` options that are supported by the different versions of RepManager.

Table 2–1 RepManager Support for -action dropall Command

RepManager Version	Command Supported
RepManager 12.1	▪ `-action dropall` Drops SYSMAN, SYSMAN_MDS, APM, OPSS, EMRUNTIME, and SYSMAN_RO. ▪ `-action drop` Drops only SYSMAN.
RepManager 11.1	▪ `-action dropall` Drops only SYSMAN and SYSMAN_MDS. ▪ `-action drop` Drops only SYSMAN.
RepManager 10.2.0.5	`-action drop` Drops only SYSMAN.

2.2 Understanding Oracle WebLogic Server Requirement

Enterprise Manager Cloud Control requires Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+.

If Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing a new Enterprise Manager Cloud Control.

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

In particular, this section covers the following:

- How Do I Verify Whether Oracle WebLogic Server Is Installed?
- Is Oracle WebLogic Server Cluster Supported?
- If Oracle WebLogic Server Already Exists, Is the Existing Domain Used?

- When and Why Do You Need Oracle WebLogic Server Credentials?
- When and Why Do You Need 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 Admin Server?

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

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

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

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

```
release  10.3.5.0 [Added]
    |_____Common Infrastructure Engineering 7.1.0.0 [Added]
    |     |_____Uninstall [Added]
    |     |_____Patch Client [Added]
    |     |_____Patch Attachment Facility [Added]
    |     |_____Clone Facility [Added]
    |_____WebLogic Server 10.3.5.0 [Added]
    |     |_____Core Application Server [Added]
    |     |_____Administration Console [Added]
    |     |_____Configuration Wizard and Upgrade Framework [Added]
    |     |_____Web 2.0 HTTP Pub-Sub Server [Added]
    |     |_____WebLogic SCA [Added]
    |     |_____WebLogic JDBC Drivers [Added]
    |     |_____Third Party JDBC Drivers [Added]
    |     |_____WebLogic Server Clients [Added]
    |     |_____WebLogic Web Server Plugins [Added]
    |     |_____UDDI and Xquery Support [Added]
    |     |_____Server Examples [Added]
    |     |_____Evaluation Database [Added]
    |     |_____Workshop Code Completion Support [Added]
    |_____Oracle Configuration Manager 10.3.3.1 [Added]
    |     |_____Data Collector [Added]
    |_____Oracle Coherence 3.6.0.3 [Not Installed]
          |_____Coherence Product Files [Not Installed]
          |_____Coherence Examples [Not Installed]
```

2.2.2 Is Oracle WebLogic Server Cluster Supported?

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

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

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

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

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

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

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

2.2.5 When and Why Do You Need Node Manager Credentials?

While installing or upgrading to Enterprise Manager Cloud Control, you are prompted to enter the Node Manager password for the default Node Manager user account, which is `nodemanager`. The password is used for configuring the Node Manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

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

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

For example,

```
/u01/app/Oracle/gc_inst/user_projects/domains/EMGC_
DOMAIN/em/EMGC_OMS1/emgc.properties
```

2.2.7 How Do You Verify Whether Admin Server Is Running?

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

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

Here, host and port are values specified in the `EM_INSTANCE_HOST` and `AS_HTTPS_PORT` parameters, respectively, in the emgc.properties file. This properties file is available in the following location, that is, in the OMS home (first OMS) that was initially installed:

```
<OMS_HOME>/gc_inst/user_projects/domains/EMGC_DOMAIN/em/EMGC_
OMS1/emgc.properties
```

2.2.8 How Do You Start Admin Server?

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

```
emctl start oms
```

2.3 Understanding Installation Directories

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

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

2.3.1 What Is Oracle Inventory Directory?

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

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

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

- While installing Enterprise Manager Cloud Control using the installation wizard, you can enter the *oraInventory* directory in the Oracle Inventory screen. When you enter it in this screen, you must also select the appropriate operating system group name that will own the *oraInventory* directories. The group you select must have write permission on the *oraInventory* directories.
- While installing Enterprise Manager Cloud Control in silent mode, that is, without using the installation wizard, you can enter the *oraInventory* directory using the `-invPtrLoc` parameter. This parameter considers the path to a location where the inventory pointer file (`oraInst.loc`) is available.

  For example

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

  Note: Ensure that the *oraInventory* directory is not in a shared location. If it is, change it to a non-shared location.

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

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

2.3.2 What Is Oracle Middleware Home?

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

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

For example,

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

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

- If Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ are already installed in your environment, then the installation wizard automatically detects them and displays the absolute path to the middleware home where they are installed.

  In this case, validate the middleware home that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location. Ensure that the middleware home you select or enter is a middleware home that does not have any Oracle homes for the OMS and the Management Agent.

- If Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ are NOT already installed in your environment, then the installation wizard automatically installs them for you while installing Enterprise Manager Cloud Control.

  In this case, enter the absolute path to a directory where you want to have them installed. Ensure that the directory you enter does not contain any files or subdirectories.

  For example,

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

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

2.3.3 What Is Oracle Management Service Instance Base Location?

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

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

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

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

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

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

2.3.4 What Is Oracle Home?

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

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

Component	Default Oracle Home	Sample Location
Oracle Management Service	`oms`	`/u01/app/Oracle/Middleware/oms`

Oracle Management Agent	**For Management Agent Installed with OMS:**
	`agent/core/12.1.0.1.0`
	For Standalone Management Agent:
	`core/12.1.0.1.0`
		For Management Agent Installed with OMS:
		`/u01/app/Oracle/Middleware/agent/core/12.1.0.1.0`
		For Standalone Management Agent:
		`/u01/app/Oracle/software/core/12.1.0.1.0`

Oracle Management Plug-In (agent-specific plug-ins)	**For Management Agent Installed with OMS:**
	`agent/plugins`
	For Standalone Management Agent:
	`plugins`
		For Management Agent Installed with OMS:
		`/u01/app/Oracle/Middleware/agent/plug-ins`
		For Standalone Management Agent:
		/u01/app/Oracle/software/plugins

Oracle Management Plug-In (OMS-specific plug-ins)	`plugins`	`/u01/app/Oracle/software/plugins`

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

2.3.5 What Is Installation Base Directory?

While installing a Management Agent using the Add Host Targets Wizard, you are required to enter an *Installation Base Directory*.

Installation Base Directory is a directory where the Management Agent home is created.

For example, if the installation base directory is `/u01/app/oracle`, then the Management Agent home is created as `/u01/app/oracle/core/12.1.0.1.0`.

2.3.6 What is Agent Instance Directory?

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

While installing Enterprise Manager Cloud Control, this directory is created within the middleware home.

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

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

However, while installing a standalone Management Agent, this directory is created in the installation base directory.

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

`/u01/app/Oracle/agent_inst`

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

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

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

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

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

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

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

2.4 Understanding Additional Components Installed

This section describes the additional components that are installed along with the core components of Enterprise Manager Cloud Control. In particular, this section covers the following:

- What Is Oracle Configuration Manager?
- What Are Software Updates?

2.4.1 What Is Oracle Configuration Manager?

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

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

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

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

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

Otherwise, enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to My Oracle Support. To understand how the configuration information can be manually collected and uploaded, see the steps outlined in Section 2.4.1.1.

If you want to enable it after installing Enterprise Manager Cloud Control, then see Section 2.4.1.2.

2.4.1.1 Manually Collecting and Uploading Configuration Information

To manually collect the configuration information, follow these steps:

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

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

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

2. Upload the `ocmconfig.jar` file to a Service Request on My Oracle Support.
3. Repeat Step (1) and Step (2) from the Management Agent home.

2.4.1.2 Enabling Oracle Configuration Manager After Installing Enterprise Manager Cloud Control

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

1. Set the environment variable `ORACLE_CONFIG_HOME` to the Oracle Management Service Instance Base. Oracle Management Service Instance Base is the directory where the configuration files of the OMS are created.
   - In bash terminal, run the following command:

     ```
     export ORACLE_CONFIG_HOME=<absolute_path_to_gc_inst>
     ```

   - In other terminals, run the following command:

     ```
     setenv ORACLE_CONFIG_HOME <absolute_path_to_gc_inst>
     ```

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

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

3. From the Management Agent home, run the following command:

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

2.4.2 What Are Software Updates?

While installing or upgrading Enterprise Manager Cloud Control, you can choose to install software updates.

Software updates include interim patches, critical patch updates, prerequisite updates, install updates, and so on released by Oracle periodically.

2.4.2.1 How Can You Download the Software Updates?

You can either manually download the software updates or have the Enterprise Manager Cloud Control Installation Wizard automatically download them for you.

- **Manual Download by User:** If you choose to manually download the software updates yourself, then run the following utility and provide the required information:

  ```
  <DVD>/install/utility/downloadSWUpdates -u <My_Oracle_
  Support_Username>
  ```

  Note: If you want to know about the different arguments that can be passed with the utility, then run the following command:

  ```
  <DVD>/install/utility/downloadSWUpdates -h
  ```

  Manual download option is best suited when you are installing Enterprise Manager Cloud Control in silent mode. Oracle recommends you to use this option even while installing in graphical mode.

  For information on where the software updates get downloaded by default, and for information on how to download to a custom location, see Section 2.4.2.3.

- **Automatic Download by Installation Wizard:** If you choose to have the Enterprise Manager Cloud Control Installation Wizard automatically download the software updates, then on the Software Updates screen of the installation wizard, enter the *My Oracle Support* account user name and password. The installation wizard will connect to *My Oracle Support* and automatically download the updates from there.

2.4.2.2 When Can You Apply the Software Updates?

You can apply the software updates in one of the following ways depending on the download mechanism:

- **Manual Download by User:** If you have manually downloaded the software updates, then:
  - **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 the updates are available, and click **Search for Updates**. To search the computer and select the location, click **Browse**.
  - **In Silent Mode:** Before you invoke the installer using the response file, edit the response file to set the `INSTALL_UPDATES_SELECTION` parameter to

"staged". Then, for the STAGE_LOCATION parameter, enter the absolute path to the location where the updates are available.

- **Automatic Download by Installation Wizard:** If you want to automatically download and apply the software updates from *My Oracle Supoprt*, then:
  - **In Graphical Mode:** On the Software Updates screen of the installation wizard, select **Search for Updates**, and 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.
  - **In Silent Mode:** Before you invoke the installer using the response file, edit the response file to set the INSTALL_UPDATES_SELECTION parameter to "download". Then, enter your *My Oracle Support* credentials in the MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES and the MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES parameters.

Oracle strongly recommends you to apply them while the installation is in progress for the following reasons:

- Keeping track of the availability of software updates at the time of installation is difficult
- Keeping track of the patch numbers, and manually downloading them and applying them after installation is a cumbersome process

Automatically downloading and applying the software updates during installation saves time and effort, and ensures that you do not miss out on important software updates.

2.4.2.3 Where Are the Software Updates Downloaded?

By default, the software updates are downloaded and stored in a subdirectory titled Updates in the temporary directory. For example, /tmp/Updates.

If you do not want the software updates to be downloaded in the temporary directory location, then run the following command and enter a download location of your choice:

```
<DVD>/install/utility/downloadSWUpdates -u <My_Oracle_Support_
Username> -s <Custom_Download_Location>
```

The following options can be passed with this script:

-u <My Oracle Support Username>

-p <My oracle Support Password>

-ph <Proxy Host> [Optional Parameter]

-po <Proxy Port> [Optional Parameter]

-pu <Proxy Username> [Optional Parameter]

-pp <Proxy Password> [Optional Parameter]

-s <Download Location> [Optional Parameter]

2.5 Understanding Configuration Assistants

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

2.5.1 What Are Configuration Assistants?

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

Note: Even when you perform a software-only installation of Enterprise Manager, when you run the `configureGC.sh` script to configure the installation, the configuration assistants are internally run.

2.5.2 What Configuration Assistants Are Run by the Installation Wizard?

Table 2–3 lists the configuration assistants run by the installation wizard for the different installation types.

Note: For information about these installation types, see Section 2.1.3.

Table 2–3 Configuration Assistants Run for Different Installation Types

Installation Type	Configuration Assistant
Create a new Enterprise Manager System *(Install type offered by the Enterprise Manager Cloud Control installation Wizard)*	▪ Plugins Prerequisites Check ▪ Repository Configuration ▪ MDS Schema Configuration ▪ OMS Configuration ▪ Plugins Deployment and Configuration ▪ Plugins Inventory Migration ▪ Oracle Configuration Manager Repeater Configuration ▪ Agent Configuration Assistant

Table 2–3 (Cont.) Configuration Assistants Run for Different Installation Types

Installation Type	Configuration Assistant
Upgrade to Enterprise Manager 11g *(Install type offered by the Enterprise Manager Cloud Control installation Wizard)*	**Upgrading Enterprise Manager Cloud Control** ■ *1-System Upgrade Approach:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the previous row of this table), except for the *Repository Configuration Assistant* and the *Agent Configuration Assistant*. Instead of the *Repository Configuration Assistant*, *Repository Upgrade Configuration Assistant* is run. And the *Agent Configuration Assistant* is not run because the Management Agent is not upgraded as it is predeployed by the *Enterprise Manager 12c Upgrade Console*. ■ *2-System Upgrade Approach:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the previous row of this table), except for the *Repository Configuration Assistant*. Instead of the *Repository Configuration Assistant*, *Repository Upgrade Configuration Assistant* is run. ■ *1-System Upgrade Approach on a Different Host:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the previous row of this table), except for the *Repository Configuration Assistant*. Instead of the *Repository Configuration Assistant*, *Repository Upgrade Configuration Assistant* is run. **Upgrading Additional OMS** ■ *1-System Upgrade Approach:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the first row of this table), except for *Repository Configuration Assistant*, *MDS Schema Configuration Assistant*, and Agent Configuration Assistant. The *Agent Configuration Assistant* is not run because the Management Agent is not upgraded as it is predeployed by the *Enterprise Manager 12c Upgrade Console*. ■ *2-System Upgrade Approach:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the first row of this table). ■ *1-System Upgrade Approach on a Different Host:* The configuration assistants run for this approach are the same as the ones run for a fresh installation (as described in the first row of this table) except for *Repository Configuration Assistant*, *MDS Schema Configuration Assistant*, and *Agent Configuration Assistant*.

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

2.5.3 What Do You Do When Configuration Assistants Fail?

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

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

2.6 Understanding Prerequisite Checks

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

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

- What Prerequisite Checks Are Run by Default?
- How Can You Run Prerequisite Checks in Standalone Mode?

2.6.1 What Prerequisite Checks Are Run by Default?

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

- Prerequisite check for verifying whether the installation is being done on a certified operating system.
- Prerequisite check for verifying whether all the certified packages and libraries have been installed.
- Prerequisite check for verifying whether the glibc package has been installed. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether there is sufficient disk space in the `temp` directory. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether there is sufficient disk space in the inventory directory.
- Prerequisite check for verifying whether there is *write* permission in the inventory directory.*(Not applicable for OMS installation)*
- Prerequisite check for verifying whether the software is compatible with the current operating system.
- Prerequisite check for verifying whether there is sufficient physical memory.
- Prerequisite check for verifying the required `ulimit` value. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying the host name.
- Prerequisite check for verifying whether the `LD_ASSUME_KERNEL` environment variable is set. *(Not applicable for Management Agent installation)*
- Prerequisite check for verifying whether proper timezone is set.
- Prerequisite check for verifying whether there is 4 GB of swap space. *(Not applicable for Management Agent installation)*

2.6.2 How Can You Run Prerequisite Checks in 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.

Table 2–4 shows the commands you need to run to run the prerequisite checks in standalone mode:

Table 2–4 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>/install/runInstaller -prereqchecker PREREQ_CONFIG_ LOCATION=<Software_ Location>/stage/prereq -entryPoint "oracle.sysman.top.oms_Core" -prereqLogLoc <absolute_path_to_log_ location> -silent -waitForCompletion`

Note: On Microsoft Windows, replace `/runInstaller` with `setup.exe`. Also, `<Software_Location>` mentioned in the commands in Table 2–4 refer to the location where the Enterprise Manager software is available. For example, DVD. If you have downloaded the software from Oracle Technology Network (OTN), then enter the absolute path to that downloaded location.

2.7 Understanding Limitations of Enterprise Manager Cloud Control

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

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

2.7.1 Can You Access Unlicensed Components?

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

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

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

2.7.2 What Are the Limitations with DHCP-Enabled Machines?

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

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

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

2.8 Understanding Other Miscellaneous Concepts

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

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

2.8.1 What Is a Host List File?

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

If you choose to select an external file, then ensure that the file contains only the host name (Example 2–1), or the host name followed by the platform name (Example 2–2).

Example 2–1 External File with Only the Host Names

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

Example 2–2 External File with the Host Names and Platform Names

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

2.8.2 What Scripts Are Run During the Installation Process?

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

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

> **Note:** Ensure that the central inventory location you specify must NOT be on a shared file system. If it is already on a shared file system, then switch over to a non-shared file system.

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

  `$Home/oraInventory/oraInstRoot.sh`

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

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

  `<OMS_HOME>/allroot.sh`

Part II

Installing Enterprise Manager System

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

- Chapter 3, "Installing Enterprise Manager System in Silent Mode"
- Chapter 4, "Installing Enterprise Manager Software Now and Configuring Later"

3

Installing Enterprise Manager System in Silent Mode

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

- Overview
- Before You Begin
- Prerequisites
- Installation Procedure
- After You Install

> **Note:** Do NOT install the Enterprise Manager system on an OCFS file system. This file system is not supported.

3.1 Overview

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 multiple other hosts.

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

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

3.2 Before You Begin

Before you begin, keep these points in mind:

- You can install Enterprise Manager Cloud Control only on a single host—locally on the server where you invoke the installation wizard with a response file. You cannot install on multiple or remote hosts.
- Enterprise Manager Cloud Control 12*c* can communicate only with Oracle Management Agent 12*c*, and not with any earlier release of the Management Agent.
- You must not set the `ORACLE_HOME` and `ORACLE_SID` environment variables. You must ensure that the Oracle directories do NOT appear in the PATH.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6 v24 and Oracle WebLogic Server 11g Release 1 (10.3.5), but only if they do not exist in your environment.
- If Oracle WebLogic Server 11g Release 1 (10.3.5) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6 v24+ (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).
  - Download JDK 1.6 v24+ for your platform from the platform vendor's Web site. For example, download SUN JDK 1.6 v24+ for Linux platforms from Oracle Web site. Similarly, download the JDK for other platforms from other vendors' trusted Web sites.
  - If you already have JDK, then verify its version by navigating to the `<JDK_ Location>/bin` directory and running the following command:

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

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

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

    For example,

    ```
    <JDK home>/bin/java -d64 -jar <absolute_path _to_wls1035_
    generic.jar>
    ```
  - If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.5) on Linux 32-bit platforms, then download and use either the `wls1035_ linux32.bin` file or the `wls1035_generic.jar` file.

    For example,

    ```
    <JDK home>/bin/java  -jar <absolute_path _to_wls1035_
    generic.jar>
    ```
  - You must follow the instructions outlined in the *Oracle® Fusion Middleware Installation Guide for Oracle WebLogic Server* to install Oracle WebLogic Server. The guide is available in the Fusion Middleware documentation library available at:

    http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html
  - You must ensure that the Oracle WebLogic Server installation is a typical installation, and even if you choose to perform a custom installation, ensure

that components chosen for custom installation are the same as the ones associated with a typical installation.

– You must ensure that the user installing the WebLogic Server is the same as the one installing Enterprise Manager Cloud Control.

- You must not install Enterprise Manager Cloud Control in a middleware home that is on an NFS-mounted drive. Installing Enterprise Manager on an NFS-mounted drive causes the Oracle HTTP Server to restart frequently, which in turn makes the OMS inaccessible. If you are forced to install on such a shared drive, then ensure that the OMS instance base directory (`gc_inst`) is created in a non-NFS-mounted location.
- You must ensure that the Oracle WebLogic Server 11g Release 1 (10.3.5) installed by the Enterprise Manager Cloud Control Installation Wizard or by you is dedicated for Enterprise Manager Cloud Control. You must not have any other Oracle Fusion Middleware product installed in that middleware home.

  Enterprise Manager Cloud Control cannot coexist with any Oracle Fusion Middleware product in the same middleware home because the `ORACLE_COMMON` property is used by both the products.
- By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to `"skip"`. However, if you want to apply them during installation, then you can modify this variable as described in Table 3–2.
- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

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

  When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.
- You must upgrade all *existing* EMCLI clients of the earlier release to 12c Release 1 so that they can work with Enterprise Manager Cloud Control. This means, you must discard the old one and set up a new one.

  For information about setting up a new EMCLI client, see the *Enterprise Manager Command Line Interface Download* page within the Cloud Control console. To access that page, in Cloud Control, from the **Setup** menu, select **My Preferences**, and then, click **Command Line Interface**.
- You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc.

  On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

3.3 Prerequisites

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

3.4 Installation Procedure

This section covers the following:

- Installing Enterprise Manager
- Using Advanced Installer Options
- Understanding the Limitations
- Editing Response File for Installing Software

3.4.1 Installing Enterprise Manager

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

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

   `<Software_Location>/response/new_install.rsp`

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

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

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

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

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

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

   - Otherwise, run the following command:

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

     Note: For information about the additional, advanced options you can pass while invoking the installer, refer to Section 3.4.2.

Note:

- If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and rerun the configuration assistant. For more information, see Appendix D.

3.4.2 Using Advanced Installer Options

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

- If you want to install on a host that has multiple host names (for examle, virtual hosts), then pass the fully qualified host name using the `ORACLE_HOSTNAME` argument while invoking the installer. Ensure that the host name you enter does not have underscores.

  For example:

  ```
  ./runInstaller ORACLE_HOSTNAME=host1.foo.com -silent
  -responseFile <absolute_path>/new_install.rsp
  ```

  Note: Ensure that the host name you enter does not have underscores.

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

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

  For example,

  ```
  ./runInstaller EM_STAGE_DIR=/home/john/software/oracle/pafdir
  -silent -responseFile <absolute_path>/new_install.rsp
  ```

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

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

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

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

3.4.3 Understanding the Limitations

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

Table 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`
`b_startAgent=FALSE`
	1. Start the OMS:
	`$<OMS_HOME>/bin/emctl start oms`
	2. Secure the Management Agent:
	`$<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`
	6. Manually configure the EMCLI tool in the $<ORACLE_HOME>/bin directory. To do so, refer to the *Oracle Enterprise Manager Command Line Interface Guide*.

`START_OMS=TRUE`
`b_startAgent=FALSE`
	1. Secure the Management Agent:
	`$<AGENT_HOME>/bin/emctl secure agent`
	2. Start the Management Agent:
	`$<AGENT_HOME>/bin/emctl start agent`
	3. Add the targets:
	`$<AGENT_HOME>/bin/emctl config agent addinternaltargets`
	4. Upload the targets:
	`$<AGENT_HOME>/bin/emctl upload agent`

`START_OMS=FALSE`
`b_startAgent=TRUE`
	1. Start the OMS:
	`$<OMS_HOME>/bin/emctl start oms`
	2. Secure the Management Agent:
	`$<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`
	5. Manually configure the EMCLI tool in the $<ORACLE_HOME>/bin directory. To do so, refer to the *Oracle Enterprise Manager Command Line Interface Guide.*

3.4.4 Editing Response File for Installing Software

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 Cloud Control in silent mode.

Table 3–2 Editing Response File for Installing Enterprise Manager System

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

SECURITY_UPDATES_VIA_MYORACLESUPPORT	▪ Enter `TRUE` if you want to download and install security updates. Then, enter the credentials for the following variables:
	`MYORACLESUPPORT_USERNAME`
	`MYORACLESUPPORT_PASSWORD`
	▪ Enter `FALSE` if you do not want to download and install security updates:

DECLINE_SECURITY_UPDATES	▪ Enter `TRUE` if you want to decline the security updates. In this case, you should have entered `False` for `SECURITY_UPDATES_VIA_MYORACLESUPPORT`. ▪ Enter `FALSE` if you do not want to decline the security updates. In this case, you should have entered `TRUE` for `SECURITY_UPDATES_VIA_MYORACLESUPPORT`.

INSTALL_UPDATES_SELECTION	By default, this variable is set to `"skip"` indicating that the software updates will not be installed during installation.
	▪ If you want to install the software updates from My Oracle Support, then set this variable to `"download"`. Then, enter the credentials for the following parameters:
	`MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES`
	`MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES`
	▪ If you want to install the software updates from a staged location, then set this variable to `"staged"`. Then, for the `STAGE_LOCATION` parameter, enter the absolute path, which leads to the `Updates` directory, where the software updates are available.

PROXY_USER	Enter the user name that can be used to access the proxy server. **Note:** Applies only if you have set the `SECURITY_UPDATES_VIA_MYORACLESUPPORT` variable to `TRUE` and/or the `INSTALL_UPDATES_SELECTION` variable to `"download"`, and only if your connection to the Internet requires you to connect through a proxy.

Table 3–2 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
PROXY_PWD	Enter the password that can be used to access the proxy server. **Note:** Applies only if you have set the `SECURITY_UPDATES_VIA_MYORACLESUPPORT` variable to `TRUE` and/or the `INSTALL_UPDATES_SELECTION` parameter to `"download"`, and only if your connection to the Internet requires you to connect through a proxy.
PROXY_HOST	Enter the name of the proxy host. **Note:** Applies only if you have set the `SECURITY_UPDATES_VIA_MYORACLESUPPORT` variable to `TRUE` and/or the `INSTALL_UPDATES_SELECTION` parameter to `"download"`, and only if your connection to the Internet requires you to connect through a proxy.
PROXY_PORT	Enter the port used by the proxy server. **Note:** Applies only if you have set the `SECURITY_UPDATES_VIA_MYORACLESUPPORT` variable to `TRUE` and/or the `INSTALL_UPDATES_SELECTION` parameter to `"download"`, and only if your connection to the Internet requires you to connect through a proxy.
ORACLE_MIDDLEWARE_HOME_LOCATION	Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24. For example, `u01/app/Oracle/Middleware`. Ensure that the middleware location has *write* permission. And that this is not an NFS-mounted location. If you have already installed them manually, then enter the location where you have installed them. For more information about this location, see Section 2.3.2. **Note:** Ensure that the middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same middleware home.
WLS_ADMIN_SERVER_USERNAME	By default, `weblogic` is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then skip this variable. However, if you want to have a custom name, then enter the name of your choice.
WLS_ADMIN_SERVER_PASSWORD	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_PASSWORD	By default, `nodemanager` is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
NODE_MANAGER_CONFIRM_PASSWORD	Confirm the password for the node manager user account.

Table 3–2 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
ORACLE_INSTANCE_HOME_LOCATION	By default, `gc_inst` is considered as the OMS Instance Base directory for storing all OMS-related configuration files, and it is created in the middleware home. If you want to accept the default location and the directory name, then skip this variable. However, if you want to have a custom location and a custom directory name, then enter the absolute path to the custom location leading up to the custom directory name. For more information about this location, see Section 2.3.5. **Note:** If you have entered an NFS-mounted drive for the `ORACLE_MIDDLEWARE_HOME_LOCATION` parameter, then ensure that the location you enter for this parameter is a non-NFS-mounted location.
DATABASE_HOSTNAME	Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores. For example, `db.host.com` 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: `$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conndesc '"(DESCRIPTION= (ADDRESS_LIST=(FAILOVER=ON) (ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521)) (ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=EMREP)))"' -repos_user sysman`
LISTENER_PORT	Enter the listener port to connect to the existing database. For example, `1532`
SERVICENAME_OR_SID	Enter the service name or the system ID (SID) of the existing database. For example, `orcl`
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	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.
SYSMAN_CONFIRM_PASSWORD	Confirm the SYSMAN user account's password.

Table 3–2 (Cont.) Editing Response File for Installing Enterprise Manager System

Parameter	Description
MANAGEMENT_ TABLESPACE_LOCATION	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 `+<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 Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data.
CONFIGURATION_DATA_ TABLESPACE_LOCATION	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 Cloud Control requires this data file to store configuration information collected from the monitored targets.
JVM_DIAGNOSTICS_ TABLESPACE_LOCATION	Enter the absolute path to a location where the data file (`mgmt_ad4j.dbf`) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name. For example, `/home/john/oradata/mgmt_ad4j.dbf` Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).
AGENT_REGISTRATION_ PASSWORD	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	Confirm the agent registration password.
STATIC_PORTS_FILE	By default, ports described in Section 2.1.6 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 Response File for Installing Enterprise Manager System

Parameter	Description

PLUGIN_SELECTION	By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed with the Enterprise Manager system.
	
	However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.
	
	For example,
	
	`PLUGIN_ SELECTION={"oracle.sysman.empa","oracle.sysman.vt"}`
	
	If you want to install any plug-in that is not available in the software kit, then do the following:
	
	1. Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location:
	
	`http://www.oracle.com/technetwork/oem/grid-control/downloads/index.html`
	
	2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded.
	
	3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins:
	
	`./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>`

3.5 After You Install

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

4

Installing Enterprise Manager Software Now and Configuring Later

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

- Overview
- Before You Begin
- Prerequisites
- Installing Software

> **Note:** Do NOT install the Enterprise Manager system on an OCFS file system. This file system is not supported.

4.1 Overview

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

This approach helps you plan your installation according to the time and priorities you have. While you can perform this software-only installation in graphical and silent mode, this chapter describes how you perform it in graphical mode.

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

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

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

Note:

- Java Development Kit (JDK) 1.6 v24 and Oracle WebLogic Server 11g Release 1 (10.3.5) are installed only if they do not exist in your environment.
- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.5), then follow the guidelines outlined in Section 4.2.
- In addition to the mandatory plug-ins listed above, you can optionally install other plug-ins available in the software kit. The installer offers a screen where you can select the optional plug-ins and install them. However, if you want to install some plug-ins that are not available in the software kit, then refer to the point about installing additional plug-ins in Section 4.4.1.3.1.

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

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

  For example, if the middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/Middleware/gc_inst`.
- Configures Oracle Management Repository in the existing, certified Oracle Database.
- Runs the following configuration assistants to configure the installed or upgraded components:
  - Plugins Prerequisites Check
  - Repository Configuration
  - MDS Schema Configuration
  - OMS Configuration
  - Plugins Deployment and Configuration
  - Plugins Inventory Migration
  - Oracle Configuration Manager Repeater Configuration
  - Agent Configuration Assistant

4.2 Before You Begin

Before you begin, keep these points in mind:

- You can install Enterprise Manager Cloud Control using the installation wizard only on a single host, that is, locally on the server where the wizard is invoked. You cannot install on multiple or remote hosts.
- Enterprise Manager Cloud Control 12*c* can communicate only with Oracle Management Agent 12*c*, and not with any earlier release of the Management Agent.
- You must not set the `ORACLE_HOME` and `ORACLE_SID` environment variables. You must ensure that the Oracle directories do NOT appear in the PATH.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6 v24 and Oracle WebLogic Server 11g Release 1 (10.3.5), but only if they do not exist in your environment.
- *(Only for Graphical Mode)* You must set the `DISPLAY` environment variable.
  - In bash terminal, run the following command:

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

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

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

    For example, `setenv DISPLAY my.example.com:1.0`
- If Oracle WebLogic Server 11g Release 1 (10.3.5) does not exist and if you choose to manually install it, then ensure that you install it using JDK 1.6 v24+ (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).
  - Download JDK 1.6 v24+ for your platform from the platform vendor's Web site. For example, download SUN JDK 1.6 v24+ for Linux platforms from Oracle Web site. Similarly, download the JDK for other platforms from other vendors' trusted Web sites.
  - If you already have JDK, then verify its version by navigating to the `<JDK_Location>/bin` directory and running the following command:

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

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

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

    For example,

    ```
    <JDK home>/bin/java -d64 -jar <absolute_path _to_wls1035_generic.jar>
    ```
  - If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.5) on Linux 32-bit platforms, then download and use either the `wls1035_linux32.bin` file or the `wls1035_generic.jar` file.

For example,

```
<JDK home>/bin/java  -jar <absolute_path _to_wls1035_
generic.jar>
```

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

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

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

  - You must ensure that the user installing the WebLogic Server is the same as the one installing Enterprise Manager Cloud Control.

- You must not install Enterprise Manager Cloud Control in a middleware home that is on an NFS-mounted drive. Installing Enterprise Manager on an NFS-mounted drive causes the Oracle HTTP Server to restart frequently, which in turn makes the OMS inaccessible. If you are forced to install on such a shared drive, then ensure that the OMS instance base directory (`gc_inst`) is created in a non-NFS-mounted location.

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

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

- *(Only for Silent Mode)* By default, the software updates cannot be applied during installation because the `INSTALL_UPDATES_SELECTION` variable in the response file is set to `"skip"`. However, if you want to apply them during installation, then you can modify this variable as described in Section 4.4.2.1.1.

- By default, the upload ports and console ports as described in Section 2.1.6 are used.

- Oracle offers bug fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for bug fixes offered by Oracle also ends. For more information, see the *Oracle Lifetime Support Policy* available at:

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

  When determining supportability and certification combinations for an Enterprise Manager Cloud Control installation, you must consider Enterprise Manager Cloud Control's framework components as well as the targets monitored by Enterprise Manager Cloud Control. Oracle recommends keeping your Cloud Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.

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

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

- You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc.

  On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

4.3 Prerequisites

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

4.4 Installation Procedure

This section describes the following:

- Installing in Graphical Mode
- Installing in Silent Mode

4.4.1 Installing in Graphical Mode

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

- Installing Software
- Running Root Script
- Configure Software
- Performing Post-Configuration Tasks

4.4.1.1 Installing Software

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

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

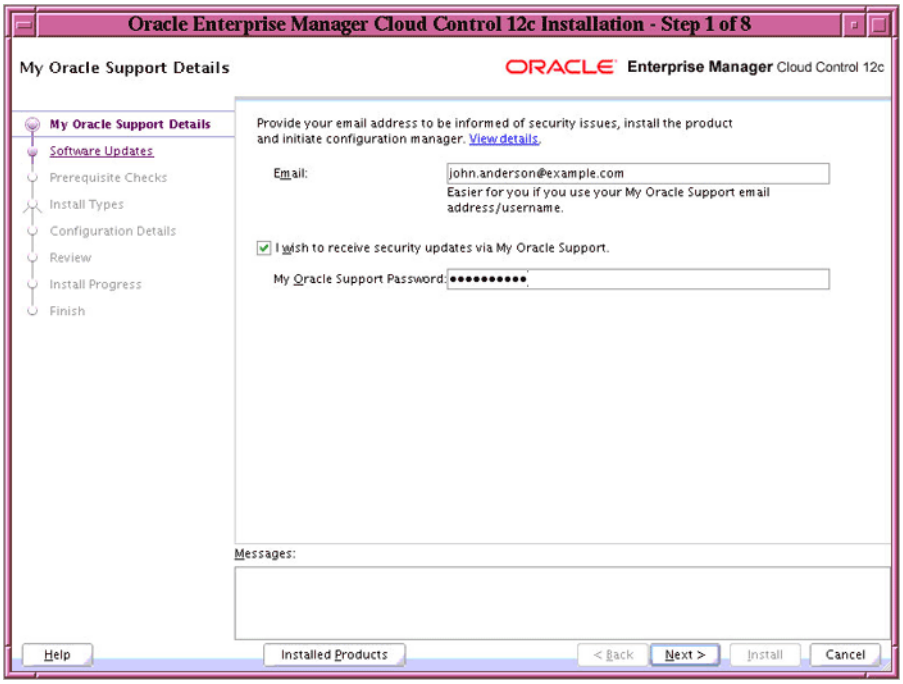
   Invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

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

Note:

- In this command, `<Software_Location>` refers to either the DVD or the location where you have downloaded software kit.
- For information about the additional, advanced options you can pass while invoking the installer, refer to Section 4.4.1.1.1.
- The central inventory location you enter must NOT be on a shared file system.

2. **Enter My Oracle Support Details**

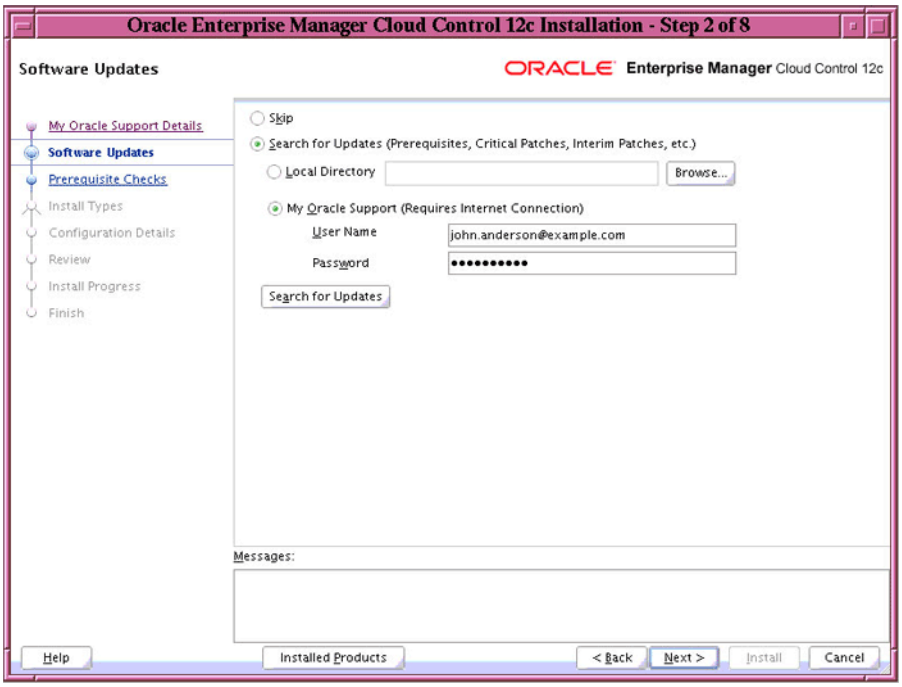


(Optional) On the My Oracle Support Details screen, enter your *My Oracle Support* credentials to enable Oracle Configuration Manager. If you do not want to enable Oracle Configuration Manager now, go to Step (3).

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

Note: For information about manually collecting the configuration information and uploading it to *My Oracle Support*, see Section 2.4.1.1.

3. Click **Next**.
4. **Install Software Updates**



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

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

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

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

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

  Note: For more information about software updates, and how you can manually download them, see Section 2.4.2.

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

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

---

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

---

5. Click **Next**.

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

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

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

6. **Enter Oracle Inventory Details**

   On the Oracle Inventory screen, do the following. You will see this screen only if this turns out to be your first ever installation of an Oracle product on the host.

   a. Enter the full path to a directory where the inventory files and directories can be placed.

   Note:

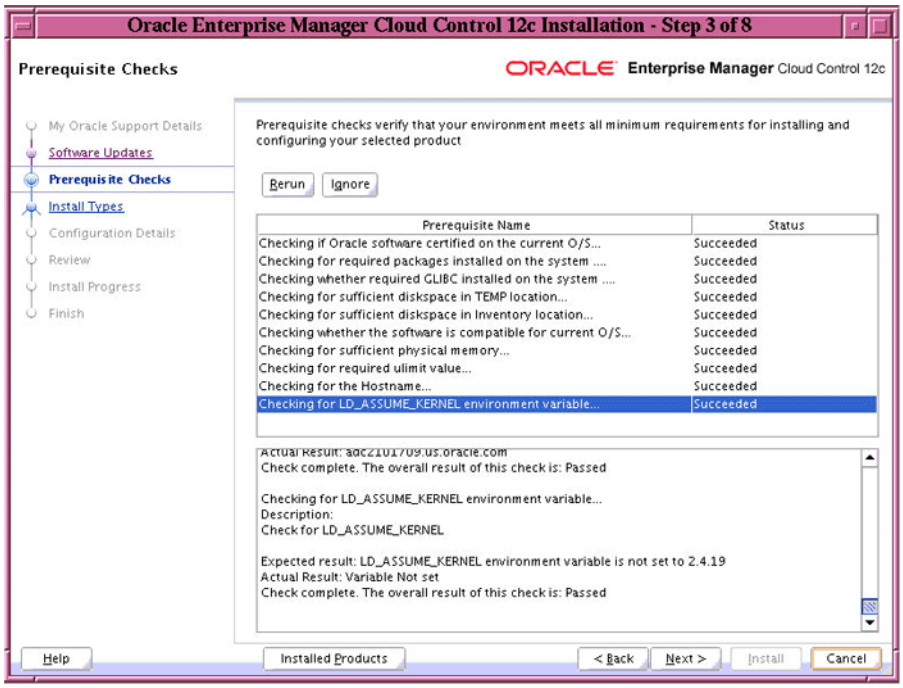
   - The central inventory location you enter must NOT be on a shared file system. If it is already on a shared file system, then switch over to a non-shared file system by following the instructions outlined in *My Oracle Support* note 1092645.1
   - If this is the first Oracle product on the host, then the default central inventory location is `/home/<user_name>/oraInventory`. However, if you already have some Oracle products on the host, then the central inventory location can be found in the `oraInst.loc` file. The `oraInst.loc` file is located in the `/etc` directory for Linux and AIX, and in the `/var/opt/oracle` directory for Solaris, HP-UX, and Tru64.

   ---

   b. Select the appropriate operating system group name that will own the Oracle inventory directories. The group that you select must have *write* permissions on the Oracle Inventory directories.

7. Click **Next**.

8. **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. It checks for the required operating system patches, operating system packages, and so on.

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

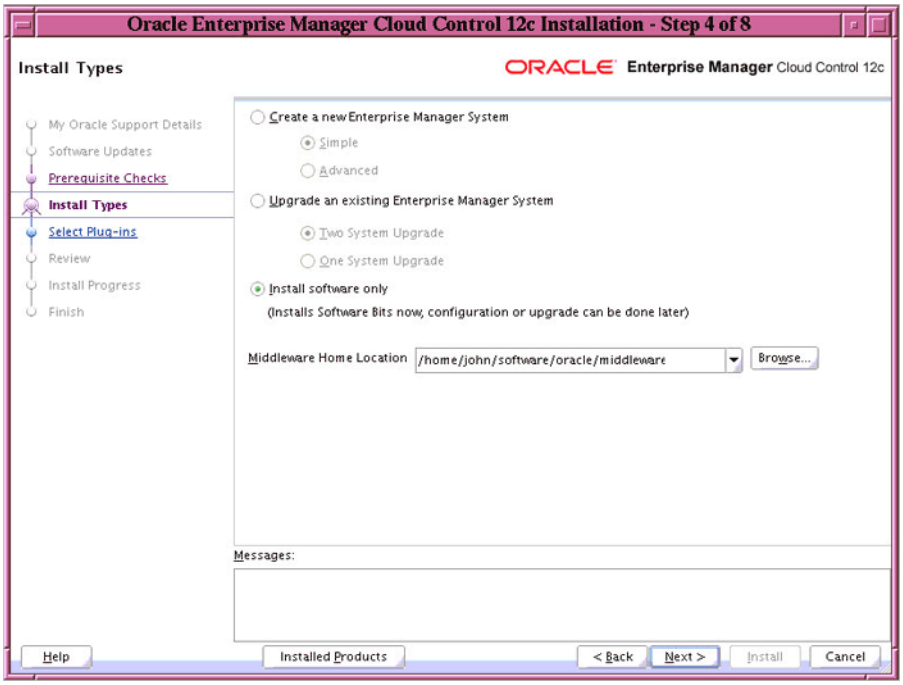
- If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the installation. The screen provides details on why the prerequisites failed and how you can resolve them. After you correct the problems, return to this screen and click **Rerun**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

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

- Although Oracle recommends you to investigate and correct the problems, if you are compelled to proceed without resolving them, then select **Ignore** to ignore the warnings and failures.

  However, all package requirements must be met or fixed before proceeding any further. Otherwise, the installation might fail.

9. Click **Next**.
10. **Select Installation Type**



On the Install Types screen, do the following:

a. Select **Install software only**.

b. Validate or enter the middleware home location.

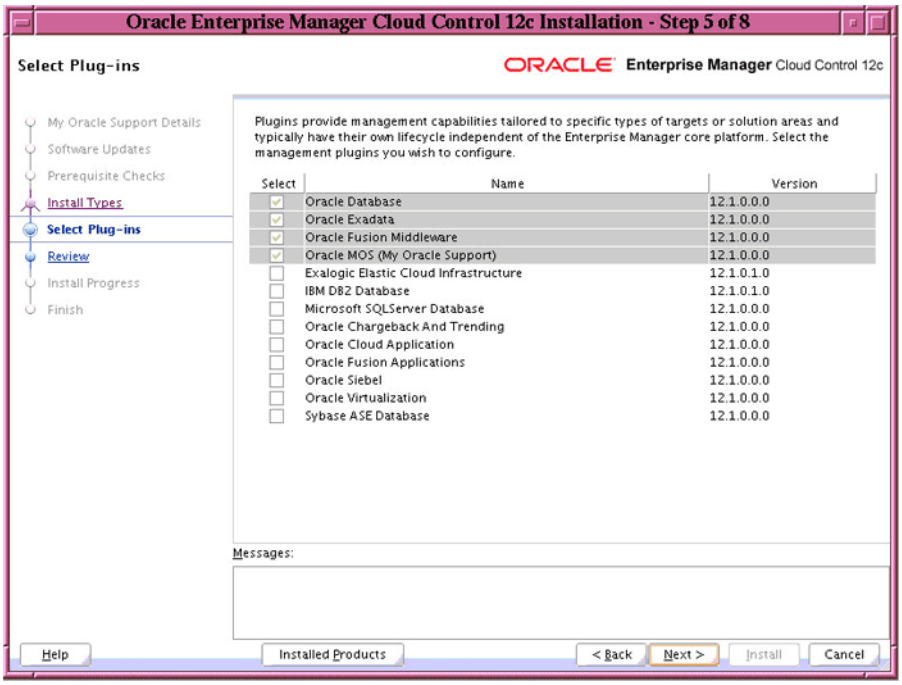
Note:

- If Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 are already installed in your environment, then the installer automatically detects them and displays the absolute path to the middleware home where they are installed. In this case, validate the middleware home location that is detected and displayed by default. If the location is incorrect, then enter the path to the correct location. Ensure that the middleware home location you select or enter is a middleware home location that does not have any Oracle homes for Oracle Management Service and Oracle Management Agent.
- If Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 are NOT already installed in your environment, then the installer automatically installs them for you while installing the Enterprise Manager system. In this case, enter the absolute path to a directory where you want to have them installed. For example, `/oracle/software/`. Ensure that the directory you enter does not contain any files or subdirectories.

---

11. Click **Next**.

12. **Select Plug-Ins**



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

Note: 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.

---

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

    On the Review screen, review the details you provided for the selected installation type.

    - If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
    - After you verify the details, if you are satisfied, click **Install** to begin the installation process.

15. On the Install Progress screen, view the overall progress (in percentage) of the installation.
16. On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

4.4.1.1.1 Using Advanced Installer Options The following are some additional, advanced options you can pass while invoking the installer:

- If you want to install on a host that has multiple host names (for example, virtual hosts), then pass the `ORACLE_HOSTNAME` argument while invoking the installer. Ensure that the host name you enter does not have underscores.

  For example,

  ```
  ./runInstaller ORACLE_HOSTNAME=host1.foo.com
  ```

- 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.

  For example,

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

- If you want to install some plug-ins that are not in the software kit, then follow these steps:

  1. Manually download the plug-ins from the Enterprise Manager Download page on OTN, and store them in an accessible location.

     http://www.oracle.com/technetwork/oem/grid-control/downloads/index.html

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

     ```
     ./runInstaller -pluginLocation <absolute_path_to_plugin_
     software_location>
     ```

     The Select Plug-In screen of the installation wizard displays a list of plug-ins available in the software kit as well as the plug-ins available in this custom location. You can choose the ones you want to install.

4.4.1.2 Running Root Script

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

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

4.4.1.3 Configure Software

To configure Enterprise Manager Cloud Control, follow these steps:

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

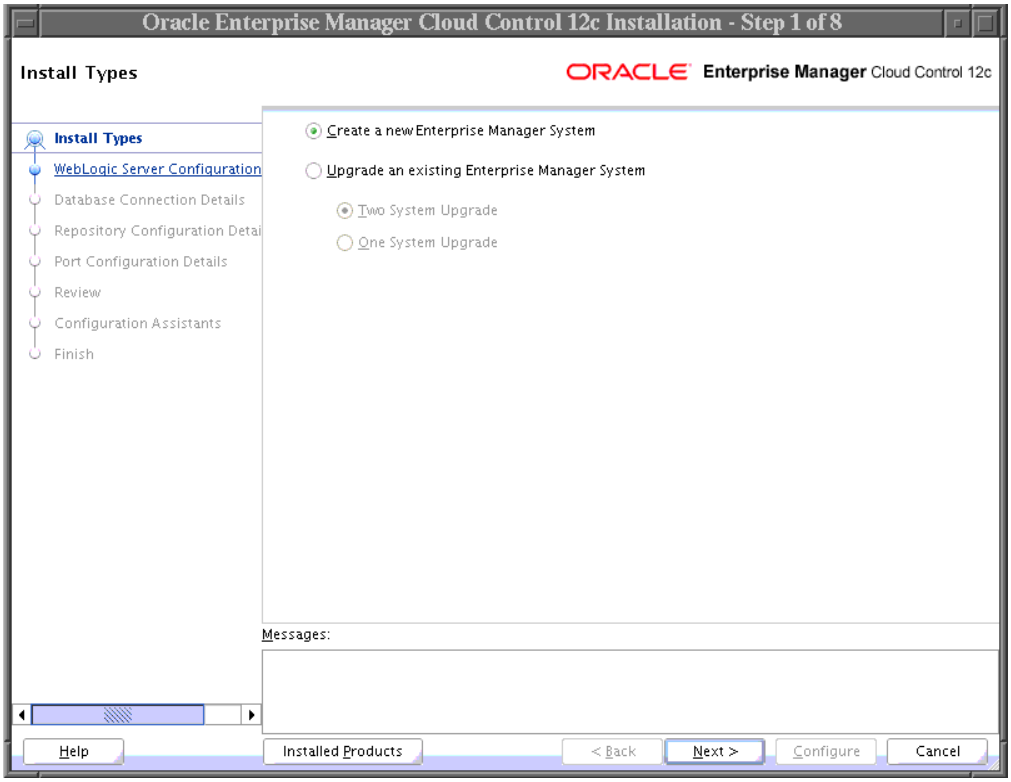
   Invoke the installation wizard as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

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

Note:

- While installing the software binaries as described in Section 4.4.1.1, if you had passed the argument -invPtrLoc, then pass the same argument here as well.
- For information about the additional, advanced options you can pass while invoking the script, refer to Section 4.4.1.3.1.

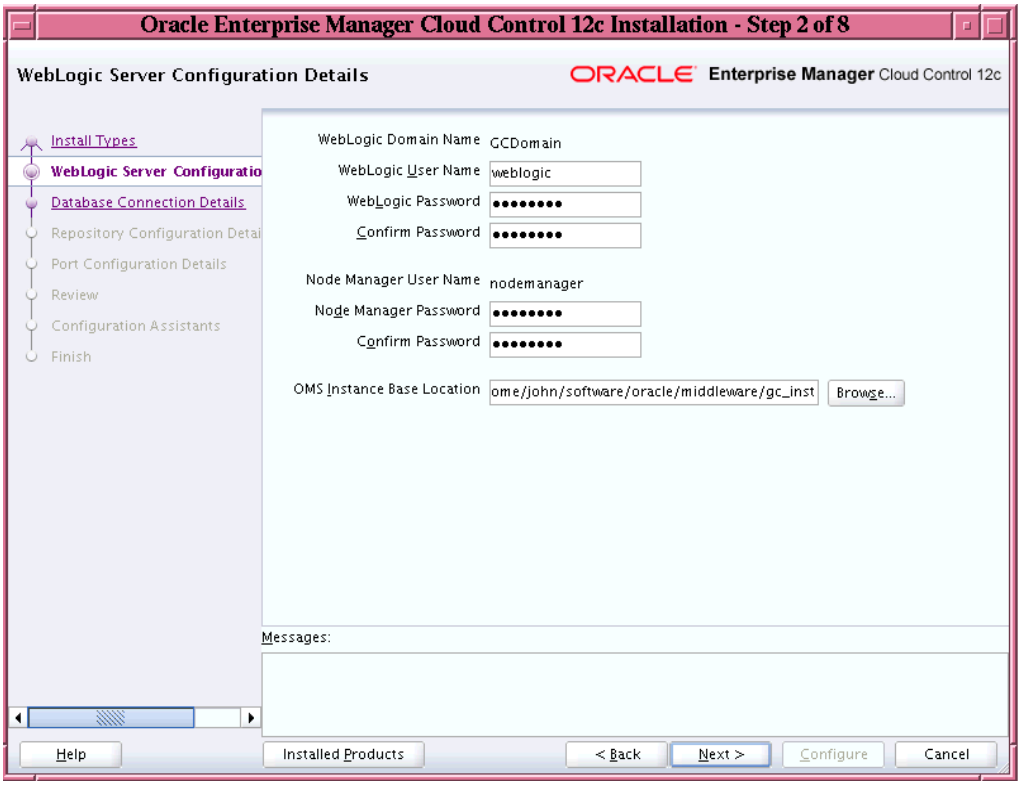
2. **Select Installation Type**



In the installation wizard, on the Install 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.

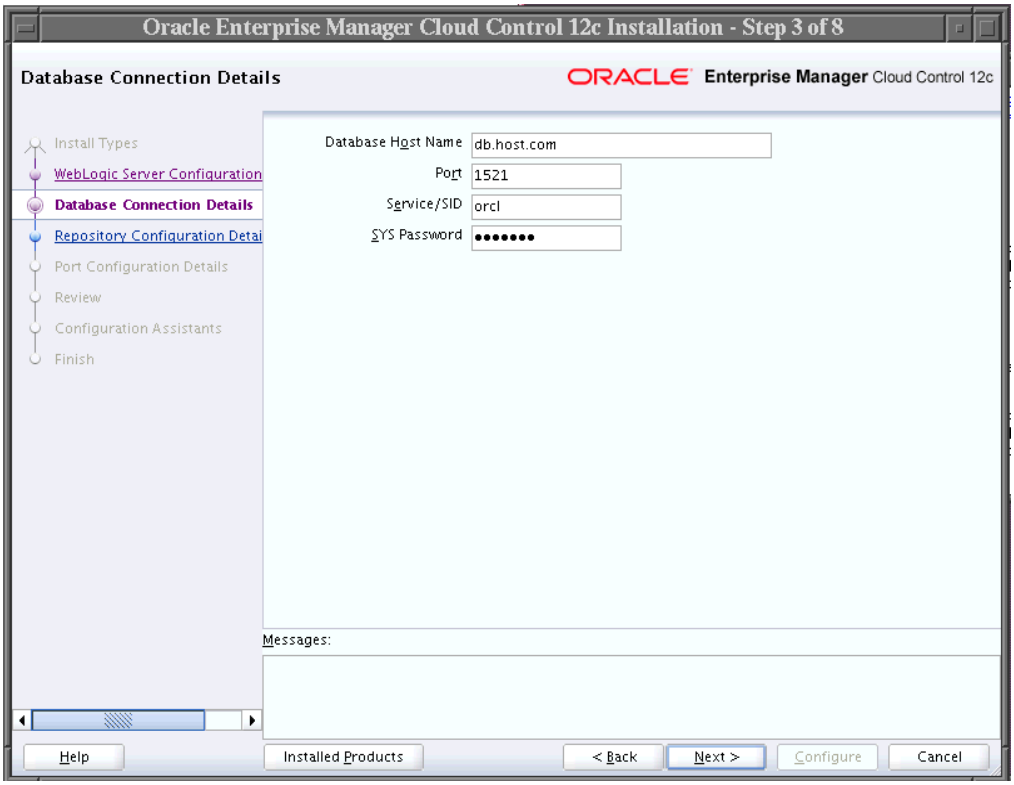
Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

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

A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

By default, the Oracle Management Service instance base location is `gc_inst`, which is created in 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, enter the fully qualified name of the host where the existing database resides, the database's listener port and its service name or system ID (SID), and the SYS user account's password.

The installer uses this information to connect to the existing, certified Oracle Database for creating the SYSMAN schema. SYSMAN schema holds most of the relational data used in managing Enterprise Manager Cloud Control.

Note: If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

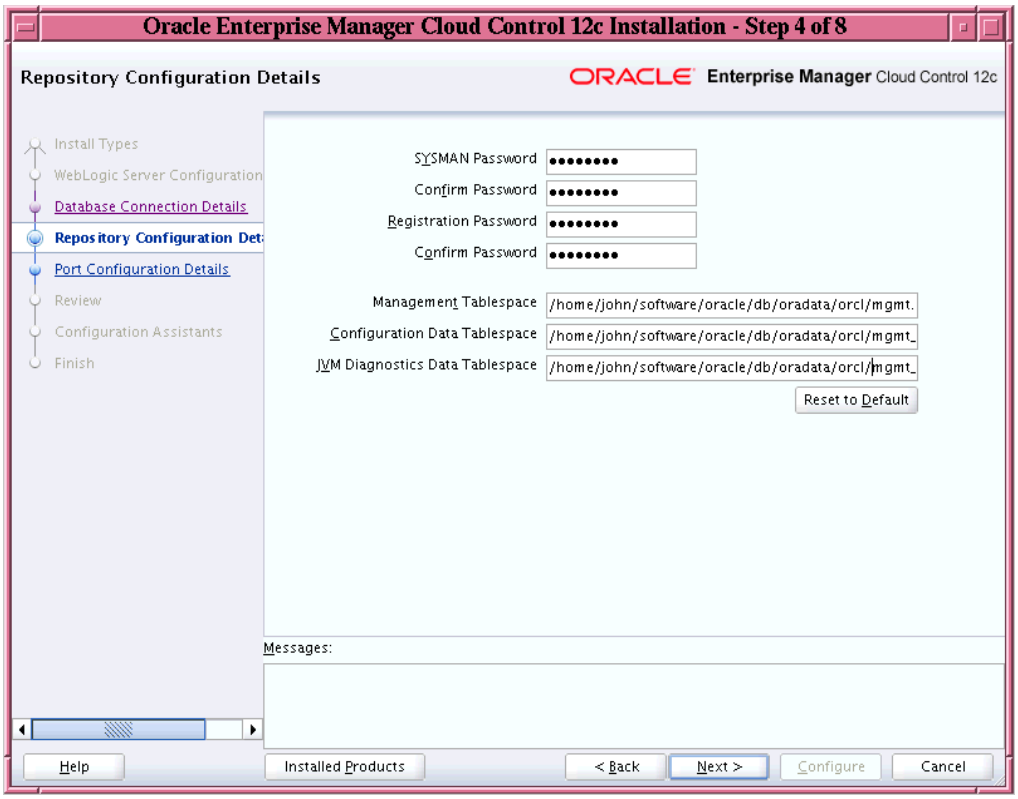
---

7. Click **Next**.

Note: If you are connecting to an Oracle RAC database, and if you have entered the virtual host name of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connect string with information about the other nodes that are part of the cluster. Update the connect string and click **OK**. If you want to test the connection, click **Test Connection**.

---

8. **Enter Repository Configuration Details**



On the Repository Configuration Details screen, do the following:

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

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

---

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

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

---

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

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

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`

e. For **JVM Diagnostics Data Tablespace**, enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (`mgmt_ad4j.dbf`) can be stored. Ensure that the specified path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

For example, `/u01/oracle/prod/oradata/mgmt_ad4j.dbf`

Note: If you are configuring the Management Repository on a database that uses Oracle Automatic Storage Management (Oracle ASM) for storage, then when you enter the data file location, only the disk group is used for creating the tablespaces. For example, if you specify `+DATA/a.dbf`, then only `+DATA` is used for creating the tablespaces on Oracle ASM, and the exact location of the data file on the disk group is decided by Oracle Managed Files.

---

9. Click **Next**.

10. Customize Ports

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

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

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

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

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

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

---

11. Click **Next**.
12. **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 **Configure** to begin the installation process.
13. **Track the Progress**

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

    Note:

    - If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and rerun the configuration assistant. For more information, see Appendix D.
    - If you accidently exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the configuration assistant in silent mode. For Microsoft Windows platforms, invoke `runConfig.bat` script.

      ```
      $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_
      HOME=<absolute_path_to_OMS_home> MODE=perform
      ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
      0_0.xml}
      ```

    ---
14. **End the Installation**

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

4.4.1.3.1 Using Advanced Script Options

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

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

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

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

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

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

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

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

4.4.1.4 Performing Post-Configuration Tasks

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

4.4.2 Installing in Silent Mode

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

- Installing Software
- Running Root Script
- Configuring Software
- Performing Post-Configuration Tasks

4.4.2.1 Installing Software

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

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

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

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

2. Edit the response file and enter appropriate values for the variables described in Table 4–1.
3. Invoke the installer as a user who belongs to the `oinstall` group you created. For information about creating operating system groups and users, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
   - If this is the first Oracle product you are installing on the host, then run the following command:

     ```
     ./runInstaller -silent -responseFile <absolute_
     path>/software_only.rsp [-invPtrLoc <absolute_path_to_
     oraInst.loc>]
     ```

   - Otherwise, run the following command:

     ```
     ./runInstaller -silent -responseFile <absolute_
     path>/software_only.rsp
     ```

     Note:

     - The central inventory location you enter must NOT be on a shared file system.
     - For information about the additional, advanced options you can pass while invoking the installer, refer to Section 3.4.2. The central inventory location you enter must NOT be on a shared file system

4.4.2.1.1 Editing Response File for Installing Software

Table 4–1 describes what variables you must edit and how you must edit them in the `new_install.rsp` response file for installing the software binaries.

Table 4–1 Editing Response File for Installing Enterprise Manager Software

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

SECURITY_UPDATES_VIA_ MYORACLESUPPORT	▪ Enter `TRUE` if you want to download and install security updates. Then, enter the credentials for the following variables:
	`MYORACLESUPPORT_USERNAME`
	`MYORACLESUPPORT_PASSWORD`
	▪ Enter `FALSE` if you do not want to download and install security updates:

DECLINE_SECURITY_ UPDATES	▪ Enter `TRUE` if you want to decline the security updates. In this case, you should have entered `False` for `SECURITY_UPDATES_VIA_MYORACLESUPPORT`. ▪ Enter `FALSE` if you do not want to decline the security updates. In this case, you should have entered `TRUE` for `SECURITY_UPDATES_VIA_ MYORACLESUPPORT`.

Table 4–1 (Cont.) Editing Response File for Installing Enterprise Manager Software

Parameter	Description

INSTALL_UPDATES_ SELECTION	By default, this variable is set to `"skip"` indicating that the software updates will not be installed during installation.
	▪ If you want to install the software updates from My Oracle Support, then set this variable to `"download"`. Then, enter the credentials for the following parameters:
	`MYORACLESUPPORT_USERNAME_FOR_ SOFTWAREUPDATES`
	`MYORACLESUPPORT_PASSWORD_FOR_ SOFTWAREUPDATES`
	▪ If you want to install the software updates from a staged location, then set this variable to `"staged"`. Then, for the `STAGE_LOCATION` parameter, enter the absolute path, which leads to the `Updates` directory, where the software updates are available.

ORACLE_MIDDLEWARE_ HOME_LOCATION	Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24. For example, `u01/app/Oracle/Middleware`. Ensure that the middleware location has *write* permission to create the Oracle homes for OMS and Management Agent. If you have already installed them manually, then enter the location where you have installed them. For more information about this location, see Section 2.3.2. **Note:** Ensure that the middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same middleware home.

Table 4–1 (Cont.) Editing Response File for Installing Enterprise Manager Software

Parameter	Description

PLUGIN_SELECTION	By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed with the Enterprise Manager system.
	
	However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.
	
	For example,
	
	`PLUGIN_ SELECTION={"oracle.sysman.empa","oracle.sysman.vt"}`
	
	If you want to install any plug-in that is not available in the software kit, then do the following:
	
	1. Manually download the plug-ins from the Enterprise Manager download page on OTN, and store them in an accessible location:
	
	`http://www.oracle.com/technetwork/oem/grid-control/downloads/index.html`
	
	2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded.
	
	3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins:
	
	`./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>`

4.4.2.2 Running Root Script

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

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

4.4.2.3 Configuring Software

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

1. Copy the following response file to an accessible location on the host where you copied the software binaries of Enterprise Manager Cloud Control:

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

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

2. Edit the response file and enter appropriate values for the variables described in Table 4–2.

3. Configure the software binaries by invoking the `ConfigureGC.sh` script passing the response you edited in the previous step:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh -silent
-responseFile <absolute_path>/new_install.rsp [-invPtrLoc
<absolute_path_to_inventory_directory>]
```

Note:

- While installing the software binaries as described in Section 4.4.2.1, if you had passed the argument -invPtrLoc, then pass the same argument here as well.
- For information about the additional, advanced options you can pass while invoking the script, refer to Section 4.4.1.3.1.

Note:

- If any repository-related prerequisite check fails, then run the check manually. For instructions, see the appendix on EM Prerequisite Kit in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
- If a configuration assistant fails, the installer stops and none of the subsequent configuration assistants are run. Resolve the issue and rerun the configuration assistant. For more information, see Appendix D.

4.4.2.3.1 Editing Response File for Configuring Software

Table 4–2 describes what variables you must edit and how you must edit them in the `new_install.rsp` file for configuring the software binaries.

Table 4–2 Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
WLS_ADMIN_SERVER_ USERNAME	By default, `weblogic` is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.
WLS_ADMIN_SERVER_ PASSWORD	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_ CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_ PASSWORD	By default, `nodemanager` is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
NODE_MANAGER_CONFIRM_ PASSWORD	Confirm the password for the node manager user account.

Table 4–2 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
ORACLE_INSTANCE_HOME_LOCATION	By default, `gc_inst` is considered as the OMS Instance Base directory for storing all OMS-related configuration files. If you want to accept the default directory, then blank. However, if you want to have a custom directory, then enter the name of the custom directory. Whether you accept the default directory or enter a custom one, by default, the directory is created under the parent directory of the middleware home. For example, if the middleware home is `/u01/app/Oracle/Middleware`, then the directory is is `/u01/app/Oracle/gc_inst`. For more information about this location, see Section 2.3.5.
DATABASE_HOSTNAME	Enter the fully qualified name of the host where the existing database resides. Ensure that the host name does not have underscores. For example, `db.host.com` 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: `$<OMS_HOME>/bin/emctl config oms -store_repos_details -repos_conndesc '"(DESCRIPTION= (ADDRESS_LIST=(FAILOVER=ON) (ADDRESS=(PROTOCOL=TCP)(HOST=node1-vip.example.com)(PORT=1521)) (ADDRESS=(PROTOCOL=TCP)(HOST=node2-vip.example.com)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=EMREP)))"' -repos_user sysman`
LISTENER_PORT	Enter the listener port to connect to the existing database. For example, `1532`
SERVICENAME_OR_SID	Enter the service name or the system ID (SID) of the existing database. For example, `orcl`
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	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.
SYSMAN_CONFIRM_PASSWORD	Confirm the SYSMAN user account’s password.

Table 4–2 (Cont.) Editing Response File for Configuring Enterprise Manager Software

Parameter	Description
MANAGEMENT_ TABLESPACE_LOCATION	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 Cloud Control requires this data file to store information about the monitored targets, their metrics, and so on. Essentially, everything else other than configuration data, software library data, and audit data.
CONFIGURATION_DATA_ TABLESPACE_LOCATION	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 Cloud Control requires this data file to store configuration information collected from the monitored targets.
JVM_DIAGNOSTICS_ TABLESPACE_LOCATION	Enter the absolute path to a location where the data file for JVM Diagnostics data tablespace (`mgmt_ad4j.dbf`) can be stored. Ensure that the specified path leads up to the file name. For example, `/home/john/oradata/mgmt_ad4j.dbf` Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).
AGENT_REGISTRATION_ PASSWORD	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	Confirm the agent registration password.
STATIC_PORTS_FILE	By default, ports described in Section 2.1.6 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.

4.4.2.4 Performing Post-Configuration Tasks

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

Part III

Installing Oracle Management Agent

This part describes the different ways of installing Oracle Management Agent. In particular, this part contains the following chapters:

5

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 section covers the following:

- Overview
- Before You Begin
- Prerequisites
- Installation Procedure
- After You Install

5.1 Overview

Installing a Management Agent in silent mode is only an alternative to installing it using the Add Host Target Wizard. While the Add Host Target Wizard requires you to use its GUI-rich interview screens for providing all the installation details, the silent mode requires you to use a response file for providing the installation details and a deployment script (`agentDeploy.sh`) for silently installing the Management Agent using the information supplied in the response file.

The response file and the deployment script are available as part of the Management Agent software. Instead of creating a response file, you can also choose to pass the values as separate arguments while invoking the deployment script.

Installing in silent mode is best suited when you want to install an additional Management Agent on a destination host, from the destination host itself, and without using the Add Host Target Wizard in the Enterprise Manager Cloud Control console.

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

```
<installation_base_directory>
    |_____core
          |_____12.1.0.1.0
    |_____plugins
    |_____plugins.txt
    |_____plugins.txt.status
    |_____agent_inst
    |_____sbin
    |_____agentimage.properties
```

5.2 Before You Begin

Before you begin installing a Management Agent, keep these points in mind:

- Before installing the Management Agent, you must procure the Management Agent software from the OMS host and transfer it to the destination host for installation. The Management Agent software you procure contains the core binaries required for installation, the response file to be edited and passed, and the `agentDeploy.sh` script.

  By default, the OMS host contains the Management Agent software for the platform on which the OMS is running. For example, if the OMS host is Linux x86, then the Management Agent software available by default is only for Linux x86.

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

  For information on Self Update and how you can use it to download the software, see the chapter on Self Update in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- You can run the `agentDeploy.sh` script only from the destination host.
- You can install only on one host at a time using the `agentDeploy.sh` script, therefore use this approach when you want to install only on a few hosts.
- You can provide the installation details either in a response file or as values for individual arguments that can be passed while invoking the `agentDeploy.sh` script. However, Oracle recommends that you create a response file and capture the information there.
- You can install even if the OMS is unreachable. In this case, you must pass the special option `-forceConfigure` while invoking the `agentDeploy.sh` script. For more information, see Table 5–3.

  Typically, you will use this option only when you are installing the Management Agent before installing the OMS, and you know for sure that you will install the OMS later on the host and port mentioned in the response file.

  However, do not pass the option `-forceConfigure` when installing the Management Agent using software-only method as described in Chapter 9.

- You cannot run any preinstallation or postinstallation scripts as part of the installation process. Of course, you can run manually them after the installation ends.
- By default, the `agentDeploy.sh` script 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
- You must not install two Management Agents on the same host. This disrupts the communication with the OMS.

5.3 Prerequisites

Before installing the Management Agent, ensure that you meet the following prerequisites.

Table 5–1 Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Software Requirements	*(For Microsoft Windows)* Ensure that you have installed Cygwin on the destination host. For more information, see the chapter on installing Cygwin in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Operating System Requirements	Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager Certification Matrix available on *My Oracle Support*.
	To access this matrix, follow these steps:
	1. Log in to *My Oracle Support*, and click the **Certifications** tab.
	2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**.
	3. From the **Release** list, select **12.1.0.1.0**, and click **Search**.
	Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:
	`cat /etc/release`
	You should see the output similar to the following. Here, `s10s_u6` indicates that update 6 is already installed.
	`Solaris 10 10/08 s10s_u6wos_07b SPARC`

Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
User and Operating System Group Requirement	Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created. For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
/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: `12.123.123.12  mypc.cn.company.com  mypc`
SUDO Requirements	*(Only for UNIX)* Ensure that you have SUDO privileges to invoke `/bin/sh` as *root*.
PATH Environment Variable Requirements	(*For Microsoft Windows*) On the destination host, 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) on both the hosts.
Path Validation Requirements	Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Port Requirements	Ensure that the default ports described in Section 2.1.6.1 are free.

Table 5–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

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.
Installation Base Directory Requirements	Ensure that the installation base directory is empty. Ensure that the installing user owns the installation base directory. Ensure that the installer user or the root user owns all the parent directories. Ensure that the root user owns the root directory. For example, if the installation base directory is `/scratch/OracleHomes/agent`, and *oracle* is the installing user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or *root* user, and the root directory (`/`) must be owned by *root* user.
Agent Instance Home Requirements	Ensure that the agent instance home location you specify in the response file is empty.
Permission Requirements	■ Ensure that the installation base directory is empty, and ensure that you (in fact, all users accessing the Installation Base Directory) have *read* and *execute* permission on all the directories that lead up to the Installation Base Directory. For example, if the Installation Base Directory is `/home/john/oracle/software/agent/`, then you must have *read* and *execute* permissions on all the directories, mainly `home`, `john`, `oracle`, `software`, and `agent`. ■ 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. 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.

Table 5–1 (Cont.) Prerequisites for Installing Oracle Management Agent in Silent Mode

Requirement	Description
Central Inventory (oraInventory) Requirements	▪ Ensure that you allocate 100 MB of space for the Central Inventory. ▪ Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `/etc/oraInst.loc` file, ensure that the inventory location specified there is not pointing to a shared location. If it is, change it to a non-shared location by following the instructions outlined in *My Oracle Support* note 1092645.1. ▪ Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all remote 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 remote host, then ensure that you enter the path to an alternative inventory location using the `INVENTORY_LOCATION` or `-invPtrLoc` arguments as described in Table 5–3.
Agent User Account Permissions and Rights (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. ▪ Increase quotas. ▪ Replace process level token. ▪ Log in as a batch job. To verify whether the agent user has these rights, follow these steps: 1. Launch the Local Security Settings. 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 Settings**. 2. In the Local Security Settings window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**.
Permissions for cmd.exe (For Microsoft Windows)	(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`

5.4 Installation Procedure

To install a Management Agent in silent mode, follow these steps:

1. On the OMS host, from the OMS home, log in to the EMCLI client. EMCLI Client is available by default with every OMS installation, so you need not install the client separately.

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

For example,

```
$<OMS_HOME>/bin/emcli login -username=sysman
-password=2benot2be
```

Note: The user name must always be `sysman`. Do not enter any other user name.

2. Synchronize EMCLI:

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

3. Identify the platforms for which the Management Agent software is available on the OMS host:

   ```
   $<OMS_HOME>/bin/emcli get_supported_platforms
   ```

   This command lists all the platforms for which the Management Agent software is available on the OMS host. Example 5–1 shows a sample output of the command.

Example 5–1 Output Showing Software Availability for Different Platforms

```
--------------------------------------------------
Version = 12.1.0.1.0
Platform Name = Linux x86
--------------------------------------------------
Version = 12.1.0.1.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
--------------------------------------------------
Version = 12.1.0.1.0
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, download the software for the required platform using the Self Update console.

   For information on Self Update and how you can use it to download the software, see the chapter on Self Update in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

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

   ```
   $<OMS_HOME>/bin/emcli get_agentimage -destination=<download_
   directory> -platform="<platform>" -version=<version>
   ```

   For example,

   ```
   ./emcli get_agentimage -destination=/tmp -platform="Linux
   x86" -version=12.1.0.1.0
   ```

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 on the OMS host.

- `-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, you will see the file `12.1.0.1.0_AgentCore_46.zip`. For information on the contents of this core software, see Section 5.4.3.

5. 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 FTP software to transfer the file. For example, FileZilla.

6. On the destination host, extract the contents of the ZIP file using the unzip utility:

   ```
   unzip /tmp/<software_zip_file> -d <software_extract_location>
   ```

   For example,

   ```
   unzip /tmp/12.1.0.1.0_AgentCore_46.zip -d /tmp/agtImg
   ```

7. Edit the response file `agent.rsp` as described in Table 5–2.

   ```
   <software_extract_location>/agent.rsp
   ```

8. Invoke the deployment script and pass the response file:

   ```
   <software_extract_location>/agentDeploy.sh AGENT_BASE_
   DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_
   path_to_responsefile>
   ```

Note:

- Instead of creating a response file, if you choose to pass all the arguments explicitly while invoking the deployment script.

  However, the mandatory ones are `OMS_HOST`, `EM_UPLOAD_PORT`, and `AGENT_REGISTRATION_PASSWORD`.

  For example,

  ```
  /tmp/agtImg/agentDeploy.sh AGENT_BASE_
  DIR=/scratch/agent12c OMS_HOST=my.example.com EM_
  UPLOAD_PORT=14511 AGENT_REGISTRATION_
  PASSWORD=2bornot2b
  ```

- When you pass the arguments while invoking the deployment script, these values need not be given with double quotes. However, when you provide them in a response file, the values need to be in double quotes (except for the argument `b_startAgent`).
- In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see Section 5.4.2.

9. Run the root scripts when you are prompted. For more information, see Section 5.5.

5.4.1 Creating a Response File

Table 5–2 describes the various parameters you must include in the response file.

Table 5–2 Creating a Response File for Installing Oracle Management Agent in Silent Mode

Parameter	Description
OMS_HOST	Enter the OMS host name. For example, `OMS_HOST="my.omsserver.com"`
EM_UPLOAD_PORT	Enter the upload port (HTTP or HTTPS) for communicating with the OMS. For example, `EM_UPLOAD_PORT="14511"`
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 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 5–2 (Cont.) Creating a Response File for Installing Oracle Management Agent in Silent Mode

Parameter	Description
AGENT_INSTANCE_HOME	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="/john/oracle/instance_dir/inst_mydir"`
AGENT_PORT	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.
b_startAgent	Enter `TRUE` if you want the Management Agent to start automatically once it is installed and configured. Otherwise, enter `FALSE`. For example, `b_startAgent=TRUE`
ORACLE_HOSTNAME	Enter the fully qualified domain name of the host where you want to install the agent. For example, `ORACLE_HOSTNAME="my.agentserver.com"`
s_agentHomeName	Enter the name of the Oracle home you want to see created for the Management Agent. For example, `s_agentHomeName="agent12gR1"`
s_agentServiceName	Enter the customized Management Agent service name. If you leave this field blank, then it gets defaulted to *Oracle*+<oracle_home_name>+*Agent*.

5.4.2 Understanding the Options Supported by agentDeploy.sh Script

Table 5–3 lists the options supported by the `agentDeploy.sh` script.

Table 5–3 Understanding the Options Supported by agentDeploy.sh Script

Options	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.
-invPtrLoc	Considers the Oracle Inventory directory for storing inventory details. Enter the absolute path to the `oraInst.loc` file that contains the location of the `OraInventory` directory. **Important:** If you enter a value for this option, do NOT use the `INVENTORY_LOCATION` option.
INVENTORY_LOCATION	Considers the Oracle Inventory directory for storing inventory details. Enter the absolute path to the `OraInventory` directory. **Important:** ■ If you enter a value for this option, do NOT use the `-invPtrLoc` option. ■ Do NOT use this option if you already have the `/var/opt/oracle/oraInst.loc` on HP and Solaris platforms, and `/etc/oraInst.loc` file on all other UNIX platforms.
-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 Chapter 9. **Note:** This option does not apply if you are cloning using a ZIP file.
-configOnly	Configures the software binaries, and does not install any software binaries. Use this when you have performed a software-only installation using the `-softwareOnly` option, so that only the configuration is done to the copied software binaries. For more information, see Chapter 9. **Note:** This option does not apply if you are cloning using a ZIP file.

Table 5–3 (Cont.) Understanding the Options Supported by agentDeploy.sh Script

Options	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.

5.4.3 Understanding the Contents of the Downloaded Management Agent Software

Table 5–4 describes the contents of the core Management Agent software you download before installing the Management Agent.

Table 5–4 Contents of the Downloaded Management Agent Software

Files	Description
12.1.0.1.0_PluginsOneoffs_<platform id>.zip	Plug-in ZIP file containing all the discovering plug-ins, which were installed with the OMS, Oracle Home discovery plug-in, and Oracle Home monitoring plug-in.
agentcoreimage.zip	Archived ZIP file containing the core agent bits and agent set-uid binaries.
agentDeploy.sh	Shell 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.

5.5 After You Install

After you install the Management Agent, follow these steps:

1. (Only for UNIX Operating Systems) When prompted, manually run the following scripts as a *root* user. If you do not have SUDO privileges, then request your Administrator who has the privileges to run these 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 `root.sh` script from the Management Agent home:

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

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:

   ```
   $<INSTANCE_HOME>/bin/emctl status agent
   ```

   Note: If the status of the Management Agent is down for some reason, then manually start the Management Agent by running the following command from its Oracle home:

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

   b. Navigate to the Management Agent home and run the following command to see a message that confirms that EMD upload completed successfully:

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

3. Verify if all the plug-ins were installed successfully. To do so, access the following log file from the Management Agent home, and search for the sentence *WARN:Plugin configuration has failed*.

   ```
   $<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger-<timestamp>.log
   ```

   If you find the sentence, resolve the issue by running the `AgentPluginDeploy.pl` script from the Management Agent home. In this command, all `<AGENT_HOME>` references refer to the Management Agent home.

   ```
   $<AGENT_HOME>/perl/bin/perl <AGENT_
   HOME>/bin/AgentPluginDeploy.pl -oracleHome <AGENT_HOME>
   -agentDir <AGENT_BASE_DIR> -pluginIdsInfoFile <AGENT_BASE_
   DIR>/plugins.txt -action configure -emStateDir <AGENT_
   INSTANCE_HOME>
   ```

   For example,

   ```
   /home/john/programs/oracle/EMGC_Main_
   20SH/agent/core/12.1.0.1.0/perl/bin/perl
   /home/john/programs/oracle/EMGC_Main_
   20SH/agent/core/12.1.0.1.0/bin/AgentPluginDeploy.pl
   -oracleHome /home/john/programs/oracle/EMGC_Main_
   20SH/agent/core/12.1.0.1.0 -agentDir
   /home/john/programs/oracle/EMGC_Main_20SH/agent
   ```

```
-pluginIdsInfoFile /home/john/programs/oracle/EMGC_Main_
20SH/agent/core/12.1.0.1.0/sysman/install/plugins.txt -action
configure -emStateDir /home/john/programs/oracle/EMGC_Main_
20SH/agent/agent_inst
```

4. By default, the host and the Management Agent get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

   To monitor the other targets, you need to add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

   For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

6

Installing Oracle Management Agent Using RPM File

This chapter describes how you can install Oracle Management Agent (Management Agent) using its `.rpm` file. In particular, this section covers the following:

6.1 Overview

Installing a Management Agent using its `.rpm` file is primarily a silent way of installing a Management Agent. In this method, you download the `.rpm` file to a temporary directory on the destination host, and install it directly on the destination host without using any response file. Since you install it directly on the destination host, it is best suited for installing a few Management Agents, one at a time.

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

```
<installation_base_directory>
    |_____core
          |_____12.1.0.1.0
    |_____plugins
    |_____agent_inst
    |_____sbin
    |_____plugins.txt
    |_____agentimage.properties
```

Note: 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

6.2 Before You Begin

Before you begin installing a Management Agent, keep these points in mind:

- Agent RPM is available only for Linux 32-bit and Linux 64-bit platforms.
- You procure the Management Agent software from the OMS host and transfer it to the destination host for installation. The Management Agent software contains the core binaries required for installation, the response file to be edited and passed, and the `configure.pl` script.

  By default, the OMS host contains the Management Agent software for the platform on which the OMS is running. For example, if the OMS host is Linux x86, then the Management Agent software available by default is only for Linux x86.

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

  For information on Self Update and how you can use it to download the software, see the chapter on Self Update in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
- You can install only on one host at a time, therefore use this approach when you want to install only on a few hosts.
- You cannot run any preinstallation or postinstallation scripts as part of the installation process. Of course, you can run manually them after the installation ends.
- By default, the `.rpm` file 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
- You must not install two Management Agents on the same host. This disrupts the communication with the OMS.

6.3 Prerequisites

Before installing the Management Agent, ensure that you meet the following prerequisites.

Table 6–1 Prerequisites for Installing Oracle Management Agent Using RPM File

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent Using RPM File

Requirement	Description

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 this matrix, follow these steps:
	1. Log in to *My Oracle Support*, and click the **Certifications** tab.
	2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**.
	3. From the **Release** list, select **12.1.0.1.0**, and click **Search**.
	Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:
	`cat /etc/release`
	You should see the output similar to the following. Here, `s10s_u6` indicates that update 6 is already installed.
	`Solaris 10 10/08 s10s_u6wos_07b SPARC`

Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
User and Operating System Group Requirement	Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created. For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Permission Requirements	Ensure that the agent base directory you specify in the properties file is empty and has *write* permission
Path Validation Requirements	Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
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.
Installation Base Directory Requirements	Ensure that the installing user owns the installation base directory. Ensure that the installer user or the root user owns all the parent directories. Ensure that the root user owns the root directory. For example, if the installation base directory is `/scratch/OracleHomes/agent`, and *oracle* is the installing user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or *root* user, and the root directory (`/`) must be owned by *root* user.

Table 6–1 (Cont.) Prerequisites for Installing Oracle Management Agent Using RPM File

Requirement	Description
Permission Requirements	■ Ensure that you (in fact, all users accessing the Installation Base Directory) have *read* and *execute* permission on all the directories that lead up to the installation base directory. For example, if the Installation Base Directory is `/home/john/oracle/software/agent/`, then you must have *read* and *execute* permissions on all the directories, mainly `home`, `john`, `oracle`, `software`, and `agent`. ■ Ensure that the `/usr/lib/oracle` directory exists and it has *write* permission.
Port Requirements	Ensure that the default ports described in Section 2.1.6.1 are free.
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 for the Central Inventory. ■ Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `/etc/oraInst.loc` file, ensure that the inventory location specified there is not pointing to a shared location. If it is, change it to a non-shared location by following the instructions outlined in *My Oracle Support* note 1092645.1. ■ Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all remote hosts.

6.4 Installation Procedure

To install a Management Agent using its `.rpm` file, follow these steps:

1. On the OMS host, from the OMS home, log in to the EMCLI client. EMCLI Client is available by default with every OMS installation, so you need not install the client separately.

   ```
   $<OMS_HOME>/bin/emcli login -username=<username>
   -password=<password>
   ```

   For example,

   ```
   $<OMS_HOME>/bin/emcli login -username=sysman
   -password=2benot2be
   ```

2. Synchronize EMCLI:

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

3. Identify the platforms for which the Management Agent software is available on the OMS host:

   ```
   $<OMS_HOME>/bin/emcli get_supported_platforms
   ```

   This command lists all the platforms for which the Management Agent software is available on the OMS host. Example 6–1 shows a sample output of the command.

Example 6–1 Output Showing Software Availability for Different Platforms

```
-------------------------------------------------
Version = 12.1.0.1.0
Platform Name = Linux x86
-------------------------------------------------
Version = 12.1.0.1.0
Platform Name = Oracle Solaris on x86-64 (64-bit)
-------------------------------------------------
Version = 12.1.0.1.0
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, download the software for the required platform using the Self Update console.

For information on Self Update and how you can use it to download the software, see the chapter on Self Update in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

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

```
$<OMS_HOME>/bin/emcli get_agentimage_rpm
-destination=<download_directory> -platform="<platform>"
-version=<version>
```

For example,

```
./emcli get_agentimage_rpm -destination=/tmp -platform="Linux
x86" -version=12.1.0.1.0
```

Note: 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.

  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 `.rpm` file; this must match one of the platforms listed in the previous step for which the software is available on the OMS host.

- `-version` is the version of the Management Agent for which you want to download the `.rpm` file; this is an optional argument. If you do not pass this argument, then the version is defaulted to the OMS version.

The command downloads the `.rpm` file of the core Management Agent to the destination directory you entered. For example, `oracle-agt-12.1.0.1.0-1.0.i386.rpm`

5. 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 FTP software to transfer the file. For example, FileZilla.
6. On the destination host, run the `.rpm` file as a *root* user to install the Management Agent:

   ```
   rpm -ivh <download_directory>/<rpm_file>
   ```

   For example,

   ```
   rpm -ivh /tmp/oracle-agt-12.1.0.1.0-1.0.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/config.pl
   ```

7. Edit the `agent.properties` file as described in Table 6–2. The file is availabe in the following location:

   ```
   /usr/lib/oracle/agent/agent.properties
   ```

8. Run the following command to complete the installation:

   ```
   /etc/init.d/config.pl
   ```

6.4.1 Editing agent.properties File

Table 6–2 describes the various parameters you must include in the response file.

Table 6–2 Creating a Response File for Installing Oracle Management Agent Using an RPM File

Parameter	Description
s_OMSHost	*(Mandatory)* Enter the host name of the OMS to which you want to connect.
s_OMSPort	*(Mandatory)* Enter the upload port (HTTP or HTTPS) to communicate with the OMS.
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 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.
agentUserName	*(Mandatory)* Enter the user name with which you want to install the Management Agent.
agentUserGroup	*(Mandatory)* Enter the group to which the Management Agent user should belong.

Table 6–2 (Cont.) Creating a Response File for Installing Oracle Management Agent Using an RPM File

Parameter	Description
OraInvLoc	*(Optional)* Enter the absolute path to the Central Inventory where the Management Agent user has *write* permission. For example, `OraInvLoc =/usr/lib/oraInventory`

BASEDIR	*(Optional)* Enter the absolute path to the installation base directory where you want to install the Management Agent.
	For example,
	`/home/john/oracle/agent`
	If you do not enter the path to the installation base directory, then by default, the Management Agent is installed in the following location:
	`/usr/lib/oracle/core/12.1.0.1.0`

ORACLE_HOSTNAME	*(Only for Virtual Hosts)* Enter the virtual host name where you want to install the Management Agent.

6.5 After You Install

After you install the Management Agent, follow these steps:

1. Verify the installation:

   a. Navigate to the Management Agent instance home and run the following command to see a message that confirms that the Management Agent is up and running:

   ```
   $<INSTANCE_HOME>/bin/emctl status agent
   ```

   Note: If the status of the Management Agent is down for some reason, then manually start the Management Agent by running the following command from the Management Agent instance home:

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

   b. Navigate to the Management Agent and run the following command to see a message that confirms that EMD upload completed successfully:

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

2. Verify if all the plug-ins were installed successfully. To do so, access the following log file from the Management Agent home, and search for the sentence *WARN:Plugin configuration has failed*.

   ```
   $<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger-<timestamp>.log
   ```

   If you find the sentence, resolve the issue by running the `AgentPluginDeploy.pl` script from the Management Agent home.

   ```
   $<AGENT_HOME>/perl/bin/perl <AGENT_
   HOME>/bin/AgentPluginDeploy.pl -oracleHome <AGENT_HOME>
   -agentDir <AGENT_BASE_DIR> -pluginIdsInfoFile <AGENT_BASE_
   DIR>/plugins.txt -action configure -emStateDir <AGENT_
   INSTANCE_HOME>
   ```

For example,

```
/home/john/programs/oracle/EMGC_Main_
20SH/agent/core/12.1.0.1.0/perl/bin/perl
/home/john/programs/oracle/EMGC_Main_
20SH/agent/core/12.1.0.1.0/bin/AgentPluginDeploy.pl
-oracleHome /home/john/programs/oracle/EMGC_Main_
20SH/agent/core/12.1.0.1.0 -agentDir
/home/john/programs/oracle/EMGC_Main_20SH/agent
-pluginIdsInfoFile /home/john/programs/oracle/EMGC_Main_
20SH/agent/core/12.1.0.1.0/sysman/install/plugins.txt -action
configure -emStateDir /home/john/programs/oracle/EMGC_Main_
20SH/agent/agent_inst
```

3. By default, the host and the Management Agent get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

   To monitor the other targets, you need to add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

   For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

7

Cloning Oracle Management Agent

This chapter explains how you can clone an existing Oracle Management Agent (Management Agent). In particular, this section covers the following:

7.1 Overview

Oracle Management Agent (Management Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to monitor the targets running on that managed host.

Therefore, if you want to monitor a target running on a host, you must first convert that unmanaged host to a managed host by installing an Oracle Management Agent, and then manually discover the targets running on it to start monitoring them.

However, the Management Agent you install using other installation types is always a fresh installation without any customized configuration that you had done or interim one-off patches that you had applied to other running Management Agents.

If you want to install an additional Management Agent that is identical to the existing well-tested, pre-patched, and running Management Agent, then the best option is to clone the existing instance. This saves time and effort in patching a fresh installation all over again and bringing it to the current state.

You can clone an existing Management Agent in graphical or silent mode.

- In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. The wizard enables you to select a source Management Agent, which you want to clone, and identify one or more remote hosts on which you want to clone it.

  The wizard first copies the source Management Agent image to the host on which Oracle Management Service (OMS) is running, and then, it transfers that copied image to the destination hosts. Although the wizard can be used for remotely cloning one, single Management Agent, it is best suited for mass-deployment of Management Agents, particularly while mass-deploying Management Agents of different releases on hosts of different platforms.

- In silent mode, you use a compressed file (ZIP), which you transfer. Understandably, this is a much easier method because you compress the Oracle home of an existing Management Agent and transfer it to the destination host without having to specify any parameters or values in an interview screen, but still retaining all its configuration settings and applied one-off patches.

  However, in silent mode, you can install only on one destination host at any given time. Once you are done with cloning of a Management Agent on a host, you must redo the procedure to clone on another host. Therefore, you cannot clone on multiple hosts simultaneously, and as a result, this approach is best suited when you want to clone only on a few hosts, one host after the other.

Understandably, as a prerequisite, you need to have at least one Management Agent in your environment, and its software binaries must be accessible from all the hosts where you want to clone an additional Management Agent. Therefore, note that this installation type must be used for installing only additional Management Agents in your environment.

After installing a Management Agent, to monitor a target, add the target to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

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

```
<installation_base_directory>
    |_____core
          |_____12.1.0.1.0
    |_____plugins
    |_____plugins.txt
    |_____agent_inst
    |_____sbin
    |_____agentimage.properties
```

7.2 Before You Begin

Before you begin installing an Oracle Management Agent, keep these points in mind:

- *(Only for Graphical Mode)* The Add Host Targets Wizard converts an unmanaged host to a managed host in the Enterprise Manager system by cloning an existing Oracle Management Agent.
- Oracle Management Agent 12*c* communicates only with Oracle Management Service 12*c* and not with any earlier release of Enterprise Manager.
- *(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.
- While cloning, the source Management Agent is not shut down.
- *(Only for Graphical Mode)* If you have multiple hosts, sharing a common mounted drive, then install the Management Agents in two different phases:

1. First, clone the Management Agent to the host where the drive is shared by selecting the deployment type **Clone Existing Agent** in the Add Host Targets Wizard. Follow the instructions outlined in this chapter.
2. Then, install a Management Agent on all other hosts that access the shared, mounted drive by selecting the deployment type **Add Host to Shared Agent** in the Add Host Targets Wizard. (Here, you will select the Management Agent you installed in the previous step.) For more information, follow the instructions outlined in Chapter 8.

- Cloning on shared clusters is NOT supported. If you have an Oracle RAC Cluster with multiple nodes, then you must clone the Management Agent on each of the nodes separately. In other words, in the Add Host Targets Wizard, you must add each node explicitly as a destination host.
- *(Only for Graphical Mode)* The Add Host Targets Wizard uses SSH to establish connectivity between Oracle Management Service (OMS) and the remote hosts where you want to install the Management Agents
- *(Only for Graphical Mode)* Only SSH1 (SSH version 1) and SSH2 (SSH version 2) protocols offered by OpenSSH are supported for deploying a Management Agent.
- *(Only for Graphical Mode)* SSH public key authentication and password-based authentication are supported. So you can use an existing SSH public key authentication without exposing your passwords. You can provide a dummy password in the wizard, and the wizard will internally use the underlying public key infrastructure to perform the installation.
- *(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 root 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, and set it to run as User_X that has the root privileges. In this case, the wizard logs in to the hosts as User_A, but clones as User_X.
- By default, the Add Host Targets Wizard configures only the following types of plug-ins:
  - All plug-ins that were configured with the Management Agent you are cloning.
  - Oracle Home discovery plug-in
  - Oracle Home monitoring plug-in
- 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.
- You must not install two Management Agents on the same host. This disrupts the communication with the OMS.

7.3 Prerequisites

Before cloning the Management Agent, ensure that you meet the following prerequisites.

Table 7–1 Prerequisites for Cloning Oracle Management Agent

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Software Requirements *(Only for Graphical Mode)*	*(For Microsoft Windows)* Ensure that you have installed Cygwin on the destination host. For more information, see the chapter on installing Cygwin in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Operating System Requirements	Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager Certification Matrix available on *My Oracle Support*.
	To access this matrix, follow these steps:
	1. Log in to *My Oracle Support*, and click the **Certifications** tab.
	2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**.
	3. From the **Release** list, select **12.1.0.1.0**, and click **Search**.
	Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:
	`cat /etc/release`
	You should see the output similar to the following. Here, `s10s_u6` indicates that update 6 is already installed.
	`Solaris 10 10/08 s10s_u6wos_07b SPARC`

Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
User and Operating System Group Requirement	Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created. For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
/etc/hosts File Requirements *(Only for Silent Mode)*	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: `12.123.123.12 mypc.cn.company.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 `mypc.cn.company.com` and the short name is `mypc`, then add the following line in the `/etc/hosts` file: `12.123.123.12 mypc.cn.company.com mypc`

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

Requirement	Description
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.
Permission Requirements	■ Ensure that the installation base directory you specify is empty and has *write* permission. ■ Ensure that the instance directory is empty and has *write* permission.
SUDO Requirements	*(Only for UNIX)* Ensure that the installing user has SUDO privileges to invoke `/bin/sh` as *root*.
PATH Environment Variable Requirements	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*) Ensure that the SCP binaries (for example, /usr/local/bin/scp) are in the `PATH` environment variable.
Path Validation Requirements	Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
IPV 6 Requirements *(Only for Graphical Mode)*	If you are installing from an ipv6 OMS to a non-ipv6 host, then follow these step: 1. Navigate to the following location on the OMS home: `$<OMS_HOME>/oui/prov/resources/` 2. Check the property value of PING_PATH in the following files in this order: a. ssPaths_<plat>.properties b. sPaths.properties c. Paths.properties 3. Change the property value of PING_PATH from `/bin/ping` to `/bin/ping6`
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.

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

Requirement	Description
Installation Base Directory Requirements	Ensure that the installing user owns the installation base directory. Ensure that the installer user or the root user owns all the parent directories. Ensure that the root user owns the root directory. For example, if the installation base directory is `/scratch/OracleHomes/agent`, and *oracle* is the installing user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or *root* user, and the root directory (`/`) must be owned by *root* user.
Read and Execute Permission Requirements	Ensure that you (in fact, all users accessing the Installation Base Directory) have *read* and *execute* permission on all the directories that lead up to the Installation Base Directory. For example, if the Installation Base Directory is `/home/john/oracle/software/agent/`, then you must have *read* and *execute* permissions on all the directories, mainly `home`, `john`, `oracle`, `software`, and `agent`.

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 port, run the following command:
	
	`netstat -anp | grep <port_no>`
	
	If the port is a non-default port, that is, any port other than 22, then update the `SSH_PORT` property in the following file that is present in the OMS home:
	
	`$<OMS_HOME>/oui/prov/resources/Paths.properties`

Ping Requirements
 	
(Only for Graphical Mode)
	If a firewall configured in your environment does not allow any ping traffic, then ensure that you do the following:
	
	1. Take a backup of the following file from the OMS home:
	
	For Linux Platforms:
	
	`$<OMS_ HOME>/oui/prov/resources/sPaths.properties`
	
	For Other Platforms:
	
	`$<OMS_HOME>/oui/prov/resources/ssPaths_ <platform>.properties`
	
	For example, `ssPaths_aix.properties` if the OMS is on AIX platform.
	
	2. Edit the original properties file and change `PING_ PATH=/bin/ping` to `PING_PATH=/bin/true`.

Software Availability Requirements *(Only for Graphical Mode)*	**For Cloning an Existing Management Agent** Ensure that you already have Oracle Management Agent 12*c* running in your environment. Ensure that the platform on which it is running is the same as the platform of the destination hosts on which you want to clone. **For Installing a Management Agent Using Shared Oracle Home** Ensure that you already have Oracle Management Agent 12*c* installed as a *Master Agent* in a shared, mounted location
Installation Base Directory Requirements *(Only for Graphical Mode)*	Ensure that the installation base directory you specify is empty and has *write* permission.

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

Requirement	Description

plugins.txt File Update Requirements
(Only for Silent Mode)
	(Only if you installed additional plug-ins to the Management Agent later)
	By default, when you install a Management Agent, it is automatically configured with the Oracle Home discovery plug-in, the Oracle Home monitoring plug-in, and all the discovery plug-ins that were configured with the OMS from where the Management Agent is being deployed. However, if you install any additional plug-ins later, then follow these steps:
	1. Edit the `plugins.txt` file from the installation base directory.
	2. Add entries in the following format for every additional plug-in you installed:
	`<plug-in_name>|<plug-in_version>|<plug-in_type>`
	For example,
	`oracle.sysman.oh|12.1.0.1.0||discovery`
	Note: To find the plug-in name, plug-in version, and plug-in type, see the `plugins` directory in the installation base directory. For each plug-in, you should see a subdirectory titled based on the plug-in name, type, and version.
	For example, `oracle.sysman.db.discovery.plugin_12.1.0.1.0`
	Here, `oracle.sysman.db` is the plug-in name, `discovery` is the plug-in type, and `12.1.0.1.0` is the plug-in version.
	3. Save the `plugins.txt` file.

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 for the Central Inventory.
	■ Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `/etc/oraInst.loc` file, ensure that the inventory location specified there is not pointing to a shared location. If it is, change it to a non-shared location by following the instructions outlined in *My Oracle Support* note 1092645.1.
	■ Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all remote hosts. If you do not have these permissions on the default inventory (typically at `/etc/oraInst.loc`) on any remote host, then ensure that you specify the path to an alternative inventory location by using one of the following options in the Additional Parameters field of the Add Host Targets Wizard:
	`INVENTORY_LOCATION=<absolute_path_to_inventory_directory>`
	`-invPtrLoc <absolute_path_to_oraInst.loc>`

Port Requirements	Ensure that the default ports described in Section 2.1.6.1 are free.

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

Requirement	Description
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. ■ Increase quotas. ■ Replace process level token. ■ Log in as a batch job. To verify whether the agent user has these rights, follow these steps: **1.** Launch the Local Security Settings. 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 Settings**. **2.** In the Local Security Settings window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**.
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`
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.

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

Requirement	Description
Browser Requirements *(Only for Graphical Mode)*	■ Ensure that you use a certified browser as mentioned in the Enterprise Manager Certification Matrix available on *My Oracle Support*. To access this matrix, follow these steps: 1. Log in to *My Oracle Support*, and click the **Certifications** tab. 2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**. 3. From the **Release** list, select **12.1.0.1.0**, and click **Search**. ■ If you use Microsoft Internet Explorer 8 or 9, do the following: ■ Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the **Tools** menu, click **Compatibility View** to disable it if it is enabled. Also, click **Compatibility View Settings** and deregister the Enterprise Manager Cloud Control console URL. ■ Enable XMLHTTP. To do so, from the **Tools** menu, click **Internet Options**. Click the **Advanced** tab, and under the **Security** heading, select **Enable native XMLHTTP support** to enable it.

7.4 Cloning Procedure

This section describes the following:

- Cloning in Graphical Mode
- Cloning in Silent Mode

7.4.1 Cloning in Graphical Mode

To clone a Management Agent in graphical mode, follow these steps:

1. In Cloud Control, do one of the following:
   - From the **Setup** menu, select **Add Target**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.
   - From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.
2. On the Host and Platform page, do the following:

a. Accept the default name assigned for this session or enter a unique name of your choice. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name. For example, `add_host_operation_1`

   A unique deployment activity name enables you to save the cloning details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.

b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to clone the Management Agent.

   Note:

   - Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
   - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
   - You must ensure that the host name you enter does not have underscores.

   Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager. For information on how the host name entries must appear in the host file, see Section 7.4.1.2.

   Note: When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

   As you can clone only if the source host and destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

   Note: If you are cloning a Management Agent on a platform that is different from the platform on which the OMS is running, then ensure that you have the software for that platform. If you do not have that software, then go to the Self-Update page within Enterprise Manager Cloud Control, and download the software.

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: If you have multiple hosts sharing a common mounted drive, then install the Management Agents in two different phases:

1. In the Add Host Targets Wizard, select the deployment type **Clone Existing Agent**, and clone the Management Agent to the host where the drive is shared.
2. In the Add Host Targets Wizard, select the deployment type **Add Host to Shared Agent**, and install a Management Agent on all other hosts that access the shared, mounted drive. (Here, you will select the Management Agent you cloned in the previous step as the master agent or shared agent.)

---

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 base directory where you want the software binaries, security files, and inventory files of Management Agent to be copied.

For example, `/usr/home/software/oracle/agentHome`.

Note: Ensure that the installation base directory you enter 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.

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 the SSH connectivity between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.

f. For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

If you leave this field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see Section 7.5.

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

Note: In the Privilege Delegation setting, the `%RUNAS%` is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

The custom port you enter must not be busy. If you are not sure, you can leave this field blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

If you want to run the script as `root`, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see Table 7–2.

   For example, if you want to provide the inventory pointer location file, then enter `-invPtrLoc` followed by the absolute path to the file location.

j. Repeat Step 3 (b) to Step 3 (i) for every other row you have in the table.

k. Click **Next**.

4. On the Review page, review the details you have provided and if you are satisfied with the details, then click **Deploy Agent** to clone the Management Agent.

   If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

   When you click **Deploy Agent** and submit the deployment session, you are automatically taken to the Add Host Status page that enables you to monitor the progress of the deployment session.

Note: On the Add Host Status page, if you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:

```
$<OMS_
HOME>/sysman/prov/agentpush/<timestampdir>/applogs/d
eployfwk.log
```

This error usually occurs when the job system is not enabled on the source Management Agent you are cloning. Ensure that the job system is enabled.

7.4.1.1 Supported Additional Parameters

Table 7–2 lists the additional parameters supported for cloning a Management Agent.

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`
-invPtrLoc	Enter the absolute path to the inventory file that has the location of the Central Inventory (oraInventory). For example, `-invPtrLoc /tmp/oraInst.loc`
s_agentServiceName	*(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, `DBAgent`

Table 7–2 (Cont.) Supported Additional Parameters

Parameter	Description
EM_STAGE_DIR	Enter the absolute path to a custom location that can be created as a temporary Provisioning Advisor Framework (PAF) staging directory. By default, every time you install a Management Agent, a PAF staging directory is created for copying the Software Library entities related to the deployment procedures. By default, this location is the scratch path location (`/tmp`). The location is used only for provisioning activities—entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends. If you want to override this location with a custom location, you can pass this option and enter a custom location. For example, `EM_STAGE_DIR=/home/john/software/oracle/pafdir`

7.4.1.2 Format of Host List File

In the Add Host Targets Wizard, you can click **Load from File** to add the hosts listed in a file. However, ensure that the file you select has one of the following formats:

- Only the host name.

  For Example,

  ```
  host1.example.com

  host2.example.com
  ```

- The host name followed by the platform name.

  For Example,

  ```
  host1.example.com linux

  host2.example.com aix
  ```

  The supported platform names are linux_x64, linux, solaris, hpunix, hpi, linux_zseries64, aix, linux_ppc64, windows_x64, solaris_x64, win32.

7.4.2 Cloning in Silent Mode

To clone a Management Agent manually, follow these steps:

1.
2. Set the following environment variables as described in Table 7–3.
3. Navigate to the temporary directory:

   ```
   cd $T_WORK
   ```

4. Create an interim ZIP file compressing the directories and files present in the Management Agent home:

   ```
   zip -r agentcoreimage.zip $AGENT_BASE_DIR/core $AGENT_BASE_
   DIR/sbin $AGENT_BASE_DIR/plugins $AGENT_BASE_DIR/plugins.txt
   $AGENT_BASE_DIR/agentimage.properties
   ```

5. Copy the `agentDeploy.sh` to the temporary directory:

   ```
   cp $AGENT_HOME/sysman/install/agentDeploy.sh .
   ```

6. Copy the UNZIP utility to the temporary directory:

```
cd $AGENT_HOME/bin/unzip .
```

7. Copy the `agentimage.properties` to the temporary directory:

   ```
   cd $AGENT_BASE_DIR/agentimage.properties .
   ```

8. Create the final ZIP file with all the contents to be transferred, in the temporary directory:

   ```
   zip -r agent.zip $T_WORK/*
   ```

9. Transfer the ZIP file to the installation base directory of the destination host using a file transfer utility (for example, FTP).

10. Extract the contents of the ZIP file.

11. Create a response file titled `agent.rsp` (in the same directory) as described in Table 5–2.

    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.

12. Invoke the deployment script and pass the response file:

    ```
    <Installation_Base_Directory>/agentDeploy.sh AGENT_BASE_
    DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_
    path_to_responsefile>
    ```

    Note:

    - Instead of creating a response file, if you choose to pass the values in separate arguments, then invoke the deployment script with some mandatory arguments in the following way:

      ```
      <Installation_Base_Directory>/agentDeploy.sh
      AGENT_BASE_DIR=<absolute_path_to_agentbasedir>
      OMS_HOST=<oms_hostname> EM_UPLOAD_PORT=<em_
      upload_port> AGENT_REGISTRATION_
      PASSWORD=<password>
      ```

    - In addition to passing the agent base directory and a response file (or individual mandatory arguments with installation details), you can also pass other options that are supported by the deployment script. For more information, see Section 5.4.2.

7.4.2.1 Setting Environment Variables for Cloning Agent Using ZIP File

Table 7–3 lists the environment variables you need to set and describes how you can set them.

Table 7–3 Setting Environment Variables for Cloning Agent Using ZIP File

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/app/Oracle/software/agent ▪ 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/app/Oracle/software/agent
AGENT_ HOME	Set it to the Oracle home of the Management Agent. For example, `/u01/app/Oracle/software/agent/core/12.1.0.1.0`	▪ In bash terminal, run the following command: export AGENT_HOME=<absolute_path_ to_agent_home> For example, export AGENT_ HOME=/u01/app/Oracle/software/agent /core/12.1.0.1.0 ▪ In other terminals, run the following command: setenv AGENT_HOME <absolute_path_to_ agent_home> For example, setenv AGENT_HOME /u01/app/Oracle/software/agent/core/1 2.1.0.1.0
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

7.5 After You Clone

After you clone the Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization**, **Remote Prerequisite Check**, and **Agent Deployment**.

Note: In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.

If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

- Ignore the warning or failure, and continue with the session if you prefer.
  - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select Continue, Ignoring Failed Hosts.
  - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do, click **Continue** and select **Continue, All Hosts**.
- Fix the problem by reviewing the error description carefully, understanding its cause, and taking action as recommended by Oracle.
  - You can choose to retry the deployment of Management Agents with the same installation details. To do so, click **Retry** and select Retry Using Same Inputs.
  - You can retry the deployment of Management Agents with modified installation details. To do so, click **Retry** and select Update Inputs and Retry.

Note: If you see the error message *Copying Source Agent Image Failed*, then refer to the following log file in the OMS home:

```
$<OMS_
HOME>/sysman/prov/agentpush/<timestampdir>/applogs/d
eployfwk.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. Verify the installation as described in Section 5.5.

8

Installing Shared Agent

This chapter describes how you can install a *Shared Agent* with the help of a central, shared Oracle home location of an existing Oracle Management Agent (Management Agent) that is installed on an NFS-mounted drive.

8.1 Overview

If you want to install additional Management Agents on hosts that share a mounted drive where a Management Agent is already installed, then the best option is to use the software binaries of the shared Oracle home from the mounted drive and configure the remote hosts to be managed by that Management Agent, thus capitalizing on the NFS visibility and saving hard disk space on the remote hosts.

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 the *Shared Agents* or *NFS Agents*.

You can install a *Shared Agent* in graphical or silent mode. In graphical mode, you use the Add Host Targets Wizard that is accessible from within the Enterprise Manager Cloud Control console. In silent mode, you use the `AgentNFS.pl` script.

The wizard and the script use the software binaries from the shared Oracle home and configure an instance directory on each of the destination hosts for storing configuration files such as `emd.properties`, `targets.xml`, `log files`, and so on.

> **Note:** 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 at a given time. Therefore, if you want to install only a few Management Agents, then use the `AgentNFS.pl` script

8.2 Before You Begin

Before you begin, 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.
- The *Shared Agent* can communicate only with Oracle Management Service 12*c* and not with any earlier release of Enterprise Manager.
- 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. Therefore, if you have hosts running on different platforms, then you must have one deployment session per platform.
- 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)* SSH public key authentication and password-based authentication are supported. So you can use an existing SSH public key authentication without exposing your passwords. You can provide a dummy password in the wizard, and the wizard will internally use the underlying public key infrastructure to perform the installation.
- *(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 root 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, and set it to run as User_X that has the root privileges. In this case, the wizard logs in to the hosts as User_A, but installs as User_X.
- By default, the Add Host Targets Wizard 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
- You must not install two Management Agents on the same host. This disrupts the communication with the OMS.

8.3 Prerequisites

Before installing a *Shared Agent*, ensure that you meet the following prerequisites:

Table 8–1 Prerequisites for Installing Shared Agent

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Software Requirements *(Only for Graphical Mode)*	*(For Microsoft Windows)* Ensure that you have installed Cygwin on the destination host. For more information, see the chapter on installing Cygwin in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Operating System Requirements	Ensure that you install the Management Agent only on certified operating systems as mentioned in the Enterprise Manager Certification Matrix available on *My Oracle Support*.
	To access this matrix, follow these steps:
	1. Log in to *My Oracle Support*, and click the **Certifications** tab.
	2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**.
	3. From the **Release** list, select **12.1.0.1.0**, and click **Search**.
	Note: If you use Oracle Solaris 10, then ensure that you have update 9 or higher installed. To verify whether it is installed, run the following command:
	`cat /etc/release`
	You should see the output similar to the following. Here, `s10s_u6` indicates that update 6 is already installed.
	`Solaris 10 10/08 s10s_u6wos_07b SPARC`

Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
User and Operating System Group Requirement	Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created. For more information, see the chapter on creating operating system groups and users in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
Software Availability Requirements	Ensure that you already have Oracle Management Agent 12*c* installed as a *Master Agent* in a shared, mounted location
/etc/hosts File Requirements *(Only for Silent Mode)*	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: `12.123.123.12  mypc.cn.company.com  mypc`

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

Requirement	Description
Destination Host Requirements *(Only for Graphical Mode)*	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 `mypc.cn.company.com` and the short name is `mypc`, then add the following line in the `/etc/hosts` file: `12.123.123.12 mypc.cn.company.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.
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.
Installation Base Directory Requirements	Ensure that the installing user owns the installation base directory. Ensure that the installer user or the root user owns all the parent directories. Ensure that the root user owns the root directory. For example, if the installation base directory is `/scratch/OracleHomes/agent`, and *oracle* is the installing user, then the `/scratch/OracleHomes/agent` directory must be owned by *oracle*, directories `scratch` and `OracleHomes` must be owned by either *oracle* or *root* user, and the root directory (/) must be owned by *root* user.
Instance Directory Requirements	Ensure that the instance directory you enter is empty and has *write* permission.
Shared Oracle Home Requirements	Ensure that the *Master Agent* home is accessible from the destination host where you want to install the *Shared Agent*.
SUDO Requirements	*(Only for UNIX)* Ensure that the installing user has SUDO privileges to invoke `/bin/sh` as *root*.
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*) Ensure that the SCP binaries (for example, /usr/local/bin/scp) are in the `PATH` environment variable.
Path Validation Requirements *(Only for Graphical Mode)*	Validate the path to all command locations. For more information, see the appendix on validating command locations in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

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

Requirement	Description
IPV 6 Requirements *(Only for Graphical Mode)*	If you are installing from an ipv6 OMS to a non-ipv6 host, then follow these step: 1. Navigate to the following location on the OMS home: `$<OMS_HOME>/oui/prov/resources/` 2. Check the property value of PING_PATH in the following files in this order: a. ssPaths_<plat>.properties b. sPaths.properties c. Paths.properties 3. Change the property value of PING_PATH from `/bin/ping` to `/bin/ping6`

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 port, run the following command:
	`netstat -anp | grep <port_no>`
	If the port is a non-default port, that is, any port other than 22, then update the `SSH_PORT` property in the following file that is present in the OMS home:
	`$<OMS_HOME>/oui/prov/resources/Paths.properties`

Ping Requirements
(Only for Graphical Mode)
	If a firewall configured in your environment does not allow any ping traffic, then ensure that you do the following:
	1. Take a backup of the following file from the OMS home:
	For Linux Platforms:
	`$<OMS_ HOME>/oui/prov/resources/sPaths.properties`
	For Other Platforms:
	`$<OMS_HOME>/oui/prov/resources/ssPaths_ <platform>.properties`
	For example, `ssPaths_aix.properties` if the OMS is on AIX platform.
	2. Edit the original properties file and change `PING_ PATH=/bin/ping` to `PING_PATH=/bin/true`.

Port Requirements	Ensure that the default ports described in Section 2.1.6.1 are free.
Installing User Requirements	■ Ensure that the user installing the Shared Agent is the same as the user who installed the Master Agent. ■ 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.

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

Requirement	Description

Central Inventory (oraInventory) Requirements	■ Ensure that you allocate 100 MB of space for the Central Inventory.
	■ Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `/etc/oraInst.loc` file, ensure that the inventory location specified there is not pointing to a shared location. If it is, change it to a non-shared location.
	■ Ensure that you have *read*, *write*, and *execute* permissions on `oraInventory` on all remote hosts. If you do not have these permissions on the default inventory (typically at `/etc/oraInst.loc`) on any remote host, then ensure that you specify the path to an alternative inventory location by using one of the following options in the Additional Parameters field of the Add Host Targets Wizard:
	`INVENTORY_LOCATION=<absolute_path_to_inventory_directory>`
	`-invPtrLoc <absolute_path_to_oraInst.loc>`

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. ■ Increase quotas. ■ Replace process level token. ■ Log in as a batch job. To verify whether the agent user has these rights, follow these steps: 1. Launch the Local Security Settings. 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 Settings**. 2. In the Local Security Settings window, from the tree structure, expand **Local Policies**, and then expand **User Rights Assignment**.
Permissions for cmd.exe *(Only for Microsoft Windows)*	(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`
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.

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

Requirement	Description
Browser Requirements *(Only for Graphical Mode)*	■ Ensure that you use a certified browser as mentioned in the Enterprise Manager Certification Matrix available on *My Oracle Support*. To access this matrix, follow these steps: 1. Log in to *My Oracle Support*, and click the **Certifications** tab. 2. On the Certifications page, in the **Certification Search** region, from the **Product** list, select **Enterprise Manager Cloud Control**. 3. From the **Release** list, select **12.1.0.1.0**, and click **Search**. ■ If you use Microsoft Internet Explorer 8 or 9, do the following: ■ Turn off the compatibility view mode. To do so, in Microsoft Internet Explorer, from the **Tools** menu, click **Compatibility View** to disable it if it is enabled. Also, click **Compatibility View Settings** and deregister the Enterprise Manager Cloud Control console URL. ■ Enable XMLHTTP. To do so, from the **Tools** menu, click **Internet Options**. Click the **Advanced** tab, and under the **Security** heading, select **Enable native XMLHTTP support** to enable it.

8.4 Installation Procedure

This section describes the following:

- Installing in Graphical Mode
- Installing in Silent Mode

8.4.1 Installing in Graphical Mode

To install a *Shared Agent* in graphical mode, follow these steps:

1. In Cloud Control, do one of the following:
   - From the **Setup** menu, select **Add Targets**, and then, click **Auto Discovery Results**. On the Auto Discovery Results page, select a host you want to monitor in Enterprise Manager Cloud Control, and click **Promote**.
   - From the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host**.
2. On the Host and Platform page, do the following:

a. Accept the default name assigned for this session or enter a unique name of your choice. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name. For example, `add_host_operation_1`

   A unique deployment activity name enables you to save the installation details specified in this deployment session and reuse them in the future without having to enter all the details all over again in the new session.

b. Click **Add** to enter the fully qualified name and select the platform of the host on which you want to install the Management Agent.

   Note:

   - Oracle recommends you to enter the fully qualified domain name of the host. For monitoring purpose, Enterprise Manager Cloud Control adds that host and the Management Agent with the exact name you enter here.
   - You must enter only one host name per row. Entering multiple host names separated by a comma is not supported.
   - You must ensure that the host name you enter does not have underscores.

   Alternatively, you can click either **Load from File** to add host names stored in a file, or **Add Discovered Hosts** to add host names from a list of hosts discovered by Enterprise Manager.For information on how the host name entries must appear in the host file, see Section 7.4.1.2

   Note: When you click **Add Discovered Hosts** and add hosts from a list of discovered hosts, the host's platform is automatically detected and displayed. The platform name is detected using a combination of factors, including hints received from automated discovery and the platform of the OMS host. This default platform name is a suggestion, so Oracle strongly recommends you to verify the platform details before proceeding to the next step.

   As the *Shared Agent* can be installed only if the source host and the destination host are running on the same platform, set the platform for the first host in the first row of the table and from the **Platform** list, select **Same for All Hosts**. This will ensure that the platform name you selected for the first host is also set for the rest of the hosts in the table.

   Note: If you are installing a Management Agent on a platform that is different from the platform on which the OMS is running, then ensure that you have the software for that platform. If you do not have that software, then go to the Self-Update page within Enterprise Manager Cloud Control, and download the software.

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 this location is accessible from all the destination hosts.

d. For **Instance Directory**, enter the absolute path to a directory 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`.

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 the SSH connectivity between the OMS and the remote hosts, then you may not have a password for your user account. In this case, create a named credential with a dummy password. Do NOT leave the password field blank.

---

f. For **Privileged Delegation Setting**, validate the Privilege Delegation setting to be used for running the root scripts. By default, it is set to the Privilege Delegation setting configured in Enterprise Manager Cloud Control.

If you leave this field blank, the root scripts will not be run by the wizard; you will have to run them manually after the installation. For information about running them manually, see Section 8.5.

This setting will also be used for performing the installation as the user set in the Run As attribute of the selected Named Credential if you had set the user while creating that Named Credential.

Note: In the Privilege Delegation setting, the `%RUNAS%` is honored as the root user for running the root scripts and as the user set in the Run As attribute of the Named Credential for performing the installation.

g. For **Port**, accept the default port (3872) that is assigned for the Management Agent to communicate, or enter a port of your choice.

   The custom port you enter must not be busy. If you are not sure, you can leave it blank. Enterprise Manager Cloud Control automatically assigns the first available free port within the range of 1830 - 1849.

h. (Optional) In the Optional Details section, enter the absolute path to an accessible location where the preinstallation and postinstallation scripts you want to run are available. Note that only one preinstallation or one postinstallation script can be specified.

   If you want to run the script as `root`, then select **Run as Root**. If the script is on the host where OMS is running and is not on the host where you want to install the Management Agent, then select **Script on OMS**. In this case, the script will be copied from the OMS host to the destination hosts, and then run on the destination hosts.

i. (Optional) For **Additional Parameters**, enter a whitespace-separate list of additional parameters that you want to pass during the installation. For a complete list of supported additional parameters, see Table 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.

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.

8.4.2 Installing in Silent Mode

To install a *Shared Agent* in silent mode, follow these steps:

1. Create a response file titled `AgentNFS.rsp` as described in Table 8–2.

   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 *Master Agent* home, which is visible as a shared location, and pass the response file.

```
<AGENT_HOME>/perl/bin/perl  <AGENT_
HOME>/sysman/install/AgentNFS.pl -responseFile=<absolute_
path_to_response_file>
```

For example,

```
/scratch/agent_base_dir/core/12.1.0.1.0/perl/bin/perl
/scratch/agent_base_
dir/core/12.1.0.1.0/sysman/install/AgentNFS.pl
-responseFile=/home/john/AgentNFS.rsp
```

Note:

- Instead of creating a response file, you can choose to pass all the arguments explicitly while invoking the script. In this case, invoke the script in the following way:

  ```
  <AGENT_HOME>/perl/bin/perl  <AGENT_
  HOME>/sysman/install/AgentNFS.pl AGENT_INSTANCE_
  HOME=<absolute_path_to_instance_dir> ORACLE_
  HOME=<absolute_path_to_master_agent_oracle_home>
  <parameter1>=<value1>  <parameter2>=<value2>
  <parameter3>=<value3> . . .
  ```

  For example,

  ```
  /scratch/agent_base_
  dir/core/12.1.0.1.0/perl/bin/perl /scratch/agent_
  base_
  dir/core/12.1.0.1.0/sysman/install/AgentNFS.pl
  AGENT_INSTANCE_HOME=/home/john/agent_inst ORACLE_
  HOME=/scratch/agent_base_dir/core/12.1.0.1.0
  AGENT_PORT=1832 AGENT_REGISTRATION_
  PASSWORD=welcome b_startAgent=TRUE
  ```

- If the *Master Agent* was installed using the Add Host Targets Wizard, then ensure that you pass the following arguments with these values:

  ```
  AGENT_REGISTRATION_PASSWORD=<password>
  ```

  ```
  b_startAgent=TRUE
  ```

- Do NOT pass the `-invPtrLoc` argument because, by default, the location `<AGENT_HOME>/oraInst.loc` is honored, where `<AGENT_HOME>` is the *Master Agent*. Also ensure that the Oracle Inventory directory, to which the inventory file points, is not in a shared location.

---

3. When prompted to run the `root.sh` script, run it from the instance directory of the Management Agent:

   ```
   <AGENT_INSTANCE_HOME>/root.sh
   ```

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

   ```
   /usr/local/bin/sudo /scratch/OracleHomes/agent_inst/root.sh
   ```

4. Repeat Step (1) to Step (3) on the remaining hosts where you want to install the *Shared Agent*.

8.4.2.1 Creating a Response File

For silently installing a *Shared Agent*, you must invoke the `AgentNFS.pl` script and pass a response file that captures all the required information. Table 8–2 describes the various parameters you must include in the response file.

Table 8–2 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, `/scratch/agent_base_dir/core/12.1.0.1.0`
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, `/home/john/agent_inst`
b_startAgent	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*.
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 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, `Welcome456` **Note:** If the *Master Agent* was installed using the Add Host Targets Wizard, then you must pass this parameter.

8.5 After You Install

After you install a *Shared Agent*, follow these steps:

1. *(Only for Graphical Mode)* Verify the installation on the Add Host Status page. Review the progress made on each of the phases of the deployment operation — **Initialization**, **Remote Prerequisite Check**, and **Agent Deployment**.

Note: In the Add Host Targets Wizard, after you click **Deploy Agent** to install one or more Management Agents, you are automatically taken to the Add Host Status page.

If you want to view the details or track the progress of all the deployment sessions, then from the **Setup** menu, select **Add Target**, and then, click **Add Targets Manually**. On the Add Targets Manually page, select **Add Host Targets** and click **Add Host Results**.

If a particular phase fails or ends up with a warning, then review the details provided for each phase in the Agent Deployment Details section, and do one of the following:

- Ignore the warning or failure, and continue with the session if you prefer.
  - You can choose to proceed with the deployment of Management Agents only on those remote hosts that have successfully cleared the checks, and you can ignore the ones that have Warning or Failed status. To do so, click **Continue** and select Continue, Ignoring Failed Hosts.
  - You can choose to proceed with the deployment of Management Agents on all the hosts, including the ones that have Warning or Failed status. To do, 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:

   ```
   $<INSTANCE_HOME>/bin/emctl status agent
   ```

   Note: If the status of the Management Agent is down for some reason, then manually start the Management Agent by running the following command from its Oracle home:

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

   b. Navigate to the *Shared Agent* home and run the following command to see a message that confirms that EMD upload completed successfully:

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

3. (Only for UNIX Operating Systems) If you had ignored the prerequisite check warning about not having root privileges, SUDO binaries, or SUDO privileges, then manually run the following scripts as a *root* user from each of the hosts where the cloning was done. If you do not have SUDO privileges, then request your Administrator who has the privileges to run these scripts.

- If this is the first Oracle product you just cloned 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 `root.sh` script from the Management Agent home:

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

4. By default, the host and the *Shared Agent* get automatically added to the Enterprise Manager Cloud Control console for monitoring. None of the targets running on that host get automatically discovered and monitored.

   To monitor the other targets, you need to add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

   For information about discovering targets in Enterprise Manager Cloud Control, refer to the chapter on adding targets in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

9

Installing Oracle Management Agent Software Now and Configuring Later

This chapter explains how you can install only the software binaries of Oracle Management Agent (Management Agent) at one point and configure the installation at a later stage. In particular, this chapter covers the following:

9.1 Overview

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.

9.2 Before You Begin

Before you begin installing a Management Agent, review the points outlined in Section 5.2.

9.3 Prerequisites

Before installing the Management Agent, ensure that you meet the prerequisites described in Section 5.3.

9.4 Installation Procedure

To install only the software binaries of a Management Agent in silent mode, follow these steps:

1. Follow the Step (1) to Step (7) outlined in Section 5.4.
2. Invoke the deployment script and pass the response file with the `-softwareOnly` argument:

```
<Software_Extracted_Location>/agentDeploy.sh AGENT_BASE_
DIR=<absolute_path_to_agentbasedir> RESPONSE_FILE=<absolute_
path_to_responsefile> -softwareOnly
```

Note: Do not pass the option `-forceConfigure`.

9.5 Configuration Procedure

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
```

Note: The response file you pass here is the same response file you passed in Section 9.4.

Note: Do not pass the option `-forceConfigure`.

9.6 After You Install

After you install the Management Agent, follow the steps outlined in Section 5.5.

Part IV

Advanced Installation and Configuration

This part describes the advanced installation and configuration tasks you can perform after you have installed Enterprise Manager Cloud Control and have started using the product.

In particular, this part contains the following chapters:

10

Introduction to Enterprise Manager Advanced Configuration

This chapter introduces you to Enterprise Manager advanced configuration and provides basic information about your Enterprise Manager installation. It describes the directory structure and how to make Enterprise Manager accessible to all your users.

After you review this chapter, you can move on to the other advanced configuration tasks described in this manual.

Specifically, this chapter includes the following topics:

10.1 Types of Advanced Configuration Tasks

Enterprise Manager is designed to install easily with a set of standard configuration settings so you can get up and running with the software quickly.

However, Oracle realizes that hardware and software management requirements vary dramatically among business enterprises. As a result, Enterprise Manager can be reconfigured after installation so you can:

- Implement Enterprise Manager security and firewall features.
- Enable End-User Performance Monitoring for your Web applications.
- Reconfigure Enterprise Manager components when you need to modify the topology of your network environment.
- Maintain and troubleshoot the Enterprise Manager components as your business grows.

10.2 Understanding the Enterprise Manager Directory Structure

Before you perform maintenance and advanced configuration tasks, you must be familiar with the directories and files that are copied to disk when you install Enterprise Manager. Understanding where specific files are located can help you if you need to troubleshoot installation or configuration problems.

When installing Enterprise Manager, if you select a location that does not contain WebLogic Server, then JDK will be installed in the `jdk16` directory before installation of WebLogic Server.

Use the following sections to become familiar with the directories that are created on your disk when you install Enterprise Manager:

- Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c
- Understanding the Enterprise Manager Directories Installed with Management Service
- Understanding the Enterprise Manager Directories Installed with Management Agent
- Identifying the Agent Instance Home When Using the emctl Command

10.2.1 Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager Cloud Control 12c

When you install Oracle Enterprise Manager Cloud Control 12c, you install the Oracle Management Service. With the Oracle Management Service, you install the following Oracle home directories:

- Oracle Management Service home directory
- Middleware WebTier home directory
- Middleware Common home directory
- Oracle Management Service Instance home directory
- Oracle Management Agent home directory
- Oracle Management Service Plugins home
- Oracle Management Agent Plugins home

10.2.1.1 About the Oracle Management Service Home Directory

The Oracle Management Service is a J2EE application that is installed and deployed using the Oracle WebLogic Server.

The installation procedure installs the Enterprise Manager components within the Cloud Control Home, including the Oracle Management Service. For more details about the OMS directories, see About the Oracle Management Service Home Directory.

Information about the directories that are specific to the Fusion Middleware installation can be found in the Fusion Middleware documentation.

10.2.1.2 About the Oracle Management Agent Home (AGENT_HOME) Directory

In addition to the Oracle Management Service home directory, the installation procedure installs the Oracle Management Agent that is used to gather management data and perform administration tasks for the targets on the Oracle Management Service host.

The Oracle Management Agent is installed in a separate Oracle home directory which is at the same level as the Fusion Middleware home directory. For more details, see Understanding the Enterprise Manager Directories Installed with Management Agent.

10.2.1.3 Summary of the Important Directories in the Oracle Management Service Home

Figure 10–1 shows some of the important directories you should be familiar with in a typical Cloud Control installation. You can use this information as you begin to maintain, troubleshoot, and configure the Oracle Management Service installation.

Figure 10–1 Directories Installed with Enterprise Manager

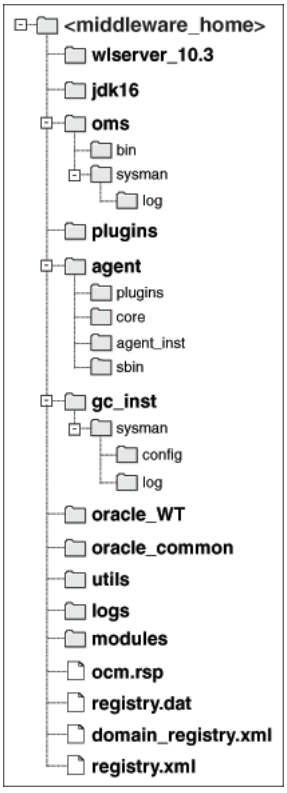


Table 10–1 describes the directories installed with Enterprise Manager.

Table 10–1 Directories Installed with Enterprise Manager

Directory	Description
wlserver_10.3, logs, utils, modules	These directories contain Fusion Middleware files.
jdk16	This directory contains JDK configuration files.
oms	This directory contains OMS configuration files. For more information, see Understanding the Enterprise Manager Directories Installed with Management Service.
plugins	This directory contains metadata plug-ins configuration files installed on the OMS.
agent	This directory contains agent configuration files. For more details, see Understanding the Enterprise Manager Directories Installed with Management Agent.
gc_inst	The OMS instance home directory. For more details, see Understanding the Enterprise Manager Directories Installed with Management Service.

Table 10–1 (Cont.) Directories Installed with Enterprise Manager

Directory	Description
oracle_WT	This directory contains Oracle WebTier configuration files.
oracle_common	This directory contains common files used by OMS, Oracle WebTier, and WebLogic Server directories.

10.2.2 Understanding the Enterprise Manager Directories Installed with Management Service

Table 10–2 describes in detail the Oracle Management Service directories installed with Oracle Management Service. In the table, `ORACLE_HOME` refers to the Oracle Management Service home directory in which the Oracle Management Service is installed and deployed.

Table 10–2 Important Directories in the Management Service Oracle Home

Directory	Description
`ORACLE_HOME/bin`	The `bin` directory in the Management Service home contains commands used to control the components of the Cloud Control installation.
`OMS_INSTANCE_HOME`	This directory contains configuration files for OMS home. The default `OMS_INSTANCE_HOME` location is `gc_inst`.
`OMS_INSTANCE_HOME/sysman`	The `sysman` directory in the OMS instance home contains the system management files associated with this Cloud Control installation.
`OMS_INSTANCE_HOME/sysman/log`	This directory contains log files for the Oracle Management Service.
`OMS_INSTANCE_HOME/sysman/config`	The `config` directory contains Management Service configuration files.
`ORACLE_HOME/sysman/log`	This directory contains schema log files. The repository log files are under `sysman/log/schemamanager`. The install logs are under `ORACLE_HOME/cfgtoollogs`. The operation logs are under `OMS_INSTANCE_HOME/em/EMGC_OMS1/sysman/log`.

10.2.3 Understanding the Enterprise Manager Directories Installed with Management Agent

The Oracle Management Agent is installed automatically when you install Oracle Management Service. This local instance of the Oracle Management Agent gathers management information about the targets on the Oracle Management Service host. You can then manage those targets, such as the host itself, from the Cloud Control Console.

You can install additional Oracle Management Agents using different installation methods. This enables you to install the Oracle Management Agent on the hosts throughout your enterprise. The Oracle Management Agent can then gather management data about the targets on each host so those targets can be managed from the Cloud Control Console.

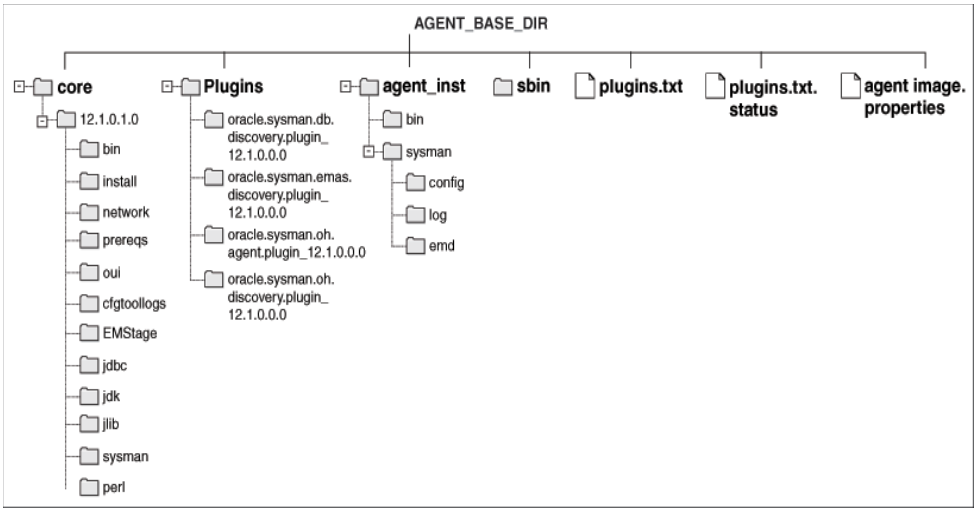
Specifically, the Oracle Management Agent files are installed into the same directory structure shown in the `agent` directory when you install the Oracle Management Service (Figure 10–1).

The agent directory structure, when you install a standalone agent or install the OMS is the same. The AGENT_BASE_DIR is the directory where agent is installed and contains the following main directories:

- AGENT_HOME
- AGENT_INSTANCE_HOME
- SBIN_HOME
- PLUGIN_HOME

The directory that contains the files required to run the Oracle Management Agent is referred to as the AGENT_INSTANCE_HOME directory. For example, to start or stop an Oracle Management Agent, you use the emctl command located in the bin directory of the AGENT_INSTANCE_HOME. Similarly, to configure files for the Oracle Management Agent, you modify the configuration files in the sysman/config directory of the AGENT_INSTANCE_HOME. See Figure 10–2 for the agent directory structure.

Figure 10–2 Agent Directory Structure



10.2.3.1 Summary of the Important Directories in the Oracle Management Agent Home

Table 10–3 describes some of the important agent directories.

Table 10–3 Important Directories in the Oracle Management Home

Directory	Description
AGENT_HOME	The AGENT_HOME directory contains all the binaries required to configure and run the Oracle Management Agent on this host. The default AGENT_HOME location is AGENT_BASE_DIR/core/12.1.0.1.0. This directory serves as the Oracle Home for the Oracle Management Agent.
AGENT_HOME/bin	This directory contains binaries for the Oracle Management Agent.

Table 10–3 (Cont.) Important Directories in the Oracle Management Home

Directory	Description
AGENT_HOME/install	This directory contains installation-related files for deploying the agent.
AGENT_HOME/network	This directory contains network module files for deploying the agent.
AGENT_HOME/prereqs	This directory contains prerequisite files for EMPrereqKit.
AGENT_HOME/oui	This directory contains files related to the installer framework.
AGENT_HOME/cfgtoollogs	This directory contains agent deployment and configuration log files.
AGENT_HOME/EMStage	This directory is used by the provisioning framework for provisioning activities.
AGENT_HOME/sysman/admin	This directory contains the files used by the Oracle Management Agent to define agent core target types (such as databases, hosts, and so on), to run configuration scripts, and other administrative tasks.
AGENT_INSTANCE_HOME	The AGENT_INSTANCE_HOME directory contains agent-related configuration files after agent is installed and configured. The default AGENT_INSTANCE_HOME location is AGENT_BASE_DIR/agent_inst.
AGENT_INSTANCE_HOME/bin	The AGENT_INSTANCE_HOME/bin directory in the Cloud Control Home contains the emctl command that controls the Oracle Management Agent for this host. You use the following emctl commands in this directory to start and stop the Oracle Management Agent on this host: <AGENT_INSTANCE_HOME>/bin/emctl start agent <AGENT_INSTANCE_HOME>/bin/emctl stop agent
AGENT_INSTANCE_ HOME/sysman/config	This directory contains the configuration files for the Oracle Management Agent. For example, this is where Enterprise Manager stores the emd.properties file. The emd.properties file defines settings such as the Oracle Management Service upload URL for this particular agent.
AGENT_INSTANCE_ HOME/sysman/log	This directory contains the log files for the Oracle Management Agent.
AGENT_INSTANCE_ HOME/sysman/emd	The emd directory contains information about targets discovered on hosts.
SBIN_HOME	This directory contains set UIDs for the agent. The default location is AGENT_BASE_DIR/sbin.
PLUGIN_HOME	This directory contains all the discovery and monitoring plugins required for the agent. The default location is AGENT_BASE_DIR/plugins.

10.2.3.2 Understanding the Oracle Management Agent Directory Structure on Windows

When you install the Oracle Management Agent on a Windows system, the directory structure of the AGENT_HOME directory is the same as the directory structure for installations on a UNIX system.

10.2.4 Identifying the Agent Instance Home When Using the emctl Command

When you install Cloud Control, the resulting directory structure can often include multiple subdirectories with the same name. For example, you can have a `bin` directory within the agent_instance_home directory. Use the `emctl` command within the `agent_instance_home/bin` directory to control the Oracle Management Agent.

In addition, you can have a `bin` directory within the Oracle Management Service Oracle home. Use the `emctl` command in this directory to control the Oracle Management Service.

To quickly identify the Agent Instance home that is controlled by the files in a particular `bin` directory, use the following command:

```
$PROMPT> emctl getemhome
```

This command displays the path to the current Agent Instance home that will be affected by commands executed by this instance of the `emctl` command.

10.3 Enabling Enterprise Manager Accessibility Features

As part of the effort to make Oracle products, services, and supporting documentation accessible and usable to the disabled community, Enterprise Manager offers several features that make management data available to users of assistive technology. Enterprise Manager provides the following accessibility features:

- Support for Screen Reader
- Support for High Contrast
- Support for Large Fonts

To enable Screen Reader support, you must modify the following configuration settings:

1. Enable Accessibility Mode in My Preferences.
2. Set uix-config.xml flag.
3. Set web.xml flag.

10.3.1 Enabling Enterprise Manager Accessibility Mode

To enable screen reader mode, do the following:

1. On the Cloud Control home page, from the **Setup** menu, select **My Preferences** and then select **Accessibility**.
2. In the Accessibility Preference page, select **I use a screen reader**. Click **Apply**.

   ADF accessibility mode is a session based setting which takes place immediately and does not require you to restart the Enterprise Manager Management Service.

For ADF pages, you will see an Accessibility Preferences dialog after logging into Cloud Control for the first time. The settings in this dialog are the same as those in the Accessibility Preference page mentioned above.

10.3.2 Setting uix-config.xml Flag

To enable screen reader mode for UIX pages, do the following:

1. Locate the `uix-config.xml` configuration file.

   To locate the `uix-config.xml` file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

   ```
   ./oms11g/sysman/archives/emgc/deployments/EMGC_
   DOMAIN/emgc.ear/em.war/WEB-INF/uix-config.xml
   ```

2. Open the `uix-config.xml` file using a text editor and set the following entry:

   ```
   <!-- An alternate configuration that disables accessibility features  -->
   <default-configuration>
   <accessibility-mode>screenReader</accessibility-mode>
   </default-configuration>
   ```

3. Save and close the file.
4. Restart the Oracle Management Service.

> **Note:** UIX accessibility mode is a product-wide setting. You will have to restart the Enterprise Manager Management Service for this setting to take effect.

10.3.3 Configuring web.xml File

To configure web.xml file, follow these steps:

1. Locate the `web.xml` configuration file.

   To locate the `web.xml` file in a Cloud Control installation, change directory to the following location in the Oracle Management Service home:

   ```
   ./oms11g/sysman/archives/emgc/deployments/EMGC_
   DOMAIN/emgc.ear/em.war/WEB-INF/web.xml
   ```

2. Open the `web.xml` file with your favorite text editor and locate the following six lines of the file:

   ```
   <!-- Uncomment this to enable textual chart descriptions
   <context-param>
   <param-name>enableChartDescription</param-name>
   <param-value>true</param-value>
   </context-param>
   -->
   ```

3. Remove comments from this section by deleting the first line and the last line of this section so that the section consists of only these 4 lines:

   ```
   <context-param>
   <param-name>enableChartDescription</param-name>
   <param-value>true</param-value>
   </context-param>
   ```

4. Save and exit the file.
5. Restart the Oracle Management Service.

10.3.4 Verifying That Screen Reader Support Is Enabled

Throughout Enterprise Manager, charts are used to display performance data. For most users, these charts provide a valuable graphical view of the data that can reveal trends and help identify minimum and maximum values for performance metrics.

However, charts do not convey information in a manner that can be read by a screen reader. To remedy this problem, you can configure Enterprise Manager to provide a complete textual representation of each performance chart. By default, support for the textual representation of charts is disabled. When textual description for charts is enabled, Enterprise Manager displays a small icon for each chart that can be used as a drill-down link to the textual representation.

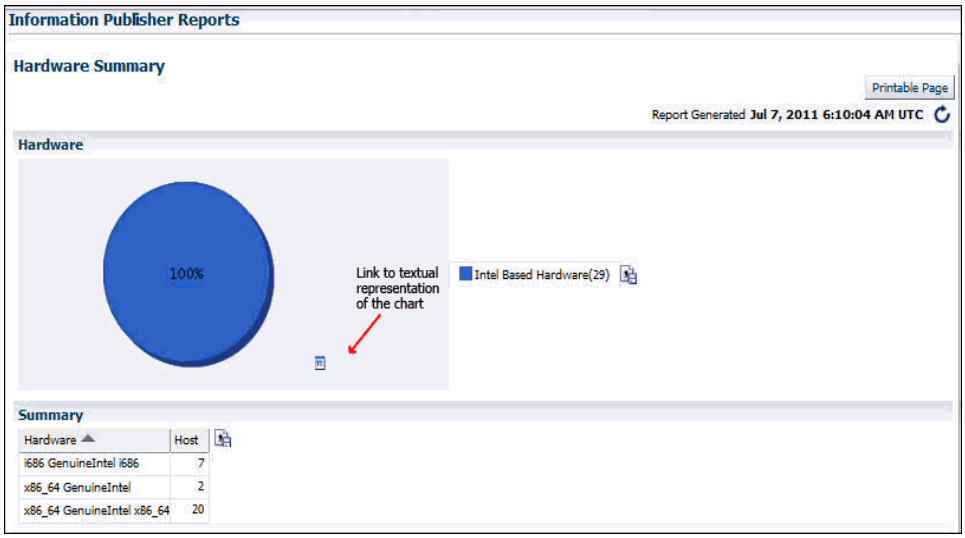
To verify whether Screen Reader support has been enabled for ADF pages, follow these steps:

1. On the Cloud Control home page, click **Help** and then select **About Enterprise Manager**.
2. In the About Enterprise Manager dialog box, ensure that **Accessibility Preference - Screen Reader Support** is set to **Enabled**.
3. If **Accessibility Preference - Screen Reader Support** is set to **Disabled**, follow the steps listed in Enabling Enterprise Manager Accessibility Features.

To verify whether Screen Reader support has been enabled for UIX pages, follow these steps:

1. On the Cloud Control home page, from the **Enterprise** menu, select **Reports** and then select **Information Publisher Reports**.
2. In the Information Publisher Reports page, click **Hardware Summary**. The Hardware Summary page is displayed. If accessibility setting has been enabled, you will see the icon shown in Figure 10–3:

Figure 10–3 Icon Representing Textual Representation of Charts



****

11

Performing Additional Configuration Tasks

This chapter contains the following sections:

11.1 Understanding Default and Custom Data Collections

When you install the Oracle Management Agent on a host computer, Enterprise Manager automatically begins gathering a default set of metrics that you can use to monitor the performance and availability of each targets on that host. For some of these target metrics, Enterprise Manager provides default threshold settings that determine when you will be notified that there is a problem with the metric.

See Also: *About Alerts* in the Enterprise Manager online help

For selected metrics, you can customize the default thresholds. When you make these types of customizations, Enterprise Manager saves the new settings in a file on the local disk. The following section provides more information about how these settings are saved.

11.1.1 How Enterprise Manager Stores Default Collection Information

Enterprise Manager stores the default collection criteria for each target in the following location on each Oracle Management Agent host:

AGENT_HOME/sysman/admin/default_collection/

For some targets, you can use the Oracle Enterprise Manager Release 12*c* Cloud Control Console to modify the default metric collection settings. For example, you can modify the default thresholds for your host targets. When you make these types of

modifications, Enterprise Manager creates a new instance collection file in the following directory:

```
AGENT_HOME/sysman/emd/collection/
```

This collection file overrides the default collection information stored in the `sysman/admin/default_collection` directory.

11.2 Enabling Multi-Inventory Support for Configuration Management

Every time you install an Oracle software product on a host computer, Oracle Universal Installer saves information about the software installation on your hard disk. The directories and files that contain this software configuration information are referred to as the Oracle Universal Installer inventory.

> **See Also:** *Oracle Universal Installer and OPatch User's Guide*

When you use Enterprise Manager to monitor your Oracle software installations, Enterprise Manager takes advantage of information saved in the Universal Installer inventory.

As it gathers information about the configuration of your host computer, by default, Enterprise Manager assumes that you have one Oracle Universal Installer inventory on the host. Specifically, Enterprise Manager recognizes the inventory that Oracle Universal Installer uses when you run the Universal Installer on the host.

However, in some cases, you may have more than one inventory. For example, you may have worked with Oracle Support to clone your Oracle software installations. For those cases, you can use the following procedure to be sure that Enterprise Manager can track and manage the software information in multiple inventories on the same host.

Caution: Enabling support for multiple inventories is optional and available only for advanced users who are familiar with the Oracle Universal Installer inventory architecture and who have previously worked with multiple inventories on a managed host. This procedure is not required for hosts where normal installations have been performed.

To set up Enterprise Manager so it can read multiple inventories on a host, follow these steps:

1. Locate the *OUIinventories.add* file in the following directory:

   ```
   $ORACLE_HOMEsysman/config
   ```

   The Management Agent state listed in this example represents an installation for Database Control. For more information about the Management Agent state to use for other installations, see Section 11.2.1, "AGENT_HOME Versus AGENT_STATE Directories" on page 11-3.

2. Open *OUIinventories.add* using a text editor.

   Instructions within the file describe the format to use when identifying multiple inventories, as well other techniques for mapping Oracle Homes.

3. Carefully review the instructions within the file.

4. Add entries to the file for each additional inventory on the managed host.
5. Save your changes and close the file.

During its next collection of host configuration information, Enterprise Manager will start gathering software configuration information from the inventories that you identified in the *OUIinventories.add* file, in addition to the default inventory that Enterprise Manager normally collects.

Alternatively, to see the data gathered from the additional inventories before the next regularly-scheduled collection, navigate to the Host home page in the Cloud Control console, click the **Configuration** tab, and click the Refresh Data icon next to the page timestamp.

Note: If there any irrecoverable problems during the collection of the default inventory (for example, if the inventory file or directory protections prevent Enterprise Manager from reading the inventory), inventories listed in *OUIinventories.add* file are also not collected.

If the Enterprise Manager is able to read the default inventory, but there is a problem reading an additional inventory listed in the *OUIinventories.add* file, Enterprise Manager issues a collection warning for those inventories. However, Enterprise Manager does collect the configuration information for the other inventories.

11.2.1 AGENT_HOME Versus AGENT_STATE Directories

The Management Agent recognizes two main directory structures; its installation directory where software binaries and all unchanging metadata are stored, and its configuration/state directory where all customizations and output/log content are stored and/or generated. In a normal Management Agent installation, these two directories are the same. However, they can be different in the following cases:

- Oracle RAC Agent installation (*$ORACLE_HOME* versus *$ORACLE_HOME/<hostname>*)
- Database Control installation (*$ORACLE_HOME* versus *$ORACLE_HOME/<nodename>_<sid>*)
- State-only Management Agent deployment (using the `emctl deploy agent` command -- *$ORACLE_HOME* versus *$EMSTATE*)

In each of the above cases, there will be multiple instances of the Management Agent running off the same binaries installation. The different instances have different locations to maintain separate configurations but use the same set of binaries. The command `emctl status agent` provides the values of the Management Agent's binaries and state locations.

11.3 Manually Configuring a Database Target for Complete Monitoring

When you first discover an Oracle Database target, you should check the monitoring credentials to be sure the password for the DBSNMP database user account is set correctly in the database target properties.

Besides setting the monitoring credentials, no other configuration tasks are required to monitor an Oracle Database target.

However, when you monitor an Oracle9*i* database, there is some additional configuration required if you want to monitor certain types of database performance metrics using the Cloud Control console.

To monitor these additional performance metrics Enterprise Manager requires that Oracle Statspack and some additional Enterprise Manager packages be installed and configured in the database you are monitoring.

> **See Also:** "Using Statspack" in *Oracle Database Performance Tuning Guide and Reference* in the Oracle9i Documentation Library

If these additional objects are not available and configured in the database, Enterprise Manager will not be able to gather the data for the complete set of performance metrics. In addition, Enterprise Manager will not be able to gather information that otherwise could be readily available from the Database home page, such as Bad SQL and the Top SQL Report.

You can use the Configure Database wizard in the Cloud Control console to install the required packages into the database, or you can use the following manual procedure.

> **See Also:** "Modifying Target Properties" in the Enterprise Manager online help for information on configuring managed targets, including database targets

To manually install Statspack and the other required database objects into an Oracle9*i* database that you are managing with Enterprise Manager, you can use SQL*Plus and the following procedure:

1. Log in to the database host using an account with privileges that allow you to write to the database home directory and to the Management Agent home directory.

   For each of the commands in this procedure, replace AGENT_HOME with the actual path to the Oracle Management Agent home directory and replace ORACLE_HOME with the path to the database home directory.

2. Start SQL*Plus and connect to the database using the SYS account with SYSDBA privileges.

   For example:

   ```
   $PROMPT> ./sqlplus "connect / as sysdba"
   ```

3. Enter the following command to run the database dbmon script:

   ```
   SQL> @AGENT_HOME/sysman/admin/scripts/db/config/dbmon
   ```

   The script will display the following prompt:

   ```
   Enter value for dbm_password:
   ```

4. When prompted, enter the password for the DBSNMP account.

   The script performs several configuration changes and returns you to the SQL*Plus prompt.

5. Connect as the DBSNMP user.

   For example:

   ```
   SQL> connect DBSNMP
   ```

6. Enter the following command:

```
SQL> @AGENT_HOME/sysman/admin/scripts/db/config/response.plb
SQL> grant EXECUTE on dbsnmp.mgmt_response to OEM_MONITOR;
```

> **Note:** The above script should not be run on an Oracle database of version 8.1.7 or prior. Oracle does not support SQL Response Time for 8.1.7 databases or prior.

7. Connect as SYS and enter the following command to create the PERFSTAT user:

```
SQL> @ORACLE_HOME/rdbms/admin/spcreate
```

> **Note:** The `spcreate` script will prompt you for a default tablespace and default temporary tablespace for the PERFSTAT user. Do not specify the SYSTEM tablespace as the default tablespace for the PERFSTAT user. For more information, see "Using Statspack" in the *Oracle Database Performance Tuning Guide*

8. Connect as the PERFSTAT user.

   For example:

```
SQL> connect PERFSTAT;
```

9. Enter the following commands from the PERFSTAT user account:

```
SQL> define snap_level='6';
SQL> define cinterval='1';
SQL> define cjobno='-1';
SQL> @AGENT_HOME/sysman/admin/scripts/db/config/spset
```

10. Connect as the SYS user and enter the following command:

```
SQL> grant OEM_MONITOR to dbsnmp;
```

11. If the database you are modifying is an Oracle8*i* database, also enter the following commands as the SYS user:

```
grant select on sys.ts$ to OEM_MONITOR;
grant select on sys.seg$ to OEM_MONITOR;
grant select on sys.user$ to OEM_MONITOR;
grant select on sys.obj$ to OEM_MONITOR;
grant select on sys.sys_objects to OEM_MONITOR;
grant select on sys.file$ to OEM_MONITOR;
grant select on sys.attrcol$ to OEM_MONITOR;
grant select on sys.clu$ to OEM_MONITOR;
grant select on sys.col$ to OEM_MONITOR;
grant select on sys.ind$ to OEM_MONITOR;
grant select on sys.indpart$ to OEM_MONITOR;
grant select on sys.indsubpart$ to OEM_MONITOR;
grant select on sys.lob$ to OEM_MONITOR;
grant select on sys.lobfrag$ to OEM_MONITOR;
grant select on sys.partobj$ to OEM_MONITOR;
grant select on sys.tab$ to OEM_MONITOR;
grant select on sys.tabpart$ to OEM_MONITOR;
grant select on sys.tabsubpart$ to OEM_MONITOR;
grant select on sys.undo$ to OEM_MONITOR;
```

12. For any supported database version, enter the following command from the SYS account:

    ```
    SQL> show parameter job_queue_processes
    ```

    If the output from the *show parameter* command is zero, then perform the following steps to modify the *job_queue_processes* initialization parameter:

    If you start the database using an spfile, enter the following command:

    ```
    SQL> alter system set job_queue_processes = 2 SCOPE=BOTH;
    ```

    Otherwise, do the following:

    a. Enter the following command:

       ```
       SQL> alter system set job_queue_processes = 2;
       ```

    b. Exit SQL*PLUS and update the *init.ora* database configuration file with the following entry so the parameter will be applied whenever the database is restarted:

       ```
       job_queue_processes=2
       ```

13. Exit SQL*Plus and change directory to the following directory in the home directory of the Management Agent that is monitoring the database:

    AGENT_HOME/bin

14. Reload the Management Agent by entering the following command:

    ```
    $PROMPT> ./emctl agent reload
    ```

15. Using the Cloud Control console, return to the Database home page and verify that the Bad SQL and Top SQL Report metrics are now being gathered.

11.4 Modifying the Default Login Timeout Value

To prevent unauthorized access to the Cloud Control console, Enterprise Manager will automatically log you out of the Cloud Control console when there is no activity for a predefined period of time. For example, if you leave your browser open and leave your office, this default behavior prevents unauthorized users from using your Enterprise Manager administrator account.

By default, if the system is inactive for 45 minutes or more, and then you attempt to perform an Enterprise Manager action, you will be asked to log in to the Cloud Control console again.

> **Caution:** As stated in the previous paragraphs, the timeout value for logging in to the Cloud Control console is defined in order to protect your system from unauthorized logins. If you make changes to the login timeout value, be sure to consider the security implications of leaving your session open for other than the default timeout period.

To increase or decrease the default timeout period:

1. Change directory to the following location in the Oracle Application Server home directory where the Management Service was deployed:

   IAS_HOME/sysman/config/

2. Using your favorite text editor, open the *emoms.properties* file and add the following entry:

```
oracle.sysman.eml.maxInactiveTime=time_in_minutes
```

3. For example, if you want to change the default timeout period to one hour, add the following entry:

```
oracle.sysman.eml.maxInactiveTime=60
```

4. Save and close the *emoms.properties* file.
5. Restart the Management Service.

Note: The default timeout value does not apply when you restart the Web server or the Oracle Management Service. In both of those cases, you will be asked to log in to the Cloud Control console, regardless of the default timeout value.

11.5 Configuring Clusters and Cluster Databases in Cloud Control

This section describes how to configure clusters, cluster databases, and discover instances.

11.5.1 Configuring Clusters

To add a cluster target that was installed but not discovered as a target automatically during installation, perform the following steps:

1. Click **All Targets** from the Targets page.
2. Select **Cluster** from the Add menu and click **Go**. The Add Target: Cluster page appears.
3. Optional: Specify the cluster name and provide the Clusterware home path if it is installed on the cluster.
4. To add hosts to the cluster, use the arrow buttons to move items from Available Hosts to Selected Hosts. The hosts you select must not already belong to a cluster.
5. Click **Add** to save the cluster target to the targets.xml file on every selected host.

See Also: The Enterprise Manager online help for more information about configuring clusters

11.5.2 Configuring Cluster Databases

After you have added the cluster target, you can add a cluster database target either from the Databases page or from the All Targets page.

To add a cluster database target, perform the following steps:

1. In the Enterprise Manager Cloud Control Console, select one of the following entry locations:
   - From the Databases page, click **Add**. The Add Database Instance Target: Specify Host page appears.

- From the All Targets page, select **Database Instance** from the Add drop-down menu, then click **Go**. The Add Database Instance Target: Specify Host page appears.

2. Specify any host member of the cluster target where the cluster databases reside, then click **Continue**. The Add Database: Specify Source page appears.
3. Keep the default option (on all hosts in the cluster) selected and click **Continue**. This option sends requests to all Management Agents in the cluster to perform discovery.

   After target discovery completes, the newly discovered Oracle RAC databases appear in the *Targets Discovered on Cluster* page. If the databases do not appear, see the Troubleshooting section below.
4. If the desired targets do not appear in the Cluster Databases table, or if the discovered targets are not configured appropriately, click **Manually Add**. The Properties page of the Configure Cluster Database wizard appears.
5. Provide the required values for the Properties table.
6. You must specify at least one instance in the Instances table. If no instances appear in the table, click **Add**. The Properties: Add Instance page appears. Provide the required values, then click **OK**. The Properties page of the Configure Cluster Database wizard reappears.
7. Click **Next**. For database versions 10.1 and higher, Enterprise Manager bypasses the Install Packages, Credentials, and Parameters steps, and goes directly to the Review page.
8. Click **OK**. The Targets Discovered on Cluster page reappears, and displays the newly added cluster database and instances.

See Also: The Enterprise Manager online help for more information about configuring cluster databases

11.5.3 Discovering Instances Added to the Cluster Database

If you need to configure additional instances, follow these steps:

1. In Enterprise Manager, click **Databases** in the Targets page, and navigate to the desired **Cluster Database Home** page.
2. Click **Monitoring Configuration** in the Related Links section. The Properties page of the Configure Cluster Database wizard appears.
3. Provide the required information in the Properties table at the top of the page.
4. Examine the Instances table. One or more additional instances may exist, but may not appear in the Instances table. If this is the case, click **Add** to discover the instance in the cluster database. The Properties: Add Instance page appears.
5. Provide the required information, then click **OK**. The wizard Properties page reappears, and displays the added instance view.
6. Click **Check Connection** to ensure that the connection is working.

See Also: The Enterprise Manager online help for more information about discovering instances added to the cluster database

11.5.3.1 Troubleshooting

If you encounter configuration issues, check the following required conditions to ensure that automatic discovery is able to function correctly:

- The host user running the Management Agent is able to run the SRVCTL utility in the Oracle home and retrieve the database configuration.
- The host user running the Management Agent is able to connect to the database through SQLPLUS using OS authentication.
- The Oratab (UNIX) or Registry (Windows) contains information about the database.

If automatic discovery still does not resolve your configuration issues after you have ensured the conditions previously listed, you can manually configure cluster databases (see Section 11.5.2, "Configuring Cluster Databases").

11.6 Collecting Client Configurations

A client is comprised of a host and operating system user. Client configuration data that is collected includes:

- Hardware for the client.
- Operating system (includes information such as operating system properties, file systems, and patches) for the client.
- Operating system-registered software.
- Network data, which includes:
  - Latency to the Web server
  - Bandwidth to the Web server
- Client-specific data items that describe the configuration of the browser used to access the client configuration collection applet, which includes:
  - Browser type (vendor)
  - Browser version
  - JVM vendor (of the JVM used to run the client configuration collection applet)
  - JVM version (of the JVM used to run the client configuration collection applet)
  - Proxy server (if specified)
  - Proxy server exceptions
  - Browser cache size (MB)
  - Browser cache update frequency
  - Supported HTTP version
- Other client-oriented data items, including:
  - Client configuration collection applet identifier (version, defined in the applet code)
  - Application URL (from which the client configuration collection applet was accessed)
  - Boot drive serial number (not available from diskless systems)
  - Collection timestamp (from the client configuration collection applet JSP)

- Collection durations, in milliseconds
- Client IP address
- Effective client IP address - if a network proxy server is being used between the client and the Web server providing the client configuration collection applet, the effective client IP address will be the IP address of the proxy server.

11.6.1 Configuring the Client System Analyzer

The Client System Analyzer (CSA) allows Web server administrators to collect and analyze end-user client data. The client data is collected by an applet, diagnosed and sent back to the CSA application. The Oracle Management Agent uploads this data to the Enterprise Manager Management Repository. After the client configuration data has been collected by the client configuration collection applet and written to the Web server directory specified by the CSA applet, the client configuration data is uploaded to the Oracle Management Repository.

You can either use the Client System Analyzer in the Cloud Control application pre-installed with Enterprise Manager or you can deploy CSA independently to your Web server.

11.6.1.1 Client System Analyzer in Oracle Cloud Control

Client System Analyzer in Cloud Control - An instance of CSA is pre-installed with Enterprise Manager. If you use this option, you can collect client data without setting up a separate Web server. To activate the pre-installed CSA application in Enterprise Manager, click **Deployments**. Then click **Client System Analyzer in Cloud Control** and use the button provided to activate the application. Once CSA is activated, end-users can use the URL provided to run the CSA applet. The CSA applet can collect base client configuration information from client systems and Oracle Collaboration Suite client information from Oracle Collaboration Suite client systems.

- To download the CSA applet and have it collect base client configuration information, a client should use the Client System Analyzer URL in this format: *http[s]://management-service-host:port/em/public/ecm/csa/CSA*
- To download the CSA applet and have it collect Oracle Collaboration Suite client configuration information, a client should use the Client System Analyzer URL in this format: *http[s]://management-service-host:port/em/public/ecm/csa/CSA?application=OCS*

11.6.1.2 Deploying Client System Analyzer Independently

The Client System Analyzer Application can be deployed independently to any J2EE-capable Web server. Click the **Deployments** tab. Then click **Getting Started with Client System Analyzer** and click **Deploy Client System Analyzer Application**. Follow these steps to deploy the CSA applet and collect the client configuration data.

1. Download the CSA Application:

   The CSA application includes the CSA directory along with the necessary JSP applet files. The application is packaged as an EAR file. To download this default EAR file, click **Download Client System Analyzer Application**. You can customize the default CSA EAR file by modifying the following:

   - Rules - This file contains a default set of rules against which the client data is evaluated. You can customize and add rules before deploying CSA.
   - Context parameters - You can customize the context parameters in the *web.xml* file.

- Custom classes - You can provide customized applet classes that can be used to perform tasks like collecting additional data, changing the behavior of the applet, and performing certain operations on the client.

2. Deploy CSA to any J2EE Web server.

   The CSA application is deployed on an Application Server as a regular J2EE application. Once the CSA application is deployed, context parameters can be changed similar to other web applications.

3. Direct users to the CSA.

   In order for the client data to be collected, the user must access the CSA application. Users can access the CSA JSP page directly or by using a link from another application. Users can be automatically redirected to CSA using the following methods:

   - HTTP Server (Apache's *mod_rewrite*) - This option does not require changes in the Web application.
   - Servlet Filter - A servlet filter is a program that filters requests to and from the server. The *CSA_filter.jar* file contains the servlet filter classes. The servlet filter and the filter mapping need to be added to the Web application.
   - CSA Redirection JSP - The CSA Redirection JSP (*CSARedirect.jsp*) page can be included into the Web application.

4. Configure Enterprise Manager.

   Collected client data is recorded in the Receive File Directory on the Web server. To upload the collected client data into Enterprise Manager, you need to do the following:

   - Add a CSA Collector Target to the Enterprise Manager Management Agent. To do so, click **Add Collector** and choose a target from the list.
   - Specify the absolute path to the Receive File Directory. The path specified must be the same as the path specified in the *outputDir* parameter of the CSA application. By default, the client data is stored in the Receive File Directory *csa_results* under the context root of the Client System Analyzer Web application, but this can be configured by changing the applications's *outputDir* context parameter.

5. Test the CSA Deployment.

   To verify the CSA deployment, click the URL of the CSA page and check if the client data is collected.

11.6.2 Configuration Parameters

The Client System Analyzer (CSA) can be further configured by modifying the context parameters in the CSA application's WAR file.

Table 11–1 Configuration Parameters

Parameter	Description	Default Value
alertWhenDone	If set to true, a message indicating that the applet has been executed is displayed.	false
appletJAR	The name of the JAR file.	CSA.jar

Table 11–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
application	The name of the application associated with this CSA instance. If the application parameter value is not specified, then the Collection Tag has a value of Default.	none
autoRedir	If set to "true", this causes the CSA JSP page to automatically use the Sun JVM if JVM was set to JInitiator and the client does not have the appropriate version of JInitiator installed.	false
bwTestFile	The name of the file that is downloaded from the server during the bandwidth test.	CSA.mb (included with CSA)
bwTestMsec	The amount of time the applet should spend on the bandwidth test. The applet computes bandwidth by counting the number of bytes it can download in this interval.	200 ms
classid	The "classid" field for the OBJECT tag. Applicable only if JVM is set to "JInitiator." The classid for Sun is "clsid:8AD9C840-044E-11D1-B3E9-00805F499D93" codebase - the "codebase" field for the OBJECT tag. Applicable only if JVM is set to "JInitiator."	None – this field MUST be set if JVM is set to "JInitiator," and is ignored otherwise
codebase	The codebase field for the OBJECT tag. Applicable only if the JVM is set to "JInitator".	The default for Sun is http://java.sun.com/products/plugin/autodl/jinstall-1_4_2-windows-i586.cab#Version=1,4,0,0
collectCookie	The list of the names of cookies to be collected. This parameter is a comma-separated list of cookie names. Only cookies for the current OS user in the current browser will be collected. The Administrator can specify asterisk (*) to collect all of the current user's cookies for the current browser.	If this field is not present, no cookies will be collected.
cookieDomain	The domain of the CSA cookie.	If either the domain or path of the cookie is not set, cookies are disabled
cookieMaxAge	The maximum duration, in seconds, of the cookie on the client machine.	1 year
cookiePath	The path of the CSA cookie	If either the domain or path is not specified, cookies are disabled.
customClass	The name of the class used to collect custom data.	none – the default behavior is for no custom code to be executed
customKey1 customKey2 customKey3	The values of the three custom keys. All client collections done by a CSA JSP page that uses this deployment descriptor will have these values for the custom keys. These values can be overridden by custom code.	If no custom key values are specified, none will be collected (unless they are collected by custom code)
descriptionFile	The full path of a text file containing the description that will be displayed on the deployment page. The contents of the file should be HTML-formatted text.	None

Table 11–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
destURL	Specifies the destination URL. This is the URL to which the "Proceed" button on the CSA JSP page is linked.	If no destURL is specified, the "Proceed" button will take the user to the referring page; if there is no referring page, the "Proceed" button will not be displayed.
destURLResultsParam	Specifies the name of the URL parameter that will be added to the "destination URL" to indicate the client's compliance level. For example, if the value was "compliance", and the client's overall compliance level was critical, then the parameter "compliance=critical" would be added to the destination URL.	Sun
JVM	This determines the type of JVM that is to be used. If the value is ""Sun," the JSP page will direct the browser to use the Sun JVM. If the value is "Oracle," the page will direct the browser to use Oracle Jinitiator. If the value is "any," the JSP will write out the standard "applet" tag, which causes the client to use whichever JVM is plugged into the browser.	Sun
maxExecInterval	Parameter that is added to CSA cookie payload. When the redirection logic reads the cookie, if the timestamp of the cookie differs from the current time by more than this value, the applet is deployed again. This parameter can be overridden by the "csa execInterval" context parameter in the redirection JSP filter.	90 days
maxFileSize	Maximum amount of data, in KB, that can be posted back to the receiver in a single request. If the size of the posted data exceeds this limit, the request is rejected and any data already written to the hard drive is deleted.	100
maxOutputFiles	Maximum number of output files that can be present in XML OutputDir.	100
outputDir	Directory to which CSA configuration xml files will be written. Both the applet page and the receiver page must read this parameter, and this parameter must be identical for both pages.	By default, the output files are written into the "csa_results" subdirectory of the application root directory (if the application root directory exists, and if the subdirectory exists or can be created). Using the default value for this parameter is not recommended.
outputEnabled	Enables or disables creation of output XML files. Applicable to both applet and receiver pages.	By default, the XML files are created and stored in the XMLOutputDir.

Table 11–1 (Cont.) Configuration Parameters

Parameter	Description	Default Value
pluginspage	Used to direct the user to the JVM installer under Netscape, since Netscape does not support automatic installation. Applicable only if JVM is Jinitiator. Default for Sun is `http://java.sun.com/products/plugin/index.html#download`	none - This field must be set if JVM is set to "JInitiator" and is ignored otherwise.
receiver	The URL to which the applet should post the collected data. **Note:** When setting this parameter, the administrator must ensure that the version of the receiver is the same as the version of the applet.	Default is to look for "CSAr.jsp" in the same path as the CSA JSP page
ruleFile	Specifies the path on the server, relative to the web application root, of the file that contains the rules to be evaluated.	rules.xml
script	Specifies a script, provided by the administrator, which can be run on the CSA XML file before it is marked for upload by the agent.	none - If no script is specified, no script will be run.
type	The type field for the OBJECT tag rendered by the CSA JSP page to deploy the applet. This is only applicable if the JVM is set to JInitiator. If the JVM is set to Sun, the type is `application/x-java-applet`.	none - this field must be set if JVM is set to "JInitiator," and is ignored otherwise
viewData	If set to true, this parameters allows the end-user to view the collected data after it is posted to the server.	false

In addition to these parameters, the CSA redirection parameters can also be configured. Redirection can be enabled either by using a servlet filter or by including a CSA redirection JSP file in some other page. The following context parameters must be available for the redirection to work.

Table 11–2 Configuration Parameters

Parameter Name	Description	Default Value
csaURL	The URL of the CSA JSP page to which the user should be redirected.	No default: This value must be set or redirection cannot work.
execInterval	The interval, in seconds, between executions of CSA. If the difference between the cookie's age and the current server time is greater than execInterval, the user is re-directed.	None. If the execInterval is not set, then the user is only redirected if there is a CSA cookie.
redirectURL	The URL to which the user should be directed after CSA has executed	None. If this parameter is not set, the user is directed back to the originally requested page
UIMode	0 - synchronous (in the current browser window) 1 - asynchronous visible 2 - asynchronous invisible	synchronous

11.6.2.1 Associating the Parameters with an Application

In certain cases, different sets of parameters may be required for different applications. For example, two different applications may have different rule sets and custom code, and the administrator may want to associate them with different CSA Collector Targets. In this scenario, the administrator can specify the *ruleFile*, *appletJar*, *script*, and *outputDir* parameters for a particular application by using the context parameters

<application name> ruleFile, *<application name> appletJar*, and so on. If an application is specified, either as a context parameter or through the URL, then CSA is executed using the parameter values specific to the application. If no application is specified, or if one of the parameters for an application is not overridden, the default parameters are used.

11.6.3 Rules

Custom rules can be supplied to the CSA application so that the users receive immediate feedback as to whether their systems satisfy certain constraints. A sample RULES file is shown in Example 11–1 followed by a description of each tag contained in the file.

Example 11–1 Sample RULES

```
<RULES>
<RULE>
<NAME>Client has sufficient memory</NAME>
<DESCRIPTION>Checks to see if the client has enough memory to run the
application</DESCRIPTION>
<VIOLATION> //ROWSET[@TABLE='MGMT_ECM_HW']/ROW/AVAIL_MEMORY_SIZE_IN_MB[number()
&lt; $arg=SIZE$] </VIOLATION>
<SEVERITY level="CRITICAL">
<PARAM id='SIZE'>100</PARAM>
<MOREINFO>
<TEXT>Application cannot run with less than 100 MB. </TEXT>
</MOREINFO>
</SEVERITY>
<SEVERITY level="WARNING">
<PARAM id='SIZE'>150</PARAM>
<MOREINFO>
<TEXT>Approaching minimum memory level</TEXT>
</MOREINFO>
</SEVERITY>
</RULE>
</RULES>
```

Example 11–1 demonstrates a rule that can be used to check whether or not the client has sufficient memory to run the application. The <VIOLATION> is an XPATH expression that the applet will evaluate against an XML file that contains all of the data it has collected. Since the violation is an XPATH expression embedded in an XML file, certain characters in the XPATH, such as '<', '>', and '&', must be replaced with entities. If the XPATH expression returns a non-null node set, the rule has failed. In this case, the rule will fail if the client's available memory is less than a certain amount. The actual amount that triggers a violation can be configured by using different severity levels.

In Table 11–3, the applet will first replace the substring "$arg=SIZE$" in the VIOLATION expression with "100" and then evaluate the expression. If the client's available memory is less than 100 MB, then the rule will fail with critical status. The applet will indicate the status along with the message *Application cannot run with less than 100 MB of memory*. If the rule passes through successfully, the applet will then replace *$arg=SIZE$* with 150 and try again; if the rule fails, the applet will display the message *Approaching minimum memory level*. If the applet goes through all specified severity levels and does not find a violation, the rule is successful.

Table 11–3 Tags in the RULES File

Tag Name	Description
RULES	This is the top-level tag for the XML file
BUNDLE	This tag specifies the resource bundles used for translation. The value of the tag is either the name of a file or a Java class name. The rule engine reads this string and first attempts to find a file in the applet JAR that has this name. This file is expected to contain a mapping of resource IDs to strings in various languages. If such a file does not exist, then the string is treated as the name of a Java resource bundle class. Strings in a resource bundle are referenced using the syntax `<resource id>@<bundle id>`.
PRECONDITION	This tag is used to specify an XPATH expression that must return a non-null node set in order for a rule to be evaluated. The "id" attribute specified the ID of the precondition. A rule can specify a list of preconditions that should be evaluated by listing their IDs.
RULE	This tag represents an individual node that is to be evaluated. The rule's severity is specified using a <SEVERITY> tag. At least one severity tag must be specified for a rule. The tag has an optional "precondition" attribute, which is used to specify a list of precondition IDs separated by commas. Before the rule is evaluated, all of the preconditions must be met. If the pre-conditions are not met, the rule has a status of "Not Applicable" and is not displayed in the client UI at all. The children of a RULE tag are NAME, DESCRIPTION, VIOLATION, SEVERITY, and MOREINFO.
NAME	This tag specifies the name of the rule and identifies the tag in the repository. **Note:** This tag must contain a value and cannot be blank.
DESCRIPTION	This is the description of the rule.
VIOLATION	This tag lists the violations that are to be checked for a given rule. The violation is specified in the CSA Condition Language.
SEVERITY	A rule can have three severity levels: INFO, WARNING, and CRITICAL. The SEVERITY node must contain a number of ARG children equal to the number of arguments that can be accepted by the expression in the VIOLATION node. When the rule engine evaluates a rule, it evaluates the condition in VIOLATION for each of the sets of arguments specified in the severity levels, starting with CRITICAL and moving down in order of severity. As soon as the engine encounters a condition that fails, the rule is declared a failure, with a severity level equal to the severity level of the argument that caused the failure. If the conditions for all specified levels are met, the rule passes.
PARAM	This tag specifies the value of an argument that should be substituted into an expression. The 'id' attribute of the tag must match the name of one of the arguments in the expression.
MOREINFO	This tag specifies the information that is displayed if the user clicks the "more information" button that is displayed next to a failed rule. The children of MOREINFO are TEXT and ARG. **Note**: The MOREINFO node can be a child either of the severity node (in the case where multiple severities are specified) or of the rule itself.

Table 11–3 (Cont.) Tags in the RULES File

Tag Name	Description
TEXT	This tag specifies the text to be displayed when the "More Info" button is clicked. The "resource" attribute specifies a string in a resource bundle – if this string is not present, the value of the node is displayed instead. The text (either in the resource bundle or in the node itself) can specify a location for arguments to be inserted by using "{0}", "{1}", and so on. In this case, the expressions in the ARG nodes are evaluated and inserted into the text in the order in which they are specified. If there are more ARG nodes specified than there are slots in the string, the extra nodes are ignored.
ARG	This tag specifies an expression in the CSA Condition Language that can be evaluated and inserted into the MOREINFO text.

See Also: Enterprise Manager online help associated with the Getting Started with CSA page

11.6.4 Customization

In addition to writing custom classes to collect custom properties, the administrator can also specify custom properties in the deployment descriptor. Custom property names are specified by including a context parameter of the form *csa value_<name>*. The <name> field of the context parameter name is treated by the Client System Analyzer (CSA) as the custom property name, and the value of the parameter is treated as the custom property value. Similarly, administrators can specify the type, *type_ui*, *name_ui*, *display_ui*, and *history_tracking* fields for a custom property by using `csa_type_<name>`, `csa_type_ui_<name>`, `csa_name_ui_<name>`, `csa_display_ui_<name>`, and `csa_history_tracking_<name>` parameters, respectively. Custom properties can also be specified on the CSA Applet URL, using the same naming convention.

11.6.5 CSA Deployment Examples

The following sections outline sample use cases for client configurations.

11.6.5.1 Using Multiple Collection Tags

An administrator can check the compatibility of users with two distinct Web applications. The first is an online teaching website that delivers content using a number of various plug-ins, allowing an administrator to be sure that all users have the required installed plug-ins. The second is a software distribution portal that allows an administrator to ensure that all users downloading software from the portal have the required hardware and operating system. In this case, though both applications require their own set of rules, the administrator can use a single CSA instance for both applications through the use of collection tags displayed in the following list:

1. Choose a collection tag for each application, such as "teaching" and "distribution".
2. Create two separate rule files, one for each application.
3. Use context parameters to map each rule file to the corresponding application, as shown in Example 11–2.
4. Create the appropriate links from each application to CSA. The links from the teaching and distribution applications should have *application=teaching* and *application=distribution*, respectively, in the query string. This ensures that users of each application have the correct collection tags when running CSA.

Example 11–2 Using Collection Tags for Selecting a Rule File

```
<context-param>
  <param-name>csa teaching ruleFile</param-name>
  <param-value>teaching_rules.xml</param-value>
</context-param>

<context-param>
  <param-name>csa distribution ruleFile</param-name>
  <param-value>distribution_rules.xml</param-value>
</context-param>
```

Example 11–2 shows only the use of collection tags for selecting a rule file. However, collection tags can be used for any of the CSA context parameters.

Collection tags also affect how client configurations are stored in the Enterprise Manager Management Repository. If the user comes to CSA using the link from the teaching application in Example 11–2, then in addition to running the rules for the *teaching* collection tag, CSA also causes this tag to be stored with the client configuration data in the Management Repository. The collection tag forms part of the unique identifier for the client configuration, which makes it possible for a single client to have multiple configurations in the Management Repository, each with its own tag. Collection tags can be associated with Enterprise Manager targets in order to restrict access to client data; an Enterprise Manager user can only view a client configuration if he or she has view privileges on a target that is associated with the collection tag for that client configuration.

In Example 11–2, suppose that host H1, application server A1, and database D1 are used to host the teaching application, while host H2, application server A2, and database D2 are used for the distribution application. All 6 targets are monitored by Enterprise Manager, with user X having access to A1, H1, and D1 and user Y having access to A2, H2, and D2. Since each of the two Enterprise Manager users is monitoring the resources used for one of the applications, it may also make sense to have each user also monitor the application's clients. In that case, an Enterprise Manager super user would associate the *teaching* tag with A1, D1, or H1 and associate the *distribution* tag with A2, D2, or H2. This allows user X to see all client configurations with the *teaching* tag and user Y to see all configurations with the *distribution* tag.

11.6.5.2 Privilege Model for Viewing Client Configurations

Collection Tags are used to restrict access to client data in Enterprise Manager. A client configuration is visible to the user only if the Collection Tag for that configuration is associated with a target on which the user has View privileges. For example, if collection tag C is associated with target T1, then only those users that can view target T1 will be able to see client configurations that have tag X. In Example 11–2, user X will be able to see client configurations with the *teaching* tag because user X has view privileges on targets that are associated with the *teaching* tag. However, user X will not be able to see any client configurations with the *distribution* tag because that tag is not associated with any targets that user X can see. Super users can associate collection tags with targets by using the Collection Tag Associations page, which can be accessed from the Deployments tab or from the Client System Analyzer in Cloud Control link on the Setup page. Super users can view all client configurations regardless of any collection tag associations.

11.6.5.3 Using the Customization API Example

If the administrator is interested in the user's settings for an e-mail client in addition to the normal CSA data, the administrator can add this information to the other data collected by CSA through the use of the customization API, as shown in Example 11–3.

1. Create the Java classes required to gather the information. The administrator can create as many classes as necessary, but there must be at least one class that implements `oracle.symsan.eml.ecm.csa.CSAResultInterface` and one that implements `oracle.sysman.eml.ecm.csa.CSACustomInteface`, both of which are shown in Example 11–3. Assume that the former is acme.csa.custom and the latter is acme.csa.result.
2. Set the value of the "customClass" parameter in CSA to "acme.csa.custom"

Example 11–3 Customization API

```
public interface CSACustomInterface {

    /**
     * requires: none
     * effects: returns a CSAResultInterface object that may contain custom
     * properties. Other effects are determined by the customActions method
     * in the implementing class
     * modifies: unknown - dependent on implementing class.
     * @param inputData contains client config data collected by default, plus
     * applet parameters, etc.None of the data in the inputData is guaranteed
     * to be there as there could have been collection errors.
     * @return a data structure that may contain custom properties
     */
    CSAResultInterface customActions(CSAInputInterface inputData);
}

public interface CSAResultInterface {

    /**
     * requires: none
     * effects: returns an array of custom properties
     * modifies:none
     * @return String[][7] where ...
     *
     * String[i][0] is a name
     * String[i][1] is a value of the i-th row. (Type and name must be unique.)
     * String[i][2] is a type/category of data (could be null),
     * String[i][3] is the displayed value of the name of the property
     * String[i][4] is the displayed value of the type of the property
     * String[i][5] indicates data item (ie "Y") whose history should be computed
     * String[i][6] indicates data item (ie "Y") should be displayed in default UI
     */
    String[][] getResultsData();
}

public interface CSAInputInterface {

    /**
    * Get data value for given name
    * requires: name is not null
    * effects: returns the data value associated with the name
    * modifies: none
    * @param name the name of the key whose value is to be returned
    * @return the value assocaited with name
```

```
     *
     */
     String getDataValue(String name);

     /**
     * Get table-formatted data.
     * requires: name is not null
     * effects: returns the table with this name
     * modifies: none
     * @param name the name of the table
     * @return the rows of the child tables
     *
     */
     CSAInputInterface[] getDataTable(String name);
}
```

The additional data collected by the custom code will be stored in the table MGMT_ECM_CSA_CUSTOM. To add data to this table, the custom code returns it in an object that implements *CSAResultInterface*. The custom code can also manipulate the normal data collected by CSA by modifying the *CSAInputInterface* object passed to the customActions method by the applet.

Since the custom code is executed before rules are evaluated, the administrator can also write rules based on the custom data. For example, if the administrator wants to write a rule that raises a critical error if the user does not have the correct IMAP server set up his or her e-mail client, the administrator would write custom code that retrieves the IMAP server settings and stores in them in the MGMT_ECM_CSA_CUSTOM table and then writes a rule that checks these values.

11.6.5.4 Using the CSA Servlet Filter Example

Since CSA does not involve the use of a Management Agent on the user's machine, there is no way to keep the data in the Management Repository up to date unless end users run CSA periodically. One way to ensure that they do is to check whether or not users have run CSA recently, and if they have not, to inform them to run CSA again. This check can be accomplished using the CSA servlet filter provided by Oracle.

The CSA servlet filter works by checking the cookie that CSA sets in the user's browser whenever it runs. The payload of this cookie indicates the time at which CSA was last run. To use the filter, the administrator places it in front of some frequently accessed application, such as an employee portal. The administrator then sets the interval at which he or she wants users to run CSA. Whenever a user tries to connect to the portal application, the filter intercepts the request and checks the CSA cookie. If the cookie is not present or if it is older than the execution interval specified by the administrator, the user is directed to the CSA page; if not, the user is allowed to proceed to the application.

Assume that Acme Corporation has a CSA instance deployed at *www.acme.com/csa/CSA.jsp*. Assume also that the company has a portal at *www.acme.com/portal* that can be used by employees to check e-mail, access their personal information, or display news about the company. Because the portal is accessed frequently by employees, the administrator at Acme decides that the portal can be used to keep CSA data up to date. The administrator would take the following steps:

1. Download the CSA servlet filter classes. These classes are contained in a JAR file, *CSA_filter.jar*, which can be downloaded from the *Deploy Client System Analyzer* page in the Enterprise Manager Cloud Control console.

2. Place the JAR file in the *WEB-INF/lib* directory of the application to which the filter will be applied.
3. Specify context parameters for the filter. In this case, the administrator wants users to run CSA every 30 days and return to the portal homepage after CSA has finished.

```
<context-param>
  <param-name>csa csaURL</param-name>
 <param-value>www.acme.com/csa/CSA.jsp</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>
```

An alternative is to have CSA run in a separate browser window in the background. This can be set up by using the csa_uiMode parameter. If the parameter is set to 1, the filter will open a new browser window that is the same size as the original window and go to the CSA page. If the parameter is set to 2, CSA will run in *invisible* mode; in this case, the filter will open a new browser window and immediately minimize it, and it will close the window as soon as CSA has completed.

11.6.5.5 Sample Deployments

In the following sample deployment examples, there are three primary actors. The first is the CSA administrator, who is responsible for setting up CSA. The second is the Enterprise Manager user, who will be viewing the client data in Enterprise Manager. The third is the end user, whose data is being collected by CSA.

11.6.5.5.1 Example 1: Helpdesk

In this example, the CSA administrator is using CSA to support the operations of a helpdesk. End users who have problems running a particular application can call customer support, and the customer support technician can, if necessary, instruct the user to go to a particular URL and run CSA. The Enterprise Manager users are the support personnel who will use the data collected by CSA to assist the end user. To speed up the process of diagnosing the customer's problem, the CSA administrator creates some rules in a file called *rules.xml* so that the helpdesk personnel can quickly identify potential problems. In the simplest case, suppose that the helpdesk is being set up to provide support for a single application. The application is running on an application server on host application.acme.com, which has an Enterprise Manager Management Agent installed on it that sends data back to the Management Service at *oms.acme.com/em*. The helpdesk personnel who will be looking at client data can log into Enterprise Manager as the user *helpdesk*, which does not have super user privileges.

1. The CSA administrator adds *rules.xml* to the CSA.war file contained in *CSA.ear*.
2. Deploy the EAR file to the application server using the Application Services Control console.
3. Use the Application Services Control console to set the necessary context parameters, such as *ruleFile* and *outputDir*.
4. Optionally, the administrator can choose a collection tag for the CSA data by specifying a value for the *application* context parameter. If no tag is chosen, the tag *Default* will be used.

5. An Enterprise Manager user with super user privileges adds a CSA Collector Target to the Management Agent on *application.acme.com* and sets its receive file directory to the directory specified in the *outputDir* parameter of CSA.
6. An Enterprise Manager superuser creates the collection tag associations needed to allow the helpdesk users to look at the data. For example, the superuser could associate the tag *Default* with host *application.acme.com* and then give the *helpdesk* Enterprise Manager user view privileges on the host.

With the setup previously described, when a user calls the helpdesk to ask for support with the application, the helpdesk technician can instruct the user to run CSA from the appropriate URL on application.acme.com. The Management Agent collects the data after a certain interval and loads it into the Management Repository. The helpdesk technician can then log into Enterprise Manager as *helpdesk* and find the customer's information by searching for an identifying field such as the customer's operating system user name or host name. By default, the Management Agent will check the output directory for new data every two minutes, but this interval can be shortened by editing the file *$ORACLE_HOME/sysman/admin/default_collection/oracle_csa_collector.xml*.

11.6.5.5.2 Example 2: Inventory

In Example 11–4, a system administrator is in charge of keeping track of the hardware and software used by employees in two different departments, Human Resources (HR) and Sales. This administrator serves as both the Enterprise Manager user and the CSA administrator. The setup for this case is similar to the one described in the example on using servlet filters, but in this case, each department has its own portal application, at hr.acme.com/portal and sales.acme.com/portal, respectively. The administrator sets up an application server on host *server1.acme.com* and deploys CSA with the URL *http://server1.acme.com/csa/CSA.jsp*. A Management Agent on server1.acme.com collects data and sends to a Management Server at *oms.acme.com/em*. The administrator would like to collect data once every 30 days and to have CSA run in invisible mode. The administrator would also like to distinguish data from the two different departments by using two separate collection tags, *hr* and *sales*. The administrator can log into Enterprise Manager as sysman and will thus be able to see clients with both tags.

The administrator arranges to have users directed to CSA by deploying the CSA servlet filter on both applications. Most of the filter context parameters for the two applications will be identical. However, because each application corresponds to a different tag, the values of the *csa csaURL* parameter will be slightly different. For the HR portal, the value would be *http://server1.acme.com/csa/CSA.jsp?application=hr*, and for the sales portal, the value would be *http://server1.acme.com/csa/CSA.jsp?application=sales*.

Example 11–4 Inventory Code

```
<context-param>
  <param-name>csa csaURL</param-name>
 <param-value>www.acme.com/csa/CSA.jsp?application=sales</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>

<context-param>
  <param-name>csa uiMode</param-name>
```

```
  <param-value>2</param-value>
</context-param>
```

Under this setup, users in the HR department who are directed to CSA from the HR portal will have the tag *hr*, and users from the sales department will have the tag *sales*. Thus, if the administrator wants to see information about only hardware on machines in the HR department, he or she can simply use the *Collection Tag* filter on the Client Configurations page in Enterprise Manager and set it to *hr*.

11.6.5.5.3 Example 3: Problem Detection

In this example, the goal is to use CSA to inform end users of potential problems they may experience while running an application. The setup is similar to the one used in Example 2. In this example, however, the CSA administrator creates rules for each application. In addition, the administrator wants CSA to run in the original browser window to ensure that end users are aware of any potential problems.

Example 11–5 displays the context parameter values for the CSA servlet filter on the sales portal.

Example 11–5 Context Parameter Values for CSA Servlet Filter

```
<context-param>
  <param-name>csa csaURL</param-name>
 <param-value>www.acme.com/csa/CSA.jsp?application=sales</param-value>
</context-param>

<context-param>
  <param-name>csa execInterval</param-name>
  <param-value>2592000</param-value>
</context-param>

<context-param>
  <param-name>csa uiMode</param-name>
  <param-value>0</param-value>
</context-param>
```

Example 11–6 represents the context parameter definitions to map rules to collection tags.

Example 11–6 Context Parameter Definitions Mapping Rules to Collection Tags

```
<context-param>
  <param-name>csa sales ruleFile</param-name>
  <param-value>sales_rules.xml</param-value>
</context-param>

<context-param>
  <param-name>csa distribution ruleFile</param-name>
  <param-value>hr_rules.xml</param-value>
</context-param>
```

11.7 Configuring Privilege Delegation Providers

A privilege delegation provider is defined as a program that allows a logged in user to perform an activity with the privileges of another user. Typically, the privileges that are granted to a specific user are administered centrally.

Enterprise Manager preferred credentials allow you to use two types of privilege delegation providers:

- **Sudo**

  Sudo allows a permitted user to execute a command as the super user or another user, as specified in the sudo user administration file (*sudoers*). If the invoking user is root or if the target user is the same as the invoking user, no password is required. Otherwise, sudo requires that users authenticate themselves with a password by default.

  Note: (In the default configuration, this is the user's password, not the root password.

  Sudo determines who is an authorized user by consulting the file */etc/sudoers* file. Once a user has been authenticated, a timestamp is updated and the user may then use sudo without a password for a short period of time (5 minutes unless overridden in the *sudoers* file).

- **PowerBroker**

  Symark PowerBroker enables UNIX system administrators to specify the circumstances under which other users may run certain programs such as root (or other important accounts). The result is that responsibility for such actions as adding user accounts, fixing line printer queues, and so on, can be safely assigned to the appropriate people, without disclosing the root password. The full power of root is thus protected from potential misuse or abuse. For example, modifying databases or file permissions, or erasing disks.

  Symark PowerBroker can access existing programs as well as its own set of utilities that execute common system administration tasks. Utilities being developed to run on top of Symark PowerBroker can manage passwords, accounts, backups, line printers, file ownership or removal, rebooting, logging people out, killing their programs, deciding who can log in to where from where, and so on. They can also provide TCP/IP, Load Balancer, cron, NIS, NFS, FTP, rlogin, and accounting subsystem management. Users can work from within a restricted shell or editor to access certain programs or files as root.

  For additional information about Sudo or PowerBroker, see their respective product documentation.

Using Enterprise Manager's command line interface (EMCLI), you can set/edit privilege delegation provider properties for a host. See the *Oracle Enterprise Manager Command Line Interface* guide for more information. See your privilege delegation provider documentation for detailed setup and configuration information.

11.7.1 Creating a Privilege Delegation Setting

A privilege delegation setting can be created using the Enterprise Manager CLI command line interface's *create_privilege_delegation_setting* verb.

You can also configure a host with a Privilege Delegation setting, apply a Privilege Delegation setting template or unconfigure the Privilege Delegation setting by clicking **Setup** on the Enterprise Manager home page and then choosing *Manage Privilege Delegation Settings* from the left menu panel.

11.7.1.1 Creating a Sudo Setting Using EMCLI

Use the *create_privilege_delegation_setting* EMCLI verb to create a sudo privilege delegation setting. For explicit syntax and examples, see EMCLI command line help or the *Oracle Enterprise Manager Command Line Interface* guide.

Variables

You can used the following variables when using EMCLI to set the privilege delegation settings. Variables are case-sensitive.

Variable	Definition
%RUNAS%	Run the command as this user.
%USERNAME%	Name of the user running the command.
%COMMAND%	Sudo Command

Syntax

```
emcli create_privilege_delegation_setting -setting_name=sudo_
setting_1 -setting_type=SUDO -settings="SETTINGS:<command to be
used with all the options>"
```

The following example illustrates using EMCLI to create a sudo setting. Here, sudo is installed in */opt/sudo/bin*.

Example 11–7 Using EMCLI to Create a Sudo Setting

```
>emcli create_privilege_delegation_setting -setting_name=sudo_setting_1 -setting_
type=SUDO -settings="SETTINGS:/opt/sudo/bin/sudo -S -u %RUNAS% %command%"
```

11.7.1.2 Creating a PowerBroker Setting Using EMCLI

Use the *create_privilege_delegation_setting* EM CLI verb to create a PowerBroker privilege delegation setting.

Variables

You can used the following variables when using EMCLI to set the privilege delegation settings. Variables are case-sensitive.

Variable	Definition
%RUNAS%	Run the command as this user.
%USERNAME%	Name of the user running the command.
%COMMAND%	Sudo Command
%PROFILE%	Use this profile to run the command

Syntax

```
>emcli create_privilege_delegation_setting -setting_
name=powerbroker_setting_1 -setting_type=POWERBROKER
-settings="SETTINGS:<command to be used with all the
```

```
options>;[PASSWORD_PROMPT_STRING,<password prompt for
PowerBroker>]"
```

Example 11–8 Using EMCLI to Create a Sudo Setting

```
./emcli create_privilege_delegation_setting -setting_name=sudo_setting_1 -setting_
type=SUDO -settings="SETTINGS: /opt/powerbroker/bin/pbrun -u %RUNAS% %command%"
```

Note: In this example, PowerBroker is installed in */opt/powerbroker* directory and its password prompt is "Password:".

11.7.2 Applying Privilege Delegation Settings

Once you have created a privilege delegation setting, you must apply this setting to selected targets. As with the setting creation process, you use EMCLI to apply the privilege delegation setting to specified targets. The setting can be applied to one or more hosts or to a composite (Group) target (the group must contain at least one host target).

You can also apply a Privilege Delegation setting using the Cloud Control console by clicking **Setup** on the Enterprise Manager Home page and then choosing *Manage Privilege Delegation Settings* from the left menu panel.

11.7.2.1 Applying Settings to Host Targets Using EMCLI

Use the *apply_privilege_delegation_setting* EMCLI verb to apply privilege delegation settings to a host target.

Syntax

```
emcli apply_privilege_delegation_setting -setting_name=<setting
name> -target_type=host -target_names="host1;host2;..." -input_
file="FILE:hosts.txt" -force="yes/no"
```

To apply privilege delegation properties to a large number of hosts, you can specify a file containing all hosts by using the *-input_file* option in place of the *-target_names* option, as shown in the following example.

Example 11–9 Using EMCLI to Apply Privilege Delegation Settings to a Host Target

```
./emcli apply_privilege_delegation_setting -setting_name=<setting name> -target_
type=host -input_file="FILE: /mydirectory/file.txt" -force=yes
```

11.7.2.2 Applying Settings to a Composite Target

Use the *apply_privilege_delegation_setting* EMCLI verb to apply privilege delegation settings to a composite (group) target.

Syntax

```
emcli apply_privilege_delegation_setting -setting_name=<setting
name> -target_type=composite -target_names="group"
-force="yes/no"
```

Example 11–10 Using EMCLI to Apply Privilege Delegation Settings to a Composite Target

```
./emcli apply_privilege_delegation_setting -setting_name=<setting name> -target_
type=composite -input_file="FILE: /mydirectory/file.txt" -force=yes
```

Once the setting has been applied successfully to host targets, you can set their preferred credentials using EMCLI or through the Cloud Control console.

11.7.3 Disabling Host Privilege Delegation Provider Settings Using EMCLI

To disable a privilege delegation setting, an administrator can create a new setting with disabled status and can apply it to the targets. This *disabled setting* can be applied to any privilege delegation provider (Sudo/PowerBroker). It will remove the setting from the host.

1. Create a new privilege delegation setting.

```
./emcli create_privilege_delegation_setting -setting_name= disabled_setting
-setting_type=SUDO -disabled=yes
```

2. Apply the new setting to one or more targets.

```
./emcli apply_privilege_delegation_setting -setting_name= disabled_setting
-target_type=host  -target_names="host1;host2;..."  -force=yes
```

11.7.4 Sudo Configuration: Sudoers File

Enterprise Manager uses a trust-based model that permits specification of responsibilities with a high degree of granularity. Administrators can set up **sudo** or **pbrun** configuration entries to assign specific Enterprise Manager functional privileges to their OS users. A new executable has been introduced in the Management Agent called **nmosudo**. Administrators will be able to configure **sudo**/**pbrun** such that a less privileged user can run **nmosudo** as a more privileged user.

In the following example, if an administrator wants user 'joe' to run any Enterprise Manager job as user 'oracle', the corresponding entry in the */etc/sudoers* file would be:

```
(JOB_USERS) ALL : (RUNAS_USERS) AGENT_HOME /bin/nmosudo *
```

Where 'joe' would be in the JOB_BACKUP_USERS list and 'oracle' would be in the RUNAS_USERS list.

Enterprise Manager will guarantee that the **nmosudo** executable will only honor requests to run remote operation requests from the OMS via the Agent. **nmosudo** will not run the remote operation if it cannot validate that the request came from the Agent. Thus, as shown in the example above, it will not be possible for user 'joe' to invoke **nmosudo** directly from the command line and run a Perl script as user 'oracle'.

Note: To ensure system security, the administrator must provide the full path to the **nmosudo** executable.

11.7.5 Configuring Privilege Delegation Providers Using Cloud Control Console

Enterprise Manager Cloud Control allows you to configure Privilege Delegation Providers through functionality provided through its user interface. Using Cloud Control, you can avoid the command line interface while performing essentially the same functions.

The following sections describe the functions you can perform using the Cloud Control interface.

11.7.5.1 Configuring Sudo Settings For a Host Using Enterprise Manager Cloud Control Console

You can use Enterprise Manager to create a Sudo setting by using the Cloud Control console. You can create privilege delegation settings either by creating the setting directly on a host target, or by creating a PDP setting template that you can apply to multiple hosts.

To create a privilege delegation Sudo setting directly on a host, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. Setup > Manage > Privilege Delegation Settings.
2. For any host target appearing in the table, click **Edit**. Enterprise Manager takes you to the *Host Privilege Delegation Setting* page.
3. Select the **Sudo** privilege delegation type.
4. Enter the privilege delegation command to be used.
5. Click **Update** to apply the settings to the host.

> **Note:** If the host has been configured with either the Sudo or Powerbroker setting, choosing *None* on this page will remove (or disable) the setting.

11.7.5.2 Configuring PowerBroker Settings For a Host Using the Cloud Control Console

You can create privilege delegation settings either by creating the setting directly on a host target, or by creating a PDP setting template that you can apply to multiple hosts.

To create a privilege delegation PowerBroker setting directly on a host, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. Setup > Manage Privilege Delegation Settings.
2. For any host target appearing in the table, click **Edit**. Enterprise Manager takes you to the *Host Privilege Delegation Setting* page.
3. Select the **PowerBroker** privilege delegation type.
4. Enter the privilege delegation command to be used and the optional Password Prompt.
5. Click **Update** to apply the settings to the host.

> **Note:** If the host has been configured with either the Sudo or Powerbroker setting, choosing *None* on this page will remove (or disable) the setting.

11.7.5.3 Applying Settings to Multiple Host Targets Using the Cloud Control Console

You apply Privilege Delegation settings to a target using Privilege Delegation setting templates. If no template with the desired Privilege Delegation settings exists, you must first create the template on the *Manage Privilege Delegation Settings Template* page.

To create a template, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. Setup>*Manage Privilege Delegation Settings*.
2. From the Related Links section, click **Manage Privilege Delegation Setting Templates**.
3. Select a privilege delegation type (Sudo or PowerBroker) and click **Go**.
4. Fill in the requisite privilege delegation setting information.
5. Click **Save**.

If the desired privilege delegation settings template already exists, you need only apply the template to the desired host(s). To apply the template to the hosts, follow these steps:

1. Navigate to the *Manage Privilege Delegation Settings* page. *Setup > Manage Privilege Delegation Settings*.
2. Select the desired privilege delegation settings template from the Apply drop-down menu.
3. Click **Go** to access the *Apply Settings* page.
4. Add the targets (hosts) to which you want to apply the privilege delegation settings template.
5. Click **Apply**. Enterprise Manager displays the *Past Apply Operations* page where you can view the queue of scheduled apply operations along with those that are scheduled/pending. From this page, you can **Stop** or **Delete** apply operations.

You can also apply privilege delegation settings from the *Manage Privilege Delegation Setting Templates* page.

11.7.5.4 Disabling Host Privilege Delegation Provider Settings For One or More Hosts Using Cloud Control Console

You can disable a Privilege Delegation setting using the Cloud Control console. To disable a privilege delegation setting using this method, follow these steps:

1. Click **Setup** to access the *Enterprise Manager Configuration* page.
2. From the left menu, click **Manage Privilege Delegation Settings**.

   Cloud Control displays the *Manage Privilege Delegation Settings Page*.
3. Select the host(s) from which to clear the privilege delegation settings.
4. Click **Clear**. Enterprise Manager asks you whether to proceed with the privilege setting disable operation.
5. Click **Yes**.

11.8 Installing a Self-Signed Certificate For Production Environments

Out of the box, WebLogic Server is seeded with a demo certificate that references a short hostname, CN=<short hostname>. Oracle recommends that you seed a proper certificate for production environments. Additionally, if you use a full hostname in your URL, you will receive a warning because the hostname in the URL does not match the short hostname in certificate.

To install a self-signed certificate, run the following command:

```
DOMAIN_HOME/bin/secureWebLogic.sh -admin_host <hostname> -admin_
port <port#> -admin_user <username> [-admin_pwd <pwd>]
```

For Windows platforms, use the following command:

```
DOMAIN_HOME\bin\secureWebLogic.bat -admin_host <hostname>
-admin_port <port#> -admin_user <username> [-admin_pwd <pwd>]
```

To enable security for the Agent, run the following command:

```
ORACLE_HOME/bin/emctl secure fmagent -admin_host <hostname>
-admin_port <port#> -admin_user <username> [-admin_pwd <pwd>]
```

For Windows platforms, use the following command:

```
ORACLE_HOME\bin\emctl.bat secure fmagent -admin_host <hostname>
-admin_port <port#> -admin_user <username> [-admin_pwd <pwd>]
```

11.9 Modifying Web Service Retry Values

When Web Service invocations are made within Enterprise Manager, it is possible for the call to fail with a transient *connection refused* error. In this scenario, the invocation can be retried with a loop.

There are two parameters that can affect the retries. The first is *oracle.sysman.emSDK.webservices.outbound.WSI_num_retries*, which specifies the total number of times the call will be made in a loop. The second is *oracle.sysman.emSDK.webservices.outbound.WSI_retry_interval*, which is the amount of time in milliseconds that will transpire between each retry. The default value for the number of retries is 6 while the default value for the interval is 10000 (10 seconds). These values can be modified by specifying different values in *emoms.properties* using the following steps:

1. Change directory to the following location in the Fusion Middleware home directory where the Management Service was deployed:

   IAS_HOME/sysman/config/

2. Using your favorite text editor, open the *emoms.properties* file and add the following entry:

   oracle.sysman.emSDK.webservices.outbound.WSI_num_retries=<value>

   For example, if you want to change the default number of retries to 10, add the following entry:

   ```
   oracle.sysman.emSDK.webservices.outbound.WSI_num_retries=10
   ```

3. Save and close the *emoms.properties* file.

4. Restart the Oracle Management Service.

12

Configuring Enterprise Manager for Firewalls

Firewalls protect a company's Information Technology (IT) infrastructure by providing the ability to restrict network traffic by examining each network packet and determining the appropriate course of action.

Firewall configuration typically involves restricting the ports that are available to one side of the firewall, for example the Internet. It can also be set up to restrict the type of traffic that can pass through a particular port such as HTTP. If a client attempts to connect to a restricted port (a port not covered by a security "rule") or uses a protocol that is incorrect, then the client will be disconnected immediately by the firewall. Firewalls can also be used within a company Intranet to restrict user access to specific servers.

You can deploy the components of Oracle Enterprise Manager on different hosts throughout your enterprise. These hosts can be separated by firewalls. This chapter describes how firewalls can be configured to allow communication between the Enterprise Manager components.

This chapter contains the following topics:

12.1 Firewall Configuration Considerations

Firewall configuration should be the last phase of Enterprise Manager deployment. Before you configure your firewalls, make sure you are able to log in to the Cloud Control console and that your Management Agents are up and monitoring targets.

If you are deploying Enterprise Manager in an environment where firewalls are already installed, open the default Enterprise Manager communication ports for all traffic until you have completed the installation and configuration processes and are certain that you are able to log in to Cloud Control and that your Oracle Management Agents are up and monitoring targets.

The default communication ports for Enterprise Manager are assigned during the installation. If you modify the default ports, be sure to use the new port assignments when you configure the firewalls.

If you are enabling Enterprise Manager Framework Security for the Oracle Management Service, 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 Oracle Management Service 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.

12.1.1 Enabling ICMP Echo Requests on Firewalls

Oracle Management Service 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 be 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 Oracle Management Service to check the status of the machine.

By default, port 7 will be used for the ICMP Echo Request.

12.2 Overview of Enterprise Manager Components and Ports

As described in the previous sections of this chapter, it is important to understand and identify the ports used by each of the Oracle Enterprise Manager components before you configure your firewalls.

12.2.1 Viewing a Summary of the Ports Assigned During Installation

The last panel in the Oracle Enterprise Manager Cloud Control installer, which is displayed just before the actual installation is started, list all of the ports assigned during the installation.

Post-installation, you can view these values in the `staticports.ini` file at the following location on the OMS host:

`<MIDDLEWARE_HOME>/.gcinstall_temp/staticports.ini`

You can get the Middleware Home value by viewing the Oracle Home target for the Oracle Management Service in Cloud Control.

12.2.2 Default Port Assignments for Enterprise Manager Components

Table 12–1 notes the default ports and/or port ranges assigned to various Enterprise Manager components that should be accessible through a firewall. These components include WebLogic Server components created as part of the WebLogic domain the Enterprise Manager installation belongs to, as well as optional components such as JVM Diagnostics and Application Dependency and Performance.

Table 12–1 Default Ports and Port Ranges for Enterprise Manager Components

Port	Default Values
Enterprise Manager Upload HTTP Port	4889 - 4898
Enterprise Manager Upload HTTPS (SSL) Port	1159, 4899 - 4908
Management Agent Port	3872
Management Repository Database Port	1521

Table 12–1 (Cont.) Default Ports and Port Ranges for Enterprise Manager Components

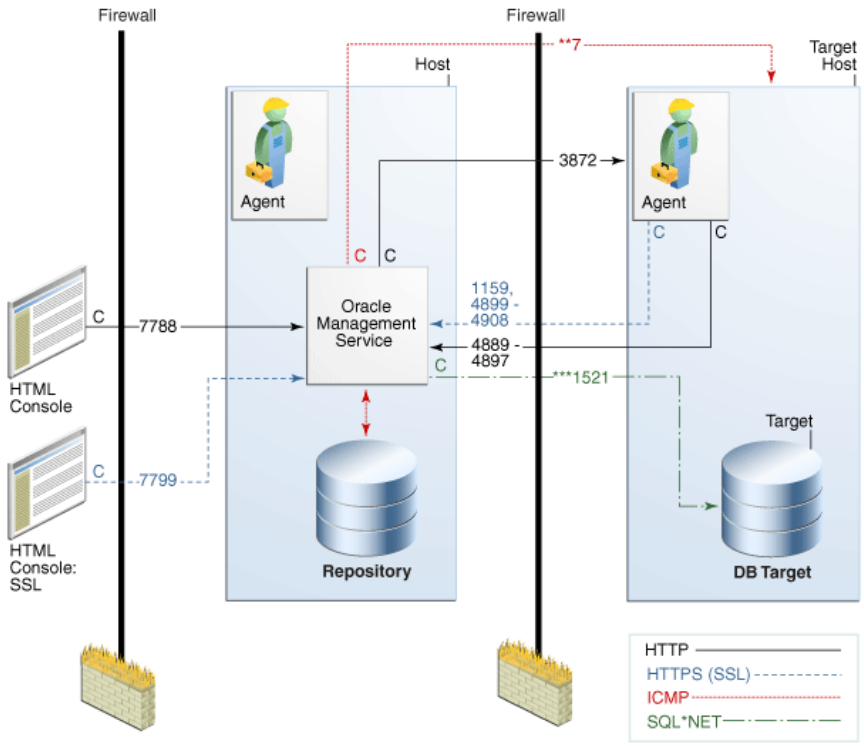
Port	Default Values
Cloud Control Console HTTP Port	7788 - 7798
Cloud Control Console HTTPS (SSL) Port	7799 -7809
EM Domain WebLogic Admin Server HTTP Port	7001
EM Domain WebLogic Admin Server HTTPS (SSL) Port	7101 - 7200
Cloud Control Managed Server HTTP Port	7201 - 7300
Cloud Control Managed Server HTTPS (SSL) Port	7301 - 7400
WebLogic Node Manager HTTPS (SSL) Port	7401 - 7500
JVM Diagnostics Managed Server	3800
JVM Diagnostics Managed Server (SSL)	3801
Application Dependency and Performance RMI Registry Port	51099
Application Dependency and Performance Java Provider Port	5503
Application Dependency and Performance Remote Service Controller Port	55000

12.3 Firewall Configurations for Enterprise Management Components

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 12–1 provides a topology of an Enterprise Manager system that is using a firewall, and also illustrates the default ports that can be used.

Figure 12–1 Firewall Port Requirements (Default)



The conventions used in the preceding illustration are as follows:

Table 12–2 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.
***	Are the Database listener ports.

Notes:

- The direction of the arrows specify the direction of ports.
- Port 1159, 4898-4989 specify that 1159 is the default. If this port is not available, the Management Service will search in the range that is specified.
- 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 agent will make the call.

The following sections describe the ports and types of data required by Enterprise Manager in a secure, firewall-protected environment:

- Firewalls Between Your Browser and the Cloud Control Console

12.3.1 Firewalls Between Your Browser and the Cloud Control Console

Connections from your browser to the Cloud Control console are performed over the default port used for your Oracle HTTP Server.

For example, the default, non-secure port for the Oracle HTTP Server is usually port 7788. If you are accessing the Cloud Control console using the following URL and port, then you must configure the firewall to allow the Cloud Control console to receive HTTP traffic over port 7788:

```
http://mgmthost.acme.com:7788/em
```

On the other hand, if you have enabled security for your Oracle HTTP Server, you are likely using the default secure port for the server, which is usually port 7799. If you are accessing the Cloud Control console using the following URL and port, then you must configure the firewall to allow the Cloud Control console to receive HTTPS traffic over port 7799:

```
https://mgmthost.acme.com:7799/em
```

12.3.2 Configuring the Management Agent on a Host Protected by a Firewall

If your Management Agent is installed on a host that is protected by a firewall and the Oracle Management Service 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 Oracle Management Service.
- Configure the firewall to allow incoming HTTP traffic from the Oracle Management Service on the Management Agent port. Regardless of whether or not Enterprise Manager Framework Security has been enabled, the default port is 3872. Incoming traffic can be received only if the port corresponding to the Management Agent is open in the firewall.

12.3.2.1 Configuring the Management Agent to Use a Proxy Server

You can configure the Management Agent to use a proxy server for its communications with a Oracle Management Service outside the firewall, or to manage a target outside the firewall.

1. Select **Agents** from the **Setup** menu.
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 `proxyHost` and `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.

12.3.2.2 Configuring the Firewall to Allow Incoming Communication From the Oracle Management Service

While the Management Agents in your environment must upload data from your managed hosts to the Oracle Management Service, the Oracle Management Service must also communicate with the Management Agents. As a result, if the Management Agent is protected by a firewall, the Oracle Management Service must be able to contact the Management Agent through the firewall on the Management Agent port.

By default, the Enterprise Manager installation procedure assigns port 3872 to the Management Agent. However, if that port is occupied, the installation may assign an alternate port number.

After you determine the port number assigned to the Management Agent, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

> **See Also:** Your firewall documentation for more information about opening specific ports for HTTP or HTTPS traffic.

12.3.3 Configuring the Oracle Management Service on a Host Protected by a Firewall

If your Oracle Management Service 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 Oracle Management Service to use a proxy server for its communications to the Management Agents.
- Configure the firewall to allow incoming HTTP traffic from the Management Agents on the Management Repository upload port.

  If you have enabled Enterprise Manager Framework Security, the upload URL uses port 1159 by default. If this port is not available, Enterprise Manager will default to first available port in the range 4899-4908. If you have *not* enabled Enterprise Manager Framework Security, the upload port is the first available port in the range 4889 - 4897.

12.3.3.1 Configuring the Oracle Management Service to Use a Proxy Server to Communicate with Management Agents

This section describes how to configure the Oracle Management Service to use a proxy server for its communications with Management Agents outside the firewall.

To configure the Oracle Management Service to use a proxy server, do the following:

1. Select **Proxy Settings** from the **Setup** menu.
2. Under "Agent Connection Setting", click **Manual Proxy Configuration**.
3. Supply the necessary HTTP or HTTPS property values for your configuration.

4. Click **Apply** to save your changes to the `OMS_HOME/sysman/config/emd.properties` file for the OMS instance.
5. After you have supplied your configuration, supply a Management Agent URL (or use the URL supplied by default) to test it.

12.3.3.2 Configuring the Firewall to Allow Incoming Management Data From the Management Agents

While the Management Agents in your environment must contact the Management Agents on your managed hosts, the Oracle Management Service must also be able to receive upload data from the Management Agents. If the Oracle Management Service is behind a firewall, you must configure the firewall to allow the Management Agents to upload data on the upload port.

By default, the Enterprise Manager installation procedure assigns port 4889 as the Repository upload port. However, if that port is occupied, the installation will assign an alternate port number.

In addition, when you enable Enterprise Manager Framework Security, the upload port is automatically changed to the secure 1159 HTTPS port.

Administrators can also change the upload port after the installation.

After you determine the port number assigned to the Oracle Management Service upload port, you must then configure the firewall to allow incoming HTTP or HTTPS traffic (depending upon whether or not you have enabled Enterprise Manager Framework Security) on that port.

> **See Also:** Your firewall documentation for more information about opening specific ports for HTTP or HTTPS traffic

12.3.3.3 Enabling Oracle Management Service to Access My Oracle Support

Unless online access to the Internet is strictly forbidden in your environment, Oracle Management Service 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:

- `support.oracle.com`
- `login.oracle.com`
- `servicecentral.sun.com`
- `updates.oracle.com`
- `loginadc.oracle.com`

12.3.3.4 About the dontProxyfor Property

When you configure the Oracle Management Service 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 Oracle Management Service and several Management Agents on hosts that are inside the company firewall. These hosts are in the internal `.acme.com` and `.acme.us.com` domains.
- You have installed several additional Management Agents on hosts that are outside the firewall. These hosts are installed in the `.acme.uk` domain.

- You have configured Enterprise Manager to automatically check for critical software patches on My Oracle Support.

In this scenario, you want the Oracle Management Service to connect directly to the Management Agents inside the firewall without using the proxy server. On the other hand, you want the Oracle Management Service 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 Oracle Management Service 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.acme.com
proxyHost=80
dontProxyFor=.acme.com, .acme.us.com
```

12.3.4 Firewalls Between the Oracle Management Service and the Management Repository

Secure connections between the Management Service and the Management Repository are performed using features of Oracle Advanced Security. As a result, if the Management Service and the Management Repository are separated by a firewall, you must configure the firewall to allow Oracle Net firewall proxy access.

12.3.5 Firewalls Between Cloud Control and a Managed Database Target

When you are using the Cloud Control console to manage a database, you must log in to the database from the Cloud Control 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 Oracle Management Service to communicate with the database through the Oracle Listener port.

You can obtain the Listener port by reviewing the Listener home page in the Cloud Control console.

See Also: *Oracle Database Advanced Security Administrator's Guide*

12.3.6 Firewalls Used with Multiple Oracle Management Services

Enterprise Manager supports the use of multiple Oracle Management Services that communicate with a common Management Repository. For example, using more than one Oracle Management Service can be helpful for load balancing as you expand your central management capabilities across a growing e-business enterprise.

When you deploy multiple Oracle Management Services in an environment protected by firewalls, be sure to consider the following:

- Each Management Agent is configured to upload data to one Oracle Management Service. As a result, if there is a firewall between the Management Agent and its Oracle Management Service, you must configure the firewall to allow the

Management Agent to upload data to the Management Service using the upload URL.

> **See Also:** "Configuring the Management Agent on a Host Protected by a Firewall" on page 12-5

> "Configuring the Oracle Management Service on a Host Protected by a Firewall" on page 12-6

- In addition, each Oracle Management Service 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 Oracle Management Service you deploy can communicate over HTTP or HTTPS with any Management Agent in your enterprise.

  Otherwise, a Oracle Management Service without access to a particular Management Agent may report incorrect information about whether or not the Management Agent is up and running.

  > **See Also:** "About Availability" in the Enterprise Manager online Help for information about how Enterprise Manager determines host and Management Agent availability

12.3.7 Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons

Oracle Beacons provide application performance availability and performance monitoring. They are part of the Service Level Management features of Enterprise Manager.

> **See Also:** "About Service Level Management" in the Enterprise Manager Online Help

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) to transfer data between Beacon 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.

13

Installing ADP with Advanced Installation Options

This chapter describes how you can install Application Dependency and Performance (ADP) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

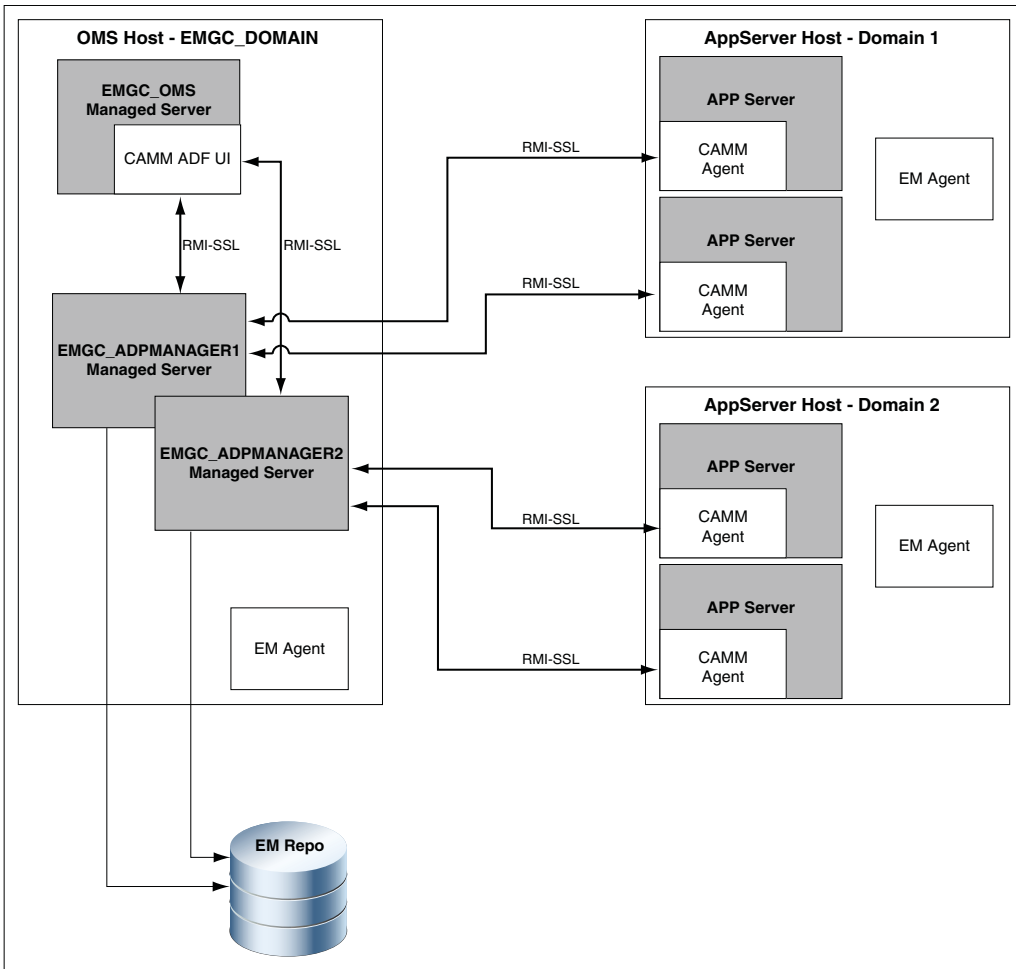
13.1 Application Dependency and Performance Architecture

Application Dependency and Performance (ADP) is one of the critical functionalities in Enterprise Manager Cloud Control that allows you to analyze Java EE, SOA, and Portal applications. It captures the complex relationships among various application building blocks in its application schema model - the core of the Oracle intelligent platform. To manage these applications effectively, enterprises must first gain an understanding of the complex relationships among the business functions, associated interconnected components, and the underlying runtime environments. To enable clear and accurate understanding, IT organizations need holistic, service-oriented views that span across heterogeneous environments.

Using the insights stored in Application Schema, ADP is able to deliver an Application Service Management (ASM) environment that self-customizes out-of-the-box, evolves with change, minimizes expert involvement, and delivers a holistic, service-oriented view across heterogeneous environments.

ADP employs a multi-tier, fully distributed, configurable architecture to provide the scalability and flexibility to meet the changing needs of enterprise deployments.

Figure 13–1 ADP Architecture



ADP Manager is the core analytical engine of the ADP ASM system. In real-time, ADP Manager performs complex mathematical modeling and statistical calculations with summarized data from all ADP Java Agents. ADP Manager can be configured with a backup to provide higher level of availability.

ADP Java Agents are the data collectors of the ADP ASM system. ADP Java Agents are deployed to all managed application servers to perform a series of tasks including collecting performance managements, tracking contextual relationships, and summarizing data in real-time while introducing as little overhead as possible.

13.2 Before you Begin

Before installing an ADP Manager, or an ADP Agent, review the points outlined in the *Basic Install Guide*.

13.3 Prerequisites

Before installing an ADP Manager, or an ADP agent, ensure that you meet the prerequisites described in the *Basic Install Guide.*

13.4 Installation Procedure

This section describes the following:

- Deploying ADP Manager on a Previously Created Managed Server
- Deploying ADP Agents (Remote Deployment)

13.4.1 Deploying ADP Manager on a Previously Created Managed Server

To deploy ADP Manager on a previously created managed server, you must log in with `SYSMAN` account (a default Super Administrators account that is installed with Enterprise Manager).

This section contains the following topics:

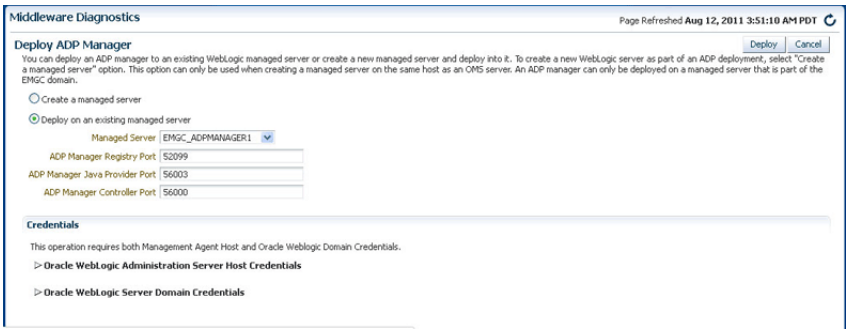
- Deploying ADP Manager on an OMS Host
- Deploying ADP Manager on a Separate Host from OMS (Remote Deployment)

13.4.1.1 Deploying ADP Manager on an OMS Host

To deploy ADP Manager on a previously created managed server running on an OMS host, perform the following steps:

1. In Cloud Control, from the **Setup** menu, select **Middleware Diagnostics**.
2. On the Middleware Diagnostics page, click **Deploy ADP Manager.**

   The ADP Manager deployment page appears.
3. To deploy ADP Manager on an existing managed server, select **!Deploy on an existing managed server.**



Perform the following steps

a. From the **Managed Server** menu, select the WebLogic Managed Server on which you want to deploy the ADP Manager application. Ensure that you select managed server with the name `EMGC_ADPMANAGER*` to deploy the ADP manager application.

   For example, `EMGC_ADPMANAGER1`, `EMGC_ADPMANAGER2`, and so on.

b. The Port numbers for **ADP Manager Registry Port, ADP Manager Java Provider Port,** and **ADP Manager Controller Port** are populated with the default values 51099, 55003, and 55000 respectively. You can change these values by entering custom value if required.

Note: An ADP Manager can only be deployed on a managed server that is part of the EMGC domain.

---

4. Depending on the host selected in the previous step, you are prompted for the credentials. The following cases are possible:

   - If you select the same host (`EMGC_OMS1`) where the Administration Server is running, then you must enter the **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials**.
   - If you select a host (`EMGC_OMS2`) different from the Administration Server to deploy ADP Manager, then in addition to **Oracle WebLogic Administration Server Host Credentials** and **Oracle WebLogic Server Domain Credentials**, you must provide **Oracle WebLogic Managed Server Host Credentials**.

   Where,

   Oracle WebLogic Administration Server Host Credentials are credentials for the host where the WebLogic Administration Server is running.

   Oracle WebLogic Server Domain Credentials are credentials of the WebLogic domain for Enterprise Manager Cloud Control.

   Oracle WebLogic Managed Server Host Credentials are the credentials of the host machine where the managed server is running.

5. Click **Deploy** to submit the job.

   The ADP Deployment Status Page appears with a link to the job status page, click the link to see the status of the job that you submitted.

Note: After the ADP Application is successfully deployed on the targeted managed server, to view the managed server in the WebLogic Domain, or to add a ADP agents, ensure that you refresh the WebLogic Domain as follows:

1. In Cloud Control, from **Targets** menu, select **Middleware**. On the Middleware home page, select the WebLogic Domain on which the ADP Manager application is deployed.
2. From the WebLogic Domain menu, select **Refresh WebLogic Domain**, and click **Continue**.
3. All the newly added targets are discovered in the WebLogic Domain, and then click **Add Targets**.
4. After adding the targets successfully, close the dialog box, and then click **OK**.

13.4.1.2 Deploying ADP Manager on a Separate Host from OMS (Remote Deployment)

To deploy ADP Manager on a separate host from OMS (remote deployment), you must perform the following tasks:

- Prerequisites
- Installation Procedure

Prerequisites

Before deploying ADP Manager on a separate host from OMS (remote deployment), perform the following steps:

Note: This section will use the following convention:

- `host-a` is the host where the OMS server is running
- `host-b` is the remote host which means that there is no OMS running on the host machine.

1. Install a Management Agent on `host-b` (remote host)

   For information about installing a Management Agent, see *Basic Install Guide*.

2. Install WebLogic Server on `host-b` using Enterprise Manager Software Only installation option.

   For information about performing a software only install, see

   These WebLogic Server bits must be registered with the Enterprise Manager Domain running on `host-a`, so that all the managed servers appear under the same WebLogic Domain.

   Note: For a successful installation, all managed servers running on different hosts in a WebLogic Domain must have the same version and patch level.

3. Configure a new managed server (`ADPRemoteServer`) using the WebLogic Server Administration Console as follows:

   a. Log into the Enterprise Manager WebLogic Domain console (`EMGC_DOMAIN`) of `host-a`.

      The WebLogic Server Administration Console home page appears.

   b. In Weblogic Server Administration Console, from the Domain Structure section, select Environment and then click **Servers**.

   c. On the Create a New Server page, enter the Server Name, Server Listen Address, and Server Listen port.

      Note: Ensure that the Server Listen Address corresponds to the listen address of the remote host, and the Server Listen port is free on the remote host.

4. Configure a new machine using the WebLogic Server Administration Console as follows:

   a. Log into the Enterprise Manager WebLogic Domain console (`EMGC_DOMAIN`) of `host-a`.

      The WebLogic Server Administration Console home page appears.

   b. In WebLogic Server Administration Console, from the Domain Structure section, select Environment and click **Machines.**

   c. To associate this machine with the nodemanager running on host-b, associate this machine with the nodemanager running on host-b, enter the **Listen Address** of the remote host, and the node manager port number which is 5556 by default.

      This node manager primarily controls the start and stop of a remote host.

d. Click **Finish** to create the machine.

5. Select the new created machine, and click on **Servers** to add the managed server (`ADPRemoteServer`) to this machine. This step associates the machine with the nodemanager running on `host-b`.

6. To extend the WebLogic Domain, a template of the Enterprise Manager Cloud Control domain running on `host-a` is created using the following command:

```
./pack.sh - domain = $DOMAIN_HOME -template = <absolute_path_to_the_new_
weblogic_template> - template_name="My WebLogic Domain" -managed={true}

Where:

$DOMAIN_HOME is the location of EMGC domain on host-a.

<absolute_path_to_the_new_weblogic_template> is the location where you want to
create the template.
```

7. Copy `emgcdomain.jar from host-a` (where the OMS is running) to `host-b` (remote host).

8. Run the following command to `unpack emgcdomain.jar` template on host-b:

```
./unpack.sh -domain = $DOMAIN_HOME -template= <absolute_path_to_domain_
template_created>

Where:

$DOMAIN_HOME is the domain location of EMGC on host-b (remote host)

<absolute_path_to_domain_template_created> is the location of the template on
host-b where emgcdomain.jar template is present.
```

9. To enroll the WebLogic Domain with node manager, perform the following steps on `host-b`:

   a. Run the following command to update the node manager properties file so that it can start monitoring the remote host:

      ```
      $WEBLOGIC_HOME/common/bin/wlst.sh

      nmEnroll($DOMAIN_HOME)
      ```

   b. Start the Node Manager as follows:

      ```
      $WEBLOGIC_HOME/bin/startNodeManager.sh
      ```

      Note: Ensure that you set the property in the nodemanager property file before starting the Node Manager. You can set the property in one of the following methods:

      - Manually edit the nodemanager.properties file to set the property `startScriptEnabled=true.`
      - Run the script `setNMProps.sh` as follows: `$MIDDLWARE_HOME/oracle_common/common/bin/setNMProps.sh`

   c. Perform the following steps to modify `startWebLogic.sh`:

      a. Navigate to the following location:

- On Unix : `$DOMAN_HOME/bin/startWebLogic.sh`

- On Windows : `$DOMAN_HOME/bin/startWebLogic.cmd`

b. Set maximum heap size (`-Xmx`) to 1.7GB for 64 bit systems and set maximum permanent generation (`-XX:MaxPermSize`) to 768M for 64 bit systems as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1740m -XX:MaxPermSize=768m"
```

c. Set max heap size to 1.4GB for 32 bit systems and set maximum permanent generation to 512M for 32 bit system as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1434m -XX:MaxPermSize=512m"
```

10. Perform the following steps on host-a, and then start the `ADPRemoteServer` as follows:

a. Copy the `emreposauthbean.jar` file to the following location:

```
$ cp $OMS_HOME/sysman/jlib/emreposauthbean.jar
<middleware_home>/wlserver_10.3/server/lib/mbeantypes/
```

Where, `$OMS_HOME` is the location of the OMS server on host-a

b. Import SSL Certificate to Enterprise Manager Agent Trust store present on the host where managed server (`ADPRemoteServer)` is running.

c. Start the managed server (`ADPRemoteServer)` from the WebLogic Server Administration Console to complete the WebLogic Server setup.

11. Perform the following steps to discover the new managed server running on `host-b`:

a. In cloud Control, from **Targets** menu, select **Middleware.**

On the Middleware page, from the list of WebLogic Servers running, select the WebLogic Domain (`EMGC_DOMAIN`) where the managed server is deployed.

b. On The Cloud Control Domain page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

The new server now gets registered in the Enterprise Manager Cloud Control Domain.

12. Restart the server for all the changes to take effect.

Installation Procedure

To deploy ADP Manager on a separate host from OMS (remote deployment), perform the following steps:

Note: For a successful remote deployment, ensure that:

- You install Enterprise Manager agent on the remote machine, and point it to the OMS running on a different managed server present in the same Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`)
- The remote WebLogic Server version and patch level should match with servers in Enterprise Manager Domain (`EMGC_DOMAIN`). To ensure that the versions and patch levels match, Oracle recommends that you install WebLogic by selecting the Software Only install option in the Enterprise Manager OUI install.

1. In Cloud Control, from **Setup** menu, select **Middleware Diagnostics**.
2. From the Middleware Diagnostics page, click **Deploy Application Dependency and Performance Manager (ADP).**

   The ADP Manager deployment page appears.
3. To deploy ADP Manager on the managed server running on a separate host from OMS, perform the following steps:
   a. Select **Deploy on an existing Managed Server**. For example, `EMGC_ADPMANAGER2`, `EMGC_ADPMANAGER3`, and so on.
   b. The Port numbers for **ADP Manager Registry Port, ADP Manager Java Provider Port,** and **ADP Manager Controller Port** are populated with the default values 51099, 55003, and 55000 respectively. You can change these values by entering custom value if required
4. In the Credentials section, provide **Oracle WebLogic Administration Server Host Credentials**, **Oracle WebLogic Domain Credentials**, and **Oracle WebLogic Managed Server Host Credentials.**

   Where,

   Oracle WebLogic Administration Server Host Credentials are credentials for the host where the WebLogic Administration Server is running.

   Oracle WebLogic Domain Credentials are credentials of the WebLogic domain in the Enterprise Manager Cloud Control.

   Oracle WebLogic Managed Server Host Credentials are the credentials of the host machine where the Managed Server is running.
5. Click **Deploy** to submit the job.

   The progress page appears with a link to the job processing page. Click the link to see the status of the job that you submitted.

13.4.2 Deploying ADP Agents (Remote Deployment)

To deploy ADP Agents on a Weblogic Domain which is monitored by the Management Agent present in the Enterprise Manager WebLogic Domain, perform the following steps:

Note: This section will use the following convention:

- `host-a` corresponds to the WebLogic Domain where the ADP Agent will be deployed.
- `host-b` corresponds to the Enterprise Manager Domain (`EMGC_DOMAIN`) where the Management Agent is deployed to monitor the WebLogic Domain on host-a.

1. In Cloud Control, from **Targets** menu, select **Middleware**.

   The Middleware page displays a list of all the Middleware targets discovered and managed in Cloud Control. Click target name to select the desired target.

2. On the Middleware page, click **Oracle WebLogic Domain**. Ensure that the selected domain is not an Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`).

   Note: ADP Agent cannot be deployed on a managed server (WebLogic Server) present in the Enterprise Manager domain.

   All the managed servers present in the selected domain appear on the domain home page.

3. From the **WebLogic Domain** menu, select **Diagnostics,** and then click **Setup Diagnostics Agents** to deploy ADP agents to the selected managed servers.

4. On the Deploy Diagnostics Agents page, choose the Oracle WebLogic Server (managed server) to which you want to deploy the ADP agents.

   Note:

   Ensure that you retain the selection of only those Diagnostic Agent(s) that you want to deploy to each of the managed server, deselect the others.

   In Addition to the managed server selected, the ADP Agent is deployed to the Administration Server of the selected domain.

   By default, the following servers appear deselected:

   - The Administration server.
   - All the managed servers that are not up and running.
   - If the **Deployed Version** and the **Version to Deploy** are the same, and the status of the already deployed ADP agent is up and running.

5. In the Diagnostics Agent Configuration section, enter the **ADP Configuration Properties** for the selected agents:

   - Select the desired ADP Manager from the **ADP Manager** list.

     The ADP agents after deployment will report to the selected ADP Manager.

   - If you select the **Update Remote Start configuration** option, then some configuration scripts run in the background to facilitate the monitoring process. Select this option if you use node manager to stop or start the WebLogic Servers to which ADP agent is being deployed.

Important: If WebLogic domain on `host-a` is discovered using Management Agent on `host-b`, then you must do the following:

1. Navigate to the following location:

   ```
   <WEBLOGIC_HOME>/server/lib

   Where,
   <WEBLOGIC_HOME> is the full abstract path to the Weblogic home
   for the monitored WebLogic domain on host-a.
   ```

2. Do the following to generate `wlfullclient.jar`:

   If the WebLogic Server version is 10.3.x or higher, then run the following command:

   ```
   java -jar wljarbuilder.jar
   ```

   If the WebLogic Server version is less than 10.3.x, then use other WebLogic installations (10.3.x or higher) to create the `wlfullclient.jar`.

   For example, you can use the `<WEBLOGIC_DOMAIN>` corresponding to the EMGC domain for generating the `wlfullclient.jar`, since Enterprise Manager setup uses JDK6.

3. Copy the following files from `<WEBLOGIC_HOME>/server/lib/` to `<AGENT_HOME>/sysman/jlib` directory:

   - `wlfullclient.jar`
   - `cryptoj.jar`
   - `webserviceclient+ssl.jar`
   - `wlcipher.jar`

   Where `<AGENT_HOME>` is the Oracle home for the Management agent on host-b.

6. If Management Agent present on host-b is used to monitor the WebLogic Domain on host-a (remote Agent) where the ADP Agent will be deployed, then you must provide credentials for **Oracle WebLogic Administration Server Host Credentials**, **Oracle WebLogic Domain Credentials, Oracle Enterprise Manager WebLogic Administration Server Host Credentials,** and **Oracle Enterprise Manager WebLogic Domain Credentials.**

   Where,

   Oracle WebLogic Administration Server Host Credentials are the credentials for the host-b, where the Management Agent used to discover the monitored domain is present.

   Oracle WebLogic Domain Credentials are credentials of the WebLogic domain of host-a, where the ADP Agent will be deployed.

   Oracle Enterprise Manager WebLogic Administration Server Host Credentials are credentials of host-b where the Administrator Server of `EMGC_DOMAIN` exists.

   Oracle Enterprise Manager WebLogic Domain Credentials are credentials of the WebLogic Domain of host-b (`EMGC_DOMAIN`).

7. Click **Deploy** to submit the job.

The status page appears with a link to the job status. Click the link to see the status of the job that you submitted.

Note:

- Restart the administration server, and the managed servers to which the ADP Agents have been deployed. These servers should be restarted only after the deployment has completed successfully.
- If the ADP Agent deployment fails with an SSL handshake error, see "SSL Handshake Failure Agent Deployment Errors" to fix the problem.

13.5 After You Install

After installing the ADP Managed Server, or the ADP Agent, follow the steps outlined in the *Basic Installation Guide*

14

Installing JVMD with Advanced Install Options

This chapter describes how you can install JVM Diagnostics (JVMD) in the Enterprise Manager Cloud Control environment.

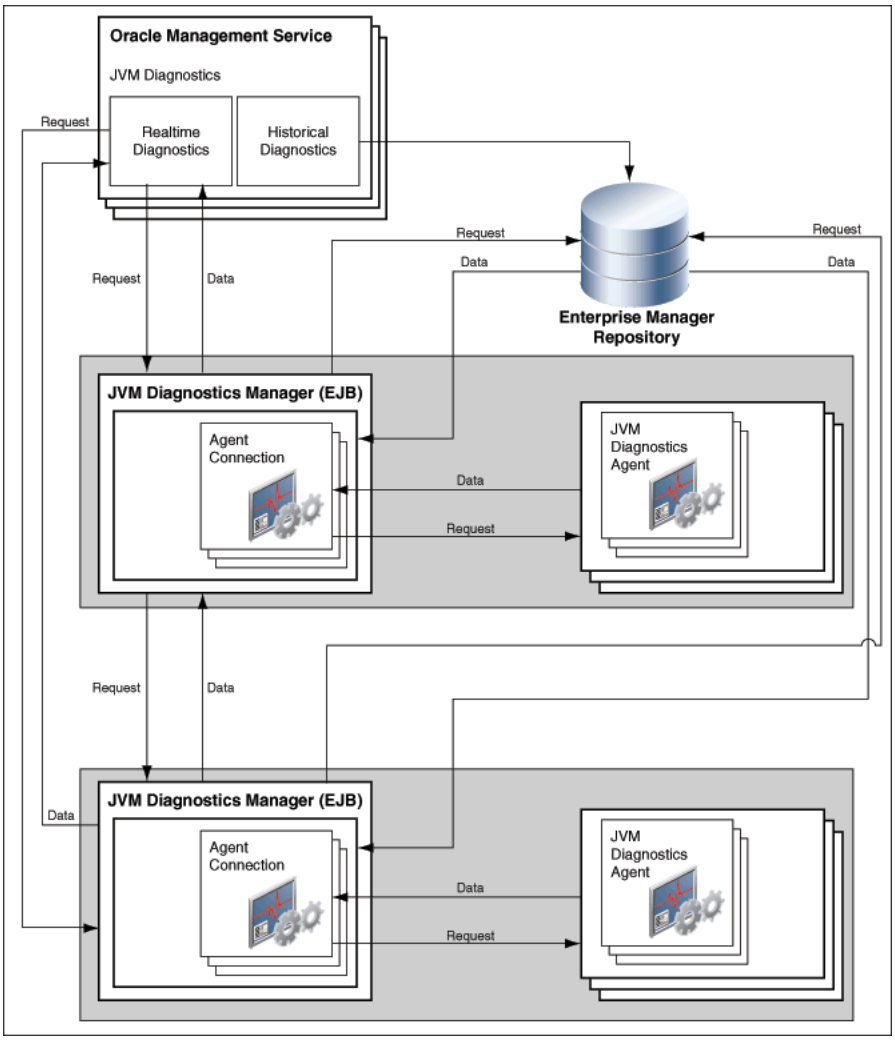
In particular, this chapter covers the following:

14.1 JVMD Architecture

JVM Diagnostics is integrated with Oracle Enterprise Manager Cloud Control. It primarily enables administrators to diagnose performance problems in Java applications in the production environment. By eliminating the need to reproduce problems, it reduces the time required to resolve these problems thus improving application availability and performance. Using JVMD, administrators will be able to 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 14–1 JVMD Architecture



JVMD Manager is the core analytical engine of the JVMD monitoring system. JVMD Manager collects runtime data from JVMD Agents on request from OMS or while monitoring during which it sends periodic requests to the JVMD agents and collects runtime JVM data and stores it into repository. Multiple JVMD Managers 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 in real-time while introducing minimal overhead.

The JVMD Manager runs as an Enterprise JavaBeans (EJB) Technology on a WebLogic Server. The JVMD Agent is deployed on the targeted JVM (the one running a production WebLogic Server). It collects real-time data and transmits it to the JVM Diagnostics Manager. This data is stored in the Management Repository, and the collected information is displayed on Enterprise Manager Cloud Control console for monitoring purposes. The communication between the JVMD Manager and the JVMD Agent can be a secure (SSL) or non-secure connection.

14.2 Before you Begin

Before installing an JVMD Manager, or an JVMD Agent, review the points outlined in the *Basic Install Guide*.

14.3 Prerequisites

Before installing the JVMD Manager, or the JVMD agent, ensure that you meet the prerequisites described in the *Basic Install Guide.*

14.4 Installation Procedure

This section contains the following topics:

- Deploying JVMD Manager on a Previously Created Managed Server
- Deploying JVMD Agents

14.4.1 Deploying JVMD Manager on a Previously Created Managed Server

To deploy JVMD Manager on a previously created managed server, you must log in with `SYSMAN` account (a default Super Administrators account that is installed with Enterprise Manager).

The following deployment options are possible:

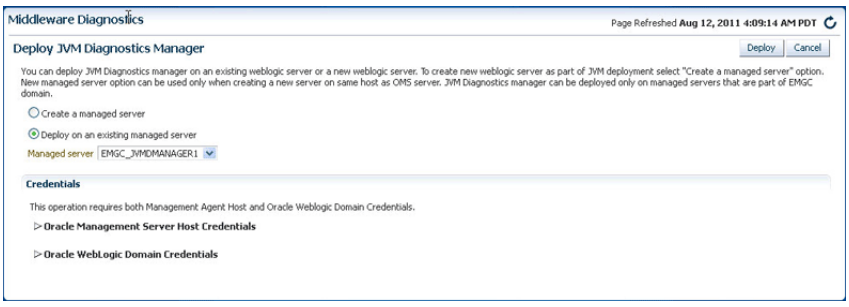
- Deploying JVMD Manager on an OMS Host
- Deploying JVMD Manager on a Separate Host from OMS (Remote Deployment)

14.4.1.1 Deploying JVMD Manager on an OMS Host

To deploy JVMD Manager on a previously created managed server which is running on an OMS host, perform the following steps:

1. In Cloud Control, from **Setup** menu, select **Middleware Diagnostics**.
2. On the Middleware Diagnostics page, click **Deploy JVM Diagnostics Manager (JVMD).**

   The JVMD Manager deployment page appears.
3. To deploy JVMD Manager on the managed server running on an OMS host, perform the following steps:
   a. Select **Deploy on an existing Managed Server**.
   b. From the **Managed Server** menu, select the managed server on which you want to deploy the JVMD Manager. For example, `EMGC_JVMDMANAGER1` , `EMGC_JVMDMANAGER2` , and so on.



The managed server selected for deploying JVMD Manager can be of any WebLogic Domain including Enterprise Manager Cloud Control domain.

4. Specify the O**racle Management Server Host Credentials** and **Oracle WebLogic Server Domain Credentials**:

   Where,

   Oracle Management Server Host Credentials are the credentials for the host machine where the Managed Server is created.

   Oracle WebLogic Server Domain Credentials are credentials of the Weblogic domain in the Enterprise Manager Cloud Control.

5. Click **Deploy** to submit the job.

   The progress page appears with a link to the job processing page. Click the link to see the status of the job that you submitted.

Note: After the JVMD Application is successfully deployed on the targeted managed server, to view the managed server in the WebLogic Domain, or to add a JVMD agents, ensure that you refresh the WebLogic Domain as follows:

1. In Cloud Control, from **Targets** menu, select **Middleware**. On the Middleware home page, select the WebLogic Domain on which the JVMD Manager application is deployed.
2. From the WebLogic Domain menu, select **Refresh Weblogic Domain**, and click **Continue**.
3. All the newly added targets are discovered in the WebLogic Domain, and then click **Add Targets**.
4. After adding the targets successfully, close the dialog box, and then click **OK**.

14.4.1.2 Deploying JVMD Manager on a Separate Host from OMS (Remote Deployment)

To deploy JVMD Manager on a separate host from OMS (remote deployment), you must perform the following tasks:

- Prerequisites
- Installation Procedure

Prerequisites

Before deploying JVMD Manager on a separate host from OMS (remote deployment), perform the following steps:

Note: This section will use the following convention:

- `host-a` is the host where the OMS is running
- `host-b` is the remote host which does not have an OMS on the machine.

---

1. Install a Management Agent on `host-b` (remote host)

   For information about installing a Management Agent, see *Basic Install Guide*.

2. Install WebLogic Server on `host-b` using Enterprise Manager Software Only installation option.

   For information about performing a software only install, see

   These WebLogic Server bits must be registered with the Enterprise Manager Domain running on `host-a`, so that all the managed servers appear under the same WebLogic Domain.

   Note: For a successful installation, all managed servers running on different hosts in a WebLogic Domain must have the same version and patch level.

3. Configure a new managed server (`JVMDRemoteServer`) using the WebLogic Server Administration Console as follows:

   a. Log into the Enterprise Manager WebLogic Domain console (`EMGC_DOMAIN`) of `host-a`.

      The WebLogic Server Administration Console home page appears.

   b. In Weblogic Server Administration Console, from the Domain Structure section, select Environment and then click **Servers**.

   c. On the Create a New Server page, enter the Server Name, Server Listen Address, and Server Listen port.

      Note: Ensure that the Server Listen Address corresponds to the listen address of the remote host, and the Server Listen port is free on the remote host.

4. Configure a new machine using the WebLogic Server Administration Console as follows:

   a. Log into the Enterprise Manager WebLogic Domain console (`EMGC_DOMAIN`) of `host-a`.

      The WebLogic Server Administration Console home page appears.

   b. In Weblogic Server Administration Console, from the Domain Structure section, select Environment and click **Machines.**

   c. On the Create a New Machine page, to associate this machine with the nodemanager running on `host-b`, enter the **Listen Address** of the remote host, and the node manager port number which is 5556 by default.

      This node manager primarily controls the start and stop of a remote host.

   d. Click **Finish** to create the machine.

5. Select the new created machine, and click on **Servers** to add the managed server (`JVMDRemoteServer`) to this machine. This step associates the machine with the nodemanager running on `host-b`.

6. To extend the WebLogic Domain, a template of the Enterprise Manager Cloud Control domain running on `host-a` is created using the following command:

   ```
   ./pack.sh -domain = $DOMAIN_HOME -template = <absolute_path_to_the_new_
   weblogic_template> - template_name="My WebLogic Domain" -managed={true}

   Where:
   ```

```
$DOMAIN_HOME is the location of EMGC domain on host-a.

<absolute_path_to_the_new_weblogic_template> is the location where you want to
create the template.
```

7. Copy `emgcdomain.jar from host-a` (where the OMS is running) to `host-b` (remote host).

8. Run the following command to `unpack emgcdomain.jar` template on host-b:

```
./unpack.sh -domain = $DOMAIN_HOME -template= <absolute_path_to_domain_
template_created>

Where:

$DOMAIN_HOME is the domain location of EMGC on host-b (remote host)

<absolute_path_to_domain_template_created> is the location of the template on
host-b where emgcdomain.jar template is present.
```

9. To enroll the WebLogic Domain with node manager, perform the following steps on `host-b`:

   a. Run the following command to update the node manager properties file so that it can start monitoring the remote host:

      ```
      $WEBLOGIC_HOME/common/bin/wlst.sh

      nmEnroll($DOMAIN_HOME)
      ```

   b. Start the Node Manager as follows:

      ```
      <Weblogic Home>server/bin/startNodeManager.sh
      ```

      Note: Ensure that you set the property in the nodemanager property file before starting the Node Manager. You can set the property in one of the following methods:

      - Manually edit the nodemanager.properties file to set the property `startScriptEnabled=true.`
      - Run the script `setNMProps.sh` as follows: `$MIDLLEWARE_HOME/oracle_common/common/bin/setNMProps.sh`

   c. Perform the following steps to modify `startWebLogic.sh`:

      a. Navigate to the following location:

         - On Unix : `$DOMAN_HOME/bin/startWebLogic.sh`

         - On Windows : `$DOMAN_HOME/bin/startWebLogic.cmd`

      b. Set maximum heap size (`-Xmx`) to 1 GB for 64 bit systems and set maximum permanent generation (`-XX:MaxPermSize`) to 768M for 64 bit systems as follows:

         ```
         USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:MaxPermSize=768m"
         ```

         Note: If the remote Managed Server is started using sun JVM, then you must add following memory options to `USER_MEM_ARGS`: `XX:+Unlock-DiagnosticVMOptions` and `XX:+UnsyncloadClass`.

c. Set max heap size to 1 GB for 32 bit systems, and maximum permanent generation to 512M for 32 bit system as follows:

```
USER_MEM_ARGS="-Xms256m -Xmx1024m -XX:MaxPermSize=512m"
```

10. Perform the following steps on host-a, and then start the `JVMDRemoteServer` as follows:

    a. Copy the `emreposauthbean.jar` file to the following location:

    ```
    $ cp $OMS_HOME/sysman/jlib/emreposauthbean.jar $MIDDLWARE_
    HOME/wlserver_10.3/server/lib/mbeantypes/
    ```

    Where, `$OMS_HOME` is the location of the OMS server on host-a.

    b. Import SSL Certificate to Enterprise Manager Agent Trust store present on the host where managed server (`JVMDRemoteServer)` is running.

    c. Start the managed server (`JVMDRemoteServer)` from the WebLogic Server Administration Console to complete the WebLogic Server setup.

11. Perform the following steps to discover the new managed server running on `host-b`:

    a. In cloud Control, from **Targets** menu, select **Middleware.**

    On the Middleware page, from the list of WebLogic Servers running, select the WebLogic Domain (`EMGC_DOMAIN`) where the managed server is deployed.

    b. On the Cloud Control Domain page, from the **WebLogic Domain** menu, select **Refresh WebLogic Domain**.

    The new server now gets registered in the Enterprise Manager Cloud Control Domain.

12. Restart the server for all the changes to take effect.

Installation Procedure

To deploy JVMD Manager on a separate host from OMS (remote deployment), perform the following steps:

Note: For a successful remote deployment, ensure that:

- You install Enterprise Manager agent on the remote machine, and point it to the OMS running on a different managed server present in the same Enterprise Manager Cloud Control domain (`EMGC_DOMAIN`)
- The remote WebLogic Server version and patch level should match with servers in Enterprise Manager Domain (`EMGC_DOMAIN`). To ensure that the versions and patch levels match, Oracle recommends that you install WebLogic by selecting the Software Only install option in the Enterprise Manager OUI install.

---

1. In Cloud Control, from **Setup** menu, select **Middleware Diagnostics**.
2. From the Middleware Diagnostics page, click **Deploy JVM Diagnostics Manager (JVMD).**

   The JVMD Manager deployment page appears.

3. To deploy JVMD Manager on the managed server running on a separate host from OMS, perform the following steps:

   a. Select **Deploy on an existing Managed Server**.

   b. From the **Managed Server** menu, select the managed server on which you want to deploy the JVMD Manager. For example, `EMGC_JVMDMANAGER1`, `EMGC_JVMDMANAGER2`, and so on.

4. Specify the O**racle WebLogic Managed Server Host Credentials** and **Oracle WebLogic Domain Credentials**:

   Where,

   Oracle WebLogic Domain Credentials are credentials of the Weblogic domain in the Enterprise Manager Cloud Control.

   Oracle WebLogic Managed Server Host Credentials are the credentials for the host machine where the Managed Server is created.

5. Click **Deploy** to submit the job.

   The progress page appears with a link to the job processing page. Click the link to see the status of the job that you submitted.

14.4.2 Deploying JVMD Agents

To deploy JVMD Agents on a Weblogic Domain which is monitored by the Management Agent present in the Enterprise Manager Weblogic Domain, perform the following steps:

Note: This section will use the following convention:

- `host-a` corresponds to the WebLogic Domain where the JVMD Agent will be deployed.
- `host-b` corresponds to the Enterprise Manager Domain (`EMGC_DOMAIN`) where the Management Agent is deployed to monitor the WebLogic Domain on host-a.

---

1. In Cloud Control, from **Targets** menu, select **Middleware**.

   The Middleware page displays a list of all the Middleware related targets discovered, and being managed in Cloud Control. Click target name to select the desired target.

2. From the Middleware page, click **Oracle WebLogic Domain**.

   All the managed server present in the domain appear in the domain home page.

Note: JVMD Agent cannot be deployed on the ADP Managed Server present in the Enterprise Manager Domain. You can deploy JVMD Agents on Admin Server, OMS Server, or JVMD Managed Server in the Enterprise Manager Domain, or on any other WebLogic Domain.

---

3. From the **WebLogic Domain** menu, select **Deploy Diagnostics Agents** to deploy agents to the selected managed servers.

4. On the Deploy Diagnostics Agents page, choose the Oracle WebLogic Server (managed server) to which you want to deploy the JVMD Agents.

Note: Ensure that you retain the selection of only those Diagnostic Agent(s) that you want to deploy to each of the managed server, deselect the others.

By default, the following servers appear deselected:

- The Administration server.
- All the managed servers that are not up and running.
- If the **Deployed Version** and the **Version to Deploy** are the same, and the status of the already deployed JVMD agent is up and running.

5. In the Diagnostics Agent Configuration section, enter the **JVMD Configuration Properties** for the selected agents.

   Select the desired JVMD manager from the **JVMD Manager** list. The JVMD agents selected for deployment will report to this JVMD Manager.

   Important: If WebLogic domain on `host-a` is discovered using Management Agent on `host-b`, then you must do the following:

   1. Navigate to the following location:

      ```
      <WEBLOGIC_HOME>/server/lib

      Where,
      <WEBLOGIC_HOME> is the full abstract path to the Weblogic home
      for the monitored WebLogic domain on host-a.
      ```

   2. Do the following to generate `wlfullclient.jar`:

      If the WebLogic Server version is 10.3.x or higher, then run the following command:

      ```
      java -jar wljarbuilder.jar
      ```

      If the WebLogic Server version is less than 10.3.x, then use other WebLogic installations (10.3.x or higher) to create the `wlfullclient.jar`.

      For example, you can use the `<WEBLOGIC_DOMAIN>` corresponding to the EMGC domain for generating the `wlfullclient.jar`, since Enterprise Manager setup uses JDK6.

   3. Copy the following files from `<WEBLOGIC_HOME>/server/lib/` to `<AGENT_HOME>/sysman/jlib` directory:

      ```
      - wlfullclient.jar

      - cryptoj.jar

      - webserviceclient+ssl.jar

      - wlcipher.jar
      ```

      Where `<AGENT_HOME>` is the Oracle home for the Management agent on host-b.

6. If Management Agent present on host-b is used to monitor the Weblogic Domain on host-a (remote Agent) where the JVMD Agent will be deployed, then you must provide credentials for **Oracle Weblogic Administration Server Host Credentials** and **Oracle WebLogic Domain Credentials.**

Where,

Oracle WebLogic Administration Server Host Credentials are the credentials for the host-b, where the Mangement Agent used to discover the monitored domain is present.

Oracle WebLogic Domain Credentials are credentials of the WebLogic Domain of host-a, where the JVMD Agent will be deployed.

7. Click **Deploy** to submit the job.

   The progress page appears with a link to the job processing page. Click the link to see the status of the job that you submitted.

Note: If the JVMD Agent deployment fails with an SSL handshake error, see "SSL Handshake Failure Agent Deployment Errors" to fix the problem.

14.5 After You Install

After installing the JVMD Managed Server, or the JVMD Agent, follow the steps outlined in the *Basic Installation Guide*

15

Installing BI Publisher on Enterprise Manager

Oracle Business Intelligence (BI) Publisher is Oracle's primary reporting tool for authoring, managing, and delivering all your highly formatted documents. BI Publisher ships standard with Enterprise Manager Cloud Control 12c.

This chapter covers the following topics:

15.1 Overview

Though BI Publisher is still deployed as a separate installation, Enterprise Manager can be configured to integrate a BI Publisher installation within an Enterprise Manager domain: BI Publisher is installed into the same WebLogic Server domain as Enterprise Manager. Once configured, you will be able to take advantage of the standard features of BI Publisher such as:

- Highly formatted, professional quality, reports, with pagination and headers/footers.
- PDF, Excel, Powerpoint, Word, and HTML output of reports.
- Develop your own custom reports against the Enterprise Manager repository. (read-only repository access)
- Integration with Enterprise Manager Security.

- Grant varying levels of BI Publisher functionality to different Enterprise Manager administrators.
- Use BI Publisher's scheduling capabilities and delivery mechanisms such as e-mail and FTP.
- Format (report) can be edited separately from the data definition (data model).
- Standardized Enterprise Manager subtemplate for headers.
- Full NLS support for BI Publisher Report output.

> **Note:** The Information Publisher (IP) reporting framework is still supported for Enterprise Manager 12c, however, new report development using this framework has been deprecated for Enterprise Manager 12c.

15.2 BI Publisher Installation and Integration with Enterprise Manager 12c

The following procedures assume that you are familiar with both BI Publisher and Enterprise Manager installations. Refer to the *Oracle Enterprise Manager Basic Installation Guide* and the *Oracle Enterprise Manager Advanced Installation and Configuration Guide* for detailed information about Enterprise Manager.

15.2.1 Enterprise Manager and BI Publisher Inventory

Both Enterprise Manager and BI Publisher must be installed with a centralized inventory file. This means that `/etc/oraInst.loc` points to the same directory for both installs. Although it is possible to install both products with a special inventory specific to each product, this configuration is not a supported and will not allow complete integration between Enterprise Manager 12c and BI Publisher 11g.

15.2.2 Installing Enterprise Manager and Required Infrastructure

Run the Enterprise Manager 12c installer. Some of the Enterprise Manager provided BI Publisher Reports are part of the Chargeback and Trending plug-in, so these plug-ins will need to be installed in order to obtain those reports.Make sure to choose the **Advanced** installation type so that you can choose to install Enterprise Manager plug-ins, such as the Chargeback and Trending plug-ins, which contains several BI Publisher Reports.

> **Note:** Refer to the *Oracle Enterprise Manager Basic Installation Guide* for complete installation specifics.

15.2.2.1 Installing BI EE Using Software-only Install

Important: Integration requires Oracle Business Intelligence Enterprise Edition 11g (version 11.1.1.5.)

Do a software-only install of BI EE using the below steps:

1. Run the BI EE Publisher Installer: (Disk1/runInstaller).
2. (Optional) Choose E-Mail address for updates and click **Next**.
3. **VERY IMPORTANT**: Choose the **Software-only Install**.

4. Click **Next**. Prerequisite checks will run.
5. After passing prerequisite checks run, click **Next**.
6. Choose the Middleware home of your Enterprise Manager installation. This is the Middleware home that you created previously.
7. BI Oracle Home name must be left as the default *Oracle_BI1*. Click **Next**.
8. (Optional) Enter MOS credentials to be notified of security updates. Click **Next**.

When the software-only install of BI EE completes successfully, proceed to Section 15.2.2.2.

15.2.2.2 Integrating BI Publisher with Enterprise Manager Using the configureBIP Script

1. Integrating BI Publisher with Enterprise Manager will require changing the domain configuration. It is highly recommended to back up the domain in case of unforeseen errors during configuration. File permissions for the domain files must be maintained when creating a backup. For example, from the `<Instance_Home>/user_projects/domains` directory, run:

   ```
   zip -r EMGC_DOMAIN.zip EMGC_DOMAIN
   ```

2. From the OMS instance's `ORACLE_HOME/bin` directory, execute the *configureBIP* script from the command line. The script takes four inputs and then performs the Repository Creation Utility (RCU) step and then takes two more inputs, performs the extend-domain operations and finally deploys the Enterprise Manager-supplied BI Publisher Reports to the newly installed BI Publisher Web application.

   Script Input

   1. Enter a database user with sysdba privilege (typically 'sys'), then enter the password. (Enterprise Manager Repository database)
   2. Enter the *adminserver* and then the *nodemanager* password. These accounts are part of Enterprise Manager WebLogic Domain.

   Script Operation (RCU Steps)

   Script Operation describes what the *configureBIP* script is doing.

   1. RCU runs to create the BI Publisher schema. Note there will be some output printed on the screen.
   2. You will know that RCU was successful, if you see the following:

      ```
      ...
      ...
      Repository Creation Utility - Create : Operation Completed
      ```

   Extend Domain Steps

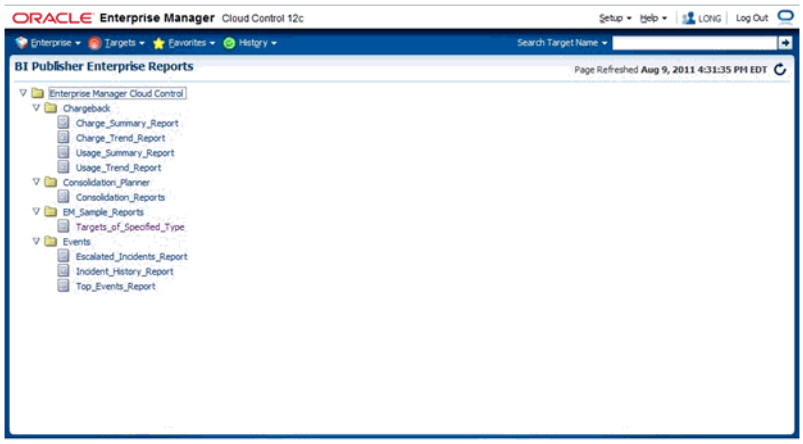
   1. You will then be asked to enter BI Publisher HTTP and HTTPS ports (either one or both). The script will identify free ports and ask if you want to take them as a default. Once entered, Extend Domain will then run
   2. The Enterprise Manager-supplied BI Publisher Reports will be deployed to the newly installed BI Publisher Web application.
   3. Once processing is complete, you will see something like the following screen output:

      ```
      Extending domain with BI Publisher. This may take a few minutes...
      ```

```
BI Publisher server running at http://host.us.oracle.com:9701/xmlpserver.
BI Publisher server running at https://host.us.oracle.com:9702/xmlpserver.
Registering BI Publisher with Enterprise Manager and deploying reports...
Successfully setup BI Publisher with Enterprise Manager
```

15.3 Verifying Integration of BI Publisher with Enterprise Manager

1. Log in to Enterprise Manager.
2. From the **Enterprise** menu, choose **Reports** and then **BI Publisher Enterprise Reports**.
3. Click the *refresh* icon at the top right of the Enterprise Manager window.
4. Enterprise Manager displays a tree list showing all of the Enterprise Manager-supplied BI Publisher reports as shown in the following graphic.



5. Click on the provided Enterprise Manager Sample Report: *Targets_of_Specified_Type*
6. Log in to BI Publisher using your Enterprise Manager credentials.
7. You will see the sample report rendered on the screen. You can then use the full capabilities of BI Publisher such as PDF report generation and e-mail.

15.4 Allowing Access to BI Publisher for Enterprise Manager Administrators

Once integrated, BI Publisher reports conform to the Enterprise Manager security model. The primary security attributes that apply to BI Publisher Reports are:

- Permissions
- Roles (or groups in the LDAP case)

15.4.1 Permissions

Enterprise Manager ships with certain Oracle-provided BI Publisher catalog objects. These catalog objects consist of:

- Folders
- Reports (layout definitions and translations)

- Datamodels (SQL queries against the Enterprise Manager repository)
- Subtemplates (standard Enterprise Manager header shown above all pages of all report output)

These catalog objects are created when BI Publisher is installed and integrated with Enterprise Manager. They are placed in the "Enterprise Manager Cloud Control" folder. These catalog objects are created with certain permissions that, combined with the roles/groups below, achieve the desired security model.

15.4.2 Roles (groups in the LDAP case)

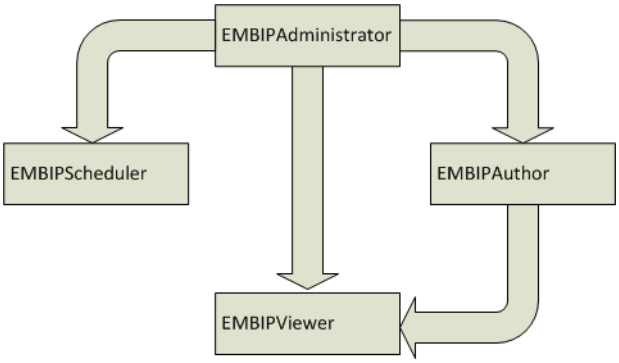
In addition, when BI Publisher is installed, four roles are created (non-LDAP), or in the LDAP case, four groups need to be created. These roles/groups are combined with the permissions on the catalog objects in the above folder to achieve the rules shown in the following sections.

15.4.3 BI Publisher Security Model

Below is a description of the effective security model placed on BI Publisher catalog objects that ship with Enterprise Manager.

- *None* - Enterprise Manager administrators without any BI Publisher role can receive BI Publisher Reports via delivery channels such as E-Mail or FTP.
- **EMBIPViewer** - Enterprise Manager administrators with this BI Publisher role can receive e-mails plus can view the Enterprise Manager-supplied BI Publisher reports.
- **EMBIPScheduler** - Enterprise Manager administrators with this BI Publisher role can receive e-mails and can schedule the Enterprise Manager supplied BI Publisher reports if they also have the **EMBIPViewer** role.
- **EMBIPAuthor** - Enterprise Manager administrators with this BI Publisher role can receive e-mails, view the Enterprise Manager-supplied BI Publisher reports, and can create new reports in their private folder. They can also copy the Enterprise Manager-supplied BI Publisher reports and customize them.
- **EMBIPAdministrator** (Super Users) - Enterprise Manager administrators with this BI Publisher role have complete access to BI Publisher.

The following diagram shows the hierarchy of the above roles:



Enterprise Manager Super Administrators

In a non-LDAP environment, all Enterprise Manager Super Administrators are automatically granted the **EMBIPAdministrator** role to facilitate setting up BI Publisher.

In an LDAP environment, Enterprise Manager Super Administrators are not automatically granted **EMBIPAdministrator** access to BI Publisher. See Section 15.5 for more information on allowing access to BI Publisher for Enterprise Manager Administrators in a LDAP environment.

15.5 Granting the EMBIP* roles to Enterprise Manager/BI Publisher Administrators

In the non-LDAP case, the domain policy store (OPSS) is used to control Enterprise Manager administrator access to objects in the BI Publisher catalog.

OPSS is the repository of system and application-specific policies. Details regarding OPSS can be found in the Oracle® Fusion Middleware Security Guide. In a given domain, there is one store that stores all policies (and credentials) that all applications deployed in the domain may use. As both Enterprise Manager and BI Publisher are separate applications, it is necessary to grant BI Publisher specific roles to Enterprise Manager administrators

In a non-LDAP environment, the command-line tool **wlst.sh** is used to manipulate the OPSS.

15.5.1 Granting BI Publisher roles to Enterprise Manager Administrators (non-LDAP) Using wlst.sh

wlst.sh can be used to grant access to the BI Publisher UI to Enterprise Manager administrators.

The following wlst.sh usage example demonstrates of using **wlst.sh** to grant view access to the Enterprise Manager administrator named "JERRY" (italicized items are entered at the command-line). It is important to use uppercase letters for Enterprise Manager Administrator names.

```
$MW_HOME/oracle_common/common/bin/wlst.sh
wls:/EMGC_DOMAIN/serverConfig> connect('weblogic','<pw>','t3s://host:port')

wls:/EMGC_DOMAIN/serverConfig>
grantAppRole(appStripe="obi",appRoleName="EMBIPViewer",principalClass="weblogic.se
curity.principal.WLSUserImpl",principalName="JERRY")
```

To revoke access to View BI Publisher reports from the user JERRY (case is important), enter the following:

```
wls:/EMGC_DOMAIN/serverConfig>
revokeAppRole(appStripe="obi",appRoleName="EMBIPViewer",principalClass="weblogic.s
ecurity.principal.WLSUserImpl",principalName="JERRY")
```

15.5.2 Propagation Time for Changes to OPSS

When changing an Enterprise Manager administrator's BI Publisher access privileges (**EMBIPViewer**, **EMBIPAdministrator**, **EMBIPScheduler**, **EMBIPAuthor**) the Super Administrator needs to wait 15 minutes for the changes to propagate through OPSS and become effective. The change will then be effective the next time the administrator logs into BI Publisher.

15.6 Allowing Access to BI Publisher for Enterprise Manager Administrators in a LDAP environment

As both Enterprise Manager and BI Publisher are separate applications, it is necessary to grant BI Publisher specific roles to Enterprise Manager administrators, which in this case are groups defined in the external LDAP. These different BI Publisher groups allow varying access to the BI Publisher UI. So, you can add an external LDAP user as a member of one or more of these external LDAP group above, and BI Publisher will expose specific parts of the BI Publisher UI to that user when they log in to BI Publisher. These groups, which need to be created as described in the following section, are coordinated with the permissions of the catalog object in the "Enterprise Manager Cloud Control" folder.

In an LDAP environment, similar concepts are employed to grant access to BI Publisher for different Enterprise Manager administrators. However, in an LDAP environment, Enterprise Manager administrators credentials are stored in the LDAP system.

In order to achieve the required security model described in Section 15.4.3, the following steps must be performed:

- The administrator of the LDAP server needs to create the following four external groups:
  - EMBIPAdministrators
  - EMBIPViewers
  - EMBIPSchedulers
  - EMBIPAuthors
- Make EMBIPAdministrators member of EMBIPAuthors

  Make EMBIPAdministrators member of EMBIPSchedulers

  Make EMBIPAuthors member of EMBIPViewers

> **Note:** In LDAP, the terminology and concepts can seem backwards and confusing. For example, you want the *EMBIPAuthors* group to have as a member the *EMBIPAdministrators* group.

Then, in order to grant access to BI Publisher and its catalog objects, the administrator of the LDAP server needs to make respective Enterprise Manager/LDAP users a member of one or more of the above LDAP groups.

15.7 Configuring BI Publisher with a Custom Trust Store

If you reconfigure your AdminServer to use a custom trust store, then you must also configure BI Publisher accordingly. This also requires the trust store for the OMS to contain the certificate for the BI Publisher-managed server.

In order to use a trusted certificate from a signing authority, create a Java Key Store (JKS) containing the user certificate of BI Publisher server.

> **Note:** If you use an e-mail server with SSL, you will need to add the e-mail server's certificate to your trust store as well.

15.8 BI Publisher Administration

Please refer to the BI Publisher documentation for instructions on configuring BI Publisher settings.

Common administrative tasks:

- Configuring server properties
- Configuring report delivery options

15.9 EMBIP* Roles: Granting Access to Folders and Catalog Objects

By default, the shipping security model (as described in Section 15.4.3, applies to BI Publisher catalog objects that are inside the "Enterprise Manager Cloud Control" folder. This is due to the fact that the catalog objects that exist in this folder are set up with a default set of permissions. See Section 15.4.1. BI Publisher catalog objects that are outside of this folder will not automatically contain these same permissions. For example, BI Publisher ships with numerous reports in a shared folder called "Samples". If it is desired to grant access to this folder to Enterprise Manager/BI Publisher users, other than EMBIPAdministrator, it is necessary for a BI Publisher super administrator (EMBIPAdministrator) to change the permissions of this folder. They do so by selecting the folder "Samples" and choosing "Permissions" in the bottom left task bar. They then need to add the four privileges (EMBIPAdministrator, EMBIPViewer, EMBIPAuthor, EMBIPScheduler) and grant appropriate access to that privilege such as *View report*, *run report online*, to EMBIPViewer. The administrator can model the appropriate privileges to grant based on any of the shipping Enterprise Manager reports (for example, Targets_of_Specified_Type).

Individual users, who have EMBIPAuthor, can develop reports in their own private folders. These reports will not be available to other users.

Note: The shared folder "Enterprise Manager Cloud Control" contains Enterprise Manager- provided BI Publisher Reports and is reserved for such. No custom-developed reports may be put in this folder hierarchy, and the default security model that ships with Enterprise Manager specifically prohibits this.

Note: Only reports in the "Enterprise Manager Cloud Control" will show up in the Enterprise Manager BI Publisher Enterprise Reports menu (Enterprise -> Reports -> BI Publisher Enterprise Reports).

If a BI Publisher administrator (EMBIPAdministrator) wishes to create a new shared folder outside of the "Enterprise Manager Cloud Control" folder, they can do so. These reports would not show up in the Enterprise Manager BI Publisher reports menu but would be available to other Enterprise Manager administrators as long as appropriate permissions are granted as previously described.

15.10 Access to Enterprise Manager Repository

All BI Publisher reports are granted read-only access to the Enterprise Manager Repository. This access is via the BI Publisher data source named **EMREPOS**. This access is via the Enterprise Manager user **MGMT_VIEW**, which is a special internal Enterprise Manager user who has read-only access to the Enterprise Manager

Published **MGMT$** and **GC$** database views. In addition, when reports are run, they are further restricted to the target-level security of the user running the report. For example, if user JOE has target-level access to "hostabc" and "database3", when user JOE runs a BI Publisher report (any report) he can only view target-level data associated with these two targets.

15.11 Troubleshooting

- Before attempting to re-run configureBIP, be sure to kill any existing BI Publisher processes.
- If BI Publisher is able to run successfully, but BI Publisher registration with Enterprise Manager fails, you can retry the registration by running:

```
emcli login -username=<admin username> -password=<admin password>
emcli sync
emcli setup_bipublisher -proto=http[s] -host=<bip_host> -port=<bip_port>
-uri=xmlpserver
```

- If the domain becomes corrupted, and you created a backup of your domain, you can restore your domain using the backup file.
  1. Stop the OMS and AdminServer using `emctl stop oms -all`
  2. Go to `<Instance_Home>/user_projects/domains`, move the <domain name> folder, and unzip the backed up <domain name> folder into its place.
  3. Restart the OMS and AdminServer using `emctl start oms`.

15.12 Managing the BI Publisher Server

BI Publisher operates as a separate, managed server in the same WebLogic domain that contains the OMS(s) and the AdminServer.

In order to shut down the BI Publisher managed server, do the following:

1. log in to the AdminServer console as the WebLogic user with the correct password.
2. Click on **Servers**
3. Click the **Control** tab underneath the text **Summary of Servers**.
4. Place a check-mark next to the managed server BI Publisher.
5. Double-check to make sure the check-mark is next to the BI Publisher managed server and not the EMGS_OMSx or EMGC_ADMINSERVER managed servers.
6. Click **Shutdown** and choose when work completes.
7. Wait until BI Publisher has shut down. You can monitor the status of this operation by clicking on the refresh icon (the two arrows in a circle) above the text **Customize this Table**.

To start the BI Publisher managed server, do the following:

1. Navigate to the control page using steps 1-4 above.
2. Place a check-mark next to the managed server BI Publisher.
3. Double-check to make sure the check-mark is next to the BI Publisher managed server and not the EMGS_OMSx or EMGC_ADMINSERVER managed servers.
4. Click **Start**.

5. Wait until BI Publisher has started. You can monitor the status of this operation by clicking on the refresh icon (the two arrows in a circle) above the text **Customize this Table**.

Part V

Deinstallation

In particular, this part contains the following chapters:

- Chapter 16, "Deinstalling Enterprise Manager Cloud Control"
- Chapter 17, "Deinstalling Oracle Management Agent"
- Chapter 18, "Deinstalling ADP and JVMD"

16

Deinstalling Enterprise Manager Cloud Control

This chapter describes how you can deinstall Enterprise Manager Cloud Control (the entire Enterprise Manager system, or one or more Oracle Management Services). In particular, this chapter covers the following:

16.1 Prerequisites

Before you deinstall Enterprise Manager Cloud Control, follow these steps:

1. Delete Oracle Management Service (OMS):
   - Deconfigure the plug-ins:

     ```
     $<OMS_HOME>/bin/pluginca -action deconfig -plugins
     <pluginname=pluginversion>
     ```

     For example,

     ```
     $<OMS_HOME>/bin/pluginca -action deconfig -plugins
     oracle.sysman.db=12.1.0.1.0,oracle.sysman.xa=12.1.0.1.0,or
     acle.sysman.emas=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,o
     racle.em.soee=12.1.0.1.0
     ```

   - Deconfigure and remove the OMS:

     ```
     $<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. Shut down Oracle Management Agent (Management Agent) by running the following command from the Management Agent home:

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

3. If you want to deinstall the entire Enterprise Manager system, including Oracle Management Repository (Management Repository) that is configured in your database, then follow these steps:

   a. Ensure that there are no SYSMAN users logged in.

   b. Drop the Enterprise Manager Cloud Control schema (SYSMAN schema) and the Metadata schema (MDS schema) from the Management Repository by running the following command from the OMS home:

   ```
   $<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <database_
   host> <repository_database_port> <repository_database_sid>
   -action dropall -dbUser <repository_database_user>
   -dbPassword <repository_database_password> -dbRole
   <repository_database_user_role> -reposName <repository_
   name> -reposPassword <repository_password> -mwHome
   <middleware_home> -mwOraHome <middleware_ora_home>
   -oracleHome <OMS_HOME>
   ```

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

   RepManager 12*c* and 11.1 support `-action dropall` (drops SYSMAN as well as SYSMAN_MDS) and `-action drop` (drops only SYSMAN). However, RepManager 10.2.0.5 supports `-action drop` (drops only SYSMAN)

   c. Manually delete the data files `mgmt.dbf` and `mgmt_ecm_depot1.dbf` from the database home.

   WARNING: Once the Management Repository is dropped, it CANNOT be retrieved. Therefore, drop the Management Repository ONLY IF you want to deinstall the entire Enterprise Manager Cloud Control system, that is, all your OMSes, Management Agents, and also the Management Repository. If you want to deinstall only an OMS (additional OMS installation), then do not drop the Management Repository.

16.2 Deinstallation Procedure

This section describes the following:

- Deinstalling in Graphical Mode
- Deinstalling in Silent Mode

16.2.1 Deinstalling in Graphical Mode

To deinstall Enterprise Manager Cloud Control in graphical mode, follow these steps:

Note: Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Invoke the installer from the OMS home by running the following command:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall [-removeallfiles]
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/`.
- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.

2. In the installation wizard, on the My Oracle Support Details screen, click **Installed Products**.
3. On the Inventory screen, select the plug-in homes, and click **Remove**.
4. On the Inventory screen, select the `sbin` home, and click **Remove**.
5. On the Inventory screen, select the Java Development Kit (JDK) home, and click **Remove**.

Note: Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

Note: After deinstalling JDK, do NOT exit the installer. If you exit the installer inadvertently, then follow these steps:

1. Manually download and install JDK 1.6 v24+ on the OMS host. If you already have this supported version, then you can reuse it.
2. Invoke the installer again and pass the absolute path to the location where you have JDK:

   ```
   $<OMS_HOME>/oui/bin/runInstaller -deinstall -jreLoc
   <JDK_HOME> [-removeallfiles] [-invPtrLoc <absolute_
   path_to_oraInst.loc>]
   ```

6. On the Inventory screen, select the Oracle WebTier home, and click **Remove**.
7. On the Inventory screen, select the following, and click **Remove**.
   - OMS home
   - Management Agent home
   - Oracle Common directory
8. On the Inventory screen, click **Cancel**.
9. On the My Oracle Support Details screen, click **Exit** to exit the installation wizard.
10. Deinstall Oracle WebLogic Server 11g Release 1 (10.3.5) following the instructions outlined in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*. See the chapter that describes how you can deinstall the software.

    The *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* is available in the Oracle WebLogic Server documentation library available at:

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

Note: Deinstall Oracle WebLogic Server 11g Release 1 (10.3.5) only if it was installed by the installation wizard while installing the Enterprise Manager system.

16.2.2 Deinstalling in Silent Mode

To deinstall Enterprise Manager Cloud Control in silent mode, follow these steps:

Note: Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Deinstall the plug-in homes:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_plug-in_home}" [-removeallfiles
-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/`.

  If you invoke the installer from here, then do NOT pass `-removeallfiles`.
- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
- To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.

For example,

```
$<OMS_HOME>/oui/bin/runInstaller  -deinstall -silent "REMOVE_
HOMES={/home/oracle/middleware/agent/plugins/oracle.sysman.ssa.oms.plugin_
12.1.0.1.0,/home/oracle/middleware/agent/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0}" -removeAllFiles -invPtrLoc
/home/oracle/oraInst.loc
```

2. Deinstall the `sbin` home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_sbin_home}" [-removeAllFiles]
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/home/oracle/middleware/agent/sbin}" -removeAllFiles
-invPtrLoc /home/oracle/oraInst.loc
```

3. Deinstall the Java Development Kit (JDK) home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_jdk_home}" [-removeAllFiles]
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/home/oracle/middleware/jdk16}" -removeAllFiles
-invPtrLoc /home/oracle/oraInst.loc
```

Note: Deinstall JDK only if it was installed by the installation wizard while installing the Enterprise Manager system. Otherwise, you can skip this step.

4. Manually download and install JDK 1.6 v24+ on the OMS host. If you already have this supported version, then you can reuse it.
5. Deinstall the Oracle WebTier home:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_web_tier}" -jreLoc <JDK_HOME>
[-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/home/oracle/middleware/Oracle_WT}" -jreLoc
</home/oracle/jdk> -removeAllFiles -invPtrLoc
/home/oracle/oraInst.loc
```

6. Deinstall the OMS, the Management Agent, and the Oracle Common directory:

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={absolute_path_to_oracle_homes_and_directories_to_be_
deinstalled}" -jreLoc <JDK_HOME> [-removeAllFiles]
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note: The argument `REMOVE_HOMES` accepts more than one path separated by a comma.

For example,

```
$<OMS_HOME>/oui/bin/runInstaller -deinstall -silent "REMOVE_
HOMES={/home/oracle/middleware/oms,/home/oracle/middleware/ag
ent/core/12.1.0.1.0,/home/oracle/middleware/oracle_common}"
-jreLoc </home/oracle/jdk> -removeAllFiles -invPtrLoc
/home/oracle/oraInst.loc
```

7. Deinstall Oracle WebLogic Server 11g Release 1 (10.3.5) following the instructions outlined in the *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*. See the chapter that describes how you can deinstall the software.

   The *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server* is available in the Oracle WebLogic Server documentation library available at:

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

Note: Deinstall Oracle WebLogic Server 11g Release 1 (10.3.5) only if it was installed by the installation wizard while installing the Enterprise Manager system.

16.3 After You Deinstall

The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. You might also see the OMS instance base directory and the Oracle home for Web Tier. You can manually delete these files and directories.

You must also manually delete the auto-start script titled S98gcstartup. To do so, navigate to the `/etc/rc.d/` directory, and search for the auto-start 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`

17

Deinstalling Oracle Management Agent

This chapter describes how you can deinstall Oracle Management Agent (Management Agent). In particular, this chapter covers the following:

- Prerequisites
- Deinstallation Procedure
- After You Deinstall

> **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.

17.1 Prerequisites

Before you deinstall a Management Agent, shut it down by running the following command from the Management Agent home:

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

17.2 Deinstallation Procedure

This section describes the following:

- Deinstalling in Graphical Mode
- Deinstalling in Silent Mode
- Deinstalling Shared Agent
- Deinstalling Oracle Management Agent Installed Using an RPM File

17.2.1 Deinstalling in Graphical Mode

To deinstall a Management Agent in graphical mode, follow these steps:

> **Note:** Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Invoke the installer from the Management Agent home by running the following command:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall
[-removeallfiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- You can invoke the installer even from the directory where you downloaded the software. For example, `<software_location>/`.
- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
- For Microsoft Windows, invoke the `setup.exe` file.

2. In the installation wizard, click **Installed Products.**
3. On the Inventory screen, select the plug-in homes, and click **Remove.**
4. On the Inventory screen, select the `sbin` home, and click **Remove.**
5. On the Inventory screen, select the Management Agent, and click **Remove.**

17.2.2 Deinstalling in Silent Mode

To deinstall a Management Agent in silent mode, follow these steps:

Note: Deinstall the components in the order described in this procedure. Otherwise, the installation wizard displays an error.

1. Deinstall the plug-in homes:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_plug-in_home}"
[-removeallfiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- When you run `runInstaller -help`, you will see the option `-nowarningonremovefiles` listed. This option is currently not supported and has no effect even if you use it.
- On Microsoft Windows, invoke the `setup.exe` file.
- On Microsoft Windows, `-invPtrLoc` is not supported.
- To deinstall multiple plug-ins, enter the plug-in homes separated by a comma.

For example,

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_
HOMES={/home/oracle/agent/plugins/oracle.sysman.emas.oms.plug
in_
12.1.0.1.0,/home/oracle/agent/plugins/oracle.sysman.emct.oms.
plugin_12.1.0.1.0}" -removeAllFiles -invPtrLoc
/home/oracle/oraInst.loc
```

2. Deinstall the sbin home:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_sbin_directory}"
[-removeAllFiles] [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

For example,

```
 $<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={/home/oracle/agent/sbin}" -removeAllFiles
-invPtrLoc /home/oracle/oraInst.loc
```

3. Deinstall the Management Agent:

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={absolute_path_to_agent_oracle_home}"
-removeAllFiles -invPtrLoc <absolute_path_to_oraInst.loc>
```

For example,

```
$<AGENT_HOME>/oui/bin/runInstaller -deinstall -silent
"REMOVE_HOMES={/home/oracle/agent/core/12.1.0.1.0}"
-removeAllFiles -invPtrLoc /home/oracle/oraInst.loc
```

17.2.3 Deinstalling Shared Agent

To deinstall a Shared Agent, follow these steps:

1. Identify the dependent plug-ins and the sbin home to be detached from the Central Inventory:
   a. On the host where the Shared Agent is installed, open the following file from the Central Inventory:

      <absolute_path>/oraInventory/ContentsXML/inventory.xml

   b. Make a note of the dependent plug-ins listed within the <REFHOMELIST> and </REFHOMELIST> tags.

      For example,

```
<HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
TYPE="O" IDX="1">
<REFHOMELIST>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.discovery.pl
ugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.db.discovery.pl
ugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.emas.discovery.
plugin_12.1.0.0.0"/>
<REFHOME
LOC="/home/john/software/oracle/agent/plugins/oracle.sysman.oh.agent.plugin
_12.1.0.0.0"/>
</REFHOMELIST>
</HOME>
```

   c. Make a note of the sbin directory listed within the <REFHOMELIST> and </REFHOMELIST> tags.

      For example,

```
<HOME NAME="nfs5515" LOC="/home/john/software/oracle/agent/core/12.1.0.0.0"
TYPE="O" IDX="1">
<REFHOMELIST>
<REFHOME LOC="home/john/software/oracle/agent/sbin"/>
</REFHOMELIST>
```

d. Detach the dependent plug-ins you identified in Step 1 (b) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc
ORACLE_HOME=<plug-in_home>  -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.1.0/oui/bin/r
unInstaller -detachHome -silent -waitForCompletion
-invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.1.0/oraInst.l
oc ORACLE_
HOME=/home/john/software/oracle/agent/plugins/oracle.sysma
n.emas.discovery.plugin_12.1.0.1.0  -nogenerateGUID
```

Note: This step detaches only one plug-in at a time. Therefore, if you have multiple plug-ins, repeat this step to detach every other dependent plug-in.

---

e. Detach the sbin home you identified in Step 1 (c) from the Central Inventory. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/oui/bin/runInstaller -detachHome -silent
-waitForCompletion -invPtrLoc <absolute_path>/oraInst.loc
ORACLE_HOME=<sbin_home>  -nogenerateGUID
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.1.0/oui/bin/r
unInstaller -detachHome -silent -waitForCompletion
-invPtrLoc
/home/john/software/oracle/agent/core/12.1.0.1.0/oraInst.l
oc ORACLE_HOME=/home/john/software/oracle/agent/sbin
-nogenerateGUID
```

f. Deinstall the Shared Agent. To do so, run the following command from the *Master Agent* home that is visible on the host where your *Shared Agent* is installed:

```
$<AGENT_HOME>/perl/bin/perl  <AGENT_
HOME>/sysman/install/NFSAgentDeInstall.pl AGENT_INSTANCE_
HOME=<absolute_path_to_agent_instance_home> ORACLE_
HOME=<absolute_path_to_agent_home>
```

For example,

```
/home/john/software/oracle/agent/core/12.1.0.1.0/perl/bin/
perl
/home/john/software/oracle/agent/core/12.1.0.1.0/sysman/in
```

```
stall/NFSAgentDeInstall.pl AGENT_INSTANCE_
HOME=/home/john/software/oracle/agent/agent_inst ORACLE_
HOME=/home/john/software/oracle/agent/core/12.1.0.1.0
```

17.2.4 Deinstalling Oracle Management Agent Installed Using an RPM File

To deinstall a Management Agent that was installed using a `.rpm` file, follow these steps:

1. Deinstall the Management Agent as described in one of the following sections:
   - To deinstall in graphical mode, see Section 17.2.1.
   - To deinstall in silent mode, see Section 17.2.2.
2. Run the following command as a *root* user:

   ```
   rpm -e <rpm_name>
   ```

> **Note:** As a prerequisite, ensure that you have Resource Package Manager (RPM) installed on the host.

17.3 After You Deinstall

After you deinstall the Management Agent, follow these steps:

1. *(Only for Graphical Mode)* Verify whether the Oracle homes and other directories were successfully deinstalled. To do so, follow these steps:
   a. Invoke the installation wizard by running the following command from the Management Agent home:

      ```
      $<AGENT_HOME>/oui/bin/runInstaller
      ```

      > **Note:** On Microsoft Windows, invoke the `setup.exe` file.

   b. In the installation wizard, on the My Oracle Support Details screen, click **Installed Products**.
   c. On the Inventory screen, check whether or not the Oracle homes and other directories you deinstalled appear. If the deinstallation was successful, then those Oracle homes and directories should not appear.
2. The Oracle homes you deinstalled are deregistered from the central inventory. However, some files might still remain in these Oracle homes. If they do, you can manually delete them.

   You must also manually delete the auto-start script titled S98gcstartup. To do so, navigate to the `/etc/rc.d/` directory, and search for the auto-start 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`.

   > **Note:** These auto-start scripts are not available on Microsoft Windows.

3. If you deinstalled on a Microsoft Windows platform, then follow these steps. Ensure that you are logged in as a user with Administrator privileges on that host.

   Remove Entries from Microsoft Windows Registry

   a. Start the registry editor by selecting **Start** and then **Run**. Type `regedit` and click **OK**.

   b. In the Registry Editor window, in the left pane, expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, and then **Oracle**. Under the **Oracle** directory, delete the following:

      (a) KEY_agent12g*n*

      (b) KEY_sbin12g*n*

      Note: Here, *n* refers to a numeral indicating the agent instance. For example, `KEY_sbin12g9` for the first agent installation.

   c. Expand **HKEY_LOCAL_MACHINE**, **SOFTWARE**, **Oracle**, and then **Sysman**. Under the **Sysman** directory, delete the Management Agent service. For example, `Oracleagent12g9Agent`.

   d. Expand **HKEY_LOCAL_MACHINE**, **SYSTEM**, **CurrentControlSet**, and then **Services**. Under the **Services** directory, delete the Management Agent keys.

   e. Expand **HKEY_LOCAL_MACHINE**, **SYSTEM**, **ControlSet002**, and then **Services**. Under the **Services** directory, delete the Management Agent service.

   f. Close the registry editor.

   Clean Up Environment Settings

   1. Open the Environment Variables window.

      On Microsoft Windows NT, select **Start**, **Settings**, **Control Panel**, **System**, and then **Environment**.

      On Microsoft Windows XP or 2000, select select **Start**, **Settings**, **Control Panel**, **System**, **Advanced**, and then **Environment Variables**.

   2. In the System Variables section, click the variable PATH and modify the value.

   3. Delete Management Agent home.

   4. Click **Apply** and then click **OK**.

   5. Close the Control Panel window.

   6. Restart the host.

18

Deinstalling ADP and JVMD

This chapter describes how you can deinstall Application Dependency and Performance (ADP), and JVM Diagnotics (JVMD) in the Enterprise Manager Cloud Control environment.

In particular, this chapter covers the following:

- Deinstallation Procedure for ADP
- Deinstallation Procedure for JVMD

18.1 Deinstallation Procedure for ADP

The section contains the following topics:

- Deinstalling ADP Manager
- Deinstalling ADP Agents

18.1.1 Deinstalling ADP Manager

To remove the ADP Manager application running on the managed server, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **Middleware**.
2. On the Middleware page, from **Middleware Features** menu, select **Application dependency and Performance**.

   The Application dependency and Performance is displayed.
3. From the **Registration** tab, select the ADP manager application, and click **Remove**.

Note: After removing the ADP Manager from the Enterprise Manager Weblogic Domain (`EMGC_DOMAIN`), log into the WebLogic Server Administration Console, and delete the ADP Manager application, and then remove the ADP Manager Server Instance.

For information about Starting and Stopping Servers, log into WebLogic Server Administration Console, and click the **F1** help. Alternately, you can follow the instructions outlined in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*. The guide is available in the Fusion Middleware documentation library available at:

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

---

4. Connect to the host machine where the managed server was present, and navigate to the following location to manually delete the managed server:

   ```
   $DOMAIN_HOME/<ADP_managed_server>

   Where, $DOMAIN_HOME is the location of the Cloud Control domain
   ```

18.1.2 Deinstalling ADP Agents

To remove the agents which are deployed to the ADP Manager, perform the following steps:

1. In Cloud Control, from **Targets** menu, select **Middleware.**
2. On the Middleware page, from **Middleware Features** menu, select **Application dependency and Performance**.

   The Application dependency and Performance is displayed.
3. From the **Configuration** tab, select the desired ADP Manager application on which the agent(s) have been deployed.
4. Expand the ADP Manager menu, select **Resource Configuration**.
5. From the Resource table, select the agent name, and click **Edit Resource**, and then click **Deploy**.
6. From the Deploy Parameters table, select the servers to undeploy the agent. Change the default menu select from **Deploy** to:
   - **Remove**, to erase all the agent files from the application servers.
   - **Disable**, to remove the agent startup arguments from the application servers

   Note: Select the **Server Started by Node Manager** option only when the node manager is used.

18.2 Deinstallation Procedure for JVMD

For information about deinstalling the JVMD Managers and JVMD Agents, log into WebLogic Server Administration Console, and click the **F1** help. Alternately, you can follow the instructions outlined in the *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help*. The guide is available in the Fusion Middleware documentation library available at:

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

Part VI

Appendixes

This part contains the following appendixes:

- Appendix A, "Using RepManager Utility"
- Appendix B, "Installation and Configuration Log Files"
- Appendix C, "Collecting OCM Data in Enterprise Manager and Ops Center Environments"
- Appendix D, "Troubleshooting"

A

Using RepManager Utility

This appendix describes the RepManager utility. In particular, this appendix covers the following:

- Overview
- Supported Actions and Commands

A.1 Overview

RepManager is a utility that enables you to create, upgrade, and drop Oracle Management Repository, selectively purge plug-ins, and load dlf messages to Oracle Management Repository. This utility is available in the Oracle Management Service (OMS) home:

For UNIX operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager
```

For Microsoft Windows operating systems:

```
$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager.bat
```

This utility is invoked by Repository Configuration Assistant while installing a complete Enterprise Manager system, and by Repository Upgrade Configuration Assistant while upgrading to Enterprise Manager Cloud Control. For information about these Configuration Assistants, see Section 2.5.1.

A.2 Supported Actions and Commands

Table A–1 shows the list of actions and their associated commands supported by the RepManager utility.

Table A–1 Actions and Commands Supported by RepManager

Action	Command	Description	Example
create	`$<OMS_ HOME>/sysman/admin /emdrep/bin/RepMan ager <repository_ database_host> <repository_ database_port> <repository_ database_sid> -dbUser sys [-dbPassword <sys password>] -dbRole sysdba -reposName sysman [-reposPassword <password of sysman user>] -action create [-mwHome <middleware home>] -pluginDepList "<pluginid1>=<plug inid1 home>,<pluginid2>= <pluginid2 home>" -dlfSources "<oms home>,<plugin1 home>,<plugin2home >"`	Use this action to create an Oracle Management Repository with the following parameters: ▪ Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be created. ▪ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home to create the Oracle Management Repository. ▪ Specify the comma-separated list of plugin-information according to dependency to be deployed. You can pass a file with this option, the contents being the comma-separated list of plugin-information according to dependency to be deployed. If the pluginDepList is missing or has a value of empty list i.e., "{}", $<OMS_ HOME>/sysman/admin/emdrep/plugininfo/pluginDepList is read, by default, to get plugin dependency list. ▪ Specify the comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being the comma-separated locations for DLF files from platform/plugins. If the dlfSources option is missing or has a value of empty list i.e., "{}", $<OMS_ HOME>/sysman/admin/emdrep/plugininfo/dlfSources is read, by default, to get dlf resource locations. If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.	`$<OMS_ HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action create -mwHome /scratch/weblogic/middleware -pluginDepList <pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
preupgrade	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -action preupgrade [-mwHome <middleware home>]-pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"`	Use this action to perform steps before upgrading an Oracle Management Repository with the following parameters: ■ Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded. ■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home to upgrade the Oracle Management Repository. ■ Specify the comma-separated list of plugin-information according to dependency to be deployed. You can pass a file with this option, the contents being the comma-separated list of plugin-information according to dependency to be deployed. If the pluginDepList is missing or has a value of empty list i.e. "{}", $<OMS_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList is read, by default, to get plugin dependency list. ■ Specify the comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being the comma-separated locations for DLF files from platform/plugins. If the dlfSources option is missing or has a value of empty list i.e., "{}", $<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources is read, by default, to get dlf resource locations. If this option is missing and default dlfSources file is not present, only dlf files for platform will be picked. If this is present, only the DLFs under these sources will be picked up.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action preupgrade -mwHome /scratch/weblogic/middleware -pluginDepList <pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
upgrade	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -action upgrade [-mwHome <middleware home>]-pluginDepList "<pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>" -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"` **Note:** Run preupgrade before performing upgrade action.	Use this action to upgrade an Oracle Management Repository with the following parameters: ▪ Specify the host, port, and SID to connect to Oracle RDBMS where Oracle Management Repository is to be upgraded. ▪ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home to upgrade the Oracle Management Repository. ▪ Specify the comma-separated list of plugin-information according to dependency to be deployed. You can pass a file with this option, the contents being the comma-separated list of plugin-information according to dependency to be deployed. If the pluginDepList is missing or has a value of empty list i.e. "{}", $<OMS_HOME>/sysman/admin/emdrep/plugininfo/pluginDepList is read, by default, to get plugin dependency list. ▪ Specify the comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being the comma-separated locations for DLF files from platform/plugins. If the dlfSources option is missing or has a value of empty list i.e. "{}", $<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources is read, by default, to get dlf resource locations. If this option is missing and default dlfSources file is not present, only dlf files for Platform would be picked. If this is present, only the DLFs under these sources will be picked up.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action upgrade -mwHome /scratch/weblogic/middleware -pluginDepList <pluginid1>=<pluginid1 home>,<pluginid2>=<pluginid2 home>`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
transX	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -reposName sysman -reposPassword <password of sysman user> -action transx [-mwHome <middleware home>] -dlfSources "<oms home>,<plugin1 home>,<plugin2home>"` **Note:** You can also run `-do transX`. 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 create, preupgrade, and upgrade actions.	Use this action to load the translation resources to the Oracle Management Repository with the following parameters: ■ Specify the host, port, and SID to connect to Oracle RDBMS to load translation resources to Oracle Management Repository. ■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home to load translation resources to Oracle Management Repository. ■ Specify the comma-separated locations for DLF files from platform/plugins. You can pass a file with this option, the contents being the comma-separated locations for DLF files from platform/plugins. If the dlfSources option is missing or has a value of empty list i.e. "{}", $<OMS_HOME>/sysman/admin/emdrep/plugininfo/dlfSources is read, by default, to get dlf resource locations. If this option is missing and default dlfSources file is not present, only dlf files for Platform would be picked. If this is present, only the DLFs under these sources will be picked up.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -reposName sysman -action transx -mwHome /scratch/WLS/middleware`
resume	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -resume retry -checkpointLocation <directory where schemamanager stores checkpoints> [-mwHome <middleware home>]`	Use this action to resume the last failed action, for example, create or upgrade. ■ Specify the host, port, and SID to connect to Oracle RDBMS where the action is to be resumed. ■ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home where the action is to be resumed. ■ Specify the location at which to resume the step. The checkpoint location is $<OMS_HOME>/sysman/log/schemamanager.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -resume retry -checkpointLocation /scratch/weblogic/middleware/oms11g/sysman/log/schemamanager -mwHome /scratch/weblogic/middleware`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
drop	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -action drop [-mwHome /scratch/weblogic/middleware]` **Note:** Ensure that there are no active SYSMAN sessions, scheduler jobs, and dbms_jobs running, and no SYSMAN users logged in. To ensure this, stop the OMS using the command `emctl stop oms -all` on all OMSes.	Use this action to drop the SYSMAN schema as follows: ▪ Specify the host, port, and SID to connect to Oracle RDBMS from which the SYSMAN schema is to be dropped. ▪ Specify the database user and password, repository name (SYSMAN) and password for the SYSMAN user, and middleware home.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action drop -mwHome /scratch/weblogic/middleware`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
dropall	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -action dropall [-mwHome <middleware home>] [-mwOraHome <Oracle Home>]`  **Note:** Ensure that there are no active sessions for SYSMAN, SYSMAN_MDS SYSMAN_OPSS, and SYSMAN_APM. To ensure this, stop the OMS using the command `emctl stop oms -all` on all OMSes. **Note:** If BI Pubilsher (BIP) had been installed and configured, then BIP should be stopped using the Admin Server before running this command.	Use this action to remove all Enterprise Manager repository schemas as follows: ▪ Specify the host, port, and SID to connect to Oracle RDBMS from which all schemas are to be dropped. ▪ Specify the database user and password, repository name (SYSMAN) and password for SYSMAN user, and middleware home.	`$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action dropall -mwHome /scratch/weblogic/middleware -mwOraHome /scratch/weblogic/middleware/oms11g`

Table A–1 (Cont.) Actions and Commands Supported by RepManager

Action	Command	Description	Example
pluginpurge	$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_database_host> <repository_database_port> <repository_database_sid> -dbUser sys -dbPassword <sys password> -dbRole sysdba -reposName sysman -reposPassword <password of sysman user> -action pluginpurge -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 to deinstall a plug-in from the repository as follows: ▪ Specify the host, port, and SID to connect to Oracle RDBMS from which the plug-in is to be deinstalled. ▪ To specify the comma-separated list of plugin-information to be purged from Enterprise Manager Repository with EM-EXT model.	$<OMS_HOME>/sysman/admin/emdrep/bin/RepManager dadvmc0217.foo.xyz.com 1521 db3 -dbUser sys -dbRole sysdba -reposName sysman -action pluginpurge -pluginPurgeList "oracle.sysman.myyempwpax.oms.plugin_12.1.0.1.0=/scratch/weblogic/middleware/plugins/oracle.sysman.myyempwpax.oms.plugin_12.1.0.1.0" -mwHome /scratch/weblogic/middleware

Note: RepManager 12.1 and 11.1 support "-action dropall" (drops users SYSMAN, SYSMAN_BIP, SYSMAN_MDS, SYSMAN_APM, BIP, and SYSMAN_OPSS in 12g, drops users SYSMAN and SYSMAN_MDS in 11g) and "-action drop" (drops only SYSMAN). However, RepManager 10.2.0.5 supports only "-action drop" (drops only SYSMAN, the only users associated with the repository in this version).

Note: If you do not specify passwords during RepManager actions, you will be prompted to do so.

B

Installation and Configuration Log Files

This appendix lists the locations of the various log files that are created during the prerequisites check, installation, and configuration phases of Enterprise Manager Cloud Control components.

In particular, this appendix covers the following:

- Enterprise Manager Cloud Control Installation Logs
- Add Host Log Files

B.1 Enterprise Manager Cloud Control Installation Logs

This section describes the following log files that are created while installing Enterprise Manager Cloud Control:

- Installation Logs
- Configuration Logs

B.1.1 Installation Logs

The following are the installation logs, which provide complete information on the installation status:

- `oraInventory/logs/installActions<timestamp>.log`
- `<ORACLE_HOME>/cfgtoollogs/oui/installActions<timestamp>.log`

> **Note:** The `installActions` log file is located in the `oraInventory` directory by default. This log file will be copied on to the above-mentioned Oracle home location after the installation is complete.

B.1.2 Configuration Logs

This section describes the following configuration logs:

- General Configuration Logs
- Repository Configuration Logs
- Secure Logs

B.1.2.1 General Configuration Logs

The Oracle Management Service (OMS) configuration logs are located in the following location of the Oracle home of the OMS.

```
<ORACLE_HOME>/cfgtoollogs/omsca
```

Table B–1 lists the configuration logs for different installation types.

Table B–1 General Configuration Logs

Installation Type	Location
Install a new or Upgrade Enterprise Manager system	▪ `<ORACLE_HOME>/cfgtoollogs/CfmLogger` ▪ `<ORACLE_HOME>/cfgtoollogs/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/oracle.sysman.top.oms.<timestamp>.log` **Note:** `<ORACLE_HOME>` refers to the Oracle home of the OMS.
Install Oracle Management Agent	▪ `<ORACLE_HOME>/cfgtools/cfgfw/CfmLogger` ▪ `<ORACLE_HOME>/cfgtools/cfgfw/oracle.sysman.top.agent.<timestamp>.log` **Note:** `<ORACLE_HOME>` refers to the Oracle home of the Management Agent.

B.1.2.2 Repository Configuration Logs

This section describes the following repository configuration logs:

- SYSMAN Schema Operation Logs
- MDS Schema Operation Logs

B.1.2.2.1 SYSMAN Schema Operation Logs

The SYSMAN schema operation logs are available in the following location of the Oracle home of the OMS. Listed in this directory is an overall log file, `emschema.log`, which logs all the actions performed by all the instances of RepManager run.

```
$<ORACLE_HOME>/sysman/log/schemanager/
```

In this location, for each run of RepManager, a new subdirectory is created based on the time at which the RepManager was run.

For example, if the RepManager was run and an instance was created at 09/29/2007 12:50PM, then the following subdirectory is created.

```
$<ORACLE_HOME>/sysman/log/schemananager/m_092907_1250_PM/
```

An instance of RepManager (or equivalently RepManager) can have multiple schema actions, mainly CREATE, DROP, UPGRADE, TRANSX, and RESUME_RETRY. For each action, a subdirectory is created.

For example, if a CREATE action is performed by a RepManager instance at 09/29/2006 12:51PM, then the following subdirectory is created. Listed under this

subdirectory are RCU-related log files and `emschema.log.CREATE` log file that logs the CREATE action-specific messages.

`$<ORACLE_HOME>/sysman/log/schemananager/m_092907_1250_PM/m_092907_1251PM.CREATE/`

In general, in `$<ORACLE_HOME>/sysman/log/schemananager/m_<time-stamp>/m_<time-stamp>.<schema-action>`, the following files are created:

- RCU per component (i.e. init, common, modify, drop, config, outofbox, preupgrade log
- RCU log
- Schema action-specific RCU logs
- TransX action-specific log (`emrep_config.log`)

If the any of the schema operations (CREATE/UPGRADE/PREUPGRADE/DROP) fail in SQL execution, and if you retry the operation by clicking **Retry**, then a separate subdirectory titled `m_<time-stamp>.RESUME_RETRY` is created.

The following shows the overall directory structure of repository operation logs for different schema actions:

```
$<ORACLE_HOME>/sysman/log/schemamanager
               emschema.log
        m_030210_0349_AM
            m_030210_0325_AM.TRANSX
                emrep_config.log
                emschema.log.TRANSX
        m_030210_0438_AM
            m_030210_0438_AM.DROP (Same structure for Drop and Dropall actions)
                rcu.log
                emschema.log.DROP
                em_repos_drop.log
        m_030210_0450_AM
            m_030210_0450_AM.CREATE
                 custom_comp_create_tbs.log
                 em_repos_common.log
                 em_repos_init.log
                 emrep_config.log.3
                 emrep_config.log.2
                 emrep_config.log.1
                 emrep_config.log
                 emschema.log
                 rcu.log
                 emschema.log.CREATE
                 em_repos_config.log
        m_030210_1006_PM
            m_030210_1006_PM.RESUME_RETRY
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                emschema.log
                rcu.log
                emschema.log.RESUME_RETRY
                em_repos_modify.log
        m_030210_1021_PM
            m_030210_1021_PM.UPGRADE
                em_repos_init.log
```

```
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                emschema.log
                rcu.log
                emschema.log.UPGRADE
                em_repos_modify.log
        m_030210_1100_PM
            m_030210_1100_PM.PREUPGRADE
                em_repos_preupgrade.log
                emschema.log.PREUPGRADE
                rcu.log
                em_repos_init.log
                emrep_config.log.3
                emrep_config.log.2
                emrep_config.log.1
                emrep_config.log
                em_repos_common.log
        m_030210_1125_PM
            m_030210_1125_PM.MY_ORACLE_SUPPORT
                emschema.log.MY_ORACLE_SUPPORTm_030210_1135_PM
            m_030210_1135_PM.PLUGINPURGE
                emschema.log.PLUGINPURGE
em_repos_pluginpurge.log
rcu.log
```

B.1.2.2.2 EMPrereqKit Logs

For EMPrereqKit, the logs are available at the `<oraInventoryLoc>/logs/` location.

The details of execution of the prerequisites per prerequisite components location is available at:

`<oraInventoryLoc>/logs/emdbprereqs/LATEST/repository.log or emprereqkit.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.log`

B.1.2.2.3 MDS Schema Operation Logs

MDS Schema Creation Log

For MDS schema creation operation, the following log is available in the Oracle home of the OMS:

`$<ORACLE_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log`

For more information, review the following logs from the Oracle home of the OMS:

`$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/mds.log`

`$<ORACLE_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/rcu.log`

MDS Schema Drop Logs

For MDS schema drop operation, the following logs are available in the location you specified by using the `-logDir` argument while invoking the MDS schema drop command:

```
$<user_specified_location>/mds.log
```

```
$<user_specified_location>/emmdsdrop_<timestamp>.log
```

However, if you did not specify any custom location while invoking the MDS schema drop command, then the logs are created in the Oracle home of the OMS. For example, `/scratch/OracleHomes/oms12c/mds.log` and `/scratch/OracleHomes/oms12c/emmdsdrop_<timestamp>.log`.

B.1.2.3 Secure Logs

For OMS, the following secure log is available in the OMS Instance Base location. Here, *<oms_name>*, for example, can be *EMGC_OMS1*.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/secure.log
```

For Management Agents, the following secure log is available in the Oracle home of the Management Agent.

```
<Agent_Instance_Home/sysman/log/secure.log
```

B.1.2.4 Oracle Management Service Logs

The following log files that provide information about the running OMS are available in the OMS Instance Base location. Here, *<oms_name>*, for example, can be *EMGC_OMS1*.

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.trc
```

```
<OMS_INSTANCE_HOME>/em/<oms_name>/sysman/log/emoms.log
```

B.2 Add Host Log Files

This section describes the locations for the following Add Host log files:

- Initialization Logs
- Application Prerequisite Logs
- System Prerequisite Logs
- Agent Installation Logs
- Other Add Host Logs

B.2.1 Initialization Logs

Table B–2 lists the initialization logs of the remote host and their locations. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS

Table B–2 Initialization Logs

Log File	Location
`<hostname>_deploy.log`	`<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/applogs`

B.2.2 Application Prerequisite Logs

Table B–3 lists the application prerequisite logs and their locations. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS, and the <install_type> mentioned in this table refer to one of the installation types mentioned in Table B–4.

Table B–3 Prerequisite Logs

Log File	Location
prereq<time_stamp>.log	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/
prereq<time_stamp>.out	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/
prereq<time_stamp>.err	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/<install_type>_logs/<hostname>/

Table B–4 Install Types

Install Type	Description	Target Operating System Type
emagent_install	New Agent Installation	UNIX
emagent_clone	Agent Cloning	UNIX
nfs_install	Shared Agent Installation	UNIX

B.2.3 System Prerequisite Logs

Table B–5 lists the system prerequisite logs and their locations. Note that<ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–5 System Prerequisite Logs

Log File	Location
prereq<time_stamp>.log	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
prereq<time_stamp>.out	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/
prereq<time_stamp>.err	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/prereqlogs/productprereq_logs/<hostname>/

B.2.4 Agent Installation Logs

Table B–6 lists the agent installation logs and their locations. Note that<ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–6 Agent Installation Logs

Log File	Location	Description
install.log/.err	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/logs/<hostname>	Fresh and Cloned Agent install logs
nfs_install.log/.err	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/logs/<hostname>	Shared Agent installation logs
cfgfw/*.log	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/cfgtoollogs/<hostname>	Agent Configuration logs

B.2.5 Other Add Host Logs

Table B–7 lists all the other installation logs that are created during an agent installation using the Add Host wizard. Note that <ORACLE_HOME> mentioned in this table refer to the Oracle home of the OMS.

Table B–7 Other Add Host Logs

Logs	Location	Description
EMAgentPushLogger<TIMESTAMP>.log	<ORACLE_HOME>/sysman/prov/agentpush/logs/	Agent Deploy application logs.
remoteInterfaces<TIMESTAMP>.log	<ORACLE_HOME>/sysman/prov/agentpush/logs/	Logs of the remote interfaces layer.
deployfwk.log	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/applogs/	Add Host Deployment Framework logs
ui.log	<ORACLE_HOME>/sysman/prov/agentpush/<time-stamp>/applogs/	Add Host User Interface logs.

C

Collecting OCM Data in Enterprise Manager and Ops Center Environments

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 Configuration Manager (OCM)
- Oracle Enterprise Manager Harvester (Oracle Harvester)
- Oracle Enterprise Manager Ops Center Harvester (Ops Center Harvester)

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 or Ops Center to manage targets in your enterprise, we recommend that you use Oracle Harvester or Ops Center Harvester respectively to upload the configurations managed by them to Oracle. Otherwise, use OCM.

C.1 Oracle Configuration Manager

OCM is installed as part of the Oracle product installation. 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.

C.2 The Harvesters

Note: The harvesters only harvest data for targets that are managed by Enterprise Manager and Ops Center.

Uploading the configuration data through a harvester removes the requirement of having OCM installed in each product home.

The available harvesters are: Oracle Harvester which collects configuration data in the Enterprise Manager environment and Ops Center Harvester which collects configuration data in the Ops Center environment.

The Ops Center Harvester and Oracle Harvester have the same OCM dependencies. Each harvester enables the gathering of target configuration data by leveraging Enterprise Manager and Ops Center collection methods thus precluding the need to install OCM on target homes managed by each harvester.

Details shared by the harvesters:

- Data is uploaded by default against the same credentials with which OCM in the Oracle Management Service (OMS) home or the Controller home for Ops Center is configured.
- Require OCM to be configured and running in the OMS home for Enterprise Manager or the Controller home for Ops Center.
- Gathers target configuration data from either the Ops Center database or Management Repository
- Automatically run periodically so no user intervention is required

C.2.1 Oracle Harvester

When you install Enterprise Manager, Oracle Harvester and Oracle Configuration Manager 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.

For Enterprise Manager releases 11.1 and later, 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. For example:

1. Locate the OMS instance home.

   In the $ORACLE_HOME/sysman/config/emInstanceMapping.properties file (where ORACLE_HOME is the Oracle Home of the OMS), there is an entry referencing a file called emgc.properties.

   The directory in which the emgc.properties file is located is the "instance home" of the OMS. In the following example, /u01/app/oracle/product/gc_inst/em/EMGC_OMS1 is the instance home of the OMS:

   EMGC_OMS1=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1/emgc.properties

2. Set the environment variable ORACLE_CONFIG_HOME to the directory of this emgc.properties file.

   Example:

   $export ORACLE_CONFIG_HOME=/u01/app/oracle/product/gc_inst/em/EMGC_OMS1

3. Configure OCM.

For Enterprise Manager release 10.2.0.5, OCM must be installed and configured in the Oracle Home.

In Enterprise Manager releases 11.1 and earlier, Oracle Harvester can only upload configuration data against the same credentials with which OCM in the OMS home is configured.

New For Enterprise Manager Release 12.1

By default, all targets are uploaded using the credentials used to register Oracle Configuration Manager in the OMS Home. In Enterprise Manager release 12.1, you have the option of assigning a Customer Support Identifier (CSI) to each target home.

The Oracle Harvester supports uploading configuration data to different CSIs for each different Oracle Home.

The steps include:

1. Ensuring that the Oracle Harvester has run. This job runs automatically.
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 the preferred 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.

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. 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.

C.2.1.1 Supported Targets in Oracle Harvester

Oracle Harvester collects configuration data from Enterprise Manager releases 10.2.0.5, 11.1, and 12.1. Depending on the version 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 represented in the following table is collected by Oracle Harvester.

Table C–1 Supported Targets in Enterprise Manager (EM)

Target	EM 10.2.0.5	EM 11.1	EM 12.1
Host	Yes	Yes	Yes
Oracle Application Server	Yes	Yes	Yes
Oracle Database	Yes	Yes	Yes
Oracle Home	Yes	Yes	Yes
Oracle Exadata Storage Server	No	Yes	Yes
Oracle Virtual Manager	No	Yes	Yes
Oracle WebLogic Server	No	Yes	Yes
Management Agent	No	No	Yes
Management Repository	No	No	Yes
Oracle Database Machine	No	No	Yes
Oracle Fusion Applications	No	No	Yes
Oracle Fusion Middleware	No	No	Yes
Oracle Management Service	No	No	Yes
Oracle SOA Suite	No	No	Yes

C.2.1.2 Configuration Data Not Available in My Oracle Support

Configuration data for targets collected from Oracle Harvester running in Enterprise Manager releases 10.2.0.5 and 11.1 will show up in My Oracle Support only if one of the following conditions is met:

- OCM collector is not installed in the product home where the target is present and is not uploading the configuration for the target that is collected from Oracle Harvester in Enterprise Manager releases 10.2.0.5 or 11.1.
- Thirty days have passed since the OCM collector last uploaded the configuration data for the target.

Configuration data for targets collected from Oracle Harvester running in Enterprise Manager release 12.1 display in My Oracle Support immediately.

In Enterprise Manager release 11.1, if you do not want to wait for 30 days for Oracle Harvester collected configuration data to display in My Oracle Support, you can execute the following SQL script against the Management Repository:

```
sql> insert into mgmt_ocm_upl_props (name,str_value) values('is_gc_force','true');
sql> commit;
```

Bounce the OMS after executing the SQL script.

C.2.2 Ops Center Harvester

The Ops Center Harvester leverages the scale of Ops Center manageability by providing OCM collection capabilities for all systems managed by the Ops Center starting with release 11.1.

Ops Center Harvester collects configuration data from the Management Repository creating a host target for each managed asset and an Ops Center target containing summary information about the Ops Center instance.

OCM and the Ops Center Harvester are bundled with Ops Center, and are installed in a fixed location on the Ops Center Enterprise Controller. Ops Center Harvester requires OCM to be installed in: /var/opt/sun/xvm/ocm/ which is governed by the Ops Center Installer.

The Ops Center Harvester utilizes the credentials entered during the OCM setup for uploading configuration data. You must explicitly configure OCM during the overall Ops Center install process, that is, you must complete the OCM configuration. Otherwise the Ops Center Harvester will not run.

Host targets collected by the Ops Center Harvester should appear in My Oracle Support with a Source of "Oracle Enterprise Manager Ops Center Harvester".

Additional information on Ops Center Harvester is available at:

http://wd0338.oracle.com/archive/cd_ns/E11857_01/nav/management.htm

C.3 Additional Information

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. Access the **Collector** tab. The **What**, **Why**, **How**, **Using It**, and **Additional Resources** sections all contain useful information.

C.4 Troubleshooting Configuration Data Collection Tools

The following sections describe how to resolve issues with the configuration data collections.

In Enterprise Manager releases 10.2.0.5 and 11.1, 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 Enterprise Manager release 10.2.0.5 look at:

    `ORACLE_HOME/sysman/log/emoms.trc`

  - For Enterprise Manager release 11.1, look at:

    ```
    INSTANCE_HOME/sysman/log/emoms.trc
    ```

  - For Enterprise Manager release 12.1, 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
  ```

C.4.1 Oracle Harvester Collection Fails If the state/upload/external Directory Is Missing

If the Oracle Harvester collection fails with the following error, the required directory named *external* is missing.

```
[JobWorker 75210:Thread-61] ERROR gcharvester.GcCollectionMgr initOcm.? - GC OCM
Harvester: Caught GC Harvester exception from GCInit.init(): The installed version
of Oracle Configuration Manager in the ORACLE_HOME
(/scratch/aime/work/midlwre8937/oms11g) is prior to 10.3.1. The Grid Control
Configuration harvesting requires at a minimum, 10.3.1
```

The *external* directory is missing in one of the following:

- $ORACLE_HOME/ccr/hosts/<local_host_name>/state/upload directory (Enterprise Manager release 10.2.0.5)
- $ORACLE_INSTANCE_HOME/ccr/state/upload directory (Enterprise Manager releases 11.1 and later).

To resolve this issue:

- In Enterprise Manager release 10.2.0.5, create the directory $ORACLE_HOME/ccr/hosts/<local_host_name>/state/upload/external.
- In Enterprise Manager releases 11.1 and later, create the directory $ORACLE_INSTANCE_HOME/ccr/state/upload/external.

(Bug 12795503)

C.4.2 Oracle Configuration Manager Is Not Running

When OCM is not running, you may see the following error:

```
2011-08-29 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 is correctly installed and configured in the appropriate directories. In particular:

- For Enterprise Manager release 10.2.0.5, OCM must be installed and configured (and running in connected mode) in the Oracle Home of the targets it is managing.
- For Enterprise Manager releases 11.1 and later, OCM must be installed in the OMS Oracle Home and configured (and running in connected mode) in the OMS Instance Home.

C.4.3 Configuration Data Not Available in My Oracle Support

When you look at My Oracle Support and do not find configuration data, it could be that the Oracle Harvester collection did not run.

To resolve this issue, verify that the OCM was installed and configured in the appropriate directories (execute `emCCR status`). In particular:

- For Enterprise Manager release 10.2.0.5, OCM must be installed and configured (in connected mode) in the Oracle Home of the OMS. To verify that OCM is running, execute the following command:

  ```
  $ORACLE_HOME/ccr/bin/emCCR status
  ```

- For Enterprise Manager releases 11.1 and later, 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`

C.4.4 Only a Subset of the Targets Is Collected by the Oracle Harvester

If many targets are uploaded to the Management Repository but only a subset of the targets is collected by the Oracle Harvester, it could be because the same error was encountered 10 times during a collection, causing the Oracle Harvester to stop collecting. Look at the appropriate log file to verify that this error has occurred.

Resolve the issue by running the following SQL script against the Management Repository. This script forces the Oracle Harvester to ignore this collection error and continue collecting the remaining target information.

```
sql> insert into mgmt_ocm_upl_props (name,str_value) values('ignore_
errors','true');
sql> commit;
```

Bounce the OMS after executing the SQL script.

(Bug 11734389)

D

Troubleshooting

This appendix describes how to troubleshoot issues that you might encounter while working with Enterprise Manager Cloud Control.

- Troubleshooting Configuration Assistant Failures
- Troubleshooting ADP and JVMD Failures

Note: Add a note in the beginning of the appendix to state that users need to run runConfig.bat instead of `runConfig.sh` on Microsoft Windows platforms

---

D.1 Troubleshooting Configuration Assistant Failures

This section describes the log files you must review and the actions you must take when the following configuration assistants fail:

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

D.1.1 Plugins Prerequisites Check Configuration Assistant

Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`

- $<OMS_HOME>/cfgtoollogs/pluginca/configplugin_prereq_check_<timestamp>.log

Workaround Steps

Run the following command:

```
$<OMS_HOME>/oms/bin/pluginca -action prereqCheck -oracleHome
<oms_home_path> -middlewareHome <middleware_home_path> -plugins
<plugin_id>=<plugin_version>
```

> **Note:** For multiple plug-ins, separate the plug-in details with a comma. For example, `-plugins <plugin_id>=<plugin_version>, <plugin_id>=<plugin_version>`

D.1.2 Repository Configuration Assistant

Log Files

Review the following log files:

- $<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
- $<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.<ACTION>/

> **Note:** <ACTION> refers to any of the schema actions, for example, CREATE, TRANSX, MY_ORACLE_SUPPORT, and so on.

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Clean up the Management Repository by running the following command:

   ```
   $<OMS_HOME>/sysman/admin/emdrep/bin/RepManager <repository_
   database_host> <repository_database_port> <repository_
   database_sid> -action dropall -dbUser <repository_database_
   user> -dbPassword <repository_database_password> -dbRole
   <repository_database_user_role> -mwHome <middleware_home>
   -mwOraHome <oms_oracle_home> -oracleHome <oms_oracle_home>
   ```

   > **Note:**
   >
   > - For Microsoft Windows, invoke `RepManager.bat`.
   > - RepManager 12.1 and 11.1 support `-action dropall` (drops SYSMAN as well as SYSMAN_MDS) and `-action drop` (drops only SYSMAN).
   > - RepManager 10.2.0.5 supports `-action drop` (drops only SYSMAN)

3. Rerun the configuration assistant.

If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

Note: For Microsoft Windows, run `runConfig.bat`.

D.1.3 MDS Schema Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

For more information, review the following log files:

- `<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/mds.log`
- `$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_<timestamp>.CREATE/rcu.log`

Workaround Steps

Follow these steps:

1. Drop the MDS schema by running the following command from the OMS home:

   ```
   $<OMS_HOME>/sysman/admin/emdrep/bin/mdsschemamanager.pl
   -action=-dropRepository -connectString=<database_connect_
   string> -dbUser= <database_user> -dbPassword=<database_
   password> -oracleHome=<OMS_oracle_home> -mwHome=<middleware_
   home>
   ```

   Where `<database_connect_string>` must be in the following format:`<database_host>:<database_port>:<database_sid>`

2. Rerun the Configuration Assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

Note: For Microsoft Windows, run `runConfig.bat`.

D.1.4 OMS Configuration Assistant

Log Files

Review the following log files:

- If the installer fails BEFORE the OMS configuration assistant starts running, then review the following log file:

  ```
  $<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
  ```

- If the installer fails AFTER the OMS configuration assistant starts running, then review the following log file:

  ```
  $<OMS_HOME>/cfgtoollogs/omsca/omsca_<timestamp>.log
  ```

Workaround Steps

Follow these steps:

1. Check whether any Java processes are running from the middleware home. To do so, run the following command from the host where the OMS is running:

   ```
   ps -ef | grep java | grep <Oracle_Middleware_Home>
   ```

2. Kill all the running processes, except for installer-related Java processes, by the running the following command. The installer-related Java processes run from the temp directory, so you can ignore the processes from that directory.

   ```
   kill -9 <process_id>
   ```

3. Remove the Oracle Management Service Instance Base by running the following command:

   ```
   rm -rf <OMS_Instance_Home>
   ```

4. Rerun the Configuration Assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

Note: For Microsoft Windows, run `runConfig.bat`.

D.1.5 Plugins Deployment and Configuration Configuration Assistant

Log Files

Review the following log files:

- `$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- `$<OMS_HOME>/cfgtoollogs/pluginca/configplugin_deploy_<timestamp>.log`

Workaround Steps

Run the following command:

```
$<OMS_HOME>/oms/bin/pluginca -action deploy -oracleHome <oms_home_path> -middlewareHome <middleware_home_path>   -plugins <plugin_id>=<plugin_version>
```

Note: For multiple plug-ins, separate the plug-in details with a comma. For example, `-plugins <plugin_id>=<plugin_version>, <plugin_id>=<plugin_version>`

D.1.6 Start Oracle Management Service Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Run the following command:

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

D.1.7 Plugins Inventory Migration Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

Note: For Microsoft Windows, run `runConfig.bat`.

D.1.8 Oracle Configuration Manager Repeater Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

   Note: For Microsoft Windows, run `runConfig.bat`.

D.1.9 OCM Configuration for OMS Configuration Assistant

Log Files

Review the following log file:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

   If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

   ```
   $<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
   MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
   0_0.xml}
   ```

   Note: For Microsoft Windows, run `runConfig.bat`.

D.1.10 Agent Configuration Assistant

Log Files

Review the following log files:

- `$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log`
- If secure fails, then review the following log file:

  `$<AGENT_HOME>/sysman/log/secure.log`
- In the log file, search for the following statement:

  `SEVERE:Plugin configuration has failed.`

  If you find this statement, then review the following log file:

  ```
  $<AGENT_INSTANCE_HOME>/install/logs/agentplugindeploy_
  <timestamp>.log
  ```

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

   If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

Note: For Microsoft Windows, run `runConfig.bat`.

If you are installing in silent mode, then run the following command from the Management Agent home:

```
$<AGENT_HOME>/sysman/install/agentDeploy.sh OMS_HOST=<oms_
host_name> EM_UPLOAD_PORT=<oms_upload_https_port> AGENT_
REGISTRATION_PASSWORD=<agent_reg_password>
```

Note: Enter the HTTPS port (secure port) for the EM_UPLOAD_PORT argument.

D.1.11 Agent Upgrade Configuration Assistant

Log Files

If the agent upgrade configuration assistant fails, then review the following log file:

```
$<AGENT_HOME>/cfgtoollogs/cfgfw/CfmLogger_<timestamp>.log
```

Workaround Steps

Resolve the cause of the issue, and rerun the configuration assistant from the Jobs page of the Enterprise Manager Cloud Control console.

Note: The Jobs page referred to here is the page within the earlier release of the Enterprise Manager Cloud Control console.

D.1.12 Repository Upgrade Configuration Assistant

Log Files

Review the following log files:

```
$<OMS_HOME>/cfgtoollogs/cfgfw/emmdscreate_<timestamp>.log
```

```
$<OMS_HOME>/sysman/log/schemamanager/m_<timestamp>/m_
<timestamp>.<ACTION>/
```

Note: (`<ACTION>` refers to any of the schema actions, for example, PREUPGRADE, UPGRADE, TRANSX, and so on.)

Workaround Steps

Follow these steps:

1. Resolve the cause of the issue.
2. Rerun the configuration assistant.

   If you are installing in graphical mode, then return to the Enterprise Manager Cloud Control Installation Wizard and click **Retry**.

If you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

If you are installing in silent mode, then rerun the `runConfig.sh` script from the OMS home:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<oms_home_path>
MODE=perform ACTION=configure COMPONENT_XML={encap_oms.1_0_0_
0_0.xml}
```

Note: For Microsoft Windows, run `runConfig.bat`.

D.2 Troubleshooting ADP and JVMD Failures

This section discribes how to troubleshoot the errors encountered while deploying ADP/JVMD Managers, and ADP/JVMD Agents:

- ADP Manager Name Conflict
- Failure to Deploy ADP Agent On a Target
- Manual Steps for WebLogic 10.0.X if the JVM Vendor is SUN
- SSL Handshake Failure Agent Deployment Errors
- Copying ADP Agent Zip or Javadiagnosticagent Ear Step Failure

D.2.1 ADP Manager Name Conflict

Error Message

When you deploy ADP Manager to an existing managed server whose instance (for example: `EMGC_ADPMANAGER2`) has not been completely removed, then the new deployment of ADP manager with the same name fails on the unzip step with the following error:

```
@ Are you sure you haven't deployed adp manager to a managed server with name
@ <ADP_managed_server> already?
```

Workaround Steps

To remove the existing managed server completely, perform the following steps:

1. Follow the steps listed in Chapter 18 to remove the ADP Manager application and the managed server to which the ADP application is deployed.
2. Connect to the host machine where the managed server was present, and navigate to the following location to manually delete the managed server (`EMGC_ADPMANAGER2`):

   ```
   $DOMAIN_HOME/<ADP_managed_server>

   Where, $DOMAIN_HOME is the location of the Cloud Control domain
   ```

D.2.2 Failure to Deploy ADP Agent On a Target

Error Message

While deploying the ADP Agent, the deployment job may fail on the Deploy ADP Agent On Target step, with the following error:

```
Failed to connect to
https://<host>:<port>/HttpDeployer/HttpDeployerServlet
```

Also, if you check the output of the Deploy HttpDeployer OnTarget (the previous step), then you will see a message as follows:

```
Operation is pending and will be activated or cancelled when the
ongoing edit session is activated or cancelled.
```

Workaround Steps

To correct this error, perform the following steps:

1. Log into WebLogic Administration Console of the domain where the ADP Agent was to be deployed.
2. On the Administration home page, click **Save Changes** or **Discard Changes**, and start deploying the ADP agent afresh.

D.2.3 Manual Steps for WebLogic 10.0.X if the JVM Vendor is SUN

If you are using WebLogic Server 10.0.X, then you must perform some additional manual steps before using the Diagnostics Agent deployment page for deploying ADP Agents:

Workaround Steps

If the JVM vendor of Management Agent is SUN, then you must perform the following steps, and then proceed with the agent deployment:

1. Navigate to `<emd_plugin_root_of_em_agent>/scripts/diagagent/deploy_camm.pl`.

   Where, `emd_plugin_root_of_em_agent` corresponds to `<emd_root_of_em_agent>/plugins/oracle.sysman.emas.agent.plugin_12.1.0.0.0`.

   `emd_root_of_em_agent` corresponds to the Management Agent that was used to discover the WebLogic domain where the ADP agent is to be deployed.

2. Do the following:

   - If the operating system of the host where the Management Agent is present is Linux, then on line 139, add a comma seperated value (illustrated in bold) as follows:

     ```
     -cp",$classpathWLS,"-Dweblogic.security.SSL.ignoreHostnameVerify=true",
     "-Dsun.lang.ClassLoader.allowArraySyntax=true",
     "-Djava.security.egd=file:/dev/./urandom",
     ```

   - If the operating system of the host where the Management Agent is present is Windows, then on line 176, add a comma seperated value (illustrated in bold) as follows

     ```
     -cp",$classpathWLS,"-Dweblogic.security.SSL.ignoreHostnameVerify=true",
     "-Dsun.lang.ClassLoader.allowArraySyntax=true",
     "-Djava.security.egd=file:/dev/./urandom",
     ```

Important: If WebLogic domain on `host-a` (WebLogic Domain where the ADP Agent is deployed) is discovered using Management Agent on `host-b` (Enterprise Manager Domain (`EMGC_DOMAIN`) where the Management Agent is deployed to monitor the WebLogic Domain on `host-a`), then do the following:

1. Navigate to the following location:

   `<WEBLOGIC_HOME>/server/lib`

2. Do the following to generate `wlfullclient.jar`:

   If the WebLogic Server version is 10.3.x or higher, then run the following command:

   ```
   java -jar wljarbuilder.jar
   ```

   If the WebLogic Server version is less than 10.3.x, then use other WebLogic installations (10.3.x or higher) to create the `wlfullclient.jar`.

   For example, you can use the `<WEBLOGIC_DOMAIN>` corresponding to the EMGC domain for generating the `wlfullclient.jar`, since Enterprise Manager setup uses JDK6.

3. Copy the following files from `<WEBLOGIC_HOME>/server/lib/` to `<AGENT_HOME>/sysman/jlib` directory:

   - `wlfullclient.jar`
   - `cryptoj.jar`
   - `webserviceclient + ssl.jar`
   - `wlcipher.jar`

D.2.4 SSL Handshake Failure Agent Deployment Errors

Error Message

If the WebLogic Domain is SSL enabled using a demo certificate, then the agent deployment may fail due to an SSL Handshake Failure. The following error normally occurs because the demo certificate is not present in `AgentTrust.jks`:

```
Certificate chain received from myhost.acme.com - 123.34.11.11
was not trusted causing SSL handshake failure. Check the
certificate chain to determine if it should be trusted or not.
If it should be trusted, then update the client trusted CA
configuration to trust the CA certificate that signed the peer
certificate chain. If you are connecting to a WLS server that is
using demo certificates (the default WLS server behavior), and
you want this client to trust demo certificates, then specify
-Dweblogic.security.TrustKeyStore=DemoTrust on the command line
for this client.
```

Note: If the WebLogic Domain is using a production certificate, then this issue will not occur as `AgentTrust.jks` has trusted certificates from all well known CA's.

Workaround Steps

To correct the error, import WebLogic demo certificate to Management Agent keystore as follows:

1. Export WebLogic Demo certificate from `cacerts` file. This file is present under the WebLogic home of the Middleware installation at the following location:

```
keytool -export -keystore $WEBLOGIC_HOME/server/lib/cacerts
-alias certgencab -file mycert.cer
```

Press **Enter** when prompted for a password.

2. Import WebLogic Demo certificate to TrustStore of Oracle Management Agent as follows:

```
keytool -import -keystore $ORACLE_
HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.
jks -alias wlscertgencab -file mycert.cer
```

Enter the password **welcome** when prompted, and press **Enter.**

To check if the certificate has been imported correctly, run the following command:

```
keytool -list -keystore $ORACLE_
HOME/core/12.1.0.0.0/stage/sysman/config/montrust/AgentTrust.jks
```

Where, `$ORACLE_HOME` is Oracle Management Agent home.

Press **Enter** when prompted for password, a certificate with the name `wlscertgencab` is generated with the current date.

D.2.5 Copying ADP Agent Zip or Javadiagnosticagent Ear Step Failure

Error Message

If the users who installed the OMS, and the Management Agent are not in the same group, then the job fail on Copying ADP Agent Zip step for an ADP agent, and Copy Javadiagnosticagent Ear step for a JVMD agent, with the following error:

```
oracle.sysman.emSDK.emd.comm.RemoteOperationException: Error while streaming
JobReader:java.io.IOException: Broken pipe
```

Workaround Steps

To correct the error, either install the Enterprise Manager Agent using OMS host user credentials.

OR

Enable `sudo` or `Powerbroker` settings for the agent host, so that the job runs as if run by an OMS host user.

To set the `sudo`, or `Powerbroker` settings, do the following:

1. In Cloud Control, from the **Setup** menu, select **Security,** and then click **Privilege Deligation.**
2. On the Manage Privilege Delegation Settings page, do the following:
   a. Select the **Sudo** or **PowerBroker** from the type menu.
   b. Enter the host name, or alternatively select the name from the list of host targets. Ensure that the host selected corresponds to the EM Agent; this agent must be the one monitoring the WebLogic Domain where the ADP/JVMD agents have to be deployed.
   c. Click **Go**.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

W