# Oracle® Enterprise Manager

Grid Control Installation and Configuration Guide

10*g* Release 5 (10.2.0.5.0)

**E10953-15**

January 2011

Oracle Enterprise Manager Grid Control Installation and Configuration Guide, 10*g* Release 5 (10.2.0.5.0)

E10953-15

Primary Author: Aravind Jayaraaman

Contributing Author: Dennis Lee, Leo Cloutier, Jacqueline Gosselin, Pushpa Raghavachar, Aparna Kamath

# Contents

## Part I Overview and Preinstallation

### 1 Getting Started with Enterprise Manager Grid Control

### 2 Overview of Enterprise Manager Grid Control

## 3 Preinstallation Requirements

## 4 Things to Know Before Installation

# Part II Installing Enterprise Manager Grid Control

## 5 Overview of the Installation Process

## 6 Accessing the Installation Software

## 7 Using Oracle Universal Installer

## 8 Installing Enterprise Manager Grid Control

## 9 Installing Enterprise Manager Grid Control in Silent Mode

## 10 Deploying Management Agent

## 11 Deploying Management Agent in Silent Mode

## 12 Deploying Management Agent on a Cluster

## 13 Cloning Management Agent

## 14 Prerequisites for Installing Enterprise Manager Grid Control on Oracle RAC

# Part III Postinstallation Configuration

## 15 Postinstallation Configuration Tasks

## Part IV Advanced Enterprise Manager Configuration

## 16 Advanced Configuration Overview

## 17 Grid Control Common Configurations

## 18 Configuring Enterprise Manager for Active and Passive Environments

## 19 Configuring Enterprise Manager for Firewalls

## 20 Reconfiguring the Management Agent and Management Service

## 21 Additional Configuration Tasks

## Part V Upgrading Enterprise Manager Grid Control

## 22 Upgrading Enterprise Manager Grid Control

# Part VI Deinstalling Enterprise Manager Grid Control and Management Agent

## 23 Deinstalling Enterprise Manager Grid Control

## 24 Deinstalling Management Agent

# Part VII Appendixes

## A Troubleshooting Enterprise Manager

## B Installation and Configuration Log Files

## C Agent Log Files

## D Platform-Specific Package and Kernel Requirements

## E Firewall Port Requirements

## F Using the Staticports.ini File

## G Agent Deploy Application - Installation Prerequisites

## H Additional Parameters for Agent Deploy Application

## I Oracle Reserved Words

## Index

# Preface

This guide is your primary source of preinstallation requirements and certifications, and describes the installation options, and postinstallation configuration information for Enterprise Manager Grid Control (Grid Control).

This preface contains the following topics:

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

## Intended Audience

This guide is written for Oracle Database system administrators who want to install and configure Grid Control. You should already be familiar with Oracle Database and the administrative tasks you want to perform.

## Purpose of the Document

This guide should be used for installing only the full releases of Enterprise Manager 10g Grid Control Release 2 or higher. A *full release* refers to the first, complete Enterprise Manager 10g Grid Control Release 2 or higher software that was released for a particular platform.

A full release comprises all three components that form Grid Control, mainly Oracle Management Service, Oracle Management Repository, and Oracle Management Agent. You can use the full release to install either all three components or only an additional Oracle Management Service or Oracle Management Agent.

You can also use this guide to upgrade an existing Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enterprise Manager 10 Grid Control Release 2 or higher. For example, you can use this guide to upgrade an existing Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) to Enterprise Manager 10g Grid Control Release 2 (10.2.0.1).

The following shows the full releases of Enterprise Manager 10g Grid Control Release 2 or higher that were released for various platforms. Use this guide for installing only these releases.

| Full Release | Targeted Platforms |
|---|---|
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.1.1) (RECUT) | Linux x86 |
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) | ■ Solaris (SPARC)<br>■ HP-UX (PARISC)<br>■ AIX5L Based Systems |
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.2.1) (RECUT) | Microsoft Windows (32-Bit) |

| Full Release | Targeted Platforms |
|---|---|
| Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) | ■ Linux X86_64<br>■ HP-UX ( Itanium ) |

In addition, there have been Patch Sets released periodically to patch these full releases and move them to higher releases. For example, Enterprise Manager 10g Release 2 (10.2.0.2) Patch Set was released for Linux x86 platform. The patch set helps you patch Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux x86 and move it to Release 2 (10.2.0.2).

This guide does not describe the patching procedures. The patching procedures are furnished in the Patch Set Notes document, which is packaged with the Patch Set, not in this guide. You can download the Patch Sets and the relevant Patch Set Notes from My Oracle Support (formerly Metalink).

**Note:**

Patch Sets help you to only *patch* any previous releases of Grid Control and (or) Management Agent; they DO NOT *upgrade* your existing releases to newer full releases, say Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) to Enterprise Manager 10g Grid Control Release 2 (10.2.0.1).

**If you do not have a previous release, but want to have the most recent release of Grid Control, then first install a full release and then use the Patch Sets to patch it to a higher release.**

## Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at `http://www.oracle.com/accessibility/`.

### Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

### Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

### Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

## Related Documents

For more information, see the following books in the Oracle Enterprise Manager documentation set:

- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Quick Installation Guide*
- *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*
- *Oracle Enterprise Manager Policy Reference Manual*
- *Oracle Enterprise Manager Metric Reference Manual*
- *Extending Oracle Enterprise Manager*
- *Oracle Enterprise Manager Command Line Interface*
- *Oracle Enterprise Manager SNMP Support Reference Guide*

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

`http://otn.oracle.com/documentation/oem.html`

Oracle Enterprise Manager also provides extensive online Help. Click **Help** at the top of any Enterprise Manager page to display the online help window. This installation guide has been designed to work in close association with the online help provided with the installation.

## Conventions

The following table describes those conventions and provides examples of their use.

| Convention | Meaning | Example |
|---|---|---|
| **Bold** | Bold typeface indicates an element in the user interface. | Click **Help** for more information. |
| *Italics* | Italic typeface indicates book titles or emphasis. | *Oracle Database Concepts*<br>Ensure that the recovery catalog and target database do *not* reside on the same disk. |

| Convention | Meaning | Example |
|---|---|---|
| lowercase monospace (fixed-width font) | Lowercase monospace typeface indicates executables, file names, directory names, and sample user-supplied elements. Such elements include computer and database names, net service names, and connect identifiers, as well as user-supplied database objects and structures, column names, packages and classes, user names and roles, program units, and parameter values.<br>**Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown. | Enter `sqlplus` to open SQL*Plus.<br>The password is specified in the `orapwd` file.<br>Back up the datafiles and control files in the `/<DVD>/oracle/dbs` directory.<br>The `department_id`, `department_name`, and `location_id` columns are in the `hr.departments` table.<br>Set the `QUERY_REWRITE_ENABLED` initialization parameter to `true`.<br>Connect as `oe` user.<br>The `JRepUtil` class implements these methods. |

# Part I

## Overview and Preinstallation

The part of this guide introduces Enterprise Manager Grid Control and provides information about preinstallation requirements and certifications including hardware, software, browser, and target certifications.

This part contains the following chapters:

- Chapter 1, "Getting Started with Enterprise Manager Grid Control"
- Chapter 2, "Overview of Enterprise Manager Grid Control"
- Chapter 3, "Preinstallation Requirements"
- Chapter 4, "Things to Know Before Installation"

# 1 Getting Started with Enterprise Manager Grid Control

After the installation, Enterprise Manager Grid Control (Grid Control) is automatically started. You can immediately log in to Grid Control with the SYSMAN account and begin using Enterprise Manager.

This chapter describes Enterprise Manager's ready-to-use configuration, recommends the tasks to be performed after installation to begin customizing it for your particular environment, and contains information on how to configure the Management Agent and the Oracle Management Service (OMS). The following topics are covered in this chapter:

- Enterprise Manager's Ready-To-Use Configuration
- Using the Enterprise Manager Grid Control Console for the First Time
- Controlling the Management Repository, Service, and Agent

## 1.1 Enterprise Manager's Ready-To-Use Configuration

At install time, the following tasks are automatically performed, with no user interaction required:

- The default super administrator SYSMAN account is created with the password you specified.
- The SYSMAN account is automatically configured to receive e-mail notifications if you provided the e-mail notification settings at installation time.
- E-mail notifications are set up with default Notification Rules for the critical conditions.
- Supported targets located on the same host machine as the Management Agent are automatically discovered.

### 1.1.1 Default Super Administrator: SYSMAN

A default super administrator account, SYSMAN, is created with the password you specified during the installation. After installation, you can immediately log in to the Grid Control Console with this user name and password to perform management tasks. The SYSMAN account owns the database schema containing the Management Repository.

**See Also:** *Setting Up Enterprise Manager for Your Environment* chapter of *Oracle Enterprise Manager Concepts* to learn more about the SYSMAN user account

### 1.1.2 E-mail Notifications

The SYSMAN account is automatically configured to receive e-mail notifications from Enterprise Manager if, during installation, you specified the Outgoing (SMTP) Mail Server and SYSMAN e-mail address. Also, as part of the self-monitoring feature, a script is created that enables the user to be notified by e-mail in the event that Enterprise Manager stops unexpectedly.

**Note:** If you do not specify the mail server, there will be no notification. If you specify the mail server, but not the e-mail address, the system is set up to send e-mail notifications, but the SYSMAN account does not receive any notifications. If you did not specify the information during installation, you can set up e-mail notification afterwards using Enterprise Manager Grid Control.

### 1.1.3 Notification Rules

E-mail notifications are set up with default Notification Rules for the critical conditions that could occur for all supported target types. For example, for the database target type, a rule is created such that e-mail notifications are sent when any database becomes unavailable, or if any of its key performance metrics (Datafile Usage percentage, Archiver Hung Error Stack, Tablespace Space Used%, and others) becomes critical. The e-mail notifications are sent to the e-mail address associated with the SYSMAN account. These rules are public; when other administrators are created, they can subscribe to them later.

**See Also:** For more information on the notification rules, in Enterprise Manager, click **Preferences,** then **Rules.** Click **Help** on that page.

### 1.1.4 Automatic Discovery

The first time the Management Agent is started, most supported targets that are located on the same host machine as the Management Agent are automatically discovered, and default monitoring levels and data collections are automatically enabled.

All targets, such as Oracle Collaboration Suite targets, Web applications, clusters, and Beacons are discovered automatically during the installation phase itself. But, you must manually discover the targets that have been installed after the Management Agent installation.

**Caution:** If you are performing an Oracle RAC agent installation on Microsoft Windows, only the host and cluster targets are discovered (automatically) during the installation phase. To discover all other targets, you must execute the following command on each node:

```
<AGENT_HOME>/bin/agentca -d
```

**See Also:**

- To view a list of certified targets for Grid Control, see Section 3.2, "Operating System, Browser, Target Certification".
- *Managing Oracle Collaboration Suite* available on Oracle Technology Network, for instructions on discovering Oracle Collaboration Suite targets
- Adding Targets to Be Monitored and Administered by Enterprise Manager in the Oracle Enterprise Manager online Help for information on manual discovery

#### 1.1.4.1 Troubleshooting Issues Concerning Target Discovery

If you are unable to discover targets on a Management Agent host, check for the following problems.

When the Management Agent is installed, an automatic discovery is performed to detect any existing Oracle9*i* Application Server release 9.0.2 or 9.0.3 instances. If the 9.0.2 or 9.0.3 Oracle9*i*AS instances were installed by a different OS user than the user that installs the Management Agent, then the file protections on targets.xml file within that Oracle9*i* Application Server installation may prevent the Management Agent from reading the file. This prevents the discovery of that Oracle9*i* Application Server instance.

To confirm that this is the problem, check the Management Agent logs located at `AGENT_HOME/sysman/log/` for *permission denied* errors, where `AGENT_HOME` is the Oracle home for the Management Agent. To correct the problem, set the file permissions so that it can be read by the user who installed the Management Agent.

This problem does not occur when discovering other existing Oracle Application Server versions on a machine.

**See Also:** Section 15.4, "Configuring Database and ASM Targets for Monitoring" for more information, if you encounter problems monitoring Oracle Database 10*g* or ASM targets

## 1.2 Using the Enterprise Manager Grid Control Console for the First Time

Enterprise Manager Grid Control provides a Web-based console for managing your entire enterprise.

The first column describes actions that you may want to perform; the second contains considerations and reasons for performing the action; the third helps you navigate to the appropriate online Help page in Enterprise Manager.

All Help topics are contained within the Setting Up Enterprise Manager directory of the online Help.

### 1.2.1 Enabling or Disabling the Licensed Function

Before you begin using Enterprise Manager Grid Control, you must first set the access levels according to your licensing agreement with Oracle. To do this, perform the following steps using a super administrator account, such as SYSMAN.

1. After you log in using SYSMAN, in the Grid Control console, click **Setup,** then **Management Pack Access.**
2. Select **Grant Access** or **Remove Access** for each pack, according to the terms of your licensing agreement.

3. Click **Apply** to save your changes. Once access is removed, the function associated with the selected pack is no longer available for any targets managed by Enterprise Manager Grid Control.

## 1.3 Controlling the Management Repository, Service, and Agent

The OMS and the Grid Control console are automatically started after the Enterprise Manager installation. This section provides information on how to manipulate the Management Agent and OMS after installation.

**See Also:**

- *Understanding the Directory Structure* section of *Oracle Enterprise Manager Advanced Configuration* for information on Enterprise Manager's directory structure
- *Oracle Enterprise Manager Advanced Configuration* for information on configuring Enterprise Manager components, such as Management Agents and Beacons for use in a firewall environment

### 1.3.1 Starting the Management Repository Database

If you need to start the Management Repository database, use SQL*Plus to connect to Oracle as SYSDBA, and then issue the `STARTUP` command.

**Caution:** During a restart of a machine, the repository database startup script runs automatically only if you have performed the Enterprise Manager installation using a new database.

For all other Enterprise Manager installation types, you will have to manually start the repository database on reboot.

**See Also:**

- *Maintaining and Troubleshooting the Enterprise Repository* chapter of *Oracle Enterprise Manager Advanced Configuration* for instructions on managing the repository database, such as how to drop the repository schema
- *Starting Up and Shutting Down* chapter in the *Oracle Database Administrator's Guide* for detailed instructions on starting up a database

### 1.3.2 Starting and Stopping the OMS

The relevant `emctl` commands are listed in Table 1.1.

You must be in the `OMS_HOME/bin` directory to issue the `emctl` commands, where `OMS_HOME` is the Oracle Application Server home directory in which the OMS is installed and deployed.

**Note:** To execute the `opmnctl` commands, you must be in the `OMS_HOME/opmn/bin` directory.

***Table 1–1 Commands to Start and Stop OMS***

| If you want to | Enter the following command |
|---|---|
| Start the OMS | `emctl start oms` |
| Stop the OMS | `emctl stop oms` |
| Verify status of the OMS | `emctl status oms` |
| Verify status of all OPMN processes | `opmnctl status` |
| Start all components of Oracle Application Server, including OMS and Web Cache | `opmnctl startall` |
| Stop all components of Oracle Application Server, including OMS and Web Cache | `opmnctl stopall` |

**Note:** Use the same `emctl` commands on Microsoft Windows as well, to perform the above-mentioned actions. Optionally, you can use `emctl.bat` and `opmnctl.bat` on Microsoft Windows, though the extension is not mandatory.

**Caution:** During a reboot of a machine, the OMS startup script runs automatically to start the OMS only if you have performed the Enterprise Manager installation using a new database. In this case, you do not have to manually start the OMS.

For all other Enterprise Manager installation types, you will have to manually start the OMS on reboot.

**See Also:** Starting and Stopping Enterprise Manager Components section of the *Introduction to Enterprise Manager Advanced Configuration* chapter of *Oracle Enterprise Manager Advanced Configuration* at

`http://otn.oracle.com/documentation/oem.html`

### 1.3.3 Starting and Stopping the Management Agent

The relevant `emctl` commands for UNIX are listed in Table 1.2.

You must be in the `<AGENT_HOME>/bin` directory to issue the `emctl` commands, where AGENT_HOME is the Oracle home directory for your Management Agent. Note that this directory is different than the `<AS_HOME>/bin` directory, which is for the Oracle Application Server Control Agent.

***Table 1–2 Commands to Start and Stop Management Agent***

| If you want to | Enter the following command |
|---|---|
| Start the Management Agent | `emctl start agent` |
| Stop the Management Agent | `emctl stop agent` |

*Table 1–2 (Cont.) Commands to Start and Stop Management Agent*

| If you want to | Enter the following command |
|---|---|
| Verify status of the Management Agent | `emctl status agent` |

**Note:** On Microsoft Windows, the services are started automatically by the operating system.

**Caution:** During a restart of a machine, the agent startup script runs automatically to start the Management Agent only if you have performed the Enterprise Manager installation using a new database, or have installed only the Management Agent.

For all other Enterprise Manager installation types, you will have to manually start the agent when you restart the machine.

**See Also:** Starting and Stopping Enterprise Manager Components section of the *Introduction to Enterprise Manager Advanced Configuration* chapter of *Oracle Enterprise Manager Advanced Configuration* at:

`http://otn.oracle.com/documentation/oem.html`

### 1.3.4 Starting Oracle Application Server Console

Oracle Application Server Control console is the Web-based management tool for Oracle Application Server and is used to monitor the Enterprise Manager targets.

After successful Enterprise Manager installation, you must manually start the Application Server console before starting the Enterprise Manager console.

To start the Application Server console, go to the OMS Oracle home and execute the `start iasconsole` command. The usage is as follows:

```
<OMS_HOME>/bin/emctl start iasconsole
```

### 1.3.5 Accessing Oracle Application Server Console from Enterprise Manager Grid Control Console

To access the Oracle Application Server console from the Enterprise Manager Grid Control console, follow these steps:

1. Log in to Enterprise Manager Grid Control.
2. Click **Targets** and then **All Targets**.
3. From the Search list, select **Oracle Application Server**, and click **Go**.
4. From the results table, click the name of the Oracle Application Server that was installed with Enterprise Manager Grid Control to view its home page.
5. On the Oracle Application Server Home page, from the Related Links section, click **Administer** to access the Application Server console.

**Note:**

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

```
<Oracle_Home>/bin/emctl secure oms
```

The above-mentioned command secures only OMS but does not secure the Oracle Application Server that was installed with Enterprise Manager Grid Control. This is an expected behaviour, and it is not required to secure the Oracle Application Server that was installed with Enterprise Manager Grid Control.

However, if you have a standalone Oracle Application Server and if you want to secure that, then run the following command:

```
emctl secure em
```

### 1.3.6 Accessing Enterprise Manager Grid Control

To log in to the Grid Control console, use the following URL:

```
http://<oms_hostname>.<domain>:<port>/em
```

or

```
https://<oms_hostname>.<domain>:<port>/em
```

If you are uncertain about the port number, you can refer to one of the following files:

- `ORACLE_HOME/install/setupinfo.txt` as displayed by Oracle Universal Installer at the end of the installation
- `ORACLE_HOME/install/portlist.ini` on the OMS machine
- `<OMS Home>/sysman/config/emoms.properties`

  Here, check the `properties` `oracle.sysman.emSDK.svlt.ConsoleServerPort` and `oracle.sysman.emSDK.svlt.ConsoleServerHTTPSPort` for unsecure and secure ports respectively.

When the login dialog box appears, enter the user name and password for the super administrator SYSMAN.

**Note:**

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

```
<Oracle_Home>/bin/emctl secure oms
```

The above-mentioned command secures only OMS but does not secure the Oracle Application Server that was installed with Enterprise Manager Grid Control. This is an expected behaviour, and it is not required to secure the Oracle Application Server that was installed with Enterprise Manager Grid Control.

However, if you have a standalone Oracle Application Server and if you want to secure that, then run the following command:

```
emctl secure em
```

**See Also:**

- *Enterprise Manager Security* chapter of *Oracle Enterprise Manager Advanced Configuration* for more information on Grid Control security
- Viewing a Summary of the Ports Assigned During the Application Server Installation section of the *Configuring Firewalls* chapter of *Oracle Enterprise Manager Advanced Configuration* for more information on port settings
- *Viewing and Modifying Application Server Port Assignments* in the Enterprise Manager online Help.

### 1.3.7 Unlock the DBSNMP User Account

To unlock the DBSNMP user account:

1. From the Grid Control console, navigate to the Database Home page and click **Administration** to display the list of administration functions.
2. Under Users and Privileges, click **Users** to display the list of all user accounts. If you are prompted to log in to the database, make sure to use a database user account with DBA privileges such as SYSTEM.
3. Find and select the DBSNMP user account, select **Unlock User** from the Actions menu, and click **Go** to confirm your choice.
4. Set the DBSNMP password as described in the Section 1.3.8, "Set Monitoring Credentials" section. Once the password is set, monitoring can begin.

### 1.3.8 Set Monitoring Credentials

You must reset the monitoring credentials for database and ASM targets if the passwords you specified during installation were different from the defaults that Enterprise Manager expects. If you change a password at any time, make sure to update all components using that password as well.

This section contains the following subsections:

- Setting Monitoring Credentials for Database Targets
- Setting Monitoring Credentials for ASM Targets

#### 1.3.8.1 Setting Monitoring Credentials for Database Targets

To set the monitoring credentials for a single-instance or cluster Oracle Database 10*g* target:

1. From the Grid Control console, navigate to the Configure Database: Properties page:

   a. On the **Targets** tab, click **Databases** to display the list of database targets.

   b. Find and select the database target and click **Monitoring Configuration.**

   Enterprise Manager displays the Configure Database: Properties page.

2. Enter the correct password for the DBSNMP user in the **Monitor Password** field and click **Test Connection** to verify the monitoring credentials.
3. If the connection is successful, click **Next,** then click **Submit.**

You should now be able to view the complete Database Home page for the Oracle Database 10*g* target. For more information, see *Specifying New Target Monitoring Credentials* in *Oracle Enterprise Manager Advanced Configuration*.

#### 1.3.8.2 Setting Monitoring Credentials for ASM Targets

> **Note:** You must ensure the DBSNMP password that is required to monitor database targets is correctly set, before proceeding to set the monitoring credentials for the Automatic Storage Management targets.

To set the monitoring credentials for an ASM target:

1. From the Grid Control console, click **All Targets** on the **Targets** tab to display a list of all managed targets.
2. Find and select the ASM target that you want to modify.
3. Click **Configure** to display the ASM Monitoring Configuration page.
4. Enter the ASM SYS password in the **Password** field and click **OK.**

You should now be able to view the complete home page for the ASM target without any Management Agent or collection errors. For more information, see *Specifying New Target Monitoring Credentials* in *Oracle Enterprise Manager Advanced Configuration*.

### 1.3.9 Privileges Required for Accessing the Database Performance Tab

The following privileges are required for accessing the Performance tab of a database target:

- create session
- select_catalog_role
- select any dictionary

If you do not have these privileges, you may see an error while accessing the Performance tab.

# 2

# Overview of Enterprise Manager Grid Control

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

This chapter contains the following sections:

- Grid Control Overview
- Grid Control Architecture

## 2.1 Grid Control Overview

Grid Control is a system management software that delivers centralized monitoring, administration, and life cycle management functionality for the complete Oracle IT infrastructure, including systems running Oracle and non-Oracle technologies. Your infrastructure may comprise multiple Oracle Databases, Oracle WebLogic Managed Servers, Web applications deployed on these servers, hosts running these targets, and so on. You can, of course, use the individual product consoles to monitor the status of each of these targets, but it becomes cumbersome to shuttle between multiple console windows and track the performance of each of these targets using so many windows.

Grid Control offers a single-window solution that allows you to monitor and manage the complete Oracle IT infrastructure from a single console. Grid Control also offers support for monitoring certain non-Oracle products, for example, IBM WebSphere Application Server, Microsoft SQL Server, Juniper Networks NetScreen Firewall, and so on.

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

For more information about Grid Control, visit our Web site access the following URL:

`http://www.oracle.com/enterprise_manager/index.html`

## 2.2 Grid Control Architecture

Although Grid Control is viewed as a single entity, technically, it is built with the following software components:

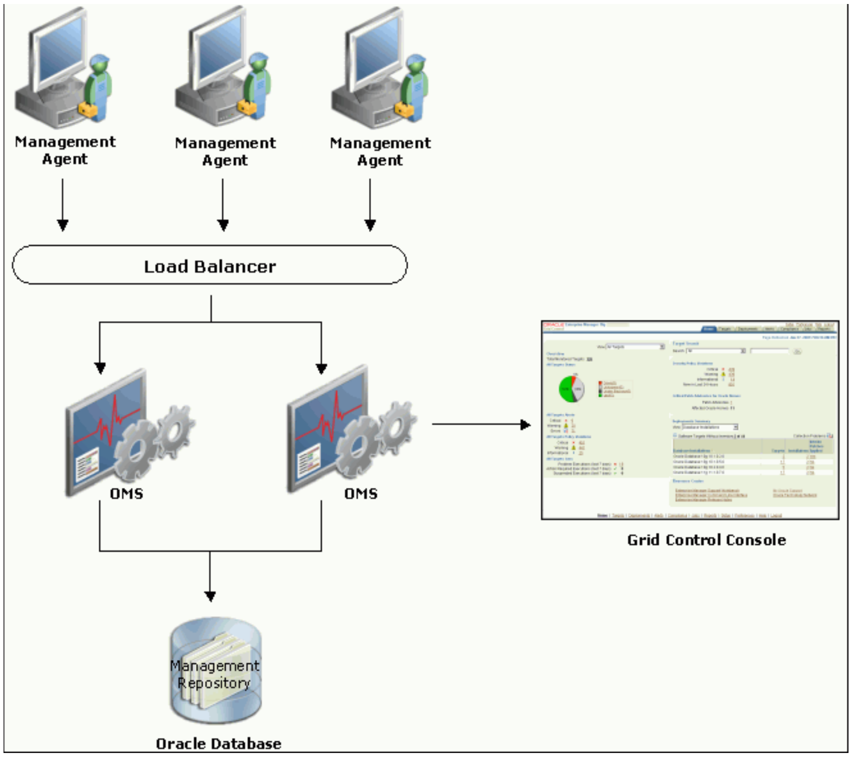
- Oracle Management Service (OMS)

- Oracle Management Agent (Management Agent)
- Oracle Management Repository (Management Repository)

While OMS acts as the brain of the Grid Control architecture responsible for communicating with Management Agents and a central repository that stores information, Management Agent acts as the hands and legs of a body responsible for collecting information from the monitored targets and transporting them to OMS. And, Management Repository is the repository configured in Oracle Database to store the collected information.

The following illustrates the Grid Control architecture:

***Figure 2–1 Enterprise Manager Grid Control Architecture***



After installing Grid Control, what you see is the Grid Control Console, the user interface that displays information about the health of the monitored targets. However, internally, OMS orchestrates with Management Agents to discover targets, monitor and manage them, and store the collected information in a repository for future reference and analysis.

To summarize, Grid Control has the following core componets:

***Table 2–1 Enterprise Manager Grid Control Components***

| Component | Definition |
|---|---|
| Oracle Management Agent (*Management Agent*) | Management Agent is an integral software component that is deployed on each monitored host. It is responsible for monitoring all the targets running on those hosts, communicating that information to the middle-tier Oracle Management Service, and managing and maintaining the hosts and its targets. |

***Table 2–1 (Cont.) Enterprise Manager Grid Control Components***

| **Component** | **Definition** |
|---|---|
| Oracle Management Service (*OMS*) | OMS is a J2EE Web application that orchestrates with Management Agents to discover targets, monitor and manage them, and store the collected information in a repository for future reference and analysis. OMS also renders the user interface for the Grid Control console. OMS is deployed to the application server that is installed along with other core components of Grid Control. |
| Oracle Management Repository (*Management Repository*) | Management Repository is the storage location where all the information collected by the Management Agent gets stored. It consists of objects such as database jobs, packages, procedures, views, and tablespaces.<br>Technically, OMS uploads the monitoring data it receives from the Management Agents to the Management Repository. The Management Repository then organizes the data so that it can be retrieved by OMS and displayed in the Grid Control console. Since data is stored in the Management Repository, it can be shared between any number of administrators accessing Grid Control.<br>Management Repository is configured in Oracle Database. This Oracle Database can either be an existing database in your environment or a new one installed along with other core components of Grid Control. |
| Grid Control Console | Grid Control Console is the user interface you see after you install Grid Control. From the Grid Control console, you can monitor and administer your entire computing environment from one location on the network. All the services within your enterprise, including hosts, databases, listeners, application servers, and so on, are easily managed from one central location. |

# 3 Preinstallation Requirements

This chapter provides information about the preinstallation requirements you must meet before installing Enterprise Manager Grid Control (Grid Control).

In particular, this chapter covers the following:

- Hardware Requirements
- Operating System, Browser, Target Certification
- Software Requirements
- Network Requirements
- Operating System Groups and Users Requirements

## 3.1 Hardware Requirements

This section lists the recommended hardware requirements for running the various Grid Control deployment sizes on all the supported platforms. In particular, this section covers the following:

- Recommended CPU and Memory Allocation
- Temporary Disk Space Requirements on HP-UX
- Temporary Disk Space Requirements on IBM AIX
- Considering Resource Allocation

### 3.1.1 Recommended CPU and Memory Allocation

Table 3–1 and Table 3–2 approximate the host, CPU, and physical memory requirements for running a Grid Control deployment (typical scenario with 2 to 3 GHz machines), based on experiences with real-world Grid Control deployments.

*Table 3–1 CPU and Memory Allocation for Oracle Management Service*

| Deployment Size | Host | CPU/Host | Physical Memory (RAM)/Host | Total Recommended Space |
|---|---|---|---|---|
| Small (100 monitored targets) | 1 | 1 (3 GHz) | 2 GB | 2 GB |
| Medium (1,000 monitored targets) | 1 | 2 (3 GHz) | 2 GB | Number of OMS x 5 GB |
| Large (10,000 monitored targets) | 2 | 2 (3 GHz) | 2 GB | Number of OMS x 10 GB |

*Table 3–2 CPU and Memory Allocation for Oracle Management Repository*

| Deployment Size | Host | CPU/Host | Physical Memory (RAM)/Host | Total Repository Storage |
|---|---|---|---|---|
| Small (100 monitored targets) | 1[1] | 1 (3 GHz) | 2 GB | 10 GB |
| Medium (1,000 monitored targets) | 1 | 2 (3 GHz) | 4 GB | 30 GB |
| Large (10,000 monitored targets) | 2 | 4 (3 GHz) | 6 GB | 150 GB |

[1] Share Host with the Oracle Management Service for small deployments.

**For Oracle Management Agent** (Management Agent), the hard disk space required is 400 MB for Linux (32-bit) and500 MB for Microsoft Windows (32-bit). For information about hard disk space required for other platforms, see the Agent Best Practices document available at the following URL:

`http://www.oracle.com/technology/products/oem/pdf/10gr2_agent_deploy_bp.pdf`

> **ATTENTION:** Oracle recommends that you allocate a minimum default size of 1 GB hard disk space for the `MGMT_ECM_DEPOT_TS` tablespace and allocate the rest of the recommended repository database space for the `MGMT_TABLESPACE`.
>
> Oracle also recommends that you keep the auto-extend feature enabled for the tablespace data files.
>
> Note that the space requirement increases as the number of monitored targets increase, along with the input/output performance demands on the storage devices.

## 3.1.2 Temporary Disk Space Requirements on HP-UX

To determine the amount of free disk space available in the `/tmp` directory, enter the following command:

```
# bdf /tmp
```

If there is less than 1.2 GB of disk space available in the `/tmp` directory, then complete one of the following steps:

- Delete unnecessary files from the `/tmp` directory.
- Set the `TEMP` and `TMPDIR` environment variables to a writable directory with at least 1.2 GB of available disk space.
- Extend the file system that contains the `/tmp` directory. If required, contact your system administrator for information about extending file systems.

## 3.1.3 Temporary Disk Space Requirements on IBM AIX

To determine the amount of free disk space available in the `/tmp` directory, enter the following command:

```
# df /tmp
```

If there is less than 1300 MB of disk space available in the /tmp directory, then complete one of the following steps:

- Delete unnecessary files from the /tmp directory.
- Set the TEMP and TMPDIR environment variables to a writable directory with at least 1300 MB of available disk space.
- Extend the file system that contains the /tmp directory. If required, contact your system administrator for information about extending file systems.

For Management Agent deployments, make sure that /tmp directory has 1300 MB of disk space available on the target machine.

### 3.1.4 Considering Resource Allocation

Carefully consider resource allocation when choosing the disk on which you want to install Oracle Management Service (OMS) and the database that will house the Oracle Management Repository (Management Repository).

Grid Control's ready-to-use monitoring starts generating information upon installation, meaning that resource consumption begins immediately. As such, consider the base system resource consumption prior to installing. Select your installation locations strategically, taking into account system load, memory usage, and disk input/output.

For example, you can split the input/output load across disks. Avoid installing the database, which will house the Management Repository, or the OMS on the swap volume, a volume with a busy state (as per iostat) of 10 percent or more, or on a memory-constrained system. As with any data-intensive application, if your Management Repository is going to service a large number of targets, it is important to tune the database appropriately to maximize input/output capacity. Refer to the *Database Performance Tuning Guide* for more information.

While adding more resources can help alleviate potential problems (for instance, adding a second disk dedicated to the OMS on a system), understanding and accounting for resource allocation is the best way to achieve strategic setup and good performance.

## 3.2 Operating System, Browser, Target Certification

For information about the operating systems, browsers, and targets certified for Grid Control, see the My Oracle Support note 412431.1.

To access this note, access My Oracle Support (formerly Metalink) at the following URL. Once you log in, select the **Certify** tab. On the Certify page, click **View Certifications by Product**, and from the list, select **Enterprise Manager 10g Grid Control**. On the following page, click note 412431.1.

http://metalink.oracle.com/

For detailed information on the required packages and kernel parameters for each platform, see Appendix D, "Platform-Specific Package and Kernel Requirements".

**Note:** Oracle offers code fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for code 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 Grid Control installation, you must consider Enterprise Manager Grid Control's framework components as well as the targets monitored by Enterprise Manager Grid Control.  Oracle recommends keeping your Grid Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.

For information about the certified combinations of Enterprise Manager Grid Control components and monitored targets, see *My Oracle Support* note.412431.1.

## 3.3 Software Requirements

This section describes the software requirements for each Grid Control component. In particular, this section covers the following:

- Oracle Management Repository Software Requirements
- Oracle Management Service Software Requirements
- Oracle Management Agent Software Requirements

### 3.3.1 Oracle Management Repository Software Requirements

Grid Control requires an Oracle Database where the Management Repository can be created.

- **For Enterprise Manager Grid Control with a New Database:** Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux or 10.2.0.2 for Microsoft Windows) comes with an embedded Oracle Database 10*g* Release 1 (10.1.0.4). Therefore, if you install Enterprise Manager Grid Control with a new database, then this Oracle Database is installed automatically and you do not need to install any other software manually.
- **For Enterprise Manager Grid Control with an Existing Database:** If you install Enterprise Manager Grid Control with an existing database, then ensure that you have a certified Oracle Database as described in My Oracle Support note 412431.1.

  If you want to use a RAC database, which is configured on a virtual host as the existing database, then refer to My Oracle Support note 561441.1.

  If you want to use Oracle Database 11g as the existing database, then you must follow one of these methods. The instructions for these methods are described in My Oracle Support note 467677.1.

  - **Method 1:** Install Enterprise Manager 10g Grid Control Release 2 (for example, 10.2.0.1 Linux or 10.2.0.2 Microsoft Windows) with a database certifeid for that base release. Then, patch Grid Control to Enterprise Manager 10g Grid Control Release 4 (10.2.0.4 or higher) and upgrade the database to Oracle Database 11g.

- **Method 2:** Install Enterprise Manager 10g Grid Control Release 4 (10.2.0.4 or higher) directly using the *software-only and configure later* method as described in Section 8.6, "Installing 'Software-Only' and Configuring Later" with a database certifeid for that base release. Then, upgrade the database to Oracle Database 11g.

> **Note:** When using an existing database for the Management Repository, ensure that all software, patches, and tuning requirements are met for the existing database and host, as well as for the Management Repository. For more information on the recommended database initialization parameters refer to Section 8.4.3.1, "Check Database Initialization Parameters".

### 3.3.2 Oracle Management Service Software Requirements

OMS has NO additional software requirements.

OMS is installed with and deployed on Oracle Application Server. As a result, when you install the OMS, the installation procedure first installs Oracle Application Server.

Specifically, the installation procedure installs the Oracle Application Server J2EE and Web Cache installation type. The OMS  is deployed on its own OC4J container in this application server instance.

### 3.3.3 Oracle Management Agent Software Requirements

The software requirements for Management Agents depend on the installation method chosen for installing them.

- **agentDownload Script:** If you choose to install Management Agents using the agentDownload script on Linux as well as Microsoft Windows platforms, then you need WGET software. For information about agentDownload script, see Section 10.3.1, "Overview".

  To download the WGET software, access the following URL:

  `http://gnuwin32.sourceforge.net/packages/wget.htm`

- **Agent Deploy Application:** If you choose to install Management Agents using the Agent Deploy application, then you need an SSH software to set up SSH connectivity between the host running OMS and the host where the Management Agent needs to be installed. For information about Agent Deploy application, see Section 10.1, "Installing Management Agent Using Agent Deploy Application".

  For Linux platforms, the SSH software is available on the hosts by default. However, for Microsoft Windows platforms, you need to download and install Cygwin Suite. To download Cygwin Suite, access the following URL:

  `http://www.cygwin.com`

  For detailed information on the required packages and kernel parameters for each platform, see Appendix D, "Platform-Specific Package and Kernel Requirements".

**Note:** Oracle offers code fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for code 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 Grid Control installation, you must consider Enterprise Manager Grid Control's framework components as well as the targets monitored by Enterprise Manager Grid Control.  Oracle recommends keeping your Grid Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license.

For information about the certified combinations of Enterprise Manager Grid Control components and monitored targets, see *My Oracle Support* note.412431.1.

## 3.4 Network Requirements

This section describes the following network requirements:

- Proximity
- Host File with Correct Host Name and IP Address
- Server Name Dependent on the Order of the IP Address Entry

### 3.4.1 Proximity

The OMS host and the Repository host must be located in close proximity to each other. Ideally, the round trip network latency between the two should be less than 1 millisecond.

See Section A.6, "Network Issues" for more information about network requirements.

### 3.4.2 Host File with Correct Host Name and IP Address

Before installing any of the components, ensure that the host names and IP addresses are configured properly in the /etc/hosts file. For example, for installing a Management Agent on a host, ensure that the host name specified in the /etc/hosts file maps to the correct IP address of that host. Otherwise, the installation can fail on the product-specific prerequisite check page.

To resolve this issue, first run the following command on the host to list all the IP addresses configured and then note the IP address for that host:

For UNIX Platforms:

```
ifconfig
```

For Microsoft Windows Platforms:

```
ipconfig
```

After noting the IP address of that host, open the /etc/hosts file and check the entries for this host name. Ensure that the host name maps to the correct IP address of that host.

Also, if DNS server is configured in your environment, then you should be able to use DNS to resolve the name of the host on which you want install OMS. For more information, contact your network administrator.

### 3.4.3 Server Name Dependent on the Order of the IP Address Entry

While installing Management Agents, note that the server name is resolved based on the entry made in the /etc/hosts file.

- If the entry in the /etc/hosts file is as shown below, then the Management Agent shows up as the fully qualified domain name.

  ```
  <ip> <fully qualified domain name> <server name>
  ```

- If the entry in the /etc/hosts file is as shown below, then the Management Agent shows up as the server name.

  ```
  <ip> <server name> <fully qualified domain name>
  ```

## 3.5 UMASK Value Requirements

The recommended "umask" is 022. Set the default file mode creation mask (umask) to 022 in the shell startup file.

For example:

**Bash shell**

```
$ . ./.bash_profile
```

**Bourne or Korn shell**

```
$ . ./.profile
```

**C shell**

```
% source ./.login
```

## 3.6 Operating System Groups and Users Requirements

The section explains what operating system groups and users you need to create and how to create them. In particular, this section covers the following:

- For All Installation Types
- For The Installation Type "Enterprise Manager Grid Control with a New Database"
- How To Create Operating System Groups and Users

### 3.6.1 For All Installation Types

The following operating system group and user are required for all installation types:

- The Oracle Inventory Group (`oinstall`)

  You must create this group the first time you install Oracle software on the system. The default name chosen for this group is `oinstall`. This group owns the Oracle inventory that is a catalog of all Oracle software installed on the system.

> **Note:** If Oracle software is already installed on the system, then the existing Oracle Inventory group must be the primary group of the operating system user that you use to install other Oracle software.

- The Oracle Software Owner User (typically, `oracle`)

  You must create this user the first time you install Oracle software on the system. This user owns all of the software installed during the installation. This user must have the Oracle Inventory group as its primary group. If you are installing Enterprise Manager Grid Control with a New Database, then the user must also have the OSDBA and OSOPER groups as secondary groups. For details about OSDBA and OSOPER groups, refer to Section 3.6.2, "For The Installation Type "Enterprise Manager Grid Control with a New Database"".

  > **Note:** In Oracle documentation, this user is referred to as the `oracle` user.

A single Oracle Inventory group is required for all installations of Oracle software on the system. After the first installation of Oracle software, you must use the same Oracle Inventory group for all subsequent Oracle software installations on that system. However, you can choose to create different Oracle software owner users, OSDBA groups, and OSOPER groups (other than `oracle`, `dba`, and `oper`) for separate installations. By using different groups for different installations, members of these different groups have DBA privileges only on the associated databases rather than on all databases on the system.

### 3.6.2 For The Installation Type "Enterprise Manager Grid Control with a New Database"

If you are installing Enterprise Manager Grid Control with a New Database, then in addition to the operation system group and user mentioned in Section 3.6.1, "For All Installation Types", the following are also required:

- The OSDBA group (`dba`)

  You must create this group if you do not have Oracle Database already installed. It identifies the operating system user accounts that have database administrative privileges (the SYSDBA privilege). The default name for this group is `dba`.

- The OSOPER group (`oper`)

  This is an optional group. Create this group if you want a separate group of operating system users to have a limited set of database administrative privileges (the SYSOPER privilege). By default, members of the OSDBA group also have the SYSOPER privilege.

- An unprivileged user

  Verify that the unprivileged user nobody exists on the system. The nobody user must own the external jobs (extjob) executable after the installation.

  > **See Also:** For more information about the OSDBA and OSOPER groups and the SYSDBA and SYSOPER privileges, see *Oracle Database Administrator's Reference for UNIX-Based Operating Systems* and *Oracle Database Administrator's Guide*.

## 3.6.3 How To Create Operating System Groups and Users

The following sections describe how to create the required operating system users and groups:

- Creating the Oracle Inventory Group
- Creating the OSDBA Group
- Creating an OSOPER Group (Optional)
- Creating the Oracle Software Owner User

> **Note:** As an alternative to creating local users and grouops, you can create the appropriate users and groups in a directory service, for example, Network Information Services (NIS). For information about using directory services, contact your system administrator or refer to your operating system documentation.

### 3.6.3.1 Creating the Oracle Inventory Group

You must create the Oracle Inventory group if it does not already exist. The following subsections describe how to determine the Oracle Inventory group name, if it exists, and how to create it if necessary.

#### 3.6.3.1.1 Determining Whether the Oracle Inventory Group Exists

When you install Oracle software on the system for the first time, Oracle Universal Installer creates the `oraInst.loc` file. This file identifies the name of the Oracle Inventory group and the path to the Oracle Inventory directory.

To determine whether the Oracle Inventory group exists, enter the following command:

```
# more /etc/oraInst.loc
```

If the output of this command shows the `oinstall` group name, then the group already exists.

If the `oraInst.loc` file exists, then the output from this command looks like:

```
inventory_loc=/u01/app/oracle/oraInventory
inst_group=oinstall
```

The `inst_group` parameter shows the name of the Oracle Inventory group, `oinstall`.

#### 3.6.3.1.2 Creating the Oracle Inventory Group

If the `oraInst.loc` file does not exist, then create the Oracle Inventory group using the following command:

```
# /usr/sbin/groupadd oinstall
```

### 3.6.3.2 Creating the OSDBA Group

You must create an OSDBA group in the following cases:

- An OSDBA group does not exist, for example, if you do not have Oracle Database already installed on the system.
- An OSDBA group exists, but you want to give a different group of operating system users database administrative privileges in a new Oracle installation.

If the OSDBA group does not exist or if you require a new OSDBA group, then create it as follows. In the following command, use the group name `dba` unless a group with that name already exists.

```
# /usr/sbin/groupadd dba
```

#### 3.6.3.3 Creating an OSOPER Group (Optional)

Create an OSOPER group only if you want to identify a group of operating system users with a limited set of database administrative privileges (SYSOPER operator privileges). For most installations, it is sufficient to create only the OSDBA group. If you want to use an OSOPER group, then you must create it in the following circumstances:

- If an OSOPER group does not exist, for example, if this is the first installation of Oracle Database software on the system
- If an OSOPER group exists, but you want to give a different group of operating system users database operator privileges in a new Oracle installation

If you require a new OSOPER group, then create it as follows. In the following command, use the group name `oper` unless a group with that name already exists.

```
# /usr/sbin/groupadd oper
```

#### 3.6.3.4 Creating the Oracle Software Owner User

You must create an Oracle software owner user in the following circumstances:

- If an Oracle software owner user does not exist, for example, if this is the first installation of Oracle software on the system
- If an Oracle software owner user exists, but you want to use a different operating system user, with different group membership, to give database administrative privileges to those groups in a new Oracle Database installation

##### 3.6.3.4.1 Determining Whether an Oracle Software Owner User Exists

To determine whether an Oracle software owner user named `oracle` exists, run the following command:

```
# id oracle
```

If the `oracle` user exists, then the output from this command looks like this:

```
uid=440(oracle) gid=200(oinstall) groups=201(dba),202(oper)
```

If the user exists, then determine whether you want to use the existing user or create another `oracle` user.

- To use the existing user, ensure that the user's primary group is the Oracle Inventory group and that it is a member of the appropriate OSDBA and OSOPER groups.
- To modify an existing user, refer to the Section 3.6.3.4.3, "Modifying an Oracle Software Owner User".
- To create a user, refer to Section 3.6.3.4.2, "Creating an Oracle Software Owner User".

**Note:** If necessary, contact your system administrator before using or modifying an existing user.

#### 3.6.3.4.2 Creating an Oracle Software Owner User

If the Oracle software owner user does not exist or if you require a new Oracle software owner user, then follow these steps to create one. In the following procedure, use the user name `oracle` unless a user with that name already exists.

1. To create the `oracle` user, enter a command similar to the following:

   ```
   # /usr/sbin/useradd -g oinstall -G dba[,oper] oracle
   ```

   In this command:

   - The `-g` option specifies the primary group, which must be the Oracle Inventory group, for example `oinstall`
   - The `-G` option specifies the secondary groups, which must include the OSDBA group and if required, the OSOPER group.   For example, `dba` or `dba,oper`

2. Set the password of the `oracle` user:

   ```
   # passwd oracle
   ```

#### 3.6.3.4.3 Modifying an Oracle Software Owner User

If the `oracle` user exists, but its primary group is not `oinstall` or it is not a member of the appropriate OSDBA or OSOPER groups, then enter a command similar to the following to modify it. Specify the primary group using the `-g` option and any required secondary group using the `-G` option:

```
# /usr/sbin/usermod -g oinstall -G dba[,oper] oracle
```

#### 3.6.3.4.4 Verifying that the User nobody Exists

Before installing the software, follow these steps to verify that the `nobody` user exists on the system:

1. To determine whether the user exists, enter the following command:

   ```
   # id nobody
   ```

   If this command displays information about the `nobody` user, then you do not have to create that user.

2. If the `nobody` user does not exist, then enter the following command to create it:

   ```
   # /usr/sbin/useradd nobody
   ```

# 4

# Things to Know Before Installation

This chapter provides information that helps you prepare better for a Enterprise Manager Grid Control (Grid Control) installation. Oracle recommends you to read this chapter before proceeding with the installation.

This chapter contains the following sections:

## 4.1 Understanding What This Guide Helps You Install and Upgrade

This guide helps you *install* only the full releases of Enterprise Manager 10g Grid Control Release 2 or higher. A 'full release' refers to the first, complete Enterprise Manager 10g Grid Control Release 2 or higher software that was released for a particular platform.

A full release comprises all three components that form the Grid Control, mainly Oracle Management Service (OMS), Oracle Management Repository (Management Repository), and Oracle Management Agent (Management Agent). You can use the full release to install either all three components or only an additional OMS or Management Agent.

You can also use this guide to *upgrade* an existing Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enterprise Manager 10 Grid Control Release 2 or higher. For example, you can use this guide to upgrade an existing Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) to Enterprise Manager 10g Grid Control Release 2 (10.2.0.1).

The following shows the full releases of Enterprise Manager 10g Grid Control Release 2 or higher that were released for various platforms. Use this guide for installing only these releases.

| **Full Release** | **Targeted Platforms** |
|---|---|
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.1.1) (RECUT) | Linux x86 |
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) | ▪ Solaris (SPARC)<br>▪ HP-UX (PARISC)<br>▪ AIX5L Based Systems |
| Enterprise Manager 10g Grid Control Release 2 (10.2.0.2.1) (RECUT) | Microsoft Windows (32-Bit) |
| Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) | ▪ Linux X86_64<br>▪ HP-UX ( Itanium ) |

In addition, there have been Patch Sets released periodically to patch these full releases and move them to higher releases. For example, Enterprise Manager 10g Release 2 (10.2.0.2) Patch Set was released for Linux x86 platform. The patch set helps you patch Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux x86 and move it to Release 2 (10.2.0.2).

This guide does not describe the patching procedures. The patching procedures are furnished in the Patch Set Notes document that is packaged with the Patch Set, not in this guide. You can download the Patch Sets and the relevant Patch Set Notes from My Oracle Support (formerly Metalink).

> **Note:** Patch Sets help you to only *patch* any previous releases of Enterprise Manager Grid Control and (or) Management Agent; they DO NOT *upgrade* your existing releases to newer full releases, say Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) to Enterprise Manager 10g Grid Control Release 2 (10.2.0.1).
>
> If you do not have a previous release, but want to have the most recent release of Grid Control, then first install a full release and then use the Patch Sets to patch it to a higher release.

## 4.2 Obtaining Software from Oracle Technology Network

You can download the Grid Control software from Oracle Technology Network (OTN) at:

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

**Note:** Before you download the software, Oracle recommends you to read the Enterprise Manager 10g Grid Control Certification matrix. The certification matrix shows the operating systems and browser versions on which Grid Control and Management Agent are certified.

The Enterprise Manager 10g Grid Control Certification matrix is available on My Oracle Support (formerly Metalink) at:

`http://metalink.oracle.com/`

Login and select the **Certify** tab. On the Certify page, click **View Certifications by Product** and select **Enterprise Manager 10g Grid Control**, and then click **Submit**.

### 4.2.1 Verifying the Downloaded Software

#### Verifying File Size

Verify that the file size of your downloaded software matches the file size displayed on OTN. After downloading the software, run the cksum command against the downloaded file to ensure that the file size of the downloaded software is the same as the file size on OTN.

For example, if you are downloading the Management Agent software of Release 10.2.0.3 for Linux x86 operating system, then you should see something like the following on OTN:

**For Linux x86**

*|x| Linux_Grid_Control_agent_download_10_2_0_3_0.zip (317,120,712 bytes) (cksum - 2359676224)*

The *(cksum - 2359676224)* value is the file size that you need to check. To do so, run the following command:

```
$ cksum Linux_Grid_Control_agent_download_10_2_0_3_0.zip
```

#### Verifying Platform Information

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

Do not try to try 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.

To verify the platform for which the software is downloaded, check the `shiphomeproperties.xml` file available in the `/Disk1/stage` directory.

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. The following table 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 4–1 Verifying Platform Information*

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

### 4.2.2 Extracting Software from the Zip Files

All OTN files have been archived using Info-ZIP's highly portable Zip utility. After downloading one or more of the archives, you will need the UnZip utility to extract the files.

You must unzip the archive on the platform for which it was intended. For example, if you download the software for the Linux operating system version of Grid Control, then you must unzip the file on a Linux operating system. 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 plan to store the files on a DVD-ROM, create a DVD-ROM from the contents of the zip file (extracted contents) and not the Zip files itself; you need the unzipped contents of the Zip files to do the installation.

## 4.3 Starting Oracle Universal Installer (OUI)

To set the mount point manually, complete these steps:

1. DVD-ROM users: Insert the Grid Control DVD-ROM into the DVD-ROM drive.
2. Start Oracle Universal Installer by executing the `runInstaller` script for Linux from the top directory of the DVD.

   Alternatively, you can change the directory to the `ORACLE_BASE`, the root directory where you will install the Oracle home, then specify the full path to `<DVD>/runInstaller` in OUI.

**DVD-ROM**

prompt> `cd`

prompt> `mount_point/10.2<DVD>/runInstaller`

This launches Oracle Universal Installer using which you install Grid Control.

## 4.4 Understanding Licensing Information

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 Services does not provide support for components for which licenses have not been purchased.

For more information refer to *Oracle Enterprise Manager Licensing Information*.

## 4.5 Understanding Oracle Directory

The directories in which you install the Grid Control components are called the Oracle homes. During installation, you specify the full path to a directory that contains all the Oracle homes as subdirectories. This parent directory is called the Oracle home directory or base directory.

If you choose to install Grid Control using a new database on a computer with no other Oracle software installed, Oracle Universal Installer creates an Oracle base directory for you. If Oracle software is already installed, then one or more Oracle base directories already exist. In the latter case, Oracle Universal Installer offers you a choice of Oracle base directories into which to install Oracle Database.

You are not required to create an Oracle base directory before installation, but you can do so if required. You can set the `ORACLE_BASE` environment directory, which Oracle Universal Installer will recognize.

**Note:** You can choose to create a new Oracle base directory, even if other Oracle base directories exist on that system.

Names of Oracle homes can contain only alphanumeric characters and underscores.

**ATTENTION:** Spaces are not allowed anywhere in the Oracle home directory path. The installer validates this. If you have spaces in the Oracle home directory path, the installation will fail.

## 4.6 Multiple Oracle Home Support

Grid Control is installed on multiple Oracle homes within the Oracle base directory. This means that a typical Grid Control installation creates three Oracle homes in different Oracle home directories. For example, `oms10g`, `db10g`, and `agent10g`.

**Note:** You must ensure that you install this product into a new Oracle home directory. You cannot install products from one release of Grid Control into an Oracle home directory of a different release. For example, you cannot install 10*g* R2 (10.2) software into an existing Oracle9*i* home directory. If you attempt to install this release into an Oracle home directory that contains software from an earlier Oracle release, the installation will fail.

You can install this release more than once on the same system, as long as each installation is done in a separate Oracle home directory.

## 4.7 Installing in an Existing Oracle Home

Generally, you cannot install Grid Control in an existing Oracle home, unless the Oracle home is empty.

## 4.8 Installing Enterprise Manager Grid Control As the First Oracle Software

If Grid Control is the first Oracle product that you are installing, the installer prompts you to specify an inventory directory (also called the `oraInventory` directory). This inventory directory is used by the installer to place all the installer files and directories on the computer. The installer automatically sets up subdirectories for each Oracle product to contain the inventory data.

The inventory directory is separate from the Oracle home directory.

When you specify the Oracle inventory directory path, you must also 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.

If you have a previous version of Grid Control installed on the computer, the installer uses the existing inventory directory. Ensure that you have write permissions on that directory. The best way of ensuring this is to run the installer as the same operating system user who installed the existing release of Grid Control.

### 4.8.1 Installing Additional Languages

By default, the installer installs Grid Control with text in English and in the operating system language. If you need additional languages, select the required languages in the Select Languages screen of the installer.

When you select additional languages to install, the installer also installs fonts required to display the languages.

For some components, languages are installed only if you select them during installation. In this case, if you access the application in a language that is not available, it reverts to the server locale language.

For other components, available languages are installed regardless of what you select during installation. In this case, however, fonts are installed only for the languages that are explicitly selected. When you access the application, it uses text in your language because the language was installed. However, if you do not have the appropriate fonts to render the text, the text appears as square boxes. This usually applies to the Chinese, Japanese, and Korean languages.

## 4.9 Knowing About the Ports Used for Installation

### Default Port for Enterprise Manager Grid Control

The default port for Grid Control is 4889. This is the unsecured port, that is HTTP port. If 4889 is not available, then the first available free port from the range 4889 to 4897 is selected. The default secured port, that is HTTPS port, is 1159. If 1159 is not available, then the first available free port from the range 4898 to 4908 is selected.

### Default Port for Management Agent

The default 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.

### Custom Ports

If you want to use custom ports instead of default ports, then update the `staticports.ini` file with suitable custom port numbers for the component names. The `staticports.ini` file is available in the installation DVD-ROM at the following location:

```
<DVD>/response/
```

While assigning custom pots, consider the following:

- Port numbers cannot be greater than 65536.
- If you use a port number less than 1024 for a component, you must run the component as the `root` user.
- If you use a port number less than 1024 for a component, the installer cannot start up the component at the end of installation. You may need to configure the component first before you can start it up. See the appropriate component documentation for details.

You do not have to specify port numbers for all components in the `staticports.ini` file. If a component is not listed in the file, the installer uses the default port number for that component.

To invoke `runInstaller` (`setup.exe` on Microsoft Windows) with the `staticports.ini` option, run the following command:

```
./<runInstaller or setup.exe> -staticPortsIniFile <location>/staticport.ini
```

Once the installation is complete, you can check the `ORACLE_HOME/install/portlist.ini` file to view the assigned ports.

The installer verifies that the ports specified in the file are available (free) by reading the `Properties` file in all the Oracle homes. If the installer detects that a specified port is not available, it displays a message.

A port is considered to be free only if:

- There are no Oracle products assigned to that port.
- There are no processes running on that port.

The installer does not assign a port that is not available. To fix this:

1. Edit the `staticports.ini` file to specify a different port.
2. Click **Retry.** The installer rereads the`staticports.ini` file and verifies the entries in the file again.

---

**Note:** The staticports.ini file uses the same format as the ORACLE_HOME/install/portlist.ini file, which is created after an Oracle Application Server installation. If you have installed Oracle Application Server and you want to use the same port numbers in another installation, you can use the portlist.ini file from the first installation as the staticports.ini file for subsequent installations.

---

For view the format of staticports.ini file, see Appendix F.1, "Formats for the Staticports.ini File".

In some cases, despite providing custom ports in the staticports.ini file, the installer may resort to default ports. For information about the circumstances under which the installer may use default ports instead of custom ports, see Appendix F.2, "Causes for the Installer to Use Default Ports".

## 4.10 Understanding Passwords and Restrictions

The installer prompts you to specify the passwords that are used to secure your entire Grid Control environment. This includes the OMS and the Management Repository passwords. One of the database passwords that you specify is the password required to access the application server (ias_admin). The ias_admin user is the administrative user for Oracle Application Server instances. To manage Oracle Application Server instances using Application Server Control, you must log in as ias_admin. Ensure the passwords you specify have all the required permissions.

### Password Restrictions

The following restrictions apply to passwords:

- Passwords must be between 5 and 30 characters long.
- Passwords cannot be the same as the user name.
- Passwords must include only lowercase or uppercase alphanumeric characters.

---

**Note:** The SYSMAN password can include underscore (_), hyphen (-), dollar ($), and hash (#) along with alphanumeric characters. Alphabetic characters can be lowercase or uppercase.

---

- Passwords have at least one letter, one integer, and one special character (underscore).
- Passwords cannot be Oracle reserved words. See Appendix I, "Oracle Reserved Words" for a complete list of reserved words.

Oracle recommends that the passwords that you specify are not simple or obvious words, such as welcome, account, database, or user.

After the installation,

If you want to change this default password, you can do so after the Grid Control installation by going to the Oracle home directory of the OMS and running the following command:

```
ORACLE_HOME/bin/emctl set password <old_default_password> <new_
password>
```

**Note:** If you do not remember the old ias_admin password, then follow the instructions outlined in Document ID 280587.1 that is available on My Oracle Support (formerly Metalink).

## 4.11 Understanding Permissions Required for Executing UTL_FILE

The management audit log package of the scheme owner uses the UTIL package. For this package to function properly, the Grid Control schema user (for example, sysman) must have permissions to execute this package.

To grant permissions, run this command (where sysman is the schema user):

```
grant execute on utl_file to sysman;
```

## 4.12 Understanding Limitations with DHCP-Enabled Machines

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

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

`http://metalink.oracle.com/`

## 4.13 Logging In As Root During Installation (UNIX Only)?

At least once during installation, the installer prompts you to log in as the `root` user and run a script. You must log in as `root` because the script edits files in the `/etc` directory.

### 4.13.1 Running root.sh During Installation (UNIX Only)

The installer prompts you to run the `root.sh` script in a separate window. This script creates files in the local bin directory (`/usr/local/bin`, by default).

On IBM AIX and HP UX platforms, the script the files in the `/var/opt` directory.

## 4.14 Understanding Enterprise Manager Grid Control Configuration Plug-in (EMCP)

When you perform an Grid Control installation, this installation does not include the Enterprise Manager Configuration Plug-in (EMCP) in the database Oracle home. EMCP is part of the Management Repository Oracle home only when you perform a standalone database installation.

## 4.15 Understanding Prerequisite Checks

The following are the prerequisite checks that the installer runs for each installation type.

*Table 4–2 Prerequisites Checks for Each Installation Type*

| Installation Type | Component Name | Checks |
|---|---|---|
| Installing Enterprise Manager Using New Database | `oracle.sysman.top.em_seed` | 1. Required Packages on the machine<br>2. Certified Versions (that is, whether the Oracle software is certified on the current Operating System)<br>3. Whether the required GLIBC is installed on the machine (UNIX only)<br>4. Whether the machine has sufficient physical memory<br>5. Kernel parameters<br>6. Oracle home compatibility[1]<br>7. Oracle home space check<br>8. Checking host name<br>9. Whether Oracle home is empty |
| Installing Enterprise Manager Using Existing Database | `oracle.sysman.top.oms` | 1. Required Packages on the machine<br>2. Certified Versions (that is, if the Oracle software is certified on the current operating system)<br>3. If the required GLIBC is installed on the machine (UNIX only)<br>4. If the machine has sufficient physical memory<br>5. Oracle home compatibility<br>6. If Oracle home is empty<br>7. Checking host name<br>8. Oracle home space check |
| Installing Additional Management Service | `oracle.sysman.top.oms` | 1. Required Packages on the machine<br>2. Certified Versions (that is, if the Oracle software is certified on the current operating system)<br>3. If the required GLIBC is installed on the machine (UNIX only)<br>4. If the machine has sufficient physical memory<br>5. Oracle home compatibility<br>6. If Oracle home is empty<br>7. Oracle home space check<br>8. Checking host name[2] |
| Installing Additional Management Agent | `oracle.top.agent` | 1. Required Packages on the machine<br>2. Certified Versions (that is, if the Oracle software is certified on the current operating system)<br>3. If the required GLIBC is installed on the machine (UNIX only)<br>4. The Targets monitored by the Management Agent<br>Note that the Agent monitors only those AS targets (on that host) that were installed by the same user as the one who installed Grid Control.<br>5. Oracle home compatibility<br>6. Checking host name<br>7. Oracle home space check |

[1] Disallowed component = oracle.rsf.oracore_rsf.

[2] The name of the host on which the installation is being performed should neither be localhost.localdomain nor an IP address. It must be a valid host name. At the time of invoking the installer, you can pass ORACLE_HOSTNAME=<host_name> -local as an argument.

## 4.16 Running the Prerequisite Check in Standalone Mode

You can run the prerequisite check in standalone mode prior to starting the runInstaller. This helps you identify and resolve issues that might otherwise cause the installation to fail.

Table 4–3 lists the prerequisite check that is run for each installation type followed by the command that you must execute to run these checks:

*Table 4–3 Installation Type and the Corresponding Prerequisite Check*

| Installation Type | Component Name | -entryPoint Value |
|---|---|---|
| Installing Enterprise Manager Using a New Database | oracle.sysman.top.em_seed | oracle.sysman.top.em_seed_Core |
| Installing Enterprise Manager Using an Existing Database | oracle.sysman.top.oms | oracle.sysman.top.oms_Core |
| Installing an Additional Management Service | oracle.sysman.top.oms | oracle.sysman.top.oms_Core |
| Installing an Additional Management Agent | oracle.sysman.top.agent | oracle.sysman.top.agent_Complete |

To run the prerequisite checker in standalone mode, execute the following command:

```
<DVD>/install/runInstaller -prereqchecker PREREQ_CONFIG_
LOCATION=<DVD>/rdbms/Disk1/stage/prereq -entryPoint <entryPoint Value>
-prereqLogLoc <log location>  -silent  -waitForCompletion
```

For the prerequisite checker to run successfully, ensure that the file path specified in --prereqLogLoc exists on the host.

**Note:** On Microsoft Windows, replace /runInstaller with **setup.exe** and execute the command.

# Part II

# Installing Enterprise Manager Grid Control

This part provides information and step-by-step instructions to install Enterprise Manager Grid Control and Management Agent.

This part contains the following chapters:

# 5 Overview of the Installation Process

This chapter provides an overview of the process involved in installing the *full release* of Enterprise Manager Grid Control and patching it with the latest *patch set release*.

A *full release* refers to the first, complete Enterprise Manager 10g Grid Control Release 2 or higher software that was released for a particular platform. For example, Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) was the full release for Linux platform. For more information about full releases and the platforms for which they have been released, see the Preface chapter of this guide.

A *patch set release* refers to the most recent patch set released with bug fixes, enhancements, and new value-added features. For example, Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) is the latest patch set release.

Oracle always recommends you to use the latest patch set release to take full advantage of the enhancements made in the product. For example, if you want to install the latest patch set release, that is, Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) patch set, then you must first install the full release of Enterprise Manager 10g Grid Control Release 2 or higher software that was released for your platform, and then apply the 10.2.0.5 patch set on it. This chapter helps you understand the overall process involved in installing the full release and then patching it with the latest patch set.

You can reach the latest patch set release of Enterprise Manager Grid Control using one of the following methods:

- You can **install and configure** Enterprise Manager Grid Control, and **then patch** it with the latest patch set.
- You can **install only the software binaries** of Enterprise Manager Grid Control, that is, without configuring it, and **then directly patch** it with the latest patch set. This is called the *Installing Software-Only and Configuring Later* installation method. For more information about this installation method and the circumstances under which you must use this method, see the overview provided in Section 8.6, "Installing 'Software-Only' and Configuring Later".

This chapter explains the process involved for these methods. In particular, this chapter covers the following:

- Installing and Configuring the Full Release, and then Patching
- Installing Only the Software Binaries of Full Release, and then Patching

## 5.1 Installing and Configuring the Full Release, and then Patching

The following is the process involved in **installing and configuring** the full release of Enterprise Manager Grid Control, and **then patching** it to the latest patch set release.

*Table 5–1 Process Involved in Installing and Configuring the Full Release, and then Patching*

| Steps | Description | Related Links |
|---|---|---|
| **Deciding on the Installation Type** | Understand the different installation types available for Enterprise Manager Grid Control, and decide on the installation type you want to use to meet your requirements.<br>This is critical because the components installed vary from one installation type to another, and the prerequisites to be met also are different for each installation type. | For high-level information about the installation types, see Section 8.1, "Understanding the Installation Types".<br>For more detailed information, see the *Overview* sections:<br>▪ For Enterprise Manager Grid Control with a New database, see Section 8.3.1, "Overview".<br>▪ For Enterprise Manager Grid Control with an existing database, see Section 8.4.1, "Overview".<br>▪ For additional OMS, see Section 8.5.1, "Overview". |
| **Meeting the Prerequisites** | Meet all the prerequisites before starting the installation. | ▪ For Enterprise Manager Grid Control with a New database, see Section 8.3.3, "Prerequisites".<br>▪ For Enterprise Manager Grid Control with an existing database, see Section 8.4.3, "Prerequisites".<br>▪ For additional OMS, see Section 8.5.1, "Overview". |
| **Installing the Base Release of Enterprise Manager Grid Control** | Install the base release of Enterprise Manager Grid Control by following the installation instructions outlined in this guide. | For GUI-based installation:<br>▪ For Enterprise Manager Grid Control with a New database, see Section 8.3.4, "Installing Procedure".<br>▪ For Enterprise Manager Grid Control with an existing database, see Section 8.4.4, "Installation Procedure".<br>▪ For additional OMS, see Section 8.5.5, "Installation Procedure".<br>For silent installation:<br>▪ For Enterprise Manager Grid Control with a New database, see Section 9.4, "Using Silent Mode to Install Enterprise Manager Grid Control Using a New Database".<br>▪ For Enterprise Manager Grid Control with an existing database, see Section 9.5, "Using Silent Mode to Install Enterprise Manager Grid Control Using an Existing Database".<br>▪ For additional OMS, see Section 9.6, "Using Silent Mode to Install Additional Management Service". |
| **Troubleshooting Installation-Related Known Issues** | While installing the base release, if you encounter any isssues, resolve them by following the workarounds documented in this guide. | Appendix A, "Troubleshooting Enterprise Manager" |

*Table 5–1 (Cont.) Process Involved in Installing and Configuring the Full Release, and then Patching*

| Steps | Description | Related Links |
|---|---|---|
| **Patching the Base Release to the Latest Release** | Apply the latest patch set on the base release of Enterprise Manager Grid Control so that you have the most recent release.<br>To do so, download the latest patch set from Oracle Technology Network (OTN) Web site and follow the installation instructions outlined in the Release Notes that is provided with the downloaded patch set. | You can download the patch set from:<br>`http://www.oracle.com/technology/software/products/oem/index.html` |
| **Troubleshooting Patching-Related Known Issues** | While patching the base release, if you encounter any isssues, resolve them by following the workarounds documented in the Release Notes. | |

## 5.2 Installing Only the Software Binaries of Full Release, and then Patching

The following is the process involved in **installing only the software binaries** of the full release of Enterprise Manager Grid Control (and not configuring it), and **then patching** it to the latest patch set release.

*Table 5–2 Process Involved in Installing Only the Software Binaries of Full Release, and then Patching*

| Steps | Description | Related Links |
|---|---|---|
| **Deciding on the Installation Type** | Understand the different installation types available for Enterprise Manager Grid Control, and decide on the installation type you want to use to meet your requirements.<br>This is critical because the components installed vary from one installation type to another, and the prerequisites to be met also are different for each installation type. | For high-level information about the installation types, see Section 8.1, "Understanding the Installation Types".<br>For more detailed information, see the *Overview* sections:<br>■ For Enterprise Manager Grid Control with a New database, see Section 8.3.1, "Overview".<br>■ For Enterprise Manager Grid Control with an existing database, see Section 8.4.1, "Overview".<br>■ For additional OMS, see Section 8.5.1, "Overview". |
| **Meeting the Prerequisites** | Meet all the prerequisites before starting the installation. | ■ For Enterprise Manager Grid Control with a New database, see Section 8.3.3, "Prerequisites".<br>■ For Enterprise Manager Grid Control with an existing database, see Section 8.4.3, "Prerequisites".<br>■ For additional OMS, see Section 8.5.4, "Prerequisites". |

*Table 5–2 (Cont.) Process Involved in Installing Only the Software Binaries of Full Release, and then Patching*

| Steps | Description | Related Links |
|---|---|---|
| **Installing Only the Software Binaries and Patching it Directly** | Install only the software binaries of the full release of Enterprise Manager Grid Control, and patch it directly by following the installation instructions outlined in this guide. | For GUI-based installation:<br>■ For Enterprise Manager Grid Control with an existing database, see Section 8.6.3.1, "Installing Enterprise Manager Grid Control Using an Existing Database".<br>■ For additional OMS, see Section 8.6.3.1, "Installing Enterprise Manager Grid Control Using an Existing Database".<br>For Silent installation:<br>■ For Enterprise Manager Grid Control with a New database, see Section 8.6.2.1, "Installing Enterprise Manager Grid Control Using a New Database".<br>■ For Enterprise Manager Grid Control with an existing database, see Section 8.6.2.2, "Installing Enterprise Manager Grid Control Using an Existing Database".<br>■ For additional OMS, see Section 8.6.2.3, "Installing Additional Management Service". |
| **Troubleshooting Known Issues** | If you encounter any isssues, resolve them by following the workarounds documented in this guide and the Release Notes. | Appendix A, "Troubleshooting Enterprise Manager"<br>Also see the Known Issues section of the Release Notes. |

# 6 Accessing the Installation Software

Enterprise Manager Grid Control (Grid Control) software is available on a DVD-ROM, or you can download it from the Oracle Technology Network (OTN) Web site. Oracle Management Agent (Management Agent) is one of the core components of Grid Control and therefore, it can be installed using the Grid Control installer. Alternatively, you can download the Management Agent software separately from My Oracle Support (formerly Metalink) using the Grid Control console.

This chapter describes the following:

- Accessing the Software from a Remote DVD Drive (UNIX Only)
- Accessing the Software on Remote Hosts Using Remote Access Software
- Downloading Management Agent Software Using Grid Control Console
- Using Oracle Universal Installer

## 6.1 Accessing the Software from a Remote DVD Drive (UNIX Only)

If the computer where you want to install Grid Control does not have a DVD drive, you can access the software and perform the installation from a remote DVD drive by mounting (sharing) that DVD drive.

### 6.1.1 Setting the Mount Point for the DVD-ROM on Linux

On most Linux systems, the disk mounts automatically when you insert it into the disk drive. To mount the disk, complete the following steps:

1. Insert the Oracle Enterprise Manager DVD into the disk drive.
2. To verify if the disk is automatically mounted, enter 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, enter 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>
```

### 6.1.2 Setting the Mount Point for the DVD-ROM on AIX

On most AIX systems, the disk mounts automatically when you insert it into the disk drive. To manually mount the disk, complete the following steps:

1. Switch the user to `root` user by executing the following command:

   ```
   $ su -root
   ```

2. If required, enter a command similar to the following to eject the currently mounted disk and to remove it from the drive:

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

3. Insert the disk into the drive.
4. Enter a command similar to the following:

   ```
   # /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.

5. If Oracle Universal Installer displays the Disk Location dialog box, enter the disk mount point directory path. For example: `/SD_DVD`

## 6.2 Accessing the Software on Remote Hosts Using Remote Access Software

Consider a scenario where the remote computer has the hard drive and will run Grid Control, but you do not have physical access to the computer. You can perform the installation on the remote computer, provided it is running remote access software such as VNC or Symantec pcAnywhere. You also need the remote access software running on your local computer.

You can install Grid Control on the remote computer in one of two ways:

- If you have copied the contents of the Oracle Enterprise Manager Grid Control DVD to a hard drive, you can install from the hard drive.
- You can insert the DVD into a drive on your local computer, and install from the DVD.

### 6.2.1 Installing from a Hard Drive

If you have copied the contents of the Oracle Enterprise Manger DVD to a hard drive, you can install from the hard drive.

The steps that you need to complete are the following:

1. Ensure the remote access software is installed and running on the remote and local computers.
2. Share the hard drive that contains the Oracle Enterprise Manager DVD.
3. Map a drive letter on the remote computer to the shared hard drive. You would use the remote access software to do this on the remote computer.
4. Run Oracle Universal Installer on the remote computer using the remote access software. You can access Oracle Universal Installer from the shared hard drive.

For more information on running the installer, see Section 6.4.2, "Starting the Installer" for more information.

### 6.2.2 Installing from a Remote DVD Drive

You can insert the DVD into a drive on your local computer, and install from the DVD.

The steps that you need to complete are the following:

1. Ensure the remote access software is installed and running on the remote and local computers.
2. Share the DVD content on the local computer.

   Map a drive letter on the remote computer to the shared hard drive. You would use the remote access software to do this on the remote computer.
3. Run Oracle Universal Installer on the remote computer using the remote access software. You access Oracle Universal Installer from the shared DVD drive.

For more information on running the installer, see Section 6.4.2, "Starting the Installer" for more information.

## 6.3 Downloading Management Agent Software Using Grid Control Console

The Management Agent software is also available on My Oracle Support (formerly Metalink) Web site and can be downloaded using the Download Agent Software application in the Grid Control console. The software is available in the form of a ZIP file. You can choose to download it in the default location, that is, the OMS home, or in a custom location.

> **Note:** The Download Agent Software application is available only in Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).
>
> This installation guide is mainly for the base release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) Use this guide to install the base release and then patch it with 10.2.0.5 Grid Control patch set to migrate to Enterprise Manager 10g Grid Control Release 5 (10.2.0.5). The 10.2.0.5 Grid Control patch is available on My Oracle Support (formerly Metalink).

Before downloading the Management Agent software, meet the following prerequisites:

- Set the My Oracle Support (formerly Metalink) credentials in Grid Control. To do so, click **Setup**. In the Overview of Setup page, from the menu bar on the left, click **Patching Setup**. For more information, click **Help** on that page.
- Set the proxy settings if you have a proxy server in your environment. To do so, click **Setup**. In the Overview of Setup page, from the menu bar on the left, click **Patching Setup** and then click **Proxy & Connection Settings**. For more information, click **Help** on that page.
- Ensure that the download location, that is, the directory where you want to download the software, is writable.

To download the Management Agent software using the Grid Control console, do the following:

1. In Grid Control, click **Deployments**. Grid Control displays the Deployments page.
2. On the Deployments page, from the Agent Installation section, click **Download Agent Software**. Grid Control displays the Download Agent Software page.
3. On the Download Agent Software page, in the Available Agent Software section, select the Management Agent software you want to download:

   The following describes the elements of this table:

***Table 6–1 Element Description - Available Agent Software - Downloading Management Agent***

| UI Element on the Screen | Input Required |
|---|---|
| Platform | Platform for which the Management Agent is supported.<br>While the first part of the platform name refers to the name of the supported operating system, the second part in parenthesis refers to the type of operating system, that is, 32-bit or 64-bit.<br>A 32-bit software can be installed only on a 32-bit operating system that is running on a 32-bit hardware. Similarly, a 64-bit 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 download the right software for the right platform.<br>To determine the type of your operating system, refer to document ID 421453.1 available on My Oracle Support (formerly Metalink). You can access My Oracle Support at `http://metalink.oracle.com/`. |
| Version | Version can be one of the following:<br>■ 10.2.0.4, which is Oracle Management Agent 10g Release 4 (10.2.0.4)<br>■ 10.2.0.3, which is Oracle Management Agent 10g Release 3 (10.2.0.3)<br>■ 10.2.0.2, which is Oracle Management Agent 10g Release 2 (10.2.0.2)<br>■ 10.2.0.1, which is Oracle Management Agent 10g Release 2 (10.2.0.1) |
| Available On This OMS | Indicates whether the Management Agent software is already available in the default location of the OMS from where Grid Control is being accessed. In case of multi-OMS environment, the OMS referred here is the Management Server shown in the OMS field on top of the page.<br>**Note:** This column indicates whether the software is already available only in the default location of the OMS. It does not indicate the presence of software downloaded to a non-default location or a shared location.<br>The values can be one of the following:<br>■ True, which means the software is already available on Oracle Management Service (OMS). You do not have to download it again.<br>■ False, which means the software is not available on OMS. You may want to download it. |

*Table 6–1 (Cont.) Element Description - Available Agent Software - Downloading Management Agent*

| UI Element on the Screen | Input Required |
|---|---|
| Size (MB) | Size (in megabytes) of the software ZIP file available for download.<br>Note that Grid Control actually downloads the ZIP file to the staging location and extracts the contents in the same location. The total size of all the extracted files may be more than the size mentioned here. Therefore, the space required in the staging location is at least double the size of the what is mentioned here. |

4. In the Staging Location section, select the location where you want to stage the Management Agent software.

   - Select **Default Location** if you want to download the Management Agent software to the default location, that is, to the Oracle home directory of the OMS (the one shown on top of the screen against the field **Oracle Management Service**). The default download location on the OMS is `<OMS_HOME>/sysman/agent_download/<version>`.

     In case of a single OMS environment, Grid Control downloads the software ZIP file to the default location, extracts the files to the same location, and then deletes the ZIP file, leaving only the extracted files. In case of a multi-OMS environment, Grid Control downloads the software ZIP file and extracts the files to the first OMS home (the OMS shown in the **OMS** field on top of the screen), then copies the ZIP file to the next OMS home and extracts the files there as well. Once all OMS homes have the software, Grid Control deletes the ZIP file from each of the OMS homes, leaving only the extracted files.

     For a multi-OMS environment, you must provide the credentials to access the Oracle home directories of the OMSes in the environment.

     – Select **Use Oracle Home Preferred Credentials** if you want to use preferred credentials stored in the Management Repository.

     – Select **Override Oracle Home Preferred Credentials** if you want to override them with new set of credentials. If you select this option, you can specify either the same credentials or different credentials to access the OMSes in your environment, depending on how they are configured.

   - Select **Custom Location** and specify a location of your choice if you want to download the Management Agent software to a custom location. The custom location must be accessible from all the remote hosts and OMSes, and must have 'write' permission.

     **Note:** If you select this option, then ensure that you select Another Location in the Agent Deployment application while installing the Management Agent.

     This is an ideal choice under the following conditions:

     – When you have a shared, mounted location that is visible on all OMSes. The shared location can be anywhere in the enterprise configuration.

     – When you do not want Grid Control to download the software and extract the files on all the OMSes automatically. This way, you can download the software to one particular location and manually copy the files to other OMSes, whenever required.

If the custom location already exists (that is, if you have manually created it), then Grid Control simply downloads the software ZIP file to that location. However, if the location does not exist, then Grid Control automatically creates the directories and then downloads the software there. If you already have a copy of the software in the default location, then Grid Control overwrites that with the version selected for download.

Grid Control downloads the software ZIP file to the custom location, extracts the files to the same location, and deletes the ZIP file. If you have multiple OMSes, you have to manually copy the extracted files to other OMSes.

5. Click **Download** to download the Management Agent software.

## 6.4 Using Oracle Universal Installer

The Enterprise Manager installation uses Oracle Universal Installer, a Java-based graphical user interface application that enables you to install Oracle components from a DVD, multiple DVDs, or the Web.

**See Also:** For information on using Oracle Universal Installer to install Oracle software, refer to the *Oracle Universal Installer and OPatch User's Guide*.

### 6.4.1 Specifying a Temporary Directory

When you start Oracle Universal Installer (OUI), it automatically copies some executable files and link files into the default `/tmp` directory (`C:\Documents and Settings\<user ID>\Local Settings\Temp` on Microsoft Windows) on the machine. If the machine is set to run `cron` jobs (along with many other processes that may be running) periodically, these jobs attempt to clean up the default temporary directory, thereby deleting some files and causing OUI to fail.

If there are any `cron` jobs or processes that are automatically run on the machines to clean up the temporary directories, ensure you set the `TMP` or `TEMP` environment variable to a different location (than the default location) that is secure on the hard drive (meaning a location on which the cleanup jobs are not run). Also ensure that you have write permissions on this alternative `TEMP` directory. This must be done before you execute `runInstaller` (`setup.exe` on Microsoft Windows).

**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.

### 6.4.2 Starting the Installer

Start Oracle Universal Installer by running the `runInstaller` (or `setup.exe` on Microsoft Windows) from the top-level directory of the DVD.

Alternatively, you can change the directory to the `Parent Directory` (or the root directory) where you will install the Oracle home, then specify the full path to `/runInstaller` (`setup.exe` on Microsoft Windows).

To specify a response file for a silent installation, use the following command:

```
$ ./<runInstaller or setup.exe> -responseFile <responsefile_location> <optional_
```

```
parameters> -silent
```

> **See Also:** Refer to the Creating and Customizing Response Files chapter of the *Oracle Universal Installer and OPatch User's Guide* for more information on silent installations.

When you invoke the installer, the installation runs prerequisite checks on the following:

- Operating System Version
- Operating System Packages
- Operating System Patches
- User Credentials
- TEMP and SWAP space
- DISPLAY Colors
- Additional Patches
- Kernel version
- Oracle home is empty
- Oracle home space
- Physical memory

The list of prerequisite checks that must be executed can be viewed in the initialization parameters file located in the following directory of the product-specific installation:

```
<DVD>/install/oraparam.ini
```

If a prerequisite check fails, you are prompted to continue, or stop the installation process. You may install the missing software at this point, or discontinue the installation. Note, however, that you may have newer patches that supersede the required patches.

Once you continue, follow the installation instructions on the screen. At any time while installing Enterprise Manager, you can click **Help** for information about the pages.

# 7

# Using Oracle Universal Installer

Oracle Universal Installer (OUI) is the installer used for installing Enterprise Manager Grid Control (Grid Control). OUI is a Java-based graphical user interface application that enables you to install Oracle components from a DVD, multiple DVDs, or the Web.

This chapter describes how you can use OUI. In particular, it covers the following;

- Specifying a Temporary Directory
- Starting the Installer

> **See Also:** For information on using Oracle Universal Installer to install Oracle software, refer to the *Oracle Universal Installer and OPatch User's Guide*.

## 7.1 Specifying a Temporary Directory

When you start OUI, it automatically copies some executable files and link files into the default `/tmp` directory (`C:\Documents and Settings\<user ID>\Local Settings\Temp` on Microsoft Windows) on the machine. If the machine is set to run `cron` jobs (along with many other processes that may be running) periodically, these jobs attempt to clean up the default temporary directory, thereby deleting some files and causing OUI to fail.

If there are any `cron` jobs or processes that are automatically run on the machines to clean up the temporary directories, ensure you set the `TMP` or `TEMP` environment variable to a different location (than the default location) that is secure on the hard drive (meaning a location on which the cleanup jobs are not run). Also ensure that you have write permissions on this alternative `TEMP` directory. This must be done before you execute `runInstaller` (`setup.exe` on Microsoft Windows).

> **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.

## 7.2 Starting the Installer

Start Oracle Universal Installer by running the `runInstaller` (or `setup.exe` on Microsoft Windows) from the top-level directory of the DVD.

Alternatively, you can change the directory to the `Parent Directory` (or the root directory) where you will install the Oracle home, then specify the full path to `/runInstaller` (`setup.exe` on Microsoft Windows).

To specify a response file for a silent installation, use the following command:

```
$ ./<runInstaller or setup.exe> -responseFile <responsefile_location> <optional_
parameters> -silent
```

> **See Also:** Refer to the Creating and Customizing Response Files chapter of the *Oracle Universal Installer and OPatch User's Guide* for more information on silent installations.

When you invoke the installer, the installation runs prerequisite checks on the following:

- Operating System Version
- Operating System Packages
- Operating System Patches
- User Credentials
- TEMP and SWAP space
- DISPLAY Colors
- Additional Patches
- Kernel version
- Oracle home is empty
- Oracle home space
- Physical memory

The list of prerequisite checks that must be executed can be viewed in the initialization parameters file located in the following directory of the product-specific installation:

```
<DVD>/install/oraparam.ini
```

If a prerequisite check fails, you are prompted to continue, or stop the installation process. You may install the missing software at this point, or discontinue the installation. Note, however, that you may have newer patches that supersede the required patches.

Once you continue, follow the installation instructions on the screen. At any time while installing Enterprise Manager, you can click **Help** for information about the pages.

8

# Installing Enterprise Manager Grid Control

This chapter describes the different installation options and provides instructions to install Enterprise Manager Grid Control (Grid Control). In particular, this chapter covers the following:

- Understanding the Installation Types
- Accessing the Installer
- Installing Enterprise Manager Grid Control Using a New Database
- Installing Enterprise Manager Grid Control Using an Existing Database
- Installing an Additional Management Service
- Installing 'Software-Only' and Configuring Later

## 8.1 Understanding the Installation Types

The following describes the different installation options offered by Grid Control. The hard disk space represents the *footprint* that the components of the installation consume, and the physical memory prerequisites refer to the initial RAM required for installation, and not the operating memory.

***Table 8–1 Enterprise Manager Grid Control Installation Options***

| Installation Option | Description | Hard Disk Space (Oracle Homes) | Physical Memory |
|---|---|---|---|
| Enterprise Manager 10*g* Grid Control Using a New Database | Installs Grid Control on the host, and creates a Management Repository in a new Oracle Database 10g Release 1 (10.1.0.4) Enterprise Edition.<br>*Note:* Grid Control consists of Oracle Management Service (OMS), Oracle Management Agent (Management Agent), Oracle Database where Management Repository is created, and OracleAS J2EE and Web Cache, against which is the middle-tier where OMS is deployed.<br>Also note that after installing Grid Control with a new database, that is Oracle Database 10g Release 1 (10.1.0.4), even if you upgrade to any higher release using the patch sets, the database installed is not upgraded. Therefore, even if you upgrade Grid Control, the database release remains 10.1.0.4, unless you upgrade it separately out of Grid Control installation. | ■ 4.5 GB (Linux/Solaris )<br>■ 9GB (HP-UX)<br>■ 4.5 GB (Win)<br>■ 9 GB (AIX) | ■ 2 GB (Linux/Sola -ris)<br>■ 2 Gb (HP-UX)<br>■ 2 GB (Win)<br>■ 2 GB (AIX) |

*Table 8–1 (Cont.) Enterprise Manager Grid Control Installation Options*

| Installation Option | Description | Hard Disk Space (Oracle Homes) | Physical Memory |
|---|---|---|---|
| Enterprise Manager 10*g* Grid Control Using an Existing Database | Installs Grid Control on the host, and creates the Management Repository on a qualified existing database, which may be local to the host or remote. For more information on supported repository releases, Section 3.3.1, "Oracle Management Repository Software Requirements".<br>*Note:* If the repository is on the same machine as the OMS, allow 1 GB more memory than recommended.<br>Oracle recommends installing Grid Control and Oracle Database on separate hosts. | ▪ 2.5 GB (Linux/Solaris )<br>▪ 5 GB (HP-UX)<br>▪ 2.5 GB (Win)<br>▪ 5 GB (AIX) | ▪ 2 GB (Linux/Sola -ris)<br>▪ 2 GB (HP-UX)<br>▪ 2 GB (Win)<br>▪ 2 GB (AIX) |
| Additional Management Service | Installs an additional OMS and a Management Agent. Allows you to map the additional OMS to an existing Management Repository, either local or remote. | ▪ 2 GB (all UNIX platforms)<br>▪ 2.5 Gb (Win) | ▪ 2 GB (all UNIX platforms)<br>▪ 2 GB (Win) |
| Additional Management Agent | Installs a Management Agent on the host. The OMS and Management Repository are not required on the same host as the Management Agent, but must exist within the enterprise.<br>The Management Agent may be installed on a cluster node. Oracle recommends that the target host on which you are installing the agent have a static IP address and not DHCP.<br>For instructions to install a Management Agent, see Section 10.4, "Installing Management Agent Using OUI". | ▪ 400 MB (all UNIX platforms)<br>▪ 500 MB (Win)<br>▪ 1.6 GB (AIX) | No minimum requirement |

**IMPORTANT:**

- When you perform a Grid Control installation, this installation does not include Enterprise Manager Configuration Plug-in (EMCP) in the database Oracle home. EMCP is part of the repository database Oracle home only when you perform a standalone database installation.
- No environment variable specific to Grid Control needs to be set prior to installation. The $ORACLE_HOME and $ORACLE_SID variables should not be set; Oracle directories should not appear in the PATH.
- If you install Grid Control on an NFS-mounted volume that has an Apache Server running, then ensure that the LockFile is stored outside the Oracle NFS-mounted home, on a separate local file system.
- You can have both, Enterprise Manager 10g Grid Control Release 1 as well as Enterprise Manager 10g Grid Control Release 2 on the same host.

## 8.2 Accessing the Installer

On Linux, start the Oracle Universal Installer (OUI) by running the following command:

```
<DVD>/runInstaller
```

On Microsoft Windows, start the OUI by running the following command:

```
<DVD>/setup.exe
```

Installation types are predefined component sets that determine the components to be installed. The Grid Control installation involves four top-level components, each representing an installation type. Select one of the installation types described in the following sections.

## 8.3 Installing Enterprise Manager Grid Control Using a New Database

This section introduces you to the first installation type offered by OUI, that is, *Enterprise Manager 10g Grid Control Using a New Database*. In particular, this section covers the following:

- Overview
- Before You Begin
- Prerequisites
- Installing Procedure

> **Note:** This section describes the steps required for installing the base release, that is, Enterprise Manager 10g Grid Control Release 2 (for example, 10.2.0.1 Linux or 10.2.0.2 Microsoft Windows).
>
> If you are installing Grid Control for the first time in your environment and if you want to have the latest release, then use the'Installing Software-Only and Configuring Later' option that is discussed in Section 8.6, "Installing 'Software-Only' and Configuring Later".

> **Note:** If you are installing Grid Control with a new database during the Daylight Savings Time (DST) period, then Oracle recommends you to use the 'Installing Software-Only and Configuring Later' option that is discussed in Section 8.6, "Installing 'Software-Only' and Configuring Later".

### 8.3.1 Overview

The first installation type, that is, *Enterprise Manager 10g Grid Control Using a New Database*, is the default option selected when you invoke the OUI installation wizard. It performs a complete installation and is best suited when you are installing for the first time in your environment or when you want all the components to be installed.

This installation type does the following:

- Installs Oracle Database 10*g* Release 1 (10.1.0.4) *(Contains an embedded 10g Management Repository*)
- Installs Oracle Management Service 10g Release 2 (Deployed in Oracle Application Server 10g Release 2 (10.1.2.0.2) that gets installed along with other core components)
- Installs Oracle Management Agent 10g Release 2

- Configures the Oracle Database, OMS, and Management Agent

The following describes the installation process and the software components installed for this installation type.

***Table 8–2 Installation Process for Installing Enterprise Manager Grid Control with a New Database***

| Sequence | Action | Component Installed/Configured | Description |
|---|---|---|---|
| 1 | Installation | Oracle Database 10*g* Release 1 (10.1.0.4) | In the specified installation directory, the installer creates a subdirectory for Oracle Database and places the software binaries in it. This Oracle Database contains an embedded Management Repository.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for the database is:<br>`/scratch/OracleHome/db10g` |
| 2 | Installation | Oracle Management Service 10g Release 2 | Technically, the installer installs an application server, that is, Oracle Application Server 10g Release 2 (10.1.2.0.2) where the OMS is deployed. In the specified installation directory, the installer creates a subdirectory for OMS and places the software binaries in it.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for OMS is:<br>`/scratch/OracleHome/oms10g` |
| 3 | Installation | Oracle Management Agent 10g Release 2 | In the specified installation directory, the installer creates a subdirectory for the Management Agent and places the software binaries in it. The subdirectory is agent11g.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for the Management Agent is:<br>`/scratch/OracleHome/agent10g` |
| 4 | Configuration | All | The installer runs the Configuration Assistant tools to configure all the installed components: |

## 8.3.2 Before You Begin

Before you begin, keep these points in mind:

- This installation type installs the components only on a single host, and only on that host from where the OUI installation wizard is involed, that is, where the runInstaller file (or setup.exe for Microsoft Windows platforms) is invoked.
- The default port for Oracle Database 10g Release 1 (10.1.0.4) provided with this installation type is 1521.
- The default port for Enterprise Manager Grid Control is 4889 and the default port for Management Agent is 3872. For more information about the default ports that are assigned and the possibility of using custom ports instead of default ports, see Section 4.9, "Knowing About the Ports Used for Installation".
- Oracle offers code fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for code 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 Grid Control installation, you must consider Enterprise Manager Grid Control's framework components as well as the targets monitored by Enterprise Manager Grid Control. Oracle recommends keeping your Grid Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license. For information about the certified combinations of Enterprise Manager Grid Control components and monitored targets, see *My Oracle Support* note.412431.1.

- If the Management Agent does not start up automatically when you restart the host, then do the following:

  **a.** Open the agentstup file from the Oracle home of the Management Agent:

  ```
  $ORACLE_HOME/install/unix/scripts/agentstup
  ```

  **b.** Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

  **c.** Run the root.sh script from the Oracle home of the Management Agent:

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

  **d.** Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

  **Note:** This is a one-time action to be taken. Step (a) to Step (c) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

### 8.3.3 Prerequisites

Before installing Enterprise Manager Grid Control with a new database, ensure that you meet the following prerequisites.

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

*Table 8–3 Prerequisites for Enterprise Manager 10g Grid Control Using a New Database*

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the necessary hardware and software requirements for Enterprise Manager Grid Control.<br>For information about hardware and software requirements, see Section 3.1, "Hardware Requirements" and Section 3.3, "Software Requirements", respectively. | |
| Operating System Requirements | Check if the operating system of the host is certified.<br>For information about the supported operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |

*Table 8–3 (Cont.) Prerequisites for Enterprise Manager 10g Grid Control Using a New*

| Requirement | Description | Yes/No |
|---|---|---|
| Package Requirements | Verify if the package requirements for each platform are met.<br>For information about packages to be installed for Management Agent, see Appendix D, "Platform-Specific Package and Kernel Requirements". | |
| Permission Requirements for Installation Directory | Check if the installation directory, that is, the Oracle home directory is writable. | |
| Host List and Credentials Requirements | Identify the host where you want to install Enterprise Manager Grid Control, and obtain the credentials of that host so that it can be accessed for installation. | |
| Host Name Requirement | The host name must be a valid host name. For example, *serverhost1.company.com* or *serverhost1*.<br>However, it cannot be an IP address. At the same time, it cannot be localhost.localdomain as strings used in the /etc/hosts file.<br>At the time of invoking the installer, you can pass `ORACLE_HOSTNAME=<host_name> -local` as an argument. | |
| Installing User Requirements | The following are the requirements:<br>▪ (UNIX only) The installation must NOT be run by the root user<br>▪ User must be a DBA user<br>▪ (Microsoft Windows only) User must be able to create process-level tokens<br>▪ (Microsoft Windows only) User must be able to log in as a batch job<br>▪ (Microsoft Windows only) User must be able to adjust memory quota for process<br>▪ (Microsoft Windows only) User must be part of the ORA-DBA group and have administrator permissions | |
| Installation Directory Requirements | If the specified *Installation Directory* already contains subdirectories that represent the components of Enterprise Manager Grid Control, then those subdirectories must be empty. If they are not, either delete them or keep them empty.<br>For example, if the specified *Installation Directory* already has <*install_dir/agent10g*>, <*install_dir/oms10g*>, <*install_dir/db10g*> subdirectories, then they must be empty. | |
| Oracle Inventory Location Requirements | Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `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. | |
| Targets Monitored | Remember that Enterprise Manager Grid Control will be able to monitor only those targets that are monitored by the Management Agent installed by the same user. | |

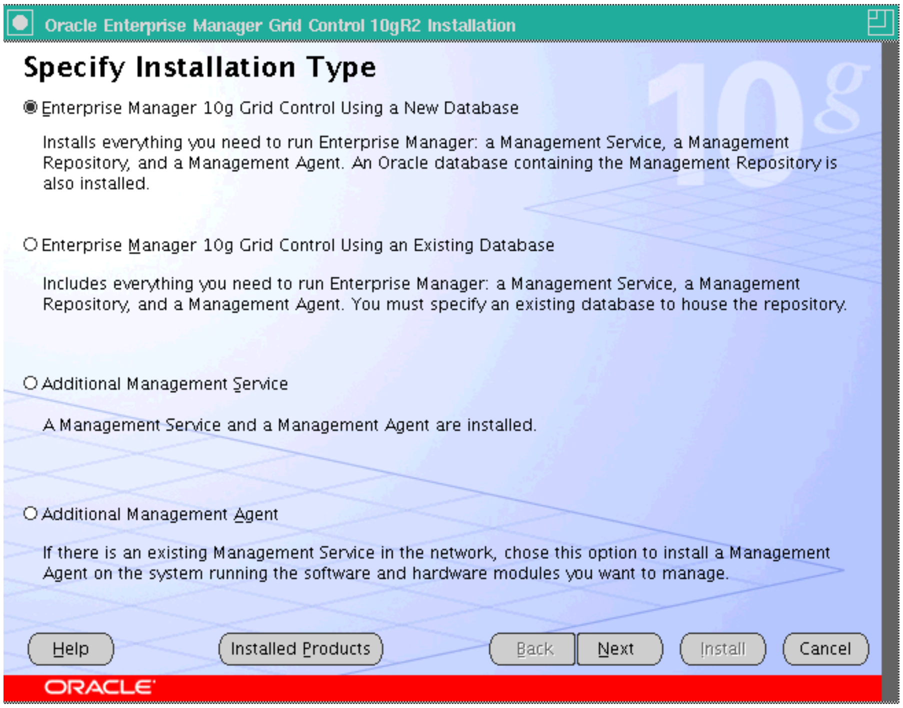
## 8.3.4 Installing Procedure

**WARNING:** The steps outlined in this section are for installing full, base releases of Enterprise Manager 10g Grid Control Release 2 or higher. For details about full, base releases and what these installation instructions can be use for, see Section 4.1, "Understanding What This Guide Helps You Install and Upgrade".

To install Enterprise Manager Grid Control using a new database, follow these steps:

1. Select the first option (**Enterprise Manager 10g Grid Control Using a New Database**). By default, this option is selected when you invoke the installer.

***Figure 8–1 Specify Installation Type***



Specify Installation Type

● Enterprise Manager 10g Grid Control Using a New Database

Installs everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. An Oracle database containing the Management Repository is also installed.

○ Enterprise Manager 10g Grid Control Using an Existing Database

Includes everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. You must specify an existing database to house the repository.

○ Additional Management Service

A Management Service and a Management Agent are installed.

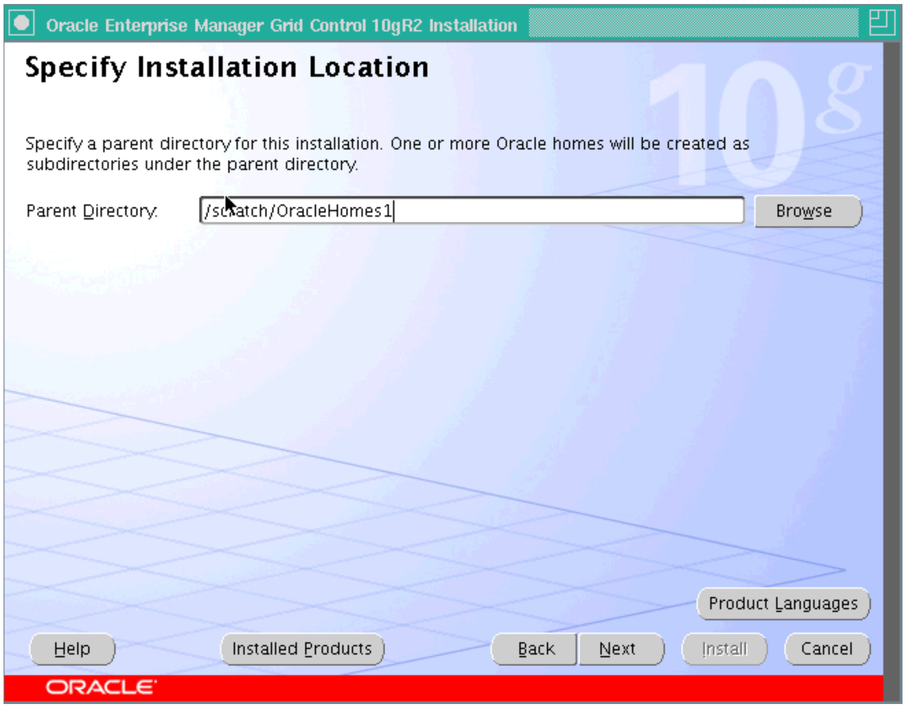
○ Additional Management Agent

If there is an existing Management Service in the network, chose this option to install a Management Agent on the system running the software and hardware modules you want to manage.

2. Click **Next.** In the Specify Installation Location screen that appears, specify a parent directory (base directory), for example, `/scratch/OracleHomes` (on Linux), for the new installation. All the Oracle homes created during this installation are created as subdirectories under this parent directory. For example: *db10g*, *oms10g*, and *agent10g*.

**Note:** Ensure you do not use symbolic links to specify the Oracle home path.

***Figure 8–2 Specify Installation Location***



Specify Installation Location

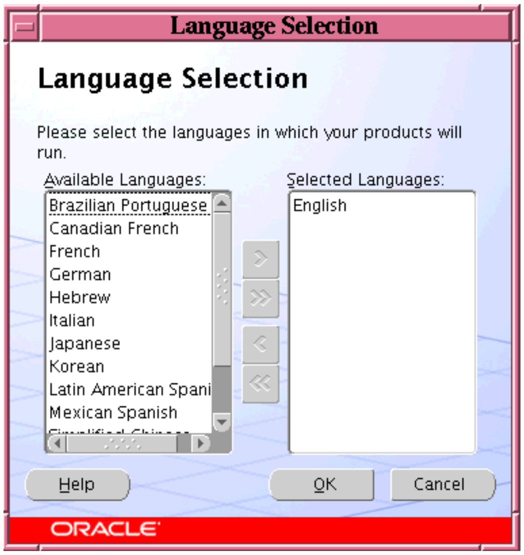
Specify a parent directory for this installation. One or more Oracle homes will be created as subdirectories under the parent directory.

Parent Directory: /scratch/OracleHomes1

The selected products are installed in the English language by default. If you want to install the product in a different language, click **Product Languages**.

The Language Selection screen appears.

***Figure 8–3 Language Selection***



Language Selection

Please select the languages in which your products will run.

Available Languages:

Selected Languages: English

Choose the languages that you want to use to run Grid Control.

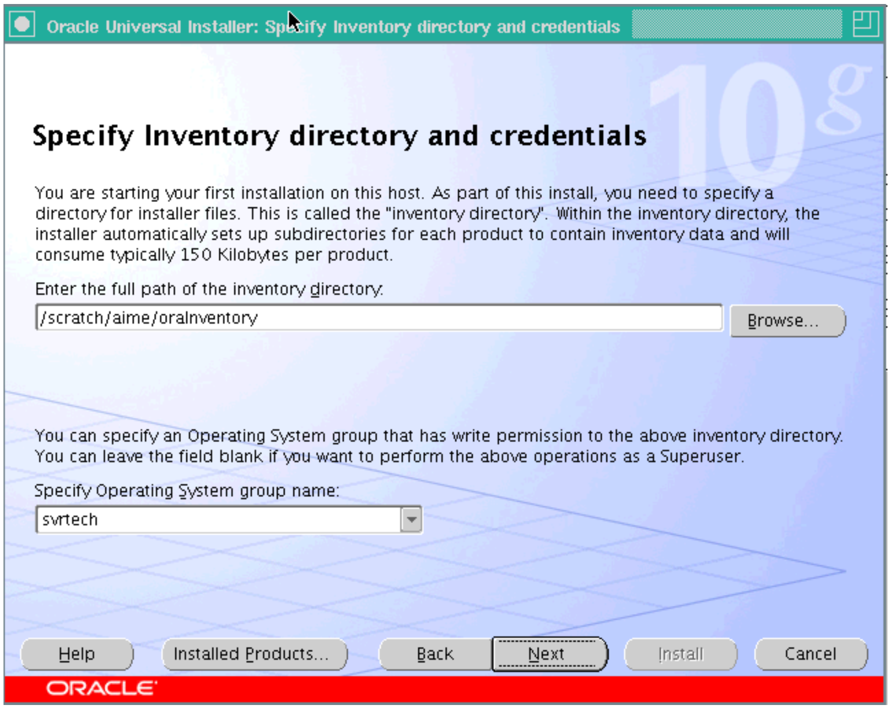
---

**Note:** The languages that you select here change the language of Grid Control only, and not the language of the installation itself.

---

3. Click **Next**. The Specify Inventory Directory and Credentials screen appears only if Grid Control is the first Oracle product that you are installing on the machine.

***Figure 8–4 Specify Inventory Directory and Credentials***



Oracle Universal Installer: Specify Inventory directory and credentials

Specify Inventory directory and credentials

You are starting your first installation on this host. As part of this install, you need to specify a directory for installer files. This is called the "inventory directory". Within the inventory directory, the installer automatically sets up subdirectories for each product to contain inventory data and will consume typically 150 Kilobytes per product.

Enter the full path of the inventory directory: /scratch/aime/oraInventory

You can specify an Operating System group that has write permission to the above inventory directory. You can leave the field blank if you want to perform the above operations as a Superuser.

Specify Operating System group name: svrtech

a. Specify the full path to the directory where Oracle Universal Installer (OUI) should place inventory files and directories. For example, `oracle_base/oraInventory` (on Linux).

---

**Note:** If you are performing the installation on a **Microsoft Windows** platform, the Specify Inventory Directory and Credentials screen will not appear.

On Microsoft Windows, the default inventory files location is `<system drive>\Program Files\Oracle\Inventory`.

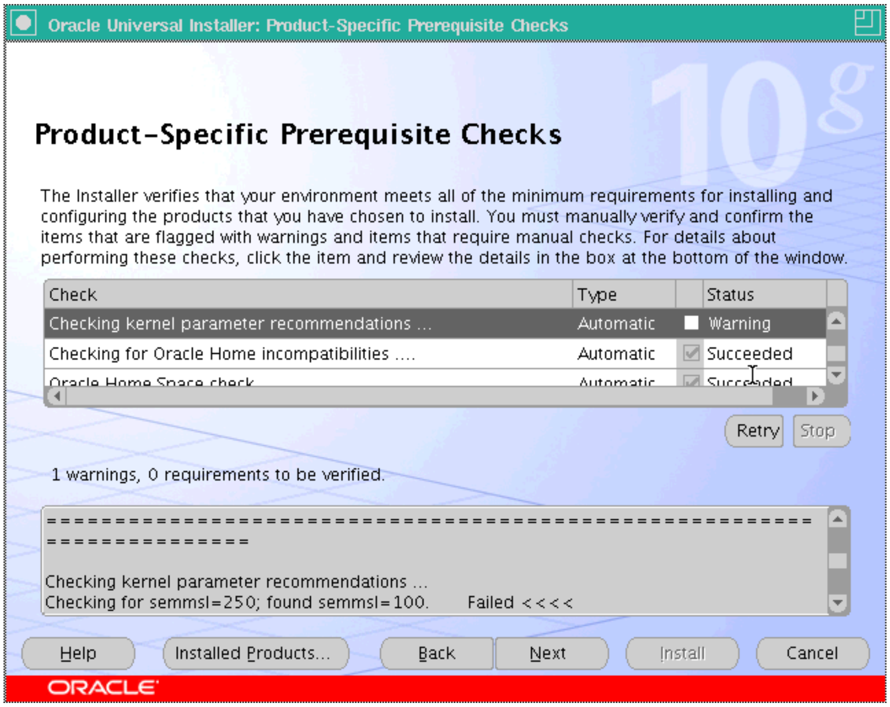
---

Refer to the Grid Control online Help for more information on guidelines recommended by Oracle for naming the directories.

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.

4. Click **Next**. The Product-Specific Prerequisite Checks screen appears.

*Figure 8–5 Product-Specific Prerequisite Checks*



Oracle Universal Installer: Product-Specific Prerequisite Checks

## Product-Specific Prerequisite Checks

The Installer verifies that your environment meets all of the minimum requirements for installing and configuring the products that you have chosen to install. You must manually verify and confirm the items that are flagged with warnings and items that require manual checks. For details about performing these checks, click the item and review the details in the box at the bottom of the window.

| Check | Type | Status |
|---|---|---|
| Checking kernel parameter recommendations ... | Automatic | □ Warning |
| Checking for Oracle Home incompatibilities .... | Automatic | ☑ Succeeded |
| Oracle Home Space check | Automatic | ☑ Succeeded |

1 warnings, 0 requirements to be verified.

```
=================================================================
===============

Checking kernel parameter recommendations ...
Checking for semmsl=250; found semmsl=100.      Failed <<<<
```

At this point, the installer runs some prerequisite checks to verify if the environment meets the minimum requirements for a successful Grid Control installation.

Early detection of system environment problems such as insufficient disk space, missing patches, inappropriate hardware, and so on results in a smoother installation later.

This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen.

**Note:** You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information, see Section 4.16, "Running the Prerequisite Check in Standalone Mode".

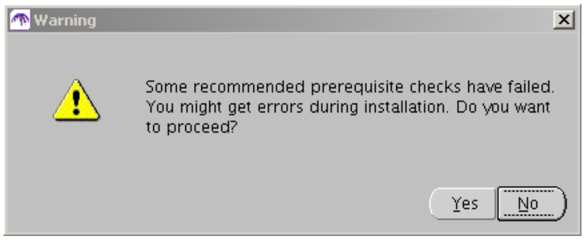
**a.** To stop all prerequisite checks, click **Stop**. At any point in time, click a prerequisite check to view its corresponding details, including the recommended user actions.

**Note:** You must manually verify and confirm all checks that were flagged with a warning, skipped (stopped by user), or failed.

**b.** To continue with the installation without retrying, click **Next**.

An error message is displayed if some recommended prerequisite checks have failed.

***Figure 8–6 Warning***



Some recommended prerequisite checks have failed. You might get errors during installation. Do you want to proceed?

**c.** Click **No** to go back and rerun the prerequisite check. Click **Yes** to ignore the message and continue with the installation.

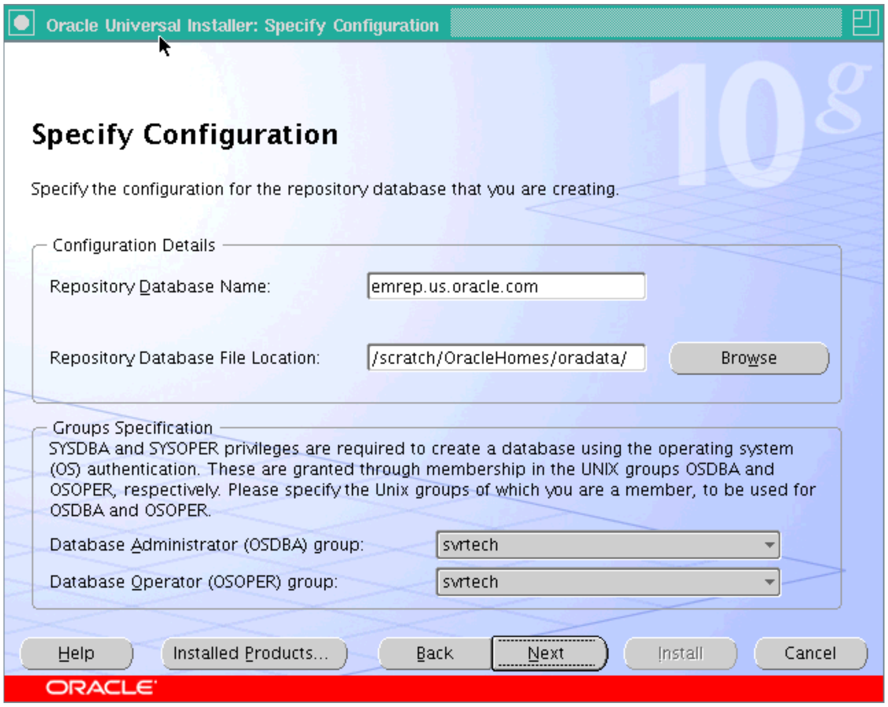
---

**Note:** It is recommended that you retry checks that were flagged with warnings, failed, or were skipped (stopped by the user) before continuing with the installation.

---

**5.** The Specify Configuration screen appears.

***Figure 8–7 Specify Configuration***



Specify Configuration

Specify the configuration for the repository database that you are creating.

Configuration Details

Repository Database Name: emrep.us.oracle.com

Repository Database File Location: /scratch/OracleHomes/oradata/

Groups Specification

SYSDBA and SYSOPER privileges are required to create a database using the operating system (OS) authentication. These are granted through membership in the UNIX groups OSDBA and OSOPER, respectively. Please specify the Unix groups of which you are a member, to be used for OSDBA and OSOPER.

Database Administrator (OSDBA) group: svrtech

Database Operator (OSOPER) group: svrtech

You must specify the configuration details for the new database that you are creating, and select the appropriate recipients of the OSDBA and OSOPER privileges (on UNIX only).

---

**Note:** Your Management Repository may also require patches to be applied after successful installation. See Section 3.2, "Operating System, Browser, Target Certification" for more information.

---

a. Specify the new Database Name and the Database File Location (location where the new database is going to reside).

---

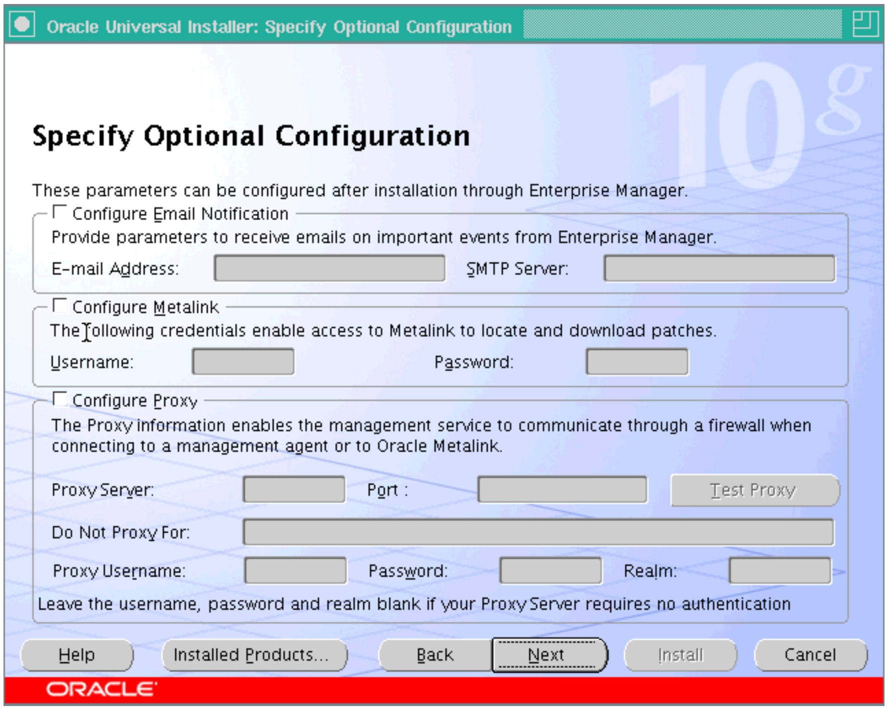
**Note:** It is recommended that you specify a fully qualified database name (for example, `emrep.<domain_name>`), though appending the database name with the domain name is not mandatory.

---

b. In the Group Specification section, select the OSDBA and OSOPER groups of which you are a member. These memberships are required to grant the SYSDBA and SYSOPER permissions that are, in turn, required to create the new database using the operating system authentication.

6. Click **Next**. The Specify Optional Configuration screen appears.

*Figure 8–8 Specify Optional Configuration*



Oracle Universal Installer: Specify Optional Configuration

Specify Optional Configuration

These parameters can be configured after installation through Enterprise Manager.

□ Configure Email Notification

Provide parameters to receive emails on important events from Enterprise Manager.

E-mail Address: SMTP Server:

□ Configure Metalink

The following credentials enable access to Metalink to locate and download patches.

Username: Password:

□ Configure Proxy

The Proxy information enables the management service to communicate through a firewall when connecting to a management agent or to Oracle Metalink.

Proxy Server: Port :

Do Not Proxy For:

Proxy Username: Password: Realm:

Leave the username, password and realm blank if your Proxy Server requires no authentication

As the name suggests, all the fields on this screen are optional, and are disabled by default. Select the required check box to enable the corresponding fields.

a. In the Configure Email Notification section, specify an appropriate e-mail address, and the corresponding SMTP server name. You will receive important information on the condition of the monitored targets, including critical alerts at this e-mail address.

   The e-mail address that you specify should be associated with the SYSMAN user to receive notifications.

The SMTP Server is the name of the mail server (for example `mail.acme.com`). For Linux, the default SMTP server is the local host name. Use the fully qualified host name (including domain).

**Note:** If you do not provide the e-mail notification information, this feature is not enabled upon installation. You may also choose to configure these settings through the Grid Control console by clicking **Notification Methods** under Setup. Refer to the Grid Control online Help for more information.

**b.** Specify the My Oracle Support (formerly Metalink) credentials.

If you prefer, you can also enter this information through the Grid Control console after installation by clicking **Patching Setup**, under Setup.

**Note:** Grid Control uses these credentials to search for and download patches from `http://oracle.com/support/metalink/index.html`

**c.** Specify the Proxy Information if Grid Control is using a proxy server for external access. Table 8–4 describes each of the fields under this section.

***Table 8–4 Specify Proxy information - Input Fields***

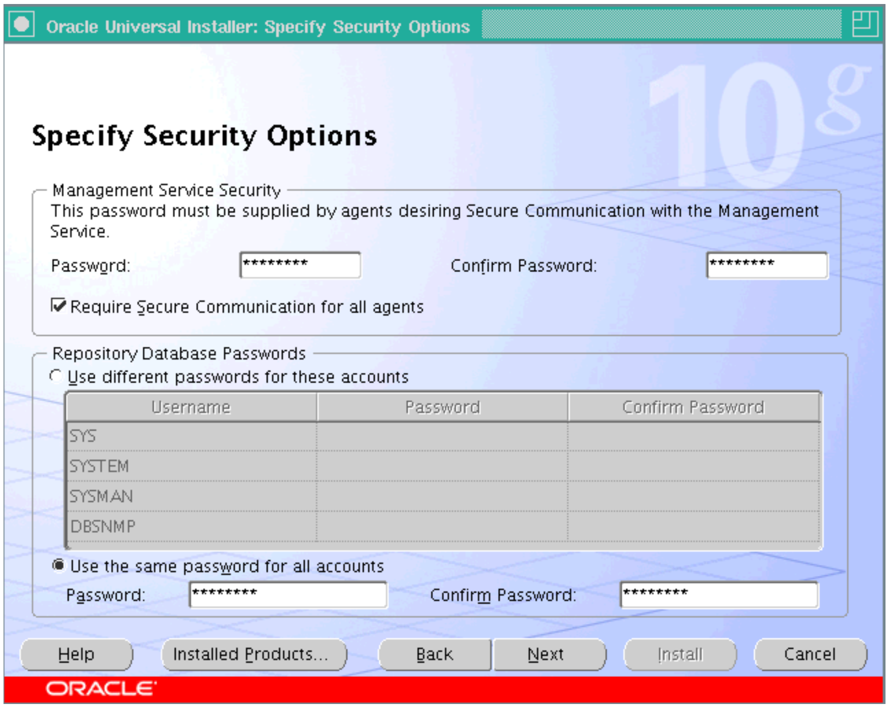
| Input | Description |
|---|---|
| Proxy Server | Specify the proxy server host name. For example, **`www-fooproxy.here.com`** |
| Port | Specify the port at which the server is listening. For example, **`80`**. See Appendix E, "Firewall Port Requirements" for more information on specifying ports when you are using a firewall in your grid environment. |
| Do Not Proxy For | Specify the URLs that do not need the proxy server to be accessed. You can specify multiple comma-separated values. For example, .here.com, .us.mycompany.com, .uk.mycompany.com, and so on.<br>Note that you must always specify *fully qualified host names.* |
| Proxy User and Password | Specify the user name and password only if the proxy server has been configured to use these credentials for authentication. These are optional fields. |
| Realm | Specify an appropriate realm value. This becomes a mandatory field only if the proxy server credentials have been configured using a realm.<br>A realm is a string value assigned by the proxy server to indicate the secure space that requires authentication. |
| Test Proxy | Click this button to verify your proxy server settings. |

**Note:** When you search for a patch, if the proxy properties (saved in the `sysman/config/emoms.properties` file) are not set, or are set incorrectly, you receive an error message indicating that Grid Control cannot access the My Oracle Support (formerly Metalink) Web site.

**Caution:** If the proxy server requires user authentication before providing access, you must specify these credentials here or through the Patching Setup screen under Setup in the Grid Control console.

7. Click **Next**. The Specify Security Options screen appears.

*Figure 8–9 Specify Security Options*



Oracle Universal Installer: Specify Security Options

Specify Security Options

Management Service Security

This password must be supplied by agents desiring Secure Communication with the Management Service.

Password: ********* Confirm Password: *********

☑ Require Secure Communication for all agents

Repository Database Passwords

○ Use different passwords for these accounts

| Username | Password | Confirm Password |
|---|---|---|
| SYS | | |
| SYSTEM | | |
| SYSMAN | | |
| DBSNMP | | |

● Use the same password for all accounts

Password: ********* Confirm Password: *********

You must specify the passwords that are used to secure your entire Grid Control environment. This screen has two sections - Management Service Security, and Repository Database Passwords.

- Management Server Security: The password that you specify here is used to secure and lock the OMS.

  Select **Require Secure Communications for all agents** if you want the secure OMS to communicate only with secure Management Agents. This is optional, though recommended.

  For example, consider you have unsecured 10.1.*n* agents in the Grid and you have secured the OMS. Now, if you select the Require Secure Communications option, then all communication between the 10.2 OMS and 10.1.*n* agents fails (because these agents have not been secured).

**Note:** To secure a Management Agent, run following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

```
<AGENT_HOME>/bin/emctl secure agent
```

- Repository Database Passwords: Specify the passwords for each of the administrative database accounts listed in Table 8–5.

*Table 8–5 Repository Database Passwords*

| User Account | Applies to | Description |
|---|---|---|
| SYS | Management Repository | Super Administrator for the Management Repository database. |
| SYSTEM | Management Repository | Administrator for the Management Repository database. |
| DBSNMP | Management Repository | Monitoring user for the Management Repository database. |
| SYSMAN | Management Repository, Application Server, and Grid Control | The default Grid Control Super Administrator and Owner of the Management Repository database schema and the Grid Control application user.<br>The default ias_admin password is the same as the password assigned to the SYSMAN account. This is required to access the Oracle application server (`ias_admin`). The `ias_admin` user is the administrative user for the Oracle Application Server console.<br>After the installation, if you want to change this default password, then go to the Oracle home directory of the OMS and run the following command:<br>`ORACLE_HOME/bin/emctl set password <old_default_password> <new_password>`<br>If you do not remember the old ias_admin password, then follow the instructions outlined in Document ID 280587.1 that is available on My Oracle Support (formerly Metalink). |

You can use the same password for all four accounts, or specify a different password for each one. These passwords are used to secure the Management Repository database.

To specify a different password for each account, select **Use different passwords for these accounts** and specify the passwords for each account.

To specify the same password for all accounts, select **Use the same password for all accounts** and specify one password to be used for all database accounts.

**Note:** The SYS, SYSMAN, DBSNMP, and SYSTEM users are privileged database users. You must remember the passwords that you specify for them. For more information on password restrictions and recommendations, see *Oracle Database Administrator's Guide*.

*Password Restrictions and Recommendations*

The following restrictions apply to passwords:

– Passwords must be between 5 and 30 characters long.

– Passwords should not start with a number.

– Passwords cannot be the same as the user name.

– Passwords must include letters (lowercase/uppercase) and numbers only.

---

**Note:** The SYSMAN password can include underscores (_), and hyphens (-), dollar ($), and hash (#) along with alphanumeric characters. Alphabetic characters can be uppercase or lowercase.

---

– Passwords cannot be Oracle reserved words. See Appendix I, "Oracle Reserved Words" for more information.

---

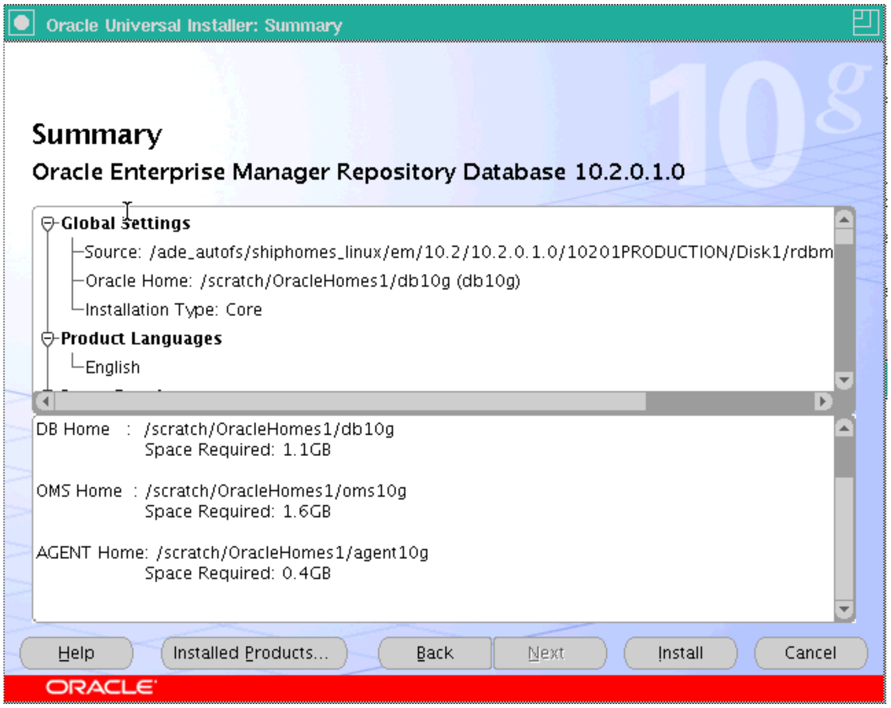
**Note:** Oracle recommends that the passwords you specify have the following characteristics:

1. Have at least one letter, one integer, and one special character (underscore).
2. Are not simple or obvious words such as welcome, account, database, or user.

---

8. Click **Next**. The Summary screen appears.

***Figure 8–10 Installation Summary***



Oracle Universal Installer: Summary

Summary

Oracle Enterprise Manager Repository Database 10.2.0.1.0

```
Global Settings
  Source: /ade_autofs/shiphomes_linux/em/10.2/10.2.0.1.0/10201PRODUCTION/Disk1/rdbm
  Oracle Home: /scratch/OracleHomes1/db10g (db10g)
  Installation Type: Core
Product Languages
  English
```

```
DB Home   : /scratch/OracleHomes1/db10g
            Space Required: 1.1GB

OMS Home  : /scratch/OracleHomes1/oms10g
            Space Required: 1.6GB

AGENT Home: /scratch/OracleHomes1/agent10g
            Space Required: 0.4GB
```

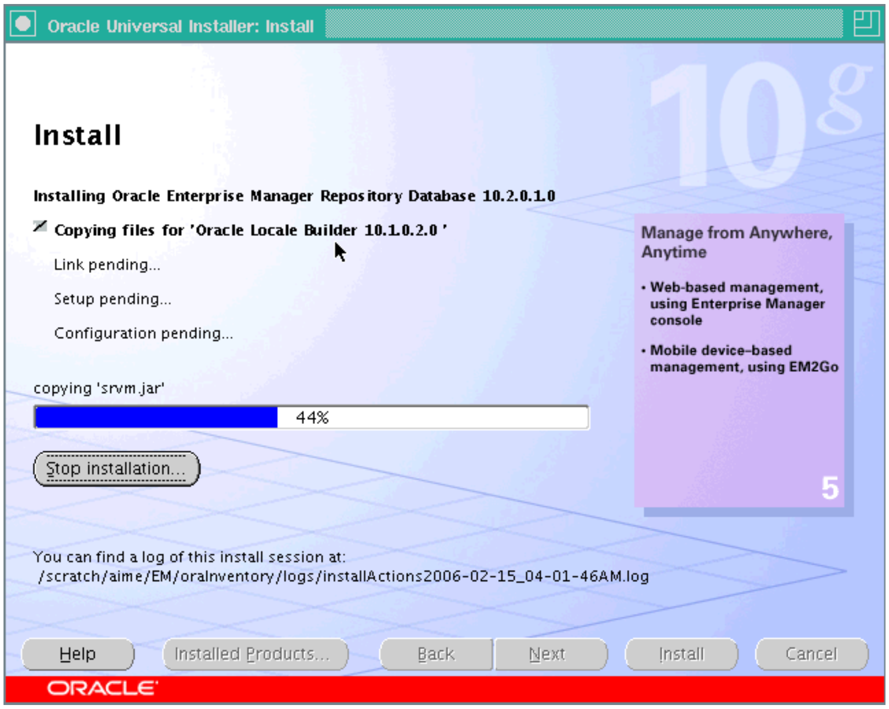
This screen provides a summary of the options that you have selected during the installation process. Depending on the installation type, it also provides any or all of the following details:

- Global Settings
- Product Languages
- Space Requirements
- Installed Products

Verify the choices that you have made.

**a.** Click **Install** to start the installation. The Install screen that appears displays the installation progress bar.

*Figure 8–11 Installation in Progress*



Oracle Universal Installer: Install

Install

Installing Oracle Enterprise Manager Repository Database 10.2.0.1.0

Copying files for 'Oracle Locale Builder 10.1.0.2.0 '

Link pending...

Setup pending...

Configuration pending...

copying 'srvm.jar'

44%

You can find a log of this install session at:
/scratch/aime/EM/oraInventory/logs/installActions2006-02-15_04-01-46AM.log

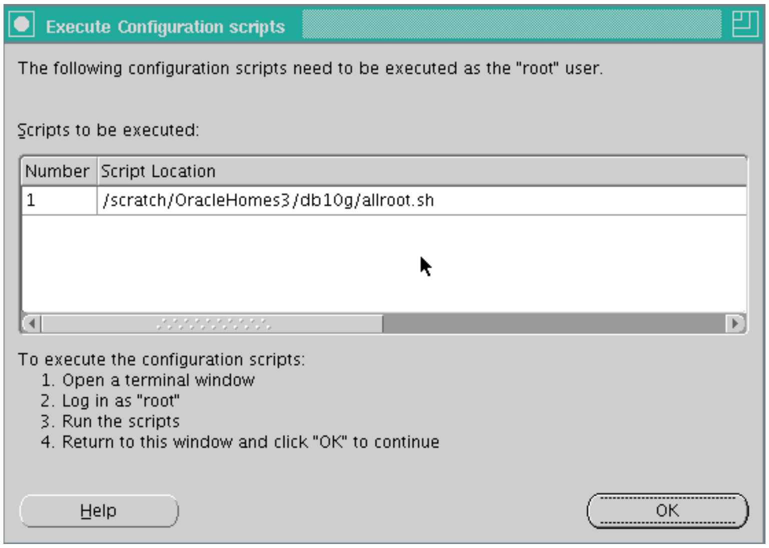
Stop installation...
10g
Manage from Anywhere, Anytime
• Web-based management, using Enterprise Manager console
• Mobile device-based management, using EM2Go
5
Help
Installed Products...
Back
Next
Install
Cancel
ORACLE

The installer seamlessly installs all Grid Control components based on the installation type you selected.

**b.** During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that appears (on UNIX only).

**Note:** The Execute Configuration Scripts dialog box will not appear on Microsoft Windows. You will be directed to the Configuration Assistants screen (step 9) in the next step.

*Figure 8–12 Execute Configuration Scripts*



The following configuration scripts need to be executed as the "root" user.

Scripts to be executed:

| Number | Script Location |
|---|---|
| 1 | /scratch/OracleHomes3/db10g/allroot.sh |

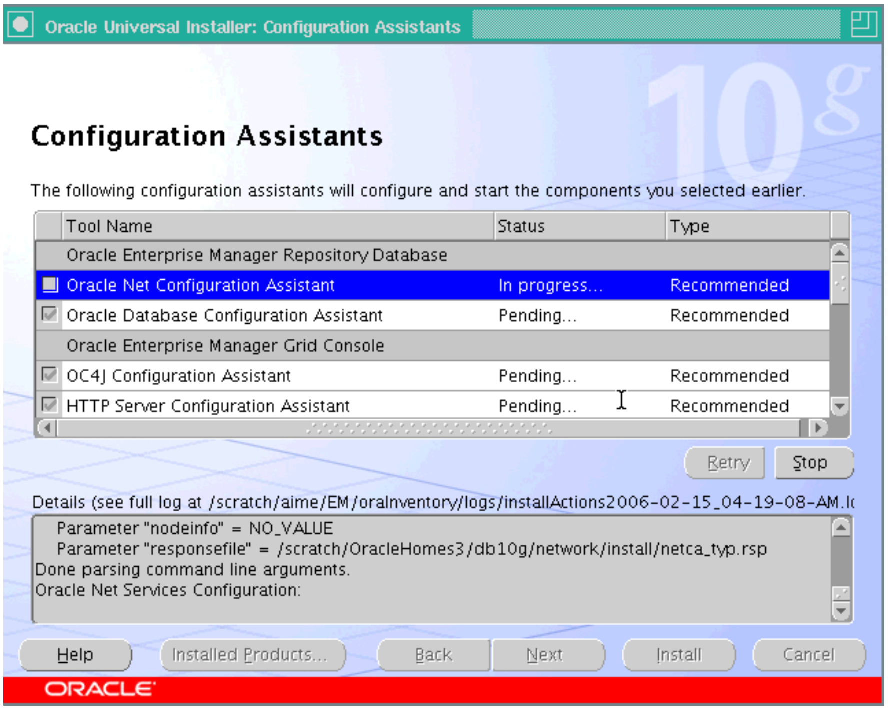
To execute the configuration scripts:
1. Open a terminal window
2. Log in as "root"
3. Run the scripts
4. Return to this window and click "OK" to continue

Go to the computer window, log in as `root`, and run these configuration scripts.

c. Return to the dialog box (shown in Figure 8–12) after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the configuration assistants.

*Figure 8–13 Configuration Assistants*



Configuration Assistants

The following configuration assistants will configure and start the components you selected earlier.

| | Tool Name | Status | Type |
|---|---|---|---|
| | Oracle Enterprise Manager Repository Database | | |
| □ | Oracle Net Configuration Assistant | In progress... | Recommended |
| ☑ | Oracle Database Configuration Assistant | Pending... | Recommended |
| | Oracle Enterprise Manager Grid Console | | |
| ☑ | OC4J Configuration Assistant | Pending... | Recommended |
| ☑ | HTTP Server Configuration Assistant | Pending... | Recommended |

Details (see full log at /scratch/aime/EM/oraInventory/logs/installActions2006-02-15_04-19-08-AM.l

```
    Parameter "nodeinfo" = NO_VALUE
    Parameter "responsefile" = /scratch/OracleHomes3/db10g/network/install/netca_typ.rsp
Done parsing command line arguments.
Oracle Net Services Configuration:
```

This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation.

Table 8–6 lists all the configuration tools that are run during a typical Grid Control installation (Install Enterprise Manager Using a new database).

*Table 8–6 Grid Control Configuration Tools*

| Product | Configuration Tool[1] |
|---|---|
| Oracle Repository Database | ■ Oracle Net Configuration Assistant<br>■ Oracle Database Configuration Assistant<br>■ OC4J Configuration Assistant |
| Oracle Enterprise Manager Grid Console | ■ OC4J Configuration Assistant<br>■ HTTP Server Configuration Assistant<br>■ Java Configuration Assistant<br>■ Web Cache Configuration Assistant<br>■ OracleAS Instance Configuration Assistant<br>■ Register DCM Plug-ins with Enterprise Manager<br>■ DCM Repository Backups Assistant<br>■ Enterprise Manager Technology Stack Upgrade<br>■ Oracle Management Service Configuration |
| Oracle Management Agent | ■ Agent Configuration Assistant |

[1] Depending on the installation type that you have selected, any or all of the configuration tools listed in this table will be run.

For more information on the installation logs that are created and their locations, see Appendix B, "Installation and Configuration Log Files". In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

**Note:** The individual log files for each configuration tool are available at the following directory:

```
ORACLE_HOME/cfgtoollogs/cfgfw
```

Besides the individual configuration logs, this directory also contains `cfmLogger_timestamp.log` (The timestamp depends on the local time and has a format such as `cfmLogger_2005_08_19_01-27-05-AM.log`.). This log file contains all the configuration tool logs.

a. To stop running a configuration tool, select it and click **Stop**.

b. To rerun a configuration tool, select it and click **Retry**.

**Note:** The installation is considered successful even if all the configuration tools fail, irrespective of their type (recommended/optional). However, failing to successfully run all the configuration tools results in an improperly configured product, which may not function. Refer to the Grid Control installation online Help for more information.

**Note:** In the event a particular configuration assistant fails, you can choose to rerun only that configuration assistant (in standalone mode). See Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation" for more information.

10. After successfully running all the recommended configuration tools, the End of Installation screen appears.

    This screen displays some important information about the products you have installed. This information is also available in the `<AGENT_HOME>/sysman/setupinfo.txt` file.

    For example, it might contain information about the URLs for particular Web applications.

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

## 8.4 Installing Enterprise Manager Grid Control Using an Existing Database

This section introduces you to the second installation type offered by OUI, that is, *Enterprise Manager 10g Grid Control Using an Existing Database*. In particular, this section covers the following:

- Overview
- Before You Begin
- Prerequisites
- Installation Procedure
- Installing on Microsoft Windows 2008 and Microsoft Windows Vista

**Note:** This section describes the steps required for installing the base release, that is, Enterprise Manager 10g Grid Control Release 2 (for example, 10.2.0.1 Linux or 10.2.0.2 Microsoft Windows).

If you are installing Grid Control for the first time in your environment and if you want to have the latest release, then use the'Installing Software-Only and Configuring Later' option that is discussed in Section 8.6, "Installing 'Software-Only' and Configuring Later".

## 8.4.1 Overview

The second installation type, that is, *Enterprise Manager 10g Grid Control Using an Existing Database*, is best suited when you already have a certified Oracle Database in your environment and when you want to use it to create the Management Repository. The existing, certified Oracle Database can be on a local or remote host. However, Oracle Real Application Clusters (RAC) databases must be on a shared disk.

To view a list of certified Oracle Database, see Document ID 412431.1 on My Oracle Support (formerly Metalink). If you want to use a RAC database, which is configured on a virtual host, as the existing database, then refer to Document ID 561441.1 on My Oracle Support (formerly Metalink).

If you want to use Oracle Database 11g as the existing database, then see Section 8.6.2.4, "Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g".

This installation type does the following:

- Installs Oracle Management Service 10g Release 2 *(Deployed in Oracle Application Server 10g Release 2 (10.1.2.0.2) that gets installed along with other core components)*
- Installs Oracle Management Agent 10g Release 2
- Configures the Management Repository *(in the existing, certified Oracle Database)*, OMS, and Management Agent.

The following describes the installation process and the software components that are installed for this installation type.

***Table 8–7 Installation Process for the Installing Enterprise Manager Grid Control with an Existing Database***

| Sequence | Action | Component Installed/Configured | Description |
|---|---|---|---|
| 1 | Installation | Oracle Management Service 10g Release 2 | Technically, the installer installs an application server, that is, Oracle Application Server 10g Release 2 (10.1.2.0.2) where the OMS is deployed. In the specified installation directory, the installer creates a subdirectory for OMS and places the software binaries in l seit.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for OMS is:<br>`/scratch/OracleHome/oms10g` |

***Table 8–7 (Cont.) Installation Process for the Installing Enterprise Manager Grid Control with an Existing Database***

| Sequence | Action | Component Installed/Configured | Description |
|---|---|---|---|
| 2 | Installation | Oracle Management Agent 10g Release 2 | In the specified installation directory, the installer creates a subdirectory for the Management Agent and places the software binaries in it. The subdirectory is agent10g.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for the Management Agent is:<br>`/scratch/OracleHome/agent10g` |
| 3 | Configuration | All | The installer runs the Configuration Assistant tools to configure all the installed components:<br>1. **Configuring Management Repository:** Creates a Management Repository in the specified existing, certified Orale Database to store all the collected information.<br>2. **Configuring OMS:** Configures the OMS.<br>3. **Configuring Management Agent:** Configures the Management Agent to enable monitoring of targets, collection of information, and so on. |

## 8.4.2 Before You Begin

Before you begin, keep these points in mind:

- The existing, certified Oracle Database must NOT have a repository already created.
- The default port for Enterprise Manager Grid Control is 4889 and the default port for Management Agent is 3872. For more information about the default ports that are assigned and the possibility of using custom ports instead of default ports, see Section 4.9, "Knowing About the Ports Used for Installation".
- Oracle offers code fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for code 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 Grid Control installation, you must consider Enterprise Manager Grid Control's framework components as well as the targets monitored by Enterprise Manager Grid Control. Oracle recommends keeping your Grid Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license. For information about the certified combinations of Enterprise Manager Grid Control components and monitored targets, see *My Oracle Support* note.412431.1.
- Do check the following:
  - If that existing database is on the same host where OMS is installed, the database gets added to the All Targets page of the Grid Control console, but you will have to provide configuration details to enable monitoring of that

database. To do so, log in to Enterprise Manager Grid Control, click **Targets** and then click **All Targets**. From the list, select the database instance and click **Configure**. In the Configure Database Instance: Properties Page, provide the details.

- If that existing database is on a different host, then ensure that that host has a Management Agent installed that points to the OMS. After that, provide configuration details in the Grid Control console to enable monitoring of that database. To provide configuration details, follow the instructions given in the previous point.

- If the Management Agent does not start up automatically when you restart the host, then do the following:

  a. Open the agentstup file from the Oracle home of the Management Agent:

  ```
  $ORACLE_HOME/install/unix/scripts/agentstup
  ```

  b. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

  c. Run the root.sh script from the Oracle home of the Management Agent:

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

  d. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

  **Note:** This is a one-time action to be taken. Step (a) to Step (c) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

### 8.4.3 Prerequisites

Before installing Enterprise Manager Grid Control with an existing database, ensure that you meet the following prerequisites.

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

***Table 8–8 Prerequisites for Enterprise Manager 10g Grid Control Using an Existing Database***

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the necessary hardware and software requirements for Enterprise Manager Grid Control.<br>For information about hardware and software requirements, see Section 3.1, "Hardware Requirements" and Section 3.3, "Software Requirements", respectively. | |
| Operating System Requirements | Check if the operating system of the host is certified.<br>For information about the supported operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |

*Table 8–8 (Cont.) Prerequisites for Enterprise Manager 10g Grid Control Using an Existing Database*

| Requirement | Description | Yes/No |
|---|---|---|
| Package Requirements | Verify if the package requirements for each platform are met.<br>For information about packages to be installed for Management Agent, see Appendix D, "Platform-Specific Package and Kernel Requirements" | |
| Sufficient Physical Memory | Ensure there is sufficient physical memory available for this installation type. For information, see Section 8.1, "Understanding the Installation Types" and Section 3.1.1, "Recommended CPU and Memory Allocation". | |
| Host List and Credentials Requirements | Identify the host where you want to install Enterprise Manager Grid Control, and obtain the credentials of that host so that it can be accessed for installation. | |
| Host Name Requirement | The host name must be a valid host name. For example, *serverhost1.company.com* or *serverhost1*.<br>However, it cannot be an IP address. At the same time, it cannot be localhost.localdomain as strings used in the /etc/hosts file.<br>At the time of invoking the installer, you can pass `ORACLE_HOSTNAME=<host_name> -local` as an argument. | |
| Permission Requirements for Installation Directory | Check if the installation directory, that is, the Oracle home directory is writable. | |
| Installing User Requirements | The following are the requirements:<br>▪ (UNIX only) The installation must NOT be run by the root user<br>▪ User must be a DBA user<br>▪ (Microsoft Windows only) User must be able to create process-level tokens<br>▪ (Microsoft Windows only) User must be able to log in as a batch job<br>▪ (Microsoft Windows only) User must be able to adjust memory quota for process<br>▪ (Microsoft Windows only) User must be part of the ORA-DBA group and have administrator permissions | |
| Installation Directory Requirements | If the specified *Installation Directory* already contains subdirectories that represent the components of Enterprise Manager Grid Control, then those subdirectories must be empty. If they are not, either delete them or keep them empty.<br>For example, if the specified *Installation Directory* already has <*install_dir/agent10g*> and <*install_dir/oms10g*> subdirectories, then they must be empty. | |

*Table 8–8 (Cont.) Prerequisites for Enterprise Manager 10g Grid Control Using an Existing Database*

| Requirement | Description | Yes/No |
|---|---|---|
| Existing Oracle Database Requirements | Ensure that the existing Oracle Database is a certified database.<br>To view a list of certified Oracle Databases, see Document ID 412431.1 on My Oracle Support (formerly Metalink). If you want to use a RAC database, which is configured on a virtual host, as the existing database, then refer to My Oracle Support note 561441.1.<br>If you want to use Oracle Database 11g as the existing database, then see Section 8.6.2.4, "Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g". | |
| Existing Oracle Database and Listener Status Requirements | Ensure that the existing, certified Oracle Database and Listener are running. | |
| Password Verification Requirements | Ensure that the profile of the Password Verification resource name has the "Default" value. If the Password Verification is enabled, repository creation may fail. | |
| Existing Oracle Database Configuration Requirements | If your existing database is configured with a Database Control, then ensure that the database control is deconfigured before installing Enterprise Manager Grid Control. For commands to be used for deconfiguring the Database Control, see the first few steps in Section 8.4.4, "Installation Procedure". | |
| NLS_LANG Environment Variable Requirements | If your operating system is Linux, then ensure the NLS_LANG environment variable is set with a value that is compatible with the operating system default locale setting and the Management Repository database character set.<br>For information on the specific values for language, territory, or character set, refer to the Globalization Support Guide of the Oracle product that you are using. | |
| Existing Oracle Database Initialization Parameters Requirements | Verify database setting - initialization parameters.<br>For a detailed list of database initialization parameter settings based on the Enterprise Manager deployment size, see Section 8.4.3.1, "Check Database Initialization Parameters". | |
| Targets Monitored | Remember that Enterprise Manager Grid Control will be able to monitor only those targets that are monitored by the Management Agent installed by the same user. | |

### 8.4.3.1 Check Database Initialization Parameters

The initialization parameters must be set correctly for your certified existing Oracle Database Enterprise Edition, to be able to create a Management Repository. You should also set all *fixed* parameters for your Management Repository database.

> **See Also:** For more information about managing initialization parameters, refer to the *Managing Initialization Parameters Using a Server Parameter File* chapter of the *Oracle Database Administrator's Guide*.

After making the changes, you must shut down and restart the database.

**See Also:** For instructions on shutting down the database, refer to the *Starting Up and Shutting Down* chapter in the *Oracle Database Administrator's Guide*.

### Fixed Initialization Parameter Values

The following table lists the parameters and their fixed values that must be met for successful Management Repository database creation. These parameters are verified by Oracle Universal Installer prerequisite checks during installation.

**Note:** Make sure that the Enterprise Edition database you select for your Management Repository has the **fine-grained access control** option set to true. This is required for successful Management Repository creation. Check `v$options` for this setting.

*Table 8–9 Fixed Initialization Parameter Values*

| Parameter | Value |
|---|---|
| job_queue_processes | 10 |
| db_block_size | 8192 |
| timed_statistics | TRUE |
| open_cursors | 300 |
| session_cached_cursors | 200 |
| aq_tm_processes | 1 |
| compatible | <currently installed Oracle Database release> (default) |
| undo_management | AUTO |
| undo_retention | 10800 |
| undo_tablespace | <any acceptable name> |
| processes | 150 |
| log_buffer | 1048576 |
| statistics_level | TYPICAL (Note that this value is specific only to Enterprise Manager 10*g* Repository Database release and later.) |
| TEMP space (Tablespace)[1] | 50 MB (extending to 100 MB) |
| _b_tree_bitmap_plans | false (hidden parameter) |

[1] The TEMP space is an initialization parameter only when you are performing a Grid Control installation using a new database.

### Variable Initialization Parameter Values

The variable parameter setting values are based on the size of the Grid Control environment. For the sake of clarity, the environment has been categorized as Small, Medium, and Large based on the number of targets in the environment, where:

- Small = Approximately 100 monitored targets
- Medium = Approximately 1000 monitored targets
- Large = 10000 or more monitored targets

Table 8–10 lists the variable parameter setting values.

*Table 8–10 Variable Initialization parameter Values*

| Size | pga_ aggregate_ target | Redo logs | db_cache_size | shared_pool_ size | sga_target |
|---|---|---|---|---|---|
| Small | 256 MB | 100 MB | 384 MB (or more) | 128 MB | 512 MB (or more) |
| Medium | 384 MB | 512 MB | 1024 MB (or more) | 384 MB | 1408 MB (or more) |
| Large | 512 MB | 1024 MB | 2048 MB (or more) | 512 MB | 2560 MB (or more) |

### 8.4.4 Installation Procedure

> **Caution:** The steps outlined in this section are for installing a full, base releases of Enterprise Manager 10g Grid Control Release 2 or higher, using an existing database. For details about full, base releases and what these installation instructions can be use for, see Section 4.1, "Understanding What This Guide Helps You Install and Upgrade".

To install Enterprise Manager Grid Control using an existing database, follow these steps:

1. If your existing database is configured with Database Control, then ensure that you deconfigure it before you begin the installation of Grid Control.

   To deconfigure Database Control for a single instance database, run the following command:

   ```
   <Database ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop
   ```

   To deconfigure Database Control for a Real Application Clusters (RAC) database, run the following command:

   ```
   <Database ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop - cluster
   ```

   After deconfiguring the Database Control, connect to the database as SYS user and run the following SQL files from the Oracle home of the database:

   ```
   <ORACLE_HOME>/rdbms/admin/dbmspool.sql
   ```

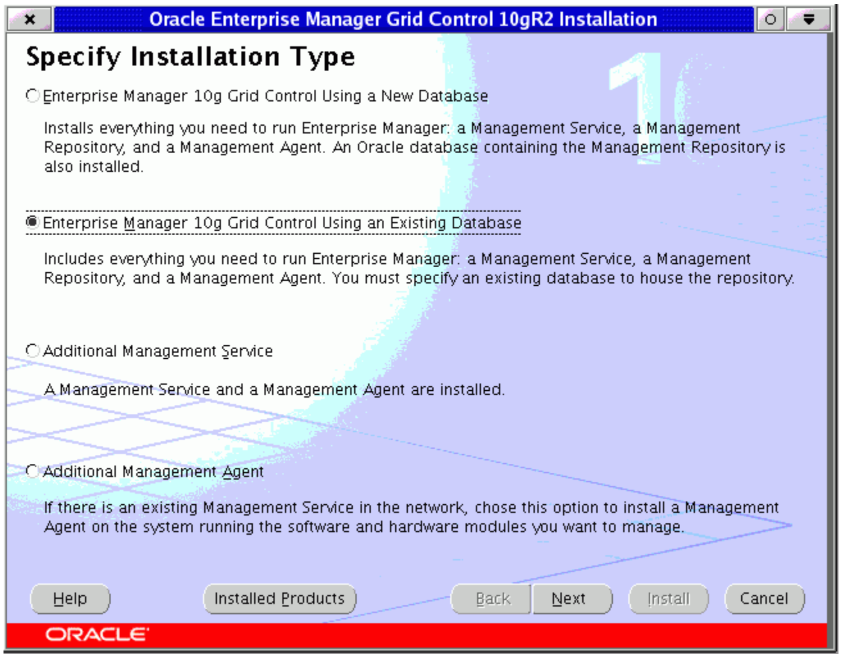
   ```
   <ORACLE_HOME>rdbms/admin/prvtpool.plb
   ```

**Note:** The command drops all the public synonyms starting with the following names created by any user for any schema:

- 'MGMT$%'
- 'MGMT_%'
- 'SMP_EMD%'
- 'SMP_MGMT%'
- 'SETEMVIEWUSERCONTEXT'
- 'DBMS_SHARED_POOL'
- 'EMD_MNTR'
- 'ECM_UTIL'

2. Start Oracle Universal Installer by running the `runInstaller` script in Linux (`<DVD>/runInstaller`) from the top directory of the DVD.
3. In the Specify Installation Type screen, select the second option (**Enterprise Manager 10g Grid Control Using an Existing Database**). Click **Next**.

***Figure 8–14 Specify Installation Type***



Oracle Enterprise Manager Grid Control 10gR2 Installation

Specify Installation Type

○ Enterprise Manager 10g Grid Control Using a New Database

Installs everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. An Oracle database containing the Management Repository is also installed.

● Enterprise Manager 10g Grid Control Using an Existing Database

Includes everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. You must specify an existing database to house the repository.

○ Additional Management Service

A Management Service and a Management Agent are installed.

○ Additional Management Agent

If there is an existing Management Service in the network, chose this option to install a Management Agent on the system running the software and hardware modules you want to manage.

4. The Specify Installation Location screen appears.
   a. Specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. All the Oracle homes created during the installation are placed as subdirectories under this parent directory. For example: `oms10g`, and `agent10g`.

**Caution:** Do not use symbolic links to specify the Oracle home path.

The installer by default installs the selected products in the English language.

b. If you want to install the product in a different language, click **Product Languages**.

   The Language Selection screen appears. Make the required language selections here, and click **Next**. See Figure 8–3, "Language Selection" for details.

5. Click **Next**. The Specify Inventory Directory and Credentials screen appears if is the first Oracle product that you are installing on the machine. See Figure 8–4, "Specify Inventory Directory and Credentials" for details.

6. Click **Next.** The Product Specific Prerequisites Check screen appears.

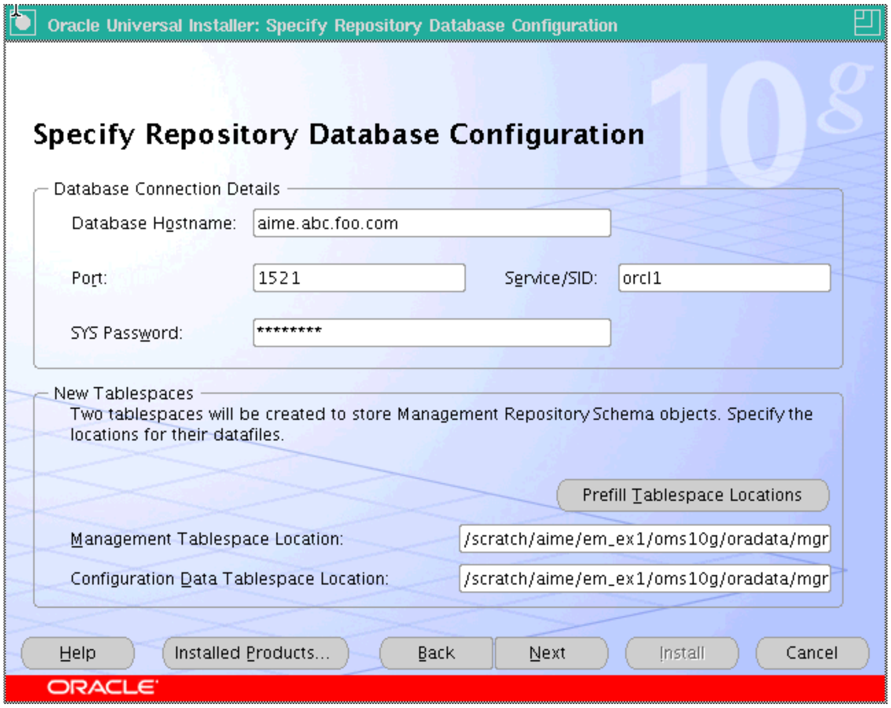
   This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

   Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen. See Figure 8–5, "Product-Specific Prerequisite Checks" for details.

   **Note:** You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information, see Section 4.16, "Running the Prerequisite Check in Standalone Mode".

7. Click **Next**. The Specify Repository Database Configuration screen appears.

***Figure 8–15 Specify Repository Database Configuration***



Oracle Universal Installer: Specify Repository Database Configuration

Specify Repository Database Configuration

Database Connection Details

Database Hostname: aime.abc.foo.com

Port: 1521

Service/SID: orcl1

SYS Password: ********

New Tablespaces

Two tablespaces will be created to store Management Repository Schema objects. Specify the locations for their datafiles.

Management Tablespace Location: /scratch/aime/em_ex1/oms10g/oradata/mgr

Configuration Data Tablespace Location: /scratch/aime/em_ex1/oms10g/oradata/mgr

Specify the connection details for the existing database in which the Management Repository should be created. The Management Repository database can be created on the following database releases:

- Oracle Database 10*g* Release 1 (10.1.0.4 and later), Enterprise Edition

> **Note:** If you are performing a Grid control installation using an existing database, ensure the database is of a 10.1.0.3 release or later.

- Oracle Real Application Clusters 10*g* Release 1 (10.1.0.4 and later)

> **Note:** If you are performing a Grid control installation using an existing database, ensure the existing Oracle RAC database is of a 10.1.0.3 release or later.

- Oracle9*i* Release 2 (9.2.0.6 and later), Enterprise Edition
- Oracle9*i* Real Application Clusters Release 2 (9.2.0.6 and later)

**a.** In the Database Connection Details section, specify a fully qualified host name, listener Port number, SID (system identifier) for the database instance, and the SYS password.

The SID identifies a specific Oracle Database and distinguishes it from other databases on the computer.

**Note:** When selecting an existing cluster database for creating the Management Repository, you can either specify the SID value, or use the OMS name.

**b.** Enter the password for the SYS user. This account is used to create the SYSMAN user, which is the primary owner of the Management Repository schema.

**c.** In the Additional Tablespace section, specify the location for the following:

- *Management Tablespace Location:* The MGMT_TABLESPACE tablespace holds data for the Management Repository.
- *Configuration Data Tablespace Location:* The MGMT_ECM_DEPOT_TS tablespace holds Configuration Management data for the Management Repository.

**Caution:** If the existing database that you have selected to create the repository already contains a SYSMAN schema, the installer will display an error similar to the following:

"The Grid Control schema already exists in the database that you have provided."

You can choose to manually drop this schema before proceeding with the repository creation.

You can also click **Continue.** The installer will then automatically drop the existing schema and create a new SYSMAN schema.

For ASM (Automatic Storage Management) devices, the tablespace locations should be specified relative to the ASM disk group. For example: `+<ASM Disk>/emrep/tablespace.dbf`

For tuning/performance reasons, Oracle recommends placing Binary large objects (BLOBs) in their own tablespace. Because Enterprise Configuration Management data support BLOBs, the Management Repository requires two tablespaces: `MGMT_TABLESPACE` and `MGMT_ECM_DEPOT_TS`.

Specify the full path of the file locations for the previously mentioned tablespaces. The directories you specify for these tablespaces must already exist for repository creation to succeed. For raw devices, you must partition your disk before specifying its location. Note that raw device path names vary across volume managers. Ensure to use the right path format for your raw device locations.

If you do not have the complete path for the tablespaces, click **Prefill Tablespace Location**. Note that the Prefill Tablespace button will be enabled only after you have specified all the Database Connection details. The installer then queries the database you have specified. Look for the SYSAUX tablespace location, and prefill that path in the appropriate box.

**Note:**

- The two tablespaces initially require 120 MB of disk space, with MGMT_TABLESPACE requiring 20 MB and MGMT_ECM_DEPOT_TS requiring about 100 MB. Ensure there is enough disk space available.
- If you are selecting an existing cluster database for the new Management Repository, the management tablespace file locations must be on a shared device that is accessible to all instances that provide the database service.

**Caution:** If the DBMS_SHARED_POOL package has not been installed at the time of the database creation, Oracle Universal Installer displays an error message and prompts you to execute this package before proceeding with the installation.

To check whether or not the DBMS_SHARED_POOL package has been installed, login to the database and execute the following query:

```
Select count(*) from dba_objects where OWNER = 'SYS'
AND object_name = 'DBMS_SHARED_POOL'
AND object_type IN ( 'PACKAGE','PACKAGE BODY') ;
```

This query should return a count of **2.**

To install the DBMS_SHARED_POOL package, execute the following script:

```
<DB_HOME>/rdbms/admin/dbmspool.sql
```

**Caution:** If you had not configure the database initialization parameters, then you might see the following error message:

The existing database is not configured to meet the requirements.

To resolve this issue, you must correctly set the database initialization parameters as described in Section 8.4.3.1, "Check Database Initialization Parameters".

8. Click **Next**. The Specify Optional Configuration screen appears.

   As the name suggests, all the fields on this screen are optional, and are disabled, by default. Select the required check box to enable the corresponding fields.

   a. In the Configure Email Notification section, specify an appropriate e-mail address, and the corresponding SMTP server name in this section. You will receive information on important developments and events in Grid Control, including critical alerts, at this e-mail address.

      The e-mail address that you specify should be associated with the SYSMAN user to receive notifications.

      The SMTP server is the name of the mail server (for example mail.acme.com). For Linux, the SMTP server must be the local host name. Use the fully qualified host name (including domain).

> **Note:** If you do not provide the e-mail notification information, this feature is not enabled upon installation. You may also choose to configure these settings through the Grid Control console by clicking **Notification Methods** under Setup. Refer to the Grid Control online Help for more information.

b. Specify the My Oracle Support (formerly Metalink) credentials if you are going to use a proxy server to access My Oracle Support.

   If you prefer, you may also enter this information through the Grid Control console after installation by clicking **Patching Setup**, under Setup.

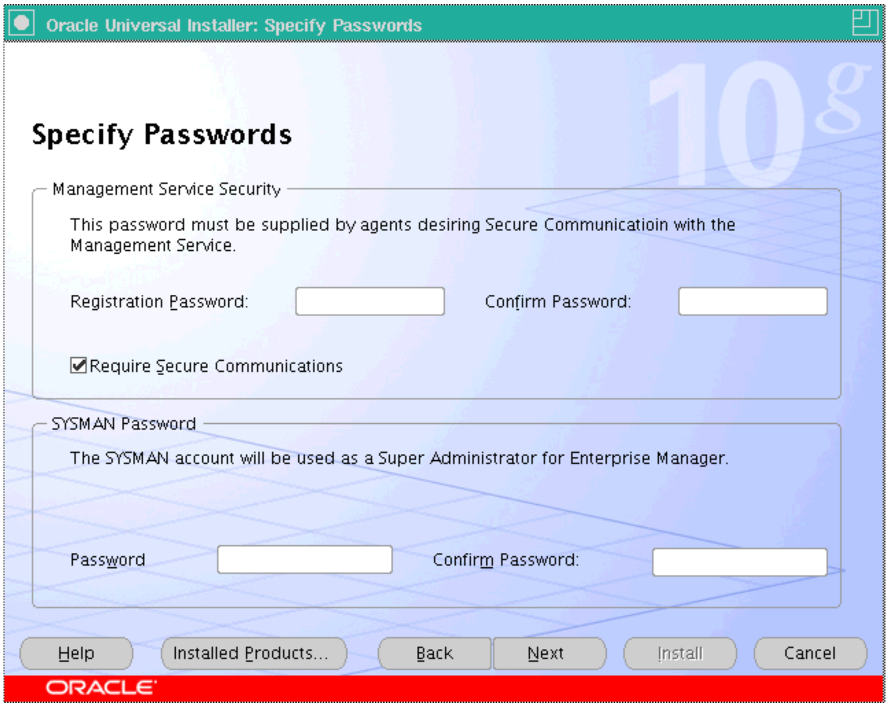
> **Note:** Grid Control uses the My Oracle Support (formerly Metalink) credentials to search for and download patches from `http://oracle.com/support/metalink/index.html`

c. Specify the Proxy Information if Grid Control is using a proxy server for external access. See Table 8–4, " Specify Proxy information - Input Fields" for a description on each of the input fields in this section.

> **Note:** If the proxy server requires user authentication before providing access, you must specify these credentials here, or through the Patching Setup screen under Setup in the Grid Control console.

9. Click **Next**. The Specify Passwords screen appears.

***Figure 8–16 Specify Passwords***



Oracle Universal Installer: Specify Passwords

Specify Passwords

Management Service Security

This password must be supplied by agents desiring Secure Communicatioin with the Management Service.

Registration Password: Confirm Password:

☑ Require Secure Communications

SYSMAN Password

The SYSMAN account will be used as a Super Administrator for Enterprise Manager.

Password Confirm Password:

   a. Specify the Management Service Security, and Repository Database passwords that are used to secure your entire Grid Control environment.

   b. Select **Require Secure Communications** if you want the secure OMS to communicate only with Secure Agents. This is optional, though recommended.

      For example, if you have 10*g* R1 (10.1.*n*) agents in the Grid environment and you have secured and locked the OMS, and selected the Require Secure Communications option, then all communication between the 10*g* R2 (10.2) OMS and 10.1 agents fails (because these agents have not been secured).

      To secure a Management Agent, run the following command from the Management Agent Oracle home of that particular target. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

      ```
      emctl secure agent
      ```

      See the section on Password Restrictions and Recommendations in this chapter for more information.

10. Click **Next**. The Summary screen appears.

    This screen provides a summary of the options that you have selected during the installation process. Depending on the installation type, this screen also provides any or all of the following details:

    - Global Settings
    - Product Languages
    - Space Requirements
    - New Installations
    - Installed Products

    Verify the choices that you have made and click **Install** to start the installation. The Install screen that appears displays the installation progress bar.

    The installer seamlessly installs all Grid Control components based on the installation type you selected.

11. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only on UNIX). Refer to Figure 8–12, "Execute Configuration Scripts".

    a. To execute these scripts, go to the computer window, log in as `root`, and run these configuration scripts.

    b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

12. The Configuration Assistants screen appears. At this point, the installer starts running the recommended Configuration Assistants.

> **Note:** The OMS Configuration Assistant will create the repository. The repository creation log (`emca_repos_create<TimeStamp>.log For example, emca_repos_create05_13_33.log`) is available at the following directory:
>
> ```
> OMS_HOME/sysman/log/
> ```

This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. Refer to Table 8–6, " Grid Control Configuration Tools" to see the list of configuration tools that are run. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

> **Note:** If you are installing Grid Control using an existing RAC database that is configured on a virtual host, and if the OMS Configuration Assistant fails, then refer to Document ID 561441.1 on My Oracle Support (formerly Metalink) at:
>
> `http://metalink.oracle.com/`

13. After successfully running all the recommended configuration tools, the End of Installation screen appears.

    This screen tells you whether or not the installation was successful, and displays some important information that you *must remember* about the products you have installed. For example, it might contain information about the URLs for particular Web applications.

> **Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:
>
> 1. Open the agentstup file from the Oracle home of the Management Agent:
>
>    ```
>    $ORACLE_HOME/install/unix/scripts/agentstup
>    ```
>
> 2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
> 3. Run the root.sh script from the Oracle home of the Management Agent:
>
>    ```
>    $<ORACLE_HOME>/root.sh
>    ```
>
> 4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:
>
>    ```
>    $<ORACLE_HOME>/bin/emctl start agent
>    ```
>
>    This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

#### 8.4.4.1 Configuration Assistant

During the installation process, if the `SYSMAN` schema already exists in the database that you specify for the Management Repository, the installer will prompt you to manually drop the schema. If this is not done, the installer will automatically drop the schema before proceeding to the next configuration assistant.

If the Oracle Management Service Configuration Assistant fails before completion, you can click **Retry**, which automatically cleans up the repository when the configuration tool is rerun. To manually clean up the repository, use the following command:

```
OMS_HOME/sysman/admin/emdrep/bin/RepManager <Host name> <Port>
<SID> -ACTION Drop
```

You may need to set the `LD_LIBRARY_PATH` to the `ORACLE_HOME/lib` directory of the OMS before running the script.

Refer to *Oracle Enterprise Manager Advanced Configuration* for further instructions on how to drop the existing repository from the database.

**Note:** The listener that is associated with the specified database must be running. Otherwise, Management Repository creation may fail.

### 8.4.5 Installing on Microsoft Windows 2008 and Microsoft Windows Vista

To install Enterprise Manager Grid Control using an existing database on Microsoft Windows 2008 and Microsoft Windows Vista, follow these steps:

1. Download patch# 6640752 for Microsoft Windows (32-Bit) from My Oracle Support. You can access My Oracle Support at:

   `http://metalink.oracle.com`

2. Extract the contents of the downloaded patch to a location on your system.

   For example: `C:\Patch_Download`

3. Download the base release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.2.0) for Microsoft Windows.

4. Extract the contents of the downloaded base release to a location on your system. For example, `C:\Base_Download`

5. Ensure that your existing database is a database that is supported on Microsoft Windows Vista or Microsoft Windows 2008. For example, Oracle Database 10g Release 2 (10.2.0.3 or 10.2.0.4).

6. Edit the response file and make changes as described in this step. Make the following changes in the response file.

   The response file is available at:

   ```
   C:\Base_Download\Disk1\install\response\emnoseed.rsp
   ```

   Make the following changes:

   a. For the FROM_LOCATION parameter, specify the full path to the `products.xml` file.

      For example:

      ```
      FROM_LOCATION="C:\Base_
      Download\Disk1\oms\Disk1\stage\products.xml"
      ```

   b. For the ORACLE_HOME parameter, specify the full path to the Oracle home directory of the OMS.

      For example:

      ```
      ORACLE_HOME="C:\OH102020\oms10g"
      ```

c. For the ORACLE_HOME_NAME parameter, specify the Oracle home name for OMS.

   For example:

   ```
   ORACLE_HOME_NAME="oms10g2"
   ```

d. For the s_agentHome parameter, specify the full path to the Oracle home directory of the Management Agent.

   For example:

   ```
   s_agentHome="C:\OH102020\agent10g"
   ```

e. For the s_agentHomeName parameter, specify the home name for Management Agent.

   For example:

   ```
   s_agentHomeName="agent10g2"
   ```

   **Note:** Ensure that the Oracle home location and the name you specify are not already existing.

7. Run the *setup.exe* file:

   ```
   C:\Patch_Download\cd\Disk1\install\setup.exe -ignoreDiskLabel
   -responseFile
   ```

   ```
   C:\Base_Download\Disk1\install\response\emnoseed.rsp
   ```

8. If the Management Agent does not restart, and if the value of agentTZRegion in the emd.properties file is *GMT*, then reset the time zone on the host where the Management Agent is installed using the following command. Here, Oracle_Home is the Oracle home directory of the Management Agent.

   ```
   <Oracle_Home>\BIN>emctl resetTZ agent
   ```

9. Patch OMS and Management Agent to 10.2.0.5.0 release.

   For patching instructions, see the Release Notes provided with the 10.2.0.5 patch set.

## 8.5 Installing an Additional Management Service

This section introduces you to the third installation type offered by OUI, that is, *Additional Management Service*. In particular, this section covers the following:

- Overview
- Scenarios
- Before You Begin
- Prerequisites
- Installation Procedure
- Installing an Additional Management Service on Microsoft Windows 2008 or Microsoft Vista
- Installing Additional Management Service in a 10.2.0.2 or 10.2.0.3 Environment

## 8.5.1 Overview

The third installation type, that is, *Additional Management Service*, installs an additional OMS to your existing Enterprise Manager Grid Control environment. This option is best suited when you already have Enterprise Manager Grid Control with a certified Oracle Database, and when you want to have another OMS for the following reasons:

- When you want to balance the load on the existing OMS
- When your existing OMS is running out of CPU or RAM resources

However, note that you can have multiple OMSes and still connect to just one Management Repository.

This installation type does the following:

- Installs Oracle Management Service 10g Release 2 *(Deployed in Oracle Application Server 10g Release 2 (10.1.2.0.2) that gets installed along with other core components)*
- Installs Oracle Management Agent 10g Release 2
- Configures the OMS and Management Agent

> **Note:** If you want to install an additional OMS to connect to Oracle Database 11g, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g".

The following describes the  installation process and software components that are installed for this installation type.

***Table 8–11 Installation Process for Installing Additional OMS***

| Sequence | Action | Component Installed/Configured | Description |
|---|---|---|---|
| 1 | Installation | Oracle Management Service 10g Release 2 | Technically, the installer installs an application server, that is, Oracle Application Server 10g Release 2 (10.1.2.0.2) where the OMS is deployed. In the specified installation directory, the installer creates a subdirectory for OMS and places the software binaries in it.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for OMS is:<br>`/scratch/OracleHome/oms10g` |
| 2 | Installation | Oracle Management Agent 10g Release 2 | In the specified installation directory, the installer creates a subdirectory for the Management Agent and places the software binaries in it. The subdirectory is agent10g.<br>For example, if the installation directory is /scratch/OracleHome, then the subdirectory created for the Management Agent is:<br>`/scratch/OracleHome/agent10g` |
| 3 | Configuration | All | The installer runs the Configuration Assistant tools to configure all the installed components. |

### 8.5.2 Scenarios

Before you proceed with the rest of the subsections in this section, let us understand the different scenerios under which you will install an additional OMS and what is the best installation procedure or approach to be adopted for each of the scenarios.

***Table 8–12 Additional OMS Installation Scenarios***

| Scenarios | Installation Approach | Reference Points |
|---|---|---|
| If you want to install an additional OMS in a complete 10.2.0.1 environment -- where the repository, the main OMS *(which comes along with the full installation of Enterprise Management Grid Control)*, and the other additional OMS are of 10.2.0.1 release. | Use the installer of the full release to install the 10.2.0.1 additional OMS. | Follow the installation instructions given in Section 8.5.5, "Installation Procedure". |
| If you want to install an additional OMS in an environment where the repository and the main OMS are of 10.2.0.2 or 10.2.0.3 release for Linux, or 10.2.0.3 release for Microsoft Windows. | **1.** Change the repository version to 10.2.0.1<br>**2.** Invoke the installer of the full release to install the 10.2.0.1 additional OMS<br>**3.** Change back the version of the repository to what it was, for example, 10.2.0.2<br>**4.** Install the additional OMS<br>**5.** Apply the patch set to migrate the additional OMS from 10.2.0.1 to the version of the repository | Follow the installation instructions given in Section 8.5.6, "Installing an Additional Management Service on Microsoft Windows 2008 or Microsoft Vista". |
| If you want to install an additional OMS in an environment where the repository and the main OMS are of 10.2.0.4 or higher release. | Install the additional OMS in a 'software-only' method, so that you only install the binaries immediately and configure it after it is patched to the higher release. | Follow the installation instructions given in Section 8.6, "Installing 'Software-Only' and Configuring Later". |

**Note:** If you want to install an additional OMS to connect to Oracle Database 11g, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g".

### 8.5.3 Before You Begin

Before you begin, keep these points in mind:

- This installation type installs the components only on a single host, and only on that host from where the OUI installation wizard is invoked, that is, from where the runinstaller or setup.exe file is invoked. Installation on multiple hosts and remote hosts is not supported.
- The default port for Enterprise Manager Grid Control is 4889 and the default port for Management Agent is 3872. For more information about the default ports that are assigned and the possibility of using custom ports instead of default ports, see Section 4.9, "Knowing About the Ports Used for Installation".

- Oracle offers code fixes for a product based on the *Oracle Lifetime Support Policy*. When the license period expires for a particular product, the support for code 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 Grid Control installation, you must consider Enterprise Manager Grid Control's framework components as well as the targets monitored by Enterprise Manager Grid Control. Oracle recommends keeping your Grid Control components and targets updated to the latest certified versions in order to receive code fixes without having to purchase an Extended Support license. For information about the certified combinations of Enterprise Manager Grid Control components and monitored targets, see *My Oracle Support* note.412431.1.

- If the Management Agent does not start up automatically when you restart the host, then do the following:

  **a.** Open the agentstup file from the Oracle home of the Management Agent:

  ```
  $ORACLE_HOME/install/unix/scripts/agentstup
  ```

  **b.** Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

  **c.** Run the root.sh script from the Oracle home of the Management Agent:

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

  **d.** Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

  > **Note:** This is a one-time action to be taken. Step (a) to Step (c) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

## 8.5.4 Prerequisites

Before installing an additional OMS, ensure that you meet the following prerequisites.

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

***Table 8–13 Prerequisites for Additional Oracle Management Service***

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the necessary hardware and software requirements for OMS.<br>For information about hardware and software requirements, see Section 3.1, "Hardware Requirements" and Section 3.3, "Software Requirements", respectively. | |

*Table 8–13 (Cont.) Prerequisites for Additional Oracle Management Service*

| Requirement | Description | Yes/No |
|---|---|---|
| Operating System Requirements | Check if the operating system of the host is certified.<br>For information about the supported operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |
| Package Requirements | Verify if the package requirements for each platform are met.<br>For information about packages to be installed for Management Agent, see Section D, "Platform-Specific Package and Kernel Requirements". | |
| Sufficient Physical Memory | Ensure there is sufficient physical memory available for this installation type. For information, see Section 8.1, "Understanding the Installation Types" and Section 3.1.1, "Recommended CPU and Memory Allocation". | |
| Permission Requirements for Installation Directory | Check if the installation directory, that is, the Oracle home directory is writable. | |
| Host List and Credentials Requirements | Identify the host where you want to install OMS, and obtain the credentials of that host so that it can be accessed for installation. | |
| Host Name Requirement | The host name must be a valid host name. For example, *serverhost1.company.com* or *serverhost1*.<br>However, it cannot be an IP address. At the same time, it cannot be localhost.localdomain as strings used in the /etc/hosts file.<br>At the time of invoking the installer, you can pass `ORACLE_HOSTNAME=<host_name> -local` as an argument. | |
| Installing User Requirements | The following are the requirements:<br>■ (UNIX only) The installation must NOT be run by the root user<br>■ User must be a DBA user<br>■ (Microsoft Windows only) User must be able to create process-level tokens<br>■ (Microsoft Windows only) User must be able to log in as a batch job<br>■ (Microsoft Windows only) User must be able to adjust memory quota for process<br>■ (Microsoft Windows only) User must be part of the ORA-DBA group and have administrator permissions | |
| Using the Same User Name, UID, GID | Use the same user name, uid, and gid as the ones used on the host where the first OMS was installed.<br>This is to ensure that both OMSes have access to the same, shared Oracle Software Library. For information about setting the user name, uid, and gid, see Section 8.5.4.1, "Using the Same User Name, UID, and GID". | |

*Table 8–13 (Cont.) Prerequisites for Additional Oracle Management Service*

| Requirement | Description | Yes/No |
|---|---|---|
| Installation Directory Requirements | If the specified *Installation Directory* already contains subdirectories that represent the components of Enterprise Manager Grid Control, then those subdirectories must be empty. If they are not, either delete them or keep them empty.<br>For example, if the specified *Installation Directory* already has <*install_dir/agent10g*> and <*install_dir/oms10g*> subdirectories, then they must be empty. | |
| Existing Oracle Database Requirements | Ensure that the existing Oracle Database is a certified database.<br>To view a list of certified Oracle Databases, see Document ID 412431.1 on My Oracle Support (formerly Metalink). If you want to use a RAC database, which is configured on a virtual host, as the existing database, then refer to My Oracle Support note 561441.1.<br>If you want to use Oracle Database 11g as the existing database, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g". | |
| Existing Oracle Database and Listener Status Requirements | Ensure that the existing, certified Oracle Database and Listener are running. | |
| Password Verification Requirements | Ensure that the profile of the Password Verification resource name has the "Default" value. If the Password Verification is enabled, repository creation may fail. | |
| NLS_LANG Environment Variable Requirements | If your operating system is Linux, then ensure the NLS_LANG environment variable is set with a value that is compatible with the operating system default locale setting and the Management Repository database character set.<br>For information on the specific values for language, territory, or character set, refer to the Globalization Support Guide of the Oracle product that you are using. | |
| Management Repository Requirements | Ensure that the existing Oracle Database is already configured with Oracle Management Repository 10g Release 2. | |
| Management Repository *emkey* Requirements | Ensure that the Management Repository has the emkey for securing OMS.<br>If the emkey is not present in the repository, then you may be prompted with a message to run a command before proceeding any further. The command mentioned in the message is incorred. Instead, restart the database, copy `emkey.ora` into `/OH/sysman/config`, and then run the following command:<br>`ORACLE_HOME/bin/emctl config emkey -copy_to_repos` | |
| Targets Monitored | Remember that Enterprise Manager Grid Control will be able to monitor only those targets that are monitored by the Management Agent installed by the same user. | |

#### 8.5.4.1 Using the Same User Name, UID, and GID

If you are installing an additional OMS on another host that will access the same, shared Oracle Software Library as the one used by the first OMS on the first host then ensure that you install the additional OMS using **the same user name** as the one used on the first host. Also ensure that you use **the same uid and gid**. This is to ensure that both the OMSes have access to the same Oracle Software Library.

### Setting UID and GID Before Installing an Additional OMS

To use the same uid and gid, do these before installing the additional OMS:

1. Run the "id" command to check the uid and gid on both the computers, one where OMS is already installed and another where you are going to install the additional OMS.
2. Decide on which computer the uid and gid need to be changed. On that computer, run the following commands to open the /etc/passwd file as root:

   ```
   sudo -s
   vi /etc/passwd
   ```

3. Set the uid (third column) and gid (fourth column) as the ones used in the first computer.
4. Save the file.
5. Open a new terminal, login as root, and run the following command to change the ownership of the directories:

   ```
   chown <username>:<groupname> -R <directory name>
   ```

6. Open a new terminal, login as the OMS user, and run the "id" command to verify that the uid and gui have changed.
7. If the changes are reflected, you can start the installation of the additional OMS.

### Setting UID and GID After Installing an Additional OMS

If you have already installed the additional OMS on the second computer before making the UID and GID settings, then do these:

1. Run the "id" command to check the uid and gid on both the computers where OMS is already.
2. Decide on which computer the uid and gid need to be changed. On that computer, stop or kill all the OMS-related processes.
3. Run the following commands to open the /etc/passwd file as root:

   ```
   sudo -s
   vi /etc/passwd
   ```

4. Change the uid (third column) and gid (fourth column) as the ones used in the first computer.
5. Save the file.
6. Now logout from the OMS that is running on this computer and re-login to ensure that the changes are reflected.
7. Open a new terminal, login as root, navigate to the OMS ORACLE_HOME (for example, /scratch/oms10203), and run the following command to change the ownership of the directories:

   ```
   chown <username>:<groupname> -R <directory name>
   ```

8. Open a new terminal, login as the OMS user, and run the "id" command again to verify that the uid and gui have changed.

9. In parallel, open a new terminal and access the other computer where the first OMS and the shared Oracle Software Library are present. Login to the first OMS as root and navigate to the shared Oracle Software Library directory.

   For example, if you the shared location is /net/OMS1/scratch/swlib, then run the following command:

   ```
   cd /scratch/swlib
   ```

10. Run the following commands to change the ownership of this shared Oracle Software Library directory:

    ```
    chown <username>:<groupname> -R <software library directory>
    ```

11. Now return to the second computer where the additional OMS is installed and start all the OMS-related processes that you had stopped.

> **Note:** If the shared Oracle Software Library is present on a different host, say other than the ones where the first OMS and second OMS are installed, then do these on that host:
>
> 1. Create a user that is the same as the user name used on hosts where the first OMS and the second OMS are installed.
> 2. Change the uid and gid as described from Step 1 to Step 8.
> 3. Change the ownership of this shared software library folder as described in Step 10.

## 8.5.5 Installation Procedure

This section explains how you can install a full, base release of OMS, which is part of Enterprise Manager 10g Grid Control Release 2 or higher. For details about full, base releases and what these installation instructions can be use for, see Section 4.1, "Understanding What This Guide Helps You Install and Upgrade".

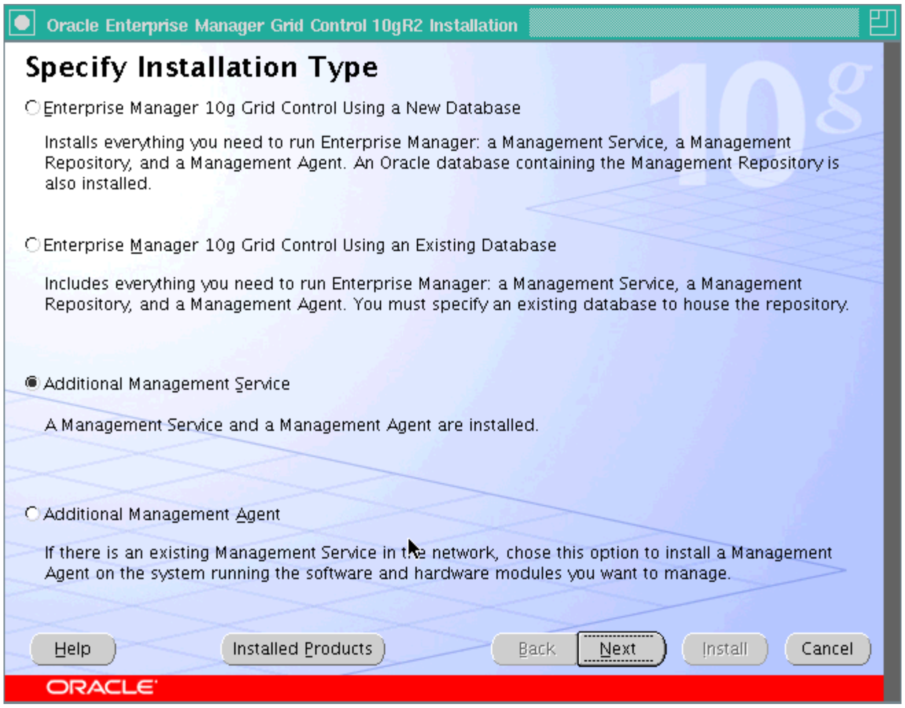
This option is best suited particularly when you want to install an additional OMS in a complete 10.2.0.1 environment -- where the repository, the main OMS (which comes along with the full installation of Enterprise Management Grid Control), and the other additional OMS are of 10.2.0.1 release. To understand the other installation scenarios, see Section 8.5.2, "Scenarios". Identify the environment that matches with the one described in that section.

> **Note:** If you want to install an additional OMS using Oracle Database 11g, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g".

To install an additional OMS, follow these steps:

1. Start Oracle Universal Installer by running the `runInstaller` script (`<DVD>/runInstaller` on Linux and `/DVD/setup.exe` on Microsoft Windows) from the top directory of the DVD.
2. In the Specify Installation Type screen, select the third option (**Additional Management Service**).

***Figure 8–17 Specify Installation Type***



Oracle Enterprise Manager Grid Control 10gR2 Installation

Specify Installation Type

○ Enterprise Manager 10g Grid Control Using a New Database

Installs everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. An Oracle database containing the Management Repository is also installed.

○ Enterprise Manager 10g Grid Control Using an Existing Database

Includes everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. You must specify an existing database to house the repository.

● Additional Management Service

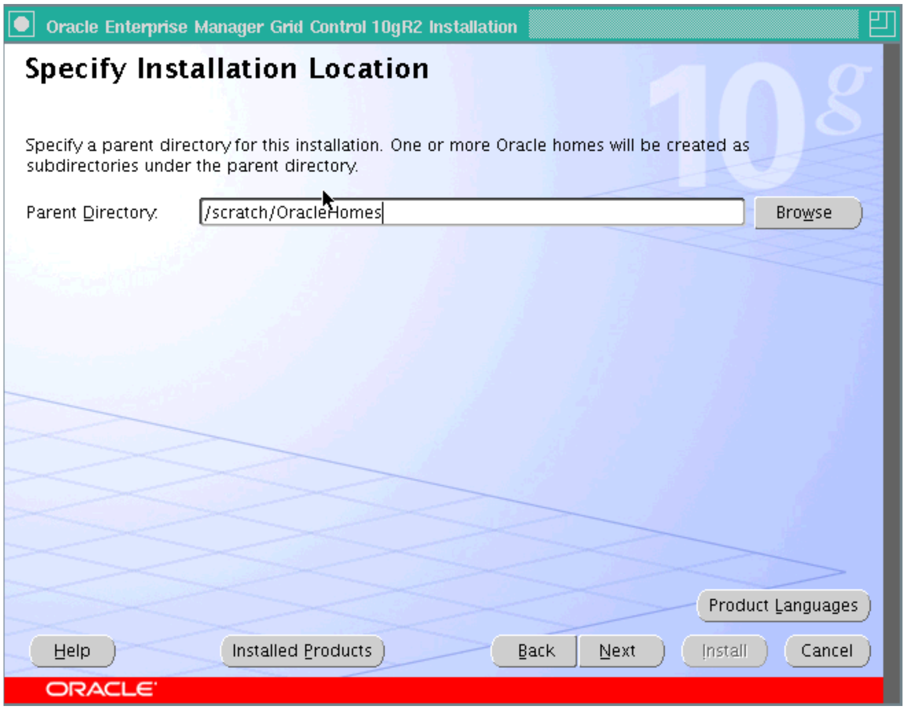
A Management Service and a Management Agent are installed.

○ Additional Management Agent

If there is an existing Management Service in the network, chose this option to install a Management Agent on the system running the software and hardware modules you want to manage.

3. In the Specify Installation Location screen, specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. The OMS home created during the installation is placed as a sub-directory under this parent directory. For example: `oms10g`.

***Figure 8–18 Specify Installation Location***



Oracle Enterprise Manager Grid Control 10gR2 Installation

Specify Installation Location

Specify a parent directory for this installation. One or more Oracle homes will be created as subdirectories under the parent directory.

Parent Directory: /scratch/OracleHomes

> **Note:** Ensure you do not use symbolic links to specify the Oracle home path.

The installer by default installs the selected products in the English language.

a. If you want to install the product in a different language, click **Product Languages**.

b. The Language Selection screen is displayed. Make the required language selections here. See Figure 8–3, "Language Selection" for details.

4. Click **Next**. The Product Specific Prerequisites Check screen appears.

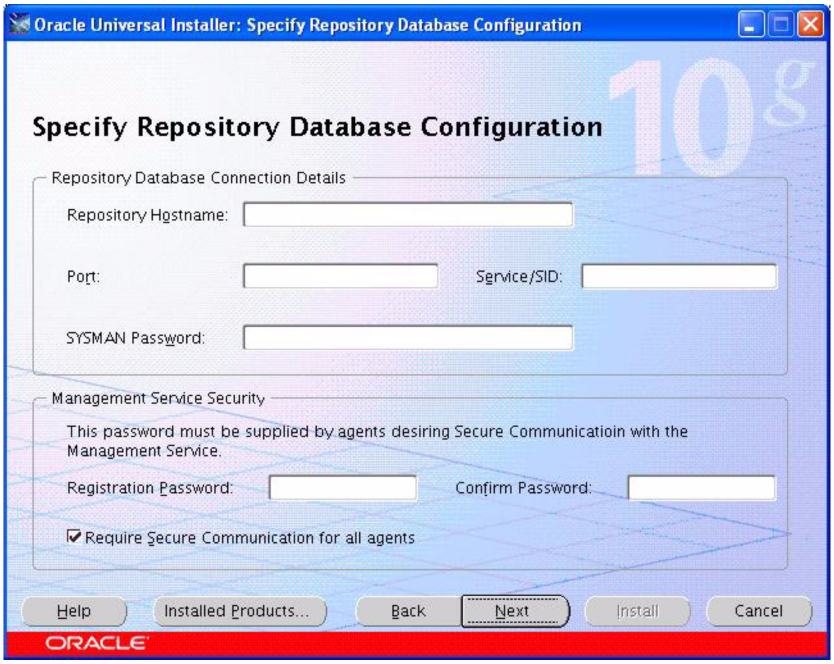
   This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

   Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen. See Figure 8–5, "Product-Specific Prerequisite Checks" for more information.

   > **Note:** You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information on running these prerequisite checks in standalone mode, see Section 4.16, "Running the Prerequisite Check in Standalone Mode".

5. Click **Next**. The Specify Repository Database Configuration screen appears.

*Figure 8–19 Specify Repository Database Configuration*



Specify Repository Database Configuration

This password must be supplied by agents desiring Secure Communicatioin with the Management Service.

☑ Require Secure Communication for all agents

**a.** You must configure the additional OMS to establish the connections with the existing Management Repository.

---

**Note:** The existing Management Repository database must be one of the following releases:

- Oracle Database 10*g* Release 1 (10.1.0.4), Enterprise Edition
- Oracle Real Application Clusters 10*g* Release 1 (10.1.0.4)
- Oracle9*i* Database Release 2 (9.2.0.6 and later), Enterprise Edition
- Oracle9*i* Real Application Clusters Release 2 (9.2.0.6 and later)

The Management Repository database may also require patches to be applied, prior to successful installation. See Section 3.2, "Operating System, Browser, Target Certification" for more information.

---

**b.** In the Repository Database Connection Details section, specify a fully qualified host name on which the Management Repository database is installed, the repository port, and the SID (system identifier) for the database instance.

The SID identifies a specific Oracle database and distinguishes it from other databases on the computer.

---

**Note:** When selecting an existing cluster database for creating a Management Repository, you must replace the SID value with the Management Service name.

---

**c.** Enter the password for the SYSMAN user (the default Super Administrator account for Grid Control).

d. In the Management Service Security section, specify the password used to secure and lock the OMS.

e. Select **Require Secure Communications for all agents** if you want the secure OMS to communicate only with Secure Agents. This is optional, though recommended.

For example, if you have 10*g* R1 (10.1.n) agents in the Grid environment, and you have secured the OMS and selected the **Require Secure Communications** option, then all communication between the Oracle Management Service 10*g* R2 (10.2) and Oracle Management Agent 10*g* R1 (10.1) fails (because these agents have not been secured).

To secure Management Agent, run the following command from the Management Agent Oracle home of that particular target. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

```
emctl secure agent
```

See the section Password Restrictions and Recommendations in this chapter for more information.

---

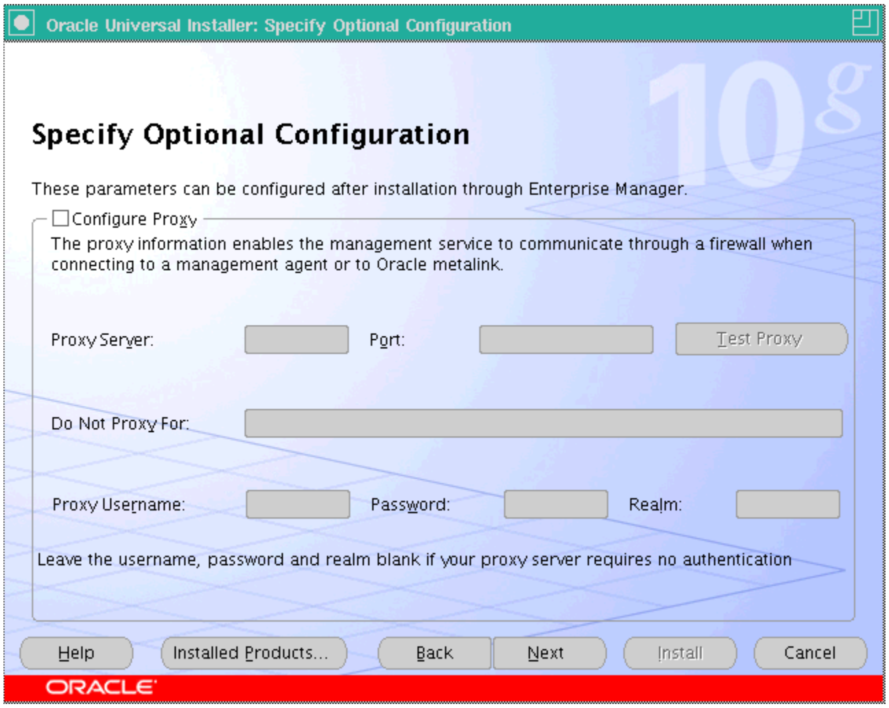
**Note:** The password that you specify here must be the same as the password that you specified to secure the OMS.

Ensure that all OMS instances using the same repository must use the same secure password.

---

6. Click **Next**. The Specify Optional Configuration screen appears.

*Figure 8–20 Specify Optional Configuration*



Oracle Universal Installer: Specify Optional Configuration

Specify Optional Configuration

These parameters can be configured after installation through Enterprise Manager.

□ Configure Proxy

The proxy information enables the management service to communicate through a firewall when connecting to a management agent or to Oracle metalink.

Proxy Server: Port:

Do Not Proxy For:

Proxy Username: Password: Realm:

Leave the username, password and realm blank if your proxy server requires no authentication

As the name suggests, all the fields on this screen are optional, and are disabled, by default. Select the required check box to enable the corresponding fields.

a. Select the Configure Proxy check box (optional) if Grid Control is using a proxy server for external access. Specify the properties for the proxy server host name (enter a fully qualified host name), port number, Do Not Proxy for list, and the Proxy user credentials. See Table 8–4, " Specify Proxy information - Input Fields" for a description of the input fields.

b. Specify an appropriate **Realm** value. This becomes a mandatory field only if the proxy server credentials have been configured using a Realm, in which case, you must specify an appropriate Realm value.

   A Realm is a string value that is assigned by the proxy server to indicate the secure space that requires authentication.

7. Click **Next**. The Summary screen appears.

   This screen displays a summary of the options that you have selected during the installation process. Depending on the installation type, this screen displays any or all of the following details:

   - Global Settings
   - Product Languages
   - Space Requirements
   - New Installations

   For more information on each of the previously listed details, see the Grid Control online Help.

   Verify the choices that you have made and click **Install** to start the installation. The installer begins installing the selected Oracle product.

8. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only for Linux). Refer to Figure 8–12, "Execute Configuration Scripts".

   a. To execute these scripts, go to the computer window, log in as `root` and run these configuration scripts.

   b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the recommended configuration tools.

   This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. Refer to Table 8–6, " Grid Control Configuration Tools" to see the list of configuration tools that are run. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

10. To complete the postinstallation configurations, log in as root (in a new terminal) and run the allroot.sh script from the Oracle home directory of the OMS (oms10g).

    For example,

```
<OMS ORACLE HOME>/allroot.sh
```

11. After successfully running all the recommended configuration tools, click **Next**. The **End of Installation** screen appears.

    This screen tells you whether or not the installation was successful and displays some important information that you must remember about the product you have installed. For example, it might contain information about the URLs for particular Web applications.

> **Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:
>
> 1. Open the agentstup file from the Oracle home of the Management Agent:
>
>    ```
>    $ORACLE_HOME/install/unix/scripts/agentstup
>    ```
>
> 2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
> 3. Run the root.sh script from the Oracle home of the Management Agent:
>
>    ```
>    $<ORACLE_HOME>/root.sh
>    ```
>
> 4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:
>
>    ```
>    $<ORACLE_HOME>/bin/emctl start agent
>    ```
>
>    This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

### 8.5.6 Installing an Additional Management Service on Microsoft Windows 2008 or Microsoft Vista

To install an additional OMS on Microsoft Windows 2008 or Microsoft Vista, follow these steps:

1. Download patch# 6640752 for Microsoft Windows (32-Bit) from My Oracle Support. You can access My Oracle Support at:

   `http://metalink.oracle.com`

2. Extract the contents of the downloaded patch to a location on your system.

   For example: `C:\Patch_Download`

3. Download the base release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.2.0) for Microsoft Windows.

4. Extract the contents of the downloaded base release to a location on your system. For example, `C:\Base_Download`

5. Edit the response file and make changes as described in this step.

   The response file is available at:

   ```
   C:\Base_Download\Disk1\install\response\oms.rsp
   ```

   Make the following changes:

   a. For the FROM_LOCATION parameter, specify the full path to the `products.xml` file.

      For example:

      ```
      FROM_LOCATION="C:\Base_
      Download\Disk1\oms\Disk1\stage\products.xml"
      ```

b. For the ORACLE_HOME parameter, specify the full path to the Oracle home directory of the OMS.

   For example:

   ```
   ORACLE_HOME="C:\OH102020\oms10g"
   ```

c. For the ORACLE_HOME_NAME parameter, specify the Oracle home name for OMS.

   For example:

   ```
   ORACLE_HOME_NAME="oms10g2"
   ```

d. For the s_agentHome parameter, specify the full path to the Oracle home directory of the Management Agent.

   For example:

   ```
   s_agentHome="C:\OH102020\agent10g"
   ```

e. For the s_agentHomeName parameter, specify the home name for Management Agent.

   For example:

   ```
   s_agentHomeName="agent10g2"
   ```

   **Note:** Ensure that the Oracle home location and the name you specify are not already existing.

6. Run the *setup.exe* file:

   ```
   C:\Patch_Download\cd\Disk1\install\setup.exe -ignoreDiskLabel
   -responseFile
   ```

   ```
   C:\Base_Download\Disk1\install\response\oms.rsp
   ```

7. If the Management Agent does not restart, and if the value of agentTZRegion in the emd.properties file is *GMT*, then reset the time zone on the host where the Management Agent is installed using the following command. Here, Oracle_Home is the Oracle home directory of the Management Agent.

   ```
   <Oracle_Home>\BIN>emctl resetTZ agent
   ```

8. Patch OMS and Management Agent to 10.2.0.5.0 release.

   For patching instructions, see the Release Notes provided with the 10.2.0.5 patch set.

### 8.5.7 Installing Additional Management Service in a 10.2.0.2 or 10.2.0.3 Environment

> **Note:** The steps outlined in this section describe how you can install an additional OMS in an environment where the repository and the main OMS are of 10.2.0.2 or 10.2.0.3 release for Linux, or 10.2.0.3 release for Microsoft Windows.
>
> If you want to install an additional OMS in an environment where the repository is of 10.2.0.4 or higher release, then see Section 8.6, "Installing 'Software-Only' and Configuring Later".
>
> If you want to install an additional OMS using Oracle Database 11g, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g".

To install an additional OMS, follow these steps:

1. Convert the repository version to 10.2.0.1.0 by using the following SQL statement:

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0' where
   component_name='CORE'; commit;
   ```

2. Invoke the installer from the 10.2.0.1.0 DVD and choose the *Additional Management Service* option.

3. Provide the repository credentials for the Specify Database Configuration Screen and click **Next**, then stop here. (Do not proceed with the install.)

4. Go to the database Oracle Home where the repository is available, and connect to the database through SQLplus.

5. Update the repository version back to what is was, that is, 10.2.0.2.0 or 10.2.0.3.0, by using the following sql statement (This code sample given below uses 10.2.0.3.0 as an example):

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.3.0' where
   component_name='CORE'; commit;
   ```

6. Return to the installer and click **Next** to proceed with the installation from where you stopped.

7. Once the installation of the base OMS (10.2.0.1 on Linux or 10.2.0.2 on Microsoft Windows) is complete, both the Management Agent and the OMS must be shut down immediately by running the following command:

   ```
   <Agent Oracle Home>/bin/emctl stop agent
   ```

   ```
   <OMS Oracle Home>/opmn/bin/opmnctl stopall
   ```

8. Patch the OMS to 10.2.0.2 or 10.2.0.3 using the 10.2.0.2 or 10.2.0.3 patch set, respectively. Refer to the Patch Set Notes that is supplied with the patch set to understand how the OMS can be patched.

9. Once the OMS has been patched successfully to 10.2.0.2 or 10.2.0.3, it will start automatically.

10. Restart the Management Agent from the Oracle Home:

    ```
    <Agent Oracle Home>/bin/emctl/start agent
    ```

## 8.6 Installing 'Software-Only' and Configuring Later

This section introduces you to the *Install Software-Only* installation type that can be used to install only the software binaries without configuring the installation. This installation type is not part of the OUI.

This section covers the following:

- Overview
- Installing 'Software-Only' and Configuring Later (Silent Mode)
- Installing 'Software-Only' and Configuring Later (GUI Mode)
- Installing 'Software-Only' and Configuring Later (Silent Mode) on Newly Supported Platforms

### 8.6.1 Overview

The 'Installing Software-Only and Configuring Later' installation method allows you to install only the software binaries of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux and 10.2.0.2 for Microsoft Windows), that is, without any configuration to the installation, and move over to the latest patch set version.

This saves time and effort, and is best suited when you are installing Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or higher **for the first time** in your environment. Since Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or higher are patch sets, you need to have a base installation to patch it. Using the 'Installing Software-Only and Configuring Later' installation method, **you can install only the software of the base release and then configure it later by applying the latest patch set (10.2.0.4 or higher)**.

This installation option is also best suited for the following cases:

- When you want to use your existing Oracle Database 10g Release 2 (10.2.0.3 or higher) to house the Management Repository, as this release of database is supported only with Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or higher.
- When you want to install Enterprise Manager Grid Control on newly supported platforms. For example, SUSE Linux Enterprise Server 10 is a new platform that is supported by Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).
- When you want to install Grid Control during the Daylight Savings Time (DST) period. This option helps you install only the software binaries of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1), and migrate to the latest patch set release (10.2.0.4 or higher) directly that has the fix for DST-related issues.

**IMPORTANT:**

- The 'Installing Software-Only and Configuring Later' installation method is supported only by Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or higher.
- **Do NOT use this method to patch or upgrade any existing, previous release** of Grid Control. For example, if you already have Enterprise Manager 10g Grid Control Release 3 (10.2.0.3), then do NOT use this method to patch or upgrade to a higher release.
- On Microsoft Windows, do the following:

  Replace ./runInstaller with setup.exe and run the command.

  Ensure that the environment variable PATH has the value `%SystemRoot%\system32;%SystemRoot%` . To set it, in Windows Explorer, right-click on **My Computer**, select **Properties**. On the Advanced tab, click **Environment Variables**. On the Environment Variables dialog, in the System Variables pane, check for the variable PATH. Click **Edit** to specify the required variable value.

## 8.6.2 Installing 'Software-Only' and Configuring Later (Silent Mode)

This section describes how you can perform the following in silent mode:

- Installing Enterprise Manager Grid Control Using a New Database
- Installing Enterprise Manager Grid Control Using an Existing Database
- Installing Additional Management Service
- Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g
- Installing Additional Management Service Using Existing Oracle Database 11g

### 8.6.2.1 Installing Enterprise Manager Grid Control Using a New Database

To install Grid Control using a new database, follow these steps:

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

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

2. Install the base release of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux or 10.2.0.2 for Microsoft Windows) using the following command:

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig -silent -responseFile <absolute_
   path>/em_with_new_db.rsp -force
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe  -noconfig -silent -responseFile <absolute_
   path>/em_with_new_db.rsp -force
   ```

**Note:**

- The em_with_new_db.rsp file is packaged with Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.4 of Chapter 9, "Installing Enterprise Manager Grid Control in Silent Mode".
- If you want to specify different passwords for the database accounts, then ensure that the following entry is added to the em_with_new_db.rsp file:

  ```
  sl_superAdminUsers={ "SYS" , "SYSTEM" , "SYSMAN" ,
  "DBSNMP" }
  ```
- Use the -force command only when you want to install in an existing, nonempty directory.

3. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the following scripts on the host where you installed the base release of Grid Control.
   - If this is the first Oracle product you just installed on the host, then run the oraInstroot.sh script from the Central Inventory:

     ```
     $ORACLE_HOME/oraInventory/oraInstRoot.sh
     ```
   - Run the allroot.sh script from the Oracle home directory of the database (for example, db10g):

     ```
     $<ORACLE_HOME>/allroot.sh
     ```
4. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```
5. Apply 10.2.0.4 or higher patch set to OMS:

   **Note:** You can download the 10.2.0.4 or higher patch set from the following location:

   http://www.oracle.com/technology/software/products/oem/index.html

   For each patch set, you might have to download either a single ZIP file or multiple ZIP files. If you have to download more than one ZIP file, then extract the contents of the ZIP files into one directory. For more information about these ZIP files and how you can extract them, see the README file associated with the patch set.

   a. Copy the patchset.rsp file from the <Patchset_Download_Location>/response/ directory to a location on your host.

   b. Edit the patchset.rsp file and make the following changes:

   **For 10.2.0.4.0 Release:**

   ```
   b_softwareonly = true
   s_sysPassword  = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   ```

**For 10.2.0.5.0 or Higher Release:**

```
b_softwareonly = true
s_sysPassword  = <sys user password>
ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
```

---

**Note:**

- The `patchset.rsp` file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.
- The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

  ```
  oracle.iappserver.st_midtier:szl_
  InstanceInformation={"welcome1"}
  ```

---

c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <absolute_
path>/patchset.rsp -force
```

---

**Note:** Use the `-force` command only when you want to install in an existing, nonempty directory.

---

6. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run `root.sh`.
7. Apply 10.2.0.4 or higher patch set to the Management Agent:

a. Copy the `patchset.rsp` file from the `<Patch Set DVD>/response/` directory to a location on your host.

b. Edit the `patchset.rsp` file and make the following changes:

```
ORACLE_HOME = <full_path_to_Oracle_home_of_Agent>
```

c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <absolute_
path>/patchset.rsp -force
```

---

**Note:** Use the `-force` command only when you want to install in an existing, nonempty directory.

---

8. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run `root.sh`.

9. (For Solaris Platforms Only), check the platform ID in the following file of the Oracle home directory of the database (for example, db10g). Ensure that the platform ID is set to 23. If it is not, then change it to 23.

   ```
   $<ORACLE_HOME>Inventory/ContentsXML/oraclehomeproperties.xml
   ```

10. Apply the interim RDBMS patch# 4329444 to the Oracle home directory of the database (for example, db10g) that houses the Management Repository.

11. (ONLY FOR 10.2.0.4.0 RELEASE) Apply patch# 7040389 to the Oracle home directory of the OMS (for example, oms10g).

12. Ensure that the `runConfig.sh` file in the Oracle home directory of the database (for example, db10g) has 'execute' permission.

    ```
    $<ORACLE_HOME>/oui/bin/runConfig.sh
    ```

13. After applying the patch, make the following settings to the environment variable - PERL5LIB:

    a. Before making changes to the environment variable, take a backup of the variable:

       For UNIX Platforms:

       ```
       setenv PERL5LIB_BACKUP $PERL5LIB
       ```

       For Microsoft Windows Platforms:

       ```
       set PERL5LIB_BACKUP=%PERL5LIB%
       ```

    b. Now make the following settings to the environment variable:

       For UNIX platforms, set it to <*OMS_ORACLE_HOME*>/perl/lib/5.6.1

       For Microsoft Windows platforms, set it to <*OMS_ORACLE_HOME*>/perl/5.6.1/lib

14. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

15. After the script runs successfully, Grid Control is configured to 10.2.0.4 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

- Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

> **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command from the Oracle home directory of the OMS:
>
> ```
> emctl secure unlock -console
> ```

16. If the script fails, then review the database configuration log file. The database configuration log file is available in `<DB_ORACLE_HOME>/cfgtoollogs/cfgfw`. Scan through the logs to see if you have the following error message:

```
The installer has detected that there are background dbms jobs currently
running in the Repository Database.
```

> **Note:** For Agent configuration logs, go to `<AGENT_ORACLE_HOME>/cfgtoollogs/cfgfw`. For OMS configuration logs, go to `<OMS_ORACLE_HOME>/cfgtoollogs/cfgfw`.

If you see the error message, then before upgrading the Management Repository, do the following:

a. Stop the running DBMS jobs by logging in to SQL as SYSDBA and running the following command:

```
SQL> exec sysman.emd_maintenance.remove_em_dbms_jobs;
```

b. Stop and restart the database.

c. Check the status of SYSMAN user account:

- Log in to SQLPlus as SYSDBA and run the following query:

```
select username,account_status from dba_users;
```

- Ensure that the SYSMAN user account is in 'open' status. If the account is not in open status, then run the following command:

```
alter user SYSMAN account unlock;
```

- Commit the changes by running the following command:

```
commit;
```

d. Rerun the `ConfigureGC.pl` script.

e. After installation is complete, restart the DBMS jobs by running the following commands, one after the other:

```
SQL> exec sysman.emd_maintenance.submit_em_dbms_jobs;
```

```
SQL> commit;
```

#### 8.6.2.2 Installing Enterprise Manager Grid Control Using an Existing Database

> **Caution:** The steps outlined in this section describe how you can install Enterprise Manager Grid Control using an existing database. Ensure that your existing database is one of the certified databases supported by Enterprise Manager 10g Grid Control. To see a list of certified databases, see Document ID 412431.1 on My Oracle Support (formerly Metalink).
>
> Access My Oracle Support at the following URL, select **Document ID** from the **Quick Find** menu, quote the document number, and click **GO** to view the document:
>
> `http://metalink.oracle.com/`
>
> If you want to use Oracle Database 11g as the existing database, then see Section 8.6.2.4, "Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g".

To install Grid Control using an existing database, follow these steps:

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

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

2. If your existing database is configured with Database Control, then ensure that you deconfigure it before you begin the installation of Grid Control.

   To deconfigure Database Control for a single instance database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop
   ```

   To deconfigure Database Control for a Real Application Clusters (RAC) database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop -
   cluster
   ```

   After deconfiguring the Database Control, connect to the database as SYS user and run the following SQL files from the Oracle home of the database:

   ```
   <ORACLE_HOME>/rdbms/admin/dbmspool.sql
   ```

   ```
   <ORACLE_HOME>rdbms/admin/prvtpool.plb
   ```

**Note:** The command drops all the public synonyms starting with the following names created by any user for any schema:

- 'MGMT$%'
- 'MGMT_%'
- 'SMP_EMD%'
- 'SMP_MGMT%'
- 'SETEMVIEWUSERCONTEXT'
- 'DBMS_SHARED_POOL'
- 'EMD_MNTR'
- 'ECM_UTIL'

3. Ensure that the database initialization parameters have the correct values to create a Management Repository in the database.

   For information about the initialization parameters to be edited and the values to be provided, see Section 8.4.3.1, "Check Database Initialization Parameters".

   **Note:** If you do not set the database initialization parameters, the installation will fail and you will find the error message "OUI-10155:Error" in the following log file:

   ```
   <DB_HOME>/cfgtoollogs/cfgfw/installActions<time_
   stamp>.log
   ```

   To resolve it, set the parameters with correct values as given in Section 8.4.3.1, "Check Database Initialization Parameters", deinstall the failed Oracle homes, and then restart the installation.

4. Log in to the database as SYSDBA and run the following command:

   ```
   @?/rdbms/admin/dbmspool.sql
   ```

   ```
   commit;
   ```

5. Install the base release of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux or 10.2.0.2 for Microsoft Windows) using the following command:

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig -silent -responseFile <absolute_
   path>/em_using_existing_db.rsp -force
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe  -noconfig -silent -responseFile <absolute_
   path>/em_using_existing_db.rsp -force
   ```

---

**Note:**

- The `em_using_existing_db.rsp` file is packaged with Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.5 of Chapter 9, "Installing Enterprise Manager Grid Control in Silent Mode".
- Use the `-force` command only when you want to install in an existing, nonempty directory.

---

6. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

7. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

8. Apply 10.2.0.4 or higher patch set to OMS:

   ---

   **Note:** You can download the 10.2.0.4 or higher patch set from the following location:

   http://www.oracle.com/technology/software/products/oem/index.html

   For each patch set, you might have to download either a single ZIP file or multiple ZIP files. If you have to download more than one ZIP file, then extract the contents of the ZIP files into one directory. For more information about these ZIP files and how you can extract them, see the README file associated with the patch set.

   ---

   a. Copy the `patchset.rsp` file from the `<Patchset_Downloaded_Location>/response/` directory to a location on your host.

   b. Edit the `patchset.rsp` file and make the following changes:

   **For 10.2.0.4.0 Release:**

   ```
   b_softwareonly = true
   s_sysPassword  = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   ```

   **For 10.2.0.5.0 or Higher Release:**

   ```
   b_softwareonly = true
   s_sysPassword  = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
   ```

> **Note:**
>
> - The `patchset.rsp` file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.
> - The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:
>
> ```
> oracle.iappserver.st_midtier:szl_
> InstanceInformation={"welcome1"}
> ```

c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <exact_
path>/patchset.rsp
```

9. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run `root.sh`.
10. (ONLY FOR 10.2.0.4.0 RELEASE) Apply the following patches depending on how the database, which houses the Management Repository, is configured:
    - If the database is configured on a virtual host, then apply patch# 5667255 to the Oracle home directory of the OMS.
    - If the database is NOT configured on a virtual host, then apply patch# 7040389 to the Oracle home directory of the OMS
11. Apply 10.2.0.4 or higher patch set to the Management Agent:

    a. Copy the `patchset.rsp` file from the `<Patch Set DVD>/response/` directory to a location on your host.

    b. Edit the `patchset.rsp` file and make the following changes:

    ```
    ORACLE_HOME = <full_path_to_Oracle_home_of__Agent>
    ```

    c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

    ```
    ./runInstaller -noconfig -silent -responseFile <absolute_
    path>/patchset.rsp -force
    ```

    > **Note:** Use the `-force` command only when you want to install in an existing, nonempty directory.

12. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run `root.sh`.
13. After applying the patch, make the following settings to the environment variable - PERL5LIB:

a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

   For UNIX Platforms:

   ```
   setenv PERL5LIB_BACKUP $PERL5LIB
   ```

   For Microsoft Windows Platforms:

   ```
   set PERL5LIB_BACKUP=%PERL5LIB%
   ```

b. Now make the following settings to the variable:

   For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

   For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib

14. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

15. After the script runs successfully, Grid Control is configured to 10.2.0.4 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

    **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:

    ```
    emctl secure unlock -console
    ```

16. If the script fails, then look at the OMS configuration log file. The OMS configuration log file is available in `<OMS_ORACLE_HOME>/cfgtoollogs/cfgfw`. Scan through the logs to see if you have the following error message:

    ```
    The installer has detected that there are background dbms jobs currently
    ```

```
running in the Repository Database.
```

> **Note:** For Agent configuration logs, go to `<AGENT_ORACLE_HOME>/cfgtoollogs/cfgfw`. For Database configuration logs, go to `<DB_ORACLE_HOME>/cfgtoollogs/cfgfw`.

If you see the error message, then before upgrading the Management Repository, do the following:

a. Stop the running DBMS jobs by logging in to SQL as SYSDBA and running the following command:

   ```
   SQL> exec sysman.emd_maintenance.remove_em_dbms_jobs;
   ```

b. Stop and restart the database.

c. Check the status of SYSMAN user account:

   - Log in to SQLPlus as SYSDBA and run the following query:

   ```
   select username,account_status from dba_users;
   ```

   - Ensure that the SYSMAN user account is in 'open' status. If the account is not in open status, then run the following command:

   ```
   alter user SYSMAN account unlock;
   ```

   - Commit the changes by running the following command:

   ```
   commit;
   ```

d. Rerun the `ConfigureGC.pl` script.

e. After installation is complete, restart the DBMS jobs by running the following commands, one after the other:

   ```
   SQL> exec sysman.emd_maintenance.submit_em_dbms_jobs;
   ```

   ```
   SQL> commit;
   ```

#### 8.6.2.3 Installing Additional Management Service

> **Caution:** The steps outlined in this section describe how you can **install an additional OMS in an environment where the repository and the main OMS are of 10.2.0.4 or higher release**. The main OMS refers to the one that was installed with the first installation of Grid Control. If you want to install an additional OMS in a 10.2.0.3 or 10.2.0.2 environment, then see Section 8.5.2, "Scenarios" to understand the approach to be adopted.
>
> Also, this installation method is only for new, additional OMS to be installed. If you already have an OMS of a lower release, then the only way to upgrade it is to patch it using the Patch Set.
>
> If you want to install an additional

To install an additional OMS, follow these steps:

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

http://www.oracle.com/technology/software/products/oem/index.html

2. Ensure that the database, which houses the repository, and its listener are running.

3. Log in to the database as SYSDBA user and convert the repository version from 10.2.0.4.0 or higher to 10.2.0.1.0 by running the following SQL statement:

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0' where
   component_name='CORE'; commit;
   ```

4. Invoke the installer of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1):

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig -silent -responseFile additional_
   mgmt_service.rsp
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe -noconfig -silent -responseFile additional_mgmt_
   service.rsp
   ```

   > **Note:** The `additional_mgmt_service.rsp` file is packaged with Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.6 of Chapter 9, "Installing Enterprise Manager Grid Control in Silent Mode".

5. Log in to the database again as SYSDBA user and convert the repository version back to what is was, that is, 10.2.0.4.0 or higher, by using the following SQL statement. The following SQL statement uses 10.2.0.4.0 as an example; therefore, it you are installing a higher release, then replace it with that release number.

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.4.0' where
   component_name='CORE'; commit;
   ```

6. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

7. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

8. Apply 10.2.0.4 or higher patch set to OMS:

**Note:** You can download the 10.2.0.4 or higher patch set from the following location:

http://www.oracle.com/technology/software/products/oem/index.html

For each patch set, you might have to download either a single ZIP file or multiple ZIP files. If you have to download more than one ZIP file, then extract the contents of the ZIP files into one directory. For more information about these ZIP files and how you can extract them, see the README file associated with the patch set.

a. Copy the `patchset.rsp` file from the `<Patchset_Downloaded_Location>/response/` directory to a location on your host.

b. Edit the `patchset.rsp` file and make the following changes:

   **For 10.2.0.4.0 Release:**

```
b_softwareonly = true
s_sysPassword  = <sys user password>
ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
```

   **For 10.2.0.5.0 or Higher Release:**

```
b_softwareonly = true
s_sysPassword  = <sys user password>
ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
```

**Note:**

- The `patchset.rsp` file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.
- The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

```
oracle.iappserver.st_midtier:szl_
InstanceInformation={"welcome1"}
```

c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <exact_
path>/patchset.rsp
```

9. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run `root.sh`.

10. Apply the following patches depending on how the database, which houses the Management Repository, is configured:
    - If the database is configured on a virtual host, then apply patch# 5667255 to the Oracle home directory of the OMS.
    - If the database is NOT configured on a virtual host, then apply patch# 7040389 to the Oracle home directory of the OMS
11. Apply 10.2.0.4 or higher patch set to the Management Agent:
    a. Copy the `patchset.rsp` file from the `<Patch Set DVD>/response/` directory to a location on your host.

    b. Edit the `patchset.rsp` file and make the following changes:

    ```
    ORACLE_HOME = <full_path_to_Oracle_home_of__Agent>
    ```

    c. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

    ```
    ./runInstaller -noconfig -silent -responseFile <absolute_
    path>/patchset.rsp -force
    ```

    **Note:** Use the `-force` command only when you want to install in an existing, nonempty directory.

12. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run `root.sh`.
13. After applying the patch, make the following settings to the environment variable - PERL5LIB:
    a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

    For UNIX Platforms:

    ```
    setenv PERL5LIB_BACKUP $PERL5LIB
    ```

    For Microsoft Windows Platforms:

    ```
    set PERL5LIB_BACKUP=%PERL5LIB%
    ```

    b. Now make the following settings to the variable:

    For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

    For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib
14. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

```
$<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
```

For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

15. After the script runs successfully, Grid Control is configured to 10.2.0.4 release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

> **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:
>
> ```
> emctl secure unlock -console
> ```

### 8.6.2.4 Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g

To install Grid Control using an existing Oracle Database 11g, follow these steps:

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

   http://www.oracle.com/technology/software/products/oem/index.html

2. If your existing database is configured with Database Control, then ensure that you deconfigure it before you begin the installation of Grid Control.

   To deconfigure Database Control for a single instance database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop
   ```

   To deconfigure Database Control for a Real Application Clusters (RAC) database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop -
   cluster
   ```

   After deconfiguring the Database Control, connect to the database as SYS user and run the following SQL files from the Oracle home of the database:

   ```
   <ORACLE_HOME>/rdbms/admin/dbmspool.sql
   ```

   ```
   <ORACLE_HOME>rdbms/admin/prvtpool.plb
   ```

---

**Note:** The command drops all the public synonyms starting with the following names created by any user for any schema:

- 'MGMT$%'
- 'MGMT_%'
- 'SMP_EMD%'
- 'SMP_MGMT%'
- 'SETEMVIEWUSERCONTEXT'
- 'DBMS_SHARED_POOL'
- 'EMD_MNTR'
- 'ECM_UTIL'

---

3. Ensure that the database initialization parameters have the correct values to create a Management Repository in the database.

   For information about the initialization parameters to be edited and the values to be provided, see Section 8.4.3.1, "Check Database Initialization Parameters".

   ---

   **Note:** If you do not set the database initialization parameters, the installation will fail and you will find the error message "OUI-10155:Error" in the following log file:

   ```
   <DB_HOME>/cfgtoollogs/cfgfw/installActions<time_
   stamp>.log
   ```

   To resolve it, set the parameters with correct values as given in Section 8.4.3.1, "Check Database Initialization Parameters", deinstall the failed Oracle homes, and then restart the installation.

   ---

4. Log in to the database as SYSDBA and run the following command:

   ```
   @?/rdbms/admin/dbmspool.sql
   ```

   ```
   commit;
   ```

5. (ONLY FOR Oracle Enterprise Linux (OEL) 5.X and Red Hat Enterprise Linux 5.X) If `/usr/lib/libdb.so.2` does not exist, then run the following command:

   ```
   ln -s /usr/lib/libgdbm.so.2.0.0 /usr/lib/libdb.so.2
   ```

6. Install the base release of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux or 10.2.0.2 for Microsoft Windows) using the following command:

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig -ignoreSysPrereqs -silent
   -responseFile <location of em_using_existing_db.rsp> use_
   prereq_checker=false b_skipDBValidation=true
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe -noconfig -ignoreSysPrereqs -silent -responseFile
   <location of em_using_existing_db.rsp> use_prereq_
   checker=false
   ```

---

**Note:** The `em_using_existing_db.rsp` file is packaged with Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.5 of Chapter 9, "Installing Enterprise Manager Grid Control in Silent Mode".

---

7. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

8. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

9. Apply 10.2.0.5 or higher patch set to OMS:

   ---

   **Note:** You can download the 10.2.0.5 or higher patch set from the following location:

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

   For each patch set, you might have to download either a single ZIP file or multiple ZIP files. If you have to download more than one ZIP file, then extract the contents of the ZIP files into one directory. For more information about these ZIP files and how you can extract them, see the README file associated with the patch set.

   ---

   a. Copy the `patchset.rsp` file from the `<Patchset_Downloaded_Location>/response/` directory to a location on your host.

   b. Edit the `patchset.rsp` file and make the following changes:

   ```
   b_softwareonly = true
   s_sysPassword  = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
   ```

**Note:**

- The `patchset.rsp` file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.
- The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

  ```
  oracle.iappserver.st_midtier:szl_
  InstanceInformation={"welcome1"}
  ```

c. Apply 10.2.0.5 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <exact_
path>/patchset.rsp
```

10. From the Oracle home directory of the OMS, run `root.sh`.
11. Apply 10.2.0.5 or higher patch set to the Management Agent:

a. Copy the `patchset.rsp` file from the `<Patch Set DVD>/response/` directory to a location on your host.

b. Edit the `patchset.rsp` file and make the following changes:

```
ORACLE_HOME = <full_path_to_Oracle_home_of__Agent>
```

c. Apply 10.2.0.5 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <absolute_
path>/patchset.rsp -force
```

**Note:** Use the `-force` command only when you want to install in an existing, nonempty directory.

12. From the Oracle home directory of the Management Agent, run `root.sh`.
13. After applying the patch, make the following settings to the environment variable - PERL5LIB:

a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

For UNIX Platforms:

```
setenv PERL5LIB_BACKUP $PERL5LIB
```

For Microsoft Windows Platforms:

```
set PERL5LIB_BACKUP=%PERL5LIB%
```

b. Now make the following settings to the variable:

   For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

   For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib

14. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

15. After the script runs successfully, Grid Control is configured to 10.2.0.5 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

    > **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:
    >
    > ```
    > emctl secure unlock -console
    > ```

16. If the script fails, then look at the OMS configuration log file. The OMS configuration log file is available in `<OMS_ORACLE_HOME>/cfgtoollogs/cfgfw`. Scan through the logs to see if you have the following error message:

    ```
    The installer has detected that there are background dbms jobs currently
    running in the Repository Database.
    ```

    > **Note:** For Agent configuration logs, go to `<AGENT_ORACLE_HOME>/cfgtoollogs/cfgfw`. For Database configuration logs, go to `<DB_ORACLE_HOME>/cfgtoollogs/cfgfw`.

    If you see the error message, then before upgrading the Management Repository, do the following:

a. Stop the running DBMS jobs by logging in to SQL as SYSDBA and running the following command:

```
SQL> exec sysman.emd_maintenance.remove_em_dbms_jobs;
```

b. Stop and restart the database.

c. Check the status of SYSMAN user account:

   - Log in to SQLPlus as SYSDBA and run the following query:

```
select username,account_status from dba_users;
```

   - Ensure that the SYSMAN user account is in 'open' status. If the account is not in open status, then run the following command:

```
alter user SYSMAN account unlock;
```

   - Commit the changes by running the following command:

```
commit;
```

d. Rerun the `ConfigureGC.pl` script.

e. After installation is complete, restart the DBMS jobs by running the following commands, one after the other:

```
SQL> exec sysman.emd_maintenance.submit_em_dbms_jobs;
```

```
SQL> commit;
```

#### 8.6.2.5 Installing Additional Management Service Using Existing Oracle Database 11g

To install an additional OMS to connect to an existing Oracle Database 11g, follow these steps:

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

   http://www.oracle.com/technology/software/products/oem/index.html

2. Ensure that the database, which houses the repository, and its listener are running.

3. Log in to the database as SYSDBA user and convert the repository version from 10.2.0.5.0 or higher to 10.2.0.1.0 by running the following SQL statement:

```
UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0' where
component_name='CORE'; commit;
```

4. Invoke the installer of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1):

   For UNIX Platforms:

```
./runInstaller -noconfig -silent -responseFile additional_
mgmt_service.rsp use_prereq_checker=false b_
skipDBValidation=true
```

   For Microsoft Windows Platforms:

```
setup.exe -noconfig -silent -responseFile additional_mgmt_
service.rsp use_prereq_checker=false
```

> **Note:** The `additional_mgmt_service.rsp` file is packaged with Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.6 of Chapter 9, "Installing Enterprise Manager Grid Control in Silent Mode".

5. Log in to the database again as SYSDBA user and convert the repository version back to what is was, that is, 10.2.0.5.0 or higher, by using the following SQL statement. The following SQL statement uses 10.2.0.5.0 as an example; therefore, it you are installing a higher release, then replace it with that release number.

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.5.0' where
   component_name='CORE'; commit;
   ```

6. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

7. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

8. Apply 10.2.0.5 or higher patch set to OMS:

   > **Note:** You can download the 10.2.0.5 or higher patch set from the following location:
   >
   > `http://www.oracle.com/technology/software/products/oem/index.html`
   >
   > For each patch set, you might have to download either a single ZIP file or multiple ZIP files. If you have to download more than one ZIP file, then extract the contents of the ZIP files into one directory. For more information about these ZIP files and how you can extract them, see the README file associated with the patch set.

   a. Copy the `patchset.rsp` file from the `<Patch Set DVD>/response/` directory to a location on your host.

   b. Edit the `patchset.rsp` file and make the following changes:

      ```
      b_softwareonly = true
      s_sysPassword  = <sys user password>
      ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
      oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
      ```

**Note:**

- The patchset.rsp file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.
- The variable oracle.iappserver.st_midtier:szl_InstanceInformation is the instance password for the current Oracle Application Server 10g. While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

  ```
  oracle.iappserver.st_midtier:szl_
  InstanceInformation={"welcome1"}
  ```

c. Apply 10.2.0.5 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <exact_
path>/patchset.rsp
```

9. From the Oracle home directory of the OMS, run root.sh.
10. Apply 10.2.0.5 or higher patch set to the Management Agent:

a. Copy the patchset.rsp file from the <Patch Set DVD>/response/ directory to a location on your host.

b. Edit the patchset.rsp file and make the following changes:

```
ORACLE_HOME = <full_path_to_Oracle_home_of__Agent>
```

c. Apply 10.2.0.5 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

```
./runInstaller -noconfig -silent -responseFile <absolute_
path>/patchset.rsp -force
```

**Note:** Use the -force command only when you want to install in an existing, nonempty directory.

11. From the Oracle home directory of the Management Agent, run root.sh.
12. After applying the patch, make the following settings to the environment variable - PERL5LIB:

a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

For UNIX Platforms:

```
setenv PERL5LIB_BACKUP $PERL5LIB
```

For Microsoft Windows Platforms:

```
set PERL5LIB_BACKUP=%PERL5LIB%
```

b. Now make the following settings to the variable:

   For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

   For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib

13. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

14. After the script runs successfully, Grid Control is configured to 10.2.0.5 release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

    **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:

    ```
    emctl secure unlock -console
    ```

## 8.6.3 Installing 'Software-Only' and Configuring Later (GUI Mode)

This section describes how you can perform the following in GUI mode:

- Installing Enterprise Manager Grid Control Using an Existing Database
- Installing Additional Management Service

**Note:** Do not use the response file because it will not be honored in GUI mode.

#### 8.6.3.1 Installing Enterprise Manager Grid Control Using an Existing Database

> **Note:** Ensure that your existing database is one of the certified databases supported by Enterprise Manager 10g Grid Control. To see a list of certified databases, see Document ID 412431.1 on My Oracle Support (formerly Metalink).
>
> Access My Oracle Support at the following URL, select **Document ID** from the **Quick Find** menu, quote the document number, and click **GO** to view the document:
>
> `http://metalink.oracle.com/`
>
> f you want to use Oracle Database 11g as the existing database, then see Section 8.6.2.4, "Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Oracle Database 11g".

To install Grid Control using an existing database, follow these steps:

1. If your existing database is configured with Database Control, then ensure that you deconfigure it before you begin the installation of Grid Control.

   To deconfigure Database Control for a single instance database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop
   ```

   To deconfigure Database Control for a Real Application Clusters (RAC) database, run the following command from the Oracle home directory of the database (for example, db10g):

   ```
   $<ORACLE HOME>/bin/emca -deconfig dbcontrol db -repos drop -
   cluster
   ```

   After deconfiguring the Database Control, connect to the database as SYS user and run the following SQL files from the Oracle home of the database:

   ```
   <ORACLE_HOME>/rdbms/admin/dbmspool.sql
   ```

   ```
   <ORACLE_HOME>rdbms/admin/prvtpool.plb
   ```

> **Note:** The command drops all the public synonyms starting with the following names created by any user for any schema:
>
> - 'MGMT$%'
> - 'MGMT_%'
> - 'SMP_EMD%'
> - 'SMP_MGMT%'
> - 'SETEMVIEWUSERCONTEXT'
> - 'DBMS_SHARED_POOL'
> - 'EMD_MNTR'
> - 'ECM_UTIL'

2. Ensure that the database initialization parameters have the correct values to create a Management Repository in the database.

   For information about the initialization parameters to be edited and the values to be provided, see Section 8.4.3.1, "Check Database Initialization Parameters".

   > **Note:** If you do not set the database initialization parameters, the installation will fail and you will find the error message "OUI-10155:Error" in the following log file:
   >
   > ```
   > <DB_HOME>/cfgtoollogs/cfgfw/installActions<time_
   > stamp>.log
   > ```
   >
   > To resolve it, set the parameters with correct values as given in Section 8.4.3.1, "Check Database Initialization Parameters", deinstall the failed Oracle homes, and then restart the installation.

3. Log in to the database as SYSDBA and run the following command:

   ```
   @?/rdbms/admin/dbmspool.sql
   ```

   ```
   commit;
   ```

4. Install the base release of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1 for Linux or 10.2.0.2 for Microsoft Windows) using the following command:

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe -noconfig
   ```

5. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

6. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

7. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

   ```
   ./runInstaller -noconfig b_softwareonly=true
   ```

8. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run `root.sh`.

9. (ONLY FOR 10.2.0.4.0 RELEASE) Apply the following patches depending on how the database, which houses the Management Repository, is configured:

   - If the database is configured on a virtual host, then apply patch# 5667255 to the Oracle home directory of the OMS.
   - If the database is NOT configured on a virtual host, then apply patch# 7040389 to the Oracle home directory of the OMS

10. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

```
./runInstaller -noconfig
```

11. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run `root.sh`.

12. After applying the patch, make the following settings to the environment variable - PERL5LIB:

    a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

       For UNIX Platforms:

       ```
       setenv PERL5LIB_BACKUP $PERL5LIB
       ```

       For Microsoft Windows Platforms:

       ```
       set PERL5LIB_BACKUP=%PERL5LIB%
       ```

    b. Now make the following settings to the variable:

       For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

       For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib

13. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.

14. After the script runs successfully, Grid Control is configured to 10.2.0.4 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

    **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:

    ```
    emctl secure unlock -console
    ```

15. If the script fails, then look at the OMS configuration log file. The OMS configuration log file is available in `<OMS_ORACLE_HOME>/cfgtoollogs/cfgfw`. Scan through the logs to see if you have the following error message:

    ```
    The installer has detected that there are background dbms jobs currently
    running in the Repository Database.
    ```

    > **Note:** For Agent configuration logs, go to `<AGENT_ORACLE_HOME>/cfgtoollogs/cfgfw`. For Database configuration logs, go to `<DB_ORACLE_HOME>/cfgtoollogs/cfgfw`.

    If you see the error message, then before upgrading the Management Repository, do the following:

    **a.** Stop the running DBMS jobs by logging in to SQL as SYSDBA and running the following command:

    ```
    SQL> exec sysman.emd_maintenance.remove_em_dbms_jobs;
    ```

    **b.** Stop and restart the database.

    **c.** Check the status of SYSMAN user account:

    - Log in to SQLPlus as SYSDBA and run the following query:

    ```
    select username,account_status from dba_users;
    ```

    - Ensure that the SYSMAN user account is in 'open' status. If the account is not in open status, then run the following command:

    ```
    alter user SYSMAN account unlock;
    ```

    - Commit the changes by running the following command:

    ```
    commit;
    ```

    **d.** Rerun the `ConfigureGC.pl` script.

    **e.** After installation is complete, restart the DBMS jobs by running the following commands, one after the other:

    ```
    SQL> exec sysman.emd_maintenance.submit_em_dbms_jobs;
    ```

    ```
    SQL> commit;
    ```

#### 8.6.3.2 Installing Additional Management Service

**Caution:** The steps outlined in this section describe how you can install an additional OMS in an environment where the repository and the main OMS are of 10.2.0.4 or higher release. The main OMS refers to the one that was installed with the first installation of Grid Control. If you want to install an additional OMS in a 10.2.0.3 or 10.2.0.2 environment, then see Section 8.5.2, "Scenarios" to understand the approach to be adopted.

Also, this installation method is only for new, additional OMS to be installed. If you already have an OMS of a lower release, then the only way to upgrade it is to patch it using the Patch Set.

If you want to install an additional OMS to connect to Oracle Database 11g, then see Section 8.6.2.5, "Installing Additional Management Service Using Existing Oracle Database 11g".

To install additional OMS, follow these steps:

1. Ensure that the database, which houses the repository, and its listener are running.
2. Log in to the database as SYSDBA user and convert the repository version from 10.2.0.4.0 or higher to 10.2.0.1.0 by running the following SQL statement:

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0' where
   component_name='CORE'; commit;
   ```

3. Invoke the installer of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1):

   For UNIX Platforms:

   ```
   ./runInstaller -noconfig
   ```

   For Microsoft Windows Platforms:

   ```
   setup.exe -noconfig
   ```

4. Log in to the database again as SYSDBA user and convert the repository version back to what is was, that is, 10.2.0.4.0 or higher, by using the following SQL statement. The following SQL statement uses 10.2.0.4.0 as an example; therefore, it you are installing a higher release, then replace it with that release number.

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.4.0' where
   component_name='CORE'; commit;
   ```

5. (For UNIX Platforms Only) Log in as a *root* user in a new terminal and run the `allroot.sh` script from the Oracle home directory of the OMS (for example, oms10g):

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

6. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS (for example, oms10g):

   ```
   $<ORACLE_HOME>/opmn/bin/opmnctl stopall
   ```

7. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the OMS (for example, oms10g) by running the following command:

   ```
   ./runInstaller -noconfig b_softwareonly=true
   ```

8. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run `root.sh`.
9. Apply the following patches depending on how the database, which houses the Management Repository, is configured:
   - If the database is configured on a virtual host, then apply patch# 5667255 to the Oracle home directory of the OMS.
   - If the database is NOT configured on a virtual host, then apply patch# 7040389 to the Oracle home directory of the OMS
10. Apply 10.2.0.4 or higher patch set to the Oracle home directory of the Management Agent (for example, agent10g) by running the following command:

    ```
    ./runInstaller -noconfig
    ```
11. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run `root.sh`.
12. After applying the patch, make the following settings to the environment variable - PERL5LIB:
    a. Before making changes to the environment variable PERL5LIB, take a backup of the variable:

       For UNIX Platforms:

       ```
       setenv PERL5LIB_BACKUP $PERL5LIB
       ```

       For Microsoft Windows Platforms:

       ```
       set PERL5LIB_BACKUP=%PERL5LIB%
       ```

    b. Now make the following settings to the variable:

       For UNIX platforms, set it to <OMS_ORACLE_HOME>/perl/lib/5.6.1

       For Microsoft Windows platforms, set it to <OMS_ORACLE_HOME>/perl/5.6.1/lib
13. Configure Grid Control by running the `ConfigureGC.pl` script from the Oracle home directory of the OMS (for example, oms10g):

    For UNIX Platforms:

    ```
    $<ORACLE_HOME>/perl/bin/perl <OMS ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is /usr/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be /usr/oracle/gc.

    For Microsoft Windows Platforms:

    ```
    $<ORACLE_HOME>\perl\5.6.1\bin\MSWin32-x86\perl <OMS ORACLE
    HOME>\sysman\install\ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is C:/Program Files/oracle/gc/oms10g, then <INSTALL_BASE_DIRECTORY> must be C:/Program Files/oracle/gc.
14. After the script runs successfully, Grid Control is configured to 10.2.0.4 release. To verify the release, do the following:
    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

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

- Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

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

**Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command:

```
emctl secure unlock -console
```

### 8.6.4 Installing 'Software-Only' and Configuring Later (Silent Mode) on Newly Supported Platforms

Enterprise Manager Grid Control is now supported on the following new platforms:

- Oracle Enterprise Linux (OEL) 5.0, 5.1, 5.2
- Red Hat Enterprise Linux 5.0, 5.1, 5.2
- SUSE Linux Enterprise 10
- HP- UX Itanium 11.31
- AIX 6.1
- HP-UX PA-RISC 11.31

However, the release that is supported on these new platforms is Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), which is a patch set. There was no full release in the past for these platforms. Ideally, you must install the full release and then patch it to 10.2.0.5, but since there was no full release on these platforms, you can follow the instructions outlined in this section to directly install the patch set on these platforms.

**Note:** Enterprise Manager Grid Control is also supported on Microsoft Windows 2008 and Microsoft Windows Vista. For instructions to install Enterprise Manager Grid Control on these platforms, see Section 8.4.5, "Installing on Microsoft Windows 2008 and Microsoft Windows Vista".

This section covers the following:

- Installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Using Existing Database
- Installing an Additional Oracle Management Service Release 5 (10.2.0.5)

**Note:** Before staring the installation, as a prerequisite, ensure that you have installed all the required packages and kernel parameters as described in Appendix D, "Platform-Specific Package and Kernel Requirements". Particularly, if you are installing on Oracle Enterprise Linux 5 or RedHat Enterprise Linux 5, then ensure that you have the default RPM.

#### 8.6.4.1 Installing Enterprise Manager 10*g* Grid Control Release 5 (10.2.0.5) Using Existing Database

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

   http://www.oracle.com/technology/software/products/oem/index.html

   > **Note:** For example, if you are installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) on Red Hat Enterprise Linux 5.0, then download the full release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) released for Linux32-bit platform. Similarly, if you are installing on HP-UX Itanium, then download the full release, that is, Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) that was released for HP-UX Itanium.

2. (ONLY FOR Oracle Enterprise Linux (OEL) 5.X and Red Hat Enterprise Linux 5.X) If */usr/lib/libdb.so.2* does not exist, then run:

   ```
   ln -s /usr/lib/libgdbm.so.2.0.0 /usr/lib/libdb.so.2
   ```

3. If your existing database is configured with Database Control, then ensure that you deconfigure it before you begin the installation of Enterprise Manager Grid Control.

   To deconfigure Database Control for a single instance database, run the following command:

   ```
   $ORACLE HOME/bin/emca -deconfig dbcontrol db -repos drop
   ```

   Where *$ORACLE_HOME* is the Oracle home directory of existing Database.

   After deconfiguring the Database Control, connect to the database as SYS user and run the following SQL files from the Oracle home of the database:

   ```
   <ORACLE_HOME>/rdbms/admin/dbmspool.sql
   ```

   ```
   <ORACLE_HOME>rdbms/admin/prvtpool.plb
   ```

   > **Note:** The command drops all the public synonyms starting with the following names created by any user for any schema:
   >
   > - 'MGMT$%'
   > - 'MGMT_%'
   > - 'SMP_EMD%'
   > - 'SMP_MGMT%'
   > - 'SETEMVIEWUSERCONTEXT'
   > - 'DBMS_SHARED_POOL'
   > - 'EMD_MNTR'
   > - 'ECM_UTIL'

4. Verify whether all the database initialization parameters are set correctly. For information about the database initialization parameters, see Section 8.4.3.1, "Check Database Initialization Parameters".

5. Install the DBMS_SHARED_POOL package by running the below commands from the Oracle home directory of the Database:

   a. Login to the database as sysdba

   b. Run the below command:

      ```
      SQL>@?/rdbms/admin/dbmspool.sql
      ```

      ```
      SQL> commit;
      ```

6. Invoke the runInstaller:

   ```
   ./runInstaller -noconfig -ignoreSysPrereqs -silent
   -responseFile <location of em_using_existing_db.rsp> use_
   prereq_checker=false
   ```

   > **Note:** The *em_using_existing_db.rsp* file is packaged with Enterprise Manager Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.5, "Using Silent Mode to Install Enterprise Manager Grid Control Using an Existing Database".

7. If this is the first Oracle product you just installed on the host, then run the orainstRoot.sh script from the Central Inventory as a root user:

   ```
   $ORACLE_HOME/oraInventory/orainstRoot.sh
   ```

   Run the `allroot.sh` from the Oracle home of the OMS as a root user

8. Stop all OPMN processes by running the following command from the Oracle home directory of the OMS:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

9. Copy the patchset.rsp file from the <Patch Set DVD>/response/directory to a location on your host.

   > **Note:** The patchset.rsp file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.

   **For 10.2.0.4.0 Release:**

   ```
   b_softwareonly = true
   s_sysPassword = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   ```

   **For 10.2.0.5.0 or Higher Release:**

   ```
   b_softwareonly = true
   s_sysPassword = <sys user password>
   ORACLE_HOME = <full_path_to_Oracle_home_of_OMS>
   ```

```
oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
```

The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. The ias_admin user is the administrative user for Oracle Application Server instances and  is required for software update installation on middle-tiers.

While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

```
oracle.iappserver.st_midtier:szl_
InstanceInformation={"welcome1"}
```

This password is same as the SYSMAN password that you specified when you first installed the Grid control in your environment.

> **Note:** After installing the Grid control in your environment if you change the SYSMAN password then ias_admin password will not get changed.

To change the ias_admin password, go to the Oracle home directory of OMS and run the below command:

```
$ORACLE_HOME/bin/emctl set password <Old ias_admin password>
<New ias_admin Password>
```

> **Note:** If you don't remember the old ias_admin password then follow the instructions from Document ID 280587.1 on My Oracle Support (formerly Metalink) at *http://metalink.oracle.com/*

10. Apply the 10.2.0.5 patch set to the Oracle home directory of the OMS (for example, /abc/product/oms10g) by running the following command:

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

11. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run root.sh.

12. Apply the 10.2.0.5 patch set to the Oracle home directory of the Management Agent

    - Copy the patchset.rsp file from the <Patch Set DVD>/response/directory to a location on yourhost.
    - Edit patchset.rsp to include the following:

      ```
      ORACLE_HOME = < Oracle home directory of the Oracle Management Agent>
      ```

    - Apply the   10.2.0.5 patch set to the Oracle home directory of the Management Agent:

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

13. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run root.sh.

14. Set the *PERL5LIB* as `<ORACLE_HOME>/perl/lib/5.6.1` where <ORACLE_HOME> is the Oracle home directory of the OMS.

15. Execute the following script from the Oracle home directory of the OMS to complete the Grid Control 10.2.0.5 install:

    ```
    $ORACLE_HOME/perl/bin/perl <ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

    For example, if the Oracle home directory of OMS is */usr/oracle/gc/oms10g*, then *<INSTALL_BASE_DIRECTORY>* must be */usr/oracle/gc*.

16. After the script runs successfully, Grid Control is configured to 10.2.0.5 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

      $<ORACLE_HOME>/bin/emctl status oms

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

      $<ORACLE_HOME>/bin/emctl status agent

    **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command from the Oracle home directory of the OMS:

    emctl secure unlock -console

#### 8.6.4.2 Installing an Additional Oracle Management Service Release 5 (10.2.0.5)

1. From the following URL, download the software for the full release of Enterprise Manager Grid Control that was release for your platform:

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

   **Note:** For example, if you are installing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) on Red Hat Enterprise Linux 5.0, then download the full release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) released for Linux32-bit platform. Similarly, if you are installing on HP-UX Itanium, then download the full release, that is, Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) that was released for HP-UX Itanium.

2. (ONLY FOR Oracle Enterprise Linux (OEL) 5.X and Red Hat Enterprise Linux 5.X). If */usr/lib/libdb.so.2* does not exist, then run:

   ```
   ln -s /usr/lib/libgdbm.so.2.0.0 /usr/lib/libdb.so.2
   ```

3. Ensure that the database, which houses the repository, and its listener are running.

4. Log in to the database as SYSDBA user and convert the repository version from 10.2.0.5.0 to 10.2.0.1.0 by running the following SQL statement:

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0' where
   component_name='CORE'; commit;
   ```

5. Invoke the installer of Enterprise Manager 10g Grid Control Release 2 (10.2.0.1):

   ```
   ./runInstaller -noconfig -ignoreSysPrereqs -silent
   -responseFile <location of additional_mgmt_service.rsp> use_
   prereq_checker=false b_skipDBValidation=true
   ```

   > **Note:** The additional_mgmt_service.rsp file is packaged with Enterprise Manager Grid Control software. Before you run this file in silent mode, ensure that you edit the file and specify all the parameters required for a successful installation. To understand the mandatory parameters you need to specify, see Section 9.6, "Using Silent Mode to Install Additional Management Service".

6. Log in to the database again as SYSDBA user and convert the repository version back to what is was, that is, 10.2.0.5.0, by using the following SQL statement:

   ```
   UPDATE sysman.mgmt_versions SET version = '10.2.0.5.0' where
   component_name='CORE'; commit;
   ```

7. If this is the first Oracle product you just installed on the host, then run the *orainstRoot.sh* script from the Central Inventory as a root user:

   ```
   $ORACLE_HOME/oraInventory/orainstRoot.sh
   ```

8. Run the *allroot.sh* from the Oracle home of the OMS as a root user

9. Stop all the OPMN processes by running the following command from the Oracle home directory of the OMS:

   ```
   $ORACLE_HOME/opmn/bin/opmnctl stopall
   ```

10. Copy the patchset.rsp file from the <Patch Set DVD>/response/directory to a location on your host.

    > **Note:** The patchset.rsp file is packaged with the Patch Set. Before editing the file, you might want to take a backup of the file to another location in order to retain the original file. Alternatively, if you want to revert to the original file, then you can always take the file from the Patch Set DVD.

    **For 10.2.0.4.0 Release:**

    ```
    b_softwareonly = true
    s_sysPassword = <sys user password>
    ORACLE_HOME = < full_path_to_Oracle_home_of_OMS >
    ```

    **For 10.2.0.5.0 or Higher Release:**

    ```
    b_softwareonly = true
    s_sysPassword = <sys user password>
    ORACLE_HOME = < full_path_to_Oracle_home_of_OMS >
    oracle.iappserver.st_midtier:szl_InstanceInformation={"ias_password"}
    ```

    The variable `oracle.iappserver.st_midtier:szl_InstanceInformation` is the instance password for the current Oracle Application Server 10g. The ias_admin user is the administrative user for Oracle Application Server instances and is required for software update installation on middle-tiers.

While specifying the password, you must use the braces and specify the password in double quotation marks. For example, if you want to specify the password welcome1, then the syntax would be:

```
oracle.iappserver.st_midtier:szl_
InstanceInformation={"welcome1"}
```

This password is same as the SYSMAN password that you specified when you first installed the Grid control in your environment.

---

**Note:** After installing the Grid control in your environment if you change the SYSMAN password then ias_admin password will not get changed.

---

To change the ias_admin password, go to the Oracle home directory of OMS and run the below command:

```
$ORACLE_HOME/bin/emctl set password <Old ias_admin password>
<New ias_admin Password>
```

---

**Note:** If you do not remember the old ias_admin password then follow the instructions from Document ID 280587.1 on My Oracle Support (formerly Metalink) at *http://metalink.oracle.com/*

---

11. Apply the 10.2.0.5 patch set to the Oracle home directory of the OMS (for example, /abc/product/oms10g) by running the following command:

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

12. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the OMS, run root.sh.
13. Apply the 10.2.0.5 patch set to the Oracle home directory of the Management Agent

    - Copy the patchset.rsp file from the *<Patch Set DVD>/response/*directory to a location on yourhost
    - Edit patchset.rsp to include the following:

      ```
      ORACLE_HOME = < Oracle home directory of the Management agent >
      ```

    - Apply the  10.2.0.5 patch set to the Oracle home directory of the Agent

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

14. (ONLY FOR 10.2.0.5.0 OR HIGHER RELEASE) From the Oracle home directory of the Management Agent, run root.sh.
15. Set the *PERL5LIB* as `<ORACLE_HOME>/perl/lib/5.6.1`. where <ORACLE_ HOME> is the Oracle home directory of the OMS.
16. Execute the following script to from the Oracle home directory of the OMS to complete the 10.2.0.5.0 install:

    ```
    $ORACLE_HOME/perl/bin/perl <ORACLE
    HOME>/sysman/install/ConfigureGC.pl <INSTALL_BASE_DIRECTORY>
    ```

For example, if the Oracle home directory of OMS is */usr/oracle/gc/oms10g*, then *<INSTALL_BASE_DIRECTORY>* must be */usr/oracle/gc*.

17. After the script runs successfully, Grid Control is configured to 10.2.0.4 or higher release. To verify the release, do the following:

    - Go to the Oracle home directory of the OMS (for example, oms10g) and run the following command:

      $<ORACLE_HOME>/bin/emctl status oms

    - Go to the Oracle home directory of the Management Agent (for example, agent10g) and run the following command:

      $<ORACLE_HOME>/bin/emctl status agent

      **Note:** For 10.2.0.5, unsecured access to Grid Control (using HTTP URL) is restricted by default. Instead, use HTTPS URL. If you still want to use the HTTP URL, then unlock it using the following command from the Oracle home directory of the OMS:

      emctl secure unlock -console

# 9

# Installing Enterprise Manager Grid Control in Silent Mode

You can install Enterprise Manager Grid Control (Grid Control) in silent mode, that is, without using the GUI-based screens. In silent mode, a response file provides the necessary installation information, typically answered by you, using stored values.

This chapter describes how you can install Grid Control in silent mode. In particular, this chapter covers the following:

- Available Response Files
- Running Response Files
- Silent Installation Process
- Using Silent Mode to Install Enterprise Manager Grid Control Using a New Database
- Using Silent Mode to Install Enterprise Manager Grid Control Using an Existing Database
- Using Silent Mode to Install Additional Management Service

> **Note:** You do not need to set the DISPLAY environment variable for silent installations using Oracle Universal Installer.

## 9.1 Available Response Files

The following lists the response files available for each installation type. You will find these response files in the `<DVD>/response` directory of the DVD-ROM.

***Table 9–1 Available Response Files for Silent Installation***

| Installation Option | Response File |
|---|---|
| Enterprise Manager 10*g* Grid Control Using a New Database | em_with_new_db.rsp |
| Enterprise Manager 10*g* Grid Control Using an Existing Database | em_using_existing_db.rsp |
| Additional Management Service | additional_mgmt_service.rsp |

## 9.2 Running Response Files

Run the response files in the following way:

- **For UNIX Platforms**

  ```
  ./runInstaller -silent -responseFile=<absolute path of the response file>
  -waitforcompletion
  ```

- **For Microsoft Windows Platforms**

  ```
  ./setup.exe -silent -responseFile <absolute path of the response file>
  ```

## 9.3 Silent Installation Process

The silent installation on a UNIX environment can bee seen as a three-step process:

1. `noconfig`: In the first step, you must run the `-noconfig` option. This will copy all the bits into the corresponding Oracle homes.
2. `allroot.sh/orainstRoot.sh`: After the bits are copied, the installer will prompt you to run the `allroot.sh` script (and `orainstRoot.sh`) or `root.sh` script (depending on. installation type).
   - Run the `orainstRoot.sh` script if this is the first Oracle product installation on your host.
   - Run the `allroot.sh` script from the first Oracle home that was created during installation.
3. `runconfig.sh`: You must pass this command to run the configuration assistants.

   **For a Grid Control installation using a new database, run:**

   ```
   <DB_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<database home path>
   ACTION=configure MODE=perform COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
   ```

   **For a Grid Control installation using an existing database, run:**

   ```
   <OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<OMS Home> MODE=perform
   ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   **For an additional OMS installation, run:**

   ```
   <OMS_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<OMS Home> MODE=perform
   ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

**Note:** If you want to use the `-noconfig` option during the silent installation, you must run the `runconfig.sh` command at the end of the installation in order to run the configuration assistants.

**Caution:** When you are using the `-noconfig` option in your installation, ensure you also pass `-silent` to invoke the installer. The `-noconfig` option must be executed only during silent installations.

## 9.4 Using Silent Mode to Install Enterprise Manager Grid Control Using a New Database

Before you begin the silent installation of Grid Control using a new database, you must meet the prerequisites described in Section 8.3, "Installing Enterprise Manager Grid Control Using a New Database".

After you meet the prerequisites, follow these steps:

1. Copy the `<DVD>/response/em_with_new_db.rsp` file to a location on the local host.
2. Modify the following entries in the response file.

***Table 9–2 Parameters to Modify in em_with_new_db.rsp File***

| Parameter | Description |
|---|---|
| FROM_LOCATION | Specify the complete path to the products.xml file. For example, FROM_LOCATION = "../stage/products.xml". |
| BASEDIR | Specify the directory where the ORACLE_HOME directories must be created. For example, on Microsoft Windows, BASEDIR = "C:\OHOME1", and on Linux, BASEDIR = "/scratch/OracleHomes". |
| INSTALLATION_NAME | Specify the name to be used for creating the Oracle home directories. For example, INSTALLATION_NAME = "OHOME1". |
| s_gdbName | Specify the global name of the database that houses the repository. For example, s_gdbName="emrep.us.oracle.com". |
| s_mountPoint | Specify the Oradata location where the datafiles are available. For example, s_mountPoint="/scratch/OracleHomes/oradata". |
| s_operGroup | Specify the UNIX group for database operators. For example, s_operGroup="g900", Group names can be obtained by executing groups command at the prompt in UNIX. |
| s_adminGroup | Specify the UNIX group for database administrators. For example, s_adminGroup="g900", Group names can be obtained by executing groups command at the prompt in UNIX. |
| s_securePassword | Specify the registration password for securing the communication between OMS and its Agents.<br>**Note:** Enterprise Manager implements a password policy requiring passwords to be at least 5 characters long, with at least one number. Passwords must start with a letter. |
| s_securePasswordConfirm | Specify the password again for confirmation. |
| b_lockedSelected | Specify whether the Management Agent communication must be locked. For example, b_lockedSelected=true/false. |
| b_passwordsDifferent | Specify whether different or same password will be used for database administration accounts. |
| sl_adminPwds | Specify different passwords for the database administration accounts - SYS, SYSTEM, SYSMAN, DBSNMP. This is required only when b_passwordsDifferent is set to "true". For example, sl_adminPwds={ "one", "two", "three", "four" }. |
| sl_adminPwdsConfirm | Specify the passwords again for confirmation. |
| s_reposPwd | Specify the password for SYSMAN user account. This is required only when b_passwordsSame is set to "true". This password will be taken for all the accounts. |
| s_reposPwdConfirm | Specify the passwords again for confirmation. |
| UNIX_GROUP_NAME | Specify the UNIX group to be set for the inventory directory. This is valid only for UNIX platforms. For example, UNIX_GROUP_NAME = "install". |

3. Invoke the runInstaller (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/em_with_new_
db.rsp
```

The following message on the `root.sh` scripts is displayed (for UNIX only):

```
WARNING:A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/db10g/allroot.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

> **Caution:** If this is the first time an Oracle product is being installed on the machine, the database listener targets will not be discovered, as the `root.sh` scripts have not been executed.

4. After the installation is complete, you must execute `orainstRoot.sh` and `allroot.sh` scripts as root (UNIX only).
5. To discover the Grid Control targets, you can execute `<Install Location>/agent10g/bin/agentca`, or discover the targets from the Grid Control console. See Section A.2.1.4, "Invoking the Agent Configuration Assistant in Standalone Mode" for more information on executing the Agent Configuration Assistant in standalone mode.

> **Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:
>
> 1. Open the agentstup file from the Oracle home of the Management Agent:
>
>    `$ORACLE_HOME/install/unix/scripts/agentstup`
>
> 2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
> 3. Run the root.sh script from the Oracle home of the Management Agent:
>
>    `$<ORACLE_HOME>/root.sh`
>
> 4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:
>
>    `$<ORACLE_HOME>/bin/emctl start agent`
>
>    This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

## 9.5 Using Silent Mode to Install Enterprise Manager Grid Control Using an Existing Database

Before you begin the silent installation of Grid Control using an existing database, you must:

- Set the initialization parameters correctly for your qualified existing Enterprise Edition database to be able to run a Management Repository. You should also set all fixed parameters for your Management Repository database. For more information about managing initialization parameters, see Section 8.4.3.1, "Check Database Initialization Parameters". Also see the chapter "Managing Initialization Parameters Using a Server Parameter File" of the *Oracle Database Administrator's Guide*.
- Meet the prerequisites mentioned in Section 8.4, "Installing Enterprise Manager Grid Control Using an Existing Database".

After you set the initialization parameters and meet the prerequisites, follow these steps:

1. Copy the `<DVD>/response/em_using_existing_db.rsp` file to a location on your local host.
2. Modify the following entries in the response file.

*Table 9–3 Parameters to Modify in em_using_existing_db.rsp File*

| Parameter | Description |
|---|---|
| FROM_LOCATION | Specify the complete path to the products.xml file. For example, FROM_LOCATION = "../oms/Disk1/stage/products.xml". |
| BASEDIR | Specify the directory where the ORACLE_HOME directories must be created. For example, on Microsoft Windows, BASEDIR = "C:\OHOME1", and on Linux, BASEDIR = "/scratch/OracleHomes". |
| INSTALLATION_NAME | Specify the name to be used for creating the Oracle home directories. For example, INSTALLATION_NAME = "OHOME1". |
| s_reposHost | Specify the name of the host where the database, which houses the Management Repository, is running. For example, s_reposHost="repo.xyz.com". |
| s_reposPort | Specify the port on which the database, which houses the Management Repository, is running. For example, s_reposPort="1521". |
| s_reposSID | Specify the SID or Service name of the database, which houses the Management Repository. For example, s_reposSID="emrep". |
| s_reposDBAPwd | Specify the DBA user account password (SYS user) that must be used for creating the repository schema. |
| s_mgmtTbsName | Specify the full path to the location where the data file for management tablespace (mgmt.dbf) can be stored. For example, s_mgmtTbsName=<*Database Oracle home*>/oradata/<*SID*>/mgmt.dbf. |
| s_ecmTbsName | Specify the full path to the location where the data file for configuration data tablespace (mgmt_ecm_depot1_.dbf) can be stored. For example, <*Database Oracle home*>/oradata/<*SID*>/mgmt_ecm_depot1.dbf. |

*Table 9–3 (Cont.) Parameters to Modify in em_using_existing_db.rsp File*

| Parameter | Description |
|---|---|
| s_securePassword | Specify the registration password for securing the communication between OMS and its Agents.<br>**Note:** Enterprise Manager implements a password policy requiring passwords to be at least 5 characters long, with at least one number. Passwords must start with a letter |
| s_securePasswordConfirm | Specify the password again for confirmation. |
| b_lockedSelected | Specify whether the Management Agent communication must be locked. For example, b_lockedSelected=true/false. |
| s_reposPwd | Specify password for repository schema owner. |
| s_reposPwdConfirm | Specify the passwords again for confirmation. |

3. Invoke the runInstaller (`setup.exe` on Microsoft Windows) by executing:

   ```
   <DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/em_using_
   existing_db.rsp
   ```

   The following message on the `root.sh scripts` appears (for UNIX only):

   ```
   WARNING:A new inventory has been created in this session. However, it has not
   yet been registered as the central inventory of this system.
   To register the new inventory please run the script '<User's Home
   Dir>/oraInventory/orainstRoot.sh' with root privileges.
   If you do not register the inventory, you may not be able to update or patch
   the products you installed.
   The following configuration scripts need to be executed as the root user.
   #!/bin/sh
   #Root script to run
   <User's Home Dir>/oraInventory/orainstRoot.sh
   <Install Location>/oms10g/allroot.sh
   To execute the configuration scripts:
       1. Open a terminal window
       2. Log in as root
       3. Run the scripts
       4. Return to this window and click OK to continue
   ```

   **Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

   1. Open the agentstup file from the Oracle home of the Management Agent:

      `$ORACLE_HOME/install/unix/scripts/agentstup`

   2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

   3. Run the root.sh script from the Oracle home of the Management Agent:

      `$<ORACLE_HOME>/root.sh`

   4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

      This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

## 9.6 Using Silent Mode to Install Additional Management Service

Before you begin the silent installation of an additional OMS, you must meet the prerequisites described in Section 8.5, "Installing an Additional Management Service".

After you meet the prerequisites, follow these steps:

1. Copy the `<DVD>/response/additional_mgmt_service.rsp` file to a location on your local host.
2. Modify the following entries in the response file.

*Table 9–4 Parameters to Modify in additional_mgmt_service.rsp File*

| Parameter | Description |
|---|---|
| FROM_LOCATION | Specify the complete path to the products.xml file. For example, FROM_LOCATION = "../oms/Disk1/stage/products.xml". |
| BASEDIR | Specify the directory where the ORACLE_HOME directories must be created. For example, on Microsoft Windows, BASEDIR = "C:\OHOME1", and on Linux, BASEDIR = "/scratch/OracleHomes". |
| INSTALLATION_NAME | Specify the name to be used for creating the Oracle home directories. For example, INSTALLATION_NAME = "OHOME1". |
| s_reposHost | Specify the name of the host where the database, which houses the Management Repository, is running. For example, s_reposHost="repo.xyz.com". |
| s_reposPort | Specify the port on which the database, which houses the Management Repository, is running. For example, s_reposPort="1521". |
| s_reposSID | Specify the SID or Service name of the database, which houses the Management Repository. For example, s_reposSID="emrep". |
| s_reposPwd | Specify password for repository schema owner. |
| b_lockedSelected | Specify whether the Management Agent communication must be locked. For example, b_lockedSelected=true/false. |
| s_securePassword | Specify the registration password for securing the communication between OMS and its Agents.<br>**Note:** Enterprise Manager implements a password policy requiring passwords to be at least 5 characters long, with at least one number. Passwords must start with a letter |
| s_securePasswordConfirm | Specify the password again for confirmation. |

3. Invoke the `runInstaller` (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/additional_
mgmt_service.rsp
```

The following message on the `root.sh scripts` is displayed (for UNIX only):

```
WARNING:A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
```

```
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/oms10g/allroot.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   `$ORACLE_HOME/install/unix/scripts/agentstup`

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
3. Run the root.sh script from the Oracle home of the Management Agent:

   `$<ORACLE_HOME>/root.sh`

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

# 10

# Deploying Management Agent

Oracle Management Agent (Management Agent) is one of the integral components of Enterprise Manager Grid Control (Grid Control) architecture. Management Agent communicates with the monitored targets, collects information about their health, transports that information to Oracle Management Service (OMS), which in turn stores the collected details in the central repository created in Oracle Database.

This chapter describes how you can install a Management Agent. In particular, it covers the following:

- Installing Management Agent Using Agent Deploy Application
- Installing Management Agent Using nfsagentinstall Script
- Installing Management Agent Using agentDownload Script
- Installing Management Agent Using OUI

> **Note:** To download the Management Agent software from My Oracle Support (formerly Metalink) using the Grid Control console, follow the instructions given in Section 6.3, "Downloading Management Agent Software Using Grid Control Console".

In addition to the installation types described in this chapter, you can also use the following installation types:

- Cluster Agent Installation

  This type of installation allows you to perform a standalone Management Agent installation on a selected cluster node, or perform a cluster Management Agent installation on a selected cluster. See Chapter 12, "Deploying Management Agent on a Cluster" for more information.

- Management Agent Cloning

  This type of installation allows you to clone an installed Management Agent (also referred to as the master Management Agent) on multiple destination Oracle homes. See Chapter 13, "Cloning Management Agent" for more information.

- Silent Installation

  This type of installation is done using the appropriate response files. These response files must be edited to prefill the correct values for an uninterrupted installation. You can also use a wrapper script that will perform these tasks and also execute the `root.sh` script (UNIX only), making this type of installation a fully automated activity. See Section 9, "Installing Enterprise Manager Grid Control in Silent Mode" for more information.

**Note:** On Microsoft Windows, after the Management Agent is installed, the Windows service names of the Management Agent are recorded as `Oracle<OH_name>Agent`. For example, Oracleagent10g1Agent, Oracleagent10g1SNMPPeerEncapsulator, Oracleagent10g1SNMPPeerMasterAgent. However, if you want to change or reconfigure the service names without the prefix "Oracle", then do the following:

- Pass the "s_agentServiceName" variable while running the runInstaller. For example, `./runInstaller s_agentServiceName="GRIDCONTROL"`
- If you are installing the Management Agent in silent mode, then provide the "s_agentServiceName" value in the response file `additional_agent.rsp`.
- If you are installing the Management Agent using agentDownload script, then provide the "s_agentServiceName" value in the response file `agent_download.rsp`.
- Before applying any one-off patch that relinks the nmo binary, Oracle recommendeds you to install the one-off for bug7436312. The nmo binary needs the steuid privilege set to root, which gets erased when nmo is relinked by the application of a one-off patch. For example, the one-off patch# 5976285 is one such patch that relinks nmo. If the prereq patch is not applied before, jobs can no longer run. The only recourse will be to manually run root.sh on the target Management Agent homes. With the prerequisite already applied to Management Agent homes, root.sh can be run from Patchwizard or it can be deferred.

**Note:** If you want to configure the Management Agent on AIX operating system, then follow the configuration steps described in *My Oracle Support* note 552404.1.

## 10.1 Installing Management Agent Using Agent Deploy Application

This section describes how you can install a Management Agent using the Agent Deploy application. In particular, this section covers the following:

- Overview
- Prerequisites
- Configurations Required for Management Agent to Communicate with Oracle Management Service with Server Load Balancer
- Installation Procedure

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 10.1.1 Overview

Agent Deploy application is an application within Grid Control console that allows you to install Management Agents using GUI-rich, interactive screens.

Although the Agent Deploy application can be used for installing one, single Management Agent, the application is best suited for installing multiple Management Agents, as a mass deployment, and is particularly useful when you want to perform remote installations across your organization.

The Agent Deploy application gives you the flexibility to specify multiple hosts on which the Management Agent needs to be installed. This helps you when you want to install the Management Agent on several hosts, in one attempt. The application connects to OMS where the Management Agent software is located and copies all the required files and scripts from there to the specified hosts, and then runs them to install the Management Agent. The connectivity between OMS and the specified hosts is established using SSH protocol.

For information about patches to be applied before performing cross-platform Agent push, see Section 5.4 of the Agent Best Practice paper located at http://www.oracle.com/technology/products/oem/pdf/10gr2_agent_deploy_bp.pdf.

**Caution:** If you are deploying the Management Agent in an environment having multiple OMS installations that are using a load balancer, then you should not access the Agent Deploy application using this load balancer. Oracle recommends that you access the OMS directly.

### 10.1.2 Prerequisites

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

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

***Table 10–1 Prerequisites for Installing a Management Agent Using Agent Deploy Application***

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the hardware and softwrae requirements.<br>For hardware requirements, see Section 3.1, "Hardware Requirements". For software requirements, see Section 3.3, "Software Requirements". | |
| Operating System Requirements | Check if that operating systemon which you are going to install the Management Agent is ceritified.<br>For information about certified operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |
| Package Requirements | Install the packages that are required for your operating system.<br>For information about packages, see Appendix G.1, "Check Platform-Specific Package Requirements for Agent Installation". | |

*Table 10–1 (Cont.) Prerequisites for Installing a Management Agent Using Agent Deploy Application*

| Requirement | Description | Yes/No |
|---|---|---|
| SSH Setup Requirements | If you are installing the Management Agent using Enterprise Manager 10g Grid Control Release 2 (10.2.0.2 or 10.2.0.1), then ensure that SSH is set up.<br>For information about setting up SSH, see Section G.2, "SSH (Secure Shell) Setup". (Note that SSH2 is supported only from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)).<br>In Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) or higher, the Agent Deploy application sets up and drops the SSH connection automatically, but if agent targets are on Microsoft Windows operating systems, then you need to setup Cygwin as explained in Section G.2, "SSH (Secure Shell) Setup". | |
| Load Balancer Requirements | If you are installing the Management Agent in an environment that has multiple OMSes managed by a Server Load Balancer (SLB), then ensure that you enable communication between the Management Agent and the host running the SLB.<br>For information about configuration to be done for SLB, see Section 10.1.3, "Configurations Required for Management Agent to Communicate with Oracle Management Service with Server Load Balancer". | |
| Operating System Group Requirements | Ensure that you are part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite. | |
| User and Operating System Group Requirement | Ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created.<br>For information about creating operating system groups and users, see Section 3.6, "Operating System Groups and Users Requirements". | |
| Path Validation Requirements | Validate the path to all command locations. For more information, see Section G.3, "Validate All Command Locations". | |
| Permission Requirements | Ensure that you have read, write, and execute permissions to `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, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.<br>For information about oraInventory permissions, see Section 4.8, "Installing Enterprise Manager Grid Control As the First Oracle Software". | |
| Oracle Inventory Location Requirements | Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `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. | |

***Table 10–1 (Cont.) Prerequisites for Installing a Management Agent Using Agent Deploy Application***

| Requirement | Description | Yes/No |
|---|---|---|
| Default Port Requirements | Ensure that the SSH daemon is running on the default port (that is, 22) on all the target hosts.<br>■ For Enterprise Manager 10g Grid Control Release 4 (10.2.0.4), the port must be 22. If it is any other port, then the installation fails.<br>■ For Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), the port can be 22 or any non-default port, that is, any port other than 22. If the port is a non-default port, then update the SSH_PORT property in the following file to ensure successful installation:<br>For default location:<br>`<OMS_HOME>/sysman/agent_download/<VERSION>/<PLATFORM>/agentdeploy/Paths.properties`<br>For another location (non-default):<br>`<OMS_HOME>/sysman/prov/resources/Paths.properties` | |
| PubkeyAuthentication Parameter Requirements | Ensure that the `PubkeyAuthentication` parameter is enabled in the sshd_config file.<br>To verify the value of this parameter, run the following command:<br>`grep PubkeyAuthentication /etc/ssh/sshd_config`<br>The result of this command must be *Yes*. If the result is *No*, then edit the `/etc/ssh/sshd_config` file and set the PubkeyAuthentication value to *Yes*. | |
| Virtual Host Requirements | If you are deploying a Management Agent on a virtual host using Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower, then you must make the following changes.<br>■ Open the following file:<br>`$ORACLE_HOME/sysman/prov/agentpush/agentpush.properties`<br>■ Change `oracle.sysman.prov.agentpush.virtualHost=false` to `oracle.sysman.prov.agentpush.virtualHost=true`.<br>**Note:** This step is applicable only if you are using Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower. Also, if you have multiple OMSes in your environment with a Software Load Balancer (SLB), then you must modify the agentpush.properties file on all OMSes.<br>In Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher, the New Agent Installation Wizard has a check box in the Hosts section that allows you to indicate that the hosts specified are virtual hosts; and therefore, you need not update the agentpush.properties file. | |

*Table 10–1 (Cont.) Prerequisites for Installing a Management Agent Using Agent Deploy Application*

| Requirement | Description | Yes/No |
|---|---|---|
| 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 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. | |
| SUDO Requirements | Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.<br>To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.<br>`<user> <hostname>=PASSWD: /home/em/agent10205/agent10g/root.sh, /bin/sh` | |
| Agent User Account Permissions and Rights (For Microsoft Windows) | (For Microsoft Windows) Ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Increase quotas.<br>■ Replace process level token.<br>■ Log in as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>**1.** Launch the Local Security Settings.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Settings**.<br>**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) Grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` | |

You can view the prerequisite checks and installation status from the Status screen in the Agent Deploy application. For more information about prerequisite checks related to Agent Deploy application, see Appendix G, "Agent Deploy Application - Installation Prerequisites".

**WARNING: Do not attempt to view the prerequisite check status while the prerequisite checks are still in progress. If you do so while the checks are still in progress, the application will display an error.**

### 10.1.3 Configurations Required for Management Agent to Communicate with Oracle Management Service with Server Load Balancer

If you are deploying a Management Agent in an environment that has multiple OMSes managed by a Server Load Balancer (SLB), then ensure that you follow these steps to enable communication between the Management Agent and the host running the SLB.

**Note:** This section is applicable only if you are using Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower. In Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher, the New Agent Installation Wizard has a new section "Load Balancer Host and Port" that allows you to specify the Load Balancer host name and port; and therefore, you need not update the agentpush.properties file.

1. Access the following file to provide the name of the host where SLB is set up:

   ```
   <OMS_HOME>/sysman/prov/agentpush/agentpush.properties
   ```

2. Uncomment the following property and provide the name of the host where SLB is set up:

   ```
   oracle.sysman.prov.agentpush.slb.host=
   ```

   Management Agents installed by the Agent Deploy application try to connect to the SLB host using the specified host name.

3. Uncomment the following property and provide the port value of the host where SLB is set up:

   ```
   oracle.sysman.prov.agentpush.slb.port=
   ```

   Management Agents installed by the Agent Deploy application try to connect to the load balancer hosts using the specified port values.

4. Ensure that you stage the agent software uniformly across all the OMS hosts that are managed by the SLB.

The following shows what values will be considered for host and port when only one of them or none of them are specified in the `agentpush.properties` file.

***Table 10–2 Host and Port Values Considered When Not Specified in agentpush.properties File***

| Property Not Specified | Host Name Considered | Port Value Considered |
|---|---|---|
| When SLB host name is not specified in the following property of the `agentpush.properties` file, but only the SLB port value is specified:<br>`oracle.sysman.prov.agentpush.slb.host` | The OMS host name specified in the following property of the `emoms.properties` file is considered.<br>`oracle.sysman.emSDK.svlt.ConsoleServerHost` | The OMS port value specified in the following property of the `emoms.properties` file is considered.<br>`oracle.sysman.emSDK.svlt.ConsoleServerPort`<br>Therefore, the port value specified in the `agentpush.properties` file is discarded. |
| When SLB port value is not specified in the following property of the `agentpush.properties` file, but only the host name is specified:<br>`oracle.sysman.prov.agentpush.slb.port` | The SLB host name specified in the following property of the `agentpush.properties` file is considered.<br>`oracle.sysman.prov.agentpush.slb.host` | The port value 80 is considered. |
| When both, SLB host and SLB port, values are not specified in the following properties of the `agentpush.properties` file *(the properties are commented by default)*:<br>`oracle.sysman.prov.agentpush.slb.host`<br>`oracle.sysman.prov.agentpush.slb.port` | The OMS host name specified in the following property of the `emoms.properties` file is considered.<br>`oracle.sysman.emSDK.svlt.ConsoleServerHost` | The OMS port value specified in the following property of the `emoms.properties` file is considered.<br>`oracle.sysman.emSDK.svlt.ConsoleServerPort` |

## 10.1.4 Installation Procedure

Agent Deploy provides the following two options for deploying the Management Agent:

- Fresh Installation of the Management Agent
- Installation Using a Shared Agent Home

**Note:** If you want to view the status of an installation or upgrade session that was previously run, click **Agent Installation Status** in the Deployments screen. However, **do not attempt to view the installation status until the installation is complete.** If you do, you will see an error.

### 10.1.4.1 Fresh Installation of the Management Agent

This option helps you perform a new installation of the Management Agent. The Agent Deploy application runs a prerequisite checker to ensure the environment meets the requirements for this installation type. See Section G.5, "Prerequisite Checks Executed by Agent Deploy" for more information.

**Note:**

- You can choose to skip the prerequisite check that is run by the Agent Deploy application. To do so, navigate to the `<OMSHOME>/sysman/prov/agentpush directory`, access the `agentpush.properties` file, and change the value of `oracle.sysman.prov.agentpush.step2` to "false", that is `oracle.sysman.prov.agentpush.step2=false`.
- On Microsoft Windows, do not open the `agentpush.properties` file using Microsoft Word software. Open it using other text editors such as VIM or Notepad.

To perform a new Management Agent installation, complete the following steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, from the Agent Installation section, click **Install Agent**.
3. On the Agent Deploy home page, select **Fresh Install**. The Installation Details screen appears.
4. In the Source Software section, select an installation source directory. This directory can either be the default directory that exists within the OMS, for example `<OMS_HOME>/sysman/agent_download/10.2.0.2.0/<platform>`, or any other location where the software is available.

   If you select **Default, from Management Server location**, then ensure that the path to the Management Agent software directory on the OMS host that you specify is visible over HTTP from all remote hosts.

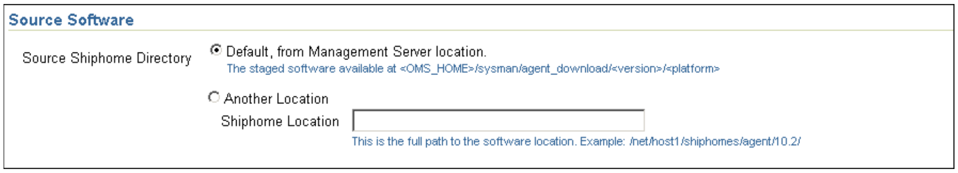
   To choose a location other than the default location from the OMS, select **Another Location**, and specify the full path to the software location where the software is staged. Ensure that the path leads up to the `product.xml` file. For example: `/net/host1/shiphomes/linux/agent/stage/products.xml`. Also ensure that this location (shared or non-shared) is accessible from all the remote hosts, and you have read permission on it.

   **Caution:** The additional parameters that you specify later in the installation process depend on the source software location that you select here.

   if you select the default software location, you must specify additional parameters that are supported by the `agentDownload` script. See Table H–1, " Parameters Supported by agentDownload Script" for a list of parameters supported by this script.

   If you select an alternative location, you must specify additional parameters that are supported by Oracle Universal Installer (OUI). See Table H–2, " Parameters Supported by Oracle Universal Installer" for a list of parameters supported by OUI.

*Figure 10–1 Source Software Section of the Installation Details Page*



● Default, from Management Server location.

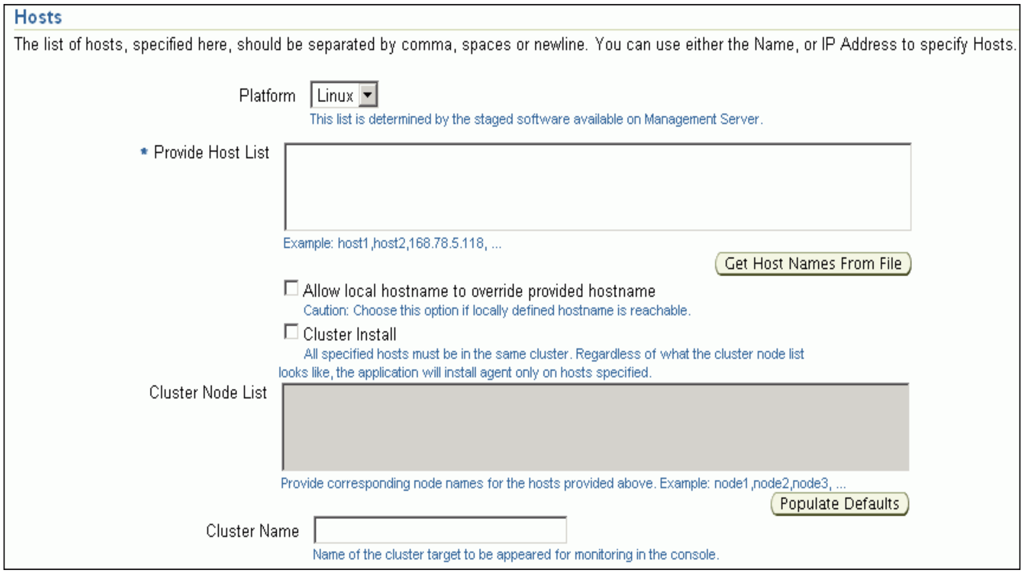
The staged software available at <OMS_HOME>/sysman/agent_download/<version>/<platform>

○ Another Location

This is the full path to the software location. Example: /net/host1/shiphomes/agent/10.2/

5. In the Version section on this screen, select the appropriate version of the Management Agent that you want to install. The values available in this list will depend on the staged software that are available on the OMS host.
6. Select the appropriate platform on which you want to perform this installation.
7. In the Hosts section, do the following:

*Figure 10–2 Hosts Section of the Installation Details Page*



The list of hosts, specified here, should be separated by comma, spaces or newline. You can use either the Name, or IP Address to specify Hosts.

Platform: Linux

This list is determined by the staged software available on Management Server.

Example: host1,host2,168.78.5.118, ...

□ Allow local hostname to override provided hostname

Caution: Choose this option if locally defined hostname is reachable.

□ Cluster Install

All specified hosts must be in the same cluster. Regardless of what the cluster node list looks like, the application will install agent only on hosts specified.

Provide corresponding node names for the hosts provided above. Example: node1,node2,node3, ...

Name of the cluster target to be appeared for monitoring in the console.

   a. Select the appropriate platform on which you want to perform this installation.
   b. In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the Management Agent installation.

**Note:**

- Ensure that you do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs. Also ensure that you use the same host names for which the SSH has been set.
- When virtual host names are provided in **Provide Host List** and when **Cluster Install** checkbox is selected, the same virtual host names will be populated in **Cluster Node List**. These virtual host names listed in **Cluster Node List** must be changed to match the actual cluster node names of the hosts. The correct cluster node names can be found in `OraInventory/ContentsXML/inventory.xml` on each remote host.

Alternatively, click **Get Host Names From File** to browse and select the file that contains a list of all the required host names.

If you choose to select a file that contains a list of all required host names, then ensure that the file format is similar to `/etc/hosts` file. Note that the first column of the file must have the host name and when you provide multiple hosts, then ensure that the hosts are mentioned in separate lines.

***Example 10–1 Host File Format***

Let's consider that you have the following hosts in your environment:

(1) host1 with fully qualified name host1.foo.com and IP address 154.87.3.229

(2) host2 with fully qualified name host2.foo.com and IP address 154.87.3.109

(3) host3 with fully qualified name host3.foo.com and IP address 154.80.5.218

In this case, the format of the host file should look like this:

```
host1
host2
host3
```

Alternatively, if you already have a file that has the following format, then you can use that file and format as is.

```
host1 host1.foo.com 154.87.3.229
host2 host2.foo.com 154.87.3.109
host3 host3.foo.com 154.80.5.218
```

The Agent Deploy application picks up only the values in the first column of the Host List file that you specify/select. Ensure that the host list format is appropriate because the Agent Deploy application does not validate this format on the selected file.

**Note:** For Grid Control 10.2.0.1 and 10.2.0.2, use the "Populate Details" button to populate the cluster node list or provide a comma-separated list.

c. Select **Allow local hostname to override provided hostname** if the specified host name is a virtual host name and not a physical host name.

For example, if the destination host name is mypc.server.com but the virtual name given to it is host1, then you can specify host1 in the **Provide Host List** text box, but select this check box to indicate that the specified host name is a virtual host name. The Agent Deploy application will internally interpret the virtual host name specified and map to its real, physical host name in the network.

**Note:** This step is applicable only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher. In Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower, the New Agent Installation Wizard does not display this check box and for specifying virtual host names, you must update the agentpush.properties file as described in Section 10.1.2, "Prerequisites".

d. Select **Cluster Install** if you want to install the Management Agent on a cluster.

e. For **Cluster Node List**, specify the cluster nodes on which the Management Agent must be installed. Ensure that you specify only the short names of the hosts, not the fully-qualified names. Alternatively, click **Populate Defaults** to populate this text box with all the host names that you had selected in step *b*.

**Note:**

- The node names that you specify here must be the host short names, not the fully-qualified names. For example, if the node is `xyz.server.us.com`, and the short name is `xyz`, then specify only `xyz` in the **Cluster Node List** field.

  If you have set up the cluster over a vendor clusterware, the node names can be different from the machine names. You can confirm the node names by executing `olsnodes` from the `<Oracle Clusterware home>` on one of the cluster nodes. If you are using Oracle Cluster release 9.2, confirm the node names by executing `lsnodes` from the cluster Oracle home. See Chapter 12, "Deploying Management Agent on a Cluster" for more information.

- When virtual host names are provided in **Host List** and when **Cluster Install** is selected, the same virtual host names will be populated in **Cluster Node List** (the next field). These virtual host names listed in the Cluster Node List textbox must be changed to match the actual cluster node names of the hosts. The correct cluster node names can be found in `OraInventory/ContentsXML/inventory.xml` on each remote host.

f. In the Cluster Name text box, specify a unique cluster name. If you are extending a cluster, specify the existing cluster name here. The cluster name that you specify here identifies that cluster in the Grid Control console.

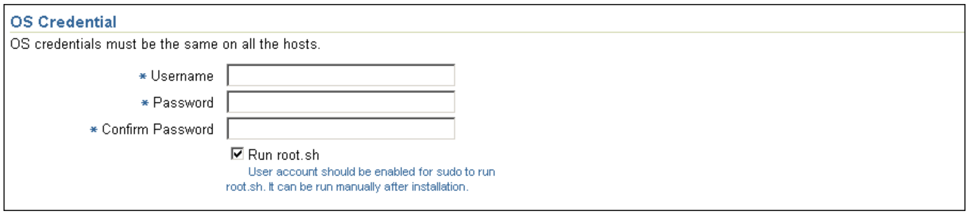
**Note:** When you select the cluster installation option, Agent Deploy performs the Management Agent installation only on those cluster nodes that you have specified, irrespective of the number of hosts that make up that cluster.

For example, if you choose to perform a cluster installation on a cluster having 10 nodes, but specified only 5 nodes, Agent Deploy installs the Management Agent only on the 5 nodes of the cluster that you have specified.

If you are extending an existing cluster, ensure that the cluster name you specify is the same as the existing cluster. You must also specify all the nodes of the existing cluster along with the new node on which you are installing the cluster Management Agent.

8. In the OS Credentials section, specify the appropriate operating system user credentials. Select **Run root.sh** (on UNIX machines only) if you want Agent Deploy to execute this script.

***Figure 10–3 OS Credentials Section of the Installation Details Page***



OS Credential

OS credentials must be the same on all the hosts.

| | |
|---|---|
| * Username | |
| * Password | |
| * Confirm Password | |
| | ☑ Run root.sh<br>User account should be enabled for sudo to run root.sh. It can be run manually after installation. |

**Note:** The OS credentials that you specify here must be the same for all the selected hosts.

The `root.sh` script runs after the configuration assistants are run and before the postinstallation scripts (if any) are run. If you do not select this option here, you must run `root.sh` on each node manually.

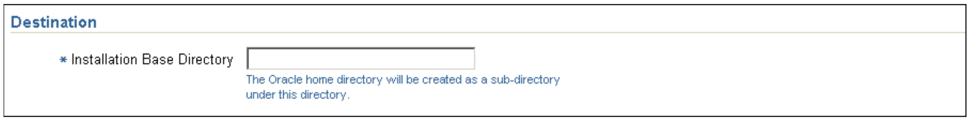
Agent Deploy application uses `sudo` to run the `root.sh` script, and therefore, you must have SUDO privileges to run the script. You must also specify the *invoking user's password* here.

If `/etc/sudoers` is configured in such a way that `sudo` never prompts for a password, then a directory with the host password as the title gets created in the invoking users home directory. To avoid this, ensure that you configure /etc/sudoers file such that running a command using sudo always prompt for a password.

9. In the Destination section, specify the absolute path for the Installation Base Directory. This directory is created on all the specified hosts, and the Management Agent Oracle home directory is created as a subdirectory under this directory.

**Note:** For the Management Agent installation to be successful, ensure that you extract the agentDownload kit before performing the installation.

*Figure 10–4 Destination Section of the Installation Details Page*



Destination

* Installation Base Directory

The Oracle home directory will be created as a sub-directory under this directory.

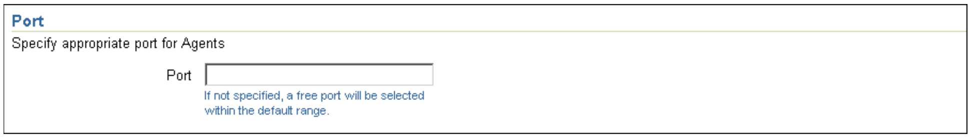
---

**Note:** Ensure you have write permissions on the installation Base Directory that you specify.

---

10. In the Port section, specify the port on which the Management Agent will communicate. The default port value for 10.2 Management Agent is 3872.

*Figure 10–5 Port Section of the Installation Details Page*



Port

Specify appropriate port for Agents

Port

If not specified, a free port will be selected within the default range.

---

**Note:** Ensure that the port you specify is not busy, otherwise the prerequisite check fails. If you do not specify a port here, then the Agent Deploy application automatically picks up a free port (3872 or in the range of 1830 - 1849).

---

11. In the Load Balancer Host and Port section, specify the name of the host and port where the Server Load Balancer is set up so that communication between the Management Agent and the host running the Server Load Balancer can be enabled. This is required only if you are deploying the Management Agent in an environment that has multiple OMSes managed by a Server Load Balancer.

    You can specify an HTTP or HTTPS port. However, if your OMS is configured only for secured communication(HTTPS), then you must specify only an HTTPS port.

---

**Note:** This step is applicable only if you are using Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher. In Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower, the New Agent Installation Wizard does not display this section and for specifying these values, you must update the agentpush.properties file as described in Section 10.1.3, "Configurations Required for Management Agent to Communicate with Oracle Management Service with Server Load Balancer".

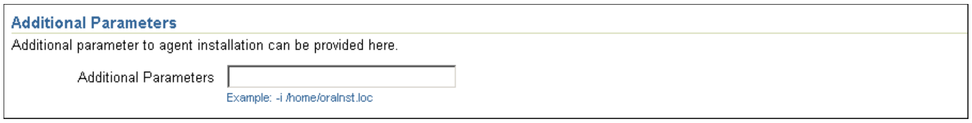
---

**Note:** If your Server Load Balancer is not functional for some reason, then you can optionally specify the host name and port of the OMS that is being managed by the Server Load Balancer. This is however not recommended, so use this option only if your Server Load Balancer has a problem.

---

12. In the Additional Parameters text box, specify any additional parameters that you want to pass during installation.

***Figure 10–6 Additional Parameters Section of the Installation Details Page***



**Additional Parameters**

Additional parameter to agent installation can be provided here.

Additional Parameters [ ]

Example: -i /home/oraInst.loc

The additional parameters you specify here depend on the software source location that you have selected.

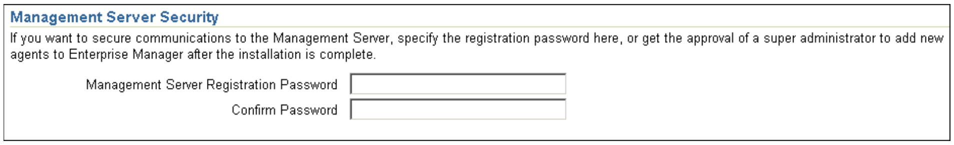
- *Default Management Service Location:* If you have selected the default software source directory, the additional parameters that you specify must be supported by the `agentDownload` script, as the Agent Deploy application uses the `agentDownload.<platform>` script to perform the installation. See Table H–1, " Parameters Supported by agentDownload Script" for a list of all the parameters supported by the `agentDownload` script.
- *Another Location:* If you have selected an alternative software location, the additional parameters that you specify must be supported by Oracle Universal Installer (OUI), as Agent Deploy then uses OUI to perform the installation. See Table H–2, " Parameters Supported by Oracle Universal Installer" for a list of parameters supported by OUI.

Oracle recommends you to specify only those parameters that you want to run in addition to the general parameters you have already provided in this page for installation. For example, in step (7), you are providing the installation base directory. Therefore, for additional parameters, try to avoid specifying the installation base directory again. If you still do so, then the value you specified in step (7) will be ignored and the value you specified here will be used instead.

And note that if you are specifying more than one parameter, then separate them with a white space. For example, `-i /etc/oraInst.loc -p /home/config/staticports.ini`.

13. Specify the Management Service Registration Password if you want to secure communications between the Management Agent and OMS. Alternatively, the super administrator can approve the addition of new agents to Grid Control after the installation is complete.

***Figure 10–7 Management Server Security Section of the Installation Details Page***



**Management Server Security**

If you want to secure communications to the Management Server, specify the registration password here, or get the approval of a super administrator to add new agents to Enterprise Manager after the installation is complete.

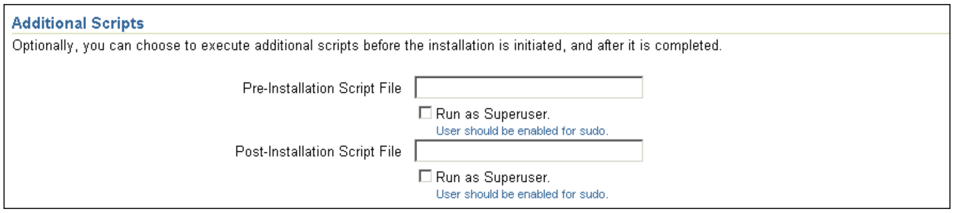
Management Server Registration Password [ ]

Confirm Password [ ]

> **Note:** An unsecure Management Agent cannot upload data to a secure OMS. Oracle also recommends for security reasons that you change the OMS password specified here after the installation is complete.

14. In the *Additional Scripts* section, specify any preinstallation and/or postinstallation scripts that you want to execute.

***Figure 10–8 Additional Scripts Section of the Installation Details Page***



**Additional Scripts**

Optionally, you can choose to execute additional scripts before the installation is initiated, and after it is completed.

Pre-Installation Script File

□ Run as Superuser.
User should be enabled for sudo.

Post-Installation Script File

□ Run as Superuser.
User should be enabled for sudo.

Select **Run as Superuser** if you want to run these scripts as `root`.

> **Note:** The preinstallation and/or postinstallation scripts that you specify must be available on all the hosts. These files are not copied onto the hosts from the software source location during installation.

15. Click **Continue**.

    Grid Control displays the My Oracle Support Details page.

16. On the My Oracle Support Details page, do the following:

    - If the host where the Management Agent is being installed has a *direct* connection to the Internet, then specify an email address and My Oracle Support (formerly Metalink) password.

      An email address is required so that security updates and install updates can be sent. You can specify any email address, but Oracle recommends you to specify the My Oracle Support user name. For example, `john.mathew@xyz.com`.

    - If the host where the Management Agent is being installed has an *indirect* connection to the Internet through a proxy server, then specify an email address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

      > **Note:** You can change the proxy server settings any time after the installation or patching process ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the Management Agent.

    - If the host where the Management Agent is being installed does not have a *direct* or *indirect* connection to the Internet, then specify the email address and leave the other fields blank.

      In this case, after you complete the installation process, 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 10.1.4.1.2, "Manually Collecting and Uploading Configuration Information to My Oracle Support (formerly Metalink)".

**Note:** If you see any errors on this page, then check whether you (the user installing the Management Agent) have the necessary *write* permissions on crontab. If you do not, then create an entry for your user account in the `/usr/lib/cron/cron.allow` file.

17. Click **Continue**.

    As part of this process, Agent Deploy performs some prerequisite checks before proceeding with the installation. When all the prerequisite checks are complete, the application displays the results. You can choose to either retry the prerequisite check on all those failed hosts, or ignore the result and proceed to install the Agent.

**Note:** After the installation and configuration phase, the Agent Deploy application checks for the existence of the Central Inventory (located at `/etc/oraInst.loc`). If this is the first Oracle product installation, Agent Deploy executes the following scripts:

1. `orainstRoot.sh` - UNIX Machines only: This creates oraInst.loc that contains the central inventory.
2. `root.sh` - UNIX Machines only: This runs all the scripts that must be executed as `root`.

If this is not the first Oracle product installation, Agent Deploy executes only the `root.sh` script.

**Note:** If you are installing the Management Agent on a cluster, then note that the preerquisite checks may take some time to complete. For more information on the prerequisite checks, installation, and configuration logs that are created, see Section B.2, "Agent Deploy Log Files".

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

**Note:** Oracle recommends that you view the installation status output (emctl status) to ensure the installation was successful. You can view this status by executing the following command:

```
<AGENT_HOME>/bin/emctl status agent
```

See Section A.1.4, "Management Agent Installation Fails" to view a sample of the `emctl status` log and to troubleshoot possible errors that may occur during installation.

#### 10.1.4.1.1 Scenarios to Consider While Performing a Cluster Agent Install

Consider the following scenarios while performing cluster installation:

**You are performing a new Agent installation on a cluster that does not have an Agent.**

This is a scenario where you have an existing cluster (`cr1` with three nodes n1, n2, and n3) but without Management Agent installation on any of the nodes. Here, if you specify only two nodes (n1 and n2) for Management Agent installation, then the Agent Deploy application updates the inventory for these two nodes and installs the Management Agent on these nodes.

Now, if you want to install the Management Agent on the third node (n3) and specify the cluster name as `cr1` and all three hosts and nodes (n1, n2, and n3) this time, then the Agent Deploy application updates the n1 and n2 inventory to include n3, and then installs the Management Agent only on the third node (n3).

**Caution:** In a scenario such as the one above, you must specify the same cluster name and include all the existing nodes of that cluster.

**You are extending a cluster, but do not include all the existing nodes.**

This is a scenario where you want to install Management Agent on the node (n4) that is an extension of the existing cluster (cr1 with nodes n1, n2, and n3.) But during the Management Agent installation, you specify only the new node (n4) in the Cluster Node List text box. Agent Deploy installs the Management Agent on n4, but does not update the inventory of the other three nodes (n1, n2, and n3) to include n4.

To ensure that the inventory of all the nodes of an existing cluster are updated, you must specify all the hosts and nodes of that cluster along with the new node (n4 in this example.)

If you have specified just the one node and the existing cluster name (cr1), Agent Deploy still creates a new cluster with the same name.

If you have specified just the one node and did not specify a cluster name, Agent Deploy computes a default cluster name and create a new cluster.

**You are installing the Management Agent on two clusters of the same name, but with different nodes.**

You have two clusters with the same name but with different nodes, for example `crs` (with n1, and n2) and `crs` (with n3 and n4), and you want both clusters to be managed by the same OMS. To distinguish the two clusters in the Grid Control console, you must do the following:

When you are installing the Management Agent on the first `crs` cluster (with nodes n1 and n2), enter a unique cluster name and perform the installation. Now, enter a different cluster name for the other `crs` cluster (with nodes n3 and n4) and perform the Management Agent installation.

Now, you can view these clusters in the Grid Control console under unique cluster names that you specified during Management Agent installation.

##### 10.1.4.1.2 Manually Collecting and Uploading Configuration Information to My Oracle Support (formerly Metalink)

To manually collect the configuration information, follow these steps:

1. On the host where the Management Agent is being installed, navigate to the following location. Here, `<OracleHome>` is the Oracle home directory of the Management Agent you installed:

   ```
   <OracleHome>/ccr/bin
   ```

2. Collect configuration information by running the following command:

   ```
   <OracleHome>/ccr/bin/emCCR collect
   ```

   For Oracle Configuration Manager 10.2.7 and higher, the collected configuration information is stored in the `<OracleHome>/ccr/hosts/<hostname>/state/upload/ocmconfig.jar` file. For lower versions of Oracle Configuration Manager, the collected configuration information is stored in the `<OracleHome>/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.

3. Upload the ocmconfig.jar file to a Service Request on My Oracle Support (formerly Metalink) at the following URL:

   `http://metalink.oracle.com/`

#### 10.1.4.2 Installation Using a Shared Agent Home

To deploy and install an Management Agent on multiple hosts using an existing Shared Agent Installation, you must have already performed a complete Grid Control product installation (including the Management Agent). Another prerequisite when using this option is that the directory where the Management Agent is installed should be NFS-mounted, meaning the directory must be a shared location on all remote hosts.

The Agent Deploy application runs a prerequisite checker to ensure the environment meets the requirements for this installation type. See Section G.5, "Prerequisite Checks Executed by Agent Deploy" for more information.

**Caution:** NFS agent deployment is not supported on a cluster. If you want the Management Agent to monitor a cluster and Oracle RAC, you must use the agent deployment with the cluster option, and not the NFS (network file system) deployment method.

**Note:** You can also perform a Shared Agent Oracle home installation using the `nfsagentinstall` script. See Section 10.2, "Installing Management Agent Using nfsagentinstall Script" for more information.

#### 10.1.4.2.1 Concepts and Prerequisites

The following sections briefly discuss the shared agent home concepts, and also list the prerequisites before starting the installation.

**EMSTATE Directory**

This is a directory for storing configuration files such as `emd.properties`, `targets.xml`, `log files`, and so on, on each host. Every host that shares the Management Agent binaries has its own `EMSTATE` directory.

**EMSTATE Directory Location**

- The `EMSTATE` directories of agents on different hosts should be local to the host instead of on the mounted drive, for security reasons.
- Since the `EMSTATE` directory contains the targets pertaining to each host, it is highly recommended to have it on a local host.

**EMSTATE Directory Space Requirements**

The initial space required for `EMSTATE` directories is 1 MB. Since all the upload files, collection files, and log files are stored in this directory, the size of the directory will increase. Consequently, Oracle recommends that you allocate sufficient space for the `EMSTATE` directories after taking these factors into account.

**Packages and OS Patches Requirement**

Currently, no packages are required by the Management Agent to run on the shared hosts.

**Operating System Credentials**

When you are performing Management Agent installation using a shared Oracle home, ensure all the specified hosts have the same operating system credentials and file system structure, including the following:

- Same User names and Group names
- Same user identifiers (UID) and group identifiers (GUID)

This is important for the Management Agent from the remote host (NFS-mounted) to execute certain programs (for example, `ORACLE_HOME/bin/nmo`) that are otherwise not accessible to other users.

**Shared oraInventory**

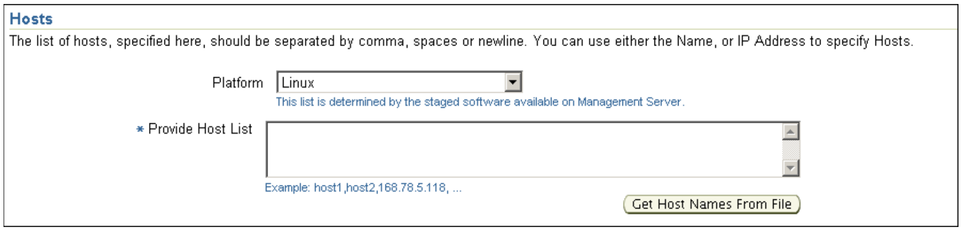
When performing a cluster Management Agent installation using a shared Management Agent Oracle home, ensure the `oraInventory` is shared (accessible by all remote hosts).

#### 10.1.4.2.2 Performing the Installation

To perform a new Management Agent installation:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, from the Agent Installation section, click **Install Agent**.
3. On the Agent Deploy home page, select **Add Hosts to Shared Agent**. The Installation Details screen appears.
4. In the Hosts section:

*Figure 10–9 Hosts Section of the Installation Details Page*



Hosts

The list of hosts, specified here, should be separated by comma, spaces or newline. You can use either the Name, or IP Address to specify Hosts.

Platform: Linux

This list is determined by the staged software available on Management Server.

* Provide Host List

Example: host1,host2,168.78.5.118, ...

**a.** Select the appropriate platform on which you want to perform this installation.

**b.** In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the Management Agent installation.

Alternatively, click **Get Host Names From File** to select the file that contains a list of all the required host names.

If you choose to select a file that contains a list of all required host names, then ensure that the file format is similar to `/etc/hosts` file. Note that the first column of the file must have the host name and when you provide multiple hosts, then ensure that the hosts are mentioned in separate lines. To understand how the format should look, see Example 10–1, "Host File Format".

The Agent Deploy application picks up only the values in the first column of the Host List file that you specify/select. Ensure that the host list format is appropriate because the Agent Deploy application does not validate this format on the selected file.

---

**WARNING: Do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs. Use the same host names for which the SSH has been set.**

---

**Caution:** If the Installation Base Directory is shared among the hosts that you have specified in the host list, the installer is invoked from one of these hosts (typically, the first host in that list).

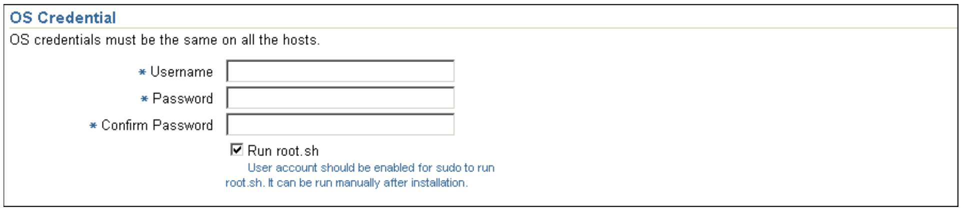
While the installation is performed on only one host, the application executes the configurations on all nodes in the list. That is, the preinstallation, postinstallation, and collect logs are executed on all the nodes.

After the installation is complete, the Installation Status screen displays the status of only this host (from which the installer was invoked). It may not necessarily list the status of all the hosts specified in the host list.

---

**5.** In the OS Credentials section:

***Figure 10–10 OS Credentials Section of the Installation Details Page***



OS Credential

OS credentials must be the same on all the hosts.

* Username

* Password

* Confirm Password

☑ Run root.sh

User account should be enabled for sudo to run root.sh. It can be run manually after installation.

**a.** Specify the appropriate operating system user credentials.

---

**Note:** The OS credentials that you specify here must be the same for all the selected hosts.

---

**b.** Select **Run root.sh** (on UNIX machines only) if you want Agent Deploy to execute this script.

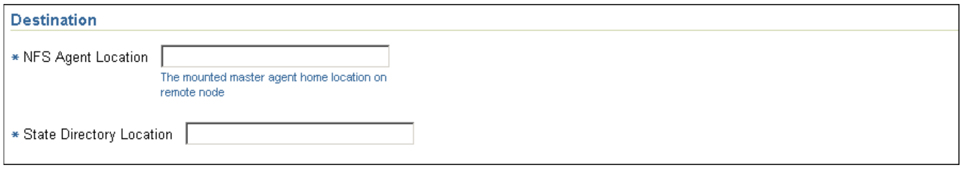
The `root.sh` script runs after the configuration assistants are run and before the postinstallation scripts (if any) are run. If you do not select this option here, you must run `root.sh` on each node manually.

Agent Deploy application uses `sudo` to run the `root.sh` script. You must specify the *invoking user's password* here.

If `/etc/sudoers` is configured in such a way that `sudo` never prompts for a password, then a directory with the host password as the title gets created in the invoking users home directory. To avoid this, ensure that you configure /etc/sudoers file such that running a command using sudo always prompt for a password.

**6.** In the Destination section:

***Figure 10–11 Destination Section of the Installation Details Page***



Destination

* NFS Agent Location

The mounted master agent home location on remote node

* State Directory Location

**a.** Specify the complete path to the NFS Agent Location. This is the shared directory location on the source Management Agent host that must be visible (NFS-mounted) from all remote hosts.

---

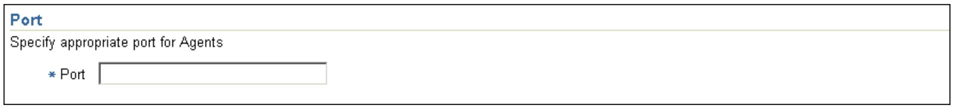
**Note:** Ensure that the directory to which the NFS Agent is mounted on the remote hosts is the same as the NFS Agent home directory on the source host. For example, if the NFS Agent is installed at /scratch/oraclehome/agent10g, then on all the target remote hosts, the location /scratch/oraclehome/agent10g must refer to the same NFS Agent home directory.

---

**b.** Specify an appropriate EMState Directory Location. This is a directory for storing configuration files such as `emd.properties`, `targets.xml`, `log` `files`, and so on, on each host. Every host that shares the Management Agent has its own `EMSTATE` directory.

7. In the Port section, specify the appropriate port on which the Management Agent will communicate. This is a mandatory field if you are using Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower.

***Figure 10–12 Port Section of the Installation Details Page***



Port

Specify appropriate port for Agents

* Port

> **Note:** Ensure that the port you specify is not busy, otherwise the prerequisite check fails. If you do not specify a port here, then the Agent Deploy application automatically picks up a free port (3872 or in the range of 1830 - 1849).

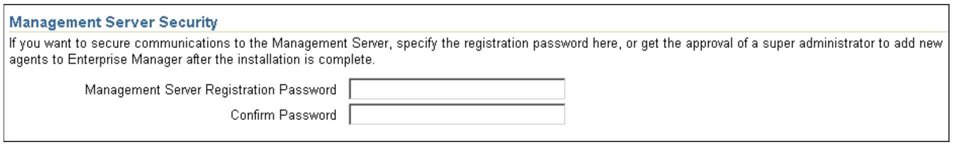
8. In the Additional Parameters section, specify the parameters that you may want to pass during installation. You can specify multiple parameters, separated by a white space.

   Oracle recommends you to specify only those parameters that you want to run in addition to the general parameters you have already provided in this page for installation. For example, in step (5), you are providing the port. Therefore, for additional parameters, try to avoid specifying the port again. If you still do so, then the value you specified in step (5) will be ignored and the value you specified here will be used instead.

> **Note:** Besides the timezone parameter (`-z`), you can also specify all the parameters that are supported by the agentDownload script. See Section H.1, "Additional Parameters Supported by agentDownload Script" for more information.

9. In the Management Server Security section:

***Figure 10–13 Management Server Security Section of the Installation Details Page***



Management Server Security

If you want to secure communications to the Management Server, specify the registration password here, or get the approval of a super administrator to add new agents to Enterprise Manager after the installation is complete.

Management Server Registration Password

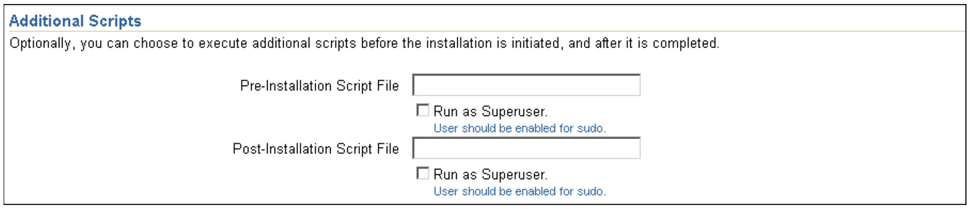
Confirm Password

Specify the Management Service Registration Password if you want to secure communications between the Management Agent and the OMS. Alternatively, the super administrator can approve the addition of new agents to Grid Control after the installation is complete.

**Note:** An unsecure Management Agent cannot upload data to the OMS. Oracle also recommends for security reasons that you change the OMS password specified here after the installation is complete.

10. In the Additional Scripts section:

*Figure 10–14 Additional Scripts Section of the Installation Details Page*



Additional Scripts

Optionally, you can choose to execute additional scripts before the installation is initiated, and after it is completed.

Pre-Installation Script File

□ Run as Superuser.
User should be enabled for sudo.

Post-Installation Script File

□ Run as Superuser.
User should be enabled for sudo.

a. Specify any preinstallation and/or postinstallation scripts that you want to execute. These scripts are optional. If you do not want to customize your installation, leave these fields blank and continue.

b. Click **Continue** to start the installation process.

**Caution:** If the shared Management Agent is the first Oracle product that is installed on the host, you must execute the following command from the `EMSTATE` directory after completing the installation:

```
<EMSTATE Dir>/bin
./emctl control agent runCollection <Host name>:host Inventory
```

As part of this process, Agent Deploy performs some prerequisite checks before proceeding with the installation. When all the prerequisite checks are complete, the application displays the results. The results include the name, type, and status for all prerequisite checks designed for the installation.

Besides the successfully run prerequisite checks, the prerequisite checks can return either one of the following messages:

- *Warning*: If there are warnings against certain prerequisite checks, you may choose to ignore these and continue with the installation (though this is not recommended).
- *Failed*: If there are failed prerequisite checks, you cannot continue with the installation if you are using Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower. A recommended course of action is to fix the failed prerequisites before proceeding with the installation. However, if you are using Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher, then you can still continue with the installation.

To fix the failed prerequisites, you can either click **Retry**, or go to the Fixup screen of the application. The Fixup screen displays the prerequisites that can be automatically fixed, and those that require manual fixes.

**Note:** You can view the status of all previous installation instances from the Status screen in the Agent Deploy application. This screen lists all Management Agent installations that were performed using Agent Deploy. You can click the corresponding Status link for each record to view the selected installation details, including user input provided during installation and the final status of that installation.

You can access the Status screen either before starting the installation process, or after the installation is complete. You cannot access the Status screen during an installation.

## 10.2 Installing Management Agent Using nfsagentinstall Script

This section describes how you can install a Management Agent using the nfsagentinstall script. In particular, this section covers the following:

- Overview
- Prerequisites
- Installation Procedure

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 10.2.1 Overview

In this installation method, the software bits of a Management Agent are shared on a NFS disk, and other hosts share these binaries to run the Management Agent processes on each of the hosts. The one that shares its binaries, in this context, is called *Master Agent*, and the one that is installed by the nfsagentinstall script is called *NFS Agent*. Here, the configuration files for each host are stored in the 'State Directory'.

However, this installation method, has the following limitations:

- You can perform only one nfsagent installation per host. Multiple nfsagent installations on the same host will fail. If you try to install multiple nfsagents, then the following warning and recommendation appear:

  ```
  Warning: An agent home exists in the specified oracle home
  ```

  ```
  Recommendation: Uninstall the existing agent that exists in
  the specified oracle home
  ```

- This installation type is not supported on clusters. In order to monitor clustered hosts or RAC databases, the best practice would be to use the Agent Deploy application with the cluster option rather than the NFS deployment model.
- This installation type is not supported on an Oracle Cluster Shared File System (OCFS) drive, but is supported on an NAS (Network Attached Storage) drive.

### 10.2.2 Prerequisites

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

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

*Table 10–3 Prerequisites for Installing a Management Agent Using nfsagentinstall Script*

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the hardware and softwrae requirements.<br>For hardware requirements, see Section 3.1, "Hardware Requirements". For software requirements, see Section 3.3, "Software Requirements". | |
| Operating System Requirements | Check if that operating system on which you are going to install the Management Agent is ceritified.<br>For information about certified operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |
| Package Requirements | Install the packages that are required for your operating system.<br>For information about packages, see Appendix G.1, "Check Platform-Specific Package Requirements for Agent Installation". | |
| Operating System Group Requirements | Ensure that you are part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite. | |
| User and Operating System Group Requirement | Ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created.<br>For information about creating operating system groups and users, see Section 3.6, "Operating System Groups and Users Requirements". | |
| Operating System Requirements | Ensure that the operating system (and version) of the target host where the NFS Agent needs to be installed is the same as the operating system (and version) of the host where the master agent is located. If the target host has a different operating system, then the NFS Agent installation will fail. For example, if the master agent is on Red Hat Linux Version 4, then the NFS agent can be installed only on those host that run Red Hat Linux Version 4. If you try to install on Red Hat Linux Version 3 or a different operating system for that matter, then the NFS installation will fail. | |
| Path Validation Requirements | Validate the path to all command locations. For more information, see Section G.3, "Validate All Command Locations". | |
| Permission Requirements | Ensure that you have read, write, and execute permissions to `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, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.<br>For information about oraInventory permissions, see Section 4.8, "Installing Enterprise Manager Grid Control As the First Oracle Software". | |
| User Credentials Requirements | Ensure that you use the same user credentials that were used to perform the master agent installation (the main Management Agent that is sharing its binaries). | |

*Table 10–3 (Cont.) Prerequisites for Installing a Management Agent Using nfsagentinstall Script*

| Requirement | Description | Yes/No |
|---|---|---|
| Verifying oraInst.loc and inventory_loc | If this shared agent installation is not the first Oracle product installation and your home directory (of the master agent installation) is shared, then you must verify the `oraInst.loc` location under the `/etc` directory.<br>If `oraInst.loc` and `inventory_loc` are located in the your home directory, then you must change this entry point to a non-shared location.<br>The `oraInst.loc` entry should look like this:<br>`inventory_loc=/<any location other than the home directory>/oraInventory`<br>`inst_group=<group to which the user belongs>` | |
| 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 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. | |
| Default Port Requirements | Ensure that the SSH daemon is running on the default port (that is, 22) on all the target hosts.<br>■ For Enterprise Manager 10g Grid Control Release 4 (10.2.0.4), the port must be 22. If it is any other port, then the installation fails.<br>■ For Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), the port can be 22 or any non-default port, that is, any port other than 22. If the port is a non-default port, then update the SSH_PORT property in the following file to ensure successful installation:<br>For default location:<br>`<OMS_HOME>/sysman/agent_download/<VERSION>/<PLATFORM>/agentdeploy/Paths.properties`<br>For another location (non-default):<br>`<OMS_HOME>/sysman/prov/resources/Paths.properties` | |
| SUDO Requirements | Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.<br>To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.<br>`<user> <hostname>=PASSWD: /home/em/agent10205/agent10g/root.sh, /bin/sh` | |

*Table 10–3 (Cont.) Prerequisites for Installing a Management Agent Using nfsagentinstall Script*

| Requirement | Description | Yes/No |
|---|---|---|
| PubkeyAuthentication Parameter Requirements | Ensure that the `PubkeyAuthentication` parameter is enabled in the sshd_config file.<br>To verify the value of this parameter, run the following command:<br>`grep PubkeyAuthentication /etc/ssh/sshd_config`<br>The result of this command must be *Yes*. If the result is *No*, then edit the `/etc/ssh/sshd_config` file and set the PubkeyAuthentication value to *Yes*. | |
| NFS-Mounted Location Requirements | Ensure that the NFS-mounted shared location is always readable from the remote hosts. | |
| Agent User Account Permissions and Rights (For Microsoft Windows) | (For Microsoft Windows) Ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Increase quotas.<br>■ Replace process level token.<br>■ Log in as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>1. Launch the Local Security Settings.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Settings**.<br>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) Grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` | |

You can view the prerequisite checks and installation status from the Status screen in the Agent Deploy application. For more information about prerequisite checks related to Agent Deploy application, see Appendix G, "Agent Deploy Application - Installation Prerequisites".

**WARNING: Do not attempt to view the prerequisite check status while the prerequisite checks are still in progress. If you do so while the checks are still in progress, the application will display an error.**

## 10.2.3 Installation Procedure

To perform a Management Agent installation using `nsfagentinstall` script, complete the following steps:

1. Configure the shared drive on the host in such a way that only one host has read/write access to this shared location, while all the other hosts have only read access.
2. From the host that has read/write access, perform Management Agent installation in the shared Oracle home location. You can use any agent deployment method. This installation is called as the *master* agent installation.
3. Stop the Management Agent from the Oracle home.

   > **Note:** You must *not* start the master agent from the installed Oracle home.

4. Now, execute the `OH/sysman/install/nfsagentinstall` script on all the hosts that should share the Management Agent binaries, including the host on which you performed the master agent installation.
5. If this Management Agent installation is the first Oracle product installation on the host, the `nfsagentinstall` script prompts you to execute the following script (on UNIX machines only). You must execute this script manually.

   ```
   <homedir>/oraInventory/orainstRoot.sh
   ```

   The `nfsagentinstall` script also prompts you to execute the `<STATEDIR>/root.sh` command. You must execute this command manually.

   > **Note:** If you already have targets running on the host where you are installing the NFS Agent, then after the NFS Agent installation completes successfully, the targets are automatically discovered and added to Grid Control. However, if you install another target on that host after the NFS Agent installation completes, then you must manually discover that newly installed target by running the `agentca` script from the `<NFSAGENT_STATEDIRECTORY>/bin` directory.

### 10.2.3.1 Usage of the nfsagentinstall Script

```
./nfsagentinstall  -s <EMSTATE Directory location> -p <port number>
```

In the preceding command syntax,

- <EMSTATE Directory location> is the full path where you want the state directory to be created by the script.
- <port number> is the port on which the Management Agent runs.

> **Note:** Specifying the <port_number> argument is optional. If you do not specify the port number, the script will automatically select the next available port from that host.

**Caution:** If the nfsagent is the first Oracle product that is installed on the host, you must run the following command from the EMSTATE directory after completing the installation:

```
<EMSTATE Dir>/bin
./emctl control agent runCollection <Host name>:host Inventory
```

## 10.3 Installing Management Agent Using agentDownload Script

This section describes how you can install a Management Agent using the agentDownload script. In particular, this section covers the following:

- Overview
- Benefits of Using the Script
- Downloading the Script
- Installation Procedure
- Installing on a Cluster
- Customizing the agentDownload Script
- Downloading Management Agent Software for Different Platforms

**Note:** This installation method is supported on Microsoft Windows only from Enterprise Manager 10g Grid Control Release 2 (10.2.0.2).

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 10.3.1 Overview

The agentDownload script uses the *pull* technology for Management Agent installations. That is, it it not necessary for the script to exist on a local file system, it must always be run from the target host computer. You must be logged in to the target host to run the script. Files are not pushed from a central location to a list of target hosts. Instead, files are pulled to the local $ORACLE_HOME from the staged product installation location.

This means that the agentDownload script needs to be launched from each target host where you want to install the Management Agent. As the installation is scripted, it is possible to use a wrapper script, Linux cron job, rdist, or a combination of operating system features to fully automate this process for mass deployments.

**Note:** Use the agentDownload script to perform Management Agentinstallation on a cluster environment. See Section 10.3.6, "Installing on a Cluster" for more information.

The agentDownload script performs the following actions:

- Creates home directories for the Management Agent and Oracle Universal Installer if they do not exist, based on the $ORACLE_HOME path specified through the command line.

- Downloads the agent_download.rsp response file from the OMS Web server.

  The OMS instantiates the response file with the name and port number of the OMS. As a result, the Management Agent you install is configured to use the OMS from which the response file was downloaded.

- Downloads an Oracle Universal Installer JAR file for the target operating system from the OMS Web server (for UNIX only).
- Extracts Oracle Universal Installer and points it to the product definition file (products.xml) hosted by the OMS Web server.
- Starts Oracle Universal Installer in silent mode from the local machine; Universal Installer pulls files from the Web server to the target machine via HTTP.

> **Note:** This script uses the -ignoresysPrereqs flag to bypass prerequisite check messages for operating system-specific patches during installation; prerequisite checks are still performed and saved to the installer logs. While this makes the Management Agent easier to deploy, check the logs to make sure the target machines on which you are installing Management Agents are properly configured for successful installation.

- The resulting installation and configuration, including the automatic discovery of managed targets on the Management Agent host, is identical to that provided by the Management Agent installation on the Grid Control DVD set.
- The agentDownload script creates a log file in the base directory that is specified using the -b option.
- At the end of a successful installation, the Agent starts and should begin successfully uploading to the OMS, presuming automatic discovery and automatic start were not disabled at the command line.

To run the script, use the following command:

```
./agentDownload.<platform> [-bcdhilmnoprtuxN]
```

For Linux operating system, the command would be as follows:

```
./agentDownload.linux [-bcdhilmnoprtuxN]
```

The descriptions of the script options are listed in Table 10–4.

*Table 10–4 AgentDownload Script Options*

| Option | Description |
|---|---|
| -b | To specify base directory of the Agent Oracle home. |
| -c | To specify the cluster nodes ("CLUSTER_ NODES={node1,node2,node3}")<br>Note that there should not be any spaces between the entries in the comma-separated nodes list. Also ensure that you specify only short names of the host, not their fully-qualified names. |
| -d | Do not automatically discover targets during installation. Host target will be created as needed. |
| -h | To display and describe the options that can be used with this script. |

*Table 10–4 (Cont.) AgentDownload Script Options*

| Option | Description |
|---|---|
| -i | To specify the location to the oraInst.loc file.<br>The oraInst.loc file contains the complete path to the inventory directory. This option can be used to point the installer to a non-default inventory. (For advanced users only.) |
| -l | To specify as local host (pass -local to runInstaller) |
| -m | To specify the OMS host name for downloading the Management Agent install. |
| -n | To specify the cluster name. |
| -o | To specify the OLD_ORACLE_HOME during upgrade |
| -p | To specify static port list file. |
| -r | To specify the port for connecting to the OMS host name. |
| -R | To use virtual host name(ORACLE_HOSTNAME) for this installation. If this is being used along with more than one cluster nodes through "-c" option, then "-l" option also needs to be passed. |
| -t | Do not automatically start the Management Agent at the end of the installation. |
| -u | To upgrade. |
| -v | To specify the location to the inventory directory. For example, /scratch/oraInvenotry. |
| -x | To debug output: Turns on shell debugging. |
| -N | Do not prompt for Agent Registration Password. |

## 10.3.2 Benefits of Using the Script

The download script deploys the standard Management Agent installation with some additional benefits:

- Can be modified for specific user environments.
- Noninteractive, silent, installations.
- Output is text-only (nongraphical).
- Management Agents installed using the script are identical to Management Agents installed with the Oracle Universal Installer graphical installation.
- Simplifies deploying Management Agents in secure Web environments that are configured to provide HTTP access.
- Provides useful installation options using the command line (including the ability to control target autodiscovery, autostarting of the Management Agent, and so on).
- Allows installation onto clustered environments.

## 10.3.3 Prerequisites

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

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

*Table 10–5 Prerequisites for Installing a Management Agent Using agentDownload Script*

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the hardware and softwrae requirements.<br>For hardware requirements, see Section 3.1, "Hardware Requirements". For software requirements, see Section 3.3, "Software Requirements". | |
| Operating System Requirements | Check if that operating systemon which you are going to install the Management Agent is ceritified.<br>For information about certified operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |
| Package Requirements | Install the packages that are required for your operating system.<br>For information about packages, see Appendix G.1, "Check Platform-Specific Package Requirements for Agent Installation". | |
| Operating System Group Requirements | Ensure that you are part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite. | |
| User and Operating System Group Requirement | Ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created.<br>For information about creating operating system groups and users, see Section 3.6, "Operating System Groups and Users Requirements". | |
| Permission Requirements | Ensure that you have read, write, and execute permissions to `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, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.<br>For information about oraInventory permissions, see Section 4.8, "Installing Enterprise Manager Grid Control As the First Oracle Software". | |
| 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 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 10–5 (Cont.) Prerequisites for Installing a Management Agent Using agentDownload Script*

| Requirement | Description | Yes/No |
|---|---|---|
| Host Name Requirements | Ensure that the name of the host on which the installation is being performed is neither `localhost.localdomain` nor an IP address. It must be a valid host name.<br>At the time of invoking the installer, you can pass `ORACLE_HOSTNAME=<host_name> -local` as an argument.<br>Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name> -local`** | |
| Install Directory Requirements | Ensure that the installation base directory does not contain any other Oracle software.<br>Ensure that this location is not a symlink.<br>Ensure that you have write permission on this location to create the `agent10g` directory. | |
| OMS Requirements | Ensure that you already have an OMS running in your enterprise because the agentDownload script needs to be downloaded from the OMS host. | |
| File-Protection Setting Requirements | Ensure that the execute binary is set and the script file has proper file-protection settings. You can use `chmod` to ensure the file has the correct privileges. | |
| WGET Requirements | The `wget` (or other file transfer mechanism) has been defined in the script. The script checks for the existence of `wget` in `/usr/local/bin/wget`, followed by `/usr/bin/wget`. If wget is not found in either of those locations, then it must be included in the `$PATH` or the script will exit with an error | |
| SUDO Requirements | Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.<br>To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.<br>`<user> <hostname>=PASSWD: /home/em/agent10205/agent10g/root.sh, /bin/sh` | |
| Load Balancer Requirements | If the OMS is using a load balancer, you must modify the `s_omsHost` and `s_omsPort` values in the following file (Here, ORACLE_HOME is the Oracle home directory of the OMS):<br>`<ORACLE_HOME>/sysman/agent_download/<version>/agentdownload.rsp` | |

*Table 10–5 (Cont.) Prerequisites for Installing a Management Agent Using agentDownload Script*

| Requirement | Description | Yes/No |
|---|---|---|
| Agent User Account Permissions and Rights (For Microsoft Windows) | (For Microsoft Windows) Ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Increase quotas.<br>■ Replace process level token.<br>■ Log in as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>1. Launch the Local Security Settings.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Settings**.<br>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) Grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` | |

## 10.3.4 Downloading the Script

The downloadable Management Agent software for the operating system of the OMS host is available on the platform-specific CD from which the OMS was installed, and from the Oracle Technology Network Web site under Mass Agent Deployment at:

`fhttp://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`

See Section 10.3.8, "Downloading Management Agent Software for Different Platforms" for more information on obtaining Management Agent installables for different platforms.

## 10.3.5 Installation Procedure

The `agentDownload` script is downloaded to a target node and run to initiate a silent Oracle Universal Installer session. The Management Agent files are copied from the staging area of the OMS home to the target node using HTTP.

To install a Management Agents, do the following:

1. Ensure that you have the correct version of the `agentDownload` script that you want to download and use for installing the Management Agent.

The `agentDownload` script is part of the Management Agent software that is available in the `agent_download` directory within the Oracle home directory of the OMS. For example, `ORACLE_HOME/sysman/agent_download/<version>/<platform>/agentDownload.<platform>`

This agent_download directory is the Web server alias created by OMS installation. The directory maps to a physical directory in the Oracle Application Server home directory where the OMS is installed and deployed. Using this Web server alias, you can download the script to the target host using the OMS URL.

The <version> is release of the Management Agent software. If you want to use a higher release of the Management Agent software or for another platform, then you can download the software for that release or platform from the following URL:

http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html

After you download the latest, you will have to extract the contents in the correct directory location. For information about this, see Section 10.3.8, "Downloading Management Agent Software for Different Platforms".

2. Download the `agentDownload` script to the target host from the OMS URL.

   As described in the previous step, using this Web server alias, you can download the script to the target host using the OMS URL. For example, if OMS is installed on `mgmthost27.acme.com`, then download the `agentDownload` script from the following URL:

   ```
   http://mgmthost27.acme.com:4889/agent_download/<version>/<platform>/agentDownload.<OS>
   ```

   For Microsoft Windows, the URL to download the script is as follows:

   ```
   http://mgmthost27.acme.com:4889/agent_download/<version>/win32/agentDownload.vbs
   ```

   For Microsoft Windows, you can also access the `agentDownload` script from the command line by running one of the following commands:

   - `wget http://mgmthost27.acme.com:4889/agent_download/<version>/<platform>/agentDownload.<OS>`
   - `wget http://mgmthost27.acme.com:4889/agent_download/<version>/win32/agentDownload.vbs`

   **Note:**

   - The default port for Grid Control is 4889. This should be available after you install the OMS.
   - The `<version>` argument represents the version of the Management Agent avaliable on OMS host.
   - The `<OS>` argument represents the platform. For example, for Linux, the script is named `agentDownload.linux`. For Windows operating systems, the script is named `agentDownload.vbs`.

Any method of retrieving the file is acceptable: cp, rcp, scp, FTP, and so on. The script can also be retrieved by opening a browser window on the target machine and saving the link to a local file.

> **Note:** If you want to download using a file-based protocol rather than HTTP, you need to modify the `$AgentDownload` URL variable to access the file system on the Management Server host instead of a URL.
>
> The URL is the following:
>
> ```
> http://${OMShost}:${httpPort}/agent_download/
> ```
>
> is a Web alias for:
>
> ```
> $OMS_HOME/sysman/agent_download/
> ```

3. Run the following command to invoke the `agentDownload` script on the target host.

   ```
   ./agentDownload.<platform> -b <base directory> -m <full path
   to the OMS host> -r <port>
   ```

   The base directory is the location in which the Oracle home directory for the Management Agent will be created. For example, if you specify `/scratch/agent_download` as the base directory, then `agent10g` is created as a subdirectory in this base directory.

   For information about the other arguments that can be used in this command, see Table 10–4, " AgentDownload Script Options". Alternatively, you can run the following command to see online help:

   ```
    ./agentDownload.<platform> -help
   ```

4. After the installation completes successfully, run the following scripts as a *root* user from each of the hosts.

   - If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the Central Inventory:

     ```
     $ORACLE_HOME/oraInventory/oraInstRoot.sh
     ```

     For example, if you are using sudo to change to a root user, then you will run the following command:

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

   - Run the `root.sh` script from the Oracle home directory of the Management Agent:

     ```
     <agent_oracle_home>/root.sh
     ```

     For example, if you are using sudo to change to a root user, then you will run the following command:

     ```
     /usr/local/bin/sudo /scratch/OracleHomes/agent10g/root.sh
     ```

   The `root.sh` script must be run as `root`; otherwise, the Grid Control job system will not be accessible to the user. The job system is required for some Grid Control features, such as hardware and software configuration tasks and configuring managed database targets.

5. Finally, secure the Management Agent.

   For Management Agents 10g Release 2 (10.2.0.2) or lower, secure the Management Agent by running the following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

   ```
   <Agent_Home>/bin/emctl secure agent
   ```

   For Management Agent 10g Release 3 (10.2.0.3) or higher, secure the Management Agent in one of the following ways:

   a. Set the environment variable AGENT_INSTALL_PASSWORD

   b. Set the password in the `agent_download.rsp` file.

   c. Do not perform Step (6.a) and Step (6.b) so that you can be prompted by the script. At the prompt, provide the Management Agent registration password.

## 10.3.6 Installing on a Cluster

The `agentDownload` script can be used to install Management Agents onto clustered environments. In order to perform this type of installation, the command-line options to be used are listed in Table 10–6.

***Table 10–6 Command-Line Options for Cluster Installation***

| Options | Description |
|---|---|
| -c | This option is followed by a comma-separated list of the nodes in the cluster. It is possible to install a standalone Management Agent that will still discover cluster targets by not specifying this option, while still specifying the cluster name with the `-n` option. |
| -n | This option is followed by the name of the cluster. This option is required for Oracle9*i* clusters; for Oracle Database 10*g* clusters, if this option is not specified, the default cluster name from the `targets.xml` file will be used. |
| -l | This option specifies that the installation should be done just on the local node of the cluster. |

For example, to use the `agentDownload` script to install a Management Agent on just the local node of a cluster that consists of nodes *host1*, *host2*, and *host3*, with cluster name *myCRS*, you must execute the following:

```
./agentDownload.<platform> -b <name of the Oracle Homes> -m <fully-qualified
Oracle Management Service host name> -r <Oracle Management Service ports> -c
"host1,host2,host3" -n myCRS -l
```

For example for Linux operating system, the command would be as follows:

```
./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889 -c
"host1,host2,host3" -n myCRS -l
```

## 10.3.7 Customizing the agentDownload Script

You can edit the contents of the `agentDownload` script so it uses a specific tool for transferring files from the OMS Web server. The contents of the file contain instructions for doing so, as shown in the following example:

```
WGET="/usr/local/bin/wget --dot-style=mega --verbose --tries=5"
InstallerDownloadCmd=$WGET
# Define the command to be used to download the jarred installer from
```

```
# the web server hosting the OMS.
# Other download possibilities: ftp; cp/scp; use local browser to save the
# link to a file on the target machine.
# This example uses wget, a GNU tool for http and ftp file transfers.
# If the products.xml referenced by the Oracle Installer is a URL, then the
# Installer will download its files via http. This greatly facilitates
# performing installs in a secure environment that may include firewalls
# and servers with limited access (no ftp server, NFS mounts not available,
# etc.).
# Enterprise Manager version number. This is used to construct the
# home name used by the installer
```

`GNU wget` is available for most platforms and can be downloaded from the following location:

```
http://www.gnu.org/software/wget/wget.html
```

## 10.3.8 Downloading Management Agent Software for Different Platforms

**To Obtain agentDownload for Unix**

Follow the instructions below to download the Management Agent installation software for Unix:

1. Download the `<platform>_Grid_Control_agent_download_10_2_0_X.zip` file from OTN:

   `http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`

2. Copy the downloaded file to the `<OMS_HOME>/sysman/agent_download/10.2.0.X.0` directory.

   **Note:** Create the `<OMS_HOME>/sysman/agent_download/10.2.0.X.0` directory, if it does not exist.

3. Go to this directory by executing the following:

   ```
   cd <ORACLE_HOME>/sysman/agent_download/10.2.0.X.0
   ```

   When you are here, confirm that the size and checksum calculation of the downloaded file match the information specified on the OTN download page.

4. Execute the following command:

   ```
   unzip <platform>_Grid_Control_agent_download_10_2_0_X.zip
   ```

5. If the agent_download.rsp file does not exist in the `<OMS_HOME>/sysman/agent_download/10.2.0.X.0` directory, do the following:

   1. Execute `mv agent_download.rsp.bak agent_download.rsp`
   2. Edit agent_download.rsp and modify `s_OMSHost="REPLACE_WITH_OMS_HOST"` and `s_OMSPort="REPLACE_WITH_OMS_PORT"` variables with the correct OMSHost and OMSPort values. For example:

      ```
      s_OMSHost="foo.us.oracle.com"
      s_OMSPort="4889"
      ```

> **Note:** Even if you are specifying a secure OMS, you must still enter the non-secure port number here.

6. Download the agentDownload script by using cp, rcp, scp, FTP, or wget utility.

   An example of using wget is as follows:

   ```
   wget http://foo:4889/agent_download/10.2.0.X.0/linux/agentDownload.linux
   ```

7. Run the following command:

   ```
   chmod +x agentDownload.linux
   ./agentDownload.linux -b <name of the Oracle Homes> -m <fully-qualified Oracle
   Management Service host name> -r <Oracle Management Service ports>
   ```

   For example:

   ```
   ./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889
   ```

   For clusters, use the following command:

   ```
   ./agentdownload.linux - b /oracle/agentinstall -m foo.us.oracle.com -r 4889 -c
   "host1,host2,host3" -n myCRS -l
   ```

   To view more options, use the ./agentdownload.linux -h command.

**To obtain agentdownload for Windows:**

Follow the instructions below, to download the Management Agent installation software for Windows:

> **Note:** Ensure that you have Microsoft Internet Explorer version 6.0 or higher installed on the host where you are downloading the script.

1. Download the `Win32_Grid_Control_agent_download_10_2_0_X.zip` file from OTN:

   ```
   http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html
   ```

2. Copy the downloaded file to the `<OMS_HOME>/sysman/agent_download/10.2.0.X.0` directory.

   > **Note:** Create the `<OMS_HOME>/sysman/agent_download/10.2.0.X.0` directory, if it does not exist.

3. Go to this directory by executing the following:

   ```
   cd <OMS_HOME>/sysman/agent_download/10.2.0.X.0
   ```

   When you are here, confirm that the size and checksum calculation of the downloaded file match the information specified on the OTN download page.

4. Extract the contents of this file by running the following:

   ```
   unzip Win32_Grid_Control_agent_download_10_2_0_X.zip
   ```

5. After extracting the contents, the `agentdownload.vbs` will be available at `<OMSHOME>/sysman/agent_download/10.2.0.X.0/win32/agentdownload.vbs`.

6. Download the `agentDownload.vbs` by using cp, rcp, scp, FTP, or wget utility on the machine where you want to install the Management Agent.

> **Note:** To download agentDownload script using wget utility, ensure that the wget utility exists on the Windows path variable

> **Note:** Before executing the `agentDownload.vbs` script, ensure *Windows Script Host version 5.6* is installed on the target Management Agent host. This is required for the script to be executed successfully.

7. Run the `agentDownload.vbs` script:

```
cscript.exe agentdownload.vbs -b <basedir name> -m
<omshostname> -r <httpport>
```

For example:

```
cscript.exe agentDownload.vbs -b /oracle/agentinstall -m foo.us.oracle.com -r
4889
```

For clusters, use the following command:

```
cscript.exe agentdownload.vbs -b <basedir name> -m
<omshostname> -r <httpport> -c <node1, node2, node3...> -n
<cluster_name> -l
```

For example:

```
cscript.exe agentdownload.vbs - b /oracle/agentinstall -m foo.us.oracle.com -r
4889 -c "host1,host2,host3" -n myCRS -l
```

## 10.4 Installing Management Agent Using OUI

This section describes how you can install a Management Agent using Oracle Universal Installer. In particular, this section covers the following:

- Overview
- Prerequisites
- Installation Procedure

> **Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 10.4.1 Overview

Oracle Universal Installer (OUI) is an interactive, GUI-based installer offered by Oracle for all its products. The OUI referred here is the installer provided for Enterprise Manager 10g Grid Control Release 2 or higher.

The default port for Management Agent is 3872. For more information about the default ports that are assigned and the  possibility of using custom ports instead of default ports, see Section 4.9, "Knowing About the Ports Used for Installation".

**Note:** By default, this installation option from Oracle Universal Installer uses the Management Agent software that is arealdy available on the host running OMS, and installs Oracle Management Agent 10g Release 1 (10.2.0.1). If you need the latest release of Management Agent, then you must patch this first release with the help of the latest patch set. The patch sets are available on My Oracle Support (formerly Metalink) at:

`http://metalink.oracle.com/`

Alternatively, to install the latest release of Management Agent, you can use the Management Agent software kit (full kit) that is available on Oracle Technology Network (OTN) at:

`http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`

You can accept the license agreement, download the software kit (zip file), extract the contents, and invoke the runInstaller from there to start Oracle Universal Installer.

**Note:** Grid Control does not support uploading of data to the same Management Repository from two Management Agents running on the same host.

## 10.4.2 Prerequisites

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

If you want, you can print out this section and write 'Yes' or 'No' against each prerequisite. This will help you to track the prerequisites you have met and the prerequisites you have not met.

*Table 10–7 Prerequisites for Installing a Management Agent Using OUI*

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the hardware and softwrae requirements.<br>For hardware requirements, see Section 3.1, "Hardware Requirements". For software requirements, see Section 3.3, "Software Requirements". | |
| Operating System Requirements | Check if that operating systemon which you are going to install the Management Agent is ceritified.<br>For information about certified operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |

*Table 10–7 (Cont.) Prerequisites for Installing a Management Agent Using OUI*

| Requirement | Description | Yes/No |
|---|---|---|
| Package Requirements | Install the packages that are required for your operating system.<br>For information about packages, see Appendix G.1, "Check Platform-Specific Package Requirements for Agent Installation". | |
| Operating System Group Requirements | Ensure that you are part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite. | |
| User and Operating System Group Requirement | Ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created.<br>For information about creating operating system groups and users, see Section 3.6, "Operating System Groups and Users Requirements". | |
| Permission Requirements | Ensure that you have read, write, and execute permissions to `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, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.<br>For information about oraInventory permissions, see Section 4.8, "Installing Enterprise Manager Grid Control As the First Oracle Software". | |
| 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 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. | |
| SUDO Requirements | Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.<br>To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.<br>`<user> <hostname>=PASSWD: /home/em/agent10205/agent10g/root.sh, /bin/sh` | |
| Install Directory Requirements | Ensure the location where you are installing the Management Agent does not contain any other Oracle software.<br>Ensure that the directory under which you are installing the agent is not a symlink. | |

*Table 10–7 (Cont.) Prerequisites for Installing a Management Agent Using OUI*

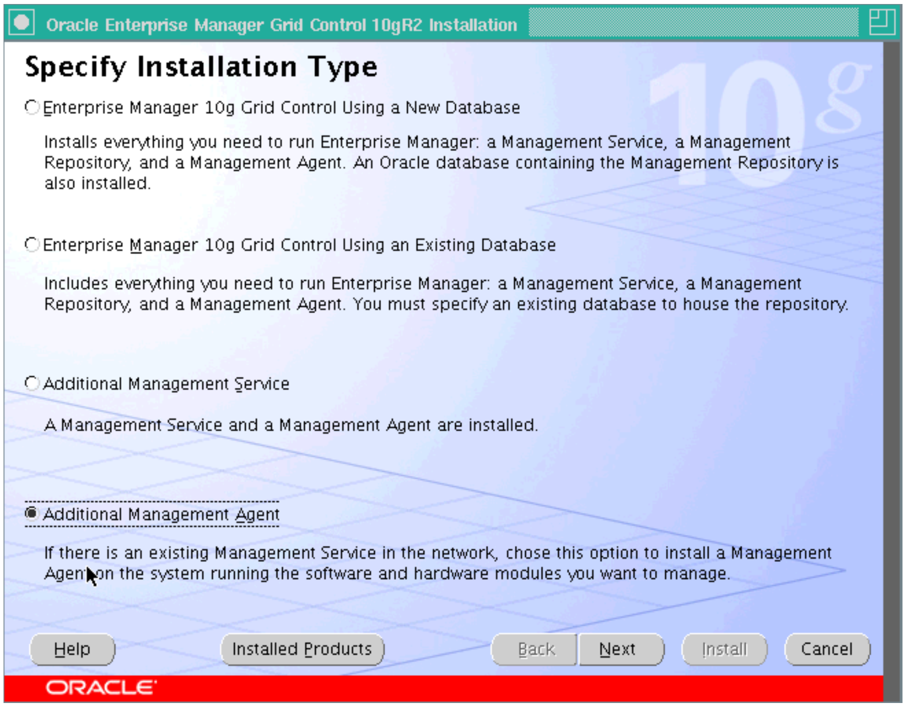
| Requirement | Description | Yes/No |
|---|---|---|
| Host Name Requirements | Ensure that the name of the host on which the installation is being performed is neither `localhost.localdomain` nor an IP address. It must be a valid host name.<br>At the time of invoking the installer, you can pass `ORACLE_HOSTNAME=<host_name> -local` as an argument.<br>Do not pass the argument as `ORACLE_HOSTNAME=<localhost.localdomain>` or `ORACLE_HOSTNAME=<IP address>`. You must pass the argument as **`ORACLE_HOSTNAME=<valid host name> -local`** | |
| Agent User Account Permissions and Rights (For Microsoft Windows) | (For Microsoft Windows) Ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Increase quotas.<br>■ Replace process level token.<br>■ Log in as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>1. Launch the Local Security Settings.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Settings**.<br>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) Grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following URL to Microsoft Web site:<br>`http://support.microsoft.com/kb/867466/en-us` | |

## 10.4.3 Installation Procedure

**WARNING:** The installation procedures given in the following sections are for installing full, base release of Oracle Management Agent, which is part of Enterprise Manager 10g Grid Control Release 2 or higher. For details about full, base releases and what these installation instructions can be use for, see Section 4.1, "Understanding What This Guide Helps You Install and Upgrade".

1. Start the Oracle Universal Installer by running the `runInstaller` script in Linux (`<DVD>/runInstaller`) from the top directory of the DVD.
2. In the Specify Installation Type screen, select the fourth option (**Additional Management Agent**), and specify the parent directory path and installation name.

***Figure 10–15 Specify Installation Type***



Oracle Enterprise Manager Grid Control 10gR2 Installation

Specify Installation Type

○ Enterprise Manager 10g Grid Control Using a New Database

Installs everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. An Oracle database containing the Management Repository is also installed.

○ Enterprise Manager 10g Grid Control Using an Existing Database

Includes everything you need to run Enterprise Manager: a Management Service, a Management Repository, and a Management Agent. You must specify an existing database to house the repository.

○ Additional Management Service

A Management Service and a Management Agent are installed.

● Additional Management Agent

If there is an existing Management Service in the network, chose this option to install a Management Agent on the system running the software and hardware modules you want to manage.

3. In the Specify Installation Location screen, specify the full path to the parent directory (base directory), for example, `/scratch/OracleHomes`. The agent home created during the installation is placed as a sub-directory under this parent directory. For example: `agent10g`.

   **Note:** Ensure you do not use symbolic links to the Oracle home path.

   The installer by default installs the selected products in the English language.

   a. If you want to install the product in a different language, click **Product Languages**.

   b. The Language Selection screen appears. Make the required language selections here, and click **Next**.

4. The Product Specific Prerequisites Checks screen appears.

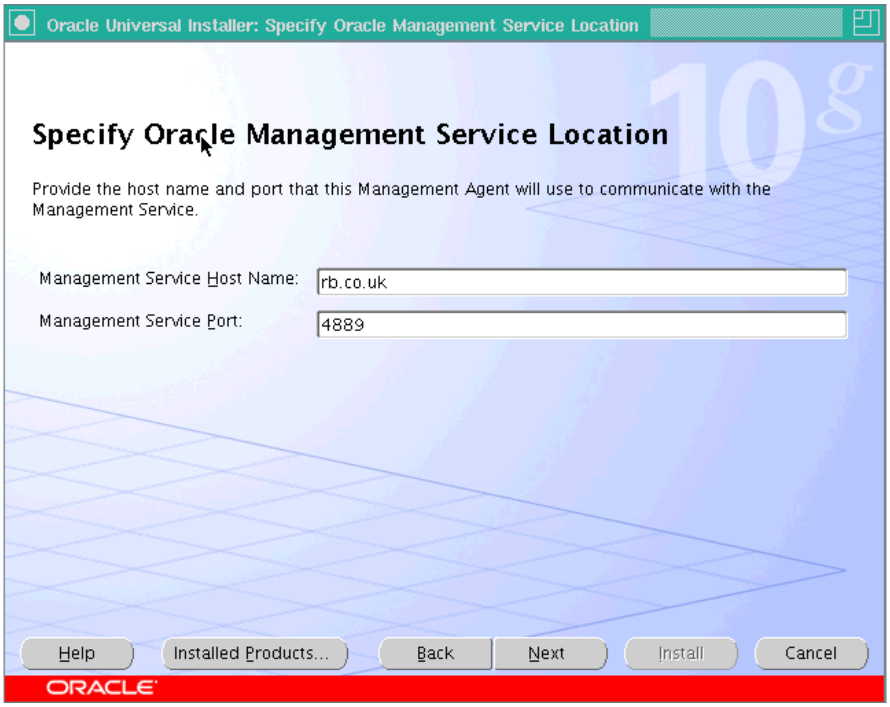
   This screen displays the name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

   Depending on the status of the automatic checks, you must verify all warning and manual checks. To do this, select the appropriate prerequisite status check box and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section at the bottom of the screen.

**Note:** You can also run these prerequisite checks in standalone mode, prior to starting the `runInstaller`. For more information on running these prerequisite checks in standalone mode, see Section 4.16, "Running the Prerequisite Check in Standalone Mode"for more information.

5. Click **Next**. The Specify Oracle Management Service Location screen appears.

***Figure 10–16 Specify Oracle Management Service Location***



Oracle Universal Installer: Specify Oracle Management Service Location

Specify Oracle Management Service Location

Provide the host name and port that this Management Agent will use to communicate with the Management Service.

Management Service Host Name: rb.co.uk

Management Service Port: 4889

   a. Specify the OMS host name. For example: `dlsun1444.acme.com`. Use the fully qualified host name (including domain). If your OMS is behind a Server Load Balancer (SLB), then specify the SLB host name.

**Caution:** When specifying the host name, ensure you do not include the protocol (that is, `http://` or `https://`).

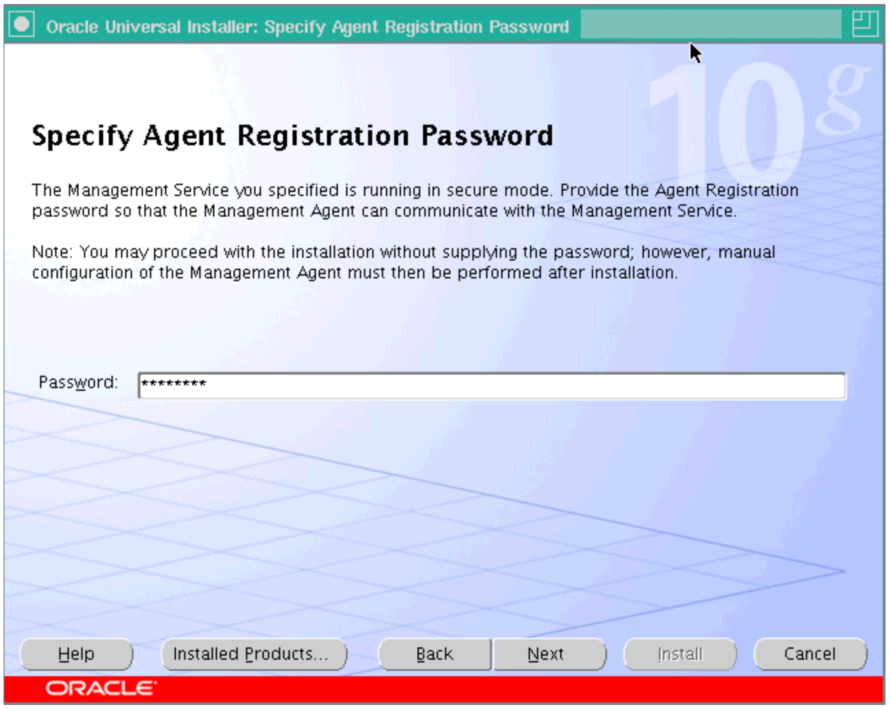
   b. Enter the port number for the OMS. The default port is 4889 and the default secure port number is 1159. If your OMS is behind an SLB, then specify the SLB port number.

**Note:**

- If you are installing Oracle Management Agent 10g Release 4 (10.2.0.4 or lower), not using a patch set but using a full Management Agent software download, then for **Management Service Port**, you must specify only a nonsecure port number (4889) even if you are specifying a secure and locked OMS. You must connect over HTTP to receive the certificate before you can connect over HTTPS.
- If you are installing Oracle Management Agent 10g Release 5 (10.2.0.5 or higher), not using a patch set but using a full Management Agent software download, then for **Management Service Port**, you can specify either a secure port number (1159) or a nonsecure port number (4889).
- If your OMS has been secured and locked, you are prompted to enter the Agent Registration password (used to secure the OMS environment). If you do not know the password, obtain it from the user who configured the OMS for SSL.

6. Click **Next**. If the OMS is found to be running in a secure mode, the Specify Agent Registration Password screen appears. You must provide the correct password to enable communications between the new Management Agent and the Secure Sockets Layer (SSL)-enabled OMS.

*Figure 10–17 Specify Agent Registration Password*



Oracle Universal Installer: Specify Agent Registration Password

Specify Agent Registration Password

The Management Service you specified is running in secure mode. Provide the Agent Registration password so that the Management Agent can communicate with the Management Service.

Note: You may proceed with the installation without supplying the password; however, manual configuration of the Management Agent must then be performed after installation.

Password: ********

> **Note:** If you do not know the password and choose to leave the Password field blank, you must do the following after installation to enable communication between the Management Agent and secure OMS:
>
> - Find out the correct password for the secure and locked OMS environment. If you do not know the password, obtain it from the user who configured the OMS for SSL.
> - If you have forgotten the password, then you can reset the password from the Grid Control console. Login to Grid Control as SYSMAN, select **Setup** from the top-right corner of the page, select **Registration Passwords** from the left menu panel, and on the Registration Password page, click **Add Registration Password**.
> - In the `<AGENT_HOME>/bin` directory, run the following command:
>
>   ```
>   emctl secure agent -reg_passwd <password>
>   ```
>
>   The variable <passwd> should be replaced with the Agent Registration password.
>
>   ```
>   emctl secure agent
>   ```
>
>   When you execute this command, you will be prompted to specify the Agent Registration password. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

7. Click **Next**. The Summary screen appears.

   This screen displays a summary of the options that you have selected during the installation process. Depending on the installation type, this screen displays any or all of the following details:

   - Global Settings
   - Product Languages
   - Space Requirements
   - New Installations

   For more information on each of the previously listed details, see the Grid Control online Help.

   Verify the choices that you have made and click **Install** to start the installation. The installer starts installing the selected Oracle product.

8. During the installation, you are prompted to execute certain configuration scripts. These scripts and their locations are listed in the Execute Configuration Scripts dialog box that is displayed (only for Linux).

   a. To execute these scripts, go to the computer window, log in as `root`, and run these configuration scripts.

   b. Return to the Execute Configuration Scripts dialog box after executing the scripts, and click **OK** to continue the installation.

9. The Configuration Assistants screen appears. At this point, the installer starts running the recommended configuration tools.

   This screen displays the name, status, and the type of each configuration tool that Oracle recommends to be run before completing the installation. In case of failure of any configuration assistant, refer to the logs and re-rerun the configuration assistants as described in Section A.2.1, "Configuration Assistants Fail During Enterprise Manager Installation".

10. After successfully running all the recommended configuration tools, click **Next**. The End of Installation screen appears.

    This screen displays some important information about the products you have installed. This information is also available in the `<AGENT_HOME>/sysman/setupinfo.txt` file.

    For example, it might contain information about the URLs for particular Web applications.

---

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

---

# 11

# Deploying Management Agent in Silent Mode

Enterprise Manager Grid Control (Grid Control) supports silent installations in which you can install the Grid Control components such as Management Agent without going through an interview phase (displaying pages or responding to questions). In silent installations, a response file provides the necessary installation information, typically answered by you, using stored values.

This chapter provides instructions to install Management Agent in silent mode. In particular, it covers the following:

- Available Response Files
- Running Response Files
- Silent Installation Process
- Using Silent Mode to Install Additional Management Agent

> **Note:** You do not need to set the DISPLAY environment variable for silent installations using Oracle Universal Installer.

## 11.1 Available Response Files

The response file available for installing Management Agent in silent mode is `additional_agent.rsp`. You may fine this response files on the installation DVD-ROM at <DVD>/response.

## 11.2 Running Response Files

Run the response files in the following way:

- **For UNIX Platforms**

  Instantiate the appropriate response file and run it as shown in the following way:

  ```
  ./runInstaller -silent -responseFile=<absolute path of the response file>
  -waitforcompletion
  ```

- **For Microsoft Windows Platforms**

  Instantiate the appropriate response file and run it as shown in the following way:

  ```
  ./setup.exe -silent -responseFile <absolute path of the response file>
  ```

## 11.3 Silent Installation Process

The silent installation on a UNIX environment can bee seen as a three-step process:

1. `noconfig`: In the first step, you must execute the `-noconfig` option. This will copy all the bits into the corresponding Oracle homes.
2. `allroot.sh/orainstRoot.sh`: After the bits are copied, the installer will prompt you to run the `allroot.sh` script (and `orainstRoot.sh`) or `root.sh` script (depending on the installation type).
   - Run the `orainstRoot.sh` script if this is the first Oracle product installation on your host.
   - Run the `allroot.sh` script from the first Oracle home that was created during installation.
3. `runconfig.sh`: You must pass this command to run the configuration assistants.

   **For an additional Management Agent installation, run:**

   ```
   <AGENT_HOME>/oui/bin/runConfig.sh ORACLE_HOME=<Agent Home> MODE=perform
   ACTION=configure
   ```

> **Note:** If you want to use the `-noconfig` option during the silent installation, you must execute the `runconfig.sh` command at the end of the installation in order to run the configuration assistants.

> **Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:
>
> 1. Open the agentstup file from the Oracle home of the Management Agent:
>
>    `$ORACLE_HOME/install/unix/scripts/agentstup`
> 2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
> 3. Run the root.sh script from the Oracle home of the Management Agent:
>
>    `$<ORACLE_HOME>/root.sh`
> 4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:
>
>    `$<ORACLE_HOME>/bin/emctl start agent`
>
>    This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

> **Caution:** When you are using the `-noconfig` option in your installation, ensure you also pass `-silent` to invoke the installer. The `-noconfig` option must be executed only during silent installations.

## 11.4 Using Silent Mode to Install Additional Management Agent

To perform a silent installation of this type:

1. Copy the `<DVD>/response/additional_agent.rsp` file to a location on your local host.

2. Modify the following entries in the response file.

***Table 11–1 Parameters to Modify in additional_agent.rsp File***

| Parameter | Description |
|---|---|
| FROM_LOCATION | Specify the complete path to the products.xml file. For example, FROM_LOCATION = "../oms/Disk1/stage/products.xml". |
| BASEDIR | Specify the directory where the ORACLE_HOME directories must be created. For example, on Microsoft Windows, BASEDIR = "C:\OHOME1", and on Linux, BASEDIR = "/scratch/OracleHomes". |
| INSTALLATION_NAME | Specify the name to be used for creating the Oracle home directories. For example, INSTALLATION_NAME = "OHOME1". |
| sl_OMSConnectInfo | SSpecify the host name and port of the OMS. The values must be in the form {"HostName","Port"}. For example, sl_OMSConnectInfo={"oms.xyz.com", "4881"}. |
| CLUSTER_NODES | If you deployed the agent to a cluster, then specify the nodes of that cluster. Separate the nodes by a comma, Do NOT include spaces between the comma-separated node list. For example, "CLUSTER_NODES={node1,node2,node3}". |

3. Invoke the `runInstaller` (`setup.exe` on Microsoft Windows) by executing:

```
<DVD>/<runInstaller or setup.exe> -silent -responseFile <location>/additional_
agent.rsp
```

The following message on the `root.sh scripts` is displayed (for UNIX only):

```
WARNING: A new inventory has been created in this session. However, it has not
yet been registered as the central inventory of this system.
To register the new inventory please run the script '<User's Home
Dir>/oraInventory/orainstRoot.sh' with root privileges.
If you do not register the inventory, you may not be able to update or patch
the products you installed.
The following configuration scripts need to be executed as the root user.
#!/bin/sh
#Root script to run
<User's Home Dir>/oraInventory/orainstRoot.sh
<Install Location>/agent10g/root.sh
To execute the configuration scripts:
    1. Open a terminal window
    2. Log in as root
    3. Run the scripts
    4. Return to this window and click OK to continue
```

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

**Caution:** The agent you are installing is not secure by default. To secure the agent, run the following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

```
AGE<NT_HOME>/bin/emctl secure agent
```

### 11.4.1 Setting Up Proxy Configuration for the Management Agent

There are two ways to specify proxy information for a Management Agent:

- Specify values for `s_proxyHost` and `s_proxyPort` using a response file when performing a silent installation using Oracle Universal Installer.
- Specify values directly through the command-line option when invoking Oracle Universal Installer. For example:

  ```
  <runInstaller or setup.exe> oracle.sysman.top.agent:s_proxyHost="<value>"
  oracle.sysman.top.agent:s_proxyPort="<value>"
  ```

# 12

# Deploying Management Agent on a Cluster

This chapter explains how a Management Agent can be deployed in a cluster-based environment. One of the options of installing a Management Agent in your environment is to install it individually on each computer. This is convenient when you want to install Management Agents only on a few computers. However, if your network is large and you have multiple computers grouped as a cluster, then installing Management Agents on all the computers, without using the available cluster, can be time-consuming and tasking.

Enterprise Manager 10g Grid Control Release 2 (or higher) offers a feature that helps you install Management Agents on multiple computers associated with a cluster, in a single installation, by pointing only to that cluster. This saves time and effort, as you reference only a cluster and have the Management Agent installed on all or some of the nodes of that cluster, in one attempt.

Therefore, if you have clusters in your environment, then use this feature to install a Management Agent either on each node of a cluster, individually, or on one or more nodes of a cluster, in a single installation. The clusters supported are Release 9.2 Clusters and Oracle Clusterware.

> **Caution:** The agent Oracle home cannot be installed in an Oracle Cluster Shared File System (OCFS) drive, but is supported on a NAS (Network Attached Storage) drive.

The following explains how Management Agents can be installed on Release 9.2 Clusters and Oracle Clusterware.

*Table 12–1 Deploying Management Agent on a Cluster*

| | Installation on 9.2 Cluster | Installation on Oracle Clusterware |
|---|---|---|
| **Method 1**<br>Installing Management Agent on Each Node of a Cluster, Individually | A Management Agent can be installed on 9.2 Cluster in any of the following ways:<br>■ Using agentDownload script<br>■ Using Agent Deploy application<br>■ Using Oracle Universal Installer (OUI) | A Management Agent can be installed on Oracle Clusterware in any of the following ways:<br>■ Using agentDownload script<br>■ Using Agent Deploy application<br>■ Using Oracle Universal Installer (OUI) |
| **Method 2**<br>Installing Management Agent on Many Nodes of a Cluster, in One Installation | | |

**IMPORTANT:** You cannot use addnode.sh script to extend Management Agents in a cluster.

## 12.1 Installing Management Agent on Each Node of a Cluster, Individually

One of the ways to install a Management Agent in a cluster-based environment is to install it on each node of a cluster, individually. This can take more time, as it involves installation of Management Agent on each and every node of a cluster. You use the cluster only to identify the nodes associated with it, but not to perform the installation on multiple nodes at a time.

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 12.1.1 Installing Management Agent on Release 9.2 Cluster

This section explains how a Management Agent can be installed on each node of a cluster, individually, on a Release 9.2 Cluster.

#### 12.1.1.1 Using the agentDownload Script

A Management Agent can be installed by running the agentDownload script on one node at a time using the correct arguments.

If you want to discover the cluster targets, then you must set the CLUSTER_NAME environment variable before running the agentDownload script, or pass the cluster name to the agentDownload script as agentDownload -n <clustername>.

```
agentDownload -b <Oracle Base Directory location> -n <clustername>
```

For detailed instructions, see Section 10.3, "Installing Management Agent Using agentDownload Script".

**Note:** If the CLUSTER_NAME environment variable is not set, the agent cannot discover any cluster targets.

#### 12.1.1.2 Using the Agent Deploy Application

A Management Agent can be installed using the Agent Deploy application that is part of Enterprise Manager Grid Control (Grid Control).

While using the Agent Deploy application to install a Management Agent on a cluster node, you must select the appropriate node of that cluster. If you want to discover the cluster targets, you must specify the correct cluster name in the Cluster Name field.

For detailed instructions, see Section 10.1.4.1, "Fresh Installation of the Management Agent".

**Note:** Ensure the nodes that you select for the agent installation are part of the cluster that you have specified in the Cluster Name field. Otherwise, the targets are not discovered.

#### 12.1.1.3 Using Oracle Universal Installer

A Management Agent can be installed by invoking the installer using Oracle Universal Installer (OUI). The interactive type is typically a one-node installation.

In this case, you can set the `CLUSTER_NAME` environment variable to the name of the cluster that you want to use for the cluster targets, before invoking the installer, that is the `runInstaller` script. If this variable is not set, the agent cannot discover any cluster targets.

For detailed instructions, see Section 10.4, "Installing Management Agent Using OUI".

### 12.1.2 Installing Management Agent on Oracle Clusterware

This section explains how a Management Agent can be installed on each node of Oracle Clusterware, individually.

#### 12.1.2.1 Using agentDownload Script

A Management Agent can be installed by running the `agentDownload` script on one node at a time using the correct arguments.

If you want to override the cluster name to be used in `targets.xml` file, you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -n <clustername>`.

```
agentDownload -b <Oracle Base Directory location> -n <clustername>
```

> **Note:** If the `CLUSTER_NAME` environment variable is not set or passed, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

For detailed instructions, see Section 10.3, "Installing Management Agent Using agentDownload Script".

#### 12.1.2.2 Using the Agent Deploy Application

A Management Agent can be installed using the Agent Deploy application that is part of Grid Control.

While using the Agent Deploy application to install a Management Agent on a cluster node, you must select the Cluster Install option, and specify the appropriate cluster node names. The cluster name that you specify here overrides the corresponding value in the `targets.xml` file.

For detailed instructions, see Section 10.1.4.1, "Fresh Installation of the Management Agent".

#### 12.1.2.3 Using Oracle Universal Installer

The Management Agent can be installed by invoking the installer using Oracle Universal Installer (OUI).

If you want to set the cluster name that will appear in `targets.xml` file, then you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, then the agent uses the cluster name that was specified during the Oracle Clusterware installation.

For detailed instructions, see Section 10.4, "Installing Management Agent Using OUI".

## 12.2 Installing Management Agent on Many Nodes of a Cluster, in One Installation

The other way to install a Management Agent in a cluster-based environment is to install it on one or more nodes of a cluster, at a time, in a single installation. This can may not take time (though it depends on the size of the cluster), as it involves installation of Management Agent on multiple nodes of a cluster, at a time, in parallel, in a single installation attempt. You use the cluster not only to identify the nodes associated with it, but also to perform the installation on multiple nodes.

**Caution:** While installing a Management Agent on multiple nodes of a Oracle Cluster that is running on a Microsoft Windows platform, only the host and cluster targets will be discovered during the installation.

To discover all other targets, you must run the following on each node of that cluster:

```
Agent Home>/bin/agentca -d -n <Cluster Name> -c <node name>
```

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

### 12.2.1 Installing Management Agent on Release 9.2 Cluster

This section explains how a Management Agent can be installed on one or more nodes of a Release 9.2 Cluster, at a time, in a single installation.

#### 12.2.1.1 Using the agentDownload Script

A Management Agent can be installed by running the `agentDownload` script with the `-c` option (for example, `-c "node1,node2,..."`). This option helps you install the Management Agent on one or more nodes that you specify.

If you want to override the cluster name that appears in `targets.xml`, then you must set the `CLUSTER_NAME` environment variable before running the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -b <Oracle Base Directory location> -n <clustername> -c "node1,node2,node3"`.

For detailed instructions, see Section 10.3, "Installing Management Agent Using agentDownload Script".

#### 12.2.1.2 Using the Agent Deploy Application

A Management Agent can be installed using the Agent Deploy application that is part of Grid Control.

While using the Agent Deploy application to install a Management Agent on multiple nodes of a cluster, you must select the **Cluster Install** option and specify all the nodes of that cluster.

If you want to discover the cluster targets, then you must specify the correct cluster name in the Cluster Name field.

For detailed instructions, see Section 10.1.4.1, "Fresh Installation of the Management Agent".

#### 12.2.1.3 Using Oracle Universal Installer

A Management Agent can be installed by invoking the installer using Oracle Universal Installer (OUI).

Ensure that you pass the `CLUSTER_NODES` variable when starting the installer, that is the `runinstaller` script, like this:

```
./runInstaller "CLUSTER_NODES={node1,node2,node3}"
```

If the `CLUSTER_NODES` variable is not passed, then the installer cannot detect the nodes and cannot perform the cluster install.

If you want to set the cluster name that appears in the `targets.xml` file, you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, the agent uses the first node as the cluster name.

For detailed instructions, see Section 10.4, "Installing Management Agent Using OUI".

### 12.2.2 Installing Management Agent on Oracle Clusterware

This section explains how a Management Agent can be installed on one or mode nodes of Oracle Clusterware, at a time, in a single installation.

#### 12.2.2.1 Using the agentDownload Script

A Management Agent can be installed by running the `agentDownload` script with the `-c` option (for example, `-c "node1,node2,..."`). This option helps you install the Management Agent on one or more nodes that you specify here.

If you want to override the cluster name that appears in `targets.xml` file, then you must set the `CLUSTER_NAME` environment variable prior to executing the `agentDownload` script, or pass the cluster name to the `agentDownload` script as `agentDownload -b <Oracle Base Directory location> -n <clustername> -c "node1,node2,node3"`.

**Note:** If the `CLUSTER_NAME` variable is not set or passed, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

For detailed instructions, see Section 10.3, "Installing Management Agent Using agentDownload Script".

#### 12.2.2.2 Using the Agent Deploy Application

A Management Agent can be installed using the Agent Deploy application that is part of Grid Control.

While using the Agent Deploy application to install a Management Agent on multiple nodes of a cluster, you must select the **Cluster Install** option and specify all the nodes of that cluster.

If you want to override the cluster name that appears in `targets.xml` file, you must specify the appropriate cluster name in the application.

For detailed instructions, see Section 10.1.4.1, "Fresh Installation of the Management Agent".

#### 12.2.2.3 Using Oracle Universal Installer

A Management Agent can be installed by invoking the installer using Oracle Universal Installer (OUI).

When you execute the `runInstaller` script, it automatically detects all the cluster nodes. You can then choose the nodes on which you want to install the Management Agent.

If you want to override the Cluster name that appears in targets.xml, you must set the `CLUSTER_NAME` environment variable before invoking the `runInstaller`. If this variable is not set, the agent uses the cluster name that was specified during the Oracle Clusterware installation.

For detailed instructions, see Section 10.4, "Installing Management Agent Using OUI".

# 13 Cloning Management Agent

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. Yes, we literally mean making identical copies!

The "Management Agent Cloning" is an installation option that allows you to make copies of your existing running Management Agents so that the same configuration changes are carried over to the newly cloned Management Agent instance - either on a single host or multiple hosts. This saves time and effort in patching a fresh installation all over again and bringing it to the current state.

You can clone a Management Agent in two ways, either from the Grid Control console or from the command line.

> **Note:** Cross platform cloning and cloning on shared clusters is not supported. For example, you cannot clone a Linux-specific Management Agent from a Linux host to a Solaris host.

This chapter describes the following:

- Cloning Management Agent Using Grid Control Console
- Cloning Management Agent Using Command Line
- Cloning Management Agent on a Cluster

> **Note:** The Agent Clone application is available only in Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).
>
> This installation guide is mainly for the base release, that is, Enterprise Manager 10g Grid Control Release 2 (10.2.0.1) Use this guide to install the base release and then patch it with 10.2.0.5 Grid Control patch set to migrate to Enterprise Manager 10g Grid Control Release 5 (10.2.0.5). The 10.2.0.5 Grid Control patch is available on My Oracle Support (formerly Metalink).

## 13.1 Cloning Management Agent Using Grid Control Console

This section describes the following:

- Prerequisites for Cloning Management Agent
- Cloning Management Agent

> **Note:** If the cloning operation fails, review the log files described in Appendix C, "Agent Log Files".

### 13.1.1 Prerequisites for Cloning Management Agent

Before you start to clone a Management Agent, meet the following prerequisites:

*Table 13–1 Prerequisites for Cloning a Management Agent*

| Requirement | Description | Yes/No |
|---|---|---|
| Hardware and Software Requirements | Ensure that you meet the hardware and softwrae requirements.<br>For hardware requirements, see Section 3.1, "Hardware Requirements". For software requirements, see Section 3.3, "Software Requirements". | |
| Operating System Requirements | Check if that operating systemon which you are going to install the Management Agent is ceritified.<br>For information about certified operating systems, see Section 3.2, "Operating System, Browser, Target Certification". | |
| Package Requirements | Install the packages that are required for your operating system.<br>For information about packages, see Appendix G.1, "Check Platform-Specific Package Requirements for Agent Installation". | |
| Load Balancer Requirements | If you are cloning the Management Agent in an environment that has multiple OMSes managed by a Server Load Balancer (SLB), then ensure that you enable communication between the Management Agent and the host running the SLB.<br>For information about configuration to be done for SLB, see Section 10.1.3, "Configurations Required for Management Agent to Communicate with Oracle Management Service with Server Load Balancer". | |
| Operating System Group Requirements | Ensure that you are part of the same operating system group that installed Oracle Application Server and/or Oracle Collaboration Suite. | |
| User and Operating System Group Requirement | Ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created.<br>For information about creating operating system groups and users, see Section 3.6, "Operating System Groups and Users Requirements". | |
| Path Validation Requirements | Validate the path to all command locations. For more information, see Section G.3, "Validate All Command Locations". | |

*Table 13–1 (Cont.) Prerequisites for Cloning a Management Agent*

| Requirement | Description | Yes/No |
|---|---|---|
| Permission Requirements | Ensure that you have read, write, and execute permissions to `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, you can specify the path to an alternative inventory location by using the `-i <location>` option in the Additional Parameters section.<br>For information about oraInventory permissions, see Section 4.8, "Installing Enterprise Manager Grid Control As the First Oracle Software". | |
| Default Port Requirements | Ensure that the SSH daemon is running on the default port (that is, 22) on all the target hosts.<br>If the port is a non-default port, that is, any port other than 22, then update the SSH_PORT property in the `paths.properties` file to ensure successful cloning of the Management Agent.<br>■ If the software for Oracle Management Agent 10g Release 4 (10.2.0.4) or higher is available, then update the following file:<br>`<OMS_HOME>/sysman/agent_download/<VERSION>/<PLATFORM>/agentdeploy/Paths.properties`<br>■ If the software of the Management Agent is not available:<br>`<OMS_HOME>/sysman/prov/resources/Paths.properties` | |
| Oracle Inventory Location Requirements | Ensure that the Oracle Inventory (`oraInventory`) is not in a shared location. When you use the `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. | |
| PubkeyAuthentication Parameter Requirements | Ensure that the `PubkeyAuthentication` parameter is enabled in the sshd_config file.<br>To verify the value of this parameter, run the following command:<br>`grep PubkeyAuthentication /etc/ssh/sshd_config`<br>The result of this command must be *Yes*. If the result is *No*, then edit the `/etc/ssh/sshd_config` file and set the PubkeyAuthentication value to *Yes*. | |
| 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 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 13–1 (Cont.) Prerequisites for Cloning a Management Agent*

| Requirement | Description | Yes/No |
|---|---|---|
| SUDO Requirements | Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.<br>To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.<br>`<user> <hostname>=PASSWD: /home/em/agent10205/agent10g/root.sh, /bin/sh` | |
| Prerequisite Check Requirements | If you want the prerequisite checks to run before the actual cloning operation could begin, then you must ensure that the software for Oracle Management Agent 10g Release 4 (10.2.0.4) or higher is available in the following location.<br>`<OMS_HOME>/sysman/agent_download/`<br>If the software is not available in this location, you can still proceed with the cloning operation but the prerequisite checks may or may not be performed, depending on the location of the Source Agent Home, that is, the Management Agent to be cloned.<br>■ If the Source Agent Home is on the host where the OMS is running, then none of the prerequisite checks are run. You can choose to proceed with the cloing operation, but if you still want to run the prerequisite checks, then ensure that the software for Oracle Management Agent 10g Release 4 (10.2.0.4) or higher is available in the location mentioned above.<br>■ If the Source Agent Home is on any other host, then except for system prerequisite checks, all other prerequisite checks are run.<br>Oracle recommends you to run the prerequisite checks so that the requirements that are not being met are identified, and unnecessary errors and installation failures are avoided beforehand. | |
| Existing Management Agent Requirements | Ensure that you have at least one existing instance of a Management Agent that can be cloned. | |
| Target Host Credentials Requirements | Ensure that the target hosts where you want to clone the Management Agent have the same credentials and file system structure. | |
| Installation Base Directory Requirements | Your installation base directory must be empty and writable.<br>Your installation base directory must NOT be a shared, mounted location. | |

*Table 13–1 (Cont.) Prerequisites for Cloning a Management Agent*

| Requirement | Description | Yes/No |
|---|---|---|
| Agent User Account Permissions and Rights (For Microsoft Windows) | (For Microsoft Windows) Ensure that the agent user account has permissions and rights to perform the following:<br>■ Act as part of the operating system.<br>■ Increase quotas.<br>■ Replace process level token.<br>■ Log in as a batch job.<br>To verify whether the agent user has these rights, follow these steps:<br>1. Launch the Local Security Settings.<br>From the **Start** menu, click **Settings** and then select **Control Panel**. From the Control Panel window, select **Administrative Tools**, and from the Administrative Tools window, select **Local Security Settings**.<br>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 indows) Grant the `Cmd.exe` program *Read* and *Execute* permissions for the user account that the batch job runs under. This is a restriction from Microsoft.<br>For more information on this restriction and to understand how you can grant these permissions, access the following Microsoft Web site URL:<br>`http://support.microsoft.com/kb/867466/en-us` | |

## 13.1.2 Cloning Management Agent

To clone a Management Agent using Grid Control console, do the following:

1. In Grid Control, click **Deployments**. Grid Control displays the Deployments page.
2. On the Deployments page, from the Agent Installation section, click **Install Agent**. Grid Control displays the Select Agent Deployment Type page.
3. On the Select Agent Deployment Type page, click **Clone Agent**. Grid Contol displays the Agent Clone: Installation Details page.
4. On the Agent Clone: Installation Details page, do the following:
   a. In the Source Agent section, provide details about the location where the running Management Agent or the archived ZIP file of the running Management Agent is available.

*Table 13–2 Element Description - Source Agent Section - Cloning Management Agent*

| UI Element on the Screen | Details Required |
|---|---|
| Source Agent Home | Specify the location where the Management Agent to be cloned is available.<br>The location can be one of the following:<br>■ Full path to the Oracle home directory of the Management Agent that you want to clone. Ensure that the path extends up to the `agent10g` directory. For example, `/home/john/Oraclehomes/agent10g/`.<br>■ Full path to the location where the archived format (ZIP file) is available, that is, if you have already archived the Oracle home directory of the Management Agent. For example, `/home/software/agent.zip`.<br>Ensure that the ZIP file contains the contents of the Oracle home directory. To ensure this, when you create the ZIP file, create it from the parent directory of the agent10g directory. For example, to ZIP the contents from `/scratch/oraclehome/agent/agent10g`, navigate to `/scratch/oraclehome/agent` directory first, and then run `zip -r agent10g agent.zip`.<br>■ Full path to the shared, NFS mounted location where the Management Agent to be cloned or the archived ZIP file is available. For example, `/home/nfsshared/agent.zip`. |
| Source Agent Home on OMS | Select this if the location you specified for Source Agent Home (above) is available on the host where OMS is running.<br>**Note:** If you want to extract the contents of an Oracle home directory to an OMS host, then the Oracle home directory of a Microsoft Windows-based Management Agent must not be extracted on a UNIX-based host (and vice versa). |

**b.** In the Hosts section, provide details about the target hosts where you want to clone the Management Agent.

*Table 13–3 Element Description - Host Section - Cloning Management Agent*

| UI Element on the Screen | Details Required |
|---|---|
| Platform | Select the platform of the host on which you want to clone.<br>Ensure that the platform you select here matches with the platform of the Source Agent Home. |

*Table 13–3 (Cont.) Element Description - Host Section - Cloning Management*

| UI Element on the Screen | Details Required |
|---|---|
| Provide Host List | Specify the hosts where you want to clone the Management Agent. You can specify either the name of the host or its IP address. Separate them by a comma or white space. For example, `host1.example.com,host2.example.com`.<br>You can specify either physical hosts or virtual hosts, but not a combination of the two. If you are specifying virtual hosts, then select **All are Virtual Hosts**.<br>If you have a file that contains a list of all required host names, then click **Get Host Names From File** and select the file. Ensure that the file format is similar to `/etc/hosts` file. |
| Cluster Name | Specify a name that can be used to form a cluster of the all the target hosts you specified. |

c. In the OS Credentials section, specify the user name and password to access the target hosts where you want to clone the Management Agent. If you are cloning on multiple hosts, then ensure that the credentials are the same for all the hosts.

   Select **Run root.sh** if you want Grid Control to run this script. Grid Control uses SUDO to run this script and prompts you to specify the "invoking user's password" when it runs the script. Ensure that you have SUDO privileges to run `/bin/sh`, otherwise, the installation may fail.

   If `/etc/sudoers` is configured in such a way that `sudo` never prompts for a password, then a directory with the host password as the title gets created in the invoking users home directory. To avoid this, ensure that you configure /etc/sudoers file such that running a command using sudo always prompt for a password.

   If you do not select **Run root.sh** here, then you must manually run the script once the installation is complete. To understand how the manually run this script, see Section 13.1.2.1, "Running root.sh Script Manually".

d. In the Destination section, specify the full path to the directory on the target hosts where you want to clone the Management Agent. For example, `/home/mark/OracleHomes`.

   Ensure that you have write permission on this installation base directory. The Oracle home directory for the Management Agent will be created as a subdirectory in this base directory. For example, if you specify `/home/mark/OracleHomes` as the installation base directory here, then Grid Control will clone the Management Agent to `/home/mark/OracleHomes/agent10g`.

e. In the Port section, specify a port on which the Management Agent can communicate with the OMS.

   The same port will be used for all the hosts specified across all platforms. If no port is specified here, the application uses the first free port that is available within the range of 1830 to 1849.

f. In the Additional Parameters section, specify any additional parameters that you want to pass during the cloning process.

For information about the additional parameters that are supported for Agent Cloning, see Appendix H, "Additional Parameters for Agent Deploy Application".

Note that if you are specifying more than one parameter, then separate them with a white space. For example, `-invPtrLoc /home/oraInst.loc -scratchPath /tmp s_OMSHost=<LoadBalancerHost> s_OMSPort=<LoadBalancerPort>`.

If you are cloning a Management Agent that was installed along with OMS, then include the following additional parameter:

```
b_chainedInstall=false, oracle.sysman.top.agent:s_
installType=AGENT
```

g. In the Management Server Security section, specify the registration password if you want to secure the communication between Management Agent and OMS.

h. In the Additional Scripts section, specify the additional scripts you want to run before and/or after cloning and configuration steps.

   The scripts you specify here must be available on all the target hosts. If you want to run the scripts as SUDO, then select **Run as Superuser**.

5. Click **Continue**. Grid Control displays the My Oracle Support Details page.
6. On the My Oracle Support Details page, do the following:

   - If the host where the Management Agent is being installed has a *direct* connection to the Internet, then specify an email address and My Oracle Support (formerly Metalink) password.

     An email address is required so that security updates and install updates can be sent. You can specify any email address, but Oracle recommends you to specify the My Oracle Support (formerly Metalink) user name. For example, `john.mathew@xyz.com`.

   - If the host where the Management Agent is being installed has an *indirect* connection to the Internet through a proxy server, then specify an email address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

     **Note:** You can change the proxy server settings any time after the installation or patching process ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the Management Agent.

   - If the host where the Management Agent is being installed does not have a *direct* or *indirect* connection to the Internet, then specify the email address and leave the other fields blank.

     In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support (formerly Metalink). To understand how the configuration information can be manually collected and uploaded, see the steps outlined in Section 10.1.4.1.2, "Manually Collecting and Uploading Configuration Information to My Oracle Support (formerly Metalink)".

7. Click **Continue**.

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.

3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

**Note:** If the installation fails, review the log files described in Appendix C, "Agent Log Files".

#### 13.1.2.1 Running root.sh Script Manually

The root.sh script is run after the installation process ends successfully. The script takes care of the postinstallation configurations to be done for Management Agent. If you install a Management Agent using the Agent Clone Wizard, then you are allowed to select an option to run root.sh script automatically.

However, if you have not selected there, then you must run the script manually after the installation completes.

To run the root.sh script manually:

1. Log in as a root user on the host. Alternatively, use the sudo command to change to a root user.

2. Run the root.sh script from the Oracle home directory of the Management Agent:

   ```
   <oracle_home>/root.sh
   ```

   For example, if you are using sudo to change to a root user, then you will run the following command:

   ```
   /usr/local/bin/sudo /scratch/OracleHomes/agent10g/root.sh
   ```

## 13.2 Cloning Management Agent Using Command Line

This section describes how you can clone a Management Agent using command line interface. In particular, this section covers the following:

- Cloning Management Agent Installed with OMS or As Additional Agent
- Logs to Review if Cloning Fails

### 13.2.1 Cloning Management Agent Installed with OMS or As Additional Agent

To clone a Management Agent that was installed with OMS or as an additional, standalone agent, do the following:

1. Install a Management Agent on a host using any of the deployment methods described in Chapter 10, "Deploying Management Agent".
2. Zip the Management Agent Oracle home that you want to clone (for example, `agent.zip`).
3. Perform a file transfer (FTP) of this zipped Oracle home onto the destination host (for example, `ftp agent.zip`).
4. In the destination host, unzip the Management Agent Oracle home.
5. Go to `$ORACLE_HOME/oui/bin/` directory and run the following command:
   - If you are cloning a Management Agent that was installed along with OMS, then run the following command:

     ```
     ./runInstaller -clone -forceClone ORACLE_HOME=<full path of Oracle home>
     ORACLE_HOME_NAME=<Oracle home name> -noconfig -silent b_
     chainedInstall=false oracle.sysman.top.agent:s_installType=AGENT
     ```

   - If you are cloning a Management Agent that was installed as a fresh standalone Management Agent, then run the following command:

     ```
     ./runInstaller  -clone -forceClone ORACLE_HOME=<full path of Oracle home>
     ORACLE_HOME_NAME=<Oracle home name> -noconfig -silent
     ```

   **Note:** By default, the cloned Management Agent does not inherit the customized parameters in the emd.properties file of the source Management Agent. In other words, the modifications to emd.properties parameters of the source Management Agent are reset to default values for the cloned, target Management Agent.

   If you want to retain the changes done to the emd.properties file, then redo the changes in the emd.properties.template file, as this is the file that is instantiated while cloning a Management Agent. Both these files are located in $ORACLE_HOME/sysman/config/, where $ORACLE_HOME is the Oracle home directory of the source Management Agent.

6. Execute the following script to run the Agent Configuration Assistant (`agentca`):

   ```
   $ORACLE_HOME/bin/agentca -f
   ```

   **Note:** The cloned Management Agent is not in the secure mode by default. You must manually secure the Management Agent by running `<Oracle_Home>/bin/emctl secure agent`. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

7. (For UNIX only) After running the configuration assistant, run the following scripts as a *root* user on the host.
   - If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the Central Inventory:

     ```
     $ORACLE_HOME/oraInventory/oraInstRoot.sh
     ```

For example, if you are using sudo to change to a root user, then you will run the following command:

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

- Run the `root.sh` script from the Oracle home directory of the Management Agent:

  ```
  $ORACLE_HOME/root.sh
  ```

  For example, if you are using sudo to change to a root user, then you will run the following command:

  ```
  /usr/local/bin/sudo /scratch/OracleHomes/agent10g/root.sh
  ```

---

**Note:** If the Management Agent does not start up automatically when you restart the host, then do the following:

1. Open the agentstup file from the Oracle home of the Management Agent:

   ```
   $ORACLE_HOME/install/unix/scripts/agentstup
   ```

2. Edit the file to replace executingUser=$USER with executingUser=`id -un`. Then, save and exit the file.
3. Run the root.sh script from the Oracle home of the Management Agent:

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

4. Restart the Management Agent by running the following command from the Oracle home of the Management Agent:

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

   This is a one-time action to be taken. Step (1) to Step (3) will ensure that the Management Agent starts up automatically every time you restart the host in the future.

---

### 13.2.2 Logs to Review if Cloning Fails

If the cloning operation fails, then review the following log files. The information in these logs might help you describe the failure while raising service requests with Oracle Support.

- <ORACLE_HOME_INVENTORY>/logs/cloneActions<latest timestamp>.log
- <ORACLE_HOME_INVENTORY>/logs/oraInstall<latest timestamp>.err
- <ORACLE_HOME_INVENTORY>/logs/oraInstall<latest timestamp>.out

For example:

```
/home/oracle/oraInventory/logs/cloneActions2008-02-14_
06-29-37AM.log
```

## 13.3 Cloning Management Agent on a Cluster

To clone a Management Agent on a cluster, do the following:

1. Install a Management Agent on a host using any of the deployment methods described in Chapter 10, "Deploying Management Agent".
2. Zip the Management Agent Oracle home that you want to clone (for example, `agent.zip`).

3. Perform a file transfer (FTP) of this zipped Oracle home to all the target nodes of the cluster (for example, `ftp agent.zip`).
4. On each target node of the cluster, unzip the Management Agent Oracle home. Oracle recommends you to maintain the same destination location on all nodes of the cluster.
5. On each target node of the cluster, go to `$ORACLE_HOME/oui/bin/` directory and run the following command:

```
./runInstaller  -clone -forceClone ORACLE_HOME=<full path of Oracle home>
ORACLE_HOME_NAME=<Oracle home name> -noconfig -silent
```

> **Note:** By default, the cloned Management Agent does not inherit the customized parameters in the emd.properties file of the source Management Agent. In other words, the modifications to emd.properties parameters of the source Management Agent are reset to default values for the cloned, target Management Agent.
>
> If you want to retain the changes done to the emd.properties file, then redo the changes in the emd.properties.template file, as this is the file that is instantiated while cloning a Management Agent. Both these files are located in $ORACLE_HOME/sysman/config/, where $ORACLE_HOME is the Oracle home directory of the  source Management Agent.

6. On each target node of the cluster, run the following script to run the Agent Configuration Assistant (`agentca`):

```
$ORACLE_HOME/bin/agentca -f -c "node1, node2, node3...."
```

> **Note:** The cloned Management Agent is not in the secure mode by default. You must manually secure the Management Agent by running `<Oracle_Home>/bin/emctl secure agent`. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

7. (For UNIX only) After running the configuration assistant, run the following scripts as a *root* user on the host.

   - If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the Central Inventory:

     ```
     $ORACLE_HOME/oraInventory/oraInstRoot.sh
     ```

     For example, if you are using sudo to change to a root user, then you will run the following command:

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

   - Run the `root.sh` script from the Oracle home directory of the Management Agent:

     ```
     $ORACLE_HOME/root.sh
     ```

For example, if you are using sudo to change to a root user, then you will run the following command:

```
/usr/local/bin/sudo /scratch/OracleHomes/agent10g/root.sh
```

# 14

# Prerequisites for Installing Enterprise Manager Grid Control on Oracle RAC

This chapter describes the preinstallation requirements to be met for Enterprise Manager Grid Control (Grid Control) in an Oracle Real Application Clusters (Oracle RAC) environment.

This chapter contains the following sections:

## 14.1 Preinstallation Requirements

Before installation, ensure the following preinstallation requirements are met.

### 14.1.1 Configure Oracle Cluster Synchronization Services (CSS)

The first time you install Grid Control on a system, Oracle Universal Installer (OUI) configures and starts a single-node version of the Oracle Cluster Synchronization Services (CSS) service. The CSS service is required to enable synchronization between an Automatic Storage Management (ASM) instance and the database instances that rely on it for database file storage. It is configured and started even if you do not choose ASM as a storage mechanism for database files.

Because it must be running before any ASM instance or database instance is started, OUI configures it to start automatically when the system starts.

For Oracle RAC installations, the CSS service is installed with Oracle Clusterware in a separate Oracle home directory. For single-node installations, the CSS service is installed in and runs from the same Oracle home as Oracle Database. For this reason, you must use caution when removing Oracle Database software from the system. Before you remove an Oracle home directory that contains Oracle Database, you must either delete the CSS service configuration, or if necessary, reconfigure the CSS service to run from another Oracle home directory.

If you plan to have more than one Oracle Database installation on a single system and you want to use Automatic Storage Management for database file storage, Oracle recommends that you run the CSS service and the Automatic Storage Management instance from the same Oracle home directory and use different Oracle home directories for the database instances.

## 14.1.2 Certification for Agents on Oracle Real Application Clusters (Oracle RAC)

> **See Also:** *Oracle High Availability Architecture and Best Practices* for information on cluster configuration recommendations.

## 14.1.3 Additional Software Requirements for Management Agent Installation on Clusters

If the Grid Control installation is on a cluster, you must install Oracle Clusterware (formerly called Oracle Cluster Ready Services) or any vendor clusterware separately, besides fulfilling all the other Oracle software requirements (see Section 3.3, "Software Requirements" for more information). Oracle Clusterware is not available on the Oracle Enterprise Manager Grid Control 10*g* Release 2 (10.2) installation media.

### 14.1.3.1 Oracle Clusterware/Vendor Clusterware

Oracle Clusterware consists of key subcomponents required by Oracle Real Application Clusters installations. It performs workload management and a component restart. For example, when an instance supporting a particular service fails, Oracle Clusterware restarts the service on the next available instance that you have configured for that service.

You must install Oracle Clusterware before installing Oracle Real Application Clusters. The software is available on the Oracle Clusterware installation media.

> **See Also:** *Oracle Enterprise Manager Licensing Information* available on the Oracle Database installation media for more information.

## 14.1.4 Preinstallation Tasks for Oracle Real Application Clusters

Before you install and use Oracle Real Application Clusters, you must configure secure shell (SSH) for the Oracle user on all cluster nodes. The installer uses the `ssh` and `scp` commands during installation to run remote commands on and copy files to the other cluster nodes. You must configure SSH so that these commands do not prompt for a password.

> **Note:** If SSH is not available, the installer attempts to use `rsh` and `rcp` instead. However, these services are disabled by default, in most Linux machines.

To configure SSH, complete the following steps on each cluster node:

1. Log in as the Oracle user.
2. If necessary, create the `.ssh` directory in the Oracle user's home directory and set the correct permissions on it:

   ```
   $ mkdir ~/.ssh
   $ chmod 755 ~/.ssh
   ```

3. Enter the following commands to generate an RSA key for version 2 of the SSH protocol:

   ```
   $ /usr/bin/ssh-keygen -t rsa
   ```

   At the prompts:

   - Accept the default location for the key file.

- Enter and confirm a password (or pass phrase) that is different from the Oracle user's password.

This command writes the public key to the `~/.ssh/id_dsa.pub` file and the private key to the `~/.ssh/id_dsa` file. Never distribute the private key to anyone.

4. Enter the following commands to generate a DSA key for version 2 of the SSH protocol:

```
$ /usr/bin/ssh-keygen -t dsa
```

At the prompts:

- Accept the default location for the key file.
- Enter and confirm a password (or pass phrase) that is different from the Oracle user's password.

This command writes the public key to the `~/.ssh/id_dsa.pub` file and the private key to the `~/.ssh/id_dsa` file. Never distribute the private key to anyone.

5. Copy the contents of the `~/.ssh/id_rsa.pub` and `~/.ssh/id_dsa.pub` files to the `~/.ssh/authorized_keys` file on this node and to the same file on all other cluster nodes.

**Note:** The `~/.ssh/authorized_keys` file on every node must contain the contents from all of the `~/.ssh/id_rsa.pub` and `~/.ssh/id_dsa.pub` files that you generated on all cluster nodes.

6. Change the permissions on the `~/.ssh/authorized_keys` file on all cluster nodes:

```
$ chmod 644 ~/.ssh/authorized_keys
```

At this point, if you use ssh to log in to or run a command on another node, you are prompted for the password (or pass phrase) that you specified when you created the DSA key.

To enable the installer to use the `ssh` and `scp` commands without being prompted for a password, follow these steps:

1. On the system where you want to run the installer, log in as the Oracle user.
2. Enter the following commands:

```
$ exec /usr/bin/ssh-agent $SHELL
$ /usr/bin/ssh-add
```

3. At the prompts, enter the password (or pass phrase) for each key that you generated.

If you have configured SSH correctly, you can now use the `ssh` or `scp` commands without being prompted for a password or a pass phrase.

4. To test the SSH configuration, enter the following commands from the same session, testing the configuration of each cluster node:

```
$ ssh nodename1 'date'
$ ssh nodename2 'date'
    .
```

.

These commands should display the date set on each node. If any node prompts for a password or pass phrase, verify that the ~/.ssh/authorized_keys file on that node contains the correct public keys.

5. To ensure that X11 forwarding will not cause the installation to fail, create a user-level SSH client configuration file for the Oracle software owner user, as follows:

   a. Using any text editor, edit to create the `~oracle/.ssh/config` file.

   b. Ensure the ForwardX11 attribute is set to `no`, for example:

   ```
   Host *
         ForwardX11 no
   ```

6. You must run the installer from this session or remember to repeat steps 2 and 3 before you start the installer from a different session.

Some of the other preinstallation tasks are listed below:

- Configure SSH on all nodes.
- Oracle Clusterware/vendor clusterware must be running.

For more detailed information on these preinstallation and installation tasks that you must perform for an Oracle RAC installation, see *Oracle Real Application Clusters Installation and Configuration Guide*.

**Note:** See Chapter 3, Grid Control Common Configurations in *Oracle Enterprise Manager Advanced Configuration Guide* for more information about installing Grid Control on RAC nodes.

# Part III

# Postinstallation Configuration

This part discusses the postinstallation configurations that you must complete after successful installation. It also provides information on the ready-to-use Enterprise Manager Grid Control configurations, along with the instructions to customize your grid environment.

This part contains the following chapters:

# 15

# Postinstallation Configuration Tasks

This chapter identifies postinstallation configuration tasks you must complete after installation. The following topics are covered in this chapter:

- Running Configuration Scripts After the Installation Process (UNIX Only)
- Checking Database Settings
- Accessing My Oracle Support (formerly Metalink) Web Site
- Configuring Database and ASM Targets for Monitoring
- Exporting Environment Variable for Starting and Stopping Agent
- Reconfiguring and Rediscovering Agent
- Installing 'Clone Support Files' After Patching
-

## 15.1 Running Configuration Scripts After the Installation Process (UNIX Only)

The following sections describe the configuration scripts to be run after the installation completes successfully.

### 15.1.1 For Silent Installations

If you have performed any of the following silent installations, you must run the `allroot.sh` script to complete the installation:

- Enterprise Manager Using New Database

  If you have selected this installation option, you must execute the `allroot.sh` script from the database Oracle home (`db10g`). For example:

  ```
  /scratch/OracleHomes/db10g/allroot.sh
  ```

- Enterprise Manager Using Existing Database

  If you have selected this installation option, execute the `allroot.sh` script from the OMS Oracle home (`oms10g`). For example:

  ```
  /scratch/OracleHomes/oms10g/allroot.sh
  ```

- Additional OMS

  If you have selected this installation option, execute the `allroot.sh` script from the OMS Oracle home (`oms10g`). For example:

```
/scratch/OracleHomes/oms10g/allroot.sh
```

Execute the `root.sh` script from the agent Oracle home if you have performed a silent installation of only the Management Agent.

This script finishes the postinstallation steps for the Management Agent, OMS, and Management Repository database. If you used interactive mode to install Enterprise Manager, you are prompted to run `allroot.sh` or root.sh (depending on the installation type selected) before completing your installation.

On the OMS machine, run the `root.sh` script as the `root` user from the `$ORACLE_HOME` directory.

> **Note:** For a cluster installation, you must run the `root.sh` script on each host of the cluster on which you installed a Management Agent.

### 15.1.2 For agentDownload Script-Based Installations

If you have performed a Management Agent installation using the agentDownload script, then run the `root.sh` script. Also, run the `oraInstroot.sh` script if this is the first Oracle product on the host.

To do so:

- Log in as a root user on the host. Alternatively, use the sudo command to change to a root user.
- If this is the first Oracle product you just installed on the host, then run the `oraInstroot.sh` script from the Central Inventory:

  ```
  $Oracle_Home/oraInventory/oraInstRoot.sh
  ```

  For example, if you are using sudo to change to a root user, then you will run the following command:

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

- Run the `root.sh` script from the Oracle home directory of the Management Agent:

  ```
  <Oracle_Home>/root.sh
  ```

  For example, if you are using sudo to change to a root user, then you will run the following command:

  ```
  /usr/local/bin/sudo /scratch/OracleHomes/agent10g/root.sh
  ```

## 15.2 Checking Database Settings

You may want to check the following settings for your Management Repository database to make sure they are set correctly.

### 15.2.1 UNDO Tablespace and Temporary Tablespace

Oracle recommends you to set the UNDO tablespace and the temporary tablespace to AUTOEXTEND ON.

> **See Also:** Managing the UNDO Tablespace chapter of the *Oracle Database Administrator's Guide* for more information.

### 15.2.2 Archive Logging

Oracle recommends that the Management Repository database have archive logging turned on for any environment where continuity of data is important. Regular backups are also recommended.

### 15.2.3 Ensure the Database is Not in QUIESCE Mode

Oracle recommends that you do not put the Management Repository database in `QUIESCE` mode. Check your Resource Plan for `INTERNAL_QUIESCE`.

1. Navigate to the Database Home page of your Management Repository.
2. On the Administration property screen, under Resource Manager, click **Resource Plans.**
3. Make sure `INTERNAL_QUIESCE` has not been selected.

In `QUIESCE` mode, only DBA transactions are processed; all other transactions are suspended. Putting the Management Repository database in the `QUIESCE` mode suspends Enterprise Manager transactions.

## 15.3 Accessing My Oracle Support (formerly Metalink) Web Site

You can search My Oracle Support (formerly Metalink) for Oracle software patches and patchsets, and download these patches or patch sets to an appropriate location in the OMS Oracle home of Enterprise Manager.

To locate the required patches or patch sets in *My Oracle Support*:

1. Go to `http://metalink.oracle.com/` and navigate to the Patches and Updates screen.
2. Here, you can either perform a simple search with limited parameters, or click **Advanced Search** to perform a more granular (detailed) search. On this screen, you can search for updates based on the patch type (patches or patch sets), product name, platform, patch number, and so on.
3. Specify `emgrid` and click **Search.** The search results display all the patch or patch sets that match the parameters you have specified.
4. Select the appropriate patch or patch set and download it to the OMS Oracle home location.

### 15.3.1 Accessing Management Packs

Oracle offers a number of management packs for Oracle Database and Oracle Application Server. For example, management packs available with the Oracle Enterprise Manager 10*g* Release 2 include: Database Change Management Pack, Database Configuration Pack, Database Diagnostics Pack, and Database Tuning Pack. Oracle Application Server supports the following packs: Application Server Configuration Pack and Application Server Diagnostics Pack.

Each pack has several premium features bundled as part of that pack.

The licensable targets (also called parent targets) that are granted access to the packs propagate that access to their dependent targets. For example, all packs that are granted to a database propagate to the host on which the database resides.

For example, if databases D1, D2, and D3 reside on host H1, and the user has access to the Database Tuning pack for database D1, then not only is the D1 database granted access to the Database Tuning pack, but the host H1 is granted access to this pack as well.

You can manage, that is grant and revoke, access to packs for various databases and application servers in your Enterprise Manager repository by using the Management Pack Access option available from the Setup screen. This Management Pack Access function is available only for super administrators.

#### 15.3.1.1 Impact of Management Packs on Targets

Whether a target has access to a pack or not has a very significant impact on the user experience. The corresponding links related to the target, which need the pack, are enabled or disabled accordingly.

To know what packs a screen needs, as well as the links in that screen, click Show Management Pack Information in the screen footer.

When the access to a pack is removed from a target, all corresponding links that need this pack are disabled.

##### Identifying the Features that Can Be Accessed in Enterprise Manager

When one or more packs on a target monitored by Enterprise Manager are not licensed, access to premium functions for that target is disabled.

For example, the **Blackout** button located on a Target home page (which you can use to move the target to the *blackout* state), is enabled only when either the Oracle Database Diagnostics Pack or the Oracle Application Server Diagnostics Pack is licensed for that target.

To determine the packs used by the current screen and to know what packs need to be licensed for any link on that screen to be enabled, click Show Management Pack Information in the footer of the Enterprise Manager Home page. Enterprise Manager displays this information for all pages you navigate to during that session.

For more information on working with Management Packs, refer to the Enterprise Manager online Help.

### 15.3.2 Optional Configurations

You can perform the following configuration activities, if required:

#### 15.3.2.1 Specifying the My Oracle Support (formerly Metalink) Credentials

Enterprise Manager uses My Oracle Support (formerly Metalink) credentials to search for and download *My Oracle Support* patches. If you did not specify your My Oracle Support credentials during installation, you can do the following:

1. On the Enterprise Manager Grid Control Home page, click **Setup.**
2. On the Setup screen, click **Patching Setup.** Grid Control displays the Patching Setup page.
3. On the Patching Setup page, in the My Oracle Support and Proxy Connection tab, in the My Oracle Support section, specify your My Oracle Support user name and password in the fields provided.
4. In the My Oracle Support section, for **Patch Search URL**, you already have a default URL, that is, https://updates.oracle.com. Retain this default URL.

You can also access My Oracle Support directly by going to the following Web site:

`http://metalink.oracle.com/`

From this screen, Oracle licensees can register for an account or log in with an existing account. Once logged in, you can search for and download patches.

#### 15.3.2.2 Setting Up Proxy Configuration for the OMS

If you have a proxy server running on the host where OMS is installed, then you must set up the proxy server settings in Enterprise Manager Grid Control so that it can use those details to access *My Oracle Support (formerly Metalink)*. Also, you can choose to use the same proxy server settings or have different settings for the OMS to communicate with its Agents.

To set up the proxy server settings for OMS to access *My Oracle Support (formerly Metalink)* and also for OMS to communicate with its Agents, do the following:

1. In Grid Control, click **Setup** from the top-right corner of the home page.
2. On the Overview of Setup page, from the vertical menu to the left, click **Patching Setup**.
3. On the Patching Setup page, in the **My Oracle Support and Proxy Connection** tab, in the My Oracle Support Connection Setting section, select **Manual Proxy Configuration** and specify the prox server host, port, realm, user name, and password.

   **Note:** Only HTTP and HTTPS protocols are supported. Also note that NTLM proxy is not currently supported.
4. If you want to use the same proxy settings for communicating with Agents, then go to Step (6). Otherwise, go to Step (5).
5. In the Agent Connection Setting section, do one of the following:
   a. If you want to use the proxy settings given in My Oracle Support Connection Setting section, then retain the default section, that is, **Use My Oracle Support connection settings**.
   b. If you want t use proxy settings different from the ones specified in My Oracle Support Connection Setting section, then select **Manual proxy configuration** and specify the proxy server details.

      **Note:** Only HTTP and HTTPS protocols are supported. And NTLM proxy is not currently supported.
6. Click **Apply**.

The proxy server settings you specify are registered in the Management Repository. However, in case of multiple OMS environment, after you set up the proxy server settings for one OMS, restart other OMSes to ensure that the proxy server settings registered for communication with Agents are propogated across all OMSes.

## 15.4 Configuring Database and ASM Targets for Monitoring

When you first view the Database Home page for an Oracle Database 10*g* target, the Database Home page may display no monitoring data and the status of the database may indicate that there is a metric collection error. This is because the DBSNMP password has not been configured, or has been locked due to unsuccessful login attempts.

Similarly, the first time you display the home page for an Automatic Storage Management (ASM) target, the status of the ASM instance may be unknown or unavailable, and the home page may indicate that the Management Agent is unavailable (down). Again, this is because you need to supply the ASM SYS password.

**Note:** You may first need to unlock the DBSNMP user account before setting the monitoring credentials. If the account is not locked, skip Section 1.3.7, "Unlock the DBSNMP User Account" in the next chapter and proceed to Section 1.3.8, "Set Monitoring Credentials" for instructions.

To fix this problem for an Oracle Database target, do the following from the Grid Control console:

1. Unlock the DBSNMP User Account (if necessary).
2. Set Monitoring Credentials.

## 15.5 Exporting Environment Variable for Starting and Stopping Agent

Before you manually start or stop an agent, ensure that you export the ORACLE_HOSTNAME environment variable. For example, `export ORACLE_HOSTNAME=<host_name>`

## 15.6 Reconfiguring and Rediscovering Agent

The Agent Configuration Assistant (`agentca`) script is used to reconfigure the agent and rediscover the targets on the machine. This script is useful when you want to rediscover a newly added target on the machine or to convert a standalone agent to a Oracle RAC Agent.

You can make use of the following options in the `agentca` script.

***Table 15–1 Agent Configuration Assistant Script Options***

| Option | Description |
|---|---|
| -n | Specify the cluster name (CLUSTER_NAME). |
| -c | Specify a comma-separated cluster node list. |
| -t | Do not start the agent after reconfiguration or target rediscovery. |
| -d | Rediscover targets. |
| -f | Reconfigure agents. |
| -i | Specify the `oraInst.loc` (oracle inventory location). This is required when the Oracle home does not exist in the central inventory. |
| -h | Get information on all the available options. |

**Note:** You must specify either the `-f` or `-d` option when executing this script. Using one of these two options is mandatory.

**Caution:** Do not use the `agentca -f` option to reconfigure any upgraded agent (standalone and RAC).

### 15.6.1 Rediscover and Reconfigure Targets on Standalone Agents

An agent automatically discovers all targets that are installed before the agent installation. Typically, rediscovering of targets is performed when you have installed new targets after an agent installation.

To rediscover new targets, execute `agentca`. The usage is as follows:

```
<Agent_Home>/bin/agentca -d [ -t -i oraInstloc ]
```

### 15.6.2 Reconfiguring a Standalone Agent to an Oracle RAC Agent

Reconfiguration of a standalone agent occurs when you want to configure this agent (with standalone configurations) as a Oracle RAC agent.

To reconfigure a standalone agent as a Oracle RAC agent, you must execute the `agentca` script with the following options:

```
<Agent_Home>/bin/agentca -f -c "node1,node2…." [-t -i oraInstloc -n CLUSTER_NAME ]
```

**Note:** The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

### 15.6.3 Reconfiguring an Existing RAC Agent

If you have added new nodes to an existing Oracle RAC, you can invoke the `agentca` script to automatically reconfigure the existing Oracle RAC agent. The `agentca` script updates the central inventory to add the new nodes information, and also discovers the new targets (if any).

When this script is executed, it takes a back-up of the `EMSTATE` directory on the local machine and creates a new `EMSTATE` directory.

**Note:** You must run this script on only one node at a time.

To reconfigure an existing Oracle RAC agent, execute `agentca` as follows:

```
prompt> <Agent_Home>/bin/agentca -f  -c "node1,node2,node3....." [-t -i
oraInst.loc -n CLUSTER_NAME]
```

**Note:** The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

### 15.6.4 Rediscovering Targets on a Oracle RAC Agent

You can rediscover the new targets that have been installed on Oracle RAC nodes by running the agent configuration assistant with the following options.

```
prompt> <Agent_Home>/bin/agentca -d  -c "node1,node2,node3....." [-t -i
oraInst.loc -n CLUSTER_NAME]
```

**Note:** The `-c` option must comprise all the nodes (including the local machine) to update the inventory.

**Caution:** You run this script on only one node at a time.

## 15.7 Installing 'Clone Support Files' After Patching

As part of the upgrade of a Grid Control installation from 10.2.0.1/10.2.0.2 to 10.2.0.3 there is a need to download and install 'Clone Support Files' from My Oracle Support (formerly Metalink) and install onto each OMS as part of a post-patch configuration task to enable clone support for many major releases of Oracle Tech stack components.

## 15.8 Restarting OMS Whenever Management Agent IP Adress Changes

Hosts with multiple network interfaces or virtual hosts bound to single or multiple network adapters are accessible by more than one IP address. However, OMS and Management Agent always select the primary host alias.

For OMS, ensure that you do not change the IP address, but if you do change it, then deinstall the OMS and install a fresh one all over again.

For Management Agent, you may change the IP address, but ensure that you restart the OMS so that the new IP address is used. If you do not restart the OMS, you will see errors when you use this Management Agent to add a new target to Grid Control.

# Part IV

## Advanced Enterprise Manager Configuration

This part describes the advanced configuration tasks you can perform after you have installed Enterprise Manager Grid Control and have started using the product. These tasks are optional and provide additional functionality for specific types of Oracle Enterprise Manager customers.

This part contains the following chapters:

- Chapter 16, "Advanced Configuration Overview"
- Chapter 17, "Grid Control Common Configurations"
- Chapter 18, "Configuring Enterprise Manager for Active and Passive Environments"
- Chapter 19, "Configuring Enterprise Manager for Firewalls"
- Chapter 20, "Reconfiguring the Management Agent and Management Service"
- Chapter 21, "Additional Configuration Tasks"

# 16

# Advanced Configuration Overview

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:

- Types of Advanced Configuration Tasks
- Understanding the Enterprise Manager Directory Structure
- Enabling Enterprise Manager Accessibility Features

## 16.1 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.

## 16.2 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.

The directories and files installed by Enterprise Manager vary, depending upon the installation options you select during the Enterprise Manager installation. The location of Enterprise Manager files and directories also varies slightly when Enterprise Manager is installed as part of an Oracle Application Server or Oracle Database 10*g* installation.

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 10g Grid Control
- Understanding the Enterprise Manager Directories Installed with the Management Agent
- Understanding the Enterprise Manager Directories Installed with Oracle Application Server
- Understanding the Enterprise Manager Directories Installed with Oracle Database 10g
- Tip for Identifying the Oracle Home When Using the emctl Command
- Configuring Database Console During and After the Oracle Database 10g Installation
- Deconfiguring Database Control

## 16.2.1 Understanding the Enterprise Manager Directories Installed with Oracle Enterprise Manager 10*g* Grid Control

When you install Oracle Enterprise Manager 10*g* Grid Control, you can select from four installation types. All of these installation types, except the Oracle Management Agent installation type, install the Oracle Management Service.

When you install the Oracle Management Service, you actually install three Oracle home directories:

- The Management Service home directory
- The Management Agent home directory
- The Database home directory

**Note:** When you install Oracle Enterprise Manager 10*g* Grid Control, Oracle Database is also installed, but will not contain Enterprise Manager Configuration Assistant (EMCA) in the Oracle Database Home.

### 16.2.1.1 About the Oracle Management Service Home Directory

The Oracle Management Service is a J2EE application in the form of an OC4J instance (OC4J_EM) that is installed and deployed using the Oracle Application Server J2EE and Web Cache installation type.

The installation procedure installs the Enterprise Manager components within the Oracle Application Server Home, including the Oracle Management Service.

Information about the directories that are specific to the Oracle Application Server installation can be found in the Oracle Application Server documentation. For example, the location of the most of the Oracle Application Server configuration and log files are described in the Oracle Application Server documentation.

**See Also:** "Configuration Files and Log Files" in the *Oracle Application Server 10g Administrator's Guide*

#### 16.2.1.2 About the Oracle Management Agent Home (AGENT_HOME) Directory

In addition to the 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 Management Service host.

By default, if the Oracle Universal Installer (or the account used to run the Universal Installer) has the proper privileges to write to the install directories, the Management Agent is installed in a separate Oracle home directory at the same level as the Oracle Application Server home directory.

However, if the Oracle Universal Installer does not have the necessary privileges, the Management Agent is installed in a subdirectory of the Oracle Application Server home directory.

#### 16.2.1.3 Summary of the Important Directories in the Management Service Home

Figure 16–1 shows some of the important directories you should be familiar with in a typical Grid Control Console installation. You can use this information as you begin to maintain, troubleshoot, and configure the Oracle Management Service installation.

***Figure 16–1 Important Oracle Management Service Installation Directories***

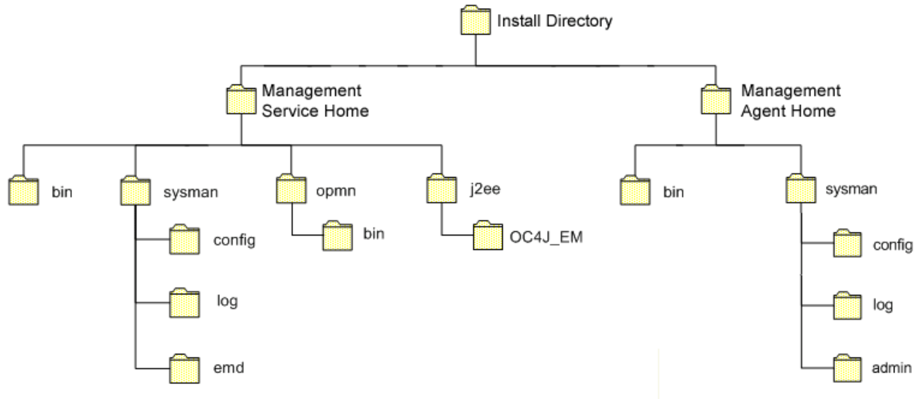


Table 16–1 describes in more detail the Management Service directories shown in Figure 16–1. In the table, ORACLE_HOME refers to the Management Service home directory in which the Oracle Management Service is installed and deployed.

***Table 16–1 Important Directories in the Management Service Oracle Home***

| Directory | Description |
|---|---|
| `ORACLE_HOME/bin` | The `bin` directory in the Oracle Application Server Home contains commands used to control the components of the Oracle Application Server J2EE and Web Cache installation, including the Application Server Control Console, which is used to monitor and configure Oracle Application Server instances.<br>Use the `emctl` command in this directory to start and stop the Application Server Control Console. For more information about the Application Server Control Console, see the *Oracle Application Server 10g Administrator's Guide*. |

*Table 16–1 (Cont.) Important Directories in the Management Service Oracle Home*

| Directory | Description |
|---|---|
| ORACLE_HOME/sysman | The sysman directory in the Oracle Application Server Home contains the system management files associated with this Oracle Application Server Release 2 (9.0.4) installation.<br>Note that the ORACLE_HOME/sysman/log directory contains the Oracle Management Service log files (emoms.log) and trace files (emoms.trc). |
| ORACLE_HOME/opmn | This directory contains files used to control the Oracle Process Manager and Notification Server (OPMN) utility. OPMN can be used to start and stop the instances of Oracle Application Server Containers for J2EE (OC4J) associated with this instance of Oracle Application Server. The Oracle Management Service runs as an application in one of those OC4J instances. |
| ORACLE_HOME/j2ee | This directory contains the files associated with the OC4J instances running in this instance of Oracle Application Server. For example, you will notice a directory for the OC4J_EM instance, which is the OC4J instance used to deploy the Management Service J2EE Web application. |
| ORACLE_HOME/hostname | For real application cluster agent install, this directory contains sysman files. |

## 16.2.2 Understanding the Enterprise Manager Directories Installed with the Management Agent

The Management Agent is installed automatically when you install the Grid Control Console. This local instance of the Management Agent gathers management information about the targets on the Management Service host. You can then manage those targets, such as the host itself, from the Grid Control Console.

The Management Agent is also available as its own install type. This enables you to install the Management Agent on the hosts throughout your enterprise. The Management Agent can then gather management data about the targets on each host so those targets can be managed from the Grid Control Console.

When you select the Additional Management Agent installation type, you install only the files required to run the Management Agent.

Specifically, the Management Agent files are installed into the same directory structure shown in the agent directory when you install the Oracle Management Service (Figure 16–1).

The directory that contains the files required to run the Management Agent is referred to as the AGENT_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_HOME. Similarly, to configure the log files for the Management Agent, you modify the configuration files in the sysman/config directory of the AGENT_HOME.

### 16.2.2.1 Summary of the Important Directories in the Management Agent Home

Table 16–2 describes some of the important subdirectories inside the AGENT_HOME directory.

*Table 16–2 Important Directories in the AGENT_HOME Directory*

| Directory | Description |
|---|---|
| AGENT_HOME | The agent directory contains all the files required to configure and run the Oracle Management Agent on this host.<br>This directory serves as the Oracle Home for the Management Agent. Later in this document, this directory is referred to as the AGENT_HOME.<br>If you install only the Management Agent on a managed host, only the files in this directory are installed. For more information, see "Understanding the Enterprise Manager Directories Installed with the Management Agent" on page 16-4. |
| AGENT_HOME/bin | The agent/bin directory in the Oracle Application Server Home contains the emctl command that controls the Management Agent for this host.<br>You use the emctl command in this directory to start and stop the Oracle Management Agent on this host. |
| AGENT_HOME/sysman/admin | This directory contains the files used by the Management Agent to define target types (such as databases, hosts, and so on), to run configuration scripts, and other administrative tasks. |
| AGENT_HOME/sysman/config | This directory contains the configuration files for the Management Agent. For example, this is where Enterprise Manager stores the emd.properties file. The emd.properties file defines settings such as the Management Service upload URL for this particular agent. |
| AGENT_HOME/sysman/log | This directory contains the log files for the Management Agent. |
| AGENT_HOME/hostname | For real application clusters, this directory contains all configuration, log files, and system files. |

#### 16.2.2.2 Understanding the Management Agent Directory Structure on Windows

When you install the 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.

For example, if you installed the Management Agent in the E:\oracle\em10gAgent directory of your Windows system, you can locate the emctl command for the Management Agent on a Windows system, by navigating to the following directory:

```
$PROMPT> E:\oracle\em10gAgent\bin
```

### 16.2.3 Understanding the Enterprise Manager Directories Installed with Oracle Application Server

When you install Oracle Application Server (Oracle Application Server), you also install the Oracle Enterprise Manager 10*g* Application Server Control Console. The Application Server Control Console provides you with the Enterprise Manager features required to manage your Oracle Application Server installation. As a result, the Oracle Application Server installation procedure installs a set of Enterprise Manager directories and files into each Oracle Application Server home directory.

In particular, the emctl commands required to control the Application Server Control Console are installed into the ORACLE_HOME/bin directory. The configuration and log files for the Application Server Control Console are installed into the ORACLE_HOME/sysman directory structure.

### 16.2.4 Understanding the Enterprise Manager Directories Installed with Oracle Database 10*g*

When you install Oracle Database 10*g*, you also install Oracle Enterprise Manager 10*g* Database Control. Database Control provides the tools you need to manage your Oracle Database 10*g* immediately after you install the database. As a result, the Oracle Database 10*g* installation procedure installs a set of Enterprise Manager directories and files into each Oracle Database 10*g* home directory.

In particular, the emctl commands required to control Database Console are installed into the ORACLE_HOME/bin directory.

The Management Agent and Management Service support files are installed in two locations in an Oracle Database 10*g* installation:

- Files that are common and shared among all instances of the database are stored in the following directory of the Oracle Database 10*g* home:

  ```
  ORACLE_HOME/sysman
  ```

  For example, the administration files, which define the supported target types and the scripts used to perform Management Agent configuration tasks are stored in the ORACLE_HOME/sysman/admin directory.

- Files that are unique to each instance of the database are stored in following directory of the Oracle Database 10*g* home:

  ```
  ORACLE_HOME/hostname_sid/ (for a single instance database)
  ORACLE_HOME/nodename_sid/ (for a cluster database)
  ```

  Throughout the rest of this guide, ORACLE_HOME/hostname_sid/ and ORACLE_HOME/nodename_sid/ may be used interchangeably. Both paths refer to the same concept – the Enterprise Manager directory for the specific database instance. The difference is that ORACLE_HOME/hostname_sid/ is used for single instance databases, while ORACLE_HOME/nodename_sid/ is used for cluster (Oracle RAC) databases. In cluster databases, nodename refers to the public name of the node, as specified during Cluster Ready Services (CRS) configuration for cluster environments.

  For example, if the database host name is mgmt1.example.com and the system identifier for the database instance is db42, the log files for the Management Agent and Management Service for that instance are installed in the following directory:

  ```
  ORACLE_HOME/mgmt1.example.com_db42/sysman/log
  ```
  If a *hostname_sid* directory does not exist in the Oracle Database 10*g* home directory, then Oracle Enterprise Manager 10*g* Database Control was never configured for the database instance.

  > **See Also:** "Configuring Database Console During and After the Oracle Database 10g Installation" on page 16-8

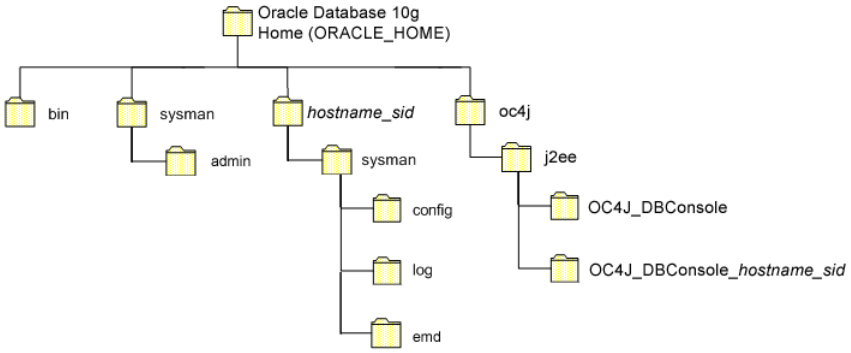
In addition, the files required to deploy the Database Console as a J2EE application are installed into the ORACLE_HOME/oc4j/j2ee directory structure. Database Console is a J2EE application that is deployed using the standalone version of Oracle Application Server Containers for J2EE (OC4J). The `OC4J_DBConsole` directory contains the template files that are used to create database-specific deployment directories for each Database Console instance deployed in the Oracle home.

The installation and configuration files are stored in the ORACLE_HOME directory in the following sub-directories:

- cfgtoollogs/cfgfw
- cfgtoollogs/dbua
- cfgtoollogs/netca
- cfgtoollogs/rconfig
- cfgtoollogs/dbca
- cfgtoollogs/emca
- cfgtoollogs/oui
- cfgtoollogs/opatch

Figure 16–2 summarizes the location of the important Enterprise Manager directories in a typical Oracle Database 10*g* home directory. Note that references to hostname_sid are for single instance databases; cluster databases have paths of the form nodename_sid instead.

***Figure 16–2 Important Enterprise Manager Directories in an Oracle Database 10g Installation***



## 16.2.5 Tip for Identifying the Oracle Home When Using the emctl Command

When you install Grid Control, Oracle Application Server, or Oracle Database 10*g*, the resulting directory structure can often include multiple subdirectories with the same name. For example, you can have a `bin` directory within the AGENT_HOME directory. Use the `emctl` command within the `AGENT_HOME/bin` directory to control the Management Agent.

In addition, you can have a `bin` directory within the Management Service Oracle home. Use the `emctl` command in this directory to control the Management Service.

To quickly identify the Oracle 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 Oracle home that will be affected by commands executed by this instance of the `emctl` command. For example, the following example shows how the current `emctl` command can be used to control the Management Service installed in the /dev1/private/em_ms_home1/ Oracle home:

```
$PROMPT> emctl getemhome
Copyright (c) 1996, 2004 Oracle Corporation. All rights reserved.
EMHOME=/dev1/private/em_ms_home1
```

## 16.2.6 Configuring Database Console During and After the Oracle Database 10*g* Installation

The following sections describe how Oracle Enterprise Manager 10*g* Database Control is configured during the Oracle Database 10*g* installation. These sections also describe how you can configure Database Console after the installation:

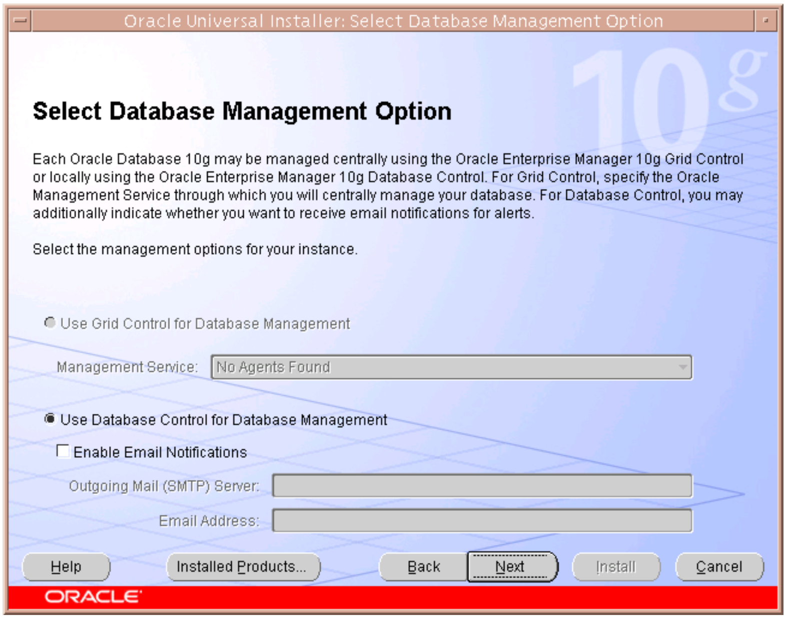
- Configuring Database Console During Installation
- Configuring Database Console with DBCA
- Configuring Database Console with EMCA
- Using EMCA with Oracle Real Application Clusters
- EMCA Troubleshooting Tips

### 16.2.6.1 Configuring Database Console During Installation

If you create a database while installing Oracle Database 10*g*, you have the option of configuring your database so it can be managed by Oracle Enterprise Manager 10*g* Grid Control Console or by Oracle Enterprise Manager Database Console.

Figure 16–3 shows the Management Options page, which allows you to select your database management options while installing Oracle Database 10*g*.

***Figure 16–3 Selecting Your Management Options While Installing Oracle Database 10g***


Oracle Universal Installer: Select Database Management Option
10g
Help
Installed Products...
Back
Next
Install
Cancel
ORACLE

**Select Database Management Option**

Each Oracle Database 10g may be managed centrally using the Oracle Enterprise Manager 10g Grid Control or locally using the Oracle Enterprise Manager 10g Database Control. For Grid Control, specify the Oracle Management Service through which you will centrally manage your database. For Database Control, you may additionally indicate whether you want to receive email notifications for alerts.

Select the management options for your instance.

○ Use Grid Control for Database Management

Management Service: No Agents Found

● Use Database Control for Database Management

□ Enable Email Notifications

Outgoing Mail (SMTP) Server:

Email Address:

To select Grid Control Console as your management option, the Oracle Management Service must be installed on a network host. In addition, the Oracle Management

Agent must be installed on the host where you are installing the database. Otherwise, the Grid Control Console option is unavailable and you must instead choose to manage your database with Database Control.

For most of the Oracle Database 10*g* installation types, you must choose either Database Control or Grid Control as your management option when you create a database during the installation.

However, if you create a database using one of the following methods, you can choose not to configure Database Console:

- Choosing to create a database during a custom installation
- Choosing the Advanced database configuration option during an Enterprise or Standard Edition installation
- Running Database Configuration Assistant (DBCA) after the installation

If you do not configure Database Console during the Oracle Database 10*g* installation, no *hostname_sid* directory is created in the resulting Oracle home directory (Figure 16–2).

#### 16.2.6.2 Configuring Database Console with DBCA

The primary method for configuring an existing Oracle Database 10*g* database so it can be managed with Database Console is to use DBCA. You can use DBCA to create a new database or to reconfigure an existing database.

> **See Also:** "Installing Oracle Software and Building the Database" in *Oracle Database 2 Day DBA* for more information about using DBCA to create a new database instance

To use DBCA to reconfigure your database so it can be managed with Database Console:

1. Log into the database host as a member of the administrative group that is authorized to install Oracle software and create and run the database.
2. Start DBCA, as follows:
   - On Windows, select **Start, point to Programs, Oracle -** ***home_name*****, Configuration and Migration Tools, and then select Database Configuration Assistant**.
   - On UNIX, change directory to the `ORACLE_HOME/bin` directory and enter the following command:

     ```
     $PROMPT> ./dbca
     ```

   The DBCA Welcome page appears.
3. Advance to the Operations page and select **Configure Database Options**.
4. Advance to the Database page and select the database you want to configure.
5. Advance to the Management Options page (Figure 16–4) and select the following options:
   - **Configure the Database with Enterprise Manager**
   - **Use Database Control for Database Management**
6. Optionally, select the options for enabling e-mail notifications and enabling daily backups.

For more information about Enterprise Manager notifications and daily backups, click **Help** on the Management Options page.

7. Advance until the **Finish** button is available.

8. Click **Finish** to reconfigure the database so it uses Database Console.

   After DBCA reconfigures the database, a new subdirectory appears in the Oracle home. This directory is named using the following format and contains Database Console configuration and state files specific to the database you just configured:

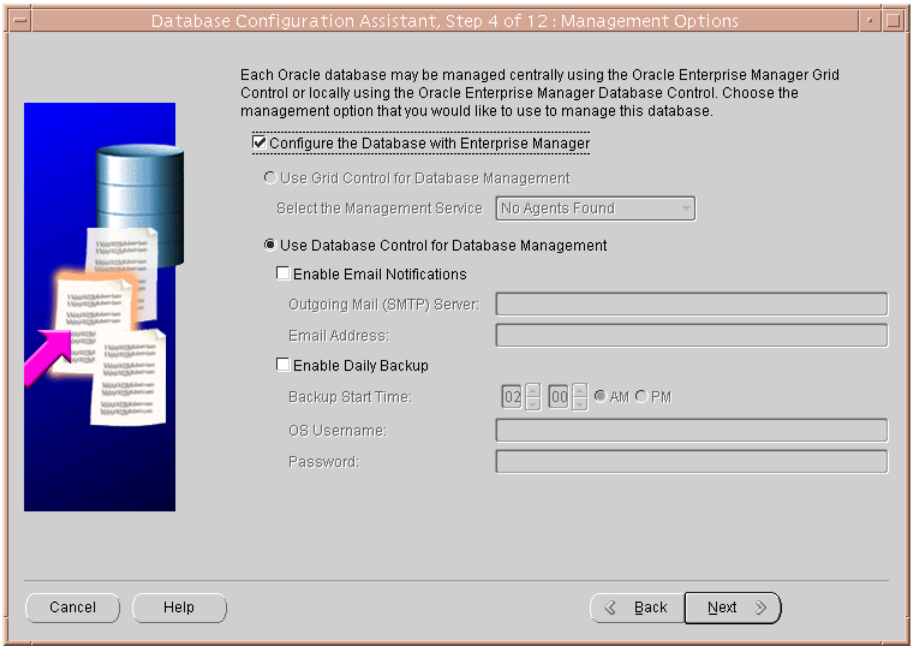
   ```
   hostname_sid
   ```

   For example:

   ```
   mgmthost1.example.com_myNewDB
   ```

   Note that for cluster databases, the directories are named nodename_sid.

***Figure 16–4 Management Options Page in DBCA***



Database Configuration Assistant, Step 4 of 12 : Management Options

Each Oracle database may be managed centrally using the Oracle Enterprise Manager Grid Control or locally using the Oracle Enterprise Manager Database Control. Choose the management option that you would like to use to manage this database.

☑ Configure the Database with Enterprise Manager

○ Use Grid Control for Database Management

Select the Management Service: No Agents Found

● Use Database Control for Database Management

□ Enable Email Notifications

Outgoing Mail (SMTP) Server:

Email Address:

□ Enable Daily Backup

Backup Start Time: 02 00 ● AM ○ PM

OS Username:

Password:

## 16.2.6.3 Configuring Database Console with EMCA

When you use DBCA to configure Oracle Database 10*g*, DBCA provides a graphical user interface to help you select Database Console options and to configure other aspects of your database.

However, if you want to use the operating system command line to configure Database Console, you can use the Enterprise Manager Configuration Assistant (EMCA).

> **WARNING:** **During the database configuration using EMCA with -repos option, the database will be unavailable and users cannot connect to the database or perform operations on the database during the time that the repository is being dropped or recreated.It should not be run on a production database unless you are fully aware of the possible impact to database availability and have planned for this eventuality.**

To configure Database Console with EMCA:

1. Set the following environment variables to identify the Oracle home and the system identifier (SID) for the database you want to manage:
   - ORACLE_HOME
   - ORACLE_SID
2. Change directory to the `ORACLE_HOME/bin` directory.
3. Start EMCA by entering the following command with any of the optional command-line arguments shown in Table 16–3:

   ```
   $PROMPT> ./emca
   ```

   Depending upon the arguments you include on the EMCA command line, EMCA prompts you for the information required to configure Database Console.

   For example, enter the following command to configure Database Console so it will perform automatic daily backups of your database:

   ```
   $PROMPT> ./emca -config dbcontrol db -backup
   ```

EMCA commands are of the form:

```
emca [operation] [mode] [flags] [parameters]
```

> **Note:** To configure Database Console for single instance database using ASM, no extra parameters need to be passed along with the EMCA command. Run the following command to configure the Database Console which will automatically detect the ASM instance:
>
> ```
> emca -config dbcontrol db -repos create
> ```

Table 16–3 describes the valid execution operations and modes, and lists the optional parameters in brackets. Table 16–4 discusses the flags and their behavior, while Table 16–5 defines the optional parameters in detail. EMCA parameters are of the form [ -parameterName parameterValue ]. Multiple parameters can be used in combination at the command line.

*Table 16–3 EMCA Command-Line Operations*

| Command | Description |
|---|---|
| emca -h \| --h \| -help \| --help | Use this option to display the Help message for the EMCA utility. The options described in Table 16–3, Table 16–4, andTable 16–5, and the valid parameters you may include are listed. |
| emca –version | Prints the version information associated with EMCA. |

*Table 16–3 (Cont.) EMCA Command-Line Operations*

| Command | Description |
|---|---|
| emca -config dbcontrol db [-repos (create \| recreate)] [-cluster] [-silent] [-backup] [parameters] | Configures Database Control for a database. Options include creating (or recreating) Database Control repository, configuring automatic backups, and performing these operations on a cluster database. |
| emca -config centralAgent (db \| asm) [-cluster] [-silent] [parameters] | Configures central agent management for a database or an Automatic Storage Management (ASM) instance. Options include performing this operation on a cluster environment.This operation will configure the database so that it can be centrally managed by the Oracle Enterprise Manager 10g Grid Control Console. To use this option, you must have previously installed the Oracle Management Service component of Enterprise Manager on a network host. In addition, the Oracle Management Agent must be installed on the host where you are running the database. |
| emca -config all db [-repos (create \| recreate)] [-cluster] [-silent] [-backup] [parameters] | Configures both Database Control and central agent management for a database. The possible configuration options are similar to those described above. |
| emca -deconfig dbcontrol db [-repos drop] [-cluster] [-silent] [parameters] | Deconfigures Database Control for a database. Options include dropping the Database Control repository and performing these operations on a cluster database. For example, you might use this command to remove the Database Control configuration from a database you are planning to delete. In such a scenario, remove the Database Control configuration before physically deleting the database. This operation does not remove the actual database or its data files. |
| emca -deconfig centralAgent (db \| asm) [-cluster] [ -silent] [parameters] | Deconfigures central agent management for a database or an ASM instance. Options include performing this operation on a cluster environment. For example, you might use this command to remove the central agent management configuration from a database you are planning to delete. In such a scenario, remove the central agent management configuration before physically deleting the database. This operation does not remove the actual database or its data files. |
| emca -deconfig all db [-repos drop] [-cluster] [-silent] [parameters] | Deconfigures both Database Control and central agent management for a database. The possible deconfiguration options are similar to those described above. |
| emca -addInst (db \| asm) [-silent] [parameters] | Configures Enterprise Manager for a new cluster instance of a database or ASM storage. For more information, refer to Section 16.2.6.5. |
| emca -deleteInst (db \| asm) [-silent] [parameters] | Deconfigures Enterprise Manager for a specific instance of a cluster database or ASM storage. This is discussed further below, in Section 16.2.6.5. |
| emca -reconfig ports [-cluster] [parameters] | Explicitly reassigns Database Control ports. Options include performing this operation on a cluster environment. For more information, refer to Section 16.2.6.6. |
| emca -reconfig dbcontrol -cluster [-silent] [parameters] | Reconfigures Database Control deployment for a cluster database. Note that this command must be used with the "-cluster" option. For more information, refer to Section 16.2.6.5. |
| emca -displayConfig dbcontrol -cluster [-silent] [parameters] | Displays information about the current deployment configuration of Database Control in a cluster environment. Note that this command must be used with the "-cluster" option. For more information, refer to Section 16.2.6.5. |

*Table 16–3 (Cont.) EMCA Command-Line Operations*

| Command | Description |
|---|---|
| emca -upgrade (db \| asm \| db_asm) [-cluster] [-silent] [parameters] | Upgrades the configuration of an earlier version of Enterprise Manager to the current version. This operation can be performed for database, ASM, or database and ASM instances together simultaneously. This does not upgrade the actual database or ASM instances, nor does it upgrade the Enterprise Manager software. Instead, it upgrades the configuration files for the specified instance so that they are compatible with the current version of the Enterprise Manager software. EMCA will attempt to upgrade all instances of the specified database and/or ASM target on the host, across all Oracle Homes (since it is likely that certain target properties, such as listener port or Oracle Home, have changed). |
| emca -restore (db \| asm \| db_asm) [-cluster] [-silent] [parameters] | Restores the current version of Enterprise Manager configuration to an earlier version. This is the inverse of the "-upgrade" option (and will reverse any changes that result from an "-upgrade" operation), and as such, the options are similar. |

*Table 16–4 EMCA Command-Line Flags*

| Flag | Description |
|---|---|
| db | Performs the operation for a database (including cluster databases). Use this option for databases that use Automatic Storage Management (ASM) to store the data files. If a database is using ASM, all the configuration operations and modes described above (except for "-upgrade" and "-restore") will detect this automatically and apply the changes to both the database and ASM instance(s). |
| asm | Performs the operation for an ASM-only instance (including cluster ASM instances). |
| db_asm | This flag can only be used in "-upgrade" and "-restore" mode. Performs the upgrade/restore operation for a database and an ASM instance together. Database and ASM instances may be upgraded or restored separately (that is, upgrading an ASM instance does not require upgrading the database instances it services). Hence, the Enterprise Manager configuration can be upgraded or restored separately for a database and its respective ASM instance. |
| -repos create | Creates a new Database Control management repository. |
| -repos drop | Drops the current Database Control management repository. |
| -repos recreate | Drops the current Database Control management repository and then recreates a new one. |
| -cluster | Performs the operation for a cluster database or ASM instance. |
| -silent | Performs the operation without prompting for additional information. If this mode is specified, all the required parameters must be entered at the command line or specified in an input file using the –respFile argument. You can view a list of the available parameters by entering emca -help at the command line. |

*Table 16–4 (Cont.) EMCA Command-Line Flags*

| Flag | Description |
|---|---|
| -backup | Configures automatic backup for a database. EMCA will prompt for daily automatic backup options. The default Enterprise Manager settings will be used to backup the database files.<br>Note: If you use this option, EMCA will use the value of the db_recovery_file_dest initialization parameter to identify the flashback recovery area for the automated backups. If that parameter is not set, EMCA will generate an error. You can modify these settings later using the Maintenance page in Database Control. For more information, see the Database Control online Help. |

*Table 16–5 EMCA Command-Line Parameters*

| Parameter | Description |
|---|---|
| -respFile | Specifies the path of an input file listing parameters for EMCA to use while performing its configuration operation. For more information, refer to Section 16.2.6.4. |
| -SID | Database system identifier |
| -PORT | Port number for the listener servicing the database |
| -ORACLE_HOME | Database Oracle Home, as an absolute path |
| -LISTENER_OH | Oracle Home from where the listener is running. If the listener is running from an Oracle Home other than the one on which the database is running, the parameter LISTENER_OH must be specified. |
| -HOST_USER | Host machine user name (for automatic backup) |
| -HOST_USER_PWD | Host machine user password (for automatic backup) |
| -BACKUP_SCHEDULE | Schedule in the form of "HH:MM" (for daily automatic backups) |
| -EMAIL_ADDRESS | E-mail address for notifications |
| -MAIL_SERVER_NAME | Outgoing Mail (SMTP) server for notifications |
| -ASM_OH | Automatic Storage Management Oracle Home |
| -ASM_SID | System identifier for ASM instance |
| -ASM_PORT | Port number for the listener servicing the ASM instance |
| -ASM_USER_ROLE | User role for connecting to the ASM instance |
| -ASM_USER_NAME | User name for connecting to the ASM instance |
| -ASM_USER_PWD | Password for connecting to the ASM instance |
| -DBSNMP_PWD | Password for DBSNMP user |
| -SYSMAN_PWD | Password for SYSMAN user |
| -SYS_PWD | Password for SYS user |
| -SRC_OH | Oracle Home of the database with Enterprise Manager configuration to be upgraded/restored |
| -DBCONTROL_HTTP_PORT | Use this parameter to specify the port you use to display the Database Control Console in your Web browser. For more information, refer to Section 16.2.6.6. |
| -AGENT_PORT | Use this parameter to specify the Management Agent port for Database Control. For more information, refer to Section 16.2.6.6. |

*Table 16–5 (Cont.) EMCA Command-Line Parameters*

| Parameter | Description |
|---|---|
| -RMI_PORT | Use this parameter to specify the RMI port for Database Control. For more information, refer to Section 16.2.6.6. |
| -JMS_PORT | Use this parameter to specify the JMS port for Database Control. For more information, refer to Section 16.2.6.6. |
| -CLUSTER_NAME | Cluster name (for cluster databases) |
| -DB_UNIQUE_NAME | Database unique name (for cluster databases) |
| -SERVICE_NAME | Database service name (for cluster databases) |
| -EM_NODE | Node from which Database Control console is to be run (for cluster databases). For more information, refer to Section 16.2.6.5. |
| -EM_SID_LIST | Comma-separated list of SIDs for agent-only configurations, uploading data to –EM_NODE. For more information, refer to Section 16.2.6.5. |

### 16.2.6.4 Using an Input File for EMCA Parameters

Instead of answering a series of prompts when you run EMCA, you can use the `-respFile` argument to specify an input file. The input file you create must be in a format similar to the following example:

```
PORT=1521
SID=DB
DBSNMP_PWD=xpE234D
SYSMAN_PWD=KDOdk432
```

After you create an EMCA input file, you can use it on the command line as follows:

```
$PROMPT> ./emca -config dbcontrol db -respFile input_file_path
```

For example, to configure the Database Console to perform daily backups and create the Database Control Management Repository, create an input file similar to the one shown in Example 16–1 and enter the following command at the operating system prompt:

```
$PROMPT> ./emca -config dbcontrol db -repos create -backup -respFile input_file_
path
```

***Example 16–1 EMCA Input File that Configures Database Control for Automatic Backup and Creates the Database Control Management Repository***

```
PORT=1521
SID=DB
DBSNMP_PWD=dow31224
SYSMAN_PWD=squN3243
HOST_USER=johnson
HOST_USER_PWD=diTf32of
SYS_PWD=qlKj4352
BACKUP_SCHEDULE=06:30
```

### 16.2.6.5 Using EMCA with Oracle Real Application Clusters

Oracle Real Application Clusters (Oracle RAC) provides a high availability database environment spanning multiple hosts. Each cluster may be made up of multiple cluster databases, each of which consists of multiple cluster database instances. A cluster database is available as long as one of its instances is available.

Each EMCA command can be used in Real Application Clusters environments; certain commands are only applicable in cluster setups. To indicate that you have a cluster database, use the –cluster flag which is available in almost every EMCA operational mode.

When you use EMCA to configure Database Console for Real Application Clusters, you configure the Database Console for each instance in the cluster. However, by default, the Database Control Console will only start on the local node. On every other node of the cluster, only the Enterprise Manager agent will start. This is because the Database Control Console opens a number of connections to the database. If an instance of the console is running on every host in the cluster, then you may easily exceed the maximum number of permitted open connections on a 32-node or 64-node environment.

To remedy this, the Database Control Console is only started on the local node. On every other node, the commands emctl start dbconsole and emctl stop dbconsole only start and stop the agent. Each of the remote agents will upload their respective data to the console running on the local node, from where you can monitor and manage all the targets in the cluster. On each instance of the Oracle RAC database, the following subdirectories will be created:

```
$ORACLE_HOME/nodename1_SID1
$ORACLE_HOME/nodename2_SID2
.
.
$ORACLE_HOME/nodenamen_SIDn
```

where SID1...SIDn are database system identifiers.

However, note that if you upgrade a 10g Release 1 cluster database (configured with Database Control) to 10g Release 2, the 10g Release 1 Database Control configuration will be retained. The 10g Release 1 Database Control has a Database Console running on each node for the real-application cluster. The console will still be started on each individual node. If you wish to modify the configuration, use the following command:

```
emca -reconfig dbcontrol -cluster -EM_NODE nodename -EM_SID_LIST SID list
```

where *nodename* is the public name of the node and *SID list* is a comma-separated list of database system identifiers. This command reconfigures the current Database Control setup and:

1. Starts a Database Control Console on *nodename*, if one has not been started yet.
2. Redirects the agents monitoring the database instances in *SID list* so that they upload their data to the console running on *nodename*. Also, agents monitoring database instances on *nodename* will also upload their data to the local console. Note that if you do not pass -EM_NODE or -EM_SID_LIST at the command line, you will be prompted for them.

-EM_NODE defaults to the local node if not specified when prompted. -EM_SID_LIST defaults to all database instances if not specified.

You may use this command to start the console on more than one node. For instance, on an 8-node cluster with node1, node2, node3, node4, node5, node6, node7, node8 and database instances oradb1, oradb2, oradb3, oradb4, oradb5, oradb6, oradb7, oradb8, you can run the following commands in succession:

```
$PROMPT> emca -reconfig dbcontrol -cluster -EM_NODE node1 -EM_SID_LIST
oradb2,oradb3,oradb4
```

```
$PROMPT> emca -reconfig dbcontrol -cluster -EM_NODE node5 -EM_SID_LIST
oradb6,oradb7,oradb8
```

In this scenario, there will be two Database Control consoles running, one on node1 and the other on node5. From either of these consoles, you can manage and monitor all targets in the cluster.

For information on the current cluster configuration, you can run:

```
emca -displayConfig dbcontrol -cluster
```

The above command prompts for the database unique name for the cluster database. This will print the current configuration onto the screen, indicating the nodes that have consoles running on them and the consoles where each agent is uploading.

For configuring Enterprise Manager for a new cluster instance of a database or ASM storage, use the following command:

```
emca -addInst db
```

On cluster databases, another common operation is the creation and deletion of database instances. After you create a new instance, you can run EMCA to configure Database Control or central agent management for that instance using the command emca -addInst db. Running EMCA does not create the actual database instance; it only configures Enterprise Manager so that you can manage the instance in a way consistent with the rest of the cluster database instances. When configuring Enterprise Manager for a new instance, run the EMCA command only after you have created the instance. Also, run the command from a node in the cluster that already has Enterprise Manager configured for its associated database instance, as these configuration settings will be propagated to the new instance. Do not run this command from the node on which the new instance was created. Note that this option can be used only in a Real Application Clusters environment, so you do not need to use the -cluster option on the command line. After running the command emca -addInst db, enter the following information for the node and database:

```
Node name: node2
Database Unique Name: EM102
Database SID: EM1022
```

To deconfigure Enterprise Manager for a specific database instance (typically before the database instance is deleted), use the inverse command, emca -deleteInst db. Running EMCA does not delete the database instance; it only removes the Enterprise Manager configuration so that you will no longer be able to manage the instance with Enterprise Manager. Ensure that you run the EMCA command before you delete the actual cluster database instance. Also, ensure that you run the command from a different node and not from the node on which the database instance will be deleted. Note that this option can be used only in a Real Application Clusters environment, so you do not need to use the -cluster option on the command line.

For more information, see Table 16–3 which describes EMCA command-line operations.

> **Note:** If you use emca -c to configure the Database Control for Real Application Clusters, check TNS_ADMIN on all cluster nodes. If different TNS_ADMIN are set for each node, the listener for the target cannot be configured correctly. If so, set the same TNS_ADMIN on all cluster nodes before executing the emca -c command.

#### 16.2.6.6 Specifying the Ports Used By the Database Console

When you initially install Oracle Database 10*g* or configure the Database Console with EMCA, the Database Console uses a set of default system ports. For example, by default, you access Database Console using port 1158 in 10*g* Release 2, as in:

```
http://host.domain:1158/em
```

This is the default port assigned to Database Control by the Internet Assigned Numbers Authority (IANA). Likewise, the default Database Control Agent port, as assigned by the IANA, is 3938.

To use ports other than the default ports, use the following EMCA command-line arguments when you initially configure the Database Console with EMCA. Alternatively, you can explicitly assign ports after configuring Database Control using the following command:

```
emca -reconfig ports [-cluster]
```

> **Note:** You can also use the following EMCA command-line arguments to configure Database Control after you have installed and configured Oracle Database 10*g*.

The following list summarizes the EMCA command-line arguments that control the standard Database Control port assignments:

- -DBCONTROL_HTTP_PORT *port_number*

  This port number is used in the Database Control Console URL. For example, if you set this port to 5570, you can then display the Database Control Console using the following URL:

  ```
  http://host.domain:5570/em
  ```

- -RMI_PORT *port_number*

  This port number is used by the Remote Method Invocation (RMI) system, which is part of the J2EE software required by Database Control. The default port can be changed if the user wants to configure a specific port for Database Console. When a port other than the default port (1521) is used, use the -RMI_PORT or -JMS_PORT options along with the emca reconfig command.

- -JMS_PORT *port_number*

  This port is used by the OC4J Java Message Service (JMS), which is part of the J2EE software required by Database Control. The default port can be changed if the user wants to configure a specific port for Database Console. When a port other than the default port (1521) is used, use the -RMI_PORT or -JMS_PORT options along with the emca reconfig command.

- -AGENT_PORT *port_number*

  This port is used by the Database Control Management Agent, which is monitoring and administering the database for the Database Control.

#### 16.2.6.7 EMCA Troubleshooting Tips

The following section describes some troubleshooting tips to consider when using EMCA to configure the Database Control:

- Using EMCA After Changing the Database Listener Port

- Upgrading Database or ASM Instances with 10g Release 2 Grid Control Agents

**16.2.6.7.1 Using EMCA After Changing the Database Listener Port** If you change the listener port of the database after you have configured Database Control, the database status will appear as down. To reconfigure Database Control so it uses the new listener port, run the EMCA command using the -config dbcontrol db [-cluster] command-line arguments.

**16.2.6.7.2 Upgrading Database or ASM Instances with 10g Release 2 Grid Control Agents** When upgrading a 10g Release 1 database and/or ASM instance that was configured for Oracle Enterprise Manager (either Database Control or a Grid Control central agent) to 10g Release 2, all Enterprise Manager targets on the relevant host(s) referring to the upgraded instance(s) will be updated automatically. This is because the upgrade involves altering the instance's Oracle Home, port, or other target-associated properties. However, some of these targets on the host(s) will not be updated successfully during the upgrade if they are managed by a 10g Release 2 Grid Control Agent. To update these targets, in the Home page for the upgraded database (or ASM) target, click the "Monitoring Configuration" link. On this page, you can update the required properties such as Oracle Home, listener port and so on to the correct values.

**16.2.6.7.3 Using EMCA When Database Host Name or IP Address Changes** When the database host name (including the domain name) or the IP address changes, deconfigure and then reconfigure the Database Console with the repository create command. Run the following command:

```
emca -deconfig dbcontrol db -repos drop
emca -config dbcontrol db -repos create
```

or

```
emca -deconfig dbcontrol db
emca -config dbcontrol db -repos recreate
```

**16.2.6.7.4 Using EMCA When the TNS Configuration Is Changed** When the TNS configuration is changed, set the environment variable and then run the following command:

```
emca -config dbcontrol db
```

## 16.2.7 Deconfiguring Database Control

You can deconfigure Database Control through EMCA, the operating system command line. To deconfigure Database Console, use the following command:

```
emca -deconfig dbcontrol db [-repos drop] [-cluster] [-silent] [parameters]
```

The above command deconfigures Database Control for a database. Options include dropping the Database Control repository and performing these operations on a cluster database. For example, you might use this command to remove the Database Control configuration. In such a scenario, remove the Database Control configuration before physically deleting the database. This operation does not remove the actual database or its data files.

To deconfigure Database Control for a single instance database, run the following command:

```
emca -deconfig dbcontrol db -repos drop -SID database sid -PORT listener port
-SYS_PWD password for sys user -SYSMAN_PWD password for SYSMAN user
```

To deconfigure Database Control for an Oracle Real Application Clusters (Oracle RAC) database, run the following command:

```
emca -deconfig dbcontrol db -repos drop -cluster -DB_UNIQUE_NAME database unique
name -PORT listener port -SYS_PWD password for sys user -SYSMAN_PWD password for
SYSMAN user -CLUSTER_NAME cluster name
```

You will need to deconfigure Database Control if you want to configure Grid Control to use a database already configured with Database Control. Grid Control will detect the Database Control SYSMAN schema and prompt the user to discard the Database Control SYSMAN schema and re-create one for Grid Control. Shutdown and deconfigure Database Control before proceeding to overwrite the SYSMAN schema.

If you are planning to configure a new database to be used as a Grid Control repository, do not configure Database Control during this database installation.

## 16.3 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.

To enable these features and provide for full accessibility, you must modify two configuration settings, which are described in the following sections:

- Enabling Enterprise Manager Accessibility Mode
- Providing Textual Descriptions of Enterprise Manager Charts

### 16.3.1 Enabling Enterprise Manager Accessibility Mode

Enterprise Manager takes advantage of user interface development technologies that improve the responsiveness of some user operations. For example, when you navigate to a new record set in a table, Enterprise Manager does not redisplay the entire HTML page.

However, this performance-improving technology is generally not supported by screen readers. To disable this feature, and as a result, make the Enterprise Manager HTML pages more accessible for disabled users, use the following procedure.

> **Note:** The following procedure is valid for both Grid Control Console and Database Console installations. Differences in the location of configuration files is noted where applicable.
>
> For information on enabling accessibility for the Application Server Control Console, see "Managing and Configuring the Application Server Control" in the *Oracle Application Server 10g Administrator's Guide*.

1. Locate the `uix-config.xml` configuration file.

   To locate the `uix-config.xml` file in a Grid Control Console installation, change directory to the following location in the Management Service home:

   ```
   ORACLE_HOME/j2ee/OC4J_EM/applications/em/em/WEB-INF (Grid Control)
   ```

   To locate the `uix-config.xml` file in a Oracle Database 10*g* installation, change directory to the following location in the database home:

```
ORACLE_HOME/oc4j/j2ee/oc4j_applications/applications/em/em/WEB-INF (Database
Control)
```

2. Open the `uix-config.xml` file using a text editor and locate the following entry:

```
<!-- An alternate configuration that disables accessibility features  -->
<default-configuration>
  <accessibility-mode>inaccessible</accessibility-mode>
</default-configuration>
```

3. Change the value of the `accessibility-mode` property from `inaccessible` to `accessible`.
4. Save and close the file.
5. Restart the Oracle Management Service (if you are modifying a Grid Control Console installation) or restart the Database Console (if you are modifying an Oracle Database 10*g* installation).

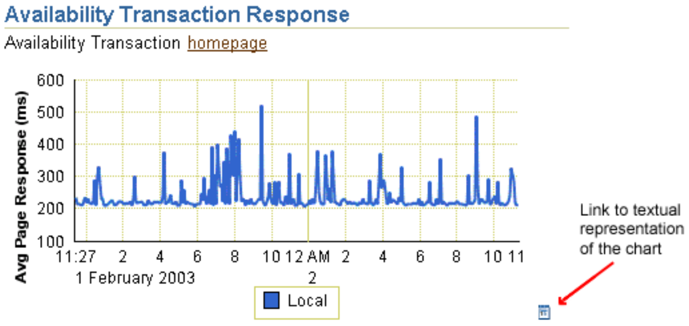
### 16.3.2 Providing Textual Descriptions of Enterprise Manager Charts

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.

Figure 16–5 shows an example of the icon that displays beneath Enterprise Manager charts when you have enabled the textual representation of charts.

***Figure 16–5 Icon Representing the Textual Representation of a Chart***


Availability Transaction Response
Availability Transaction homepage
Avg Page Response (ms)
600
500
400
300
200
100
11:27 2 4 6 8 10 12 AM 2 4 6 8 10 11
1 February 2003
2
Local
Link to textual representation of the chart

To enable the drill-down icon for the textual representation of charts:

1. Locate the `web.xml` configuration file.

   To locate the `web.xml` file in a Grid Control Console installation, change directory to the following location in the Management Service home:

   ```
   ORACLE_HOME/j2ee/OC4J_EM/applications/em/em/WEB-INF
   ```

   To locate the `web.xml` file in a Oracle Database 10*g* installation, change directory to the following location in the database home:

```
ORACLE_HOME/oc4j/j2ee/oc4j_applications/applications/em/em/WEB-INF
```

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 Management Service (if you are modifying a Grid Control Console installation) or restart the Database Console (if you are modifying an Oracle Database 10*g* installation).

# 17

# Grid Control Common Configurations

Oracle Enterprise Manager 10*g* Grid Control is based on a flexible architecture, which allows you to deploy the Grid Control components in the most efficient and practical manner for your organization. This chapter describes some common configurations that demonstrate how you can deploy the Grid Control architecture in various computing environments.

The common configurations are presented in a logical progression, starting with the simplest configuration and ending with a complex configuration that involves the deployment of high availability components, such as load balancers, Oracle Real Application Clusters, and Oracle Data Guard.

This chapter contains the following sections:

## 17.1 About Common Configurations

The common configurations described in this chapter are provided as examples only. The actual Grid Control configurations that you deploy in your own environment will vary depending upon the needs of your organization.

For instance, the examples in this chapter assume you are using the OracleAS Web Cache port to access the Grid Control console. By default, when you first install Grid Control, you display the Grid Control console by navigating to the default OracleAS Web Cache port. In fact, you can modify your own configuration so administrators bypass OracleAS Web Cache and use a port that connects them directly to the Oracle HTTP Server.

For another example, in a production environment you will likely want to implement firewalls and other security considerations. The common configurations described in this chapter are not meant to show how firewalls and security policies should be implemented in your environment.

**See Also:** Chapter 19, "Configuring Enterprise Manager for Firewalls" for information about configuring firewalls between Grid Control components

Besides providing a description of common configuration this chapter can also help you understand the architecture and flow of data among the Grid Control components. Based on this knowledge, you can make better decisions about how to configure Grid Control for your specific management requirements.

The Grid Control architecture consists of the following software components:

- Oracle Management Agent
- Oracle Management Service
- Oracle Management Repository
- Oracle Enterprise Manager 10*g* Grid Control Console

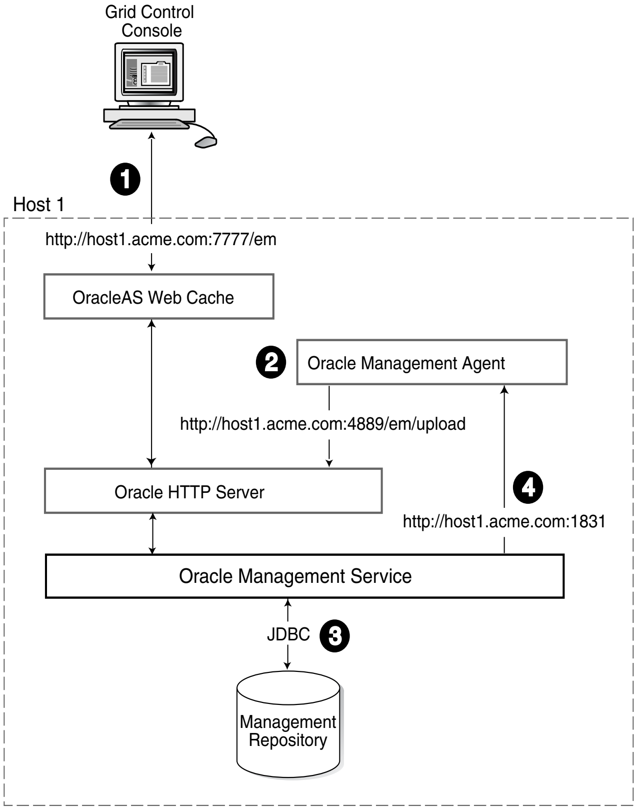
**See Also:** *Oracle Enterprise Manager Concepts* for more information about each of the Grid Control components

The remaining sections of this chapter describe how you can deploy these components in a variety of combinations and across a single host or multiple hosts.

## 17.2 Deploying Grid Control Components on a Single Host

Figure 17–1 shows how each of the Grid Control components are configured to interact when you install Grid Control on a single host. This is the default configuration that results when you use the Grid Control installation procedure to install the **Enterprise Manager 10g Grid Control Using a New Database** installation type.

*Figure 17–1 Grid Control Components Installed on a Single Host*


Grid Control Console
1
Host 1
http://host1.acme.com:7777/em
OracleAS Web Cache
2
Oracle Management Agent
http://host1.acme.com:4889/em/upload
Oracle HTTP Server
4
http://host1.acme.com:1831
Oracle Management Service
JDBC
3
Management Repository

When you install all the Grid Control components on a single host, the management data travels along the following paths:

1. Administrators use the Grid Control console to monitor and administer the managed targets that are discovered by the Management Agents on each host. The Grid Control console uses the default OracleAS Web Cache port (for example, port 7777 on UNIX systems and port 80 on Windows systems) to connect to the Oracle HTTP Server. The Management Service retrieves data from the Management Repository as it is requested by the administrator using the Grid Control console.

   **See Also:** *Oracle Application Server Web Cache Administrator's Guide* for more information about the benefits of using OracleAS Web Cache

2. The Management Agent loads its data (which includes management data about all the managed targets on the host, including the Management Service and the Management Repository database) by way of the Oracle HTTP Server upload URL. The Management Agent uploads data directly to Oracle HTTP Server and bypasses OracleAS Web Cache. The default port for the upload URL is 4889 (it if is available during the installation procedure). The upload URL is defined by the `REPOSITORY_URL` property in the following configuration file in the Management Agent home directory:

   ```
   AGENT_HOME/sysman/config/emd.properties (UNIX)
   AGENT_HOME\sysman\config\emd.properties (Windows)
   ```

   **See Also:** "Understanding the Enterprise Manager Directory Structure" on page 16-1 for more information about the AGENT_HOME directory

3. The Management Service uses JDBC connections to load data into the Management Repository database and to retrieve information from the Management Repository so it can be displayed in the Grid Control console. The Management Repository connection information is defined in the following configuration file in the Management Service home directory:

   ```
   ORACLE_HOME/sysman/config/emoms.properties (UNIX)
   ORACLE_HOME\sysman\config\emoms.properties (Windows)
   ```

   > **See Also:** "Reconfiguring the Oracle Management Service" on page 20-8 for more information on modifying the Management Repository connection information in the emoms.properties file

4. The Management Service sends data to the Management Agent by way of HTTP. The Management Agent software includes a built-in HTTP listener that listens on the Management Agent URL for messages from the Management Service. As a result, the Management Service can bypass the Oracle HTTP Server and communicate directly with the Management Agent. If the Management Agent is on a remote system, no Oracle HTTP Server is required on the Management Agent host.

   The Management Service uses the Management Agent URL to monitor the availability of the Management Agent, submit Enterprise Manager jobs, and other management functions.

   The Management Agent URL can be identified by the `EMD_URL` property in the following configuration file in the Management Agent home directory:

   ```
   AGENT_HOME/sysman/config/emd.properties (UNIX)
   AGENT_HOME\sysman\config\emd.properties (Windows)
   ```

   For example:

   ```
   EMD_URL=http://host1.acme.com:1831/emd/main/
   ```

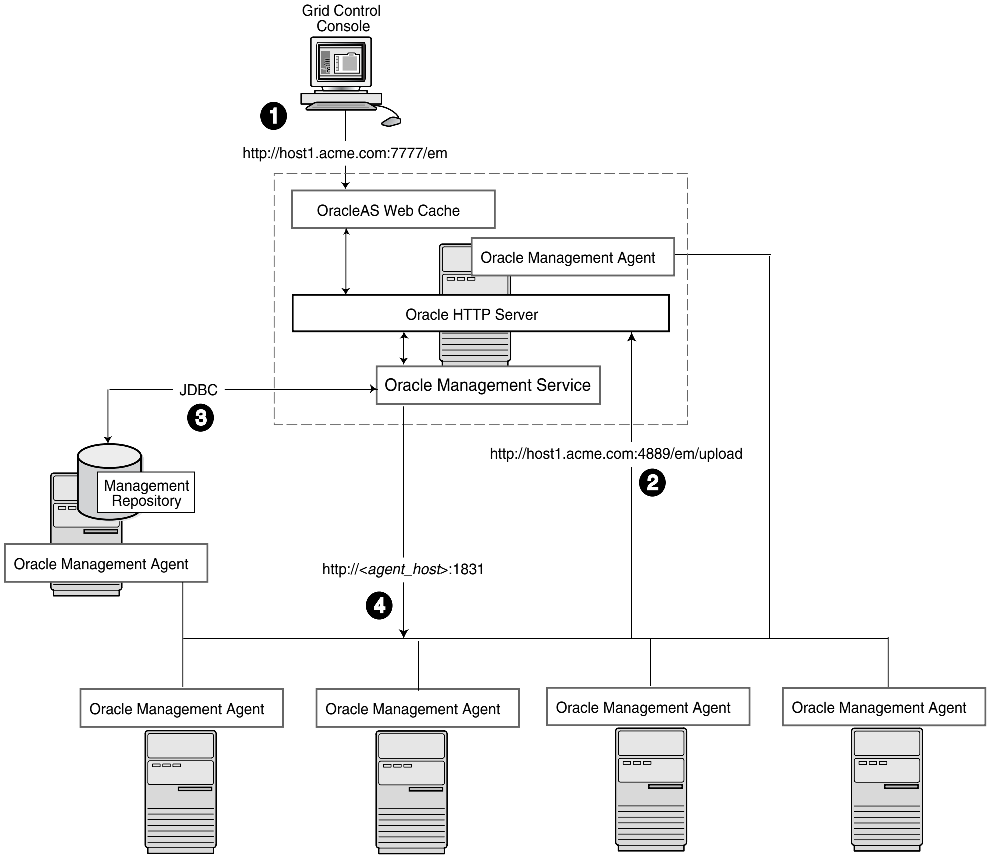
   In addition, the name of the Management Agent as it appears in the Grid Control console consists of the Management Agent host name and the port used by the Management Agent URL.

## 17.3 Managing Multiple Hosts and Deploying a Remote Management Repository

Installing all the Grid Control components on a single host is an effective way to initially explore the capabilities and features available to you when you centrally manage your Oracle environment.

A logical progression from the single-host environment is to a more distributed approach, where the Management Repository database is on a separate host and does not compete for resources with the Management Service. The benefit in such a configuration is scalability; the workload for the Management Repository and Management Service can now be split. This configuration also provides the flexibility to adjust the resources allocated to each tier, depending on the system load. (Such a configuration is shown in Figure 17–2.) See Section 17.4.2.1, "Monitoring the Load on Your Management Service Installations" for additional information.

***Figure 17–2 Grid Control Components Distributed on Multiple Hosts with One Management Service***



In this more distributed configuration, data about your managed targets travels along the following paths so it can be gathered, stored, and made available to administrators by way of the Grid Control console:

1. Administrators use the Grid Control console to monitor and administer the targets just as they do in the single-host scenario described in Section 17.2.

2. Management Agents are installed on each host on the network, including the Management Repository host and the Management Service host. The Management Agents upload their data to the Management Service by way of the Management Service upload URL, which is defined in the `emd.properties` file in each Management Agent home directory. The upload URL bypasses OracleAS Web Cache and uploads the data directly through the Oracle HTTP Server.

3. The Management Repository is installed on a separate machine that is dedicated to hosting the Management Repository database. The Management Service uses JDBC connections to load data into the Management Repository database and to retrieve information from the Management Repository so it can be displayed in the Grid Control console. This remote connection is defined in the `emoms.properties` configuration file in the Management Service home directory.

4. The Management Service communicates directly with each remote Management Agent over HTTP by way of the Management Agent URL. The Management Agent URL is defined by the `EMD_URL` property in the `emd.properties` file of each Management Agent home directory. As described in Section 17.2, the

Management Agent includes a built-in HTTP listener so no Oracle HTTP Server is required on the Management Agent host.

## 17.4 Using Multiple Management Service Installations

In larger production environments, you may find it necessary to add additional Management Service installations to help reduce the load on the Management Service and improve the efficiency of the data flow.

**Note:** When you add additional Management Service installations to your Grid Control configuration, be sure to adjust the parameters of your Management Repository database. For example, you will likely need to increase the number of processes allowed to connect to the database at one time. Although the number of required processes will vary depending on the overall environment and the specific load on the database, as a general guideline, you should increase the number of processes by 40 for each additional Management Service.

For more information, see the description of the PROCESSES initialization parameter in the *Oracle Database Reference*.

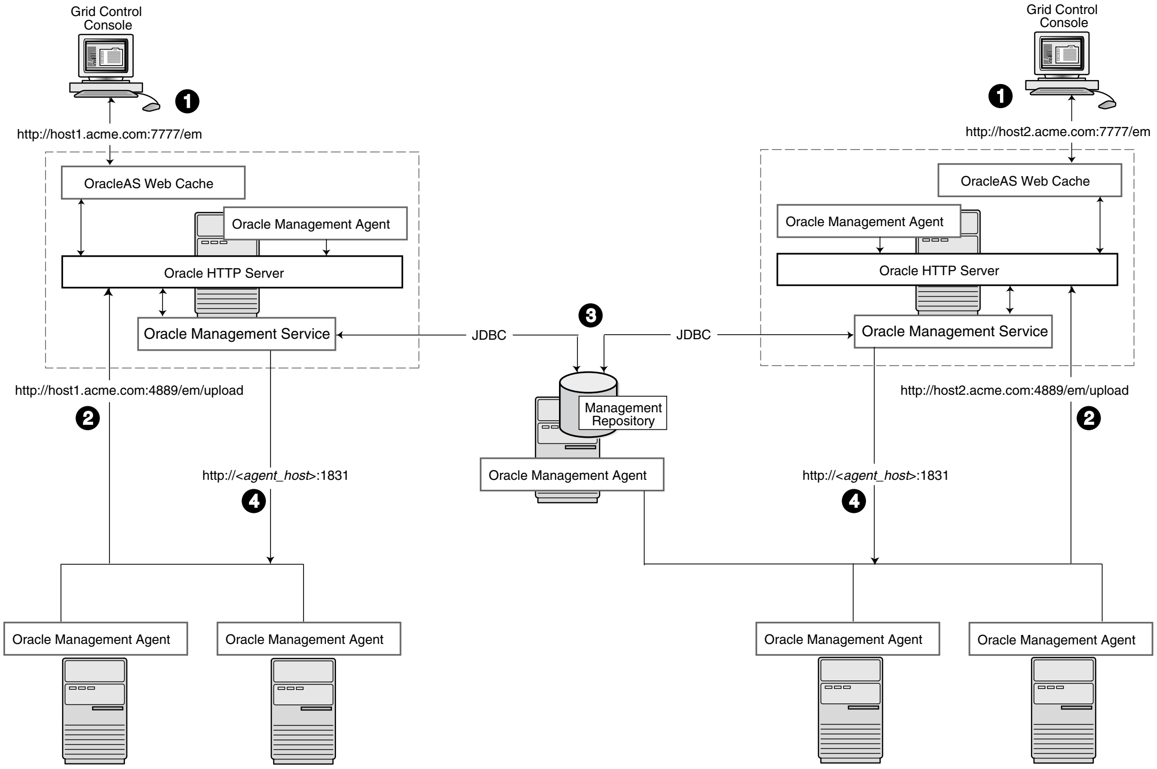
The following sections provide more information about this configuration:

- Understanding the Flow of Management Data When Using Multiple Management Services
- Determining When to Use Multiple Management Service Installations

### 17.4.1 Understanding the Flow of Management Data When Using Multiple Management Services

Figure 17–3 shows a typical environment where an additional Management Service has been added to improve the scalability of the Grid Control environment.

***Figure 17–3 Grid Control Architecture with Multiple Management Service Installations***



In a multiple Management Service configuration, the management data moves along the following paths:

1. Administrators can use one of two URLs to access the Grid Control console. Each URL refers to a different Management Service installation, but displays the same set of targets, all of which are loaded in the common Management Repository. Depending upon the host name and port in the URL, the Grid Control console obtains data from the Management Service (by way of OracleAS Web Cache and the Oracle HTTP Server) on one of the Management Service hosts.

2. Each Management Agent uploads its data to a specific Management Service, based on the upload URL in its `emd.properties` file. That data is uploaded directly to the Management Service by way of Oracle HTTP Server, bypassing OracleAS Web Cache.

   Whenever more than one Management Service is installed, it is a best practice to have the Management Service upload to a shared directory. This allows all Management Service processes to manage files that have been downloaded from any Management Agent. This protects from the loss of any one Management Server causing a disruption in upload data from Management Agents.

   Configure this functionality from the command line of each Management Service process as follows:

   ```
   emctl config oms loader -shared <yes|no> -dir <load
   directory>
   ```

**Important:** By adding a load balancer, you can avoid the following problems:

- Should the Management Service fail, any Management Agent connected to it cannot upload data.
- Because user accounts only know about one Management Service, users lose connectivity should the Management Service go down even if the other Management Service is up.

See Section 17.5, "High Availability Configurations - Maximum Availability Architecture" for information regarding load balancers.

**Note:** If deployment procedures are being used in this environment, they should be configured to use shared storage in the same way as the shared Management Service loader. To modify the location for the deployment procedure library:

1. Click the **Deployments** tab on the Enterprise Manager Home page.
2. Click the **Provisioning** subtab.
3. On the Provisioning page, click the **Administration** subtab.
4. In the Software Library Configuration section, click **Add** to set the Software Library Directory Location to a shared storage that can be accessed by any host running the Management Service.

3. Each Management Service communicates by way of JDBC with a common Management Repository, which is installed in a database on a dedicated Management Repository host. Each Management Service uses the same database connection information, defined in the `emoms.properties` file, to load data from its Management Agents into the Management Repository. The Management Service uses the same connection information to pull data from the Management Repository as it is requested by the Grid Control console.

4. Any Management Service in the system can communicate directly with any of the remote Management Agents defined in the common Management Repository. The Management Services communicate with the Management Agents over HTTP by way of the unique Management Agent URL assigned to each Management Agent.

   As described in Section 17.2, the Management Agent URL is defined by the `EMD_URL` property in the `emd.properties` file of each Management Agent home directory. Each Management Agent includes a built-in HTTP listener so no Oracle HTTP Server is required on the Management Agent host.

### 17.4.2 Determining When to Use Multiple Management Service Installations

Management Services not only exist as the receivers of upload information from Management Agents. They also retrieve data from the Management Repository. The Management Service renders this data in the form of HTML pages, which are requested by and displayed in the client Web browser. In addition, the Management Services perform background processing tasks, such as notification delivery and the dispatch of Enterprise Manager jobs.

As a result, the assignment of Management Agents to Management Services must be carefully managed. Improper distribution of load from Management Agents to Management Services may result in perceived:

- Sluggish user interface response
- Delays in delivering notification messages
- Backlog in monitoring information being uploaded to the Management Repository
- Delays in dispatching jobs

The following sections provide some tips for monitoring the load and response time of your Management Service installations:

- Monitoring the Load on Your Management Service Installations
- Monitoring the Response Time of the Enterprise Manager Web Application Target

#### 17.4.2.1 Monitoring the Load on Your Management Service Installations

If your environment is not configured with an SLB, to keep the workload evenly distributed you should always be aware of how many Management Agents are configured per Management Service and monitor the load on each Management Service.

At any time, you can view a list of Management Agents and Management Services using Setup on the Grid Control console.

Use the charts on the Overview page of Management Services and Repository to monitor:

- Loader backlog (files)

  The Loader is part of the Management Service that pushes metric data into the Management Repository at periodic intervals. If the Loader Backlog chart indicates that the backlog is high and Loader output is low, there is data pending load, which may indicate a system bottleneck or the need for another Management Service. The chart shows the total backlog of files totaled over all Oracle Management Services for the past 24 hours. Click the image to display loader backlog charts for each individual Management Service over the past 24 hours.

- Notification delivery backlog

  The Notification Delivery Backlog chart displays the number of notifications to be delivered that could not be processed in the time allocated. Notifications are delivered by the Management Services. This number is summed across all Management Services and is sampled every 10 minutes. The graph displays the data for the last 24 hours. It is useful for determining a growing backlog of notifications. When this graph shows constant growth over the past 24 hours, then consider adding another Management Service, reducing the number of notification rules, and verifying that all rules and notification methods are useful and valid.

#### 17.4.2.2 Monitoring the Response Time of the Enterprise Manager Web Application Target

The information on the Management Services and Repository page can help you determine the load being placed on your Management Service installations. More importantly, consider how the performance of your Management Service installations is affecting the performance of the Grid Control console.

Use the `EM Website` Web Application target to review the response time of the Grid Control console pages:

1. From the Grid Control console, click the **Targets** tab and then click the **Web Applications** subtab.

2. Click **EM Website** in the list of Web Application targets.
3. In the Key Test Summary table, click **homepage**. The resulting page provides the response time of the Grid Control console homepage URL.

   **See Also:** The Enterprise Manager online help for more information about using the homepage URL and Application Performance Management (also known as Application Performance Monitoring) to determine the performance of your Web Applications

4. Click **Page Performance** to view the response time of some selected Grid Control console pages.

   **Note:** The Page Performance page provides data generated only by users who access the Grid Control console by way of the OracleAS Web Cache port (usually, 7777).

5. Select **7 Days** or **31 Days** from the **View Data** menu to determine whether or not there are any trends in the performance of your Grid Control installation.

   Consider adding additional Management Service installations if the response time of all pages is increasing over time or if the response time is unusually high for specific popular pages within the Grid Control console.

   **Note:** You can use Application Performance Management and Web Application targets to monitor your own Web applications.

## 17.5 High Availability Configurations - Maximum Availability Architecture

Highly Available systems are critical to the success of virtually every business today. It is equally important that the management infrastructure monitoring these mission-critical systems are highly available. The Enterprise Manager Grid Control architecture is engineered to be scalable and available from the ground up. It is designed to ensure that you concentrate on managing the assets that support your business, while it takes care of meeting your business Service Level Agreements.

When you configure Grid Control for high availability, your aim is to protect each component of the system, as well as the flow of management data in case of performance or availability problems, such as a failure of a host or a Management Service.

Maximum Availability Architecture (MAA) provides a highly available Enterprise Manager implementation by guarding against failure at each component of Enterprise Manager.

The impacts of failure of the different Enterprise Manager components are:

- Management Agent failure or failure in the communication between Management Agents and Management Services

  Results in targets no longer monitored by Enterprise Manager, though the Enterprise Manager console is still available and one can view historical data from the Management Repository.

- Management Service failure

Results in the unavailability of Enterprise Manager console, as well as unavailability of almost all Enterprise Manager services.

- Management Repository failure

  Results in failure on the part of Enterprise Manager to save the uploaded data by the Management Agents as well as unavailability of almost all Enterprise Manager services.

Overall, failure in any component of Enterprise Manager can result in substantial service disruption. Therefore it is essential that each component be hardened using a highly available architecture.

You can configure Enterprise Manager to run in either active-active or active-passive mode using a single instance database as the Management Repository. The following text summarizes the active-active mode.

Refer to the following sections for more information about common Grid Control configurations that take advantage of high availability hardware and software solutions. These configurations are part of the Maximum Availability Architecture (MAA).

- Configuring the Management Repository
- Configuring the Management Services
- Installing Additional Management Services
- Configuring a Load Balancer
- Configuring the Management Agent
- Disaster Recovery

## 17.5.1 Configuring the Management Repository

Before installing Enterprise Manager, you should prepare the database, which will be used for setting up Management Repository. Install the database using Database Configuration Assistant (DBCA) to make sure that you inherit all Oracle install best practices.

- Configure Database
  - For both high availability and scalability, you should configure the Management Repository in the latest certified database version, with the RAC option enabled. Check for the latest version of database certified for Enterprise Manager from the Certify tab on the My Oracle Support website.
  - Choose Automatic Storage Management (ASM) as the underlying storage technology.
  - When the database installation is complete:

    Go to $ORACLE_HOME/rbdms/admin directory of the database home and execute the 'dbmspool.sql'

    This installs the DBMS_SHARED_POOL package, which will help in improving throughput of the Management Repository.
- Install Enterprise Manager

  While installing Enterprise Manager using Oracle Universal Installer (OUI), you will be presented with two options for configuring the Management Repository:
  - Option 1: Install using a new database (default install)

- Option 2: Install using an existing database.

For MAA, you should chose 'Option 2: Install using an existing database'. When prompted for the 'existing database', you can point to the database configured in the previous step to setup the Management Repository.

#### 17.5.1.1 Post Management Service - Install Management Repository Configuration

There are some parameters that should be configured during the Management Repository database install (as previously mentioned) and some parameters that should be set after the Management Service has been installed. Once the Enterprise Manager console is available, it can be used to configure these best practices in the Management Repository. These best practices fall in the area of:

- Configuring Storage
- Configuring Oracle Database 10*g* with RAC for High Availability and Fast Recover Ability
  - Enable ARCHIVELOG Mode
  - Enable Block Checksums
  - Configure the Size of Redo Log Files and Groups Appropriately
  - Use a Flash Recovery Area
  - Enable Flashback Database
  - Use Fast-Start Fault Recovery to Control Instance Recovery Time
  - Enable Database Block Checking
  - Set DISK_ASYNCH_IO

  The details of these settings are available in the *Oracle Database High Availability Best Practices*.

  Use the MAA Advisor for additional high availability recommendations that should be applied to the Management Repository. To access the MAA Advisor:

  1. On the Database Target Home page, locate the High Availability section.
  2. Click **Details** next to the Console item.
  3. In the Availability Summary section of the High Availability Console page, click **Details** next to the MAA Advisor item.

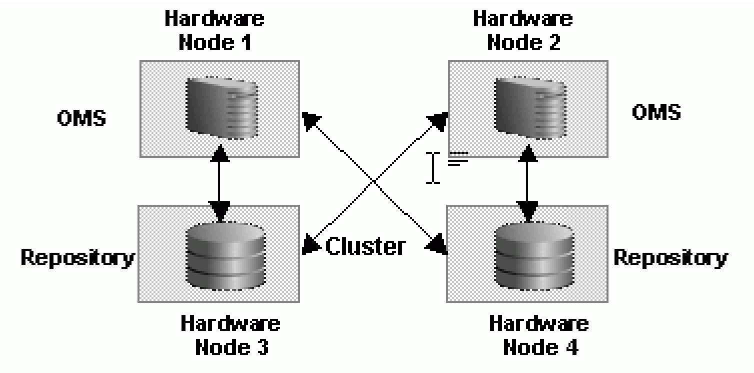
### 17.5.2 Configuring the Management Services

Once you configure the Management Repository, the next step is to install and configure the Enterprise Manager Grid Control mid-tier, the Management Services, for greater availability. Before discussing steps that add mid-tier redundancy and scalability, note that the Management Service itself has a built in restart mechanism based on the Oracle Process Management and Notification Service (OPMN). This service will attempt to restart a Management Service that is down.

#### 17.5.2.1 Management Service Install Location

If you are managing a large environment with multiple Management Services and Management Repository nodes, then consider installing the Management Services on hardware nodes that are different from Management Repository nodes (Figure 17–4). This allows you to scale out the Management Services in the future.

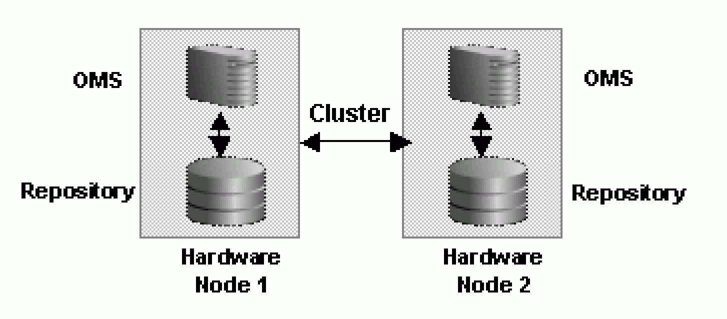
*Figure 17–4 Management Service and Management Repository on Separate Hardware*



Also consider the network latency between the Management Service and the Management Repository while determining the Management Service install location. The distance between the Management Service and the Management Repository may be one of the factors that effect network latency and hence determine Enterprise Manager performance.

If the network latency between the Management Service and Management Repository tiers is high or the hardware available for running Enterprise Manager is limited, then the Management Service can be installed on the same hardware as the Management Repository (Figure 17–5). This allows for Enterprise Manager high availability, as well as keep the costs down.

*Figure 17–5 Management Service and Management Repository on Same Hardware*



**Note:** Starting with Enterprise Manager 10g release 10.2.0.2, you can install the Management Service onto the same nodes as the RAC Management Repository. Refer to the instructions specified in the README for doing the same.

### 17.5.2.2 Configure Management Service to Management Repository Communication

Once all the Management Service processes have been installed, they need to be configured to communicate with each node of the RAC Management Repository in a redundant fashion. To accomplish this, modify the field 'emdRepConnectDescriptor' in the file $ORACLE_HOME/sysman/config/emoms.properities for each installed Management Service. The purpose of this configuration is to make the Management

Service aware of all instances in the database cluster that are able to provide access to the Management Repository through the database service 'EMREP'.

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

```
oracle.sysman.eml.mntr.emdRepConnectDescriptor=(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)))
```

After making the previous change, run the following command to make the same change to the monitoring configuration used for the Management Services and Repository target: `emctl config emrep -conn_desc "<tns alias>"`

#### 17.5.2.3 Configure Management Service to Direct Traffic Through SLB

Finally, modify the Management Service to take advantage of the capabilities of the Server Load Balancer. These modifications will cause all the Management Service nodes to redirect Enterprise Manager console traffic through the server load balancer, thereby presenting a single URL to the Enterprise Manager user.

To prevent the browser from bypassing the load balancer when a URL is redirected, Grid Control will now reconfigure the `ssl.conf` file as a part of resecuring the Management Service. After the Load Balancer is configured, issue the following command from the Management Server home: `emctl secure oms`

Modify the 'Port' in the Oracle HTTP Server configuration file at $ORACLE_HOME/Apache/Apache/conf/ssl.conf to be '443'. This assumes you are running in the default secured configuration between the Management Service and Management Agent.

### 17.5.3 Installing Additional Management Services

Install at least one additional Management Service using the Oracle Universal Installer (OUI) option 'Add Additional Management Service'.   While you need two Management Services at the minimum for High Availability, additional Management Service processes can be installed depending on anticipated workload or based on system usage data.

Now that the first Management Service has been setup for high availability, the configuration can be copied over to additional Management Services easily using new emctl commands. Note the following considerations before installing additional Management Services.

- The additional Management Service should be hosted in close network proximity to the Management Repository database for network latency reasons.
- Configure the directory used for the shared filesystem loader to be available on the additional Management Service host using the same path as the first Management Service. Refer to Section 17.5.3.1, "Configuring Shared File Areas for Management Services" for additional information.
- Additional Management Services should be installed using the same OS user and group as the first Management Service. Proper user equivalence should be setup so that files created by the first Management Service on the shared loader

directory can be accessed and modified by the additional Management Service process.

- Adjust the parameters of your Management Repository database. For example, you will likely need to increase the number of processes allowed to connect to the database at one time. Although the number of required processes will vary depending on the overall environment and the specific load on the database, as a general guideline, you should increase the number of processes by 40 for each additional Management Service.
- For the install to succeed, the emkey might need to be copied temporarily to the Management Repository on the first Management Service using `emctl config emkey -copy_to_repos` if it had been removed earlier from Management Repository as per security best practices.

Install the Management Service software using steps documented in the *Oracle Enterprise Manager Grid Control Installation and Basic Configuration Guide*. Refer to the Installing Software-Only and Configuring Later - Additional Management Service option. Update the software to the latest patchset to match the first Management Service. Note that the emctl commands to copy over the configuration from the first Management Service do not copy over any software binaries. Once you have the additional Management Service installed, use the following steps to copy over the configuration from the first Management Service.

1. Export the configuration from the first Management Service using `emctl exportconfig oms -dir <location for the export file>`
2. Copy over the exported file to the additional Management Service
3. Shutdown the additional Management Service
4. Import the exported configuration on the additional Management Service using `emctl importconfig oms -file <full path of the export file>`
5. Restart the additional Management Service
6. Setup EMCLI using `emcli setup -url=https://slb.example.com/em -username sysman -password <sysman password> -nocertvalidate`
7. Resecure the Management Agent that is installed with the additional Management Service to upload to SLB using `emctl secure agent -emdWalletSrcUrl https://slb.example.com:<upload port>/em`
8. Update the SLB configuration by adding the additional Management Service to the different pools on the SLB. Setup monitors for the new Management Service. Modify the ssl.conf file to set the Port directive to the SLB virtual port used for UI access.

#### 17.5.3.1 Configuring Shared File Areas for Management Services

The Management Service for Grid Control 10*g* Release 2 has a high availability feature called the Shared Filesystem Loader. In the Shared Filesystem Loader, management data files received from Management Agents are stored temporarily on a common shared location called the shared receive directory. All Management Services are configured to use the same storage location for the shared receive directory. The Management Services coordinate internally and distribute amongst themselves the workload of uploading files into the Management Repository. Should a Management Service go down, its workload is taken up by surviving Management Services.

1. Allow all Management Services to process the Management Agent data and take better advantage of available resources.

2. The ability of another Management Service to process Management Agent data in the event of a failure of a Management Service.

   To configure the Management Service to use Shared File system Loader, you must run the following steps:

   a. Stop all Oracle Management Services.

   b. Configure a shared receive directory that is accessible by all Management Services using redundant file system storage.

   c. Execute:

      `emctl config oms loader -shared yes -dir <loaderdirectory>` individually on all Management Service hosts, where `<loaderdirectory>` is the full path to the shared receive directory created.

   > **Note:** Enterprise Manager will fail to start if all the Management Services are not configured to point to the same shared directory. This shared directory should be on redundant storage.

   > **Note:** To modify the location for the deployment procedure library using the Enterprise Manager UI:
   >
   > 1. Click the **Deployments** tab on the Enterprise Manager Home page.
   > 2. Click the **Provisioning** subtab.
   > 3. On the Provisioning page, click the **Administration** subtab.
   > 4. In the Software Library Configuration section, click **Add** to set the Software Library Directory Location to a shared storage that can be accessed by any host running the Management Service.

3. Configure Software Library

   Since software library location has to be accessed by all Management Services, considerations similar to shared filesystem loader directory apply here too.

### 17.5.4 Configuring a Load Balancer

This section describes guidelines you can use for configuring a load balancer to balance the upload of data from Management Agents to multiple Management Service installations.

In the following examples, assume that you have installed two Management Service processes on Host A and Host B. For ease of installation, start with two hosts that have no application server processes installed. This ensures that the default ports are used as seen in the following table. The examples use these default values for illustration purposes.

*Table 17–1 Management Service Ports*

| Name | Default Value | Description | Source | Defined By |
|---|---|---|---|---|
| Secure Upload Port | 1159 | Used for secure upload of management data from Management Agents. | httpd_em.conf and emoms.properties | Install. Can be modified by `emctl secure OMS - secure port <port>` command. |
| Agent Registration Port | 4889 | Used by Management Agents during the registration phase to download Management Agent wallets, for example, during `emctl secure agent`. In an unlocked Management Service, it can be used for uploading management data to the Management Service. | httpd_em.conf and emoms.properties | Install |
| Secure Console Port | 4444 | Used for secure (https) console access. | ssl.conf | Install |
| Unsecure Console Port | 7777 | Used for unsecure (http) console access. | httpd.conf | Install |
| Webcache Secure Port | 4443 | Used for secure (https) console access. | webcache.xml | Install |
| Webcache Unsecure Port | 7779 | Used for unsecure (http) console access. | webcache.xml | Install |

By default, the service name on the Management Service-side certificate uses the name of the Management Service host. Management Agents do not accept this certificate when they communicate with the Management Service through a load balancer. You must run the following command to regenerate the certificate on both Management Services:

```
emctl secure -oms -sysman_pwd <sysman_pwd> -reg_pwd <agent_reg_
password> -host slb.acme.com -secure_port 1159 -slb_console_port
443
```

Specifically, you should use the administration tools that are packaged with your load balancer to configure a virtual pool that consists of the hosts and the services that each host provides. To insure a highly available Management Service, you should have two or more Management Services defined within the virtual pool. A sample configuration follows.

### Sample Configuration

In this sample, both pools and virtual servers are created.

1. Create Pools

   **Pool abc_upload**: Used for secure upload of management data from Management Agents to Management Services
   Members: hostA:1159, hostB:1159
   Persistence: None
   Load Balancing: round robin
   **Pool abc_genWallet**: Used for securing new Management Agents
   Members: hostA:4889, host B:4889
   Persistence: Active HTTP Cookie, method-> insert, expiration 60 minutes
   Load balancing: round robin
   **Pool abc_uiAccess**: Used for secure console access
   Members: hostA:4444, hostB:4444

Persistence: Simple (also known as Client IP based persistence), timeout-> 3000 seconds (should be greater than the OC4J session timeout of 45 minutes)
Load balancing: round robin

2. Create Virtual Servers

   **Virtual Server for secure upload**
   Address: slb.acme.com
   Service: 1159
   Pool: abc_upload
   **Virtual Server for Management Agent registration**
   Address: slb.acme.com
   Service: 4889
   Pool: abc_genWallet
   **Virtual Server for UI access**
   Address: sslb.acme.com
   Service: https i.e. 443
   Pool: abc_uiAccess

Modify the REPOSITORY_URL property in the `emd.properties` file located in the `sysman/config` directory of the Management Agent home directory. The host name and port specified must be that of the load balancer virtual service.

> **See Also:** "Configuring the Management Agent to Use a New Management Service" on page 20-1 for more information about modifying the REPOSITORY_URL property for a Management Agent

This configuration allows the distribution of connections from Management Agents equally between Management Services. In the event a Management Service becomes unavailable, the load balancer should be configured to direct connections to the surviving Management Services.

### Detecting Unavailable Management Services

To successfully implement this configuration, the load balancer can be configured to monitor the underlying Management Service. On some models, for example, you can configure a *monitor* on the load balancer. The monitor defines the:

- HTTP request that is to be sent to a Management Service
- Expected result in the event of success
- Frequency of evaluation

For example, the load balancer can be configured to check the state of the Management Service every 5 seconds. On three successive failures, the load balancer can then mark the component as unavailable and no longer route requests to it. The monitor should be configured to send the string `GET /em/upload` over HTTP and expect to get the response `Http XML File receiver`. See the following sample monitor configuration.

### Sample Monitor Configuration

In this sample, three monitors are configured: mon_upload, mon_genWallet, and mon_uiAccess.

**Monitor mon_upload**
Type: https
Interval: 60
Timeout: 181
Send String: GET /em/upload HTTP/1.0\n

Receive Rule: Http Receiver Servlet active!
Associate with: hostA:1159, hostB:1159

**Monitor mon_genWallet**
Type: http
Interval: 60
Timeout: 181
Send String: GET /em/genwallet HTTP/1.0\n
Receive Rule: GenWallet Servlet activated
Associate with: hostA:4889, hostB:4889

**Monitor mon_uiAccess**
Type: https
Interval: 5
Timeout: 16
Send String: GET /em/console/home HTTP/1.0\nUser-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)\n
Receive Rule: /em/console/logon/logon;jsessionid=
Associate with: hostA:4444, hostB:4444

> **Note:** The network bandwidth requirements on the Load Balancer need to be reviewed carefully. Monitor the traffic being handled by the load balancer using the administrative tools packaged with your load balancer. Ensure that the load balancer is capable of handling the traffic passing through it. For example, deployments with a large number of targets can easily exhaust a 100 Mbps Ethernet card. A Gigabit Ethernet card would be required in such cases.

> **See Also:** Your Load Balancer documentation for more information on configuring virtual pools, load balancing policies, and monitoring network traffic

#### 17.5.4.1 Configuring Oracle HTTP Server When Using a Load Balancer for the Grid Control Console

The Management Service is implemented as a J2EE Web application, which is deployed on an instance of Oracle Application Server. Like many Web-based applications, the Management Service often redirects the client browser to a specific set of HTML pages, such as a logon screen and a specific application component or feature.

When the Oracle HTTP Server redirects a URL, it sends the URL, including the Oracle HTTP Server host name, back to the client browser. The browser then uses that URL, which includes the Oracle HTTP Server host name, to reconnect to the Oracle HTTP Server. As a result, the client browser attempts to connect directly to the Management Service host and bypasses the load balancer.

To prevent the browser from bypassing the load balancer when a URL is redirected, Grid Control will now reconfigure the `ssl.conf` file as a part of resecuring the Management Service. After the Load Balancer is configured, issue the following command from the Management Server home: `emctl secure oms`

> **See Also:** *Oracle HTTP Server Administrator's Guide*

#### 17.5.4.2 Configuring Console URL

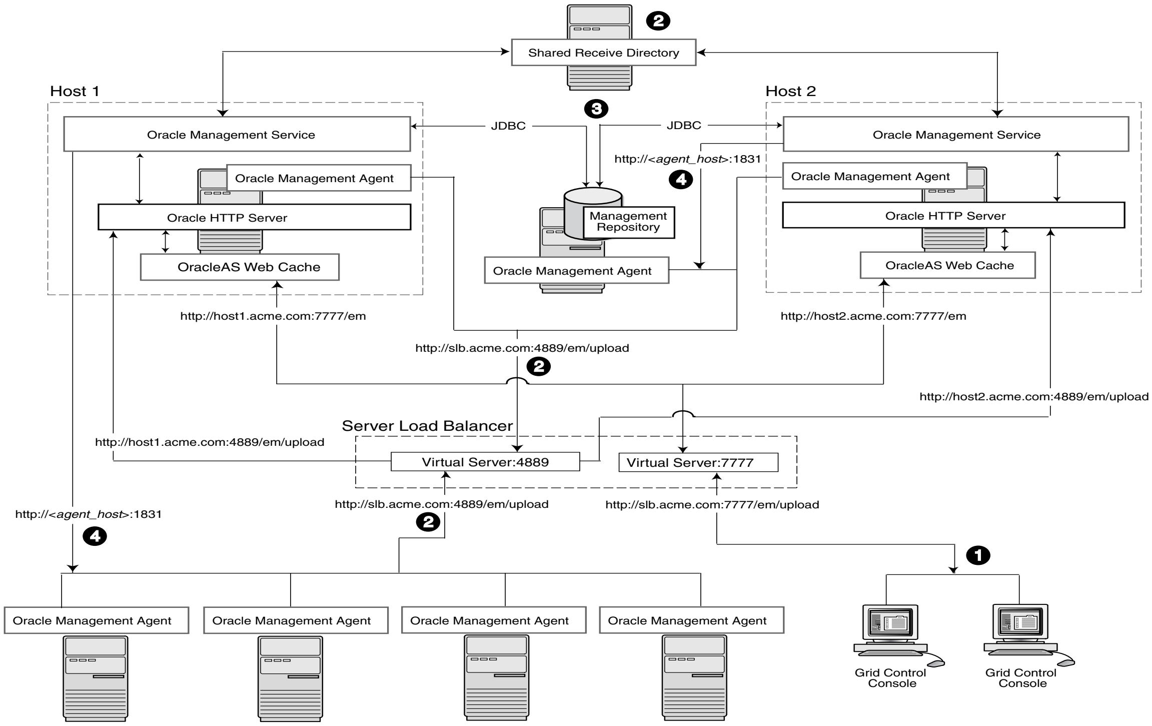
Grid Control sends out notifications and reports using e-mail with links pointing back to the Grid Control Console. When a SLB is configured, the e-mails should contain links pointing the SLB and not the individual Management Service. Go to the Management Services and Repository page on Grid Control Console. Click **Add Console URL** and specify the SLB virtual service used for UI access.

#### 17.5.4.3 Understanding the Flow of Data When Load Balancing the Grid Control Console

Using a load balancer to manage the flow of data from the Management Agents is not the only way in which a load balancer can help you configure a highly available Grid Control environment. You can also use a load balancer to balance the load and to provide a failover solution for the Grid Control console

Figure 17–6 shows a typical configuration where a load balancer is used between the Management Agents and multiple Management Services, as well as between the Grid Control console and multiple Management Services.

*Figure 17–6 Load Balancing Between the Grid Control Console and the Management Service*



In this example, a single load balancer is used for the upload of data from the Management Agents and for the connections between the Grid Control console and the Management Service.

When you use a load balancer for the Grid Control console, the management data uses the following paths through the Grid Control architecture:

1. Administrators use one URL to access the Grid Control console. This URL directs the browser to the load balancer virtual service. The virtual service redirects the browser to one of the Management Service installations. Depending upon the host name and port selected by the load balancer from the virtual pool of Management Service installations, the Grid Control console obtains the management data by

way of OracleAS Web Cache and the Oracle HTTP Server on one of the Management Service hosts.

2. Each Management Agent uploads its data to a common load balancer URL (as described in Section 17.5.5.1) and data is written to the shared receive directory.
3. Each Management Service communicates by way of JDBC with a common Management Repository, just as they do in the multiple Management Service configuration defined in Section 17.4.
4. Each Management Service communicates directly with each Management Agent by way of HTTP, just as they do in the multiple Management Service configuration defined in Section 17.

### 17.5.5 Configuring the Management Agent

The final piece of Enterprise Manager High Availability is the Management Agent configuration. Before we jump into the Management Agent configuration, it is worthwhile to note that the Management Agent has high availability built into it out of the box. A 'watchdog' process, created automatically on Management Agent startup, monitors each Management Agent process. In the event of a failure of the Management Agent process, the 'watchdog' will try to automatically re-start the Management Agent process.

Communication between the Management Agent and the Management Service tiers in a default Enterprise Manager Grid Control install is a point-to-point set up. Therefore, the default configuration does not protect from the scenario where the Management Service becomes unavailable. In that scenario, a Management Agent will not be able to upload monitoring information to the Management Service (and to the Management Repository), resulting in the targets becoming unmonitored until that Management Agent is manually configured to point to a second Management Service.

To avoid this situation, use hardware Server Load Balancer (SLB) between the Management Agents and the Management Services. The Load Balancer monitors the health and status of each Management Service and makes sure that the connections made through it are directed to surviving Management Service nodes in the event of any type of failure. As an additional benefit of using SLB, the load balancer can also be configured to manage user communications to Enterprise Manager. The Load Balancer handles this through the creation of 'pools' of available resources.

- Configure the Management Agent to Communicate Through SLB

  The load balancer provides a virtual IP address that all Management Agents can use. Once the load balancer is setup, the Management Agents need to be configured to route their traffic to the Management Service through the SLB. This can be achieved through a couple of property file changes on the Management Agents.

  Resecure all Management Agents - Management Agents that were installed prior to SLB setup would be uploading directly to the Management Service. These Management Agents will not be able to upload after SLB is setup. Resecure these Management Agents to upload to the SLB by running the following command on each Management Agent. This command is available for Management Agents available for Enterprise Manager release 10.2.0.5. Prior to this release, you must manually edit the emd.properties file and use the `secure agent` command to secure the Management Agent.

  ```
  emctl secure agent -emdWalletSrcUrl
  https://slb.example.com:<upload port>/em
  ```

- Configure the Management Agent to Allow Retrofitting a SLB

  Some installations may not have access to a SLB during their initial install, but may foresee the need to add one later. If that is the case, consider configuring the Virtual IP address that will be used for the SLB as apart of the initial installation and having that IP address point to an existing Management Service. Secure communications between Management Agents and Management Services are based on the host name. If a new host name is introduced later, each Management Agent will not have to be re-secured as it is configured to point to the new Virtual IP maintained by the SLB.

#### 17.5.5.1 Load Balancing Connections Between the Management Agent and the Management Service

Before you implement a plan to protect the flow of management data from the Management Agents to the Management Service, you should be aware of some key concepts.

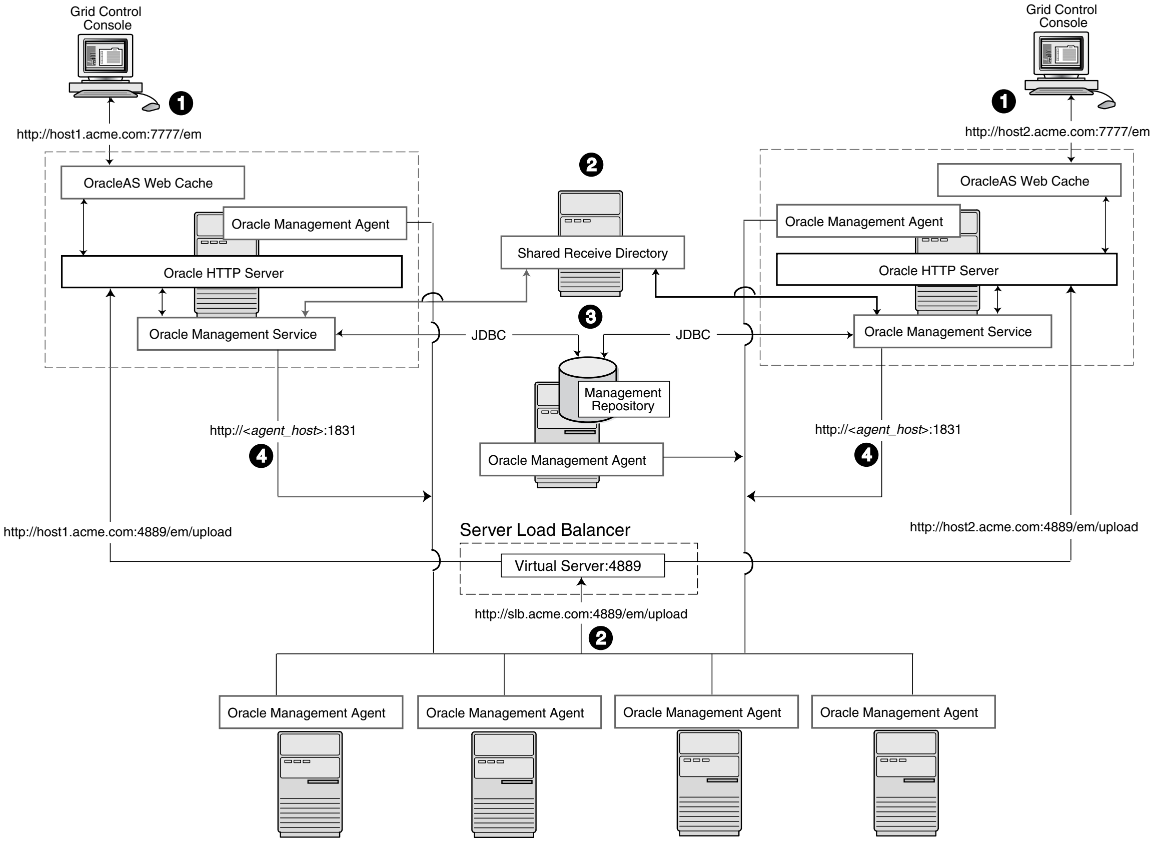
Specifically, Management Agents do not maintain a persistent connection to the Management Service. When a Management Agent needs to upload collected monitoring data or an urgent target state change, the Management Agent establishes a connection to the Management Service. If the connection is not possible, such as in the case of a network failure or a host failure, the Management Agent retains the data and reattempts to send the information later.

To protect against the situation where a Management Service is unavailable, you can use a load balancer between the Management Agents and the Management Services.

However, if you decide to implement such a configuration, be sure to understand the flow of data when load balancing the upload of management data.

Figure 17–7 shows a typical scenario where a set of Management Agents upload their data to a load balancer, which redirects the data to one of two Management Service installations.

***Figure 17–7 Load Balancing Between the Management Agent and the Management Service***



In this example, only the upload of Management Agent data is routed through the load balancer. The Grid Control console still connects directly to a single Management Service by way of the unique Management Service upload URL. This abstraction allows Grid Control to present a consistent URL to both Management Agents and Grid Control consoles, regardless of the loss of any one Management Service component.

When you load balance the upload of Management Agent data to multiple Management Service installations, the data is directed along the following paths:

1. Each Management Agent uploads its data to a common load balancer URL. This URL is defined in the `emd.properties` file for each Management Agent. In other words, the Management Agents connect to a virtual service exposed by the load balancer. The load balancer routes the request to any one of a number of available servers that provide the requested service.

2. Each Management Service, upon receipt of data, stores it temporarily in a local file and acknowledges receipt to the Management Agent. The Management Services then coordinate amongst themselves and one of them loads the data in a background thread in the correct chronological order.

   Also, each Management Service communicates by way of JDBC with a common Management Repository, just as they do in the multiple Management Service configuration defined in Section 17.4.

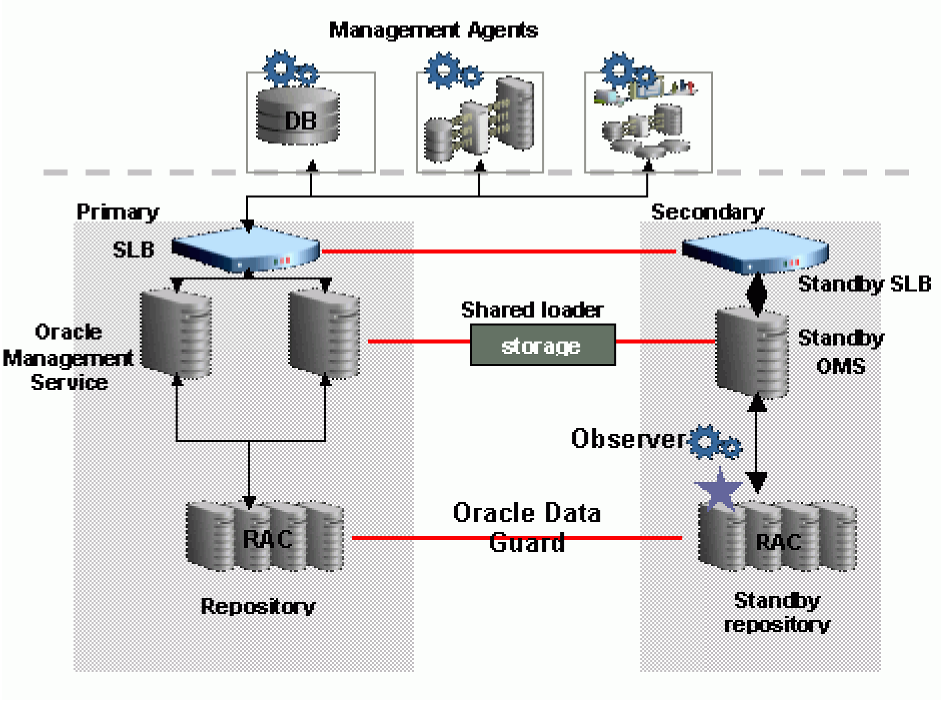
3. Each Management Service communicates directly with each Management Agent by way of HTTP, just as they do in the multiple Management Service configuration defined in Section 17.4.

### 17.5.6 Disaster Recovery

While high availability typically protects against local outages such as application failures or system-level problems, disaster tolerance protects against larger outages such as catastrophic data-center failure due to natural disasters, fire, electrical failure, evacuation, or pervasive sabotage. For Maximum Availability, the loss of a site cannot be the cause for outage of the management tool that handles your enterprise.

Maximum Availability Architecture for Enterprise Manager mandates deploying a remote failover architecture that allows a secondary datacenter to take over the management infrastructure in the event that disaster strikes the primary management infrastructure.

*Figure 17–8 Disaster Recovery Architecture*



As can be seen in Figure 17–8, setting up disaster recovery for Enterprise Manager essentially consists of installing a standby RAC, a standby Management Service and a standby Server Load Balancer and configuring them to automatically startup when the primary components fail.

The following sections lists the best practices to configure the key Enterprise Manager components for disaster recovery:

- Prerequisites
- Setup Standby Database
- Setup Standby Management Service
- Switchover
- Failover
- Automatic Failover

#### 17.5.6.1 Prerequisites

The following prerequisites must be satisfied.

- The primary site must be configured as per Grid Control MAA guidelines described in previous sections. This includes Management Services fronted by an SLB and all Management Agents configured to upload to Management Services by the SLB.
- The standby site must be similar to the primary site in terms of hardware and network resources to ensure there is no loss of performance when failover happens.
- There must be sufficient network bandwidth between the primary and standby sites to handle peak redo data generation.
- Configure shared storage used for shared filesystem loader and software library to be replicated at the primary and standby site. In the event of a site outage, the contents of this shared storage must be made available on the standby site using hardware vendor disk level replication technologies.
- For complete redundancy in a disaster recovery environment, a second load balancer must be installed at the standby site. The secondary SLB must be configured in the same fashion as the primary. Some SLB vendors (such as F5 Networks) offer additional services that can be used to pass control of the Virtual IP presented by the SLB on the primary site to the SLB on the standby site in the event of a site outage. This can be used to facilitate automatic switching of Management Agent traffic from the primary site to the standby site.

#### 17.5.6.2 Setup Standby Database

As described earlier, the starting point of this step is to have the primary site configured as per Grid Control MAA guidelines. The following steps will lay down the procedure for setting up the standby Management Repository database.

1. Prepare Standby Management Repository hosts for Data Guard

   Install a Management Agent on each of the standby Management Repository hosts. Configure the Management Agents to upload by the SLB on the primary site.

   Install CRS and Database software on the standby Management Repository hosts. The version used must be the same as that on the primary site.

2. Prepare Primary Management Repository database for Data Guard

   In case the primary Management Repository database is not already configured, enable archive log mode, setup flash recovery area and enable flashback database on the primary Management Repository database.

3. Create Physical Standby Database

   In Enterprise Manager, the standby Management Repository database must be physical standbys. Use the Enterprise Manager Console to setup a physical standby database in the standby environment prepared in previous steps. Note that Enterprise Manager Console does not support creating a standby RAC database. If the standby database has to be RAC, configure the standby database using a single instance and then use the Convert to RAC option from Enterprise Manager Console to convert the single instance standby database to RAC. Also, note that during single instance standby creation, the database files should be created on shared storage to facilitate conversion to RAC later.

4. Add Static Service to Listener

To enable Data Guard to restart instances during the course of broker operations, a service with a specific name must be statically registered with the local listener of each instance. The value for the GLOBAL_DBNAME attribute must be set to a concatenation of <db_unique_name>_DGMGRL.<db_domain>. For example, in the LISTENER.ORA file:

```
SID_LIST_LISTENER=(SID_LIST=(SID_DESC=(SID_NAME=sid_name)
     (GLOBAL_DBNAME=db_unique_name_DGMGRL.db_domain)
     (ORACLE_HOME=oracle_home)))
```

5. Enable Flashback Database on the Standby Database
6. Verify Physical Standby

   Verify the Physical Standby database through the Enterprise Manager Console. Click the Log Switch button on the Data Guard page to switch log and verify that it is received and applied to the standby database.

#### 17.5.6.3 Setup Standby Management Service

The following considerations should be noted before installing the standby Management Services.

- It is recommended that this activity be done during a lean period or during a planned maintenance window. When new Management Services are installed on the standby site, they are initially configured to connect to the Management Repository database on the primary site. Some workload will be taken up by the new Management Service. This could result in temporary loss in performance if the standby site Management Services are located far away from the primary site Management Repository database. However there would be no data loss and the performance would recover once the standby Management Services are shutdown post configuration.
- The shared storage used for the shared filesystem loader and software library must be made available on the standby site using the same paths as the primary site.

Install the Management Service software using steps documented in the *Oracle Enterprise Manager Grid Control Installation and Basic Configuration Guide*. Refer to the Installing Software-Only and Configuring Later - Additional Management Service option. Specify the primary database connection settings in the response file. Once you have the Management Service installed, use the following steps to copy over the configuration from any the primary Management Service.

1. Export the configuration from the primary Management Service using:

   ```
   emctl exportconfig oms -dir <location for the export file>
   ```

2. Copy over the exported file to the standby Management Service
3. Shutdown the standby Management Service
4. Import the exported configuration on the standby Management Service using:
   ```
   emctl importconfig oms -file <full path of the export file>
   ```
5. Make the standby Management Service point to the standby Management Repository database by updating the emoms.properties file:
   ```
   oracle.sysman.eml.mntr.emdRepConnectDescriptor=<connect
   descriptor of standby database>
   ```

6. Setup EMCLI on the standby Management Service using the URL of the primary SLB using `emcli setup -url=https://slb.example.com/em -username sysman -password <sysman password> -nocertvalidate`
7. Resecure the Management Agent that is installed with the standby Management Service to upload to primary SLB using `emctl secure agent -emdWalletSrcUrl https://slb.example.com:<upload port>/em`
8. Update the standby SLB configuration by adding the standby Management Service to the different pools on the SLB. Setup monitors for the new Management Service. Modify the ssl.conf file to set the Port directive to the SLB virtual port used for UI access.

Repeat the previous steps for setting up an additional standby Management Service.

> **Note:** To monitor a standby database completely, the user monitoring the database must have SYSDBA privileges. This privilege is required because the standby database is in a mounted-only state. A best practice is to ensure that the users monitoring the primary and standby databases both have SYSDBA privileges.

#### 17.5.6.4 Switchover

Switchover is a planned activity where operations are transferred from the Primary site to a Standby site. This is usually done for testing and validation of Disaster Recovery (DR) scenarios and for planned maintenance activities on the primary infrastructure. This section describes the steps to switchover to the standby site. The same procedure is applied to switchover in either direction.

Enterprise Manager Console cannot be used to perform switchover of the Management Repository database. The Data Guard Broker command line tool DGMGRL should be used instead.

1. Prepare Standby Database

   Verify that recovery is up-to-date. Using the Enterprise Manager Console, you can view the value of the ApplyLag column for the standby database in the Standby Databases section of the Data Guard Overview Page.

2. Shutdown the Primary Enterprise Manager Application Tier

   Shutdown all the Management Services in the primary site by running the following command on each Management Service: `opmnctl stopall`

   Shutdown the Enterprise Manager jobs running in Management Repository database: `- alter system set job_queue_processes=0;`

3. Verify Shared Loader Directory / Software Library Availability

   Ensure all files from the primary site are available on the standby site.

4. Switchover to the Standby Database

   Use DGMGRL to perform a switchover to the standby database. The command can be run on the primary site or the standby site. The switchover command verifies the states of the primary database and the standby database, affects switchover of roles, restarts the old primary database, and sets it up as the new standby database.

   SWITCHOVER TO <standby database name>;

   Verify the post switchover states:

```
SHOW CONFIGURATION;
SHOW DATABASE <primary database name>;
SHOW DATABASE <standby database name>;
```

5. Startup the Enterprise Manager Application Tier

   Startup all the Management Services on the standby site: `opmnctl startall`

   Startup the Enterprise Manager jobs running in Management Repository database on the standby site (the new primary database) - `alter system set job_queue_processes=10;`

6. Relocate Management Services and Management Repository target

   The Management Services and Management Repository target is monitored by a Management Agent on one of the Management Services on the primary site. To ensure that the target is monitored after switchover/failover, relocate the target to a Management Agent on the standby site by running the following command on one of the Management Service standby sites.

   ```
   emctl config emrep -agent <agent name> -conn_desc
   ```

7. Switchover to Standby SLB

   Make appropriate network changes to failover your primary SLB to standby SLB that is, all requests should now be served by the standby SLB without requiring any changes on the clients (browser and Management Agents).

This completes the switchover operation. Access and test the application to ensure that the site is fully operational and functionally equivalent to the primary site.

Repeat the same procedure to switchover in the other direction.

#### 17.5.6.5 Failover

A standby database can be converted to a primary database when the original primary database fails and there is no possibility of recovering the primary database in a timely manner. This is known as a manual failover. There may or may not be data loss depending upon whether your primary and target standby databases were synchronized at the time of the primary database failure.

This section describes the steps to failover to a standby database, recover the Enterprise Manager application state by resyncing the Management Repository database with all Management Agents, and enabling the original primary database as a standby using flashback database.

The word *manual* is used here to contrast this type of failover with a fast-start failover described later in Section 17.5.6.6, "Automatic Failover".

1. Verify Shared Loader Directory and Software Library Availability

   Ensure all files from the primary site are available on the standby site.

2. Failover to Standby Database

   Shutdown the database on the primary site. Use DGMGRL to connect to the standby database and execute the FAILOVER command: `FAILOVER TO <standby database name>;`

   Verify the post failover states:

   ```
   SHOW CONFIGURATION;
   SHOW DATABASE <primary database name>;
   SHOW DATABASE <standby database name>;
   ```

Note that after the failover completes, the original primary database cannot be used as a standby database of the new primary database unless it is re-enabled.

3. Resync the New Primary Database with Management Agents

   Skip this step if you are running in Data Guard Maximum Protection or Maximum Availability level as there is no data loss on failover. On the other hand, if there is data loss, you need to synchronize the new primary database with all Management Agents.

   On any one Management Service on the standby site, run the following command:

   ```
   emctl resync repos -full -name "<name for recovery action>"
   ```

   This command submits a resync job that would be executed on each Management Agent when the Management Services on the standby site are brought up.

   Repository resynchronization is a resource intensive operation. A well tuned Management Repository will help significantly to complete the operation as quickly as possible. Specifically if you are not routinely coalescing the IOTs/indexes associated with Advanced Queueing tables as described in My Oracle Support note 271855.1, running the procedure before resync will significantly help the resync operation to complete faster.

4. Startup the Enterprise Manager Application Tier

   Startup all the Management Services on the standby site by running the following command on each Management Service.

   ```
   opmnctl startall
   ```

5. Relocate Management Services and Management Repository target

   The Management Services and Management Repository target is monitored by a Management Agent on one of the Management Services on the primary site. To ensure that target is monitored after switchover/failover, relocate the target to a Management Agent on the standby site by running the following command on one of the standby site Management Services.

   ```
   emctl config emrep -agent <agent name> -conn_desc
   ```

6. Switchover to Standby SLB

   Make appropriate network changes to failover your primary SLB to the standby SLB, that is, all requests should now be served by the standby SLB without requiring any changes on the clients (browser and Management Agents).

7. Establish Original Primary Database as Standby Database Using Flashback

   Once access to the failed site is restored and if you had flashback database enabled, you can reinstate the original primary database as a physical standby of the new primary database.

   - Shutdown all the Management Services in original primary site:

     ```
     opmnctl stopall
     ```

   - Restart the original primary database in mount state:

     ```
     shutdown immediate;
     ```

     ```
     startup mount;
     ```

   - Reinstate the Original Primary Database

     Use DGMGRL to connect to old primary database and execute the REINSTATE command

```
REINSTATE DATABASE <old primary database name>;
```

- The newly reinstated standby database will begin serving as standby database to the new primary database.
- Verify the post reinstate states:

```
SHOW CONFIGURATION;
SHOW DATABASE <primary database name>;
SHOW DATABASE <standby database name>;
```

8. Navigate to the Management Services and Repository Overview page of Grid Control Console. Under Related Links, click **Repository Synchronization**. This page shows the progress of the resynchronization operation on a per Management Agent basis. Monitor the progress.

   Operations that fail should be resubmitted manually from this page after fixing the error mentioned. Typically, communication related errors are caused by Management Agents being down and can be fixed by resubmitting the operation from this page after restarting the Management Agent.

   For Management Agents that cannot be started due to some reason, for example, old decommissioned Management Agents, the operation should be stopped manually from this page. Resynchronization is deemed complete when all the jobs have a completed or stopped status.

This completes the failover operation. Access and test the application to ensure that the site is fully operational and functionally equivalent to the primary site.

Do a switchover procedure if the site operations have to be moved back to the original primary site.

#### 17.5.6.6 Automatic Failover

This section details the steps to achieve complete automation of failure detection and failover procedure by utilizing Fast-Start Failover and Observer process. At a high level the process works like this:

- Fast-Start Failover (FSFO) determines that a failover is necessary and initiates a failover to the standby database automatically
- When the database failover has completed the DB_ROLE_CHANGE database event is fired
- The event causes a trigger to be fired which calls a script that configures and starts Enterprise Manager Application Tier

Perform the following steps:

1. Develop Enterprise Manager Application Tier Configuration and Startup Script

   Develop a script that will automate the Enterprise Manager Application configuration and startup process. See the sample shipped with Grid Control in the OH/sysman/ha directory. A sample script for the standby site is included here and should be customized as needed. Make sure `ssh` equivalence is setup so that remote shell scripts can be executed without password prompts. Place the script in a location accessible from the standby database host. Place a similar script on the primary site.

```
#!/bin/sh
# Script: /scratch/EMSBY_start.sh
# Primary Site Hosts
# Repos: earth, OMS: jupiter1, jupiter2
# Standby Site Hosts
# Repos: mars, # OMS: saturn1, saturn2
LOGFILE="/net/mars/em/failover/em_failover.log"
OMS_ORACLE_HOME="/scratch/OracleHomes/em/oms10g"
CENTRAL_AGENT="saturn1.example.com:3872"

#log message
echo "###############################" >> $LOGFILE
date >> $LOGFILE
echo $OMS_ORACLE_HOME >> $LOGFILE
id >>  $LOGFILE 2>&1

#startup all OMS
#Add additional lines, one each per OMS in a multiple OMS setup
ssh orausr@saturn1 "$OMS_ORACLE_HOME/opmn/bin/opmnctl startall" >>  $LOGFILE
2>&1
ssh orausr@saturn2 "$OMS_ORACLE_HOME/opmn/bin/opmnctl startall" >>  $LOGFILE
2>&1

#relocate Management Services and Repository target
#to be done only once in a multiple OMS setup
#allow time for OMS to be fully initialized
ssh orausr@saturn1 "$OMS_ORACLE_HOME/bin/emctl config emrep -agent $CENTRAL_
AGENT -conn_desc -sysman_pwd <password>" >> $LOGFILE 2>&1

#always return 0 so that dbms scheduler job completes successfully
exit 0
```

2. Automate Execution of Script by Trigger

   Create a database event "DB_ROLE_CHANGE" trigger, which fires after the database role changes from standby to primary. See the sample shipped with Grid Control in OH/sysman/ha directory.

```
--
--
-- Sample database role change trigger
--
--
CREATE OR REPLACE TRIGGER FAILOVER_EM
AFTER DB_ROLE_CHANGE ON DATABASE
DECLARE
    v_db_unique_name varchar2(30);
    v_db_role varchar2(30);
BEGIN
    select upper(VALUE) into v_db_unique_name
    from v$parameter where NAME='db_unique_name';
    select database_role into v_db_role
    from v$database;

    if v_db_role = 'PRIMARY' then

      -- Submit job to Resync agents with repository
      -- Needed if running in maximum performance mode
      -- and there are chances of data-loss on failover
      -- Uncomment block below if required
      -- begin
      --  SYSMAN.setemusercontext('SYSMAN', SYSMAN.MGMT_USER.OP_SET_
IDENTIFIER);
      --  SYSMAN.emd_maintenance.full_repository_resync(('AUTO-FAILOVER to
'||v_db_unique_name);
```

```
      --  SYSMAN.setemusercontext('SYSMAN', SYSMAN.MGMT_USER.OP_CLEAR_
IDENTIFIER);
      -- end;

      -- Start the EM mid-tier
      dbms_scheduler.create_job(
          job_name=>'START_EM',
          job_type=>'executable',
          job_action=> '<location>' || v_db_unique_name|| '_start_oms.sh',
          enabled=>TRUE
      );
    end if;
EXCEPTION
WHEN OTHERS
THEN
    SYSMAN.mgmt_log.log_error('LOGGING', SYSMAN.MGMT_GLOBAL.UNEXPECTED_ERR,
SYSMAN.MGMT_GLOBAL.UNEXPECTED_ERR_M || 'EM_FAILOVER: ' ||SQLERRM);
END;
/
```

> **Note:** Based on your deployment, you might require additional steps to synchronize and automate the failover of SLB and shared storage used for loader receive directory and software library. These steps are vendor specific and beyond the scope of this document. One possibility is to invoke these steps from the Enterprise Manager Application Tier startup and configuration script.

3. Configure Fast-Start Failover and Observer

   Use the Fast-Start Failover configuration wizard in Enterprise Manager Console to enable FSFO and configure the Observer.

   This completes the setup of automatic failover.

## 17.6 Installation Best Practices for Enterprise Manager High Availability

The following sections document best practices for installation and configuration of each Grid Control component.

### 17.6.1 Configuring the Management Agent to Automatically Start on Boot and Restart on Failure

The Management Agent is started manually. It is important that the Management Agent be automatically started when the host is booted to insure monitoring of critical resources on the administered host. To that end, use any and all operating system mechanisms to automatically start the Management Agent. For example, on UNIX systems this is done by placing an entry in the UNIX `/etc/init.d` that calls the Management Agent on boot or by setting the Windows service to start automatically.

### 17.6.2 Configuring Restart for the Management Agent

Once the Management Agent is started, the watchdog process monitors the Management Agent and attempts to restart it in the event of a failure. The behavior of the watchdog is controlled by environment variables set before the Management

Agent process starts. The environment variables that control this behavior follow. All testing discussed here was done with the default settings.

- EM_MAX_RETRIES – This is the maximum number of times the watchdog will attempt to restart the Management Agent within the EM_RETRY_WINDOW. The default is to attempt restart of the Management Agent 3 times.
- EM_RETRY_WINDOW - This is the time interval in seconds that is used together with the EM_MAX_RETRIES environmental variable to determine whether the Management Agent is to be restarted. The default is 600 seconds.

The watchdog will not restart the Management Agent if the watchdog detects that the Management Agent has required restart more than EM_MAX_RETRIES within the EM_RETRY_WINDOW time period.

### 17.6.3 Installing the Management Agent Software on Redundant Storage

The Management Agent persists its intermediate state and collected information using local files in the `$AGENT_HOME/$HOSTNAME/sysman/emd` sub tree under the Management Agent home directory.

In the event that these files are lost or corrupted before being uploaded to the Management Repository, a loss of monitoring data and any pending alerts not yet uploaded to the Management Repository occurs.

At a minimum, configure these sub-directories on striped redundant or mirrored storage. Availability would be further enhanced by placing the entire $AGENT_HOME on redundant storage. The Management Agent home directory is shown by entering the command '`emctl getemhome`' on the command line, or from the Management Services and Repository tab and Agents tab in the Grid Control console.

### 17.6.4 Install the Management Service Shared File Areas on Redundant Storage

The Management Service contains results of the intermediate collected data before it is loaded into the Management Repository. The loader receive directory contains these files and is typically empty when the Management Service is able to load data as quickly as it is received. Once the files are received by the Management Service, the Management Agent considers them committed and therefore removes its local copy. In the event that these files are lost before being uploaded to the Management Repository, data loss will occur. At a minimum, configure these sub-directories on striped redundant or mirrored storage. When Management Services are configured for the Shared Filesystem Loader, all services share the same loader receive directory. It is recommended that the shared loader receive directory be on a clustered file system like NetApps Filer.

## 17.7 Configuration With Grid Control

Grid Control comes preconfigured with a series of default rules to monitor many common targets. These rules can be extended to monitor the Grid Control infrastructure as well as the other targets on your network to meet specific monitoring needs.

### 17.7.1 Console Warnings, Alerts, and Notifications

The following list is a set of recommendations that extend the default monitoring performed by Enterprise Manager. Use the Notification Rules link on the Preferences page to adjust the default rules provided on the Configuration/Rules page:

- Ensure the Agent Unreachable rule is set to alert on all Management Agents unreachable and Management Agents clear errors.
- Ensure the Repository Operations Availability rule is set to notify on any unreachable problems with the Management Service or Management Repository nodes. Also modify this rule to alert on the Targets Not Providing Data condition and any database alerts that are detected against the database serving as the Management Repository.

Modify the Agent Upload Problems Rule to alert when the Management Service status has hit a warning or clear threshold.

## 17.7.2 Configure Additional Error Reporting Mechanisms

Enterprise Manager provides error reporting mechanisms through e-mail notifications, PL/SQL packages, and SNMP alerts. Configure these mechanisms based on the infrastructure of the production site. If using e-mail for notifications, configure the notification rule through the Grid Control console to notify administrators using multiple SMTP servers if they are available. This can be done by modifying the default e-mail server setting on the Notification Methods option under Setup.

## 17.7.3 Component Backup

Backup procedures for the database are well established standards. Configure backup for the Management Repository using the RMAN interface provided in the Grid Control console. Refer to the RMAN documentation or the Maximum Availability architecture document for detailed implementation instructions.

In addition to the Management Repository, the Management Service and Management Agent should also have regular backups. Backups should be performed after any configuration change.

## 17.7.4 Troubleshooting

In the event of a problem with Grid Control, the starting point for any diagnostic effort is the console itself. The Management System tab provides access to an overview of all Management Service operations and current alerts. Other pages summarize the health of Management Service processes and logged errors These pages are useful for determining the causes of any performance problems as the summary page shows at a historical view of the amount of files waiting to be loaded to the Management Repository and the amount of work waiting to be completed by Management Agents.

### 17.7.4.1 Upload Delay for Monitoring Data

When assessing the health and availability of targets through the Grid Control console, information is slow to appear in the UI, especially after a Management Service outage. The state of a target in the Grid Control console may be delayed after a state change on the monitored host. Use the Management System page to gauge backlog for pending files to be processed.

### 17.7.4.2 Notification Delay of Target State Change

The model used by the Management Agent to assess the state of health for any particular monitored target is poll based. Management Agents immediately post a notification to the Management Service as soon as a change in state is detected. This infers that there is some potential delay for the Management Agent to actually detect a change in state.

# 18 Configuring Enterprise Manager for Active and Passive Environments

Active and Passive environments, also known as Cold Failover Cluster (CFC) environments, refer to one type of high availability solution that allows an application to run on one node at a time. These environments generally use a combination of *cluster* software to provide a logical host name and IP address, along with interconnected host and storage systems to share information to provide a measure of high availability for applications.

This chapter contains the following sections:

## 18.1 Using Virtual Host Names for Active and Passive High Availability Environments in Enterprise Manager Database Control

This section provides information to database administrators about configuring an Oracle Database release 10*g* in Cold Failover Cluster environments using Enterprise Manager Database Control.

The following conditions must be met for Database Control to service a database instance after failing over to a different host in the cluster:

- The installation of the database must be done using a Virtual IP address.
- The installation must be conducted on a shared disk or volume which holds the binaries, configuration, and runtime data (including the database).
- Configuration data and metadata must also failover to the surviving node.
- Inventory location must failover to the surviving node.
- Software owner and time zone parameters must be the same on all cluster member nodes that will host this database.

The following items are configuration and installation points you should consider before getting started.

- To override the physical host name of the cluster member with a virtual host name, software must be installed using the parameter ORACLE_HOSTNAME.
- For inventory pointer, software must be installed using the command parameter `invPtrLoc` to point to the shared inventory location file, which includes the path to the shared inventory location.
- The database software, the configuration of the database, and Database Control are done on a shared volume.

### 18.1.1 Set Up the Alias for the Virtual Host Name and Virtual IP Address

You can set up the alias for the virtual host name and virtual IP address by either allowing the clusterware to set it up automatically or by setting it up manually before installation and startup of Oracle services. The virtual host name must be static and resolvable consistently on the network. All nodes participating in the setup must resolve the virtual IP address to the same host name. Standard TCP tools similar to `nslookup` and `traceroute` commands can be used to verify the set up.

### 18.1.2 Set Up Shared Storage

Shared storage can be managed by the clusterware that is in use or you can use any shared file system volume as long as it is supported. The most common shared file system is NFS. You can also use the Oracle Cluster File System software.

### 18.1.3 Set Up the Environment

Some operating system versions require specific operating system patches to be applied prior to installing release 10*g*R2 of the Oracle database. You must also have sufficient kernel resources available when you conduct the installation.

Before you launch the installer, specific environment variables must be verified. Each of the following variables must be identically set for the account you are using to install the software on all machines participating in the cluster.

- Operating system variable TZ, time zone setting. You should unset this prior to the installation.
- PERL variables. Variables like PERL5LIB should be unset to prevent the installation and Database Control from picking up the incorrect set of PERL libraries.
- Paths used for dynamic libraries. Based on the operating system, the variables can be LD_LIBRARY_PATH, LIBPATH, SHLIB_PATH, or DYLD_LIBRARY_PATH. These variables should *only* point to directories that are visible and usable on each node of the cluster.

### 18.1.4 Ensure That the Oracle USERNAME, ID, and GROUP NAME Are Synchronized on All Cluster Members

The user and group of the software owner should be defined identically on all nodes of the cluster. You can verify this using the following command:

```
$ id -a
uid=1234(oracle) gid=5678(dba) groups=5678(dba)
```

## 18.1.5 Ensure That Inventory Files Are on the Shared Storage

To ensure that inventory files are on the shared storage, follow these steps:

- Create you new ORACLE_HOME directory.
- Create the Oracle Inventory directory under the new Oracle home

  ```
  cd <shared oracle home>
  mkdir oraInventory
  ```

- Create the oraInst.loc file. This file contains the Inventory directory path information required by the Universal Installer:

  1. `vi oraInst.loc`
  2. Enter the path information to the Oracle Inventory directory and specify the group of the software owner as the `dba` user. For example:

     ```
     inventory_loc=/app/oracle/product/10.2/oraInventory
     inst_group=dba
     ```

     Depending on the type of operating system, the default directory for the oraInst.loc file is either `/etc` (for example, on Linux) or `/var/opt/oracle` (for example, on Solaris and HP-UX).

## 18.1.6 Start the Installer

To start the installer, point to the inventory location file oraInst.loc, and specify the host name of the virtual group. The debug parameter in the example below is optional:

```
$ export ORACLE_HOSTNAME=lxdb.acme.com
$ runInstaller -invPtrloc /app/oracle/share1/oraInst.loc ORACLE_
HOSTNAME=lxdb.acme.com -debug
```

### 18.1.6.1 Windows NT Specific Configuration Steps

On Windows environments, an additional step is required to copy over service and keys required by the Oracle software.

1. Using regedit on the first host, export each Oracle service from under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.
2. Using regedit on the first host, export HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE.
3. Use regedit to import the files created in step 1 and 2 to the failover host.

For Windows, NT services need to be created on the failover host. For an Enterprise Manager release 10.2.0.5 Management Agent, the following command can be used:

```
emctl create service [-user <username>] [-pwd <password>] -name
<servicename>
```

This has to be done once on the failover host after doing a failover.

## 18.1.7 Start Services

You must start the services in the following order:

1. Establish IP address on the active node
2. Start the TNS listener
3. Start the database

4. Start dbconsole
5. Test functionality

In the event that services do not start, do the following:

1. Establish IP on failover box
2. Start TNS listener

   ```
   lsnrctl start
   ```

3. Start the database

   ```
   dbstart
   ```

4. Start Database Control

   ```
   emctl start dbconsole
   ```

5. Test functionality

To manually stop or shutdown a service, follow these steps:

1. Stop the application.
2. Stop Database Control

   ```
   emctl stop dbconsole
   ```

3. Stop TNS listener

   ```
   lsnrctl stop
   ```

4. Stop the database

   ```
   dbshut
   ```

5. Stop IP

## 18.2 Configuring Grid Control Repository in Active/Passive High Availability Environments

In order for Grid Control repository to fail over to a different host, the following conditions must be met:

- The installation must be conducted using a Virtual Hostname and an associated unique IP address
- Installation must occur on a shared disk/volume which holds the binaries, the configuration, and the runtime data (including the repository database)
- Configuration data and metadata must also failover to the surviving node
- Inventory location must failover to the surviving node
- Software owner and time zone parameters must be the same on all cluster member nodes that will host this OMS

### 18.2.1 Installation and Configuration

The following installation and configuration requirements should be noted:

- To override the physical host name of the cluster member with a virtual host name, software must be installed using the parameter ORACLE_HOSTNAME.

- For inventory pointer, software must be installed using the command line parameter *-invPtrLoc* to point to the shared inventory location file, which includes the path to the shared inventory location.
- The database software, the configuration of the database, and data files are on a shared volume.

If you are using an NFS mounted volume for the installation, ensure that you specify rsize and wsize in your mount command to prevent I/O issues. See My Oracle Support note 279393.1 Linux.NetApp: RHEL/SUSE Setup Recommendations for NetApp Filer Storage.

Example:

```
grid-repo.acme.com:/u01/app/share1 /u01/app/share1 nfs
rw,bg,rsize=32768,wsize=32768,hard,nointr,tcp,noac,vers=3,timeo=
600 0 0
```

> **Note:** Any reference to *shared* could also be true for non-shared failover volumes, which can be mounted on active hosts after failover.

### 18.2.2 Set Up the Virtual Host Name/Virtual IP Address

You can set up the virtual host name and virtual IP address by either allowing the clusterware to set it up or manually setting it up before installation and startup of Oracle services. The virtual host name must be static and resolvable consistently on the network. All nodes participating in the setup must resolve the virtual IP address to the same host name. Standard TCP tools such as `nslookup` and `traceroute` can be used to verify the host name. Validate using the commands listed below:

```
nslookup <virtual hostname>
```

This command returns the virtual IP address and fully qualified host name.

```
nslookup <virtual IP>
```

This command returns the virtual IP address and fully qualified host name.

Be sure to try these commands on every node of the cluster to verify that the correct information is returned.

### 18.2.3 Set Up the Environment

Some operating system versions require specific patches to be applied prior to installing 10*g*R2. The user installing and using the 10*g*R2 software must also have sufficient kernel resources available. Refer to the operating system's installation guide for more details.

Before you launch the installer, certain environment variables must be verified. Each of these variables must be set up identically for the account installing the software on ALL machines participating in the cluster:

- OS variable TZ (time zone setting)

  You should unset this variable prior to installation.

- PERL variables

  Variables such as PERL5LIB should also be unset to prevent inadvertently picking up the wrong set of PERL libraries.

- Same operating system, operating system patches, and version of the kernel. Therefore, RHEL 3 and RHEL 4 are *not* allowed for a CFC system.
- System libraries

  For example, LIBPATH, LD_LIBRARY_PATH, SHLIB_PATH, and so on. The same system libraries must be present.

### 18.2.4 Synchronize Operating System User IDs

The user and group of the software owner should be defined identically on all nodes of the cluster. This can be verified using the id command:

```
$ id -a
```

```
uid=550(oracle) gid=50(oinstall) groups=501(dba)
```

### 18.2.5 Set Up Inventory

You can set up the inventory by using the following steps:

1. Create your new ORACLE_HOME directory.
2. Create the Oracle Inventory directory under the new oracle home

   ```
   cd <shared oracle home>
   ```

   ```
   mkdir oraInventory
   ```

3. Create the oraInst.loc file. This file contains the Inventory directory path information needed by the Universal Installer.

   ```
   vi oraInst.loc
   ```

   Enter the path information to the Oracle Inventory directory, and specify the group of the software owner as the oinstall user:

   Example:

   ```
   inventory_loc=/app/oracle/product/10.2/oraInventory
   inst_group=oinstall
   ```

### 18.2.6 Install the Software

Follow these steps to install the software:

1. Create the shared disk location on both the nodes for the software binaries.
2. Point to the inventory location file oraInst.loc (under the ORACLE_BASE in this case), as well as specifying the host name of the virtual group. For example:

   ```
   $ export ORACLE_HOSTNAME=grid-repo.acme.com
   $ runInstaller -invPtrLoc /app/oracle/share1/oraInst.loc ORACLE_
   HOSTNAME=grid-repo.acme.com
   ```

3. Install the repository DB software only on the shared location. For example:

   `/oradbnas/app/oracle/product/oradb10203` using *Host1*

4. Start DBCA and create all the data files be on the shared location. For example:

   `/oradbnas/oradata`

5. Continue the rest of the installation normally.

6. Once completed, copy the files *oraInst.loc* and *oratab* to */etc*. Also copy */opt/oracle* to all cluster member hosts (*Host2*, *Host3*, and so on).

#### 18.2.6.1 Windows NT Specific Configuration Steps

On Windows environments, an additional step is required to copy over service and keys required by the Oracle software.

1. Using regedit on the first host, export each Oracle service from under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.
2. Using regedit on the first host, export HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE.
3. Use regedit to import the files created in step 1 and 2 to the failover host.

For Windows, NT services need to be created on the failover host. For an Enterprise Manager release 10.2.0.5 Management Agent, the following command can be used:

```
emctl create service [-user <username>] [-pwd <password>] -name
<servicename>
```

This has to be done once on the failover host after doing a failover.

### 18.2.7 Startup of Services

Be sure you start your services in the proper order:

1. Establish IP address on the active node
2. Start the TNS listener if it is part of the same failover group
3. Start the database if it is part of the same failover group

In case of failover, follow these steps:

1. Establish IP address on the failover box
2. Start TNS listener (`lsnrctl start`) if it is part of the same failover group
3. Start the database (`dbstart`) if it is part of the same failover group

### 18.2.8 Summary

The Grid Control Management Repository can now be deployed in a CFC environment that utilizes a floating host name.

To deploy the OMS midtier in a CFC environment, please see Section 18.3, "How to Configure Grid Control OMS in Active/Passive Environment for High Availability Failover Using Virtual Host Names".

## 18.3 How to Configure Grid Control OMS in Active/Passive Environment for High Availability Failover Using Virtual Host Names

This section provides a general reference for Grid Control administrators who want to configure Enterprise Manager 10*g* Grid Control in Cold Failover Cluster (CFC) environments.

### 18.3.1 Overview and Requirements

The following conditions must be met for Grid Control to fail over to a different host:

- The installation must be done using a Virtual Host Name and an associated unique IP address.
- Install on a shared disk/volume which holds the binaries, the configuration and the runtime data (including the recv directory).
- Configuration data and metadata must also failover to the surviving node.
- Inventory location must failover to the surviving node.
- Software owner and time zone parameters must be the same on all cluster member nodes that will host this Oracle Management Service (OMS).

### 18.3.2 Installation and Configuration

To override the physical host name of the cluster member with a virtual host name, software must be installed using the parameter ORACLE_HOSTNAME. For inventory pointer, the software must be installed using the command line parameter *-invPtrLoc* to point to the shared inventory location file, which includes the path to the shared inventory location.

If you are using an NFS mounted volume for the installation, please ensure that you specify rsize and wsize in your mount command to prevent running into I/O issues.

For example:

```
oms.acme.com:/u01/app/share1 /u01/app/share1 nfs
rw,bg,rsize=32768,wsize=32768,hard,nointr,tcp,noac,vers=3,timeo=
600 0 0
```

> **Note:** Any reference to shared failover volumes could also be true for non-shared failover volumes which can be mounted on active hosts after failover.

### 18.3.3 Setting Up the Virtual Host Name/Virtual IP Address

You can set up the virtual host name and virtual IP address by either allowing the clusterware to set it up, or manually setting it up yourself before installation and startup of Oracle services. The virtual host name must be static and resolvable consistently on the network. All nodes participating in the setup must resolve the virtual IP address to the same host name. Standard TCP tools such as nslookup and traceroute can be used to verify the host name. Validate using the following commands:

`nslookup` <*virtual hostname*>

This command returns the virtual IP address and full qualified host name.

`nslookup` <*virtual IP*>

This command returns the virtual IP address and fully qualified host name.

Be sure to try these commands on every node of the cluster and verify that the correct information is returned.

### 18.3.4 Setting Up Shared Storage

Storage can be managed by the clusterware that is in use or you can use any shared file system (FS) volume as long as it is not an unsupported type, such as OCFS V1. The most common shared file system is NFS.

**Note:** Do not create the ssl.conf file on shared storage, otherwise there is a potential for locking issues. Create the ssl.conf file on local storage.

### 18.3.5 Setting Up the Environment

Some operating system versions require specific operating system patches be applied prior to installing 10*g*R2. The user installing and using the 10*g*R2 software must also have sufficient kernel resources available. Refer to the operating system's installation guide for more details.

Before you launch the installer, certain environment variables need to be verified. Each of these variables must be identically set for the account installing the software on ALL machines participating in the cluster:

- OS variable TZ

  Time zone setting. You should unset this variable prior to installation

- PERL variables

  Variables such as PERL5LIB should also be unset to avoid association to the incorrect set of PERL libraries

### 18.3.6 Synchronizing Operating System IDs

The user and group of the software owner should be defined identically on all nodes of the cluster. This can be verified using the 'id' command:

```
$ id -a
```

```
uid=550(oracle) gid=50(oinstall) groups=501(dba)
```

### 18.3.7 Setting Up Shared Inventory

Use the following steps to set up shared inventory:

1. Create your new ORACLE_HOME directory.
2. Create the Oracle Inventory directory under the new oracle home:

   ```
   $ cd <shared oracle home>
   ```

   ```
   $ mkdir oraInventory
   ```

3. Create the oraInst.loc file. This file contains the Inventory directory path information needed by the Universal Installer.

   a. `vi oraInst.loc`

   b. Enter the path information to the Oracle Inventory directory and specify the group of the software owner as the oinstall user. For example:

   ```
   inventory_loc=/app/oracle/product/10.2/oraInventory
   ```

   ```
   inst_group=oinstall
   ```

### 18.3.8 Installing the Software

Refer to the following steps when installing the software:

1. Create the shared disk location on both the nodes for the software binaries

2. Point to the inventory location file oraInst.loc (under the ORACLE_BASE in this case), as well as specifying the host name of the virtual group. For example:

   ```
   $ export ORACLE_HOSTNAME=lxdb.acme.com
   $ runInstaller -invPtrloc /app/oracle/share1/oraInst.loc
   ORACLE_HOSTNAME=lxdb.acme.com -debug
   ```

3. Modify the results of the uname -n (node name) command by executing the UNIX command `hostname` <*unqualified name of virtual host*>. V$session reads that command immediately.

   If you are unable to modify the host name, abort the installer when the OMS configuration assistant fails at *emctl config emkey* and execute the following commands to complete the installation:

   a. Replace all host name entries with the virtual host name in *$OMS_HOME/sysman/config/emoms.properties*.

   b. `<OMS_HOME>/bin/emctl config emkey -repos -force`

   c. `<OMS_HOME>/bin/emctl secure oms`

   d. `<OMS_HOME>/bin/emctl secure lock`

   e. `<OMS_HOME>/perl/bin/perl $OMSHOME/sysman/install/precompilejsp.pl <OMS_HOME>/j2ee/OC4J_EM/config/global-web-application.xml`

      Perform this step if you are using Grid Control 10.2.0.1. Grid Control must be installed before applying the 10.2.0.4 or 10.2.0.5 patchsets.

   f. `<OMS_HOME>/bin/emctl config agent updateTZ`

   g. `<OMS_HOME>/opmn/bin/opmnctl stopall`

   h. `<OMS_HOME>/opmn/bin/opmnctl startall`

   i. `<AGENT_HOME>/bin/agentca -f`

4. Install Oracle Management Services on cluster member *Host1* using the option, "EM install using the existing DB"

5. Continue the remainder of the installation normally.

6. Once completed, copy the files *oraInst.loc* and *oratab* to */etc*. Also copy */opt/oracle* to all cluster member hosts (*Host2*, *Host3*, and so on).

### 18.3.8.1 Windows Specific Configuration Steps

On Windows environments, an additional step is required to copy over service and keys required by the Oracle software.

1. Using regedit on the first host, export each Oracle service from under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services.

2. Using regedit on the first host, export HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE.

3. Use regedit to import the files created in step 1 and 2 to the failover host.

For Windows, NT services need to be created on the failover host. For an Enterprise Manager release 10.2.0.5 Management Agent, the following command can be used:

```
emctl create service [-user <username>] [-pwd <password>] -name
<servicename>
```

This has to be done once on the failover host after doing a failover.

### 18.3.9 Starting Up Services

Ensure that you start your services in the proper order. Use the order listed below:

1. Establish IP address on the active node
2. Start the TNS listener (if it is part of the same failover group)
3. Start the database (if it is part of the same failover group)
4. Start Grid Control using opmnctl startall
5. Test functionality

In case of failover, refer to the following steps:

1. Establish IP on failover box
2. Start TNS listener using the command `lsnrctl start` if it is part of the same failover group
3. Start the database using the command `dbstart` if it is part of the same failover group
4. Start Grid Control using the command `opmnctl startall`
5. Test the functionality

### 18.3.10 Summary

The OMS mid-tier component of Grid Control can now be deployed in a CFC environments that utilize a floating host name.

To deploy the repository database in a CFC environment, see Section 18.2, "Configuring Grid Control Repository in Active/Passive High Availability Environments".

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

This section provides a general reference for Grid Control administrators who want to relocate Cold Failover Cluster (CFC) targets from one existing Management Agent to another. Although the targets are capable of running on multiple nodes, these targets run only on the active node in a CFC environment.

CFC environments generally use a combination of cluster software to provide a virtual host name and IP address along with interconnected host and storage systems to share information and provide high availability for applications. Automating failover of the virtual host name and IP, in combination with relocating the Enterprise Manager targets and restarting the applications on the passive node, requires the use of Oracle Enterprise Manager command-line interface (EM CLI) and Oracle Clusterware (running Oracle Database release 10*g* or 11*g*) or third-party cluster software. Several Oracle partner vendors provide clusterware solutions in this area.

The Enterprise Manager Command Line Interface (EM CLI) allows you to access Enterprise Manager Grid Control functionality from text-based consoles (terminal sessions) for a variety of operating systems. Using EM CLI, you can perform Enterprise Manager Grid Control console-based operations, like monitoring and managing targets, jobs, groups, blackouts, notifications, and alerts. See the *Oracle Enterprise Manager Command Line Interface* manual for more information.

## 18.4.1 Target Relocation in Active/Passive Environments

Beginning with Oracle Enterprise Manager 10g release 10.2.0.5, a single Oracle Management Agent running on each node in the cluster can monitor targets configured for active / passive high availability. Only one Management Agent is required on each of the physical nodes of the CFC cluster because, in case of a failover to the passive node, Enterprise Manager can move the HA monitored targets from the Management Agent on the failed node to another Management Agent on the newly activated node using a series of EMCLI commands.

If your application is running in an active/passive environment, the clusterware brings up the applications on the passive node in the event that the active node fails. For Enterprise Manager to continue monitoring the targets in this type of configuration, the existing Management Agent needs additional configuration.

The following sections describe how to prepare the environment to automate and restart targets on the new active node. Failover and fallback procedures are also provided.

## 18.4.2 Installation and Configuration

The following sections describe how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents communicating with the Oracle Management Service processes:

- Prerequisites
- Configuration Steps

### 18.4.2.1 Prerequisites

Prepare the Active/Passive environments as follows:

- Ensure the operating system clock is synchronized across all nodes of the cluster. (Consider using Network Time Protocol (NTP) or another network synchronization method.)
- Use the EM CLI RELOCATE_TARGETS command only with Enterprise Manager Release 10.2.0.5 (and higher) Management Agents.

### 18.4.2.2 Configuration Steps

The following steps show how to configure Enterprise Manager to support a CFC configuration using the existing Management Agents that are communicating with the OMS processes. The example that follows is based on a configuration with a two-node cluster that has one failover group. For additional information about targets running in CFC active/passive environments, see My Oracle Support note 406014.1.

1. Configure EM CLI

   To set up and configure target relocation, use the Oracle Enterprise Manager command-line interface (EM CLI). See the *Oracle Enterprise Manager Command Line Interface* manual and the *Oracle Enterprise Manager Extensibility* manual for information about EM CLI and Management Plug-Ins.

2. Install Management Agents

   Install the Management Agent on a local disk volume on each node in the cluster. Once installed, the Management Agents are visible in the Grid Control console.

3. Discover Targets

After the Active / Passive targets have been configured, use the Management Agent discovery screen in the Grid Control console to add the targets (such as database, listener, application server, and so on). Perform the discovery on the active node, which is the node that is currently hosting the new target.

### 18.4.3 Failover Procedure

To speed relocation of targets after a node failover, configure the following steps using a script that contains the commands necessary to automatically initiate a failover of a target. Typically, the clusterware software has a mechanism with which you can automatically execute the script to relocate the targets in Enterprise Manager. Also, see Section 18.4.6, "Script Examples" for sample scripts.

1. Shut down the target services on the failed active node.

   On the active node where the targets are running, shut down the target services running on the virtual IP.

2. If required, disconnect the storage for this target on the active node.

   Shut down all the applications running on the virtual IP and shared storage.

3. Enable the target's IP address on the new active node.

4. If required, connect storage for the target on the currently active node.

5. Relocate the targets in Grid Control using EM CLI.

   To relocate the targets to the Management Agent on the new active node, issue the EM CLI RELOCATE TARGET command for each target type (listener, application servers, and so on) that you must relocate after the failover operation. For example:

   ```
   emcli relocate_targets
   -src_agent=<node 1>:3872
   -dest_agent=<node 2>:3872
   -target_name=<database_name>
   -target_type=oracle_database
   -copy_from_src
   -force=yes
   ```

   In the example, port 3872 is the default port for the Management Agent. To find the appropriate port number for your configuration, use the value for the EMD_URL parameter in the emd.properties file for this Management Agent.

   **Note:** In case of a failover event, the source agent will not be running. However, there is no need to have the source Management Agent running to accomplish the RELOCATE operation. EM CLI is an OMS client that performs its RELOCATE operations directly against the Management Repository.

### 18.4.4 Fallback Procedure

To return the HA targets to the original active node or to any other cluster member node:

1. Repeat the steps in Section 18.4.3, "Failover Procedure" to return the HA targets to the active node.

2. Verify the target status in the Grid Control console.

## 18.4.5 EM CLI Parameter Reference

Issue the same command for each target type that will be failed over to (or be switched over) during relocation operations. For example, issue the same EM CLI command to relocate the listener, the application servers, and so on. Table 18–1 shows the EM CLI parameters you use to relocate targets:

*Table 18–1 EM CLI Parameters*

| EM CLI Parameter | Description |
|---|---|
| -src_agent | Management Agent on which the target was running before the failover occurred. |
| -dest_agent | Management Agent that will be monitoring the target after the failover. |
| -target_name | Name of the target to be failed over. |
| -target_type | Type of target to be failed over (internal Enterprise Manager target type). For example, the Oracle database (for a standalone database or an Oracle RAC instance), the Oracle listener for a database listener, and so on. |
| -copy_from_src | Use the same type of properties from the source Management Agent to identify the target. This is a **MANDATORY** parameter! If you do not supply this parameter, you can corrupt your target definition! |
| -force | Force dependencies (if needed) to failover as well. |

## 18.4.6 Script Examples

The following sections provide script examples:

- Relocation Script
- Start Listener Script
- Stop Listener Script

### 18.4.6.1 Relocation Script

```
#! /bin/ksh

#get the status of the targets

emcli get_targets -
targets="db1:oracle_database;listener_db1:oracle_listener" -noheader

  if [[ $? != 0 ]]; then exit 1; fi

# blackout the targets to stop false errors.  This blackout is set to expire in 30
minutes

emcli create_blackout -name="relocating active passive test targets" -
add_targets="db1:oracle_database;listener_db1:oracle_listener" -
reason="testing failover" -
schedule="frequency:once;duration:0:30"
  if [[ $? != 0 ]]; then exit 1; fi

# stop the listener target.  Have to go out to a OS script to use the 'lsnrctl set
current_listener' function

emcli execute_hostcmd -cmd="/bin/ksh" -osscript="FILE" -
```

```
input_file="FILE:/scratch/oraha/cfc_test/listener_stop.ksh" -
credential_set_name="HostCredsNormal" -
targets="host1.us.oracle.com:host"
  if [[ $? != 0 ]]; then exit 1; fi

# now, stop the database

emcli execute_sql -sql="shutdown abort" -
targets="db1:oracle_database" -
credential_set_name="DBCredsSYSDBA"
  if [[ $? != 0 ]]; then exit 1; fi

# relocate the targets to the new host

emcli relocate_targets -
src_agent=host1.us.oracle.com:3872 -
dest_agent=host2.us.oracle.com:3872 -
target_name=db1 -target_type=oracle_database -
copy_from_src -force=yes  -
changed_param=MachineName:host1vip.us.oracle.com
  if [[ $? != 0 ]]; then exit 1; fi

emcli relocate_targets -
src_agent=host1.us.oracle.com:3872 -
dest_agent=host2.us.oracle.com:3872 -
target_name=listener_db1 -target_type=oracle_listener -
copy_from_src -force=yes  -
changed_param=MachineName:host1vip.us.oracle.com
  if [[ $? != 0 ]]; then exit 1; fi

# Now, restart database and listener on the new host

emcli execute_hostcmd -cmd="/bin/ksh" -osscript="FILE" -
input_file="FILE:/scratch/oraha/cfc_test/listener_start.ksh" -
credential_set_name="HostCredsNormal" -
targets="host2.us.oracle.com:host"
  if [[ $? != 0 ]]; then exit 1; fi

emcli execute_sql -sql="startup" -
targets="db1:oracle_database" -
credential_set_name="DBCredsSYSDBA"
  if [[ $? != 0 ]]; then exit 1; fi

# Time to end the blackout and let the targets become visible

emcli stop_blackout -name="relocating active passive test targets"
  if [[ $? != 0 ]]; then exit 1; fi

# and finally, recheck the status of the targets

emcli get_targets -
targets="db1:oracle_database;listener_db1:oracle_listener" -noheader
  if [[ $? != 0 ]]; then exit 1; fi
```

### 18.4.6.2 Start Listener Script

```
#!/bin/ksh

export
```

```
ORACLE_HOME=/oradbshare/app/oracle/product/11.1.0/db
export PATH=$ORACLE_HOME/bin:$PATH

lsnrctl << EOF
set current_listener listener_db1
start
exit
EOF
```

#### 18.4.6.3 Stop Listener Script

```
#!/bin/ksh
export
ORACLE_HOME=/oradbshare/app/oracle/product/11.1.0/db
export PATH=$ORACLE_HOME/bin:$PATH

lsnrctl << EOF
set current_listener listener_db1
stop
exit
EOF
```

## 18.5 Configuring Additional Oracle Enterprise Management Agents for Use in Active and Passive Environments

In a Cold Failover Cluster environment, one host is considered the *active node* where applications are run, accessing the data contained on the shared storage. The second node is considered the *standby node*, ready to run the same applications currently hosted on the primary node in the event of a failure. The cluster software is configured to present a *Logical Host Name* and IP address. This address provides a generic location for running applications that is not tied to either the active node or the standby node.

In the event of a failure of the active node, applications can be terminated either by the hardware failure or by the cluster software. These application can then be restarted on the passive node using the same logical host name and IP address to access the new node; resuming operations with little disruption. Automating failover of the virtual host name and IP, along with starting the applications on the passive node, requires the use of the third party cluster software. Several Oracle partner vendors provide high availability solutions in this area.

### 18.5.1 Installation and Configuration

Enterprise Manager can be configured to support Cold Failover Cluster configuration in this fashion using additional Management Agents communicating to the Oracle Management Service processes.

If your application is running in an Active and Passive environment, the clusterware does the job of bringing up the *passive* or *standby* database instance in case the *active* database goes down. For Enterprise Manager to continue monitoring the application instance in such a scenario, the existing Management Agents need additional configuration.

The additional configuration steps for this environment involve:

- Installing an extra Management Agent using the logical host name and IP address generated through the cluster software.
- Modifying the targets monitored by each Management Agent once the third Management Agent is installed.

In summary, this configuration results in the installation of three Management Agents, one for each hardware node and one for the IP address generated by the cluster software. Theoretically, if the cluster software supports the generation of multiple virtual IP addresses to support multiple high availability environments, the solution outlined here should scale to support the environment.

The following table documents the steps required to configure Management Agents in a CFC environment:

*Table 18–2 Steps Required to Configure Management Agents in a Cold Failover Cluster Environment*

| Action | Method | Description/Outcome | Verification |
|---|---|---|---|
| Install the vendor specific cluster software | Installation method varies depending on the cluster vendor. | The minimal requirement is a 2-node cluster that supports Virtual or Floating IP addresses and shared storage. | Use the `ping` command to verify the existence of the floating IP address.<br>Use `nslookup` or equivalent command to verify the IP address in your environment.<br>Ensure the machine is reachable on the network by using tools like traceroute or tracert. |
| Install Management Agents to each physical node of the cluster using the physical IP address or host name as the node name. | Use the Oracle Universal Installer (OUI) to install Management Agents to each node of the cluster.<br>Change the property AgentListenOnAllNICS to FALSE in the local Management Agent emd.properties file. | When complete, the OUI will have installed Management Agents on each node that will be visible through the Grid Control console. | Check that the Management Agent, host, and targets are visible in the Enterprise Manager environment. |
| Delete targets that will be configured for high availability using the cluster software. | Using the Grid Control console, delete all targets discovered during the previous installation step that are managed by the cluster software except for the Management Agent and the host. | Grid Control Console displays the Management Agent, hardware, and any target that is not configured for high availability. | Inspect the Grid Control console and verify that all targets that will be assigned to the Management Agent running on the floating IP address have been deleted from the Management Agents monitoring the fixed IP addresses. |
| Install a third Management Agent to the cluster using the logical IP address or logical host name as the host specified in the OUI at install time.<br>**Note:** This installation should not detect or install to more than one node. | This Management Agent must follow all the same conventions as any application using the cluster software to move between nodes (that is, installed on the shared storage using the logical IP address).<br>This installation requires an additional option to be used at the command line during installation time. The 'HOSTNAME' flag must be set as in the following example:<br>(/144)-<br>>./runInstaller HOSTNAME=<Logical IP address or host name> | Third Management Agent installed, currently monitoring all targets discovered on the host running physical IP. | To verify the Management Agent is configured correctly, type `emctl status agent` at the command line and verify the use of the logical IP virtual host name. Also, verify that the Management Agent is set to the correct Management Service URL and that the Management Agent is uploading the files.<br>When the Management Agent is running and uploading data, use the Grid Control console to verify that it has correctly discovered targets that will move to the standby node during a failover operation. |

*Table 18–2 (Cont.) Steps Required to Configure Management Agents in a Cold Failover Cluster*

| Action | Method | Description/Outcome | Verification |
|---|---|---|---|
| Delete any targets from the Management Agent monitoring the logical IP that will not switch to the passive node during failover. | Use the Grid Control console to delete any targets that will not move between hosts in a switchover or failover scenario. These might be targets that are not attached to this logical IP address for failover or are not configured for redundancy. | Grid Control console is now running three Management Agents. Any target that is configured for switchover using cluster software will be monitored by a Management Agent that will transition during switchover or failover operations. | The operation is also verified by inspecting the Grid Control console. All targets that will move between nodes should be monitored by the Management Agent running on the virtual host name. All remaining targets should be monitored by a Management Agent running on an individual node. |
| Add the new logical host to the cluster definition. | Using the All Targets tab on the Grid Control console, find the cluster target and add the newly discovered logical host to the existing cluster target definition. | It is also possible (*not required*) to use the **Add Cluster Target** option on the All Targets tab, making a new composite target using the nodes of the cluster. | The Grid Control console will now correctly display all the hosts associated with the cluster. |
| Place the Management Agent process running on the logical IP under the control of the cluster software. | This will vary based on the cluster software vendor. | Management Agent will transition along with applications.<br>A suggested order of operation is covered in the next section. | Verify that the Management Agent can be stopped and restarted on the standby node using the cluster software. |

## 18.5.2 Switchover Steps

Each cluster vendor will implement the process of building a wrapper around the steps required to do a switchover or failover in a different fashion. The steps themselves are generic and are listed here:

- Shut down the Management Agent
- Shut down all the applications running on the virtual IP and shared storage
- Switch the IP and shared storage to the new node
- Restart the applications
- Restart the Management Agent

Stopping the Management Agent first, and restarting it after the other applications have started, prevents Enterprise Manager from triggering any false *target down* alerts that would otherwise occur during a switchover or failover.

## 18.5.3 Performance Implications

While it is logical to assume that running two Management Agent processes on the active host may have some performance implications, this was not shown during testing. Keep in mind that if the Management Agents are configured as described in this chapter, the Management Agent monitoring the physical host IP will only have two targets to monitor. Therefore the only additional overhead is the two Management Agent processes themselves and the commands they issue to monitor a Management Agent and the operating system. During testing, it was noticed that an overhead of between 1-2% of CPU usage occurred.

### 18.5.4 Summary

Generically, configuring Enterprise Manager to support Cold Cluster Failover environments encompasses the following steps.

- Install a Management Agent for each virtual host name that is presented by the cluster and insure that the Management Agent is correctly communicating to the Management Service.
- Configure the Management Agent that will move between nodes to monitor the appropriate highly available targets.
- Verify that the Management Agent can be stopped on the primary node and restarted on the secondary node automatically by the cluster software in the event of a switchover or failover.

# 19

# 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.

> **See Also:** Chapter 17 for more information about some of the ways you can configure the Grid Control components on your network

This chapter contains the following topics:

- Considerations Before Configuring Your Firewall
- Firewall Configurations for Enterprise Management Components
- Viewing a Summary of the Ports Assigned During the Application Server Installation

## 19.1 Considerations Before Configuring Your Firewall

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 Grid 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 the Oracle Enterprise Manager 10*g* Grid Control Console 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.

> **See Also:** Chapter 20, "Reconfiguring the Management Agent and Management Service" for information about locating and changing the default ports for the Oracle Management Service and the Oracle Management Agent

If you are enabling Enterprise Manager Framework Security for the 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 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.

## 19.2 Firewall Configurations for Enterprise Management Components

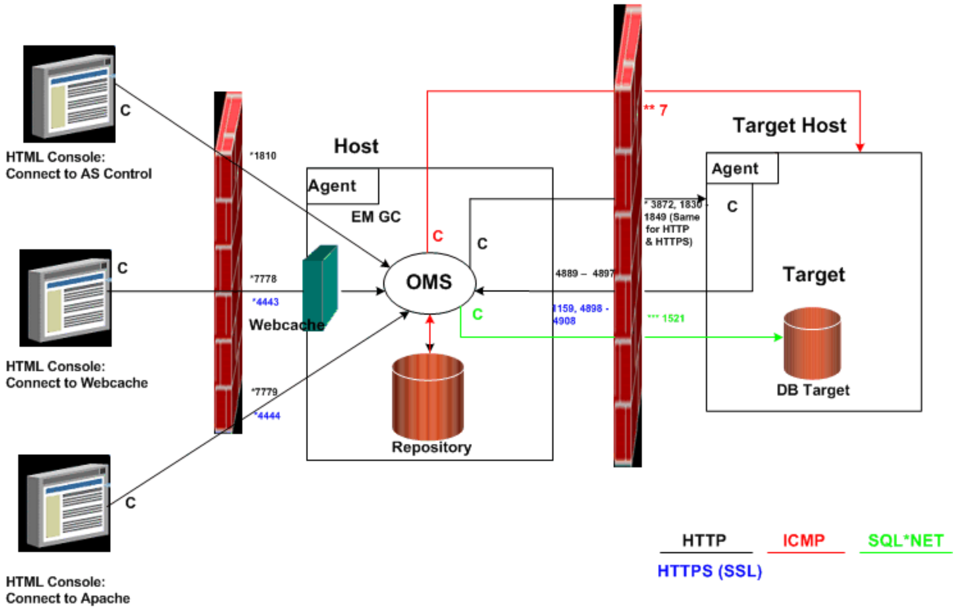
Your main task in enabling Enterprise Manager to work in a firewall-protected environment is to take advantage of proxy servers whenever possible, to make sure only the necessary ports are open for secure communications, and to make sure that only data necessary for running your business is allowed to pass through the firewall.

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 Grid Control Console
- Configuring the Management Agent on a Host Protected by a Firewall
- Configuring the Management Service on a Host Protected by a Firewall
- Firewalls Between the Management Service and the Management Repository
- Firewalls Between the Grid Control and a Managed Database Target
- Firewalls Used with Multiple Management Services
- Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons
- Configuring Firewalls When Managing Oracle Application Server

  Figure 19–1 provides a topology of an Enterprise Manager grid environment that is using a firewall, and also illustrates the default ports that can be used.

*Figure 19–1 Firewall Port Requirements (Default)*



The conventions used in the preceding illustration are as follows:

*Table 19–1 Conventions Used*

| 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. |

**Note:**

- 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.

## 19.2.1 Firewalls Between Your Browser and the Grid Control Console

Connections from your browser to the Oracle Enterprise Manager 10*g* Grid 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 7778. If you are accessing the Grid Control Console using the following URL and port, then you must configure the firewall to allow the Grid Control Console to receive HTTP traffic over port 7778:

```
http://mgmthost.acme.com:7778/em
```

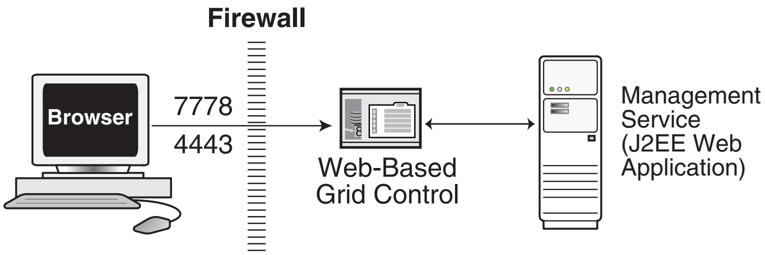
On the other hand, if you have enabled security for your Oracle HTTP Server, you are likely using the default secure port for the server, which is usually port 4443. If you are accessing the Grid Control Console using the following URL and port, then you must configure the firewall to allow the Grid Control Console to receive HTTP traffic over port 4443:

```
https://mgmthost.acme.com:4443/em
```

**See also:** *Oracle Application Server 10g Security Guide*

Figure 19–2 shows the typical configuration of a firewall between your browser and the Grid Control Console Web-based console that is rendered by the Management Service.

***Figure 19–2 Firewall Between Your Browser and the Grid Control Console***



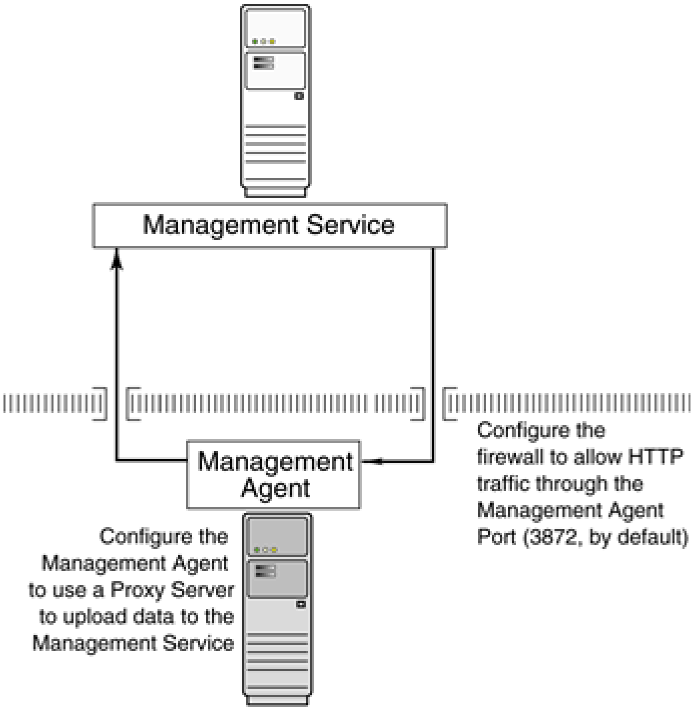
## 19.2.2 Configuring the Management Agent on a Host Protected by a Firewall

If your Management Agent is installed on a host that is protected by a firewall and the 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 Management Service.
- Configure the firewall to allow incoming HTTP traffic from the Management Service on the Management Agent port. Regardless of whether or not Enterprise Manager Framework Security has been enabled, the default port is 3872. If this default port is not available, the default port range between 1830 - 1849 is used. Incoming traffic can be received only if the port corresponding to the Management Agent is open in the firewall.

Figure 19–3 illustrates the connections the Management Agent must make when it is protected by a firewall.

*Figure 19–3 Configuration Tasks When the Management Agent is Behind a Firewall*


Management Service
Management Agent
Configure the Management Agent to use a Proxy Server to upload data to the Management Service
Configure the firewall to allow HTTP traffic through the Management Agent Port (3872, by default)

### 19.2.2.1 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 Management Service outside the firewall, or to manage a target outside the firewall.

1. Use a text editor to open the following Management Agent configuration file:

```
AGENT_HOME/sysman/config/emd.properties (UNIX)
AGENT_HOME\sysman\config\emd.properties (Windows)
```

2. Locate the following entry in the `emd.properties` file:

```
# If it is necessary to go through an http proxy server to get to the
# repository, uncomment the following lines
#REPOSITORY_PROXYHOST=
#REPOSITORY_PROXYPORT=
```

3. To enable support for authenticating the proxy server, the following additional properties need to be specified.

```
#REPOSITORY_PROXYREALM=
#REPOSITORY_PROXYUSER=
#REPOSITORY_PROXYPWD=
```

4. Edit the following properties by removing the pound sign (#) at the start of each line and entering a value as follows:

```
# If it is necessary to go through an http proxy server to get to the
# repository, uncomment the following lines
REPOSITORY_PROXYHOST=proxyhostname.domain
REPOSITORY_PROXYPORT=proxy_port
REPOSITORY_PROXYREALM=realm
REPOSITORY_PROXYUSER=proxyuser
```

```
REPOSITORY_PROXYPWD=proxypassword
```

For example:

```
REPOSITORY_PROXYHOST=proxy42.acme.com
REPOSITORY_PROXYPORT=80
REPOSITORY_PROXYREALM=
REPOSITORY_PROXYUSER=
REPOSITORY_PROXYPWD=
```

5. Save your changes and close the `emd.properties` file.
6. Stop and start the Management Agent.

**Note:** The proxy password will be rewritten when you restart the Management Agent.

#### 19.2.2.2 Configuring the Firewall to Allow Incoming Communication From the Management Service

While the Management Agents in your environment must upload data from your managed hosts to the Management Service, the Management Service must also communicate with the Management Agents. As a result, if the Management Agent is protected by a firewall, the 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 1830 to the Management Agent. However, if that port is occupied, the installation may assign an alternate port number.

**Note:** The port number for the Management Agent does not change when you enable Enterprise Manager Framework Security. For more information, see the security chapter in the *Oracle Enterprise Manager Administration Guide*.

In addition, administrators can change the Management Agent port after the installation.

**See Also:** "Chapter 20, "Reconfiguring the Management Agent and Management Service" for information about locating and changing the default ports for the Oracle Management Service and the Oracle Management Agent.

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.

### 19.2.3 Configuring the Management Service on a Host Protected by a Firewall

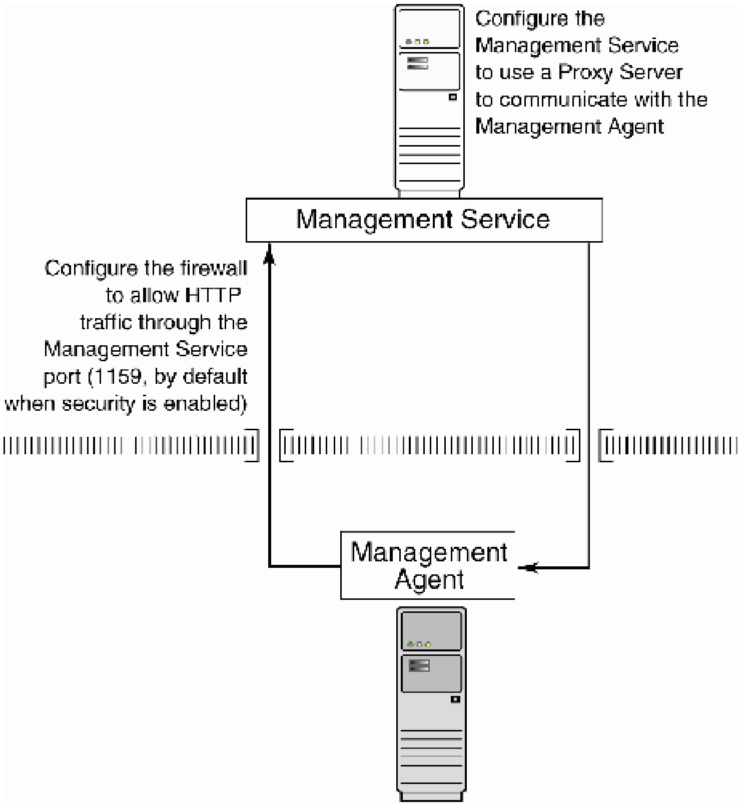
If your Management Service is installed on a host that is protected by a firewall and the Management Agents that provide management data are on the other side of the firewall, you must perform the following tasks:

- Configure the 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 4898-4989. If you have *not* enabled Enterprise Manager Framework Security, the upload port is the first available port in the range 4889 - 4897.

Figure 19–4 illustrates the connections the Management Service must make when it is protected by a firewall.

***Figure 19–4 Configuration Tasks When the Management Service is Behind a Firewall***


Configure the Management Service to use a Proxy Server to communicate with the Management Agent
Management Service
Configure the firewall to allow HTTP traffic through the Management Service port (1159, by default when security is enabled)
Management Agent

### 19.2.3.1 Configuring the Management Service to Use a Proxy Server

This section describes how to configure the Management Service to use a proxy server for its communications with Management Agents outside the firewall.

> **Note:** The proxy configuration properties described in this section are the same Management Service properties you must modify if your network is protected by a firewall and you want Enterprise Manager to search automatically for critical patches and patch sets. For more information, see "Specifying Patching Credentials" in the Enterprise Manager online Help.

To configure the Management Service to use a proxy server:

1. Use a text editor to open the following configuration file in the Management Service home directory:

   ```
   ORACLE_HOME/sysman/config/emoms.properties
   ```

2. Add the following entries to `emoms.properties` file:

   ```
   proxyHost=proxyhost.domain
   proxyPort=proxy_port
   dontProxyFor=.domain1, .domain2, .domain3, ...
   proxyRealm=realm
   proxyUser=proxyuser
   proxyPwd=proxypassword
   ```

   For example:

   ```
   proxyHost=proxy42.acme.com
   proxyHost=80
   dontProxyFor=.acme.com, .acme.us.com
   proxyRealm
   proxyUser
   proxyPwd
   ```

   The `dontProxyFor` property identifies specific URL domains for which the proxy will not be used. The `proxyRealm` property indicates the protected space that requires authentication.

   > **See Also:** "About the dontProxyfor Property" on page 19-8 for guidelines on when to use the `dontProxyFor` property

3. Save your changes and close the `emoms.properties` file.
4. Stop and start the Management Service:

   ```
   $PROMPT> ORACLE_HOME/bin/emctl stop oms
   $PROMPT> ORACLE_HOME/bin/emctl start oms
   ```

   > **Note:** The proxy password will be rewritten when you restart the Management Service.

#### 19.2.3.2 About the dontProxyfor Property

When you configure the Management Service 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 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 the Oracle*MetaLink* Internet site.

In this scenario, you want the Management Service to connect directly to the Management Agents inside the firewall without using the proxy server. On the other hand, you want the Management Service to use the proxy server to contact the

Management Agents outside the firewall, as well as the Oracle*MetaLink* Internet site, which resides at the following URL:

```
http://metalink.oracle.com
```

The following entry in the `emoms.properties` file will prevent the Management Service from using the proxy server for connections to the Management Agents inside the firewall. Connections to Oracle*MetaLink* 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
```

#### 19.2.3.3 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 Management Service must also be able to receive upload data from the Management Agents. If the 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.

> **See Also:** Chapter 20, "Reconfiguring the Management Agent and Management Service" for information about locating and changing the default ports for the Oracle Management Service and the Oracle Management Agent.

After you determine the port number assigned to the 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

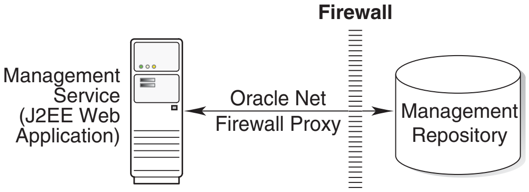
### 19.2.4 Firewalls Between the Management Service and the Management Repository

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.

> **See Also:** "Configuring Secure Sockets Layer Authentication" in the *Oracle Database Advanced Security Administrator's Guide*

Figure 19–5 shows a typical configuration of a firewall between the Management Service and the Management Repository.

***Figure 19–5 Firewall Between the Management Service and the Management Repository***


Firewall
Management Service (J2EE Web Application)
Oracle Net Firewall Proxy
Management Repository

## 19.2.5 Firewalls Between the Grid Control and a Managed Database Target

When you are using the Grid Control Console to manage a database, you must log in to the database from the Grid 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.

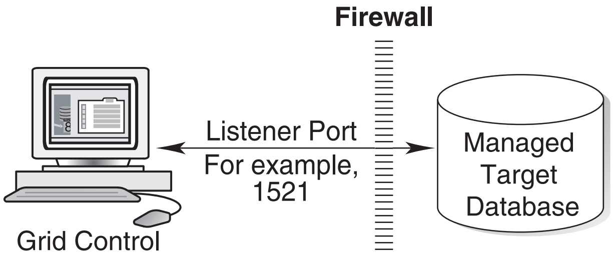
Specifically, to perform any administrative activities on the managed database, you must be sure that the firewall is configured to allow the Oracle Management Service to communicate with the database through the Oracle Listener port.

You can obtain the Listener port by reviewing the Listener home page in the Grid Control Console.

**See Also:** *Oracle Database Advanced Security Administrator's Guide*

Figure 19–6 shows a typical configuration of a firewall between Grid Control and the Management Repository.

***Figure 19–6 Firewall Between Grid Control and Managed Database Target***



## 19.2.6 Firewalls Used with Multiple Management Services

Enterprise Manager supports the use of multiple Management Services that communicate with a common Management Repository. For example, using more than one 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 Management Services in an environment protected by firewalls, be sure to consider the following:

- Each Management Agent is configured to upload data to one Management Service. As a result, if there is a firewall between the Management Agent and its 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 19-4

"Configuring the Management Service on a Host Protected by a Firewall" on page 19-6

- In addition, each 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 Management Service you deploy can communicate over HTTP or HTTPS with any Management Agent in your enterprise.

  Otherwise, a 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

### 19.2.7 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.

### 19.2.8 Configuring Firewalls When Managing Oracle Application Server

If you are using Grid Control to manage instances of Oracle Application Server, there may be other ports that you need to access through a firewall, depending upon your configurations.

For example, when you are monitoring the performance of your Oracle Application Server instance from the Grid Control Console, you can click **Administer** on the Application Server Home page to display the Application Server Control Console. If the Oracle Application Server target you are monitoring is separated from the Grid Control Console by a firewall, you will need to configure the firewall to allow an HTTP or HTTPS connection through Application Server Control Console port (usually, 1810).

**See Also:** *Oracle Application Server Administrator's Guide* for more information about configuring ports for Oracle Application Server

## 19.3 Viewing a Summary of the Ports Assigned During the Application Server Installation

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 10*g* components before you configure your firewalls.

When you install the Oracle Application Server 10*g* or the Oracle Enterprise Manager 10*g* Grid Control, you can view a list of the ports assigned during the application server installation by viewing the contents of the following file

```
ORACLE_HOME/install/portlist.ini
```

---

**Note:** The `portlist.ini` file lists the port numbers assigned during the installation. This file is not updated if port numbers are changed after the installation.

---

In addition, you can use the Application Server Control Console to view a list of all the ports in use by the application server:

1. Navigate to the Application Server home page in the Application Server Control Console.
2. Click **Ports**.

**See Also:** "Viewing and Modifying Application Server Port Assignments" in the Enterprise Manager online Help

## 19.4 Additional Considerations for Windows XP

For secure agent install, ensure that the firewall settings are disabled for HTTP/HTTPS communication for Windows XP:

1. Go to **Start**, and then select **Control Panel**.
2. In Control Panel, click **Windows Firewall**.
3. In the **Exceptions** tab in the **Windows Firewall** dialog box, click **Add Port**.
4. In the **Add a Port** dialog box, specify the name and number of the port.
5. Click **Change scope** to specify the computers for which the port is unblocked.

# 20

# Reconfiguring the Management Agent and Management Service

This chapter describes how to reconfigure Enterprise Manager if you later revisit your configuration decisions after you have installed the software.

This chapter contains the following sections:

- Reconfiguring the Oracle Management Agent
- Reconfiguring the Oracle Management Service

## 20.1 Reconfiguring the Oracle Management Agent

The following sections describe reconfiguration and tuning changes you can make to the Management Agent after you have installed Enterprise Manager. Refer to the following sections for more information:

- Configuring the Management Agent to Use a New Management Service
- Changing the Management Agent Port
- Controlling the Amount of Disk Space Used by the Management Agent
- About the Management Agent Watchdog Process
- Setting the Management Agent Time Zone
- Adding Trust Points to the Management Agent Configuration

### 20.1.1 Configuring the Management Agent to Use a New Management Service

When you install the Management Agent on a managed host, you associate the Management Agent with a particular Management Service. The Management Agent uses the Management Service URL address and port to identify and communicate with the Management Service.

After you install the Management Agent, you can later reconfigure the Management Agent so it is associated with a different Management Service. Reconfiguring the Management Agent requires no changes to the Management Service. The reconfigured Management Agent will begin communicating with the new Management Service after the Management Agent is restarted.

If you are associating the Management Agent with a Management Service that is locked, then first secure the Management Agent, and then associate it with the Management Service.

To associate the Management Agent with a new Management Service after you have installed the Management Agent:

1. Stop the Management Agent.
2. Locate the `emd.properties` file in the Management Agent home directory:

   ```
   AGENT_HOME/sysman/config/emd.properties
   ```

3. Use a text editor to open the file and locate the REPOSITORY_URL property.
4. Modify the value for the `REPOSITORY_URL` property so it references the new Management Service.

   For example:

   ```
   REPOSITORY_URL=http://mgmthost2.acme.com:4889/em/upload
   ```

5. Modify the value for the `emdWalletSrcUrl` and `emdWalletDest` properties so they reference the new Management Service and the new Oracle home path, respectively:

   For example, if the new Management Service is on a host called `mgmthost2.acme.com` and the new Oracle home is `/private/oracle/em10g`, modify the properties as follows:

   ```
   emdWalletSrcUrl=http://mgmthost2.acme.com:4889/em/wallets/emd
   emdWalletDest=/private/oracle/em10g/sysman/config/server
   ```

6. Save your changes and close the `emd.properties` file.
7. Delete all the files in the following directories:

   ```
   AGENT_HOME/sysman/emd/upload/
   AGENT_HOME/sysman/emd/state/
   ```

   > **Note:** You can use the `emctl clearstate agent` command to delete the files in the state directory.

8. Restart the Management Agent.

### 20.1.2 Securing the Management Agent

To secure the Management Agent of the new Management Service, use the following command:

```
emctl secure agent <password_to_secure_agent_against_new_mgmt_
service>
```

### 20.1.3 Changing the Management Agent Port

The Management Agent uses a predefined port number to receive requests from the Management Service. This port number is defined by default when you install the Management Agent on a managed host. If you later need to modify this port, you can use the following procedure. You might need to modify this port number if you have existing software that uses the default Management Agent port.

To change the Management Agent port:

1. Stop the Management Agent.
2. Locate the `emd.properties` file in the Management Agent home directory:

```
AGENT_HOME/sysman/config/emd.properties
```

3. Use a text editor to open the file and locate the EMD_URL property.

   For example:

   ```
   EMD_URL=http://managed_host1.acme.com:1813/emd/main
   ```

4. Modify the port number in the EMD_URL property so the Management Agent uses a new unused port on the managed host.

   For example:

   ```
   EMD_URL=http://managed_host1.acme.com:1913/emd/main
   ```

5. Start the Management Agent.

**Note:** After the changed URL is processed, the old Management Agent should not have any targets. If you want, you can then remove the old Management Agent from the Management Service.

### 20.1.4 Controlling the Amount of Disk Space Used by the Management Agent

Oracle designed the Management Agent to work within a set of disk space limits. These limits prevent the Management Agent from using too much disk space and causing performance or resource issues on your enterprise systems. However, if disk space becomes an issue, you can adjust the default settings that are used to control the amount of disk space used by the Management Agent.

As the Management Agent on a particular host gathers management data about the targets on the host, it saves the collected data on the local disk until the data is uploaded to the Management Repository. The Management Agent saves this collected data and metadata in the following directory:

```
AGENT_HOME/sysman/emd/upload
```

By default, the Management Agent will save up to 50MB of collected data in the upload directory. If the amount of collected data exceeds 50MB, data collection is stopped temporarily until the data is uploaded to the repository and more disk space becomes available.

In addition, the Management Agent checks to be sure that the percentage of disk space currently in use on the local disk does not exceed 98 percent. If this value is exceeded, the Management Agent stops collecting data and stops saving information to the Management Agent log and trace files.

You can modify these default settings as follows:

1. Stop the Management Agent.
2. Locate the `emd.properties` file in the Management Agent home directory:

   ```
   AGENT_HOME/sysman/config/emd.properties
   ```

3. Use a text editor to open the file and modify the entries shown in Table 20–1.
4. Save your changes and exit the file.
5. Restart the Management Agent.

*Table 20–1 Properties for Controlling the Disk Space Used by the Management Agent*

| Property | Explanation |
|---|---|
| UploadMaxBytesXML | Use this property in the `emd.properties` file to specify the maximum number of megabytes (MB) used by the collected data in the Management Agent upload directory. When this limit is exceeded, the Management Agent will stop collecting additional management data until the next upload to the Management Repository reduces the amount of collected data in the upload directory. |
| UploadMaxDiskUsedPct | Use this property in the `emd.properties` file to specify the maximum percentage of disk space that can be in use on the local disk before the Management Agent temporarily stops collecting additional data and stops saving information to the Management Agent log and trace files.<br>The Management Agent will begin collecting data again when the percentage of disk space in use falls to less than the percentage specified in the `UploadMaxDiskUsedPctFloor` property in the `emd.properties` file. |

## 20.1.5 About the Management Agent Watchdog Process

The Management Agent is the Enterprise Manager component that gathers the data you need to manage your enterprise efficiently. As a result, Enterprise Manager includes software that keeps track of the Management Agent processes and makes sure the Management Agent stays running.

For example, if the Management Agent quits unexpectedly, this self-monitoring process—referred to as the watchdog process—will restart the Management Agent automatically.

In most situations, the watchdog process works in the background and requires no configuration or maintenance. The watchdog process is controlled by the `emwd.pl` script located in the following directory of the Management Agent home directory:

```
AGENT_HOME/bin
```

You can identify the watchdog process by using the following commands:

```
$PROMPT> ps -ef | grep emwd
```

## 20.1.6 Setting the Management Agent Time Zone

In today’s global economy, it is not uncommon for the systems you manage to reside in multiple locations throughout the world. For example, if your company headquarters are in New Hampshire, USA, you may need to manage systems that reside in California, Canada, and in Europe.

As Enterprise Manager collects monitoring data from Management Agents running on these remote systems, it is important that the data is correlated accurately. A software failure on a machine in Ontario, Canada might be the cause of a performance problem on a machine in Hoboken, New Jersey.

To correlate this data, it is important that Enterprise Manager obtains the correct time zone for each Management Agent that you install. The following sections describe how the Management Agent obtains the time zone and how to correct the problem if the time zone for a Management Agent is incorrect:

- Understanding How the Management Agent Obtains Time Zone Information
- Resetting the Time Zone of the Management Agent Due to Inconsistency of Time Zones
- Troubleshooting Management Agent Time Zone Problems

- Troubleshooting Management Service Time Zone Problems

### 20.1.6.1 Understanding How the Management Agent Obtains Time Zone Information

When you install the Management Agent, the software attempts to obtain the current time zone of the host computer. If successful, the installation procedure updates the `agentTZRegion` property setting in the following configuration file:

```
AGENT_HOME/sysman/config/emd.properties
```

The `agentTZRegion` property can be set to any of the values listed in the following file, which is installed in the Management Agent home directory:

```
AGENT_HOME/sysman/admin/suportedtzs.lst
```

### 20.1.6.2 Resetting the Time Zone of the Management Agent Due to Inconsistency of Time Zones

You need to reset the time zone of the Management Agent when *both* of the following situations are true:

- The Management Agent has been running with a particular time zone
- Subsequently a change occurs to the time zone of the host where the Management Agent is running

To propagate the time zone change to the `emd.properties` file, perform the following:

1. Execute the following script:

   ```
   ORACLE_HOME/bin/emctl resetTZ agent
   ```

   This script updates `ORACLE_HOME/<hostname>_<sid>/sysman/config/emd.properties` so that the value of `agentTZRegion` matches that of the current time zone setting of the machine.

   > **Note:** The location of the `emd.properties` file depends on the Control Console being used:
   >
   > - For the Database Control Console, the location is usually: ORACLE_HOME/<host>_<sid>/sysman/config
   > - For the Application Server Control Console, the location is: ORACLE_HOME/sysman/config
   > - For the Grid Control Management Agent, the location is ORACLE_HOME/sysman/config
   > - For the Real Application Cluster central Management Agent, the location is usually: ORACLE_HOME/<host>/sysman/config

2. In addition, this command prompts you to run a script against the Enterprise Manager Repository. You must log in to the database as the Enterprise Manager repository user and run the script `mgmt_target.set_agent_tzrgn`. An example follows:

   ```
   SQL> exec mgmt_target.set_agent_tzrgn('em.oracle.com:1830','PST8PDT');
   SQL> commit;
   SQL> exit
   ```

em.oracle.com:1830 represents the name of the emd target.

#### 20.1.6.3 Troubleshooting Management Agent Time Zone Problems

Sometimes, during the Management Agent installation, the time zone detected by the Management Agent configuration tool is not recognized by the Management Agent. In other words, the time zone obtained by the configuration tool is not listed in the Management Agent list of supported time zones.

This problem prevents the Management Agent from starting and results in an error similar to the following:

```
Could not determine agent time zone. Please refer to the file:
ORACLE_HOME/sysman/admin/supportedtzs.lst and pick a timezone region with a
standard offset of +5:0 from GMT and update the property ’agentTZRegion’ in the
file: ORACLE_HOME/sysman/config/emd.properties
```

This error appears in one of the log files shown in Table 20–2, depending upon which Enterprise Manager product you are using.

*Table 20–2 Location of Time Zone Error in the Enterprise Manager Log Files*

| If you are using... | Look for the Time Zone Error in This File... |
|---|---|
| Grid Control Console | emagent.nohup |
| Application Server Control Console | em.nohup |
| Database Control Console | emdb.nohup |

To configure the Management Agent to use a valid time zone:

1. Enter the following command in the Management Agent home directory to identify the time zone currently being used by the host computer:

   ```
   AGENT_HOME/bin/emctl config agent getTZ
   ```

2. Note the time zone that is returned by the emctl config agent getTZ command.

   This is the time zone of the host computer.

3. Use a text editor to open the following file in the Management Agent home directory:

   ```
   AGENT_HOME/sysman/admin/supportedtzs.lst
   ```

   This file contains a list of all the time zones supported by the Management Agent.

4. Browse the contents of the supportedtzs.lst file and note the supported time zone closest to the time zone of the host computer.

5. Use a text editor to open the following Management Agent configuration file:

   ```
   AGENT_HOME/sysman/config/emd.properties
   ```

6. Locate the following property near the end of the emd.properties file:

   ```
   agentTZRegion=
   ```

7. Set the value of this property to the time zone you identified as closest to the host time zone in the supportedtzs.lst file.

   For example:

```
agentTZRegion=Europe/Warsaw
```

8. Save your changes and close the `emd.properties` file.

   You should now be able to start the Management Agent without generating the error in the log file.

#### 20.1.6.4 Troubleshooting Management Service Time Zone Problems

Section 20.1.6.3 describes how to correct potential problems that result when the Management Agent cannot determine the proper time zone. Similar problems can occur when the Management Agent finds the correct time zone, but the time zone is not recognized by the Management Service or the database where the Management Repository resides.

When the Management Service does not recognize the time zone established by the Management Agent, Enterprise Manager generates the following error:

```
OMS does not understand the timezone region of the agent.
Either start the OMS using the extended list of time zones supported by
the database or pick a value of time zone from
ORACLE_HOME/emdw/sysman/admin/nsupportedtzs.lst, update the property
'agentTZRegion' in the file
ORACLE_HOME/sysman/config/emd.properties and restart the agent.
A value which is around an offset of  -05:00 from GMT should be picked.
```

This error appears in one of the log files shown in Table 20–2, depending upon which Enterprise Manager product you are using.

There are two ways to correct this problem:

- Restart the Management Repository database using the more extensive list of time zones in the `timezlrg.dat` database configuration file, and then start the Management Agent.

  > **See Also:** "Specifying the Database Time Zone File" in the *Oracle Database Administrator's Guide*

- Specify a new time zone for the Management Agent that the Management Repository database will recognize.

  > **See Also:** "Troubleshooting Management Agent Time Zone Problems" on page 20-6 for instructions on changing the time zone assigned to the Management Agent

## 20.1.7 Adding Trust Points to the Management Agent Configuration

For Application Server components such as Oracle Portal to run on a secure sockets layer (SSL), the appropriate security certificate must be added to the Management Agent configuration files.

Perform these steps to add the relevant security certificate:

1. Obtain the certificate, which is in Base64encoded X.509 (.CER) format, in the `b64SiteCertificate.txt` file. (The file name may be different in your configuration.) An example of the contents of the file is as follows:

```
------BEGIN CERTIFICATE--------------
MIIDBzCCAnCgAw...
...... base 64 certificate content .....
------END CERTIFICATE-----------------
```

2. In the Oracle Home of the Management Agent monitoring the wallet, run the following command to add the certificate to the Management Agent:

```
${ORACLE_HOME}/bin/mkwallet -i welcome
${ORACLE_HOME}/sysman/config/monwallet
${ORACLE_HOME}/sysman/config/b64SiteCertificate.txt NZDST_CLEAR_PTP
```

## 20.2 Reconfiguring the Oracle Management Service

The following sections describe configuration changes you can make to the Management Service after you install Enterprise Manager:

- Configuring the Management Service to Use a New Management Repository
- Configuring the Management Service to Use a New Port
- Configuring the Management Service to Prompt You When Using Execute Commands

### 20.2.1 Configuring the Management Service to Use a New Management Repository

When you install and deploy the Management Service, you associate the Management Service with a Management Repository. The Management Service uses the database host, database system identifier (SID), database port, management user, and management password to identify and communicate with the Repository.

This repository information is stored in the `emoms.properties` file, which can be found in the following directory where the Oracle Management Service is installed and deployed:

```
ORACLE_HOME/sysman/config/
```

The following sections describe how to modify the repository information in the `emoms.properties` file and provide details about how Enterprise Manager keeps the Management Repository password secure.

#### 20.2.1.1 Changing the Repository Properties in the emoms.properties File

To associate the Management Service with a new repository, you must modify the repository properties saved in the `emoms.properties` configuration file:

1. Stop the Management Service.
2. Locate the `emoms.properties` file in the following directory where you installed and deployed the Management Service:

   ```
   ORACLE_HOME/sysman/config/
   ```

3. Edit the `emoms.properties` file by updating the appropriate values for the properties described in Table 20–3.

   Example 20–1 shows sample entries in the `emoms.properties` file.

4. Restart the Management Service.

*Table 20–3 Repository Properties in the emoms.properties File*

| Property | Description |
|---|---|
| emdRepUser | The Management Repository user name. The default value is SYSMAN. |
| emdRepPwd | The Management Repository password. See "About Changing the Repository Password" on page 20-9 for information of how to change the password value. |
| emdRepConnectDescriptor | The Management Repository Oracle Net Connect String for the repository database. The values specified for properties emdRepSID, emdRepServer, and emdRepPort must be the same as that of HOST, PORT, and SERVICE_NAME in the connect string. If this property is not specified, then emRepSID, emRepServer, and emRepPort properties are used to construct the connect descriptor. If the database hosting the repository is a RAC database, then the value must be configured as explained in "Configuring the Management Services" on page 17-12 |
| emdRepSID | The System Identifier (SID) for the database where the Management Repository schema resides. |
| emdRepServer | The name of the server or host computer where the repository database resides. |
| emdRepPort | The port number for the repository database. |

*Example 20–1 Sample Repository Properties in the emoms.properties File*

```
oracle.sysman.eml.mntr.emdRepUser=SYSMAN
oracle.sysman.eml.mntr.emdRepPwd=sysman
oracle.sysman.eml.mntr.emdRepConnectDescriptor=(DESCRIPTION\=(ADDRESS_
LIST\=(ADDRESS\=(PROTOCOL\=TCP)(HOST\=system12.mycompany.com)(PORT\=1521)))
(CONNECT_DATA\=(SERVICE_NAME\=oemrep1)))
oracle.sysman.eml.mntr.emdRepSID=oemrep1
oracle.sysman.eml.mntr.emdRepServer=system12.mycompany.com
oracle.sysman.eml.mntr.emdRepPort=1521
```

### 20.2.1.2 About Changing the Repository Password

For security reasons, the password stored in the `emoms.properties` file is encrypted as soon as you start the Management Service. To change the repository password in the emoms.properties file, use the `emctl config oms change_repos_pwd` command line utility. This utility prompts you for the new password for the repository. When you press ENTER after supplying the password, the utility automatically updates the password.

To modify the repository password, do the following:

1. Stop the Management Service using the following command:

   ```
   ORACLE_HOME/bin/emctl stop oms
   ```

2. Change the repository in ORACLE_HOME/sysman/config/emoms.properties by using the following command:

   ```
   ORACLE_HOME/bin/emctl config oms change_repose_pwd
   ```

3. Restart the Management Service using the following command:

   ```
   ORACLE_HOME/bin/emctl start oms
   ```

## 20.2.2 Configuring the Management Service to Use a New Port

When you install the Management Service, the port number for the Management Service is automatically set to 4889. The following procedure describes how to manually change the port number after the Enterprise Manager installation. For example, you will have to modify the port number if you attempt to install two Oracle Management Services on the same host computer.

To change the default Management Service port:

1. Stop the Management Service.
2. Locate the following `httpd_em.conf` file located in the following directory in the home directory where you installed and deployed the Management Service:

   ```
   ORACLE_HOME/sysman/config/
   ```

3. Open the `http_em.conf` file with a text editor and change all occurrences of `4889` to the new port number you want to use.
4. Save and close the `http_em.conf` file.
5. Inform the DCM layer about the port change:

   ```
   ORACLE_HOME/dcm/bin/dcmctl updateconfig -ct ohs
   ```

6. Locate the `emoms.properties` file in the same `sysman/config` directory.
7. Open the `emoms.properties` file with a text editor and change the following entry so it references the new port number of the Management Service:

   ```
   oracle.sysman.emSDK.svlt.ConsoleServerPort=4889
   ```

8. Restart the Management Service.
9. Reconfigure each Management Agent on your managed hosts to use the new management port.

   > **See Also:** "Configuring the Management Agent to Use a New Management Service" on page 20-1

To change the default Management Service port to a *secure* port:

1. Stop the Management Service using:

   ```
   ORACLE_HOME/bin/emctl stop oms
   ```

2. Change the secure port using the following command:

   ```
   ORACLE_HOME/bin/emctl secure oms -secure_port <newPortNo>
   ```

3. Inform the DCM layer about the port change:

   ```
   ORACLE_HOME/dcm/bin/dcmctl updateconfig -ct ohs
   ```

4. Start the Management Service using:

   ```
   ORACLE_HOME/bin/emctl start oms
   ```

### 20.2.3 Configuring the Management Service to Prompt You When Using Execute Commands

The Execute Host Command and Execute SQL applications enable you to execute commands against multiple hosts and multiple databases respectively.

The default, when you click the Execute button of these applications, is for the command execution to begin immediately on the specified targets. If desired, you can set up the Management Service so that a confirmation page displays when you click the Execute button.

To enable the confirmation page for each application, perform the following:

1. Stop the Management Service.
2. Locate the `emoms.properties` file where you installed the Management Service:

   ```
   ORACLE_HOME/sysman/config/emoms.properties
   ```

3. Edit the `emoms.properties` file and add the appropriate lines:

   - For the Execute Host Command, add the following line:

     ```
     oracle.sysman.cmd.tgt.multiTarget.confirmExecuteHostCommand=true
     ```

   - For Execute SQL, add the following line:

     ```
     oracle.sysman.cmd.tgt.multiTarget.confirmExecuteSQL=true
     ```

   **Note:** The text in the commands is case-sensitive.

4. Save the changes and close the `emos.properties` file.
5. Restart the Management Service.

# 21

# Additional Configuration Tasks

This chapter contains the following sections:

- Understanding Default and Custom Data Collections
- Enabling Multi-Inventory Support for Configuration Management
- Manually Configuring a Database Target for Complete Monitoring
- Modifying the Default Login Timeout Value
- Configuring Clusters and Cluster Databases in Grid Control
- Collecting Client Configurations
- Setting Up and Configuring a Software Library With Oracle Enterprise Manager
- Configuring Privilege Delegation Providers

## 21.1 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 sections provide more information about how these settings are saved:

- How Enterprise Manager Stores Default Collection Information
- Restoring Default Collection Settings

### 21.1.1 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 10*g* Grid 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 default 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.

### 21.1.2 Restoring Default Collection Settings

If you have made modifications to the metric thresholds for a particular target, you can restore the default metric collection settings by deleting the customized collection information in the `sysman/emd/collection` directory.

For example, if you want to restore the default collections for a particular database target, remove the customized collection file for that target from the `sysman/emd/collection` directory. Enterprise Manager will begin using the metric collection information stored in the `sysman/admin/default_collection` directory.

## 21.2 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 for Windows and UNIX*

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:

1. Locate the `OUIinventories.add` file in the following directory:

   ```
   $ORACLE_HOME/<nodename>_<sid>/sysman/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 21.2.1, "AGENT_HOME Versus AGENT_STATE Directories" on page 21-3.

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 Grid 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.

### 21.2.1 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:

- 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 agent status` provides the values of the Management Agent's binaries and state locations.

## 21.3 Manually Configuring a Database Target for Complete Monitoring

When you first discover an Oracle Database 10g 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 10g target.

However, when you monitor an Oracle9*i* database or an Oracle8*i* database, there is some additional configuration required if you want to monitor certain types of database performance metrics using the Grid 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 Grid 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 Grid Control Console, return to the Database home page and verify that the Bad SQL and Top SQL Report metrics are now being gathered.

## 21.4 Modifying the Default Login Timeout Value

To prevent unauthorized access to the Grid Control Console, Enterprise Manager will automatically log you out of the Grid 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 Grid Control Console again.

**Caution:** As stated in the previous paragraphs, the timeout value for logging in to the Grid 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 Grid Control Console, regardless of the default timeout value.

## 21.5 Configuring Clusters and Cluster Databases in Grid Control

This section describes how to configure clusters, cluster databases, and discovering instances.

### 21.5.1 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

### 21.5.2 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 Grid 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 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 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

### 21.5.3 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

### 21.5.3.1 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 21.5.2, "Configuring Cluster Databases").

## 21.6 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.

## 21.6.1 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 Grid Control application pre-installed with Enterprise Manager or you can deploy CSA independently to your Web server.

### 21.6.1.1 Client System Analyzer in Oracle Grid Control

Client System Analyzer in Grid 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 Grid 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

### 21.6.1.2 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.

### 21.6.2 Configuration Parameters

The Client System Analyzer (CSA) can be further configured by modifying the context parameters in the CSA application's WAR file.

***Table 21–1 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 |
| 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"<br>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 |

*Table 21–1 (Cont.) Configuration Parameters*

| Parameter | Description | Default Value |
|---|---|---|
| customKey1<br>customKey2<br>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 |
| 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. |

*Table 21–1 (Cont.) Configuration Parameters*

| Parameter | Description | Default Value |
|---|---|---|
| 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. |
| 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.<br>**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 21–2 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.<br>If this parameter is not set, the user is directed back to the originally requested page |
| UIMode | 0 - synchronous (in the current browser window)<br>1 - asynchronous visible<br>2 - asynchronous invisible | synchronous |

#### 21.6.2.1 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.

### 21.6.3 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 21–1 followed by a description of each tag contained in the file.

***Example 21–1 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 21–1 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 21–3, 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 21–3 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.<br>**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.<br>**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 21–3 (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

## 21.6.4 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.

## 21.6.5 CSA Deployment Examples

The following sections outline sample use cases for client configurations.

### 21.6.5.1 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 21–2.
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 21–2 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 21–2 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 21–2, 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 21–2, 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.

### 21.6.5.2 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 21–2, 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 Grid Control link on the Setup page. Super users can view all client configurations regardless of any collection tag associations.

#### 21.6.5.3 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 21–3.

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 21–3. 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 21–3 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.

#### 21.6.5.4 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 Grid 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.

### 21.6.5.5 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.

#### 21.6.5.5.1 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`.

#### 21.6.5.5.2 Example 2: Inventory

In Example 21–4, 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 21–4 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".

#### 21.6.5.5.3 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 21–5 displays the context parameter values for the CSA servlet filter on the sales portal.

***Example 21–5 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 21–6 represents the context parameter definitions to map rules to collection tags.

***Example 21–6 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>
```

## 21.7 Setting Up and Configuring a Software Library With Oracle Enterprise Manager

The following sections describe how to set up and configure a software library using Oracle Enterprise Manager.

### 21.7.1 Setting Up a Software Library

The software library should be located in a directory accessible by all Oracle Management Servers (OMS). If there is only one OMS, the directory can be local. For multiple OMS environments, the directory can ge on a Network File Server accessible from all Oracle Management Servers. You should ensure that there is sufficient space available on the shared storage to store file that hold the binary data for all of the components.

If you create operating system components, TAR files containing all the RPMs for a Linux installation will be stored in the software library. If you create Oracle database components, TAR files containing all the files from a reference Oracle home directory or contents from the installable media will be stored in the software library.

You should ensure that the shared storage is accessible through NFS mount points to all Oracle Management Servers in the environment.

### 21.7.2 Configuring a Software Library

The graphical user interface of the Provisioning application shows various tabs for Components, Directives, and Images. You can access all of the tabs depending on the privileges assigned to you. For example, if you have superuser privileges, you can access the Administration tab. The Administration tab contains different sections that you can use to configure various elements in the environment.

To configure a software library, follow these steps:

1. In the Software Library Configuration section of the Administration tab of the Provisioning application, press the **Add** button.
2. On the Add Software Library Location page, enter the directory location of the software library you are creating and then click **OK**.

### 21.7.3 Deleting or Cleaning Up a Software Library

To delete the software library , select the software library from the Administration tab and click Remove to delete it.

To delete the components of a software library, select the components from the software library and choose Delete. This will remove the components. To clean up the delete components completely from the File System , you must run the following command:

```
<OMS HOME>/bin/purgeDeploymentLibrary <conn string> <username>
<password> [-job <oms_host>
```

The options for this command are listed below:

<*conn string*> is of form: "jdbc:oracle:thin:@dbhost:dbport:sid" where dbhost, dbport and sid should be replaced appropriately

<*username*> is repository username

<*password*> is repository passwd

*[-job <oms_host>]* is optional; if provided a job would be submitted (schedule is immediate). The user can view the status of the job by navigating to the Jobs page on the Enterprise Manager console.

<*oms_host*> is OMS hostname

## 21.8 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 (EM CLI), 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.

## 21.8.1 Creating a Privilege Delegation Setting

A privilege delegation setting can be created using the EM CLI command line interface's `create_privilege_delegation_setting` verb.

> **Note:** You can 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 page and then choosing **Manage Privilege Delegation Settings** from the left menu panel.

### 21.8.1.1 Creating a Sudo Setting Using EM CLI

Use the `create_privilege_delegation_setting` EM CLI verb to create a sudo privilege delegation setting. For explicit syntax and examples, see EM CLI command line help or the *Oracle Enterprise Manager Command Line Interface* guide.

**Variables**

You can used the following variables when using EM CLI to set the privilege delegation settings. Variables are case-sensitive.

| Variable | Definition |
|---|---|
| %PASSWORD% | Password of the user running the command. |
| %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 EM CLI to create a sudo setting. Here, sudo is installed in `/opt/sudo/bin`.

***Example 21–7 Using EM CLI 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%"
```

### 21.8.1.2 Creating a PowerBroker Setting Using EM CLI

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 EM CLI to set the privilege delegation settings. Variables are case-sensitive.

| Variable | Definition |
|---|---|
| %PASSWORD% | Password of the user running the command. |
| %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=powerbroker_setting_1 -setting_type=POWERBROKER
-settings="SETTINGS:<command to be used with all the
options>;[PASSWORD_PROMPT_STRING,<password prompt for
PowerBroker>]"
```

***Example 21–8 Using EM CLI 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:".

## 21.8.2 Applying Privilege Delegation Setting

Once you have created a privilege delegation setting, you must apply this setting to selected targets. As with the setting creation process, you use EM CLI 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).

> **Note:** You can apply a Privilege Delegation setting by clicking **Setup** on the Enterprise Manager page and then choosing **Manage Privilege Delegation Settings** from the left menu panel.

### 21.8.2.1 Applying Settings to Host Targets

Use the `apply_privilege_delegation_setting` EM CLI 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 21–9 Using EM CLI 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
```

#### 21.8.2.2 Applying Settings to a Composite Target

Use the `apply_privilege_delegation_setting` EM CLI 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 21–10 Using EM CLI 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 EM CLI or through the Grid Control console.

### 21.8.3 Disabling Host Privilege Delegation Provider Settings

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
   ```

> **Note:** You can disable a Privilege Delegation setting by clicking **Setup** on the Enterprise Manager page and then choosing **Manage Privilege Delegation Settings** from the left menu panel.

### 21.8.4 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.

# Part V

# Upgrading Enterprise Manager Grid Control

This part provides step-by-step instructions to upgrade Enterprise Manager Grid Control.

This part contains the following chapter:

# 22 Upgrading Enterprise Manager Grid Control

This chapter describes how an existing Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release can be upgraded to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) or higher. For example, you can use the instructions outlined in this chapter to upgrade an existing Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) for Linux to Enteprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux.

A *full release* refers to the first, complete, base Enterprise Manager 10g Grid Control software that was released for a particular platform. A full release comprises all three components that form Enteprise Manager Grid Control, mainly OMS, Oracle Management Repository, and Oracle Management Agent. For more information about full releases, see Section 4.1, "Understanding What This Guide Helps You Install and Upgrade".

With the option of deploying the Enterprise Manager Grid Control (Grid Control) environment across the enterprise and in any number of permutations, upgrading the entire environment becomes a very complex activity involving updating of software and configurations in different levels (tiers) located in different machines.

The Grid Control Upgrade process aims at simplifying this entire operation and rendering it as seamless and error-free as possible.

**Caution:**

This chapter helps you *upgrade* an Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) or higher.

This chapter does not deal with *patching* procedures that help you patch a release of Enterprise Manager 10g Grid Control. For example, patching any 10.2.0.1 release to 10.2.0.2 release. Although there is basic information in this chapter, the actual patching procedures are furnished in the Patch Set Notes document that is packaged with the Patch Set, not in this guide. You can download the Patch Sets and the relevant Patch Set Notes from My Oracle Support (formerly Metalink).

The following topics are covered in this chapter:

- Software Prerequisites
- Checks to Be Performed Before Starting the Upgrade Process
- Manual Configuration to Be Performed for Upgrade
- Upgrade Scenarios

- Grid Control Upgrade

## 22.1 Software Prerequisites

Enterprise Manager 10g Grid Control Release 2 (10.2.x.x) installer upgrades only the corresponding Enterprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher components. Table 22.1 lists the supported component versions:

*Table 22–1 Supported Component Versions that Correspond to the Installation Type*

| Installation Type | OMS Version | Database Version |
|---|---|---|
| Enterprise Manager Using New Database | 10.1.0.4 and higher (with Application server 9.0.4) | 9.0.1.5 |
| Enterprise Manager Using Existing Database | 10.1.0.4 and higher (with Application server 9.0.4) | 9.2.0.6 or higher |
| Additional Management Service | 10.1.0.4 and higher (with Application server 9.0.4) | containing the 10.1.0.4 or higher OMS schema |
| Additional Management Agent[1] | Not Applicable | Not Applicable |

[1] The supported Management Agent version is 10.1.0.3 and higher.

## 22.2 Checks to Be Performed Before Starting the Upgrade Process

This section lists the checks you must perform before starting any of the Enterprise Manager 10 Grid Control Release 2 (10.2.x.x) upgrade scenarios as discussed in the following sections.

### 22.2.1 Shut Down Grid Control Before Upgrade

You must ensure that the existing Grid Control processes are shut down before starting the upgrade process.

To shut down Grid Control, execute the following commands:

```
<OMS Oracle_Home>/opmn/bin/opmnctl stopall
<AGENT_HOME>/bin/emctl stop agent
<OMS Oracle_Home>/bin/emctl stop em
```

> **Note:** Ensure you shut down all instances of the OMS that are uploading to the same repository.

These commands usually successfully shut down all Grid Control processes that are running. However, there may be instances where some processes might still be left running. Such instances may cause the upgrade to fail. To avoid this, you must ensure the following processes are not running before attempting to start the upgrade process:

- OPMN
- DCM

> **Note:** Ensure that all OMS instances uploading to the same repository are shut down before the upgrade. Such OMS instances must be upgraded simultaneously.

### 22.2.2 Check for Symbolic Links

The `<Oracle_Home>/Apache/<component>` configuration files must be examined to ensure only hard links (and *no symbolic links*) were referenced.

As part of the Enterprise Manager 10*g* Release 2 (10.2) Upgrade from 10.1, the underlying Oracle9*i*AS release 9.0.4 stack is also upgraded. During this phase, the upgrade utility attempts to replace the 10*g* Release 1 Oracle home path that is referenced in these configuration files with the new Enterprise Manager 10*g* Release 2 `ORACLE_HOME` path.

If you have customized the Oracle9*i*AS release 9.0.4 stack using symbolic links to the Oracle home, then the configuration files may also contain these references as symbolic links, instead of the complete path of the Oracle home.

For example, `<Oracle_Home>/Apache/modplsql/conf/plsq.conf` contains references to the `plsql_module`. If this path is a symbolic link, you must modify this path to be a hard link.

### 22.2.3 Customizations and User Permissions

If there have been any middle-tier customizations files that cannot be accessed using the upgrade user's credentials, ensure such customizations are removed or commented out before starting the upgrade. You can reapply these customizations after the upgrade is successfully completed.

Also ensure you (use performing the upgrade) have read and write permissions on `/temp/em`.

### 22.2.4 Recompile EMD_MAINTENANCE for Manually Upgraded Databases

If you have previously upgraded the database (from 9*i* to 10*g*) manually, you must recompile the `EMD_MAINTENANCE` package. To do this:

1. Shut down the OMS that is associated with the database.
2. Execute SQLPLUS into the upgraded database as SYSMAN.
3. Execute alter package EMD_MAINTENANCE COMPILE BODY; ensure this package has been recompiled successfully.
4. Now, start the OMS.

### 22.2.5 Verify Inventory.xml for Oracle Home Path

Ensure the `<Oracle_Inventory>/ContentsXML/inventory.xml` file to make sure the Oracle home path is the same as the components that you are upgrading.

**Note:** These paths must always be hardlinks.

### 22.2.6 Select an Agent That Is Not Secure

During the upgrade process, you can choose not to specify the Agent Registration password. This leaves the upgraded agent unsecure. The installer displays an error message when the agent's `REPOSITORY_URL` does not match with that of the OMS, indicating the agent is not bound to the OMS.

This can happen if multiple OMSs are grouped together through a load balancer, and the agent is using this load balancer to communicate with the OMSOMS.

You can also choose to secure the upgraded agent manually after the agent has been upgraded.

## 22.2.7 Shut Down Database Listener (UNIX Only)

If the current Enterprise Manger installation (10*g* Release 1) was performed using a new database, the 10*g* Release 2 (10.2) upgrade process will first attempt to upgrade Oracle Database if it has not already been upgraded manually.

In an Enterprise Manager Grid Control 10*g* Release 1 (10.1) installation using a new database, the installer performs a release 9.0.1.5 Oracle Database installation along with the other Grid Control components. When you upgrade Grid Control release 10.1 to release 10.2, the database instance is upgraded to a release 10.1.0.4 before the Grid Control migration configuration is performed.

To successfully migrate your existing Grid Control to release 10.2, the new 10.1.0.4 database listener has to be started. To do this, you must simply stop the old (release 9.0.1.5) database listener **just prior** to executing the `allRoot.sh` script.

After you stop the old listener and execute the `allRoot.sh` script, the release 10.1.0.4 listener will be started automatically.

**WARNING: Do not shut down the database listener if you are attempting to upgrade a Grid Control installation that was performed using an existing database. The upgrade will fail if the database listener is shut down.**

**Note:** On *Microsoft Windows*, you must modify the start-up type value of the old listener to *Disable*, and the start-up type value of the new listener to *Automatic* after the upgrade process is complete.

### 22.2.7.1 Impact on Firewall Ports and Software Load Balancers

During a Grid Control upgrade from 10g R1 to 10g R2, there will be some modifications to the default port values.

For example, port 1158 will no longer be used for communications between the OMS and the agent. similarly, the default port for the OMS and agent communications will now (in 10*g* R2) be 3872 and not 1830 (as in 10*g* R1) though the 1830 port will still be valid.

The Grid Control upgrade operation will preserve the ports that were being used in the original deployment. Hence, additional ports will not be required even if Grid Control was originally deployed with a firewall.

Similarly, you will not have to perform any modifications to the software load balancer (SLB) configurations after the Grid Control upgrade.

## 22.2.8 Verify Partitioning of Database

Ensure that the database where the Management Repository is configured has the *Partitioning Option* enabled. To verify this, connect to the database as SYSDBA and run the following query:

```
SQL> select value from v$option where parameter =
‘Partitioning’;
```

The result of this query should be `VALUE=TRUE`.

> **Note:** No additional partitioning license is required for Oracle Database that houses the Management Repository.

### 22.2.9 Back Up the Repository

Before you begin any upgrade or patching process, ensure that you back up the database. This helps you maintain a copy of the database that was existing before the environment was upgraded and it naturally gives you the flexibility to revert to it whenever you want.

### 22.2.10 Configuring SUDO

Before you begin any upgrade or patching process, configure SUDO in your environment. If you are unable to configure SUDO in your environment or if you have already upgraded any of the core components (OMS or Management Agent) without configuring SUDO, then follow the workaround described in *My Oracle Support* note 789363.1.

## 22.3 Manual Configuration to Be Performed for Upgrade

The following sections explain the configuration tasks to be performed for upgrading Enteprise Manager 10g Grid Control Release 1 (10.1.0.4 or higher) to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x or higher).

Also explained are tasks to be performed for patching Enterprise Manager 10g Grid Control Release 2. For example, tasks to be performed before migrating from Enterprise Manager Grid Control 10.2.0.1 (Linux) to 10.2.0.2 (Linux) or higher.

> **Caution:** This section does not deal with *patching* procedures that help you to migrate from one patch release of Enterprise Manager 10g Grid Control to another. For example, patching any 10.2.0.1 release to 10.2.0.2 release. Although there is basic information in this section, the actual patching procedures are furnished in the Patch Set Notes document that is packaged with the Patch Set. You can download the Patch Sets and the relevant Patch Set Notes from My Oracle Support (formerly Metalink).

### 22.3.1 Upgrading from 10.1.0.4 (or higher) to 10.2.x.x

The following sections describe how you can upgrade Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) or higher.

#### 22.3.1.1 PreUpgrade Tasks

The following steps describe the tasks to be performed *before* upgrading Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) or higher. For example, *before* upgrading an existing Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) for Linux to Enteprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux.

> **Note:** Before you begin any upgrade process, ensure that you back up the database.

1. Shutdown all OPMN processes and agents.
2. Perform Grid Control partition cleanup. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following command:

   ```
   SQL>exec emd_maintenance.partition_maintenance;
   ```

3. Apply fix for index/constraint issues. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following commands:

   ```
   SQL>Alter table MGMT_JOB_TYPE_INFO disable constraint PK_JOB_TYPE_INFO cascade
   drop index;
   SQL>Alter table MGMT_JOB_PARAMETER disable constraint PK_MGMT_JOB_PARAM cascade
   drop index;
   SQL>Alter table MGMT_TARGET_PROP_DEFS  disable constraint MGMT_TARGET_PROP_
   DEFS_PK cascade drop index;
   SQL> Alter table mgmt_license_definitions  disable constraint mgmt_license_
   definitions_pk cascade drop index;
   SQL> ALTER TABLE mgmt_annotation DISABLE CONSTRAINT mgmt_annotation_pk cascade
   drop index;
   ```

4. Check and enable the queue MGMT_NOTIFY_Q if it is not enabled. To do this, log into the database using SQLPLUS with SYSMAN credentials. At the SQL> prompt, execute the following commands:

   ```
   SQL> select OWNER, NAME, ENQUEUE_ENABLED from dba_queues where name='MGMT_
   NOTIFY_Q';
   If ENQUENE_ENABLED is NOT "YES", then
   exec dbms_aqadm.start_queue(queue_name => 'SYSMAN.MGMT_NOTIFY_Q');
   ```

#### 22.3.1.2 Upgrade Tasks

The following steps describe the tasks to be performed *for* upgrading Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) or higher release to a full release of Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) or higher. For example, *for* upgrading an existing Enteprise Manager 10g Grid Control Release 1 (10.1.0.4) for Linux to Enteprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux.

1. Using the shiphome, invoke OUI with -noconfig option as follows:

   ```
   ./runInstaller -noconfig
   ```

2. When prompted for upgrade options, choose both OMS and Agent for upgrade. Enter valid input values for the installation. OUI will perform a software-only install as described in Section 22.5, "Grid Control Upgrade".
3. After the software-only install, replace the pre_post_creation.sql file that is available in the upgraded release's directory with the pre_post_creation.sql extracted from the patch for bug# 5666424.

   For example, if you are upgrading from 10.1.x.x to 10.2.0.1, then replace the `$ORACLE_HOME/sysman/admin/emdrep/sql/core/v102010/pre_post_creation.sql` file with the `pre_post_creation.sql` file extracted from the patch for bug# 5666424.

4. Run the following command to launch the Configuration tool to complete the upgrade.

   If the older OMS was installed using "Enterprise Manager 10g Grid Control Using an Existing Database' install type or if it was an additional OMS installation, then run the following command:

   ```
   $NEW_OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS HOME> MODE=perform
   ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_0.xml}
   ```

   If the older OMS was installed using "Enterprise Manager 10g Grid Control Using a New Database", then run the following command:

   ```
   $NEW_OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS HOME> MODE=perform
   ACTION=configure COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
   ```

## 22.3.2 Patching 10.2.x.x and Migrating to Another Patch Set Release of 10.2.x.x

The following sections describe the tasks to be performed for patching Enteprise Manager 10g Grid Control Release 2 (10.2.x.x).

### 22.3.2.1 PrePatching Tasks

The following steps describe the tasks to be performed *before* patching Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) to another patch set release of 10.2.x.x. For example, *before* patching the existing Enteprise Manager 10g Grid Control Release 2 (10.2.0.1) for Linux to Enteprise Manager 10g Grid Control Release 2 (10.2.0.2) for Linux, using the 10.2.0.2 patch set that was released for Linux.

> **Note:** Before you begin any upgrade process, ensure that you back up the database.

1. Using the 10.2.x.x Grid Control Patch Set, invoke OUI with -noconfig option as follows:

   ```
   ./runInstaller -noconfig
   ```

   OUI will perform a software only install.

2. After the software only install, replace the `pre_data_upgrade.sql` file available in the upgraded release's directory with the `pre_data_upgrade.sql` file extracted from the patch for bug# 5666424.

   For example, if you are patching 10.2.0.1 Linux to 10.2.0.2 Linux, then replace the `$ORACLE_HOME/sysman/admin/emdrep/sql/core/v102020/pre_data_upgrade.sql` file with the `pre_data_upgrade.sql` file extracted from the patch for bug# 5666424.

3. Run the following command to launch the Configuration tool to complete the upgrade.

   ```
   OMS_HOME/oui/bin/runConfig.sh ORACLE_HOME=<OMS_HOME> ACTION=patchsetConfigure
   MODE=perform RERUN=true COMPONENT_XML={oracle.sysman.top.oms.10_2_0_x_0.xml}
   ```

> **Also:** To prepare yourself better for a patching operation, Oracle recommends you to read the patching checklist that is available as Document ID 464674.1 on My Oracle Support (formerly Metalink) at:
>
> `http://metalink.oracle.com/`

#### 22.3.2.2 Patching Tasks

For patching Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) to another patch set release of 10.2.x.x, follow the installation/patching steps provided in the Patch Set Notes or Release Notes that is packaged with the 10.2.x.x Patch Set.

When you patch multiple OMSs, after the first OMS gets patched, it restarts itself automatically, leaving the other OMSs shut down. At this point, DO NOT restart the other OMSs until you apply the latest patch on them.

> **Note:** While patching the install types "*Enterprise Manager Grid Control Using a New Database*" and "*Enterprise Manager Grid Control Using an Existing Database*" to 10.2.0.4, you might have to apply the RDBMS patch 4329444. However, this patch might conflict with some previous CPU releases (for example, April 2007 CPU) that might be applied to your repository database.
>
> In case of a conflict while applying patch 4329444, DO NOT continue with the patching process. Contact Oracle support to first resolve the patch conflict and then follow the steps outlined in the *Oracle Enterprise Manager Grid Control Release Notes for Linux and Microsoft Windows 10g Release 4 (10.2.0.4.0)* available in the document library at:
>
> `http://www.oracle.com/technology/documentation/oem.html`

#### 22.3.2.3 PostPatching Tasks

After patching any Enteprise Manager 10g Grid Control Release 2 (10.2.x.x) to another patch set release of 10.2.x.x, ensure that you download the *Clone Support Files* from My Oracle Support (formerly Metalink) and install them on each OMS. This is to enable clone support for many major releases of Oracle Tech stack components. The *Clone Support Files* are available on My Oracle Support (formerly Metalink) as one-off patches.

The concept of *Cloning* in Grid Control helps you clone any installed Oracle home that is recognized as a clonable home by Grid Control. This means you can clone the installed Oracle homes of most Oracle products as is, without having to install any additional support files. Table 22–2 shows the Oracle products that can be cloned as is. However, there may be Oracle homes that are not recognized as clonable homes by Grid Control. For such Oracle homes, you must patch Grid Control with appropriate *Clone Support Files* before starting the cloning operation.

The following Oracle products can be cloned as is, without *Clone Support Files*. Any other Oracle home that is not mention in this table needs Cloning Support Files.

***Table 22–2 Oracle Products That Can Be Cloned As Is***

| Oracle Product | Release |
|---|---|
| Oracle Database | 10.1.x and 10.2 |
| Oracle RAC Database | 10.1.x and 10.2 |
| Application Server | 10.1.2.0.0, 10.1.2.0.2 |
| Oracle Clusterware | 10.2 |

To locate these *Clone Support Files* at My Oracle Support (formerly Metalink):

1. Access `http://metalink.oracle.com/` and navigate to the **Advanced Search** option under **Patches and Updates**.
2. Select the **Enterprise Manager Grid Control** (emgrid) product from the list.
3. Select the appropriate release, platform, and patch type.
4. Enter "Clone Support Files" in the **Description** field, and click **Search**. The Patch Release Notes include instructions for installing the updated clone support files in the OMS home.

## 22.4 Upgrade Scenarios

The following upgrade scenarios are discussed in this section:

- Upgrading Oracle Management Service that Is Installed Using a New Database
- Upgrading Management Service that Is Installed Using an Existing Database
- Upgrading the Oracle Management Service
- Upgrading the Management Agent

**Caution:**

- During the upgrade process, you must ensure the monitoring agent is also upgraded along with the OMS and repository database
- Ensure that you back up the database before upgrading your environment.
- Unless you are instructed, DO NOT remove or modify any of the OMS files.

### 22.4.1 Upgrading Oracle Management Service that Is Installed Using a New Database

If the Enterprise Manager 10*g* Release 1 (10.1) was of this installation type, then the 10*g* Release 2 (10.2) installer performs an out-of-place upgrade of the release 10.1 OMS, the repository database, and the agent Oracle homes. During the upgrade, the installer creates a new Oracle home for the OMS, Management Repository, and Management Agent. The upgrade assistants upgrade the datafiles and `SYSMAN` schema, and then configure the new Oracle homes.

**Caution:** Before you start the upgrade process on Microsoft Windows, ensure the parameter `SQLNET.AUTHENTICATION_SERVICES` value is NTS (`SQLNET.AUTHENTICATION_SERVICES=NTS`). If this is not done, the Database Upgrade Assistant will fail.

You must also ensure that the listener is running, and the SQL command (`sqlplus "/as sysdba"`) is connecting to the database.

### 22.4.2 Upgrading Management Service that Is Installed Using an Existing Database

If the earlier Grid Control installation was done using an existing database, the 10*g* Release 2 installer automatically checks the remote database version (must be release 9.2.0.6 or later). If the minimum database version requirement is met, the installer not only performs an upgrade of the OMS but also upgrades the SYSMAN schema in the remote database.

**Note:** If the database version is lower than release 9.2.0.6, this database is not upgraded as part of the Grid Control upgrade process. You are required to upgrade the database separately, before proceeding with the OMS upgrade process.

**Caution:** If you are upgrading a Grid Control target (for example, database) using an upgrade mechanism other than Oracle Universal Installer, the agent you have selected must also be part of the same installation (is the agent associated with that OMS). See Section A.4.4, "Monitoring Agent Does Not Discover Upgraded Targets" for more information.

### 22.4.3 Upgrading the Oracle Management Service

If the previous Grid Control installation was for an additional OMS, the 10*g* Release 2 installer checks the remote database (must be release 9.2.0.6 or later). If this minimum database release requirement is met, the installer performs the Management upgrade.

If you are upgrading only the OMS to 10*g* Release 2 (10.2) without upgrading the monitoring agent (agent associated with that OMS), you may encounter a metric collection error. To resolve this issue, you must upgrade the monitoring agent to 10*g* Release 2 as well.

Oracle recommends upgrading the OMS and the associated (monitoring) agent at the same time.

**Caution:** Ensure you shut down the OMS that you are going to upgrade, and its associated (monitoring) agent before starting the upgrade process.

**Note:** If the database release is earlier than 9.2.0.6, this database is not upgraded as part of the Grid Control upgrade process. You are required to upgrade the database separately, before proceeding with the OMS upgrade process.

**Caution:** After successfully upgrading the 10*g* Release 1 (10.1.0.4) OMS to release 10.2, the 10.1.0.4 agents that are uploading data to this OMS may show an incorrect OMS version when you execute `./emctl status agent`.

To resolve this issue, you must stop the 10.1.0.4 agents (`./emctl stop agent`) and restart them (`./emctl start agent`).

### 22.4.4 Upgrading the Management Agent

All agent Oracle homes that need to be upgraded are detected and displayed in the Select Install or Upgrade screen of the installer. You can select the agent Oracle homes that you want to upgrade and proceed with the process.

**Note:** The agent Oracle homes that are installed as part of the first two installation types are not upgraded automatically along with the OMS Oracle homes. You must select the agent home that you want to upgrade. This agent home can be independent of the OMS home.

#### 22.4.4.1 Upgrading 10.1.0.4 Agents that Monitor User-Defined Metrics

Because the Management Agent upgrade process is an out-of-place[1] installation, upgrading an agent will create a new agent Oracle home directory. If you are using OS-based user-defined metrics that are referencing scripts located in an agent Oracle home, then such scripts will not be copied over during the upgrade process. Specifically, if a release 10.1.0.4 agent is being upgraded to release 10.2 agent, any user-defined metric scripts that may have existed in the 10.1.0.4 agent Oracle home will not be copied into the new 10.2 agent Oracle home.

In order to ensure the user-defined metrics continue to work the same, you must manually copy all user-defined metrics scripts into another directory (outside any Oracle home), and then update the user-defined metric definitions to reflect the new script location.

For example, if the user-defined script is called `myScript.sh` and is located in the 10.1.0.4 agent Oracle home (for example, `/u1/oracle/sysman/admin/scripts` directory), copy this script over to a new directory (for example, `/u1/scripts`). Now, in the definition of the user-defined metric, you must change the command line from `/u1/oracle/sysman/admin/scripts/myScript.sh` to `/u1/scripts/myScript.sh`.

**Note:** Ensure you do not delete the original Oracle home (that is 10.1.0.4 Oracle home in the preceding example) until you have changed the user-defined metric script location.

## 22.5 Grid Control Upgrade

When you invoke Oracle Universal Installer to perform an upgrade, it automatically detects the existing Grid Control installation type of the target Oracle homes and displays the components that need to be upgraded. You can select the component that you want to upgrade and proceed with the process.

**Caution:** Oracle recommends that you perform a backup of the repository before starting the upgrade process.

### 22.5.1 Upgrading Enterprise Manager Grid Control Using Oracle Universal Installer

To upgrade  Grid Control using Oracle Universal Installer (OUI), follow these steps:

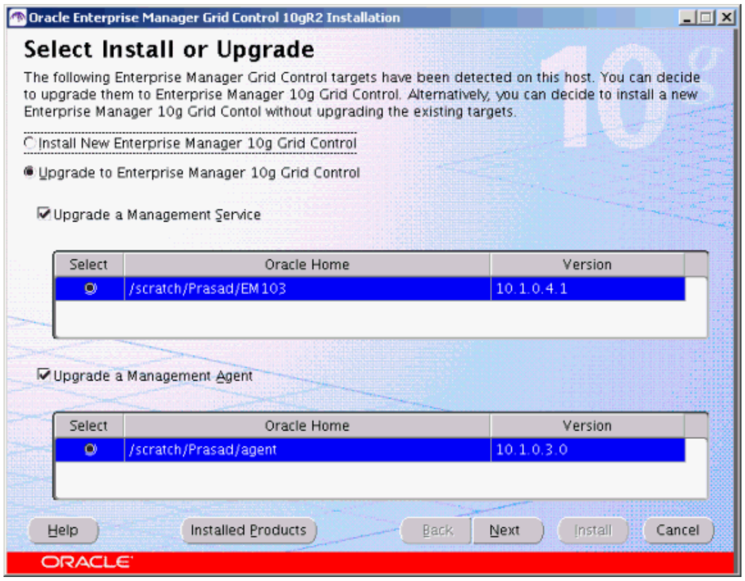
[1] Out-of-place upgrade refers to the process of installing the software in a new Oracle home. All the data and configuration files from an existing Oracle home are retrieved and migrated to the new Oracle home. After the upgrade is complete, the old Oracle home is discarded and the software can be started from the new Oracle home.

1. Start Oracle Universal Installer by running the `runInstaller` script in Linux (go to the top-level folder in the contents copied from the DVD and execute `./runInstaller` or `setup.exe` on Microsoft Windows) from the top directory of Disk1.
2. When you invoke Oracle Universal Installer, you will be presented with two choices:
   - a. Perform a new Enterprise Manager Grid Control installation

     See Section 8.1, "Understanding the Installation Types" for more information.
   - b. Products Upgrade

     Select this option to continue with the upgrade process.
3. Click **Products Upgrade**. The Select Install or Upgrade screen appears.

***Figure 22–1 Select Install or Upgrade***



Oracle Enterprise Manager Grid Control 10gR2 Installation

**Select Install or Upgrade**

The following Enterprise Manager Grid Control targets have been detected on this host. You can decide to upgrade them to Enterprise Manager 10g Grid Control. Alternatively, you can decide to install a new Enterprise Manager 10g Grid Contol without upgrading the existing targets.

○ Install New Enterprise Manager 10g Grid Control

● Upgrade to Enterprise Manager 10g Grid Control

☑ Upgrade a Management Service

| Select | Oracle Home | Version |
|---|---|---|
| ● | /scratch/Prasad/EM103 | 10.1.0.4.1 |

☑ Upgrade a Management Agent

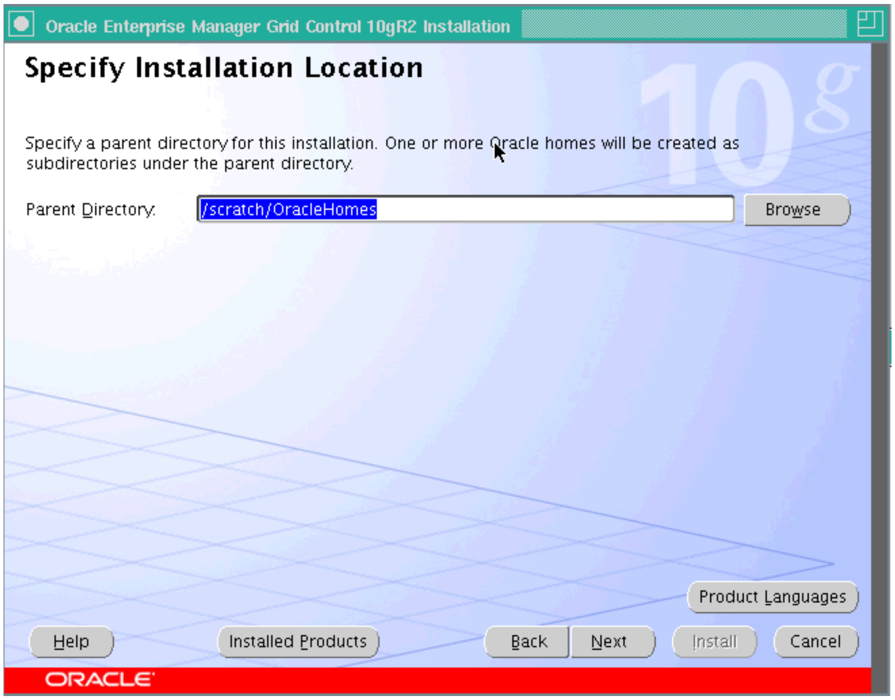
| Select | Oracle Home | Version |
|---|---|---|
| ● | /scratch/Prasad/agent | 10.1.0.3.0 |

4. The installer automatically detects the Grid Control components that require an upgrade and lists them in this screen.
5. Here, you can choose to perform the following upgrades:
   - a. OMS and the associated (monitoring) Management Agent
   - b. Only the OMS
   - c. Only the Management Agent

> **Caution:** If you are upgrading both OMS and Agent (which is part of a chain agent installation), ensure the agent you have selected is the one that is communicating with selected OMS.
>
> Also, ensure you shut down the agent and the OMS that you are going to upgrade, before starting the process.

6. Select the Oracle homes that you want to upgrade and click **Next**. The Specify Installation Location screen appears.

*Figure 22–2 Specify Installation Location*



Oracle Enterprise Manager Grid Control 10gR2 Installation

Specify Installation Location

Specify a parent directory for this installation. One or more Oracle homes will be created as subdirectories under the parent directory.

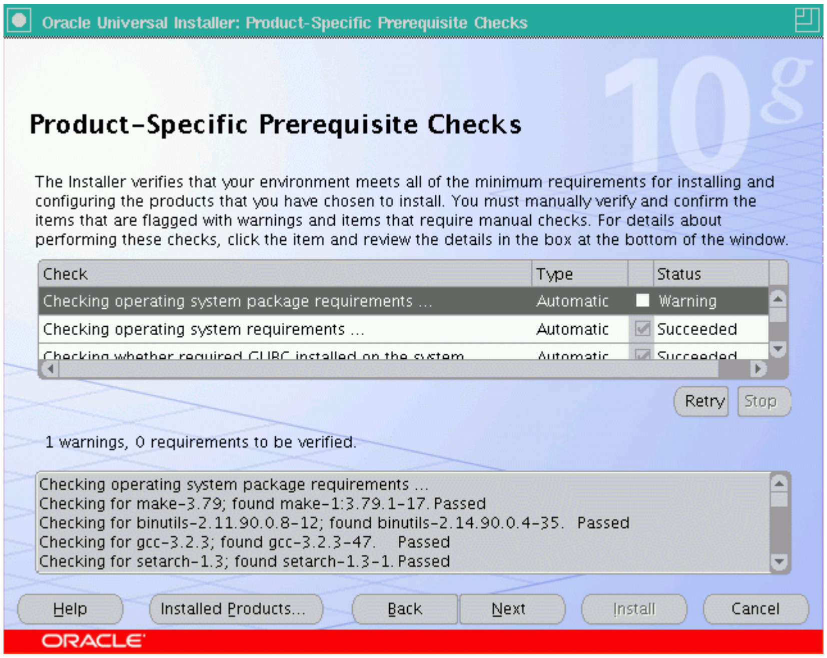
Parent Directory: /scratch/OracleHomes

Here, specify a parent directory (base directory), for example, `/scratch/OracleHomes`, for the new installation. because the installer is going to perform an out-of-place[2] upgrade, all the Oracle homes created during the upgrade will be placed as subdirectories under this parent directory.

7. Click **Next**. The Product-Specific Prerequisite Checks screen appears.

[2] Out-of-place upgrade refers to the process of installing the software in a new Oracle home. All the data and configuration files from an existing Oracle home are retrieved and migrated to the new Oracle home. After the upgrade is complete, the old Oracle home is discarded and the software can be started from the new Oracle home.

*Figure 22–3 Product-Specific Prerequisite Checks*


Oracle Universal Installer: Product-Specific Prerequisite Checks
10g
Retry
Stop
Help
Installed Products...
Back
Next
Install
Cancel
ORACLE

Product-Specific Prerequisite Checks

The Installer verifies that your environment meets all of the minimum requirements for installing and configuring the products that you have chosen to install. You must manually verify and confirm the items that are flagged with warnings and items that require manual checks. For details about performing these checks, click the item and review the details in the box at the bottom of the window.

| Check | Type | Status |
|---|---|---|
| Checking operating system package requirements ... | Automatic | □ Warning |
| Checking operating system requirements ... | Automatic | ☑ Succeeded |
| Checking whether required GLIBC installed on the system | Automatic | ☑ Succeeded |

1 warnings, 0 requirements to be verified.

```
Checking operating system package requirements ...
Checking for make-3.79; found make-1:3.79.1-17. Passed
Checking for binutils-2.11.90.0.8-12; found binutils-2.14.90.0.4-35.   Passed
Checking for gcc-3.2.3; found gcc-3.2.3-47.    Passed
Checking for setarch-1.3; found setarch-1.3-1. Passed
```

a. At this point, the installer runs some prerequisite checks to verify whether or not the environment meets the minimum requirements for a successful Enterprise Manager installation.

   Early detection of problems with the system setup reduces the chances of you encountering problems during installation; for instance, problems with insufficient disk space, missing patches, inappropriate hardware, and so on.

   This page displays the check name, type, and status for all prerequisite checks designed for the installation. Automatic checks are run first, followed by optional and manual checks.

   Depending on the status of the automatic checks, you must verify all warning and manual checks. At some point, if you have stopped the prerequisite check and want to rerun these checks, select the checks that you want to rerun and click **Retry**. As each check runs, a progress bar is shown, and test details (expected results, actual results, error messages, instructions) are displayed in the details section, at the bottom of the page.

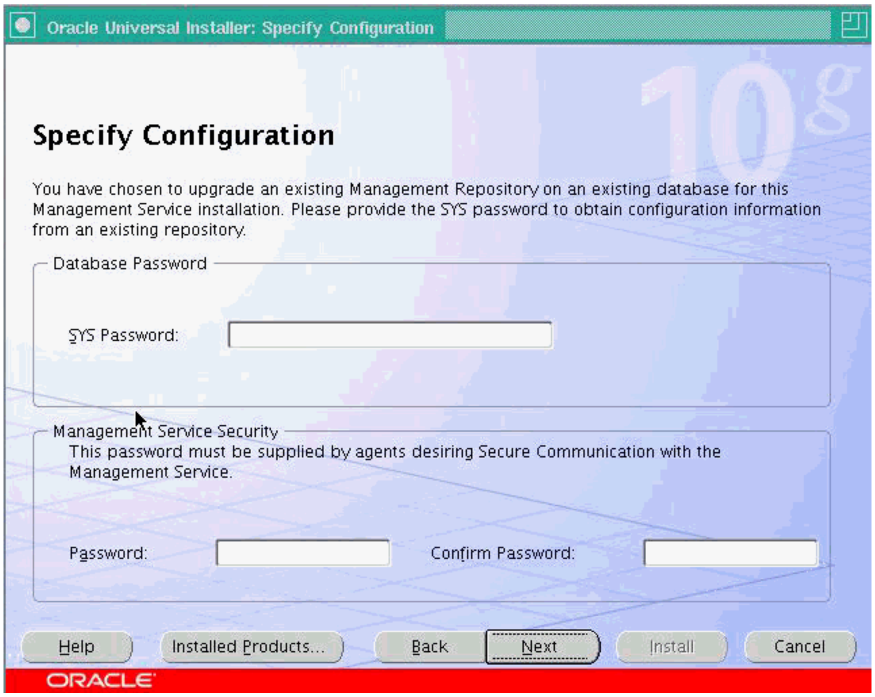
b. To stop all prerequisite checks, click **Stop**. At any point of time, click a prerequisite check to view its corresponding details, including the recommended user actions.

   **Note:** You must manually verify and confirm all checks that were flagged with a warning, skipped (stopped by user), or failed.

c. To continue with the installation without retrying, click **Next**.

8. The Specify Configuration screen appears.

*Figure 22–4 Specify Configuration*



Oracle Universal Installer: Specify Configuration

Specify Configuration

You have chosen to upgrade an existing Management Repository on an existing database for this Management Service installation. Please provide the SYS password to obtain configuration information from an existing repository.

Database Password

SYS Password:

Management Service Security

This password must be supplied by agents desiring Secure Communication with the Management Service.

Password: Confirm Password:

a. Here, you must specify the existing Database and Secure OMS passwords. The Database Password (SYS) is required to access the configuration files of the existing database repository that is associated with the OMS that you have selected for upgrade.

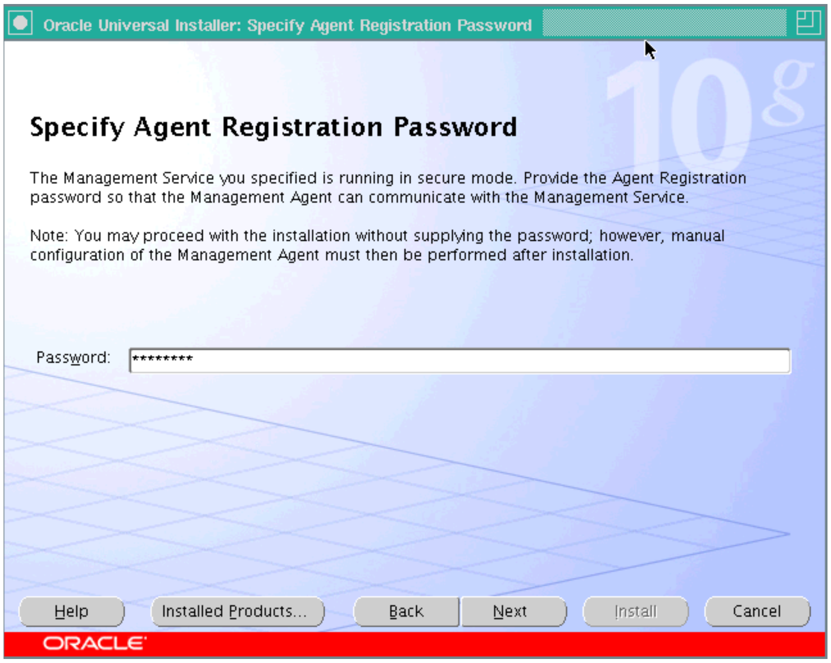
b. In the Database password section, specify the SYS Password (the default super administrator account) for the existing database repository that is associated with the selected OMS.

c. In the Management Service Security section, specify a password that will be used to secure the communications between the OMS and its agents.

**Note:** Management Service Security: This section is enabled only when the existing OMS that you are upgrading is not secure.

9. Click **Next.** If you are upgrading both OMS and Agent, but only the existing OMS is secure and locked, then the Agent Registration Password screen appears. Here, you must provide the correct password to enable communications between the secure OMS and the agent that you are upgrading.

*Figure 22–5 Specify Agent Registration Password*



Oracle Universal Installer: Specify Agent Registration Password

Specify Agent Registration Password

The Management Service you specified is running in secure mode. Provide the Agent Registration password so that the Management Agent can communicate with the Management Service.

Note: You may proceed with the installation without supplying the password; however, manual configuration of the Management Agent must then be performed after installation.

Password: ********

**Note:** This screen appears only if the base (existing) agent installation is not secure.

**Caution:** If you do not know the password and choose to leave the Password field blank, you must do the following after installation, to enable secure communication between the agent and OMS:

1. Find out the correct password for the secure OMS environment. If you do not know the password, obtain it from the user who configured the OMS for SSL.
2. In the Agent's <ORACLE_HOME>/bin directory, execute the following command:

   ```
   <AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
   ```

   The <passwd> argument must be replaced with the Agent Registration Password. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

10. The Summary screen appears. This screen displays all the Oracle homes that will be created. Depending on the type of upgrade you have selected, this page will display any of the following details:
    - Global Settings
    - Product Languages
    - Space Requirements
    - New Installations
11. Verify the choices that you have made, and click **Install** to start the upgrade.

#### 22.5.1.1 Upgrade Logs

During theOMS upgrade, the following log files are created:

- `iasua.log`

  The Oracle Application Server stack is upgraded by the OMS Upgrade Plugin. This is performed by invoking the IASUA utility. the iasua.log file is created at the following location:

  ```
  <NEW_OMS_HOME>/upgrade/log/iasua.log
  ```

- `emrepmgr.log.<pid>`

  This log is created during the schema upgrade. The upgrade output log file is located at:

  ```
  <NEW_OMS_HOME>/sysman/log/emrepmgr.log.<pid>
  ```

#### 22.5.1.2 Post-Upgrade Configuration

Perform the following configuration tasks after the upgrade is complete.

##### 22.5.1.2.1 For Oracle Management Service

After the OMS upgrade is complete, you must do the following:

- Check the `<OMS_HOME>/sysman/log/emrepmgr.log.<pid>` log file and verify whether or not there were any errors.

  > **Note:** There may be more than one `emrepmgr.log.<pid>` file present in the OMS home. Ensure you select the files that were updated most recently.

  In the log files, examine the last line to see whether or not it indicates Repository Upgrade as successfully completed or as having ended in a failure.

  If it shows a failed upgrade, search for any "ORA-" or "compilation" errors.

- After OMS upgrade (regardless of whether or not the agent has been upgraded along with it), you must execute `agentca` with discovery options in order to discover CSA targets.
- You can optionally delete the BC4J target of the old OMS home after the OMS upgrade is complete.
- You must reset the `ias_admin` password after the OMS upgrade. The `ias_admin` password is set as `welcome1` by default, during the upgrade process.
- If in the Patch Advisories page on the Grid Control console, the patch advisories and affected homes count is showing 0 (zero), do ne of the following:
  - Execute the following SQL as `sysman` and then run the `RefreshFromMy Oracle Support` job. This must be done just once after the upgrade process.

    ```
    BEGIN
    MGMT_POLICY.AUTO_ENABLE_EXISTING_TARGETS(
      p_target_type => 'host',
        p_policy_name => 'Critical Patch Advisories for Oracle Homes' );
    END;
    ```

  - Go to the Targets tab in the console and click **Hosts.** On this page, click the **Metric and Policy Settings** link for a host. Now, go to the Policies tab and click **Add Policy.** Here, select the CPF policy and associate it to the target.

- After the upgrade, if you find the links under the Web Application tasks tab (under Monitoring Configuration) in the console disabled, it means that the Application Server diagnostics pack is disabled after the upgrade. To work around this issue, do the following:

  1. Identify the system associated with the Web Application Enterprise Manager Web site.
  2. Add the new Application Server target as a member of this system.
  3. Mark the new Application Server target as a key component of the Web Application Enterprise Manager Web site.

- After the upgrade, if the performance graph is missing, do the following:

  1. Go to the Performance Metrics page under Monitoring Configuration.
  2. Add the metric and select the performance graph to be displayed on the home page. Perform similar tasks for the Usage Metrics also.

- You may fin some of the Web site targets in a broken state after the upgrade. They will show up in the All Targets page under the **Targets Not Configured** list. This does not affect their monitoring in any way. Even though the target is in a "non-configured" state, the availability is still computed and al functions remain in working order.

  To prevent these targets from showing up in that list, the user has to run the query provided below, to update a table in the repository. This query must be run after the OMS upgrade is complete.

  ```
  UPDATE MGMT_TARGETS SET broken_reason = 0, broken_str = NULL, emd_url = NULL,
  host_name = NULL
    WHERE target_guid IN (SELECT t.target_guid
                            FROM MGMT_TARGET_PROPERTIES p,
                                 MGMT_TARGETS t
                           WHERE t.target_guid = p.target_guid
                             AND t.target_type = 'website'
                             AND t.broken_reason != 0
                             AND p.property_name = 'Upgraded'
                             AND p.property_value = '1');

  COMMIT;
  ```

  After this query completes, the targets will not show up in the **Targets Not Configured** list.

#### 22.5.1.2.2 For Oracle Database Upgrade

After the Oracle Database upgrade is complete, you must do the following:

- On Microsoft Windows, if you have performed an upgrade on an installation of the type Enterprise Manager Using a New Database, you must manually modify the Listener services to make sure that the old Listener's startup type is set to `Disable`, and the new Listener's startup type is set to `Automatic`.

- There may be instances where the Enterprise Manager Using a New database installation and its subsequent upgrade encounters an abnormal growth of the `ons.log`. This can potentially take up a lot of disk space relatively quickly.

In such circumstances, you must check whether or not the `ons.log` contains repeated messages such as the following:

```
Local connection 0,127.0.0.1,6100 missing form factor
```

If such an error message is observed in the `ons.log`, perform the following steps:

1. In the Database Oracle home, rename the $ORACLE_HOME/opmn/conf/ons.config file (in order for the Listener not to find the database to sue it). For example,

   ```
   cd $ORACLE_HOME/opmn/conf
   mv ons.config ons.config.orig
   ```

2. Restart the Listener.

**22.5.1.2.3 For Management Agent** After the Oracle Management Agent upgrade is complete, if you find that the Beacon URL Watchlist items do not appear in the collections file, do the following:

1. Go to the Beacon home page.
2. Click **Past Changes.**
3. On this page, click **Sync Beacon.**

### 22.5.1.3 Enterprise Manager Grid Control Upgrade Diagnostics

This sections details some of the diagnostic checks that you should perform along with their resolutions.

#### 22.5.1.3.1 OMS Upgrade Stops At IASUA failure

Check the appropriate log file to get the facts for this occurrence. The installation dialog and the configuration framework log file is located at:

```
<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log
```

This file will list the SEVERE messages indicating the reason that iASUA (Oracle Application Server Upgrade Assistant) failed to complete successfully. If the message shows that "permission denied" on certain files, that means that the user running the installer may not have the correct privileges to run certain iAS configuration.

To resolve this issue, comments out the iAS configuration that contains these files, and then retry the upgrade again.

#### 22.5.1.3.2 OMS Upgrade Stops at EMDeploy Failure

The most common reasons that EMDeploy would fail are because of some pre-upgrade check list items that were not satisfied. The messages in the log file located at:

```
<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log
```

This file will indicate the reasons for the EMDeploy failures.

You must resolve the issue in accordance with the pre-upgrade check list items, and then retry the upgrade.

**22.5.1.3.3 OMS Upgrade Stops at the Repository Schema Upgrade (RepManager)** The most common reason that repository schema upgrade fails is when it is not able to connect to the listener. The log file mentioned below would indicate the reason that repository schema upgrade has failed.

To fix this issue, you must examine whether or not the listener that the OMS connects to is valid and live. If the OMS is of installation type Enterprise Manager Using a New Database, then you should check whether or not the old listener has been stopped, and the new listener has been started. After the listener issue is resolved, you can retry the upgrade process.

The log file is at the following location:

```
$ORACLE_HOME/sysman/log/emrepmgr.log.<pid>
```

You must examine this log file to check whether or not there are any errors.

> **Note:** There may be more than one `emrepmgr.log.<pid>` file present in the OMS home. Ensure you select the files that were updated most recently.

In the log files, examine the last line to see whether or not it indicates Repository Upgrade as successfully completed or as having ended in a failure.

If it shows a failed upgrade, search for any "ORA-" or "compilation" errors.

### 22.5.2 Upgrading Management Agent Using the Agent Deploy Application

Agent Deploy is a J2EE application that is used for mass deployment of Management Agents.

The Upgrade Agent option in this application will help you upgrade an existing Management Agent installation to a release 10.2 Management Agent.

> **Note:** If the upgrade operation fails, review the log files described in Appendix C, "Agent Log Files".

#### Prerequisites

The following are the prerequisites to be met before upgrading the management agent:

- Ensure that the SSH daemon is running on the default port (that is, 22) on all the target hosts.
  - For Enterprise Manager 10g Grid Control Release 4 (10.2.0.4), the port must be 22. If it is any other port, then the upgrade fails.
  - For Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), the port can be 22 or any non-default port, that is, any port other than 22. If the port is a non-default port, then update the SSH_PORT property in the following file to ensure successful upgrade of the agent:

    ```
    <OMS_HOME>/sysman/agent_
    download/<VERSION>/<PLATFORM>/agentdeploy/Paths.properties
    ```
- If the central inventory owner and the user upgrading the 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 user installing the agent is xyz, then ensure that abc and xyz belong to the same group, and they have read and write access to the inventory.

- Ensure that you have SUDO privileges to run `root.sh` and `/bin/sh`.

  To verify whether you have SUDO privileges to run these files, access the `/etc/sudoers` file and check whether you have a similar entry as shown below. If you do not see a similar entry, then add one.

  ```
  <user> <hostname>=PASSWD:
  /home/em/agent10205/agent10g/root.sh, /bin/sh
  ```

-

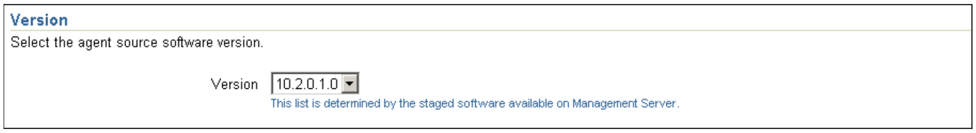
### Accessing the Agent Deploy Application

To access the Agent Deploy application, follow these steps:

1. Log in to the Grid Control console and go to the Deployments page.
2. Click **Install Agent** under the Agent Installation section.
1. Click **Upgrade Agent** to upgrade the Management Agent.  Grid Control displays the Agent Upgrade: Installation Details page.
2. In the Version section of this page, select the appropriate version of the agent software that you want to use for upgrade.

> **Note:** The values in this list will depend on the staged software that are available on the OMS host.

*Figure 22–6 Version Section of the Installation Details Screen*



Version

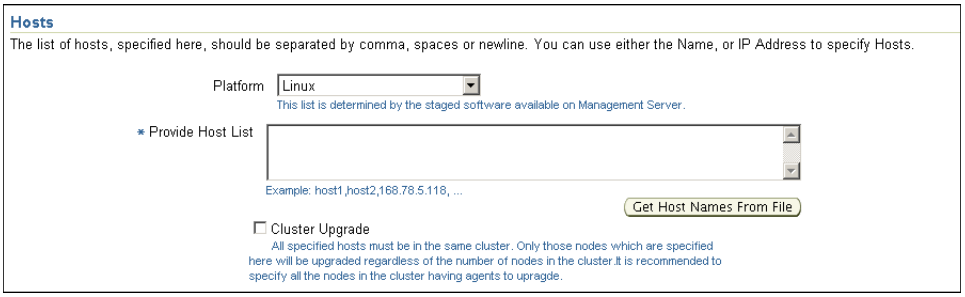
Select the agent source software version.

Version 10.2.0.1.0

This list is determined by the staged software available on Management Server.

3. In the Hosts section, do the following:

*Figure 22–7 Hosts Section of the Installation Details Screen*



Hosts

The list of hosts, specified here, should be separated by comma, spaces or newline. You can use either the Name, or IP Address to specify Hosts.

Platform Linux

This list is determined by the staged software available on Management Server.

* Provide Host List

Example: host1,host2,168.78.5.118, ...

Get Host Names From File

□ Cluster Upgrade

All specified hosts must be in the same cluster. Only those nodes which are specified here will be upgraded regardless of the number of nodes in the cluster.It is recommended to specify all the nodes in the cluster having agents to upragde.

   a. Select the appropriate platform on which you want to perform this installation.

   b. In the Provide Host List text box, specify all the hosts (host names or IP addresses) on which you want to perform the Agent installation. Alternatively, click **Get Host Names From File** to browse and select the file that contains a list of all the required host names.

**WARNING: Do not specify duplicate entries of the host list. If there are duplicate host entries in this list, the application hangs.**

**Use the same host names for which the SSH has been set.**

**Note:** You can use either a comma (,) or white space as a separator when specifying multiple hosts.

**Caution:** The Agent Deploy application picks up only the values in the first column of the Host List file that you specify or select.

Ensure the host list format is appropriate, since the Agent Deploy application does not validate this format on the selected file.

A sample host list format is provided in Table 22–3.

*Table 22–3 Sample Host List Format*

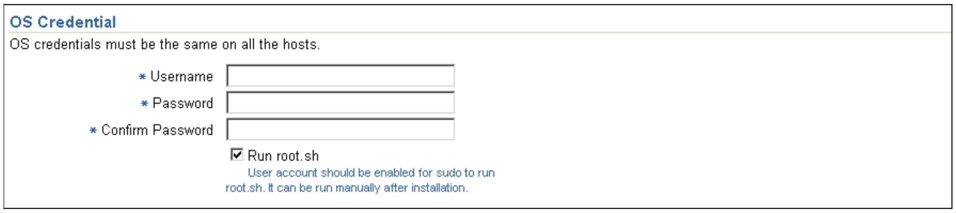
| Fully Qualified Host name | Host name | Host IP Address |
|---|---|---|
| host1.foo.com | host1 | 154.87.3.229 |
| host2.foo.com | host2 | 154.87.3.109 |
| host3.foo.com | host3 | 154.80.5.218 |

c. Select **Cluster Upgrade** if you want to upgrade the Management Agent cluster.

**Note:** The hosts that you specify must belong to the same cluster. Also, note that only the hosts that you specify here will be upgraded, irrespective of the number of hosts in that cluster. For example, if there are 10 hosts in a cluster and you specify only 5 here, Agent Deploy will upgrade only those five hosts in the cluster that you have specified.

4. In the OS Credential section, specify the appropriate operating system user credentials. Select **Run root.sh** (UNIX platforms only) if you want Agent Deploy to execute this script.

*Figure 22–8 OS Credential Section of the Installation Details Screen (UNIX Only)*



OS Credential

OS credentials must be the same on all the hosts.

| | |
|---|---|
| * Username | |
| * Password | |
| * Confirm Password | |
| | ☑ Run root.sh |

User account should be enabled for sudo to run root.sh. It can be run manually after installation.

The `root.sh` script runs after the configuration assistants are run and before the postinstallation scripts (if any) are run. If you do not select this option here, you must run `root.sh` on each node manually.

Agent Deploy application uses `sudo` to run the `root.sh` script. You must specify the *invoking user's password* here.

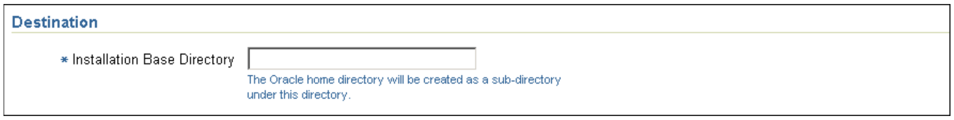
If `/etc/sudoers` is configured in such a way that `sudo` never prompts for a password, then a directory with the host password as the title gets created in the invoking users home directory. To avoid this, ensure that you configure /etc/sudoers file such that running a command using sudo always prompt for a password.

5. In the Existing Agent Information section, specify the full path to an existing agent Oracle home location. This source agent installation will be used to perform the upgrade.

> **Note:** The path of the source agent should be the same on all the remote hosts.

6. In the Destination section, specify the absolute path for the Installation Base Directory. This directory will be created on all the specified hosts, and the Agent Oracle home directory will be created as a subdirectory under this directory.

***Figure 22–9 Destination Section of the Installation Details Page***



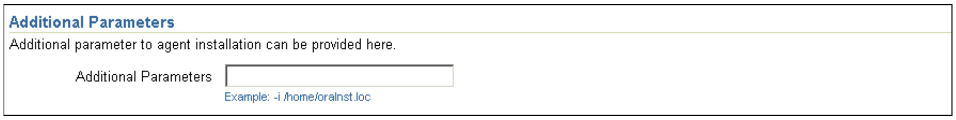
Destination

* Installation Base Directory

The Oracle home directory will be created as a sub-directory under this directory.

7. In the Additional Parameters text box, specify any additional parameters that you want to pass during installation.

***Figure 22–10 Additional Parameters Section of the Installation Details Page***



Additional Parameters

Additional parameter to agent installation can be provided here.

Additional Parameters

Example: -i /home/oraInst.loc

Oracle recommends you to specify only those parameters that you want to run in addition to the general parameters you have already provided in this page for upgrade. For example, in step (7), you are providing the installation base directory. Therefore, for additional parameters, try to avoid specifying the installation base directory again. If you still do so, then the value you specified in step (7) will be ignored and the value you specified here will be used instead.

The following are the additional parameters you can specify:

- Specify `-t` if you do NOT want to start the Agent after installation or upgrade. No value required.
- Specify `-d` if you do NOT want to initiate automatic target discovery. No value required.

- Specify `-i` if you want to provide an Inventory pointer location file. For example, `-i /etc/oraInst.loc`.
- Specify `-p` if you want to provide a file location for Static port for Agent. For example, `-p /home/config/staticports.ini`.

8. In the Management Server Security section, specify the OMS registration password to secure your communication to the OMS.
9. In the Additional Scripts section, specify any preinstallation and postinstallation scripts that you want to execute.
10. Click **Continue**. Grid Control displays the My Oracle Support Details page.
11. On the My Oracle Support Details page, do the following:
    - If the host where the Management Agent is being installed has a *direct* connection to the Internet, then specify an email address and My Oracle Support (formerly Metalink) password.

      An email address is required so that security updates and install updates can be sent. You can specify any email address, but Oracle recommends you to specify the My Oracle Support (formerly Metalink) user name. For example, `john.mathew@xyz.com`.

      If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an email address, then you will continue to receive security updates and other notifications from Oracle to that email address.
    - If the host where the Management Agent is being installed has an *indirect* connection to the Internet through a proxy server, then specify an email address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

      **Note:** You can change the proxy server settings any time after the installation or patching process ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the Management Agent.
    - If the host where the Management Agent is being installed does not have a *direct* or *indirect* connection to the Internet, then specify the email address and leave the other fields blank.

      In this case, after you complete the installation process, 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 10.1.4.1.2, "Manually Collecting and Uploading Configuration Information to My Oracle Support (formerly Metalink)".
12. Click **Continue** to start the upgrade process.

#### 22.5.2.1 Possible Parameters that You Can Specify During Agent Upgrade

The important parameters for Agent Upgrade are `-o, -b` and optionally `-i, -t`.

Table 22–4 lists all the possible parameters that you can specify.

### 22.5.3 Upgrading Management Agent Using agentDownload Script

To upgrade Management Agent using the `agentDownload` Script, follow the instructions documented below:

1. Invoke the `agendDownload` script using `-u` option.

   The `OLD_ORACLE_HOME` that you want to upgrade should be specified either by passing the `-o` option, or setting the `OLD_ORACLE_HOME` environment variable.

   Invoke the agentdownload script using the following command:

   ```
   ./agentDownload.linux -u -o <OLD_ORACLE_HOME_PATH>
   ```

   For Microsoft Windows, invoke the `agentDownload` script using the following command:

   ```
   ./agentDownload.vbs -u -o <OLD_ORACLE_HOME_PATH>
   ```

   > **Note:** The first two options (`-u` and `-o`) are mandatory. The `-b` option can be skipped if this has already been specified in the response files.

2. To construct the new Oracle home name, either pass the `-b` option, or specify these values for `BASEDIR` in the `agent_download.rsp` file.

   > **Note:** You can specify these options in the command-line even though they are present in the response file. The command-line options will have a higher precedence over the ones in response file.

3. If the base agent that you are upgrading is not secure, the script will prompt you to specify the Agent Registration Password.

You can use the options listed in Table 22–4 to execute the `agentDownload` script.

*Table 22–4 Options that You Can Use To Execute the agentDownload Script*

| Options | Description |
|---|---|
| -b | baseDirectory of the Agent Oracle home |
| -l | local (pass -local to runInstaller) |
| -n | Cluster name |
| -o | OLD_ORACLE_HOME during Upgrade |
| -u | Upgrade |
| -c | CLUSTER_NODES (to specify the cluster nodes). For example, "CLUSTER_NODES={node1,node2,node3}" |
| -p | `staticports.ini` file |
| -s | Installer stage directory |
| -t | Do NOT start the Agent |

*Table 22–4 (Cont.) Options that You Can Use To Execute the agentDownload Script*

| Options | Description |
|---|---|
| -i | Inventory pointer location file |
| -d | Do NOT initiate automatic target discovery |

**Note:** When performing an Management Agent upgrade using the `agentDownload` script, ensure you are using the `agentDownload script` from the Oracle home of the pointing OMS.

For example, if you are upgrading `agent1` that is pointing to OMS `A`, then you must use the `agentDownload` script that is located in the OMS `A` Oracle home only.

**Caution:** If you are upgrading a non-secure agent to a secure mode, the script will prompt you to specify the Agent Registration Password. Specify the correct password to secure the upgraded agent.

**Note:** If the upgrade operation fails, review the log files described in Appendix C, "Agent Log Files".

## 22.5.4 General System Installation Requirements for Real Application Clusters

Each node that is going to be part of your Oracle Real Application Clusters (Oracle RAC) installation must meet the following hardware and software requirements. You will perform step-by-step tasks for hardware and software verification for the platform-specific preinstallation procedures.

### 22.5.4.1 Hardware Requirements for Real Application Clusters Setup

Each node in a cluster requires the following hardware:

- External shared disks for storing the Oracle Clusterware files.

  Refer to the respective Oracle RAC installation guides for information on the disk configuration options that are available. Review these options before you decide which storage option to use in your Oracle RAC environment.

- One private internet protocol (IP) address for each node to serve as the private interconnect. The following must be true for each private IP address:

  – It must be separate from the public network.

  – It must be accessible on the same network interface on each node.

  – It must have a unique address on each node.

  The private interconnect is used for internode communication by both Oracle Clusterware and Oracle RAC. If the private address is available from a domain name server (DNS), then you can use that name. Otherwise, the private IP address must be available in each node's `/etc/hosts` file.

  On Microsoft Windows, this IP address must be available at the following location on each node:

  ```
  C:/Windows/<system drive>/etc/hosts file
  ```

During Oracle Clusterware installation, the information you enter as the private IP address determines which private interconnects are used by Oracle RAC database instances. They must all be in an up state, just as if their IP addresses were specified in the initialization parameter, `CLUSTER_INTERCONNECTS`. Oracle Real Application Clusters does not fail over between cluster interconnects; if one is down, then the instances using them will not start.

Oracle recommends that you use a logical IP address that is available across all private networks, and that you take advantage of any available operating system-based failover mechanism by configuring it according to your third-party vendor's instructions for using their product to support failover.

- One public IP address for each node, to be used as the Virtual IP address for client connections and for connection failover.

  This public Virtual IP address must be associated with the same interface name on every node that is part of your cluster. In addition, the IP addresses that you use for all of the nodes that are part of a cluster must be from the same subnet. If you have a domain name server (DNS), then register the host names for the Virtual IP with the DNS. The Virtual IP address should not be in use at the time of the installation, because this is a Virtual IP address that Oracle manages.

- One public fixed hostname address for each node, typically assigned by the system administrator during operating system installation. If you have a DNS, then register both the fixed IP and the VIP address with the DNS. If you do not have a DNS, then you must make sure that both public IP addresses are in the node host file.

- If you have a DNS, then you should be able to use DNS to resolve the name of the host on which you want install OMS. For more information, contact your network administrator.

#### 22.5.4.2 Software Requirements for Real Application Clusters Setup

Each node in a cluster requires a supported interconnect software protocol to support Cache Fusion, and to support Oracle Clusterware polling. Your interconnect must be certified by Oracle for your platform. You should also have a Web browser, both to enable Grid Control, and to view online documentation. For Oracle Database 10*g* requirements, Oracle Clusterware provides the same functions as third-party vendor clusterware. Using Oracle Clusterware also reduces installation and support complications. However, you may require third-party vendor clusterware if you use a non-ethernet interconnect, or if you have deployed clusterware-dependent applications on the same cluster where you deploy Real Application Clusters.

See Chapter 14, "Prerequisites for Installing Enterprise Manager Grid Control on Oracle RAC" for more information on the preinstallation tasks.

---

**Caution:** If you are upgrading a 10.1.0.*n* agent to 10.2.0.2 release, you must execute the following command before starting the upgraded agent:

```
emctl resetTZ agent
```

This command is required to correct the agent time zone.

This command will correct the agent-side time zone, and specify an additional command to be run against the repository to correct the value there.

---

**Note:** Before you change the timezone, check if there are any blackouts that are currently running or scheduled to run on any of the targets that are monitored by the upgraded agent. Do the following to check this:

1. In the Grid Control console, go to the All Targets page under Targets and locate the Agent in the list of targets. Click the agent name link. The Agent home page appears.
2. The targets monitored by the agent will be listed in the *Monitored Targets* section.
3. For each target in the list, click the target name to view the target home page.
4. In the Related Links section, click **Blackouts** to check any blackouts that are currently running or may be scheduled to run in the future.
5. If such blackouts exist, you must stop all the blackouts that are running on all the targets monitored by this agent.
6. From the console, stop all the targets that are scheduled to run on any of these monitored targets.
7. Now, run the following command from the agent home to reset the timezone;

   ```
   emctl resetTZ agent
   ```

8. After the timezone is reset, you can create new blackouts on the targets.

# Part VI

## Deinstalling Enterprise Manager Grid Control and Management Agent

This part provides information and step-by-step instructions to deinstall Enterprise Manager Grid Control and Management Agent.

This part contains the following chapters:

- Chapter 23, "Deinstalling Enterprise Manager Grid Control"
- Chapter 24, "Deinstalling Management Agent"

# 23

# Deinstalling Enterprise Manager Grid Control

This chapter describes how you can deinstall Enterprise Manager Grid Control (Grid Control). In particular, this chapter covers the following:

- Deinstalling Enterprise Manager Grid Control Using OUI
- Deinstalling Enterprise Manager Grid Control In Silent Mode

> **Note:** If you deinstall the Enterprise Manager 10*g* Grid Control or Management Agent Oracle homes using Oracle Universal Installer (OUI), the Oracle homes are de-registered from the central inventory and the `oratab` file. However, some files may remain in these Oracle homes.
>
> If an Oracle home has been removed successfully (verify this in OUI by clicking **Installed Products**), you can manually delete the files present in the Oracle home directories.

## 23.1 Deinstalling Enterprise Manager Grid Control Using OUI

To deinstall Grid Control using OUI, do the following:

1. Shut down all `opmn` processes that are running by running the following command:

   ```
   <OMS_HOME>/opmn/bin/opmn stopall
   ```

2. Shut down the Management Agent in the Agent Oracle home using the `emctl stop agent` command.
3. Stop Grid Control by running the following command:

   ```
   <OMS_HOME>/bin/emctl stop em
   ```

4. Shut down the repository database (if the database software is installed as a part of the Management Service Oracle home being uninstalled).
5. Shut down the Oracle Database listener.
6. Run the Database Configuration Assistant (DBCA) to delete the database before proceeding to deinstall the Oracle home.
7. Run the OUI and select the Oracle home to deinstall. It is removed from the Central Inventory. When you invoke OUI, pass the `-removeallfiles` parameter.

   For UNIX platforms:

```
./runInstaller -removeallfiles
```

For Microsoft Windows platforms:

```
setup.exe -removeallfiles
```

8. Manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

**Caution:** After deinstallation of certain Grid Control targets, when you try and remove the same targets from the Grid Control console, you may encounter an error.

To resolve this issue, deinstall the Grid Control targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts screen.

## 23.1.1 Additional Deinstallation Steps

For deinstalling  Grid Control from Microsoft Windows operating system, you will need to perform the following additional steps to remove entries from the registry. Ensure that you are logged in as a user with Administrator privileges on that computer.

### 23.1.1.1 Remove Entries in Windows Registry

To remove entries in Windows registry:

1. Start the registry editor. Choose Start > Run > regedit.
2. Navigate to HKEY_LOCAL_MACHINE\SOFTWARE\
3. Go to HKEY_LOCAL_MACHINE\SOFTWARE\ODBC and expand all subkeys and remove the key "Oracle in <HOME_NAME>". Check if the "Oracle ODBC Driver" key contents refer to the ORACLE_HOME to be deleted. If yes, delete the key.
4. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services. Delete the keys that begin with Oracle.
5. Go to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet2\Services. Delete the keys that begin with Oracle.
6. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\...\Application. Delete the keys whose names begin with Oracle and contain references to the EventMessageFile string entry for the ORACLE_HOME to be deleted or a location under it.
7. Go to HKEY_CLASSES_ROOT and search in the keys starting with Ora or ORCL (for example, Oracle..., ORADC... ..., OraPerf..and ORCL...). Delete keys which include string values with the specific ORACLE_HOME that is to be deleted.
8. Close the registry editor.

### 23.1.1.2 Clean Up Environment Settings

To clean up environment settings:

1. On Windows NT: Choose Start > Settings > Control Panel > System > Environment.

On Windows 2000 and Windows XP: Choose Start > Settings > Control Panel > System > Advanced > Environment Variables.

2. In the System Variables section, click the variable PATH in order to modify the value. For example, you may see a path similar to this one:

   ```
   C:\ORACLE\EM10g\BIN
   C:\PROGRAM FILES\ORACLE\JRE\1.1.7\BIN
   ```

   If you are deleting the Oracle home C:\ORACLE\EM10g, remove the C:\ORACLE\EM10g\BIN expression from the PATH variable.

   Delete any path expression in the PATH variable that contains the Oracle home to be removed or some location underneath.

3. If there is a CLASSPATH variable under "System Variables", delete the path expressions in the variable that contains the ORACLE_HOME to be removed or some location underneath.
4. Check if there are any other Oracle variables set in "System Variables". Delete those variables that contain the ORACLE_HOME that you are trying to remove. For example, ORACLE_HOME, ORACLE_SID, TNS_ADMIN, inventory_loc, and so on.
5. Click Apply and then click OK.
6. Close the Control Panel window.

#### 23.1.1.3 Delete Software and Start Menu Icons

To delete software and start menu icons:

1. On Windows NT: Choose Start > Programs > Windows NT Explorer.

   On Windows 2000 and Windows XP: Choose Start > Programs > Accessories > Windows Explorer.

2. On Windows NT: Go to %SystemDrive%\WINNT\PROFILES\ALL USERS\START MENU\PROGRAMS

   On Windows 2000 and Windows XP: Go to %SystemDrive%\DOCUMENTS AND SETTINGS\ALL USERS\START MENU\ ...\PROGRAMS

   > **Note:** These locations depend on whether the operating system was upgraded from NT or was a new install of Windows 2000 or Windows XP.

3. Delete the folders -Oracle - <HOME_NAME> where <HOME_NAME> is the Oracle home that you are trying to remove.

   > **Note:** To locate your System Drive, type echo %SystemDrive% in the Command Prompt.

4. Go to the temp directory and delete all files and directories at the following locations:

   On Windows NT: %SystemDrive%\Temp

   On Windows 2000 and Windows XP: %SystemDrive%\Documents and Settings\<username>\Local Settings\Temp\

5. Reboot the machine.

## 23.2 Deinstalling Enterprise Manager Grid Control In Silent Mode

This section describes how you can deinstall  Grid Control in silent mode. In particular, this section covers the following:

- Deinstalling Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or Lower
- Deinstalling Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or Higher

---

**Note:** If you are deinstalling  Grid Control from Microsoft Windows platform, then follow the additional steps given in Section 23.1.1, "Additional Deinstallation Steps".

---

**Caution:** After deinstallation of certain Grid Control targets, when you try and remove the same targets from the Grid Control console, you may encounter an error.

To resolve this issue, deinstall the Grid Control targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts screen.

---

### 23.2.1 Deinstalling Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or Lower

To deinstall Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower  in silent mode, that is, without using OUI, do the following:

1. Shut down all `opmn` processes that are running by executing the following command:

   ```
   <OMS_HOME>/opmn/bin/opmn stopall
   ```

2. Shut down the Management Agent in the Agent Oracle home using the `emctl stop agent` command.

3. Stop Grid Control by executing the following command:

   ```
   <OMS_HOME>/bin/emctl stop em
   ```

4. Shut down the repository database (if the database software is installed as a part of the Management Service Oracle home being uninstalled).

5. Shut down the Oracle Database listener.

6. Run the Database Configuration Assistant (DBCA) to delete the database before proceeding to deinstall the Oracle home.

7. Run the following command to deinstall  Grid Control:

   ```
   ./runInstaller -deinstall -silent "REMOVE_HOMES={absolute_
   path_to_oracle_homes_to_be_deinstalled}" -removeallfiles
   ```

   For example, if you deinstalling  Grid Control that was installed using a new database, then you must run the following command. No changes are required for the response file.

```
./runInstaller -deinstall -silent "REMOVE_
HOMES={/scratch/oraclehome/db10g,/scratch/oraclehome/oms10g,/
scratch/oraclehome/agent10g}" -removeallfiles
```

8. Manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

## 23.2.2 Deinstalling Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or Higher

To deinstall Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher in silent mode, that is, without using OUI, you have to run the `deinstall.pl` script. This deinstalls the database that was installed with Grid Control, the OMS, as well as the Management Agent. Optionally, you can run the script to drop the Grid Control schema from an existing database that was not installed along with Grid Control.

> **Note:** This deinstallation method applies only to Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or higher, and is supported only on Linux and Microsoft Window platforms.

### Deinstalling Enterprise Manager Grid Control (All Core Components)

To deinstall Grid Control, navigate to the Oracle home directory of the OMS or Management Agent, and run the following command. This command essentially deinstalls all core components residing in the base directory.

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -baseDir <full path
to the base directory>
```

For example:

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -baseDir
/john/OracleHomes
```

> **Note:** If the Management Agent is installed in a location that is different from the base directory or if the Oracle home directory of the Management Agent is different from `agent10g` (the default name), then deinstall that Management Agent separately. For instructions to deinstall Management Agent only, see Section 24.2.2, "Deinstalling Oracle Management Agent 10g Release 5 (10.2.0.5) or Higher".

> **Note:** After you deinstall the product, manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

### Deinstalling Enterprise Manager Grid Control and Dropping Grid Control Scheme from an Existing Database

Optionally, if you want to drop the Grid Control schema from an existing database that was not installed along with Grid Control, then run the following command:

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -baseDir <full path
to the base directory> -reposDrop
```

For example:

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -baseDir
/john/OracleHomes -reposDrop
```

**Note:** After you deinstall the product, manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

# 24 Deinstalling Management Agent

This chapter describes how you can deinstall Oracle Management Agent (Management Agent). In particular, this chapter covers the following:

- Deinstalling Oracle Management Agent Using OUI
- Deinstalling Oracle Management Agent in Silent Mode
- Deinstalling NFSAgent

> **Note:** If you deinstall the Enterprise Manager 10*g* Grid Control or Management Agent Oracle homes using Oracle Universal Installer, the Oracle homes are de-registered from the central inventory and the `oratab` file. However, some files may remain in these Oracle homes.
>
> If an Oracle home has been removed successfully (verify this in OUI by clicking **Installed Products**), you can manually delete the files present in the Oracle home directories.

## 24.1 Deinstalling Oracle Management Agent Using OUI

To deinstall Oracle Management Agent using OUI, do the following:

1. Shut down the Management Agent in the Agent Oracle home using the emctl stop agent command.

   For example,

   ```
   <agent_home>/emctl stop agent
   ```

2. Run the OUI and select the Agent Oracle home to deinstall. It is removed from the Central Inventory. When you invoke OUI, pass the `-removeallfiles` parameter.

   For UNIX platforms:

   ```
   ./runInstaller -removeallfiles
   ```

   For Microsoft Windows platforms:

   ```
   setup.exe -removeallfiles
   ```

If you want to deinstall the Management Agent from one node of a cluster, then follow these steps:

1. Invoke the installer on the node from where you want to deinstall the Management Agent using -local as the agrument.

   ```
   ./runInstaller -local
   ```

2. Run the following command on all other nodes of the cluster:

   ```
   ./runInstaller -updateNodeList ORACLE_HOME=<Oracle_Home_of_
   Agent> "CLUSTER_NODES=<other nodes separate by a comma
   node2>"
   ```

   For example, if you have a cluster of five nodes, and if you have run Step(1) on node1, then run this command on node2, nod3, node4, and node5:

   ```
   ./runInstaller -updateNodeList ORACLE_HOME=<Oracle_Home_of_
   Agent> "CLUSTER_NODES=<node2, node3, node4, node5>"
   ```

3. Manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

## 24.1.1 Additional Deinstallation Steps

For deinstalling Oracle Management Agent from Microsoft Windows operating system, you will need to perform the following additional steps to remove entries from the registry. Ensure that you are logged in as a user with Administrator privileges on that computer.

### 24.1.1.1 Remove Entries in Windows Registry

To remove entries in Windows registry:

1. Start the registry editor. Choose Start > Run > regedit.
2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Oracle and remove the Agent entry.

   For example, if you have Management Agent 10g, then you would select and remove the following:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Key_agent10g
   ```

3. Go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services. Delete the Agent keys.
4. Go to HKEY_LOCAL_MACHINE\SYSTEM\ControlSet2\Services. Delete the Agent service.
5. Close the registry editor.

### 24.1.1.2 Clean Up Environment Settings

To clean up environment settings:

1. On Windows NT: Choose Start > Settings > Control Panel > System > Environment.

   On Windows 2000 and Windows XP: Choose Start > Settings > Control Panel > System > Advanced > Environment Variables.

2. In the System Variables section, click the variable PATH in order to modify the value.
3. Delete Agent home.
4. Click Apply and then click OK.
5. Close the Control Panel window.
6. Reboot the computer.

After rebooting, you can start fresh Management Agent installation.

**Note:** On RAC, you have to reboot both the nodes.

## 24.2 Deinstalling Oracle Management Agent in Silent Mode

This section describes how you can deinstall Oracle Management Agent in silent mode. In particular, this section covers the following:

- Deinstalling Oracle Management Agent 10g Release 4 (10.2.0.4) or Lower
- Deinstalling Oracle Management Agent 10g Release 5 (10.2.0.5) or Higher

### 24.2.1 Deinstalling Oracle Management Agent 10g Release 4 (10.2.0.4) or Lower

To deinstall Oracle Management Agent 10g Release 4 (10.2.0.4) or Lower in silent mode, that is, without using OUI, do the following:

1. Shut down the Management Agent in the Agent Oracle home using the emctl stop agent command.

   For example,

   ```
   <agent_home>/emctl stop agent
   ```

2. Run the following command to deinstall Oracle Management Agent:

   ```
   ./runInstaller -deinstall -silent "REMOVE_HOMES={absolute_
   path_to_agent_oracle_home}" -removeallfiles
   ```

   For example:

   ```
   ./runInstaller -deinstall -silent "REMOVE_
   HOMES={/scratch/oraclehome/agent10g}" -removeallfiles
   ```

   **Note:** If you are deinstalling Enterprise Manager Grid Control from Microsoft Windows platform, then follow the additional steps given in Section 24.1.1, "Additional Deinstallation Steps".

   **Caution:** After deinstallation of certain Grid Control targets, when you try and remove the same targets from the Grid Control console, you may encounter an error.

   To resolve this issue, deinstall the Grid Control targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts screen.

3. Manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

### 24.2.2 Deinstalling Oracle Management Agent 10g Release 5 (10.2.0.5) or Higher

To deinstall Oracle Management Agent 10g Release 5 (10.2.0.5) or higher in silent mode, navigate to the Oracle home directory of the Management Agent, and run the following command.

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -agentHome <full
path to agent's Oracle home directory>
```

For example:

```
$ORACLE_HOME/install/deinstall/Deinstall.pl -agentHome
/john/agent/OracleHomes/agent10g
```

> **Note:** After you deinstall the product, manually delete all auto-start scripts that might be present in the `/etc/rc.d/` directory. For example, `/etc/rc.d/rc3.d/S98gcstartup`.

## 24.3 Deinstalling NFSAgent

If the nfsagent you want to deinstall is the *only* Oracle product installed on the host, you must check the `/etc/oraInst.loc` directory for the inventory location and perform the following steps to deinstall the agent:

1. Stop the agent using the following command:

   ```
   <EMSTATE DIR>/bin/emctl stop agent
   ```

2. On Microsoft Windows, you must delete the agent service by executing the following command:

   ```
   nmesrvops delete <service name>
   ```

3. Execute `rm -rf <inventory_location>`
4. Execute `rm -rf <EMSTATE Dir>`

If the nfsagent you want to deinstall is *not* the only Oracle product installed on the host, then go to the master agent Oracle home (using the mounted path) and perform the following steps to deinstall the agent:

1. Stop the agent using the following command:

   ```
   <EMSTATE DIR>/bin/emctl stop agent
   ```

2. On Microsoft Windows, you must delete the agent service by executing the following command:

   ```
   nmesrvops delete <service name>
   ```

3. Execute the following command from the master agent Oracle home:

   ```
   <master agent home>/oui/bin/runInstaller -detachHome ORACLE_HOME=<master agent
   home>
   ```

4. Execute `rm -rf <EMSTATE Dir>`

# Part VII

## Appendixes

Part 5 contains the following appendixes:

# A

# Troubleshooting Enterprise Manager

This appendix describes solutions to common problems and scenarios that you might encounter when installing or upgrading Enterprise Manager.

## A.1 Installation Issues

This section lists some of the most commonly encountered installation issues, and their resolutions.

### A.1.1 Installation Fails with an Abnormal Termination

If there is a daily `cron` job that is running on the system where you are installing Grid Control that cleans up the `/tmp/` directory, the installation might fail with an abnormal termination and the `installActions.err` file will log the following error: `java.lang.UnsatisfiedLinkError: no nio in java.library.path`.

The workaround is to set the `TMP` and `TEMP` environment variables to a directory other than the default `/tmp` and execute the `./runInstaller`.

### A.1.2 PERL Environment Variable is Forced on the environment During an Enterprise Manager 10*g* R2 (10.2.0.2) Installation

In a Microsoft Windows environment, if you have an existing `PERL5LIB` environment variable, the Enterprise Manager Grid Control installation will forcible overwrite this variable, in turn, forcing other applications on this host to use the new Perl version that get installed during the Management Service installation.

To work around this issue, rename the existing Perl variable as `PERL5LIB_TMP` before the OMS installation starts. You can later (after the installation is complete) change the `PERL5LIB_TMP` variable to `PERL5LIB`

**Note:** If the Perl environment variable is not set, remove this variable from the Environment Variables. To do this, from the **Control Panel**, go to **Environment Variable** under **Systems**.

### A.1.3 Installation Fails Due to Network Configuration Issues

The installation of Enterprise Manager Grid Control may fail if there are network configuration and connectivity problems.

To avoid this issue, do the following:

1. Ensure that the HOSTS file mentions the IP address and full canonical name followed by a short name or alias of the computer where OMS or Management Agent is to be installed.
2. Ensure that there are no connectivity issues between the server processes.

### Obtaining Full Canonical Name

The fully qualified domain name can be obtained with a type of double-lookup or reverse-lookup. Check the `/etc/nsswitch.conf` file to see how lookups are to be performed by the operating system.

To get the fully qualified domain name, on the computer where you want to install OMS or Management Agent, run the following commend:

```
hostname
```

To get the IP address, on the computer where you want to install OMS or Management Agent, run the following commend:

```
ifconfig
```

(For Microsoft Windows computer, run `ipconfig`)

### Checking HOST File for Correct Format

The HOSTS file should have the following format:

```
10.10.10.10 omsmachine.domain omsmachinealias
20.20.20.20 agentmachine.domain agentmachine
```

> **Note:** On Microsoft Windows computer, the HOSTS file is under `$WINDOWS/system32/drivers/etc`. On Unix machines, it is under `/etc`.

If OMS and Management Agent are on the same computer, then it is acceptable to have one IPaddress and host name listed.

> **IMPORTANT:** IDo not run OMS on a computer that is DHCP-enabled. Oracle strongly recommends you to use a static host name and IP address assigned on the network for Enterprise Manager Grid Control components to function properly.

### Verifying Network Connectivity

Run the following to test the network configuration and ensure that there are no connectivity issues:

On the computer where you want to install OMS:

```
ping <ip_address>
ping  <omsmachine.domain>
ping <omsmachine>
nslookup <ip_address>
nslookup <omsmachine.domain>
nslookup <omsmachine>
```

On the computer where you want to install Management Agent:

```
ping <ip_address>
ping  <agentmachine.domain>
ping <agentmachine>
nslookup <ip_address>
nslookup <agentmachine.domain>
nslookup <agentmachine>
```

## A.1.4 Management Agent Installation Fails

If the Management Agent installation fails, look into the emctl status log to diagnose the reason for installation failure. You can view this log by executing the following command:

```
<AGENT_HOME>/bin/emctl status agent
```

A sample log file follows and shows some of the typical problem areas shown in bold.

```
Oracle Enterprise Manager 10g Release 10.2.0.0.0.
Copyright (c) 1996, 2005 Oracle Corporation.  All rights reserved.
---------------------------------------------------------------
Agent Version     : 10.2.0.2.0
OMS Version       : 10.2.0.2.0
Protocol Version  : 10.2.0.2.0
Agent Home        : /scratch/OracleHomes2/agent10g
Agent binaries    : /scratch/OracleHomes2/agent10g
Agent Process ID  : 9985
Parent Process ID : 29893
Agent URL         : https://foo.abc.com:1831/emd/main/
Repository URL    : https://foo.abc.com:1159/em/upload
Started at        : 2005-09-25 21:31:00
Started by user   : pjohn
Last Reload       : 2005-09-25 21:31:00
Last successful upload                      : (none)
Last attempted upload                       : (none)
Total Megabytes of XML files uploaded so far :     0.00
Number of XML files pending upload          :     2434
Size of XML files pending upload(MB)        :    21.31
Available disk space on upload filesystem   :    17.78%
Last attempted heartbeat to OMS             : 2005-09-26 02:40:40
Last successful heartbeat to OMS            : unknown
---------------------------------------------------------------
Agent is Running and Ready
```

### A.1.4.1 Prerequisite Check Fails with Directories Not Empty Error During Retry

During an agent installation using Agent Deploy, the installation fails abruptly, displaying the Failure page. On clicking **Retry**, the installation fails again at the Prerequisite Check phase with an error stating the directories are not empty.

This could be because Oracle Universal Installer (OUI) is still running though the SSH connection that is closed on the remote host.

To resolve this issue, on the remote host, check if OUI is still running. Execute the following command to verify this:

```
ps -aef | grep -i ora
```

If OUI is still running, wait till OUI processes are complete and restart the SSH daemon. Now, you can click **Retry** to perform the installation.

**Note:** For more information on running the prerequisite checks in standalone mode, see Section 4.16, "Running the Prerequisite Check in Standalone Mode".

#### A.1.4.2 Agent Deployment on Linux Oracle RAC 10.2 Cluster Fails

Agent deployment on a 10.2 release of an Oracle RAC cluster may fail due to a lost SSH connection during the installation process.

This can happen if the `LoginGraceTime` value in the `sshd_config` file is 0 (zero). The zero value gives an indefinite time for SSH authentication.

To resolve this issue, modify the `LoginGraceTime` value in the `/etc/ssh/sshd_config` file be a higher value. The default value is 120 seconds. This means that the server will disconnect after this time if you have not successfully logged in.

To resolve this issue, modify the `LoginGraceTime` value in the `/etc/ssh/sshd_config` file to be a higher value. If the value is set to 0 (zero), there is no definite time limit for authentication.

#### A.1.4.3 SSH Verification Fails During Agent Installation

The most common reasons for SSH Verification to fail are the following:

- The server settings in `/etc/sshd/sshd_config file` do not allow `ssh` for user `$USER`.
- The server may have disabled the public key-based authentication.
- The client public key on the server may be outdated.
- You may not have passed the `-shared` option for shared remote users, or may have passed this option for non-shared remote users.

Verify the server setting and rerun the script to set up SSH successfully.

**Note:** For more information on how to set up SSH, see Section G.2, "SSH (Secure Shell) Setup".

##### A.1.4.3.1 Sample sshd_config File

The following `sshd_config` file sample is a server-wide configuration file with all the variables.

```
#$OpenBSD: sshd_config,v 1.59 2002/09/25 11:17:16 markus Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default values where
# possible, but leave them commented out.  Uncommented options change a
# default value.

#Port 22
#Protocol 2,1
#ListenAddress 0.0.0.0
#ListenAddress ::
```

```
# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_dsa_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 3600
#ServerKeyBits 768

# Logging
#obsoletes QuietMode
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 120
#PermitRootLogin yes
#StrictModes yes

#RSAAuthentication yes
#PubkeyAuthentication yes
#AuthorizedKeysFile.ssh/authorized_keys

# rhosts authentication should not be used
#RhostsAuthentication no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

#AFSTokenPassing no

# Kerberos TGT Passing only works with the AFS kaserver
#KerberosTgtPassing no

# Set this to 'yes' to enable PAM keyboard-interactive authentication
# Warning: enabling this may bypass the setting of 'PasswordAuthentication'
#PAMAuthenticationViaKbdInt no
```

```
#X11Forwarding no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PrintMotd yes
#PrintLastLog yes
#KeepAlive yes
#UseLogin no
#UsePrivilegeSeparation yes
#PermitUserEnvironment no
#Compression yes

#MaxStartups 10
# no default banner path
#Banner /some/path
#VerifyReverseMapping no
#ShowPatchLevel no

# override default of no subsystems
Subsystemsftp/usr/libexec/openssh/sftp-server
```

### A.1.4.4 SSH Setup Fails with "Invalid Port Number" Error

The SSH script when executed, is built to automatically verify the setup at the end, by executing the following command:

```
ssh -l <user> <remotemachine> 'date'
```

At the time of verification, you may encounter an "Invalid Port Error" indicating that the SSH setup was not successful.

This can happen if the `ssh.exe` (`sshUserSetupNT.sh` script) is not being invoked from the `cygwin` home directory.

To resolve this issue, ensure the `sshUserSetupNT.sh` script on the local OMS machine is being executed from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

If there are multiple Cygwin installations, and you want to find out which ssh.exe is being invoked, execute the following command:

```
C:\Cygwin\bin\which ssh
```

For example, when you execute the previously mentioned command, and it returns a result that is similar to the following:

```
\cygdrive\c\WINDOWS\ssh
```

This indicates that the `ssh.exe` file from Cygwin is not being invoked as there is `C:\windows` that is present before `C:\Cygwin\bin` in the PATH environment variable.

To resolve this issue, rename this ssh.exe as follows:

```
-C:\cygwin>move c:\WINDOWS\ssh.exe c:\WINDOWS\ssh.exe1
          1 file(s) moved.
```

Now, execute the `C:\Cygwin which ssh` command again.

The result should be similar to "`\usr\bin\ssh`".

This verifies that `ssh.exe` file is being invoked from the correct location (that is, from your `C:\Cygwin\bin` folder).

---

**Note:** You must ensure `C:\cygwin` is the default installation directory for the Cygwin binaries.

If you install `Cygwin` at a location other than `c:\cygwin` (default location), it can cause the SSH setup to fail, and in turn, the agent installation will fail too.

To work around this issue, you must either install `Cygwin` in the default directory (`c:\cygwin`), or update the `ssPaths_msplats.properties` file with the correct path to the `Cygwin` binaries.

You can look into the following remote registry key to find out the correct `Cygwin` path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\
```

---

---

**Note:** For more information on how to set up SSH, see Section G.2, "SSH (Secure Shell) Setup".

---

#### A.1.4.5 sshConnectivity.sh Script Fails

If you are executing the `sshConnectivity.sh` script on *Cygwin version 5.2*, the script may fail and result in the following error:

```
"JAVA.LANG.NOCLASSDEFFOUNDERROR"
```

To workaround this issue, ensure the Oracle home in the *Cygwin style path* is defined as follows:

```
ORACLE_HOME="c:/oraclehomes/oms10g/oracle"
```

You can find out the currently installed Cygwin version by executing the `uname` command on the Cygwin window.

---

**Note:** For more information on using the sshConnectivity.sh script, see Section G.2.2.1, "Setting Up SSH Using sshConnectivity.sh (Only For 10.2.0.2 Enterprise Manager Grid Control)".

---

#### A.1.4.6 Troubleshooting the "command cygrunsrv not found" Error.

During the SSH daemon setup, you may encounter a "`command cygrunsrv not found`" error. This can occur due to one of the following two reasons:

- The sshd service is not running.
- The Cygwin installation was not successful.

##### A.1.4.6.1 If SSHD Service Is Not Running

Create the sshd service, and then start a new sshd service from the `cygwin` directory.

To create the SSHD service, you must execute the following command:

```
ssh-host-config
```

The Cygwin script that runs when this command is executed will prompt you to answer several questions. Specify **yes** for the following questions:

- privilege separation
- install sshd as a service

Specify **no** when the script prompts you to answer whether or not to "create local user sshd".

When the script prompts you to specify a value for Cygwin, type `ntsec` (`CYGWIN="binmode tty ntsec"`).

Now that the SSHD service is created, you can start the service by executing the following command:

```
cygrunsrv -start sshd
```

#### A.1.4.6.2 If Your Cygwin Installation Was Unsuccessful

If restarting the SSHD service does not resolve the error, then you must reinstall Cygwin. To do this:

1. Remove the Keys and Subkeys under Cygnus Solutions using `regedit`.
2. Remove the Cygwin directory (`C:\cygwin`), and all Cygwin icons.
3. Remove the `.ssh` directory from the Documents and Settings folder of the domain user.
4. Reinstall Cygwin.

   For detailed instructions on Cygwin installation, see Section G.2.1.2, "Setting Up SSH Server (SSHD) on Microsoft Windows (Only For 10.2.0.1 and 10.2.0.3 Enterprise Manager Grid Control)"
5. Execute the following command to start SSH daemon:

   ```
   cygrunsrv -start sshd
   ```

### A.1.4.7 SSH Setup Verification Fails with "Read from socket failed: Connection reset by peer." Error

After the SSH setup is complete, the script automatically executes the following verification command:

```
ssh -l <user> <remotemachine> 'date'
```

If this command returns an error stating "Read from socket failed: Connection reset by peer", this means SSH was incorrectly set up. To resolve this issue, go to the remote machine where you attempted to set up SSH and do the following:

1. Stop the SSHD service (`cygrunsrv -stop sshd`).
2. Go to the `etc` directory (`cd /etc`).
3. Change the SSH file owner to the appropriate system (`chown <SYSTEM> ssh*`).
4. Go to the Cygwin command prompt and execute the following:

   ```
   chmod 644 /etc/ssh*
   chmod 755 /var/empty
   chmod 644 /var/log/sshd.log
   ```
5. Now, execute the verification command from the Management Service (OMS) machine (`ssh -l <user> <remote machine> 'date'`). This should display the date correctly, suggesting the SSH setup was successful.

6. Finally, start the SSHD service (from `/usr/bin/sshd`), or by executing `cygrunsrv -start sshd`.
7. Now, execute the verification command again from the OMS machine (`ssh -l <user> <remote machine> 'date'`). This should display the date correctly, suggesting the SSH setup was successful.

### A.1.4.8 SSHD Service Fails to Start

During SSHD configuration, the SSHD service is created for the local account by default. When you log in as a domain user, this account is not recognized by the service, and does not start up.

To resolve this issue, you must change the SSHD service "`Log On As`" value from `LocalSystem` to the domain user. To do this, complete the following steps:

1. Right-click on My Computer and select **Manage.**
2. In the Computer Management dialog box that appears, click **Services** under Services and Applications.
3. In the right pane, select the Cygwin SSHD service, right-click and go to Properties.
4. In the Cygwin SSHD Properties window that appears, select **This Account**.
5. Now, specify the appropriate domain name and user (in the form of `domain\user`, for example, `FOO-US\pjohn`).
6. Specify the password for this user, and click **Apply.**
7. Now, go to the Cygwin command prompt and execute the following:

   ```
   chmod 644 /etc/ssh*
   chmod 755 /var/empty
   chmod 644 /var/log/sshd.log
   ```

8. Start SSHD by executing the following command:

   ```
   /usr/sbin/sshd
   ```

### A.1.4.9 Timezone Prerequisite Check Fails

The timezone prerequisite check (`timezone_check`) will fail if the TZ environment variable is not set on the SSH daemon of the remote host.

To resolve this issue, you must set the TZ environment variable on the SSH daemon of the remote host. See Section G.2.4, "Setting Up the Timezone Variable on Remote Hosts" for more information.

Alternatively, you do the following:

- If you are installing or upgrading the agent from the default software location, set the timezone environment variable by specifying the following in the Additional Parameters section of the Agent Deploy application:

  ```
  -z <timezone>
  For example, -z PST8PDT
  ```

- If you are installing the agent from a nondefault software location, you must specify the timezone environment variable using the following command:

  ```
  s_timeZone=<timezone>
  For example, s_timezone=PST8PDT
  ```

### A.1.4.10 OMS Version Is Not Displayed

If the OMS version is not displayed in the log file, it could mean that the installed agent is not registered with a secure and locked Management Service (OMS).

You can verify this by executing the following commands:

```
emctl status oms
emctl status agent
```

To resolve this issue, you must manually secure the Management Agent by executing the following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

```
<AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
```

### A.1.4.11 Discrepancy Between Agent and Repository URL Protocols

If the agent installation is successful, the protocol for both agent and the repository URLs are the same. That is, both URLs start with the `https` protocol (meaning both are secure).

If the protocol for the agent URL is displayed as `http` instead of `https`, this means that the agent is not secure.

To resolve this issue, you must secure the agent manually by executing the following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

```
<AGENT_HOME>/bin/emctl secure agent -reg_passwd <password>
```

### A.1.4.12 Last Successful Upload Does Not Have a Time Stamp

If there is no time stamp against this parameter in the log (displays `Null`), it means that the agent is unable to upload any data.

To resolve this issue, you must perform a manual upload of the data by executing the following command, and then check the log again:

```
<AGENT_HOME>/bin emctl upload
```

### A.1.4.13 emctl status Log File is Empty

If the agent is not ready and running, the `emctl status` log displays only the copyright information. None of the parameters listed in the sample log is displayed.

The issue can occur due to any of the following reasons:

- Agent is not secure: To manually secure the agent, execute the following command. However, note that even after securing the Management Agent, some data might still be transferred over the network without being encrypted.

  ```
  <AGENT_HOME>/bin emctl secure agent -reg_passwd <password>
  ```

- Agent is not running: Check if the agent is running. If not, you can start the agent manually by executing the following command:

  ```
  <AGENT_HOME>/bin emctl start agent
  ```

- Agent port is not correct: Verify whether the agent is connecting to the correct port. To verify the port, look into the `sysman/config/emd.properties` file:

  You must also ensure the following are correctly set in the `emd.properties` file:

a. REPOSITORY_URL: Verify this URL (`http://<hostname>:port/em/upload`). Here, ensure the host name and port are correct.

b. emdWalletSrcURL: Verify if the host name and port are correct in this URL (`http://<hostname>:port/em/wallets/emd`).

c. agentTZRegion: Ensure the time zone that is configured is correct.

### A.1.4.14 Installation Fails When No Group ID or Group Name Is Created

Before you begin the installation of a Management Agent, ensure that the target host where you want to install the Management Agent has the appropriate users and operating system groups created. For information about creating required users and operating system groups, see Section 3.6, "Operating System Groups and Users Requirements".

Also ensure that the target host has the group name as well as the group id created. Otherwise, the installation will fail.

To check whether the group id, group name, user id, and user name are created, run the id command.

For example, when you run the id command, your result of the command could be something like this. Here you can see that the group 621 does not have a group name.

```
uid=31000(rparasur) gid=621 groups=502(g502),621,8500(dba),42424(svrtech)
```

To create the group name, run the following command (*specific to this example*):

```
groupadd g621 -g 621
```

Now if you run the id command, you will see this:

```
uid=31000(rparasur) gid=621(g621)
groups=502(g502),621(g621),8500(dba),42424(svrtech)
```

This way, ensure that your target host has the user id, user name, group id, and group name created. For information about creating required users and operating system groups, see Section 3.6, "Operating System Groups and Users Requirements".

### A.1.4.15 Installation Fails with Host Name Error on the Product-Specific Prerequisite Check Page

While installing a Management Agent, the installation can fail on the product-specific prerequisite page with a host name error. This happens when the host name specified in the host file does not map to the correct IP address of that host.

To resolve this issue, first run the following command on the host to list all the IP addresses configured and then note the IP address for that host:

```
ipconfig /all
```

After noting the IP address of that host, open the host file and check the entries for this host name. Ensure that the host name maps to the correct IP address of that host.

### A.1.4.16 Installation Fails While Securing Agent Communication with OMS

While installing a Management Agent, an Agent Registration password is requested if the Management Service that is specified is found to be running in a secure mode. However, despite providing the password, if the installation fails while securing the communication between the Management Agent and the Management Service, then check the password you provided.

If the password you have provided is incorrect, first, obtain the correct password from the user who configured the Management Service for SSL.

If you have forgotten the password, then reset it using the emctl command or using the Grid Control console.

If you want to reset the password using emctl command, then run the following command from the Oracle home directory of the Agent:

```
emctl setpasswd <old password> <new password>
```

If you want to reset the password using the Grid Control console, then login to Grid Control as SYSMAN, select **Setup** from the top-right corner of the page, select **Registration Passwords** from the left menu panel, and on the Registration Password page, click **Add Registration Password**.

### A.1.5 Oracle Configuration Manager Fails While Installing Management Agent

While installing the product, on the My Oracle Support page, you are required to provide email address and My Oracle Support (formerly Metalink) password. After providing the required information, when you try to navigate to the next screen and proceed with the installation, you may see some errors stating the installation of Oracle Configuration Manager failed. This error occurs when you (the user installing the Management Agent) does not have *write* permission on crontab.

To resolve this issue, check whether you (the user installing the Management Agent) have the necessary *write* permission on crontab. If you do not, then create an entry for your user account in the `/usr/lib/cron/cron.allow` file.

## A.2 Configuration Issues

This section lists some of the most commonly encountered configuration issues, and their resolutions.

### A.2.1 Configuration Assistants Fail During Enterprise Manager Installation

During the installation, if any of the configuration assistants fail to run successfully, then you can choose to run them in a standalone mode.

One of the ways to run the configuration assistants in a standalone more is to use the runConfig tool. The following is the sytax of its usage where options, such as OPTION1, OPTION2, and so on are options as described in Appendix A.2.1.6, "Options You Can Specify to Run runConfig Tool".

```
./runConfig.sh OPTION1=value1 OPTION2=value2 ...
```

Another way to run the configuration assistants in a standalone more is to use the `configToolFailedCommands` script that is created in the respective Oracle home directories. The syntax of its usage is:

```
./configToolFailedCommands
```

**Note:** The individual log files for each configuration tool are available at the following directory:

```
ORACLE_HOME/cfgtoollogs/cfgfw
```

Besides the individual configuration logs, this directory also contains `cfmLogger_timestamp.log` (The timestamp depends on the local time and has a format such as `cfmLogger_2005_08_19_01-27-05-AM.log`.). This log file contains all the configuration tool logs.

For more information about the installation logs that are created and their locations, see Appendix B, "Installation and Configuration Log Files".

The following sections describe how the runConfig tool can be used to run the configuration assistants in a standalone mode, particularly when they fail during the installation.

#### A.2.1.1 Invoking the One-Off Patches Configuration Assistant in Standalone Mode

During the installation process, this configuration assistant is executed before the Management Service Configuration Assistant is run.

This configuration assistant applies the one-off patches that are required for a successful Enterprise Manager 10*g* Release 2 installation.

To run this configuration assistant in standalone mode, you must execute the following command from the Management Service Oracle home:

```
<OMS_HOME>/perl/bin/perl <OMS_HOME>/install/oneoffs/applyOneoffs.pl
```

#### A.2.1.2 Invoking the Database Configuration Assistant in Standalone Mode

To run the Database Configuration Assistant, you must invoke the `runConfig.sh` script as:

```
<DB_Home>/oui/bin/runConfig.sh ORACLE_HOME=<DB_HOME> ACTION=Configure MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

#### A.2.1.3 Invoking the OMS Configuration Assistant in Standalone Mode

To run the OMSConfig Assistant, you must invoke the runConfig.sh as the following:

```
<OMS_Home>/oui/bin/runConfig.sh ORACLE_HOME=<OMS_HOME> ACTION=Configure
MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

#### A.2.1.4 Invoking the Agent Configuration Assistant in Standalone Mode

To run the AgentConfig Assistant, you must invoke the `runConfig.sh` as the following:

```
<Agent_Home>/oui/bin/runConfig.sh ORACLE_HOME=<AGENT_HOME> ACTION=Configure
MODE=Perform
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the above-mentioned command.

---

**Note:** While the preceding command can be used to execute the `agentca` script, Oracle recommends you execute the following command to invoke the configuration assistant:

```
Agent_Home/bin/agentca -f
```

If you want to run the `agentca` script on a Oracle RAC, you must execute the following command on each of the cluster nodes:

```
Agent_Home/bin/agentca -f -c "node1,node2,node3,...."
```

See Section 15.6, "Reconfiguring and Rediscovering Agent" for more information.

---

### A.2.1.5 Invoking the OC4J Configuration Assistant in Standalone Mode

If you want to deploy only the Rules Manager, execute the following commands:

```
/scratch/OracleHomes/oms10g/jdk/bin/java -Xmx512M
-DemLocOverride=/scratch/OracleHomes/oms10g -classpath
/scratch/OracleHomes/oms10g/dcm/lib/dcm.jar:/scratch/OracleHomes/oms10g/jlib/e
mConfigInstall.jar:/scratch/OracleHomes/oms10g/lib/classes12.zip:/scratch/Orac
leHomes/oms10g/lib/dms.jar:/scratch/OracleHomes/oms10g/j2ee/home/oc4j.jar:/scr
atch/OracleHomes/oms10g/lib/xschema.jar:/scratch/OracleHomes/oms10g/lib/xmlpar
serv2.jar:/scratch/OracleHomes/oms10g/opmn/lib/ons.jar:/scratch/OracleHomes/om
s10g/dcm/lib/oc4j_deploy_tools.jar oracle.j2ee.tools.deploy.Oc4jDeploy
-oraclehome /scratch/OracleHomes/oms10g -verbose -inifile
/scratch/OracleHomes/oms10g/j2ee/deploy.master -redeploy
```

On Microsoft Windows, replace `runConfig.sh` with `runConfig.bat` in the previously mentioned command.

### A.2.1.6 Options You Can Specify to Run runConfig Tool

You can specify the following options to execute the `runConfig` tool.

#### A.2.1.6.1 ORACLE_HOME

This is the absolute location of the Oracle home. All products/top-level components under this Oracle home that have been installed using the Oracle Universal Installer (OUI) 10*g* R 2 (10.2) are eligible for the **ACTION.** Products installed using an OUI that is earlier to 10.2 are not eligible for this ACTION.

#### A.2.1.6.2 ACTION

This is a mandatory option. This option can have values such as **`configure`**/**`clone`** / **`addnode`**/**`addlanguage`**/**`deconfigure`**/**`patchsetConfigure`**.

#### A.2.1.6.3 MODE

This is optional, and can have values such as **`perform`**/**`showStatus`**/**`listTools`**. For example, if the value is **`perform`**, then that ACTION is performed.

If **MODE** is absent, the MODE option will assume a default value of **`listTools`**.

If the value is **`showStatus`**, the status of the last-performed ACTION is displayed to the user.

**Examples**

```
Tool1 - Optional    - Failed
Tool2 - Recommended - Succeeded
Tool3 - Optional    - Succeeded
```

If the value of MODE option is **`listTools`**, a list of recommended/optional/other tools for the specified ACTION are displayed.

**Example**

```
Recommended Tools(1): Tool2
Optional Tools (2): Tool1, Tool3
Other Tools(0):
```

#### A.2.1.6.4 COMPONENT_XML

This is optional. You can specify a comma-separated list of Aggregate XML names from the OH/inventory/ContentsXML/ConfigXML/ and only these XMLs and the items dependent on them will be configured. If there are two components with the same name in the ORACLE_HOME, the one that is of a later version is considered for the ACTION option.

#### A.2.1.6.5 RESPONSE_FILE

This is optional. This is the absolute location of the response file that is used to overwrite some existing parameters. Pairs such as `ComponentID|variable = value` are to be specified in this file, per line, per variable as:

```
oracle.assistants.server|var1=true
oracle.network.client|var2=orcl
```

**Example**

```
RESPONSE_FILE=/scratch/rspfile.properties
```

**Note:** Secure variables are not stored in the instance aggregate XML files and hence while running runConfig, if any of the configuration tools that you want to run use secure variables, such as passwords, you must supply the value of these secure variables using the RESPONSE_FILE option of runConfig. Otherwise, the tools with secure variables as arguments fail.

#### A.2.1.6.6 INV_PTR_LOC

This is optional. This is the full path of `oraInst.loc` file.

The `orainst.loc` file contains `inventory_loc=<location of central inventory>`

inst_group=<>

**Example**

```
INV_PTR_LOC=<absolute path of oraInst.loc>
```

#### A.2.1.6.7 RERUN

This is **optional.** Possible values are **true** and **false**. RERUN has a default value of `false`. This means that only failed tools or those tools that were skipped are executed. All those tools that were successfully executed are skipped during the rerun.

A RERUN=true value will execute all the tools anew, including the tools that completed successful runs.

#### A.2.1.6.8 Typical Usage of the runConfig.sh

A typical usage of the runConfig.sh script is as follows:

```
./runConfig.sh ORACLE_HOME=<path of database home> ACTION=configure
MODE=perform COMPONENT_XML={encap_emseed.1_0_0_0_0.xml}
```

> **Note:** On Microsoft Windows, replace runConfig.sh with runConfig.bat or just runConfig (without the file extension).

#### A.2.1.6.9 runConfig Log Files

The log files for runConfig configActions<timestamp>.log/.err are generated under ORACLE_HOME/cfgtoollogs/oui/.

## A.2.2 Enterprise Manager Deployment Fails

Enterprise Manager deployment may fail due to the Rules Manager deployment failure.

To resolve this issue, redeploy Enterprise Manager by following these steps:

1. Move OH/j2ee/deploy.master to OH/j2ee/deploy.master.bak.
2. Execute the OH/bin/EMDeploy script.
3. Restore the OH/j2ee/deploy.master. That is, execute mv OH/j2ee/deploy.master.bak OH/j2ee/deploy.master

## A.2.3 Oracle Management Service Configuration Fails

Oracle Management Service configuration may fail due the following reasons.

### A.2.3.1 Oracle Management Service Fails While Deploying Enterprise Manager AgentPush Application

The cfgfw logs display the following error:

```
Redeploying application 'EMAgentPush' to OC4J instance 'OC4J_EMPROV'. FAILED!
ERROR: Caught exception while deploying 'EMAgentPush' to 'OC4J_
EMPROV':java.lang.reflect.InvocationTargetException at
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
```

This error is due to Ipv6 entries in /etc/hosts file. When prompted to execute root.sh or when configuration fails, do the following:

1. In <OMS Home>/sysman/install/EMDeployTool.pm, include "-Djava.net.preferIPv4Stack=true" in the command executed in deployEmEar ().
2. In <OMS Home>/opmn/conf/opmn.xml, include "-Djava.net.preferIPv4Stack=true" in java-options of all OC4J processes.

### A.2.3.2 In 'Enterprise Manager with new Database' Install, Oracle Management Service Configuration Fails While Unlocking Passwords

The cfgfw logs display the following error:

```
Failed to initialize JDBC Connection
```

This is caused when listener does not start during NetCA execution and the following error will be present in the installActions log:

```
Listener start failed. Listener may already be running.
```

To rectify this error, add the following line in <DB Home>/network/admin/listener.ora:

```
SUBSCRIBE_FOR_NODE_DOWN_EVENT_<listener_name>=OFF
```

Then, restart the listener.

#### A.2.3.3 Dropping of Repository Hangs If SYSMAN Sessions are Active

While installing Enterprise Manager using existing database, Oracle Management Service configuration hangs while dropping the repository. This is due to active SYSMAN sessions connected to the database.

To resolve this issue, shutdown any existing Enterprise Manager sessions (both Grid Control and Database Control) or other SQLPLUS SYSMAN sessions.

#### A.2.3.4 If Oracle Management Service Configuration is Retried, oracle.sysman.emSDK.svlt.ConsoleServerHost and oracle.sysman.emSDK.svlt.ConsoleServerName in emoms.properties are Swapped and There is an Extra Underscore in ConsoleServerHost

This problem only occurs with 10.2.0.1.0 Additional Oracle Management Server installation.

To resolve this issue, swap the values and remove the extra underscore in ConsoleServerName in emoms.properties present in <OMS_ORACLE_HOME>/sysman/config directory.

## A.3 Enterprise Manager Upgrade and Recovery Issues

The Enterprise Manager 10*g* Release 2 upgrade is an out-of-place upgrade, meaning that Enterprise Manager 10*g* Release 2 Oracle homes are separate from the old homes. If you decide to abort the upgrade process during the copying phase (copying of the binaries), you can simply revert to your old 10*g* Release 1 installation.

The upgrade process creates a new OMS home and a new database home. The Upgrade assistants upgrade the datafiles and `SYSMAN` schema, and then configure the new Oracle homes.

**Caution:** Do not abort the upgrade process during the configuration phase, as this will corrupt the installation. You will not be able to revert to the old 10*g* Release 1 installation either.

### A.3.1 Agent Upgrade Issues

This section lists some of the issues that you may encounter during an agent upgrade.

#### A.3.1.1 Agent Does Not Start Up After Upgrade

During an agent upgrade from 10.1.0.*n* to 10.2.0.2, the agent may fail to start up after upgrade if the time zone that is configured for the upgraded agent is different from the originally configured agent.

You can correct this issue by changing the time zone. To do this, execute the following command from the upgraded agent home:

```
emctl resetTZ agent
```

This command will correct the agent-side time zone, and specify an additional command to be run against the repository to correct the value there.

> **Caution:** Before you change the time zone, check if there are any blackouts that are currently running or scheduled to run on any of the targets that are monitored by the upgraded agent. Do the following to check this:
>
> 1. In the Grid Control console, go to the All Targets page under Targets and locate the Agent in the list of targets. Click the agent name link. The Agent home page appears.
> 2. The list of targets monitored by the agent will be listed in the *Monitored Targets* section.
> 3. For each target in the list, click the target name to view the target home page.
> 4. Here, in the Related Links section, click **Blackouts** to check any blackouts that are currently running or may be scheduled to run in the future.
> 5. If such blackouts exist, you must stop all the blackouts that are running on all the targets monitored by this agent.
> 6. From the console, stop all the targets that are scheduled to run on any of these monitored targets.
> 7. Now, run the following command from the agent home to reset the time zone;
>
>    ```
>    emctl resetTZ agent
>    ```
>
> 8. After the time zone is reset, you can create new blackouts on the targets.

#### A.3.1.2 Missing Directories When Upgrading Agent from 10.1.0.5 to 10.2.0.1

In a Windows NT RAC agent upgrade scenario, after the AgentOnly shiphome installer has completed installation, the utility <Upgrade AOH>/oui/bin/upgrade has to be executed on every single node in the RAC to complete the agent upgrade.

#### A.3.1.3 Agent Deploy Application Keeps Running Even After Upgrade on an NT Shared Location Is Successful

To upgrade the Management Agent on a shared cluster, follow these steps:

1. On the target machine, make sure that the *.backup* extension is associated with `cmd.exe`.
2. If this is not the case, then during the upgrade when the Agent Deploy application displays *installing* on the progress page, check the target machines.
3. With the exception of the first host in the hosts list, a message may appear for all other hosts displaying the following text:

   ```
   Windows cannot open this file emctl.bat.upgrade.backup
   ```

4. Select `cmd.exe` to open this file and then you will see the upgrade process proceed.

To check the extension association, open Microsoft Windows File Explorer. From the menu, select **Tools**, then select **Folder Options**, and then select the **File Types** tab. Search for the *.backup* extension.

## A.3.2 Enterprise Manager Recovery

This sections provides the instructions to be followed to perform an Enterprise Manager recovery.

### A.3.2.1 Steps to Follow for Agent Recovery

Use the following instructions to perform an agent recovery:

1. After exiting the installer, you must open a new window and change the directory to the `<New_AgentHome>/bin`.
2. Execute the script `./upgrade_recover`.
3. You can then start the old agent and continue using it. If you want to remove the installed binaries of the new agent home, use the Remove Productions function of the installer.

### A.3.2.2 Steps to Follow for OMS Recovery

If the schema has been upgraded or the upgrade was incomplete, you must manually restore the database to the backup that was taken prior to executing the OMS upgrade.

You can determine the status of the repository upgrade by looking into the log file at `<New_OMSHome>/sysman/log/emrepmgr.log.<proc_id>`. The last line of the log file provides the status of the upgrade. If the upgrade was completed without errors, it reads *Repository Upgrade Successful*. If not, the message *Repository Upgrade has errors…* is displayed.

Follow these instructions to perform an OMS recovery:

> **Note:** Before you attempt to restore the database, you must exit the Upgrade wizard. You must also ensure there are no OMS processes that are running. See Section 22.2.1, "Shut Down Grid Control Before Upgrade" for more information on shutting down the Enterprise Manager processes.

> **Caution:** Ensure all OMS processes are completely shut down. If not, the system may become unstable after the upgrade.

1. Restore the database to the backup. See Oracle Database Administrator's Guide for more information.
2. After the database is restored, start the database and listener to ensure successful restoration.
3. Open a new window and change the directory to the `<New_OMSHome>/bin`.
4. Now, execute the `./upgrade_recover`.

Start the old OMS and continue to use it. If you want to remove the binaries of the newly installed OMS home, use the Remove Productions function in the installer.

### A.3.2.3 Steps to Re-create the Repository

If the Management Service configuration plugin fails due to the repository creation failure, rerunning the configuration tool from Oracle Universal Installer drops the repository and re-creates it. However, if you want to manually drop the repository, complete the following steps:

#### A.3.2.3.1 Dropping the Repository

1. Stop the OPMN processes (`<OMSHOME>/bin/opmnctl stopall`), Management Service (`<OMS_HOME>/bin/emctl stop oms`), and Agent (`<AGENT_HOME>/bin/emctl stop agent`) before dropping the repository.
2. Set ORACLE_HOME to `OMS_OracleHome`
3. Execute `OMS_Home/sysman/admin/emdrep/bin/RepManager <hostname> <port> <SID> -action drop -output_file <log_file>`

#### A.3.2.3.2 Creating the Repository

1. Set ORACLE_HOME to `OMS_OracleHome`.
2. Execute `OMS_Home/sysman/admin/emdrep/bin/RepManager <hostname> <port> <SID> -action create -output_file <log_file>`.

**Note:** After recreating the repository, you must run the following command on all the Management Service Oracle homes to reconfigure the `emkey`:

```
emctl config emkey -repos -force
```

This command overwrites the `emkey.ora` file with the newly generated `emkey`.

**Caution:** While recreating the repository using `./Repmanager -action create` command, you may encounter the following error message:

```
java.sql.SQLExecution: ORA-28000: the account is locked during
recreation of repository.
```

*Workaround*

This error may occur if there are processes or multiple Management Services that are trying to connect to the database with incorrect SYSMAN credentials. If there are multiple login failures, the database becomes locked up and shuts down the monitoring agent.

You can resolve this issue by shutting down all the Management Services connected to the database, along with the monitoring agent.

## A.3.3 Repository Creation Fails

When installing Enterprise Manager using an existing database, the repository creation fails.

This may happen if the profile of the Password Verification resource name in the database has a value that is other than *Default*. To resolve this issue:

1. Change the Password Verification profile value to *Default*.
2. Create the repository using RepManager command.

You may also see the following error at the end of the installation when repository creation fails:

```
Enter user-name: Error accessing PRODUCT_USER_PROFILE
Warning:  Product user profile information not loaded!
You may need to run PUPBLD.SQL as SYSTEM
```

In this case, ensure that PRODUCT_USER_PROFILE exists in the repository. Otherwise, run the PUPBLD.SQL as SYSTEM.

### A.3.4 Collection Errors After Upgrade

If you upgrade only the Management Service to 10*g* Release 2 without upgrading the monitoring agent, you may encounter the following collection errors:

- Target Management Services and Repository
- Type OMS and Repository
- Metric Response
- Collection Timestamp <session_time_stamp>
- Error Type Collection Failure
- Message Target is in Broken State. Reason - Target deleted from agent

To resolve this issue, upgrade the monitoring agent along with the Management Service to 10*g* Release 2.

## A.4 Oracle Management Service Upgrade Issues

You may encounter problems during Management Service upgrade where the upgrade process aborts due to the following reasons.

### A.4.1 OMS Upgrade Stops at OracleAS Upgrade Assistant Failure

The installation dialog box and the configuration framework log file (located at`<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log`) lists `SEVERE` messages indicating the reason the Oracle Application Server Upgrade Assistant fails.

If the message displays *permission denied* on certain files, it means that the user running the installer may not have the correct permissions to run certain iAS configurations.

To resolve this issue, comment out the OracleAS configuration that contains these files and then retry the upgrade again. You can reapply the configurations after the upgrade is successfully completed.

### A.4.2 OMS Configuration Stops at EMDeploy Failure

The most common reasons for EMDeploy to fail are if:

- All Enterprise Manager processes are not shut down completely.

  To shut down Enterprise Manager, execute the following commands:

  ```
  <Oracle_Home>/opmn/bin/opmnctl stopall
  <Oracle_Home>/bin/emctl stop em
  ```

See Section 22.2.1, "Shut Down Grid Control Before Upgrade" for more information.

- Symbolic links have been used instead of hard links

  The `<Oracle_Home>/Apache/<component>` configuration files must be examined to ensure only hard links (and no symbolic links) were referenced. See Section 22.2.2, "Check for Symbolic Links" for more information.

After you have successfully resolved these issues, perform the redeploy steps manually and click **Retry** on the Upgrade wizard.

### A.4.3 OMS Configuration Stops at Repository Schema Failure (RepManager)

The most common reason the repository schema configuration fails is when it is not able to connect to the listener. The configuration framework log file (`<New_OracleHome>/cfgtoollogs/cfgfw/oracle.sysman.top.oms_#date.log`) indicates the reason for the repository schema upgrade failure.

To resolve this issue, you must verify whether or not the listener connecting to the OMS is valid and active.

Also, if you have installed the OMS using the *Install Enterprise Manager Using New Database* installation type, ensure there are no symbolic links being referenced. After you have successfully established the listener connections, click **Retry** on the Upgrade wizard.

### A.4.4 Monitoring Agent Does Not Discover Upgraded Targets

If you have upgraded an Enterprise Manager Grid Control target (for example, database) independently (that is using a regular upgrade mechanism other than the Oracle Universal Installer), the monitoring agent may fail to discover this upgraded target.

This can happen if you have specified a different Oracle home value for the upgraded target other than the one that already existed.

To resolve this issue, you must manually configure the `targets.xml`file of the monitoring agent to update the configuration details of the upgraded Oracle home information, or log in to the Enterprise Manager console, select the appropriate target, and modify its configuration parameters to reflect the upgraded target parameters.

### A.4.5 CSA Collector Is Not Discovered During Agent Upgrade

When a 10*g* Release 1 Management Service and its associated (monitoring) agent are upgraded at the same time, the agent upgrade does not discover the CSA Collector target.

To discover this target, you must run the agent configuration assistant (the `agentca` script) using the rediscovery option. See Section 15.6.1, "Rediscover and Reconfigure Targets on Standalone Agents" for more information.

### A.4.6 ias_admin Password Is Set To welcome1 After Upgrade

To resolve this issue, run the following command:

```
<New OMS Home>/bin/emctl set password welcome1 <New Password>
```

### A.4.7 Oracle Management Service Upgrade Fails If Older Listener Is Running On A Port Other Than 1521

To resolve this issue, do the following:

1. Stop the older listener when prompted to execute allroot.sh. The Oracle Management Service upgrade will fail.
2. Set the listener from the new database to run from the same non-1521 port.
3. Run the upgrade again.

### A.4.8 If TAF String Is Used in Grid Control, then Upgrade Fails

If TAF (Transparent Application Failover) string is used in 10.2.0.x.x GC, then the patching process will fail while patching an existing release of Enterprise Manager Grid Control to 10.2.0.2.0, 10.2.0.3.0, or 10.2.0.4.0 or higher.

To resolve this issue, follow below workarounds.

**Workaround 1:**

Change the ConnectDescriptor in the emoms.properties to the sqlnet ConnectDescriptor. Then try running the config tool again. After the installation completes, change the connect string back to TAF.

For example, the sqlnet connect descriptor is:

```
oracle.sysman.eml.mntr.emdRepConnectDescriptor=(DESCRIPTION\=(ADDRESS_
LIST\=(ADDRESS\=(PROTOCOL\=TCP)(HOST\=stada37.us.oracle.com)
(PORT\=1521)))(CONNECT_DATA\=(SERVICE_NAME\=emrep11.us.oracle.com)))
```

Alternatively, you can use this approach for Workaround 1:

Exit the OUI installer. Change the ConnectDescriptor in the emoms.properties to the sqlnet Connect Descriptor. Then run the following runConfig command to continue the install, and then after the installation completes, change the connect string back to TAF.

1. Navigate to the bin directory:

   ```
   cd <OMS_ORACLE_HOME>/oui/bin
   ```

2. Run the following command:

   *For Linux:*

   ```
   ./runConfig.sh ORACLE_HOME=<OMS_Oracle_Home> ACTION=patchsetConfigure
   MODE=perform COMPONENT_XML=oracle.sysman.top.oms.<version>.xml
   ```

   Here, the version can be '10_2_0_3_0'.

   *For Microsoft Windows:*

   ```
   runConfig.bat ORACLE_HOME=<OMS_Oracle_Home> ACTION=patchsetConfigure
   MODE=perform COMPONENT_XML=oracle.sysman.top.oms.<version>.xml
   ```

   Here, the version can be '10_2_0_3_0'.

**Workaround 2:**

If you upgraded the repository manually after the installation fails, then in order to run the remaining config tools by skipping the Repository Upgrade Config Tool, follow these steps:

1. Exit the OUI installer.

2. Edit the response file by adding the following parameter:

   ```
   b_reposPatchUpgrade =false
   ```

3. Navigate to the bin directory:

   ```
   cd <OMS_ORACLE_HOME>/oui/bin
   ```

4. Run the following command:

   *For Linux:*

   ```
   ./runConfig.sh ORACLE_HOME=<OMS_Oracle_Home> ACTION=patchsetConfigure
   MODE=performn COMPONENT_XML=oracle.sysman.top.oms.<version>.xml
   ```

   Here, the version can be '10_2_0_3_0'.

   *For Microsoft Windows:*

   ```
   runConfig.bat ORACLE_HOME=<OMS_Oracle_Home> ACTION=patchsetConfigure
   MODE=perform COMPONENT_XML=oracle.sysman.top.oms.<version>.xml
   ```

   Here, the version can be '10_2_0_3_0'.

## A.5 Troubleshooting Management Agent Issues

The Oracle Management Agent (Management Agent) monitors and manages different entities in your enterprise. If the system crashes or hangs due to an error, you can use the following options to diagnose, investigate and troubleshoot the problem:

- Generating a Diagnosable Dump
- Reference Counting
- Tracking CPU Thread Times

### A.5.1 Generating a Diagnosable Dump

A memory dump is printed onto the file system when any of these following events occur:

- System crash or a memory exception
- struct_id errors
- Assert failure

A dump file can also be an user generated event. The dump file provides a snapshot of the state of the agent when the crash occurred. It contains the stack and memory details, the thread that is being used, and the heap memory. The dump file is useful in determining the cause of the issue and helps better diagnosis. You can examine the stack thoroughly and view the actual thread from which the event occurred.

The dump file can be viewed on a per thread basis or component-by-component basis. Depending on the error situation, a fatal or a non-fatal dump is generated. An agent crash for example, generates a fatal dump. The dump file including its location can be customized by specifying the following properties in the `emd.properties` file.

- `DUMPDIR`: This is the directory in which the dump file is generated. By default, the file is stored in `ORACLE_HOME/sysman/dump` directory.
- `SIZETRACELIMIT`: The trace file should not exceed the value specified here. The default limit is 20 MB.

- `MAXTRACES`: The maximum number of trace files that can be retained at given point in time. By default a maximum of 10 files can be retained. The retaining policy ensures that fatal dumps are retained and non-fatal dumps are deleted.

```
Example 18.1 Non-Fatal Dump
EMAGENT Ver:10.2.0.5.0
NON-FATAL DUMP
User-initiated dumpstate


----- Call Stack Trace -----
calling              call     entry                argument values in hex
location             type     point                (? means dubious value)
-------------------- -------- -------------------- ----------------------------
nmegsm_beginDump()+  call     B6F21870             B3F70E80 ? 2 ? B3F70E80 ?
855                                                818A248 ?
nmemdisp_DumpStateR  call     B6F277E0             804F328 ? B70D86AC ? 0 ? 1 ?
eq()+280                                           B3F70F10 ? 0 ?
nmemdisp_Dispatcher  call     nmemdisp_DumpStateR  804F328 ? 80D3930 ? 0 ?
_main()+1693                  eq()                 FFFFFFFF ? 77AFF4 ? 77C820 ?
nmehl_processIncomi  call     00000000             80B2D08 ? 0 ? 0 ? 0 ? 0 ? 0 ?
ngRequest()+1028
nmtw_runWork()+53    call     00000000             80B2D08 ? B71CC0EC ?
                                                   B3F713A4 ? B6F727D7 ?
                                                   8188CF8 ? 8085400 ?
nmttp_run()+129      call     B6F282E0             8188CF8 ? 8085400 ?
                                                   B70EFAF0 ? B71CC0EC ?
                                                   804F328 ? 8070810 ?
nmttp_runSystemThre  call     nmttp_run()          8188CF8 ? 8ADFF4 ? 0 ?
ad()+33                                            B3F714C8 ? 8A43CC ? 8188CF8 ?
start_thread()+172   call     00000000             8188CF8 ? 2 ? 2 ? 2 ?
__clone()+94         call     00000000             B3F71BA0 ? 0 ? 0 ? 0 ? 0 ?
                                                   0 ?
--------------------- Binary Stack Dump ---------------------
========== FRAME [1] (nmegsm_beginDump()+855 -> B6F21870) ==========
defined by frame pointers 0xb3f70ef4  and 0xb3f70a68
CALL TYPE: call   ERROR SIGNALED: no   CALLER: nmegsm_beginDump
Dump of memory from 0xb3f70af4 to 0xb3f70ef4
B3F70AF0          00000000 00000000 00000000      [............]
B3F70B00 00000000 00000000 00000000 00000000  [................]
        Repeat 55 times
B3F70E80 B6F75934 B6F75922 B6F75934 B6F75922  [4Y.."Y..4Y.."Y..]
B3F70E90 0818A248 0818A248 00000000 00000000  [H...H...........]
B3F70EA0 00000000 00000000 00000000 00000000  [................]
        Repeat 1 times
B3F70EC0 00000000 00000000 00000000 B71CC0EC  [................]
B3F70ED0 080D3930 080D38F8 B3F70F10 00006480  [09...8.......d..]
B3F70EE0 080B3560 0804F328 00000001 0818A254  [`5..(.......T...]
B3F70EF0 00000000                             [....]
========== FRAME [2] (nmemdisp_DumpStateReq()+280 -> B6F277E0) ==========
defined by frame pointers 0xb3f71138  and 0xb3f70ef4
CALL TYPE: call   ERROR SIGNALED: no   CALLER: nmemdisp_DumpStateReq
Dump of memory from 0xb3f70ef4 to 0xb3f71138
B3F70EF0          B3F71138 B6F33C04 0804F328      [8....<..(...]
B3F70F00 B70D86AC 00000000 00000001 B3F70F10  [................]
B3F70F10 00000000 00000209 08053980 00000209  [.........9......]
B3F70F20 B4F98320 006B29B4 006B29B4 B7D546D7  [ ....)k..)k..F..]
B3F70F30 00000000 08189410 00000209 000001E9  [................]
B3F70F40 00000185 B4F9956C 00000209 00000209  [....l...........]
...
```

```
----- End of Call Stack Trace -----
------------------------------------------------------------------
Dumping component: targets
------------------------------------------------------------------
nmeetm_TargetManager = 0xb518a510

{


HEX dump
B518A510 00003072 0804F328 080850D8 B518A578  [r0..(....P..x...]
B518A520 B518A6B0 B518A700 080AC248 00000000  [........H.......]
B518A530 0000000A 00000000 0806D250 00000000  [........P.......]
B518A540 49767EC9 000000F2 00000000 080960F8  [.~vI.........`..]
B518A550 00000000 B5147780 00000000 00000000  [.....w..........]
B518A560 00000078 00000004 00000008 00000000  [x...............]
B518A570 00000000                             [....]
  ub4 struct_id = 12402
  nmectx* gctx = 0x804f328
  nmeulctx* lctx = 0x80850d8
  nmeumx_Mutex* mutex = 0xb518a578
  nmeumx_Mutex* tgtChgMutex = 0xb518a6b0
  nmeumx_Mutex* MXProgDisc_nmeetm = 0xb518a700
  nmedts_Targets* targets = 0x80ac248
  nmedts_Targets* oldTgts = (nil)
  ub4 propCompThrds = 10
  boolean bDynPropChanged = FALSE
  nmedt_Target* hostTarget = 0x806d250
  OraText* agentTgtGuid = (nil)
  time_t load_timestamp = 0xb518a540
  ubig_ora fileSize_nmeetm = 242
  OraText* parseError = (nil)
  OraText* emdTargetName_nmeetm = 0x80960f8 "stadm48.us.oracle.com:6321"
  boolean disableSelfMon_nmeetm = FALSE
  nmeuv_Vector* tgtChgEvents_nmeetm = 0xb5147780
=>   0x80b3878
=>   0x80b3668
=>   0x80de290
=>   0xb5a0f3e0
  boolean bFromCLI = FALSE
  boolean bNotAllowSave = FALSE
  sword dynamicPropReComputeInterval = 120
  sword dynamicPropReComputeMaxTries = 4
  ub4 maxDataRowsetFiles = 8
  ub4 maxDataRowsetFilesProp = 0
  ub4 DynPropRecomputeSeed = 0
}nmeetm_TargetManager
...
------------------------------------------------------------------
Dumping component: refcnt
------------------------------------------------------------------
nmeuca_CircularArray = 0xb5197720

{
      {
                thread ID = 0xb3f70cc0 "3019316128"
                struct ID = 10302
                address = 0x806d250
                count = 4
                action = 0xb70f01a4 "acquire"
```

```
             activity ID = 589827
             time (centi-seconds ago) = 134524
            call stack =
                     nmedt_Target_addReferenceCount()+87
                     nmeetm_getTargetInstanceCheckDeleted()+175
                     nmeetm_getTargetInstance()+77
                     nmeetm_getTarget()+80
                     nmecci_run()+1043
     }
}
```

### A.5.1.1 Command Line Options to Generate the Dump File

The dump file can also be generated using command line options. The command line options available are:

`$emctl dumpstate agent`: Generates a dump file at the current state.

`$emctl dumpstate agent <subsystem>`: Provides the status of a specific subsystem.

`$emctl dumpstate agent list`: Provides the list of components in the dump file.

`$emctl dumpstate agent <comp1> <comp2> <comp3>`: Provides the list of components in the dump file separated  by spaces.

### A.5.1.2 Platforms Supported

Diagnosable dumps can be generated on the following platforms:.

- Linux (x86 and x86_64)
- Solaris_Sparc
- HP-IA64.C32
- AIX.PPC32
- HP-PA32 (only object dumps - no stack traces)

## A.5.2 Reference Counting

Many of the Agent's data structures have a reference counter. This facilitates sharing of data between the subsystems like targets, metrics, jobs, in Enterprise Manager and avoids the need for duplicate objects. Reference counting is very useful in detecting memory leaks and memory corruption. Reference counting maintains a list of all reference counted objects accessed by a specific thread.

When a data structure is accessed, the reference counter associated with it is incremented. When the data structure is no longer being accessed, the reference counter is decremented. If the reference counter value is zero, the memory can be safely freed.

If the free action finds the object is not in the list maintained, it indicates that there is a memory corruption. At thread exit, objects left behind in the list indicate that there is a memory leak. When these errors occur, a dump file is generated and the errors are written into the `emagent.trc` file.

The reference counter dump contains the following details:

- Thread ID
- Struct ID
- Object Address

- Current Count
- Action (acquire or release)
- Timestamp
- Call Stack

Caller stack dumps are disabled by default. To enable it, you must specify a non-zero value for the `refCntCallStackDepth` property in the `emd.properties` file. For example, refCntCallStackDepth=0 should be "=5"

***Example A–1 Sample emagent.trc file***

```
2008-12-16 11:37:48,614 Thread-2718141344 ERROR ThreadPool: nmttp_run: Memory
leak: unreleased reference counted object: 84b25e0, structID: 11001
2008-12-16 11:37:48,614 Thread-2718141344 ERROR ThreadPool: nmttp_run: Memory
leak: unreleased reference counted object: 8642a08, structID: 11002
2008-12-16 11:37:48,614 Thread-2718141344 ERROR ThreadPool: nmttp_run: Memory
leak: unreleased reference counted object: 8585f18, structID: 11002
2008-12-16 11:37:48,614 Thread-2718141344 ERROR ThreadPool: nmttp_run: Memory
leak: unreleased reference counted object: 8557de8, structID: 11002
2008-12-16 11:37:48,614 Thread-2718141344 ERROR ThreadPool: nmttp_run: Memory
leak: unreleased reference counted object: 856d4d8, structID: 11002
2008-12-16 11:37:48,615 Thread-2718141344 WARN  diagnostics.statemgr: /ade/aime1_
dadvfb0451_ag/oracle/sysman/dump/emagent_2938_20081216113748.diagtrc dumped
2008-12-16 11:37:48,693 Thread-2718141344 WARN  diagnostics.statemgr: size:
24615,/ade/aime1_dadvfb0451_ag/oracle/sysman/dump/emagent_2938_
20081216113748.diagtrc
```

***Example A–2 Reference Count Dump***

```
EMAGENT Ver:10.2.0.5.0
NON-FATAL DUMP
Memory leak on reference counted objects

-------------------- Binary Stack Dump ---------------------

========== FRAME [6] (__clone()+94 -> 00000000) ==========
defined by frame pointers 0x0  and 0xa20384c8
CALL TYPE: call   ERROR SIGNALED: no   CALLER: __clone
----- Argument/Register Address Dump -----
Argument/Register addr=0xb70ebcb0.
Dump of memory from 0xb70ebc70 to 0xb70ebdb0
B70EBC70 74746D6E 75725F70 6E65206E 00726574  [nmttp_run enter.]
B70EBC80 74746D6E 75725F70 7865206E 203A7469  [nmttp_run exit: ]
B70EBC90 74737953 253D6D65 57202C64 656B726F  [System=%d, Worke]
B70EBCA0 64253D72 6F54202C 3D6C6174 00006425  [r=%d, Total=%d..]
B70EBCB0 6F6D654D 6C207972 206B6165 72206E6F  [Memory leak on r]
B70EBCC0 72656665 65636E65 756F6320 6465746E  [eference counted]
B70EBCD0 6A626F20 73746365 00000000 74746D6E  [ objects....nmtt]
B70EBCE0 3A632E70 746E4520 6E697265 6D6E2067  [p.c: Entering nm]
B70EBCF0 5F707474 546E7572 526B7361 79727465  [ttp_runTaskRetry]
B70EBD00 00000000 74746D6E 75725F70 7361546E  [....nmttp_runTas]
B70EBD20 64253D74 00000000 74746D6E 3A632E70  [t=%d....nmttp.c:]
B70EBD30 746E4520 6E697265 6D6E2067 5F707474  [ Entering nmttp_]
B70EBD40 546E7572 006B7361 546E7572 206B7361  [runTask.runTask ]
B70EBD50 61657263 61206574 72687420 3A646165  [create a thread:]
B70EBD60 73795320 3D6D6574 202C6425 6B726F57  [ System=%d, Work]
B70EBD70 253D7265 54202C64 6C61746F 0064253D  [er=%d, Total=%d.]
B70EBD80 68676948 74615720 614D7265 69206B72  [High WaterMark i]
B70EBD90 203A2073 00006425 00000000 6C756F43  [s : %d......Coul]
```

```
B70EBDA0 6F6E2064 72632074 65746165 72687420  [d not create thr]

Argument/Register addr=0xa2038ba0.
Dump of memory from 0xa2038b60 to 0xa2038ca0
A2038B60 00000000 00000000 00000000 00000000  [................]
A2038B70 00000000 00000000 003E6380 A2038E00  [.........c>....¡é]
A2038B80 00000000 B62A6F78 B62A7378 B62A7978  [....xo*?xs*?xy*?]
A2038B90 003E7820 00000000 00000000 00000000  [ x>.............]
A2038BA0 A2038BA0 08346750 A2038BA0 00000001  [?..¡éPg4.?..¡é....]
A2038BB0 002997A0 00000000 00000000 00000000  [?.).............]
A2038BC0 00000000 00000000 00000000 00000000  [................]
        Repeat 1 times

A2038BE0 B5493BE0 00519110 000018C9 00000B7A  [¨¤;I¦Ì..Q.¨¦...z...]
A2038BF0 00000000 A2038400 00000000 00000001  [.......¡é........]
A2038C00 085598F0 00000001 08516510 00000001  [e.U......eQ.....]
A2038C10 08559C78 00000000 00000000 00000001  [x.U.............]
A2038C20 00000000 00000000 00000000 00000000  [................]
A2038C30 00000000 00000001 00000000 00000001  [................]
A2038C40 00000000 00000000 00000000 00000000  [................]
  Repeat 5 times
{
thread ID = 0xa2038108 "2718141344"
struct ID = 11002
address = 0x8642a08
count = 3
activity ID = 16
time (centi-seconds ago) = 22
nmecci_addReferenceCount()+74
nmectc_getCollectionItem()+145
nmemdisp_GetActiveCollection()+317
nmemdisp_Dispatcher_main()+3276
nmehl_processIncomingRequest()+1028
}nmeuca_CircularArray
```

**Note:** You can also use the following emctl command to view the current reference counter history:

```
emctl dumpstate agent refcnt
```

## A.5.3 Tracking CPU Thread Times

Monitoring and managing a target involves collecting metric data and executing jobs that perform operations on the target. The CPU usage can be high under the following conditions:

- A large number of targets are being monitored
- A CPU intensive metric is being collected too often
- A job or a remote operation is not working correctly

By tracking the CPU usage per thread, you can identify the threads with high CPU usage and also identify the activities that are contributing to the high usage.

Any user operation consists of one or more activities (metric collection, jobs) whose CPU usage is tracked by the Agent. The Agent tracks CPU usage per thread at specified intervals and a dump file containing this information can be generated. The threads tracked include both Persistent and Transient threads.

Persistent threads are available throughout the lifetime of the Agent. Scheduling, HTTP Listener activity, are some of the activities related to persistent threads. Transient threads are initiated to perform a certain activity and are terminated when the activity has been completed. Metric Collection, user initiated operations like reload etc., are some of the activities related to transient threads.

You can configure the tracking and history intervals by adding the following properties to the `emd.properties` file.

- `CPUHistoryTrackInterval`: The period for which the CPU usage history should be maintained. The default minimum period is 24  hours.
- `DisableCPUUsageTracking`: Specifies whether Agent tracks CPU usage of activities.  This flag is set to False by default. If this feature is enabled, the CPU usage history is stored in the `$AGENTSTATE/sysman/emd/cputrack/emagent_<pid>_<timestamp>_cpudiag.trc` file. The dump file contains the following details:
  - The time interval for this report.
  - The CPU time the Agent process consumed during this interval.
  - The distribution of this Agent Process CPU time among agent threads.
  - Top targets with high CPU usage and the top 10 metric collections for each of these targets.
  - Top metric collections that have the highest CPU usage across all targets and a breakup by target for each of these metrics.
  - Top 10 target wide activities.

> **Note:** You can also use the following `emctl` command to generate a dump file:
>
> ```
> emctl status agent cpu
> ```

***Example A–3 Sample cpudiag.trc File***

```
Summary
Interval=2009-01-14 03:07:49 - 2009-01-14 04:08:11
Process=59.872 seconds
HttpListener=0.41%
Scheduler=1.22%
HealthMonitor=0.14%
CollectionThreads=66.35%
DispatcherThreads=3.54%
JobThreads=0.00%
RecvletThreads=1.09%

                              <------Current------>  <-------Lifetime------->
Identifier   CTime  ETime   Num   CTime  ETime   Num  LastStartTime  LastEndTime

Top 10 Persistent Threads
-Scheduler       0.733 3583.050  59  8.842  43773.370  721   2009-01-14  04:07:23
-HttpListener    0.243 3567.130  57  2.818  43787.850  700   2009-01-14  04:07:15
-HealthMonitor   0.082 3624.190  59  1.005  43837.380  707   2009-01-14  04:08:04

Top 10 Targets
oracle_database:database3 4.853    68.250
-health_check   0.614  2.030    241  7.263     66.890  2898  2009-01-14  04:08:03
2009-01-14 04:08:03
```

```
-sga_start      0.488  7.050    13   5.339     77.410  145   2009-01-14  04:08:02
2009-01-14 04:08:03
-Response       0.455  8.380    12   5.375    108.580  145   2009-01-14  04:03:33
2009-01-14  04:03:34
-propagation_msgstate_stats 0.426 8.460 12  5.011  102.230 145 2009-01-14 04:06:02
2009-01-14  04:06:03
-apply_queue_persq         0.422 8.440 12  4.811  102.980 145 2009-01-14 04:06:03
2009-01-14  04:06:03
-textIndexStats            0.403 1.820 61  4.349   22.850 725 2009-01-14 04:08:02
2009-01-14  04:08:02
-dumpFull                  0.193 8.710  5  1.819   87.720  49 2009-01-14 04:07:55
2009-01-14  04:07:57
-archFull                  0.172 6.480  5  1.704   63.460  49 2009-01-14 04:07:57
2009-01-14  04:07:58
-alertLog                  0.153 1.390  4  1.840   17.340  49 2009-01-14 04:05:28
2009-01-14  04:05:28
-wait_sess_cls             0.151 0.260  4  1.848    3.100  48 2009-01-14 03:59:19
2009-01-14  03:59:19

Top 10 Metrics
oracle_database:health_check  2.474  8.650
-oracle_database:database2       0.633  2.180  241  7.137  43.570  2900 2009-01-14
04:07:56  2009-01-14  04:07:56
-oracle_database:database        0.621  2.360  242  7.276  56.560  2902 2009-01-14
04:08:08  2009-01-14  04:08:08
-oracle_database:database3       0.614  2.030  241  7.263  66.890  2898 2009-01-14
04:08:03  2009-01-14  04:08:03
-oracle_database:Oemrep_Database 0.607  2.080  241  7.193  49.010  2921 2009-01-14
04:07:57  2009-01-14  04:07:57

Top 10 Target wide activities
-Upload                   2.102 4.020 292 33.501 208.740 3629 2009-01-14 04:08:01
2009-01-14  04:08:01
-AQRecvlet                0.655 14526.670 242  12.330 174670.980 2916 2009-01-13
16:02:04
-GetCompositeMembersReq    0.016  0.010 12  0.193  0.190  147 2009-01-14 04:05:06
2009-01-14 04:05:06
-RefreshReq               0.000  0.000  0  1.809 59.280   8
-RemoveTargetReq          0.000  0.000  0  0.694  6.030   12
```

### A.5.3.1 Platforms Supported

This feature is available on platforms that support thread CPU usage. This includes AIX and LINUX (with new kernels) and Solaris 10. For platforms that do not have the support for thread CPU usage, only elapsed times are reported.

## A.5.4 Management Agent Crashes When Target Type is "WMQ" in targets.xml File

If the Management Agent crashes when the target type is *WMQ* in the targets.xml file, then follow the workaround described in My Oracle Support note 419933.1.

# A.6 Network Issues

This section lists network issues you may encounter during Enterprise Manager installation and configuration.

## A.6.1 Incorrect Format For Entries In /etc/hosts File

This will cause the installation to hang and OUI-25031 or OUI-10104 errors in log files.

Entries in the /etc/hosts file should be in the following format:

```
IP_Address Canonical_Hostname Aliases
```

For example:

```
11.22.33.441 abc.xyz.com abc1 xyz2
```

When creating the /etc/hosts file, follow these rules:

- Host name may contain only alphanumeric characters, hyphen, and period. The name must begin with an alphabetic character and end with an alphanumeric character.
- Lines cannot start with a blank or tab character.
- Fields can have any number of blanks or tab characters separating them.
- Comments are allowed and designated by a pound sign (#) preceding the comment text.
- Trailing blank and tab characters are allowed.
- Blank line entries are allowed.
- Only one host entry per line is allowed.

Forward lookup is finding IP address given the hostname. Reverse lookup is finding hostname given the IP address. Results of forward and reverse lookups should be the same. It is usually different because of case difference (upper/lower) in hostnames and aliases.

If DNS Server is configured in your environment, then ensure that the OMS host name can be resolved through DNS. For more information, contact your network administrator.

For 10.2.0.1 Enterprise Manager installations, if a host name contains an upper case letter, securing of Agent will fail.

### A.6.2 Enterprise Manager Installation on Computers With Multiple Addresses

While installing Enterprise Manager or related components on Multi-homed (Multi-IP) machines, that is, a machine having multiple IP addresses, the host name is derived from the `ORACLE_HOSTNAME` variable that is passed along with `-local` while invoking the runInstaller.

For example, `runInstaller ORACLE_HOSTNAME=foo.us.oracle.com -local`

### A.6.3 Agent Configuration Fails on A Non-Network Computer

To resolve this error, Oracle Management Service and target host where the Agent needs to be installed should be pingable.

### A.6.4 Loopback Adapter On Windows and Related Known Issues

If installing Enterprise Manager or related components on a DHCP host, one needs to install a loopback adapter to assign a local IP address to that computer.

**Note:** Refer to section 2.4.5 Installing a Loopback Adapter of the Oracle® Database Installation Guide 10g Release 2 (10.2) for Microsoft Windows (32-Bit) Part Number B14316-02 for more information.

Ensure that the following conditions are met:

- The /etc/hosts file should contain the following entry:

  ```
  <lopback IP Address><hostname.domainname> <hostname>
  ```

  For example:

  ```
  127.0.0.1 localhost.localdomain localhost
  ```

- Ensure that the IP address specified in /etc/hosts is correct otherwise allocation of ports will fail

### A.6.5 Installation Fails  with Host Name Error on the Product-Specific Prerequisite Check Page

While installing a Management Agent, the installation can fail on the product-specific prerequisite page with a host name error. This happens when the host name specified in the host file does not map to the correct IP address of that host.

To resolve this issue, first run the following command on the host to list all the IP addresses configured and then note the IP address for that host:

```
ipconfig /all
```

After noting the IP address of that host, open the host file and check the entries for this host name. Ensure that the host name maps to the correct IP address of that host.

## A.7 Other Installation and Configuration Issues

This section lists some of the generic errors that you may encounter during Enterprise Manager installation and configuration.

### A.7.1 Storage Data Has Metric Collection Errors

The following Enterprise Manager collection error message may appear from agents installed through silent or `agentdownload` install mechanisms:

```
snmhsutl.c:executable nmhs should have root suid enabled.
```

Perform the required root install actions (using `root.sh` script on UNIX platforms only) to resolve this issue. It may take up to 24 hours before the resolution is reflected.

### A.7.2 Cannot Add Systems to Grid Environment from the Grid Control Console

You cannot add new targets to your grid environment if you do not have an agent already installed.

To install the agent from your Grid Control console:

1. Log in to the Grid Control console and go to the Deployments page.
2. Click **Install Agent** under the Agent Installation section.
3. In the Agent Deploy home page that appears, select the appropriate installation option that you want to perform. See Chapter 10, "Deploying Management Agent" for more information.

## A.8 Error During Deinstallation of Grid Control Targets

After deinstalling certain Grid Control targets, when you try to remove the same targets from the Grid Control console, you may encounter an exception with a message similar to the following:

```
java.sql.SQLException: ORA-20242: Target <target name> is monitoring other
targets. It cannot be deleted.
```

To resolve this issue, deinstall the Grid Contol targets and wait for at least 15 minutes before you attempt to remove the targets from the Grid Control console using the Hosts page. This time is required for the deinstallation information to propagate to the Management Repository.

## A.9 Discovery Issues

This section lists the discovery-related issues:

### A.9.1 Unable to Discover Targets Deployed on Hosts

For discovering any target on a host, you must have a Management Agent running on that host. However, despite having a Management Agent, you may not be able to discover the targets in Enterprise Manager Grid Control.

The possible cause may be that the entries in the listener.ora file for that host are incorrect. To resolve this issue, ensure that the entries in the listener.ora file have canonic names.

For example, the host name may be sjohn-sun1. However, it's fully qualified name may be sjohn-sun1.server.com. For the discovery to happen successfully, you must ensure that the listener.ora file for that host contains the fully qualified name entry, that is, sjohn-sun1.server.com, and not sjohn-sun1.

### A.9.2 Unable to View Metric Details of Targets

After you discover a target and add it to Enterprise Manager Grid Control, you may be able to view the status of that target, but you may not be able to view metric details. This is because the target is not fully configured and therefore, the Agent monitoring that target is unable to compute its dynamic properties or evaluate its metrics.

To circumvent this issue, after you discover the target, provide the password in the Monitoring Configuration page of the target. To access the Monitoring Configuration page, go to the Home page of the target and from the Related Links section, click **Monitoring Configuration**.

## A.10 Need More Help

If this appendix does not solve the problem you encountered, try these other sources:

- Oracle Enterprise Manager Release Notes, available on the Oracle Technology Network Web site (`http://www.oracle.com/technology/documentation`).
- Oracle

  (`http://metalink.oracle.com/`)

If you do not find a solution for your problem, log a service request.

# 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 Grid Control components.

## B.1 Enterprise Manager Grid Control Installation Log Files

During Enterprise Manager installation, the following log files are created:

1. Configuration Logs
2. Installation Logs
3. Repository Logs
4. Secure Logs

### B.1.1 Configuration Logs

lists the installation logs that are created.

*Table B–1 Installation Log Files*

| Installation Type | Log File | Location |
|---|---|---|
| Enterprise Manager Using New Database | cfm log | <DB_HOME>/cfgtools/cfgfw/cfmlogs |
| | oracle.sysman.top.em_seed.<timestamp>.log | <DB_HOME>/cfgtools/cfgfw/oracle.sysman.top.em_seed.<timestamp>.log |
| Enterprise Manager Using Existing Database | cfm log | <OMS_HOME>/cfgtools/cfgfw/cfmlogs |
| | oracle.sysman.top.oms <timestamp>.log | <OMS_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log |
| Additional Management Service | cfm log | <OMS_HOME>/cfgtools/cfgfw/cfmlogs |
| | oracle.sysman.top.oms <timestamp>.log | <OMS_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log |

*Table B–1 (Cont.) Installation Log Files*

| Installation Type | Log File | Location |
|---|---|---|
| Additional Management Agent | cfm log | <AGENT_HOME>/cfgtools/cfgfw/cfmlogs |
|  | oracle.sysman.top.agent <timestamp>.log | <AGENT_HOME>/cfgtools/cfgfw/oracle.sysman.top.oms.<timestamp>.log |

### B.1.2 Installation Logs

The installation action logs that are created will provide complete information on the installation status. This log is located at the following locations:

- `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.1.3 Repository and Secure Logs

The repository and secure logs are located in the Management Service Oracle home for the following installation types:

- Enterprise Manager Using a New Database
- Enterprise Manager Using an Existing Database
- Additional Management Service

#### B.1.3.1 Repository Log Location

The repository log is located at:

```
<OMS_HOME>/sysman/log/emrepmgr<rep log>.<pid>
```

**Note:** In the above-mentioned path, the `emrepmgr` will be the **SID**.

#### B.1.3.2 Secure Log Location

The secure log is located at:

```
<OMS_HOME>/sysman/log/<secure log>
```

If you are installing an additional Management Agent, the secure log is located at:

```
<AGENT_HOME>/sysman/log/<secure log>
```

## B.2 Agent Deploy Log Files

The following agent prerequisite check and installation logs are available at these locations:

**Connectivity Logs:** the following connectivity logs for the local node will be available at the following locations:

*Table B–2 Connectivity Log Locations*

| Log File | Location |
|---|---|
| `prereq<time_stamp>.log` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local` |
| `prereq<time_stamp>.out` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local` |
| `prereq<time_stamp>.err` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/local` |

**Prerequisite Logs:** The following prerequisite logs for `<node 1>` will be available at the following locations:

*Table B–3 Prerequisite Log Locations*

| Log File | Location |
|---|---|
| `prereq<time_stamp>.log` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>` |
| `prereq<time_stamp>.out` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>` |
| `prereq<time_stamp>.err` | `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/prereqs/<node1>` |

> **Note:** The time stamp in the log files of `prereq/install/upgrade` function may not be the same as the time-stamp in the `$OMS_HOME/sysman/prov/agentpush/<time-stamp>/`. These time stamps can differ considerably from the OMS host because these logs are generated in remote nodes and are collected back to OMS after the agent installation or upgrade.

Table B–4 lists all the other installation logs that are created during an agent installation using Agent Deploy.

*Table B–4 Installation Logs Created During Agent Installation Using Agent Deploy*

| Logs | Location | Description |
|---|---|---|
| `EMAgentPush<TIMESTAMP>.log` | `<OMS_HOME>/sysman/prov/agentpush/logs/` | Agent Deploy application logs. |

*Table B–4 (Cont.) Installation Logs Created During Agent Installation Using Agent*

| Logs | Location | Description |
|---|---|---|
| `remoteInterfaces<TIMESTAMP>.log` | `<OMS_HOME>/sysman/prov/agentpush/logs/` | Logs of the remote interfaces layer. |
| `install.log/.err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the new agent installation or new cluster agent installation. |
| `upgrade.log/.err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the upgrade operation using Agent Deploy |
| `nfsinstall.log/err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the agent installation using the Shared Agent Home option in Agent Deploy. |
| `clusterUpgrade.log/err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the cluster upgrade operation using Agent Deploy. |
| `sharedClusterUpgradeConfig.log/err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the config operation in case of upgrade on a shared cluster. |
| `config.log/err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of the configuration of shared cluster in case of an agent installation on a shared cluster. |
| `preinstallscript.log/.err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log/error of the running of preinstallation script, if specified. |
| `rootsh.log/.err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log/error of running of `root.sh`. |
| `postinstallscript.log/.err` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Log or error of running of postinstallation script, if specified. |
| `installActions<timestamp>.log, oraInstall<timestamp>.err/.out` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Logs of Oracle Universal Installer. |
| `agentStatus.log` | `<OMS_HOME>/sysman/prov/agentpush/<TIMESTAMP>/logs/<HOSTNAME>/` | Status of agent after running `emctl status agent` from the agent home. |

# C

# Agent Log Files

This appendix lists the log files you can review if the agent installation, upgrade, or cloning operation fails. The information in these logs might help you describe the failure while raising service requests with Oracle Support.

This appendix covers the following:

- Logs Present on OMS Host
- Logs Present on Target Host

---

**Note:** The `entrypoints` directory mentioned in the locations described in this section is present only in Enterprise Manager 10g Grid Control Release 5 (10.2.0.5). For Enterprise Manager 10g Grid Control Release 4 (10.2.0.4) or lower, ignore this directory in the path.

---

## C.1 Logs Present on OMS Host

The log files mentioned in this section are present on the host where OMS is running.

### Response File

The following is the response file you can review from the Oracle home directory of the OMS:

$ORACLE_HOME/sysman/agent_download/<release_number>agent_download.rsp

### Connectivity Log Files

The following are the connectivity log files you can review from the Oracle home directory of the OMS:

- $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/entrypoints/connectivity /local/prereq<time_stamp>.log
- $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/entrypoints/connectivity /local/prereq<time_stamp>.out
- $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/entrypoints/connectivity /local/prereq<time_stamp>.err

For example:

$ORACLE_HOME/sysman/prov/agentpush/2008-12-03_
02-55-17AM/prereqs/entrypoints/connectivity /local/prereq2008-12-03_
10-56-40AM.log

### Prerequisites Log Files for Targe Host

The following are the prerequisites-related log files you can review from the Oracle home directory of the OMS, for the target host on which you cloned the Management Agent.

- $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/<agent_node_name>
- Application-Related Prerequisites Log Files:

  **Installation-Specific Log Files**

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_install/<targethostname>/prereq<time_stamp>.log

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_install/<targethostname>/prereq<time_stamp>.out

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_install/<targethostname>/prereq<time_stamp>.err

  For example:

  $ORACLE_HOME/sysman/prov/agentpush/2008-12-03_
  02-55-17-AM/prereqs/entrypoints/emagent_install/strwa49/prereq2008-12-03_
  02-59-05AM.err

  **Cloning-Specific Log Files**

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_clone/<targethostname>/prereq<time_stamp>.log

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_clone/<targethostname>/prereq<time_stamp>.out

  – $ORACLE_HOME/sysman/prov/agentpush/<timestamp>/prereqs/entrypoints/emagent_clone/<targethostname>/prereq<time_stamp>.err

  For example:

  $ORACLE_HOME/sysman/prov/agentpush/2008-12-03_
  02-55-17-AM/prereqs/entrypoints/emagent_clone/strwa49/prereq2008-12-03_
  02-59-05AM.err

- System-Related Prerequisites Log Files:

  – $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/entrypoints/oracle.sysman.top.agent_Complete/<targethostname>/prereq<time_stamp>.log

  – $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/prereqs/entrypoints/oracle.sysman.top.agent_Complete/<targethostname>/prereq<time_stamp>.out

  - $ORACLE_HOME/sysman/prov/agentpush/<times-tamp>/ prereqs/entrypoints/oracle.sysman.top.agent_ Complete/<targethostname>/prereq<time_stamp>.err

  For example:

  $ORACLE_HOME/sysman/prov/agentpush/2008-12-03_02-55-17-AM/ prereqs/entrypoints/oracle.sysman.top.agent_ Complete/strwa49/prereq2008-12-03_02-59-05AM.err

### Application Log Files

The following are the application-related log files you can review from the Oracle home directory of the OMS:

- $ORACLE_ HOME/sysman/prov/agentpush/logs/EMAgentPush<time-stamp>.log
- $ORACLE_ HOME/sysman/prov/agentpush/logs/remoteInterfaces<time-stamp>.log
- $ORACLE_HOME/sysman/prov/agentpush/logs/<timestamp>/ cfgtoollogs/
- $ORACLE_HOME/j2ee/OC4J_EMPROV/log/OC4J_EMPROV_default_island_ 1/

### Logs for <agent_node>

The following are the logs you can review from the Oracle home directory of the OMS, for the agent node:

**Common Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/config.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/config.err
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/preinstallscript.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/preinstallscript.err
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/rootsh.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/rootsh.err
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/postinstallscript.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/postinstallscript.err
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/installActions<times-tamp>.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_ name>/agentStatus.log

**Installation-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/install.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/install.err

**Cloning-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/clone.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/clone.err

**Upgrade-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/upgrade.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/upgrade.err

**NFS Installation-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/nfsinstall.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/nfsinstall.err

**Cluster Upgrade-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/clusterUpgrade.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/clusterUpgrade.err

**Shared Cluster Upgrade-Specific Log Files**

- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/sharedClusterUpgradeConfig.log
- $ORACLE_HOME/sysman/prov/agentpush/<time-stamp>/logs/<agent_node_name>/sharedClusterUpgradeConfig.err

## C.2 Logs Present on Target Host

The log files mentioned in this section are present on the target host where the Management Agent was installated.

### Central Inventory Files

The following is the central inventory log file you can review from the inventory location. Check the inventory location from the $AGENT_HOME/oraInst.loc file.

$inventory_loc/ContentsXML/inventory.xml

### Installer Log Files

The following are the installer log files you can review from the inventory location. Check the inventory location from the $AGENT_HOME/oraInst.loc file.

- $inventory_loc/logs/*.log
- $inventory_loc/logs/*.out

- $inventory_loc/logs/*.err

### Configuration Assistants Log Files

The following location contains all the configuration assistants-related log files you can review from the Oracle home directory of the Management Agent.

$ORACLE_HOME/cfgtoollgs/

### Agent Log Files

The following location contains all the Agent-related log files you can review from the Oracle home directory of the Management Agent.

$ORACLE_HOME/sysman/log/

The following location contains all RAC Agent-related log files you can review from the Oracle home directory of the Management Agent.

$ORACLE_HOME/agent_node_name/sysman/log/

# D Platform-Specific Package and Kernel Requirements

This appendix lists the recommended software packages and kernel parameters required for a successful Enterprise Manager Grid Control installation on each of the supported platforms. For the most current list of supported operating system-specific software, refer to My Oracle Support (formerly Metalink) at http://metalink.oracle.com.

This appendix has the following sections:

## D.1 Package Requirements

The following sections list the package requirements for each platform.

### D.1.1 Required Packages on Linux

The following (or later) packages must be running on your Linux systems.

**Red Hat Enterprise Linux 3.0**

- glibc-2.2.4-31.7

- make-3.79
- binutils-2.11.90.0.8-12
- gcc-2.96
- openmotif21-2.1.30-9

### Red Hat Enterprise Linux 4.0

- glibc-2.3.4-2.9
- glibc-devel-2.3.4-2.9.i386.rpm
- make-3.79
- binutils-2.15.92.0.2-13
- gcc-3.4.3-22.1
- libaio-0.3.96
- glibc-common-2.3.4-2.9
- setarch-1.6-1
- pdksh-5.2.14-30
- openmotif21-2.1.30-11
- sysstat-5.0.5-1
- gnome-libs-1.4.1.2.90-44.1
- libstdc++-3.4.3-22.1
- libstdc++devel-3.4.3-22.1
- compat-libstdc++-296-2.96-132.7.2
- compat-db-4.1.25-9
- control-center-2.8.0-12
- xscreensaver-4.18-5.rhel4.2

### Red Hat Enterprise Linux 5.x

- make-3.79
- binutils-2.14
- gcc-3.2
- libXp.so.6
- libaio
- glibc-devel (64-bit)
- glibc-devel (32-bit)

### SUSE Linux Enterprise Server 9

- glibc-2.2.4-31.7
- make-3.79
- binutils-2.11.90.0.8-12
- gcc-c++

- db1
- gnome-libs
- orbit

**SUSE Linux Enterprise Server 10**

> **IMPORTANT:** This platform is supported only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

- make-3.79
- binutils-2.14
- gcc-3.2

**Oracle Enterprise Linux 4**

> **IMPORTANT:** This platform is supported only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

- make-3.79
- binutils-2.14
- gcc-3.2

**Oracle Enterprise Linux 5**

> **IMPORTANT:** This platform is supported only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

- make-3.79
- binutils-2.14
- gcc-3.2

### D.1.2 Required Packages for Linux x86_64

The following (or later) package versions must be running on your Linux x86_64 systems:

**For Red Hat Enterprise Linux 3.0**

- glibc-2.2.4-31.7
- make-3.79
- binutils-2.11.90.0.8-12
- gcc-2.96
- openmotif2.1.30-11

### For Red Hat Enterprise Linux 4.0

- glibc-2.3.4-2.9
- make-3.79
- binutils-2.15.92.0.2-13
- gcc-3.4.3-22.1
- libaio-0.3.96
- glibc-common-2.3.4-2.9
- setarch-1.6-1
- pdksh-5.2.14-30
- openmotif21-2.1.30-11
- sysstat-5.0.5-1
- gnome-libs-1.4.1.2.90-44.1
- libstdc++-3.4.3-22.1
- compat-db-4.1.25-9
- control-center-2.8.0-12
- xscreensaver-4.18-5.rhel4.2
- libstdc++devel-3.4.3-22.1
- compat-libstdc++-296-2.96-132.7.2
- glibc-devel-2.3.4-2.9.i386.rpm
- libgcc-3.2.3-20.i386.rpm
- compat-gcc-7.3-2.96.122.i386.rpm
- compat-glibc-7.x-2.2.4.32.5.i386.rpm

### For Red Hat Enterprise Linux 5.x

- make-3.79
- binutils-2.14
- gcc-3.2
- libXp.so.6
- libaio
- glibc-devel (64-bit)
- glibc-devel (32-bit)

### For SUSE Linux Enterprise Server 9

- glibc-2.2.4-31.7
- make-3.79
- binutils-2.11.90.0.8-12
- gcc-2.96
- openmotif2.1.30-11

#### For SUSE Linux Enterprise Server 10

- make-3.79
- binutils-2.14
- gcc-3.2

#### For Oracle Enterprise Linux 4

- make-3.79
- binutils-2.14
- gcc-3.2

#### For Oracle Enterprise Linux 5

- make-3.79
- binutils-2.14
- gcc-3.2

## D.1.3 Required Packages on Solaris

The following (or later) package versions must be running on your Solaris systems:

- SUNWarc
- SUNWbtool
- SUNWhea
- SUNWlibm
- SUNWlibms
- SUNWsprot
- SUNWsprox
- SUNWtoo
- SUNWi1of
- SUNWxwfnt

To check if the required operating system packages have been installed on your system, enter the following command:

```
prompt> pkginfo SUNWarc SUNWbtool SUNWhea SUNWlibm SUNWlibms SUNWsprot SUNWsprox
SUNWtoo SUNWi1 of SUNWxwfnt
```

> **Note:** If any packages are missing, contact your system administrator.

### D.1.3.1 Checking for 32-Bit and 64-Bit Application Support

Check whether or not your system is configured to support 32-bit and 64-bit applications by entering the following command:

```
prompt> /usr/bin/isainfo -v
```

### D.1.3.2 Required Patches

The patches required for the different Solaris versions are the following:

**Solaris 8**

- 108652-74 or later: X11 6.4.1: Xsun patch
- 108921-18 or later: CDE 1.4: dtwm patch
- 108940-57 or later: Motif 1.2.7 and 2.1.1: Runtime library patch
- 108773-18 or later: IIIM and X input and output method patch
- 111310-01 or later: /usr/lib/libdhcpagent.so.1 patch
- 109147-26 or later: Linker patch
- 111308-04 or later: /usr/lib/libmtmalloc.so.1 patch
- 111111-03 or later: /usr/bin/nawk patch
- 112396-02 or later: /usr/bin/fgrep patch
- 110386-03 or later: RBAC feature patch
- 111023-02 or later: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch
- 108987-13 or later: Patch for patchadd and patchrm
- 108528-26 or later: Kernel update patch
- 108989-02 or later: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch
- 108993-45 or later: LDAP2 client, libc, libthread and libnsl libraries patch
- 111023-02 or later: Unable to load fontset ... iso-1 or iso-15

**Solaris 9**

- 113096-03 or later: X11 6.6.1: OWconfig patch
- 112785-35 or later: X11 6.6.1: Xsun patch

### D.1.3.3 Checking for Patches

To determine the patches that have been installed on the system, follow these steps:

1. Run the `showrev` command with the `-p` option. The following command saves the sorted output to a file called `patchList`.
2. Enter the following command:

```
prompt> showrev -p | sort > patchList
```

3. Open the file in a text editor and search for the patch numbers.

> **Note:** If the required patches have not been installed, you can download them from http://sunsolve.sun.com.

## D.1.4 Required Packages on HP-UX PA-RISC

The following (or later) package versions must be running on your HP-UX PA-RISC systems:

**HP-UX PA-RISC 11i V1 (11.11)**

- For installation on HP-UX PA-RISC 11.11, the following packages or later versions are required:
  - HP-UX PA-RISC 11i June 2003 Consolidated Quality Patch Bundle

  - Jun03GQPK11i_Aux_Patch

- Make sure that Motif 2.1 Development Environment (X11MotifDevKit.MOTIF21-PRG)B.11.11.01 is installed

  Either install this package or create symbolic links as follows:

  1. Log in as `root`.
  2. Change directory to `/usr/lib` as follows:

     ```
     # cd /usr/lib
     ```

  3. Create the required links:

     ```
     # ln -s libX11.3 libX11.sl
     # ln -s libXIE.2 libXIE.sl
     # ln -s libXext.3 libXext.sl
     # ln -s libXhp11.3 libXhp11.sl
     # ln -s libXi.3 libXi.sl
     # ln -s libXm.4 libXm.sl
     # ln -s libXp.2 libXp.sl
     # ln -s libXt.3 libXt.sl
     # ln -s libXtst.2 libXtst.sl
     ```

- The following patches or later are required:
  - PHCO_28123, cumulative SAM patch
  - PHKL_29198, Psets Enablement Patch
  - PHNE_28476, Cumulative STREAMS Patch
  - PHNE_28923, LAN product cumulative patch
  - PHSS_28871, ld(1) and linker tools cumulative patch
  - PHSS_28880, HP aC++ -AA runtime libraries (aCC A.03.50)
  - PHCO_26331, mountall cumulative patch
  - PHCO_29109, Pthread enhancement and fixes
  - PHKL_25468, eventport (/dev/poll) pseudo driver
  - PHKL_25842, Thread Abort
  - PHKL_25993, thread nostop for NFS, rlimit, Ufalloc fix
  - PHKL_25994, Thread NOSTOP, Psets Enablement, Ufalloc
  - PHKL_25995, eventport syscalls; socket close(2); Ufalloc
  - PHKL_26468, Shared mutex synchronization support patch
  - PHKL_28489, copyin EFAULT, LDCD access type

- To determine whether or not a bundle, a product, or file set is installed, enter a command similar to the following, where *level* refers to the bundle, patch or file set.

  ```
  # /usr/sbin/swlist -l level |more
  ```

### HP-UX PA-RISC 11i V2 (11.23)

- For installation on HP-UX PA-RISC 11.23, the following packages or later versions are required:
  - Patch Bundle for HP-UX PA-RISC 11i V2 (B.11.23), September 2004

  - BUNDLE11i, Revision B.11.23.0409.3

#### HP-UX PA-RISC 11i V3 (11.31)

- Base-VXFS- B.11.31
- OnlineDiag- B.11.31.01.03

### D.1.5 Required Packages for HP-UX Itanium

The following (or later) package versions must be running on your HP-UX Itanium systems:

#### HP-UX IA-64 11i V2 (11.23)

- For installation on HP-UX 11.23, the following packages or later versions are required:
  - Patch Bundle for HP-UX 11i V2 (B.11.23), September 2004
  - BUNDLE11i, Revision B.11.23.0409.3
- The following patches or later versions are required:
  - PHSS_31849:linker + fdp cumulative patch
  - PHSS_31852: aC++ Runtime (PA A.03.61)

#### HP-UX IA-64 11i V3 (11.31)

> **IMPORTANT:** This platform is supported only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

- For installation on HP-UX 11.31, the following packages or later versions are required:
  - BUNDLE-B.11.31
- The following operating system patches or later versions are required:
  - PHKL_35936

### D.1.6 Required Packages on AIX

The follwoing packages must be running on your AIX systems:

#### AIX 5L Version 5.2

The following file sets must be installed and committed:

- bos.perf.libperfstat
- bos.perf.proctools

The following Authorized Problem Analysis Reports (APARs) must be installed:

- IY43980: libperfstat.h not ANSI-compliant
- IY44810: DSI IN BMRECYCLE
- IY45462: Definition of isnan() in math.h incorrect
- IY45707: J2 READAAHEAD/CIO INTERACTION

- IY46214: dropping partial connections leaves them on so_q0
- IY46605: exec of 32 bit application can fail on 64 bit kernel
- IY51801: race condition in aio_nwait_timeout

#### AIX 5L Version 5.3

The following file sets must be installed and committed:

- bos.perf.libperfstat
- bos.perf.proctools

The following Authorized Problem Analysis Reports (APARs) must be installed:

- IY70159: KRTL relocation problem
- IY68989: write to mmapped space hangs

#### AIX 6L Version 6.1

> **IMPORTANT:** This platform is supported only for Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

The following file sets must be installed and committed:

- bos.adt.base-0.0
- bos.adt.lib-0.0
- bos.adt.libm-0.0
- bos.perf.libperfstat-0.0
- bos.perf.perfstat-0.0
- bos.perf.proctools-0.0
- rsct.basic.rte-0.0
- rsct.compat.clients.rte-0.0
- xlC.aix61.rte-9.0.0.0
- xlC.rte-9.0.0.0

### D.1.6.1 To Verify Whether the Filesets Are Installed and Committed

To determine whether or not the required file sets are installed and committed, execute the foollowing command:

```
# lslpp -l bos.adt.base bos.adt.lib bos.adt.libm \
bos.perf.perfstat bos.perf.libperfstat
```

> **Note:** If a file set is not installed and committed, you need to install it. Refer to your operating system or software documentation for information on handling file sets.

### D.1.6.2 Verify Whether or Not APAR is Installed

To determine whether or not an authorized program analysis report (APAR) is installed, execute the following command:

```
# /usr/sbin/instfix -i -k " IY43980, IY44810,..."
```

**Note:** If an APAR is not installed, you need to install it. For installing and downloading the APAR, refer to:

`https://techsupport.services.ibm.com/server/aix.fdc`

## D.2 Kernel Parameter Requirements

The following sections list the kernel parameter requirements for each platform.

### D.2.1 Kernel Parameter Requirements on Linux

The systems must have at least the following recommended kernel parameters:

**Red Hat Enterprise Linux 3.0, SUSE Linux Enterprise Server 9, and SUSE Linux Enterprise Server 10**

- semmsl = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 2147483648
- shmmni = 4096
- shmall = 2097152
- shmmin = 1
- shmseg = 10
- filemax = 65536

**Red Hat Enterprise Linux 4.0, Red Hat Enterprise Linux 5.x, Oracle Enterprise Linux 4, and Oracle Enterprise Linux 5**

- semmsl = 250
- semmsl2 = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 536870912
- shmmni = 4096
- shmall = 2097152
- filemax = 65536
- ip_local_port_range = 1024 65000
- rmem_default = 262144
- rmem_max = 262144

- wmem_default = 262144
- wmem_max = 262144

To check your kernel parameter settings, run the commands listed in Table D–1.

*Table D–1 Execute Commands to Check Kernel parameter Settings*

| Parameter | Command |
|---|---|
| semmsl, semmns, semopm, semmni | `# /sbin/sysctl -a \| grep sem`[1] |
| shmall, shmmax, shmmni | `# /sbin/sysctl -a \| grep shm` |
| file-max | `# /sbin/sysctl -a \| grep file-max` |
| ip_local_port_range | `# /sbin/sysctl -a \| grep ip_local_port_range` |
| rmem_default | `# /sbin/sysctl -a \| grep rmem_default` |
| rmem_max | `# /sbin/sysctl -a \| grep rmem_max` |
| wmem_default | `# /sbin/sysctl -a \| grep wmem_default` |
| wmem_max | `# /sbin/sysctl -a \| grep wmem_max` |

[1] This command displays the value of the four semaphore parameters in the order listed.

To change your kernel parameter settings, use any text editor to create or edit the `/etc/sysctl.conf` file to add or modify the necessary entries. You may need to restart your system after changing kernel parameters.

> **Note:** Include lines only for the kernel parameter values that you want to change. For the semaphore parameters (`kernel.sem`), you must specify all four values in order.
>
> If the current value of any of your system's kernel parameters is higher than the recommended value, keep your current value.

For example, your `/etc/sysctl.conf` file may look like this:

```
kernel.shmall = 2097152
kernel.shmmax = 536870912
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
fs.file-max = 65536
net.ipv4.ip_local_port_range = 1024 65000
rmem_default = 262144
rmem_max = 262144
wmem_default = 262144
wmem_max = 262144
```

By specifying the values in the `/etc/sysctl.conf` file, they persist when you restart the system.

On SUSE systems only, enter the following command to ensure that the system reads the `/etc/sysctl.conf` file when it restarts:

```
# /sbin/chkconfig boot.sysctl on
```

### D.2.2 Kernel Parameter Requirements on Linux x86_64

The systems must have at least the following recommended kernel parameters:

#### Red Hat Enterprise Linux 3.0, SUSE Linux Enterprise Server 9, SUSE Linux Enterprise Server 10

- semmsl = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 2147483648
- shmmni = 4096
- shmall = 2097152
- shmmin = 1
- shmseg = 10
- filemax = 65536

#### Red Hat Enterprise Linux 4.0, Red Hat Enterprise Linux 5.x, Oracle Enterprise Linux 4.0, Oracle Enterprise Linux 5.0

- semmsl = 250
- semmsl2 = 250
- semmns = 32000
- semopm = 100
- semmni = 128
- shmmax = 536870912
- shmmni = 4096
- shmall = 2097152
- filemax = 65536
- ip_local_port_range = 1024 65000
- rmem_default = 262144
- rmem_max = 262144
- wmem_default = 262144
- wmem_max = 262144

### D.2.3 Kernel Parameter Requirements on Solaris

The system must have at least the following recommended kernel parameters:

#### Solaris 8 and 9

Verify that the following kernel parameters have been set to a equal to or greater than the value specified in Table D–2.

*Table D–2 Recommended Kernel Parameter Values for Solaris 8 and 9*

| Parameter | Recommended Value |
|---|---|
| semsys:seminfo_semmni | 100 |
| semsys:seminfo_semmsl | 256 |

*Table D–2 (Cont.) Recommended Kernel Parameter Values for Solaris 8 and 9*

| Parameter | Recommended Value |
|---|---|
| shmsys:shminfo_shmmax | 4294967295 |
| shmsys:shminfo_shmmin | 1 |
| shmsys_shminfo_shmmni | 100 |
| shmsys:shminfo_shmseg | 10 |
| semsys:seminfo_semvmx | 32767 |
| noexec_user_stack | 1 |

> **Note:** The following parameters are obsolete in Solaris 9:
>
> - `shmsys:shminfo_shmmin`
> - `shmsys:shminfo_shmseg`

### Solaris 10

On Solaris 10, verify that the kernel parameters shown in Table D–3 are set to values equal to or greater than the recommended values. Table D–3 also lists the resource controls that replace the `/etc/system` file for a specific kernel parameter.

*Table D–3 Recommended Kernel Parameter Values for Solaris 10*

| Parameter | Resource Control | Recommended Values |
|---|---|---|
| noexec_user_stack | NA | 1 |

### D.2.3.1 View and Change Kernel Parameter Values on Solaris 8 and 9

To view the current values of the kernel parameters, enter the following commands:

```
# grep noexec_user_stack/etc/system
# /usr/sbin/sysdef | grep SEM
# /usr/sbin/sysdef | grep SHM
```

To change any of the current values, follow these steps:

1. Create a backup copy of the `/etc/system` file, by using a command similar to the following:

   ```
   # cp /etc/system/etc/system.orig
   ```

2. Open the `/etc/system` file in any text editor, and if required, add lines similar to the following (edit the lines if the file already contains them):

   ```
   set semsys:seminfo_semmni=100
   set semsys:seminfo_semmsl=256
   set shmsys:shminfo_shmmax=4294967295
   set shmsys:shminfo_shmmin=1
   set shmsys_shminfo_shmmni=100
   set shmsys:shminfo_shmseg=10
   set semsys:seminfo_semvmx=32767
   set noexec_user_stack=1
   ```

3. Enter the following command to restart the system

   ```
   # /usr/sbin/reboot
   ```

4. After you have restarted the system, log in to the system and switch to the `root` user.

#### D.2.3.2 View and Change Kernel Parameter Values on Solaris 10

To view the current values of the resource control, enter the following commands:

```
#id -p //to verify the project ID
uid = 0 (Root) gid = 0 (Root) projid = 1 (user.root)
#prctl -n project.max-shm-memory -i project user.root
#prctl -n project.max=sem-ids -i project user.root
```

To change any of the current values, follow these steps:

1. To modify the value of `max-shm-memory` to 6GB:

   ```
   #prctl -n project.max-shm-memory -v 6gb -r -i project user.root
   ```

2. To modify the value of `max-sem-ids` to 256:

   ```
   #prctl -n project.max-sem-ids -v 256 -r -i project user.root
   ```

### D.2.4 Kernel Parameter Requirements on HP-UX

Verify that the kernel parameters listed in Table D–4 are set to the values greater than or equal to the recommended value shown. The procedure following Table D–4 describes how to verify and set the values.

*Table D–4 Recommended Kernel Parameter Values for HP-UX*

| Parameter | Recommended Value |
|---|---|
| ksi_alloc_max | 32768 |
| max_thread_proc | 256 |
| maxdsiz | 1073741824 |
| maxdsiz_64bit | 2147483648 |
| maxssiz | 134217728 |
| maxssiz_64bit | 1073741824 |
| maxswapchunks | 16384 |
| maxuprc | 3687 |
| msgmap | 4098 |
| msgmni | 4096 |
| msgseg | 32767 |
| msgtql | 4096 |
| ncsize | 34816 |
| nfile | 63488 |
| nflocks | 4096 |
| ninode | 34816 |
| nkthread | 7184 |
| nproc | 4096 |
| semmap | 4098 |

***Table D–4 (Cont.) Recommended Kernel Parameter Values for HP-UX***

| Parameter | Recommended Value |
|---|---|
| semmni | 4096 |
| semmns | 8192 |
| semmnu | 4092 |
| semvmx | 32767 |
| shmmax | 1073741824 |
| shmmni | 512 |
| shmseg | 120 |
| vps_ceiling | 64 |

> **Note:** The following parameters are obsolete in HP-UX 11.23:
>
> - `maxswapchunks`
> - `semmap`
>
> If the current value of any parameter is higher than the value listed in this table, do not change the value for that parameter.

#### D.2.4.1 View and Change Kernel Parameter Values

To view the current value of these kernel parameters, and to change them, if necessary, follow these steps:

1. Set the DISPLAY environment variable to specify the display of the local system. This is an optional step.

   Bourne, Bash or Korn shell:

   ```
   $ DISPLAY=localhost:0.0; export DISPLAY
   ```

   C Shell

   ```
   $ setenv DISPLAY localhost:0.0
   ```

2. Start System Administration Manager (SAM)

   # /usr/sbin/sam

3. Choose the Kernel Configuration area and the Configurable Parameters area.
4. Check the value or formula specified for each of these parameters and if necessary, modify that value or formula. Refer to the SAM Online Help for more details.
5. Exit from SAM.
6. If you have modified the value for any of the parameters, you must restart your system.

   # /sbin/shutdown -r now

7. After you have restarted the system, log in and switch to the `root` user if necessary.

## D.2.5 Kernel Parameter Requirements on HP-UX Itanium

Verify that the kernel parameters listed in Table D–5 are set to the values greater than or equal to the recommended value shown.

*Table D–5 Recommended Kernel Parameter Values on HP-UX Itanium*

| Parameter | Recommended Value |
|---|---|
| ksi_alloc_max | 32768 |
| max_thread_proc | 256 |
| maxdsiz | 1073741824 |
| maxdsiz_64bit | 2147483648 |
| maxssiz | 134217728 |
| maxssiz_64bit | 1073741824 |
| maxuprc | 3687 |
| msgmni | 4096 |
| msgseg | 32767 |
| msgtql | 4096 |
| ncsize | 34816 |
| nfile | 63488 |
| nflocks | 4096 |
| ninode | 34816 |
| nkthread | 7184 |
| nproc | 4096 |
| semmni | 4096 |
| semmns | 8192 |
| semmnu | 4092 |
| semvmx | 32767 |
| shmmax | 1073741824 |
| shmmni | 512 |
| shmseg | 120 |
| vps_ceiling | 64 |

## D.2.6 Configure Shell Limits and System Configuration Parameters on AIX

On AIX systems, you do not need to configure the kernel parameters. However, Oracle recommends that you set shell limits and system configuration parameters as described in this section.

### D.2.6.1 Configuring Shell Limits

Verify that the shell limits shown in Table D–6 are set to the values shown. The procedure following the table describes how to verify and set the values.

*Table D–6 Shell Limits*

| Shell Limit (as shown in smit) | Recommended Value |
|---|---|
| Soft FILE size | -1 (Unlimited) |
| Soft CPU size | -1 (Unlimited) |
| Soft DATA segment | -1 (Unlimited) |
| Soft STACK size | -1 (Unlimited) |

Do the following to view and change the values that are currently specified for these shell limits:

1. Execute the following command:

```
# smit chuser
```

2. In the User Name field, specify the user name of the Oracle software owner, for example `oracle`.
3. Scroll down the list and verify whether the value for the soft limits is `-1`. If not, edit the existing value as recommended in Table D–6.
4. When you have finished making changes, press **F10** to exit.

### D.2.6.2 Specifying System Configuration Parameters

Ensure the maximum number of processes allowed per user is set to 2048 or higher. The following procedure describes how to verify and set the value.

To specify the system configuration parameters:

1. Execute the following command:

```
# smit chgsys
```

2. Ensure the value shown for Maximum Number of Processes allowed per user is greater than or equal to 2048. If not, edit the existing value.
3. When you have finished making changes, press **F10** to exit.

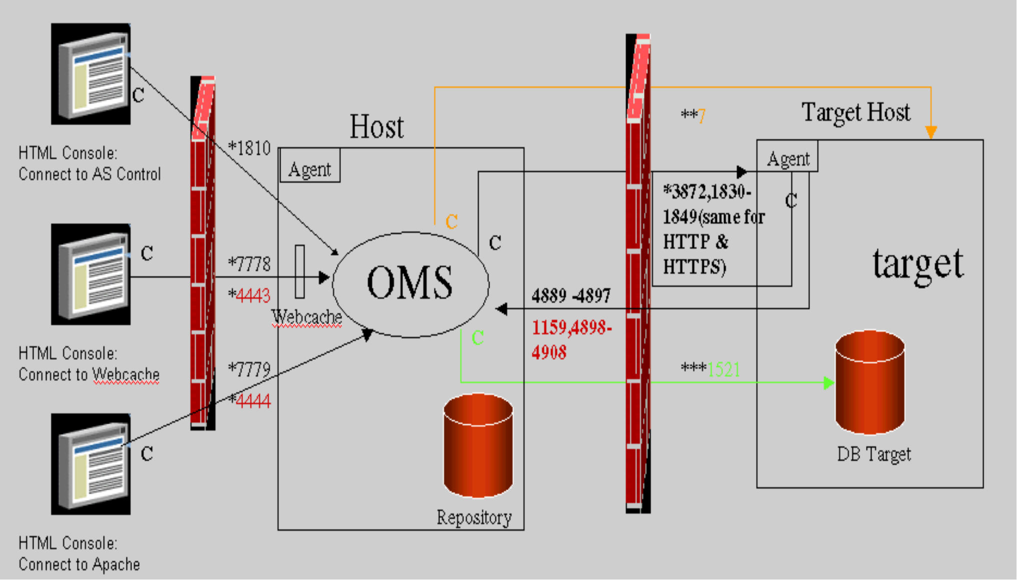
# E

# Firewall Port Requirements

If your Enterprise Manager grid environment is making use of firewalls, ensure you specify the appropriate ports.

Figure E–1 provides a topology of an Enterprise Manager grid environment that is using a firewall, and also illustrates the appropriate ports that you must specify.

***Figure E–1 Enterprise Manager Firewall Port Requirements***



The conventions used in the preceding illustration are as follows:

***Table E–1 Conventions Used***

| 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. |

**Note:**

- 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.

F

# Using the Staticports.ini File

This appendix covers the following:

- Formats for the Staticports.ini File
- Causes for the Installer to Use Default Ports

## F.1 Formats for the Staticports.ini File

The `staticports.ini` file has the following format. Replace `port num` with the port number that you want to use for the component.

```
# Enterprise Manager

#Enterprise Manager Central Agent Port=port_num
#Enterprise Manager Central Console Port=port_num
#Enterprise Manager Central Console Secure Port=port_num

# J2EE and Web Cache

#Oracle HTTP Server Listen port=port_num
#Oracle HTTP Server Listen (SSL) port=port_num
#Oracle HTTP Server Diagnostic port=port_num

#Web Cache HTTP Listen port=port_num
#Web Cache HTTP Listen (SSL) port=port_num
#Web Cache Administration port=port_num
#Web Cache Invalidation port=port_num
#Web Cache Statistics port=port_num

#Oracle Notification Server Request port=port_num
#Oracle Notification Server Local port=port_num
#Oracle Notification Server Remote port=port_num
#Application Server Control port=port_num
#Application Server Control RMI port=port_num
#Oracle Management Agent port=port_num
#Log Loader port=port_num
```

**Note:** After having specified appropriate port values, ensure you remove the comment (#) for those properties before saving the file. The values are not considered otherwise.

## F.2 Causes for the Installer to Use Default Ports

Check your `staticports.ini` file carefully, because a mistake can cause the installer to use default ports without displaying any warning. Here are some things that you should check:

- If a port is already being used by a component or any other application, do not specify that port (used port) in the `staticports.ini` file.

> **Note:** If you specify a port that is already in use, the related configuration assistant will also fail.

- If you have specified the same port for more that one component, the installation will display 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), the installer ignores the line. For the components specified on such lines, the installer assigns the default ports. The installer does not display a warning for lines with syntax errors.
- If you misspell a component name, the installer assigns the default port for the component. Names of components in the file are case-sensitive. The installer does not display a warning for lines with unrecognized names.
- If you specify a nonnumeric value for the port number, the installer 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, the installer does not display a warning. It continues and assigns default ports to all components.
- If you specify a relative path to the `staticports.ini` file (for example, `./staticports.ini`) on the command line, the installer does not find the file. The installer continues without displaying a warning and it assigns default ports to all components. You must specify a full path to the `staticports.ini` file.
- If the parameter you specify on the command line does not match the installation type that you are performing (for example, if you specify the parameter for the middle tier but you are installing the infrastructure), the installer does not give a warning. It continues and assigns default ports to all components.

G

# Agent Deploy Application - Installation Prerequisites

This appendix describes the prerequisites to performing an installation using the Agent Deploy application. It contains the following sections:

- Check Platform-Specific Package Requirements for Agent Installation
- SSH (Secure Shell) Setup
- Validate All Command Locations
- Verify User Credentials
- Prerequisite Checks Executed by Agent Deploy
- Troubleshooting Failed Prerequisite Checks
- Commands and Arguments Executed to Run Agent Deploy Plugins
- Sample Properties Files

## G.1 Check Platform-Specific Package Requirements for Agent Installation

The following lists the packages and disk space requirements for each platform.

***Table G–1 Platform-Specific Package Requirements for Agent Installation***

| Platforms | 32-Bit/ 64-Bit | Required Packages | Approx. Disk Space |
|---|---|---|---|
| HP-UX 11.31 PA-RISC 2.0 | 64-Bit | ■ Base-VXFS - B.11.31,<br>■ OnlineDiag - B.11.31.01.03 | 1.5GB |
| HP-UX 11.11 PA-RISC 2.0 | 64-Bit | ■ X11MotifDevKit - 0.0<br>■ X11MotifDevKit.MOTIF21-PRG - 0.0 | 1.5GB |
| HP-UX 11.23 PA-RISC 2.0 | 64-Bit | BUNDLE11i - B.11.23.0409.3 | 1.5GB |
| HP-UX 11.23 IA64N | 64-Bit | BUNDLE11i - B.11.23.0409.3 | 1.9GB |
| HP-UX 11.31 IA64N | 64-Bit | BUNDLE - B.11.31 | 1.9GB |
| AIX 5.2 | 64-Bit | bos.perf.proctools - 5.2.0.40 | 1.8GB |
| AIX 5.3 | 64-Bit | bos.perf.proctools - 5.3.0.50 | 1.8GB |

*Table G–1 (Cont.) Platform-Specific Package Requirements for Agent Installation*

| Platforms | 32-Bit/ 64-Bit | Required Packages | Approx. Disk Space |
|---|---|---|---|
| AIX 6.1 | 64-Bit | ■ bos.adt.base - 0.0<br>■ bos.adt.lib - 0.0<br>■ bos.adt.libm - 0.0<br>■ bos.perf.libperfstat - 0.0<br>■ bos.perf.perfstat - 0.0<br>■ bos.perf.proctools - 0.0<br>■ rsct.basic.rte - 0.0<br>■ rsct.compat.clients.rte - 0.0<br>■ xlC.aix61.rte-9.0.0.0<br>■ xlC.rte - 9.0.0.0 | 1.8GB |
| Solaris 5.8<br>(SPARC) | 64-Bit | ■ SUNWarc<br>■ SUNWbtool<br>■ SUNWhea<br>■ SUNWlibm<br>■ SUNWlibms<br>■ SUNWsprot<br>■ SUNWsprox<br>■ SUNWtoo<br>■ SUNWi1of<br>■ SUNWxwfnt | .90GB |
| Solaris 5.9<br>(SPARC) | 64-Bit | ■ SUNWlibm<br>■ SUNWlibms<br>■ SUNWsprot<br>■ SUNWsprox<br>■ SUNWtoo<br>■ SUNWi1of<br>■ SUNWxwfnt | .90GB |
| Solaris 5.10<br>(SPARC) | 64-Bit | SUNWbtool | .90GB |
| Linux x86-64<br>(Enterprise Linux 4) | 64-Bit | ■ make - 3.79<br>■ binutils - 2.15.92.0.2-13<br>■ gcc - 3.4.3-22.1 | .45GB |
| Linux x86-64<br>(Enterprise Linux 5) | 64-Bit | ■ make - 3.79<br>■ binutils-2.14<br>■ gcc - 3.2 | .45GB |
| Linux x86-64<br>(Redhat Linux 3) | 64-Bit | ■ make - 3.79,<br>■ binutils - 2.14<br>■ gcc - 3.2 | .45GB |

*Table G–1 (Cont.) Platform-Specific Package Requirements for Agent Installation*

| Platforms | 32-Bit/ 64-Bit | Required Packages | Approx. Disk Space |
|---|---|---|---|
| Linux x86-64<br>(Redhat Linux 4) | 64-Bit | ■ make - 3.79<br>■ binutils - 2.14<br>■ gcc - 3.2 | .45GB |
| Linux x86-64<br>(Redhat Linux 5) | 64-Bit | ■ make - 3.79,<br>■ binutils - 2.14<br>■ gcc - 3.2 | .45GB |
| Linux x86-64<br>(Suse Linux 8) | 64-Bit | ■ make - 3.79,<br>■ binutils - 2.14<br>■ gcc - 3.2 | .45GB |
| Linux x86-64<br>(Suse Linux 9) | 64-Bit | ■ make - 3.79<br>■ binutils-2.14<br>■ gcc - 3.2<br>■ glibc-devel-32bit - 2.4 | .45GB |
| Linux x86-64<br>(Suse Linux 10) | 64-Bit | ■ make - 3.79,<br>■ binutils-2.14<br>■ gcc - 3.2<br>■ glibc-devel-32bit - 2.4 | .45GB |
| Linux Itanium<br>(Red Hat Enterprise Linux<br>AS/ES 3.0 ia 64) | 64-Bit | ■ GLIBC>=2.3.2-95.27<br>■ Make - 3.79<br>■ binutils - 2.14<br>■ Libaio - 0.3.96 | .75GB |
| Linux Itanium<br>(Red Hat Enterprise Linux<br>AS/ES 4.0 ia 64) | 64-Bit | ■ GLIBC>=2.3.2-95.27<br>■ Make - 3.79<br>■ binutils - 2.14<br>■ Libaio - 0.3.96<br>■ gcc - 3.2 | .75GB |
| Linux Itanium<br>(SUSE Linux Enterprise<br>Server 9 ia 64) | 64-Bit | ■ GLIBC>=2.3.3-98.28<br>■ Make - 3.80<br>■ binutils - 2.14<br>■ Libaio - 0.3.102<br>■ gcc - 3.3 | .75GB |
| Linux<br>(Red Hat Enterprise Linux<br>3.0, 4.0, 5.0) | 32 | ■ Make - 3.79<br>■ binutils - 2.14<br>■ gcc - 3.2 | .75GB |
| SUSE Linux Enterprise<br>Server 9, 8, 10 | 32 | gcc Version 3.2 | .75GB |
| Oracle Enterprise Linux 4.0,<br>5.0 | 32 | ■ Make - 3.79<br>■ binutils - 2.15.92.0.2-13<br>■ gcc - 3.4.3-22.1 | .75GB |

*Table G–1 (Cont.) Platform-Specific Package Requirements for Agent Installation*

| Platforms | 32-Bit/ 64-Bit | Required Packages | Approx. Disk Space |
|---|---|---|---|
| z/Linux<br>(RedHat s390 linux 4) | 64-Bit | ■ GLIBC ATLEAST>=2.3.2-95.27<br>■ make - 3.79,<br>■ binutils - 2.1<br>■ gcc - 3.2,<br>■ libaio - 0.3.96 | .67 GB |
| z/Linux<br>(Suse s390 linux 4) | 64-Bit | ■ GLIBC ATLEAST>= 2.3.3-98.28<br>■ make - 3.79,<br>■ binutils - 2.14<br>■ gcc - 3.2,<br>■ libaio - 0.3.96 | .67 GB |
| z/Linux<br>(Suse s390 linux 3) | 64-Bit | ■ GLIBC ATLEAST>= 2.3.3-98.28<br>■ make - 3.79,<br>■ binutils - 2.14<br>■ gcc - 3.2 | .67 GB |

## G.2 SSH (Secure Shell) Setup

SSH Setup is the connectivity that is established between the host running Oracle Management Service and the host where the Management Agent needs to be installed. This is primarily required for the Agent Deploy application to install Management Agents over HTTP on remote hosts.

The Agent Depoly application is an application that is part of the Enterprise Manager Grid Control console. It is used for deploying Management Agents in your environment using an interactive user interface. The installation of a Management Agent from the source host to the remote target host happens over HTTP, and for this communication to happen over HTTP, an SSH setup is required between the two hosts. This also helps to avoid SSH authentication calls during future Agent Deploy operations.

**Caution:** The SSH Setup must always be set between the target hosts and the OMS, and never among the target hosts.

### G.2.1 Installing Management Agent Using 10.2.0.1 Enterprise Manager Grid Control

SSH Setup is required if you are installing a Management Agent using Enterprise Manager 10g Grid Control Release 2 (10.2.0.1).

In order to set up SSH, you must run the `sshUserSetup.sh` script (`sshUserSetupNT.sh` on Microsoft Windows) that is available at the following location:

```
OMS_HOME/sysman/prov/resources/scripts
```

Before running the `sshUserSetup.sh` script, check whether you have specified the correct path for the SSH_KEYGEN parameter. To find out the correct path, run the command *whereis ssh-keygen* or *which ssh-keygen* on the target host. Ensure that the same path is specified for the SSH_KEYGEN parameter. To verify this, run the following command:

```
grep SSH_KEYGEN= sshUserSetup.sh
```

For information about running this script for Unix platforms, see Appendix G.2.1.1, "Setting Up SSH on UNIX Using sshUserSetup.sh (Only For 10.2.0.1 Enterprise Manager Grid Control)".

For information about running this script for Microsoft Windows platforms, see Appendix G.2.1.2, "Setting Up SSH Server (SSHD) on Microsoft Windows (Only For 10.2.0.1 and 10.2.0.3 Enterprise Manager Grid Control)" and Appendix G.2.1.3, "Setting Up SSH on Microsoft WIndows Using sshUserSetupNT.sh (Only For 10.2.0.1 Enterprise Manager Grid Control)".

### G.2.1.1 Setting Up SSH on UNIX Using sshUserSetup.sh (Only For 10.2.0.1 Enterprise Manager Grid Control)

Usage of this script is as follows:

```
sshUserSetup.sh -hosts "<hostlist>" -user <user name> [-verify] [-confirm]
[-shared]
```

For example, `sshUserSetup.sh -hosts "host1 host2" -user sjohn`

#### Description

This script is used to set up SSH from the host on which it is run to the specified remote hosts. After this script is run, you can use SSH to execute commands on the remote hosts, or copy files between the local host and the remote hosts without being prompted for passwords or confirmations.

The list of remote hosts and their user names are specified as command-line parameters to the script.

- *-shared*

  In case you have the home directory NFS-mounted or shared across the remote hosts, the script should be used with the `-shared` option.

  To determine whether or not an Oracle Home Directory is Shared or Not Shared, consider a scenario where you want to determine whether the Oracle home directory of *user1* is shared across hosts A, B, and C or not.

  You can determine this by following these instructions:

  1. On host A, `touch ~user1/checkSharedHome.tmp`.
  2. On hosts B and C, execute `ls -al ~user1/checkSharedHome.tmp`.

     If the file is present on hosts B and C in the `~user1` directory and is identical on all nodes, it means that the user's home directory is shared.
  3. On host A, `rm -f ~user1/checkSharedHome.tmp`.

  **Note:** In the event that you accidentally pass the `-shared` option for nonshared homes or reverse, the SSH is set up for only a subset of the hosts. You will have to rerun the setup script with the correct option to rectify this issue.

- *-verify*

The -verify option allows you to verify if SSH has been set up. In this case, the script does not set up SSH, but only checks if *SSH* has been set up from the local host to the remote hosts. It then runs the date command on each remote host using SSH. In case you are prompted for a password or see a warning message for a particular host, it means the SSH  has not been set up correctly for that host.

In case the -verify option is not specified, the script sets up SSH and then does the verification as well.

- *-confirm*

  The -confirm option allows you to set up SSH with a forced change in the permissions on remote hosts. This means that the script will not prompt you to confirm the change in permissions, if you execute the script passing the -confirm option.

- *-help*

  Use this option to view the readme file for the sshUserSetup.sh script. The usage is as follows:

  ```
  sshUserSetup.sh -help
  ```

The following examples provides usage of the previously mentioned options:

```
Local host = Z
Remote Hosts = A, B, and C
Local user = sjohn
Remote users = foo (non-shared)
aime (shared)
./sshUserSetup.sh -user foo -hosts "A B C" -confirm
```

***Example G–1    Set Up SSH and Verify the Setup***

```
sshUserSetup.sh -hosts "A B C" -user foo
```

This script sets up SSH from:

- Z to A
- Z to B
- Z to C

***Example G–2    Set Up SSH and verify the Setup Without a Confirmation Prompt***

```
sshUserSetup.sh -hosts "A B C" -user foo -confirm
```

This sets up SSH between the local host and A, B, C. It also verifies the setup. However, due to the usage of the -confirm option, it assumes that users are aware of the changes that would be made on the systems and will not ask for any confirmation.

***Example G–3    Verify Existing SSH Setup***

```
./sshUserSetup.sh -hosts "A B C" -user foo -verify
```

Because the -verify option is specified, the script does not set up the SSH setup, but only verifies the existing setup.

### G.2.1.2 Setting Up SSH Server (SSHD) on Microsoft Windows (Only For 10.2.0.1 and 10.2.0.3 Enterprise Manager Grid Control)

Before starting with the SSHD setup, ensure you are not using OpenSSH and MKSNT when using the Agent Deploy application. The Agent Deploy application uses the complete Cygwin suite (full collection of the software tools packaged in Cygwin). To get the complete collection of Cygwin, do the following:

1. Ensure `OpenSSH\bin` and `mksnt` are not in your `%PATH%`. If they are, remove them by doing the following:
   a. Right-click on **My Computer** and go to Properties.
   b. In the System Properties window that appears, click **Advanced.**
   c. In this tab, click **Environment Variables.**
   d. Here, search for the Path system variable, select it, and if the `OpenSSH\bin` and `mksnt` are present in the PATH, click **Edit.**
   e. In the Edit System Variable dialog box that appears, delete these two values from the PATH, and click **OK.**
2. Now, stop the SSH Daemon if it is running from OpenSSH. To do this:
   a. Right-click on **My Computer**, and select **Manage.**
   b. In the Computer Management window that appears, go to Services under Services and Applications.
   c. In the right-pane, select the SSH daemon service and click the **Stop Service** icon.

   **Note:** Ensure you rename the installation directories of `OpenSSH` and `MKSNT`.

3. To install the full suite of Cygwin software, go to `http://www.cygwin.com`, and install Cygwin in your `C:\cygwin` directory.

   **Note:** If you are installing Cygwin into another directory than what has been previously mentioned, ensure you update the `$OMS_HOME/sysman/prov/resources/ssPaths_msplats.properties` file with the proper Cygwin binary values after installing Oracle Enterprise Manager Grid Control.

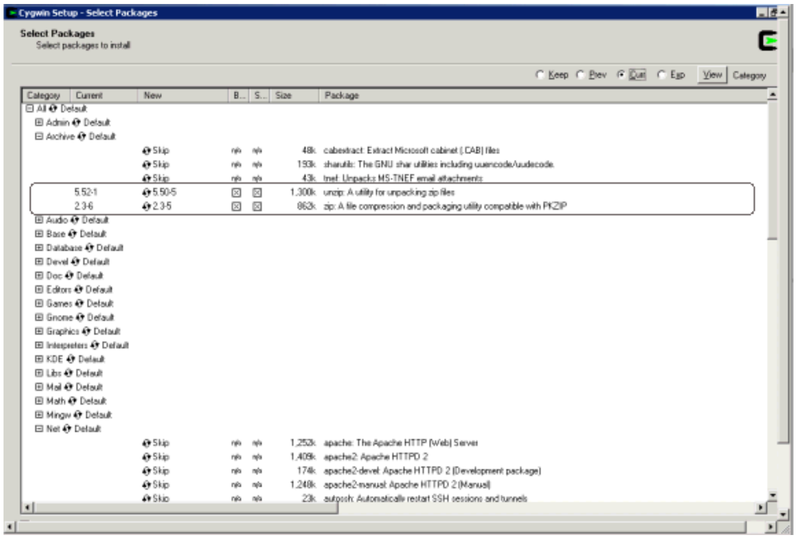
   **Caution:** If you are installing *Cygwin* at a directory that is other than `C:\cygwin` on a remote machine, you must also ensure that Cygwin is installed on the OMS machine at the exact same location.

   The Cygwin installation directory should not contain any spaces.

   While installing Cygwin, ensure you choose the following binaries:

   a. Zip, unzip binaries from the Archive package.

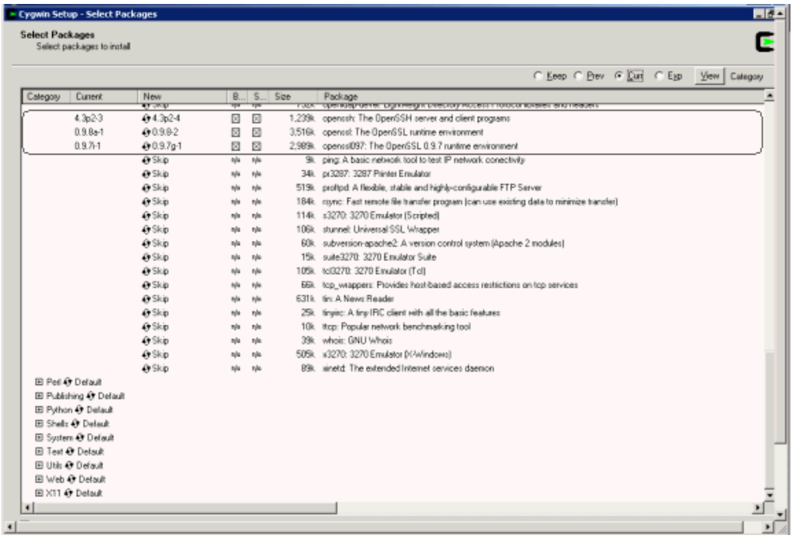
*Figure G–1 Zip Unzip Binaries*


Cygwin Setup - Select Packages
Select Packages
Select packages to install
○ Keep ○ Prev ● Curr ○ Exp
View
Category

| Category | Current | New | B... | S... | Size | Package |
|---|---|---|---|---|---|---|
| ⊟ All Default | | | | | | |
| ⊞ Admin Default | | | | | | |
| ⊟ Archive Default | | | | | | |
| | | Skip | n/a | n/a | 48k | cabextract: Extract Microsoft cabinet (.CAB) files |
| | | Skip | n/a | n/a | 193k | sharutils: The GNU shar utilities including uuencode/uudecode. |
| | | Skip | n/a | n/a | 43k | tnef: Unpacks MS-TNEF email attachments |
| | 5.52-1 | 5.50-5 | ☒ | ☒ | 1,300k | unzip: A utility for unpacking zip files |
| | 2.3-6 | 2.3-5 | ☒ | ☒ | 862k | zip: A file compression and packaging utility compatible with PKZIP |
| ⊞ Audio Default | | | | | | |
| ⊞ Base Default | | | | | | |
| ⊞ Database Default | | | | | | |
| ⊞ Devel Default | | | | | | |
| ⊞ Doc Default | | | | | | |
| ⊞ Editors Default | | | | | | |
| ⊞ Games Default | | | | | | |
| ⊞ Gnome Default | | | | | | |
| ⊞ Graphics Default | | | | | | |
| ⊞ Interpreters Default | | | | | | |
| ⊞ KDE Default | | | | | | |
| ⊞ Libs Default | | | | | | |
| ⊞ Mail Default | | | | | | |
| ⊞ Math Default | | | | | | |
| ⊞ Mingw Default | | | | | | |
| ⊟ Net Default | | | | | | |
| | | Skip | n/a | n/a | 1,252k | apache: The Apache HTTP (Web) Server |
| | | Skip | n/a | n/a | 1,409k | apache2: Apache HTTPD 2 |
| | | Skip | n/a | n/a | 174k | apache2-devel: Apache HTTPD 2 (Development package) |
| | | Skip | n/a | n/a | 1,248k | apache2-manual: Apache HTTPD 2 (Manual) |
| | | Skip | n/a | n/a | 23k | autossh: Automatically restart SSH sessions and tunnels |

**b.** OpenSSH and dependencies (automatically selected if you choose OpenSSH) from the Net package.

*Figure G–2 Net Packages*


Cygwin Setup - Select Packages
Select Packages
Select packages to install
○ Keep ○ Prev ● Curr ○ Exp
View
Category

| Category | Current | New | B... | S... | Size | Package |
|---|---|---|---|---|---|---|
| | | Skip | n/a | n/a | [illegible] | openldap-devel: Lightweight Directory Access Protocol libraries and headers |
| | 4.3p2-3 | 4.3p2-4 | ☒ | ☒ | 1,239k | openssh: The OpenSSH server and client programs |
| | 0.9.8a-1 | 0.9.8-2 | ☒ | ☒ | 3,516k | openssl: The OpenSSL runtime environment |
| | 0.9.7i-1 | 0.9.7g-1 | ☒ | ☒ | 2,989k | openssl097: The OpenSSL 0.9.7 runtime environment |
| | | Skip | n/a | n/a | 9k | ping: A basic network tool to test IP network conectivity |
| | | Skip | n/a | n/a | 34k | pr3287: 3287 Printer Emulator |
| | | Skip | n/a | n/a | 519k | proftpd: A flexible, stable and highly-configurable FTP Server |
| | | Skip | n/a | n/a | 184k | rsync: Fast remote file transfer program (can use existing data to minimize transfer) |
| | | Skip | n/a | n/a | 114k | s3270: 3270 Emulator (Scripted) |
| | | Skip | n/a | n/a | 106k | stunnel: Universal SSL Wrapper |
| | | Skip | n/a | n/a | 60k | subversion-apache2: A version control system (Apache 2 modules) |
| | | Skip | n/a | n/a | 15k | suite3270: 3270 Emulator Suite |
| | | Skip | n/a | n/a | 105k | tcl3270: 3270 Emulator (Tcl) |
| | | Skip | n/a | n/a | 66k | tcp_wrappers: Provides host-based access restrictions on tcp services |
| | | Skip | n/a | n/a | 631k | tin: A News Reader |
| | | Skip | n/a | n/a | 25k | tinyirc: A tiny IRC client with all the basic features |
| | | Skip | n/a | n/a | 10k | ttcp: Popular network benchmarking tool |
| | | Skip | n/a | n/a | 39k | whois: GNU Whois |
| | | Skip | n/a | n/a | 505k | x3270: 3270 Emulator (X-Windows) |
| | | Skip | n/a | n/a | 89k | xinetd: The extended Internet services daemon |
| ⊞ Perl Default | | | | | | |
| ⊞ Publishing Default | | | | | | |
| ⊞ Python Default | | | | | | |
| ⊞ Shells Default | | | | | | |
| ⊞ System Default | | | | | | |
| ⊞ Text Default | | | | | | |
| ⊞ Utils Default | | | | | | |
| ⊞ Web Default | | | | | | |
| ⊞ X11 Default | | | | | | |

**4.** Modify the `C:\cygwin\cygwin.bat` file to add the following line:

```
set CYGWIN=binmode tty ntsec
```

**5.** Ensure `cygrunsrv` is installed by going to `C:\cygwin\bin` and executing the following:

```
bash
cygrunsrv -h
```

---

**Note:** If you are prompted to provide a Cygwin value, enter `binmode tty ntsec`. If this returns an error message stating "service does not exist", you are on the right track, and can proceed to the next step.

If you encounter any other error message, (for example, "*command cygrunsrv not found*"), see Section A.1.4.6, "Troubleshooting the "command cygrunsrv not found" Error." for more information on troubleshooting this issue.

---

6. Open a new command prompt and execute the following:

```
bash
ssh-host-config
```

---

**Note:** Enter "*no*" when prompted to create sshd user account (message reads "`sshd user account needs to be created`").

Enter "*yes*" at all other prompts.

When prompted to answer the question "Which value should the environment variable CYGWIN have when sshd starts?", Oracle recommends that you set the value to at least "ntsec" as shown in the following example. This will enable you to change the user context without having to specify the password.

As an answer to the previously mentioned question, specify a value that is similar to the following and press **Enter**:

```
CYGWIN="binmode tty ntsec"
```

---

7. Now, open the `/etc/passwd` file, and remove only those entries of the user that you will use to connect to the OMS machine.

   For example,

   - If the user that you are employing to connect to the OMS machine is a local user, execute the following:

     ```
     /bin/mkpasswd -l -u <USER> >> /etc/passwd
     ```

   - If the user you are employing to connect to the OMS machine is a domain user, execute the following:

     ```
     /bin/mkpaswd.exe -d -u <USER> >> /etc/passwd
     /bin/mkgroup.exe -d >> /etc/group


     mkdir -p /home/<USER>  (for example, mkdir -p /home/pjohn)
     chown <USER> /home/<USER> (for example, chown pjohn /home/pjohn)
     ```

8. Start the SSH daemon.

   If the user you are employing to connect to the OMS machine is a domain user, do the following:

   a. Right-click on **My Computer**, and select Manage.

b. In the Computer Management dialog box that appears, go to Services and Applications, and select **CYGWIN sshd**.

c. Right-click **CYGWIN sshd** and select Properties.

d. In the Properties dialog box, go to the Log On tab.

e. Here, specify the domain/username and password. Click **Apply.**

f. Now, go to the CYGWIN command prompt, and execute the following:

```
chmod 644 /etc/ssh*
   chmod <USERNAME> /var/empty
   chmod 755 /var/empty
   chmod 644 /var/log/sshd.log
```

---

**Note:** If `/var/log/sshd.log` does not exist, you do not have to execute the following command:

```
chmod 644 /var/log/sshd.log
```

---

g. Start the SSH daemon by executing:

```
/usr/sbin/sshd
```

Alternatively, from the same BASH prompt, you can also execute:

```
cygrunsrv -S sshd
```

---

**Note:** Use `cygrunsrv -E sshd` to stop the SSH daemon.

---

9. You can now test your `cygwin` setup.

To do this, go to a different machine (that has the `ssh` client running), and execute the following command:

```
ssh -l <USERNAME> <localhost> 'date'

OR

ssh -l <USERNAME> <this node> 'date'
```

For example,

```
ssh -l pjohn egal07.db.funds.com 'date'
```

This command will prompt you to specify the password. When you specify the correct password, the command should return the accurate date.

#### G.2.1.3 Setting Up SSH on Microsoft WIndows Using sshUserSetupNT.sh (Only For 10.2.0.1 Enterprise Manager Grid Control)

---

**Note:** Before executing the `sshUserSetupNT.sh` script, execute the following commands to ensure the home directory has been correctly set:

1. Execute `echo $HOME`

   Ensure this displays the home directory of the current user.
2. If it points to the home directory of another user, execute the following command:

   ```
   export HOME=<Windows style absolute path of homedir>
   ```

3. Now, execute `echo $HOME` again, to verify the home directory. The `$HOME` value must be the same as that passed to `-homeDir`

---

This is the script that should be executed to set up SSH on Microsoft Windows platforms. The usage of the script is as follows:

```
./sshUserSetupNT.sh -user -asUser -asUserGrp -sshLocalDir -homeDir -hosts
-hostfile
```

For example, `./sshUserSetupNT.sh -user pjohn -asUser SYSTEM -asUserGrp root-sshLocalDir "C:\cygwin\.ssh" -homeDir "C:\Documents and Settings\pjohn" -hosts "host1 host2"`

---

**Note:** After the `SSHUserSetupNT.sh` script has been executed, you must verify the successful SSH user setup on all the hosts, individually.

That is, if you have run the script to set up SSH on two hosts (host1, and host2), you must run the following command on each host to verify successful SSH setup:

```
ssh -l <username> host1 'date'

and then run:

ssh -l <username> host2 'date'
```

---

**Caution:** You must execute the `sshUserSetupNT.sh` script on the local OMS machine from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

---

All the previously mentioned options are mandatory, and should be passed while executing the script.

**Note:** It is assumed that C:/cygwin is the default installation directory for the Cygwin binaries.

If you install cygwin at a location other than c:\cygwin (default location), it can cause the SSH setup to fail, and in turn, the agent installation will fail.

To work around this issue, you must either install cygwin in the default directory (c:\cygwin), or update the ssPaths_msplats.properties file with the correct path to the cygwin binaries.

You can look into the following remote registry key to find out the correct Cygwin path:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/
```

### Description

This script is used on Microsoft Windows platforms to set up SSH from the host on which it is run to the specified remote hosts. After this script is run, you can use SSH to execute commands on the remote hosts, or copy files between the local host and the remote hosts without being prompted for passwords or confirmations.

The list of remote hosts and their user names are specified as command-line parameters to the script.

- *-asUser*

  This is the user of the local machine on which the setup must be performed. For example, SYSTEM.

- *-asuserGrp*

  This is the group to which the specified asUser belongs.

- *-sshLocalDir*

  This is the full path to the directory where the keys should be generated for the asUser on the local machine.

- *-homeDir*

  This is the full path to the home directory of the current user.

  If the /home key (in regedit) is seen as a subkey under the Cygnus Solutions key, then the value of the /home key must have /<username> as a suffix and then be used as -homeDirm value.

  If the /home key is not found, go to the Cygwin BASH prompt and check the value of $HOME. You can now use the same value of $HOME as the value for -homeDir.

  If $HOME does not have any value (is empty), then you must update the /etc/passwd file.

  **Identifying the Correct Entry in the /etc/passwd File**

  If the /etc/passwd file has only one entry for the user, you can simply modify that value. In the event that there are multiple entries in this file, you must first identify the correct entry and then modify it.

  To identify the correct entry:

– Execute the following command if you have specified a local user during SSH setup:

```
/bin/mkpasswd -l -u <username>
```

– Execute the following command if you have specified a domain user during SSH setup:

```
/bin/mkpasswd -d -u <username>
```

Now, match the output with the corresponding entry in the `/etc/passwd` file. This is the entry that you must modify.

**Updating the -homeDir value**

All values for all users are listed as colon (:) separated entries (or fields). To update the user entry that you have identified previously, go to the penultimate value (or field) of that user entry, and modify the value of the home directory for that user.

Always specify the absolute path needed by Cygwin as value for the home directory. For example, if the path is `C:\Documents and Settings\pjohn`, modify it to:

```
/cygdrive/c/Documents and Settings/pjohn
```

Or, if the path reads `C:\cygwin\pjohn`, modify this to:

```
/cygdrive/c/cygwin/pjohn
```

Now, save the password file and reenter the BASH shell.

---

**Note:** If you have used spaces in the `$HOME` value (for example, `/cygdrive/c/Documents and Settings/pjohn`), specify the `$HOME` value in Microsoft Windows style and within double quotation marks (for example, `"C:\ Documents and Settings\pjohn"`).

---

**Note:** Specify the full path within double quotation marks (" ").

---

**Caution:** You must execute the `sshUserSetupNT.sh` script on the local OMS machine from within the `cygwin` (BASH) shell only. The script will fail to execute if done from outside this location.

---

### G.2.2 Installing Management Agent Using 10.2.0.2 Enterprise Manager Grid Control

SSH Setup is required if you are installing a Management Agent using Enterprise Manager 10g Grid Control Release 2 (10.2.0.2).

For 10.2.0.2 Management Agents, only one script for both Linux and Microsoft Windows is used. The script is sshConnectivity.sh and it is available at the following location:

```
OMS_HOME/sysman/prov/resources/scripts
```

For information about running this script, see Appendix G.2.2.1, "Setting Up SSH Using sshConnectivity.sh (Only For 10.2.0.2 Enterprise Manager Grid Control)".

### G.2.2.1 Setting Up SSH Using sshConnectivity.sh (Only For 10.2.0.2 Enterprise Manager Grid Control)

The `sshConnectivity.sh` script is used on UNIX/Microsoft Windows platforms to set up SSH from the (local) host on which it is run, to the specified remote hosts. After this script is executed, you can use SSH to run commands on the remote hosts, or copy files between the local and the remote hosts without being prompted for passwords or confirmations.

Before executing this script, you must ensure that the following environment variables are set:

- `ORACLE_HOME`

  Set this to the OMS home as an environment variable using the following command:

  For CSH shell

  ```
  setenv ORACLE_HOME /scratch/OracleHomes/oms10g
  ```

  For BASH shell

  ```
  export ORACLE_HOME= /scratch/OracleHomes/oms10g
  ```

- `SSH_LOC`

  You need not specify this if the `ORACLE_HOME` variable has already been set. If it has not been set, ensure that this value points to the directory that contains the SSH and remote interfaces JARS files (`ssh.jar`, `remoteinterfaces.jar`, `jsch.jar`).

- `OUI_JAR`

  You need not specify this if the `ORACLE_HOME` variable has already been set. If this variable has not been set, ensure that this value points to the OUI home directory.

- `JAVAHOME`

  You need not specify this if the `ORACLE_HOME` variable has already been set. If this variable has not been set, ensure that this value points to the JAVA home directory.

> **Note:** All these variables can also be passed as command-line variables to the script in the form of `var=value`.

#### G.2.2.1.1 sshConnectivity.sh Script Usage

The usage of this script is as follows:

```
./sshConnectivity.sh -user <username> -hosts <space separated
hostlist> | -hostfile <absolute path of cluster configuration file>
[-asUser <user for which the setup needs to be done on the local machine, for
example,SYSTEM>
[-asUserGrp <group that the specified asUser belongs to>]
-sshLocalDir <windows style full path of dir where keys should be
generated on the local machine for asUser>] [ -advanced ]
[-usePassphrase] [-logfile <absolute path of logfile> ] [-confirm]
[-shared] [-verify] [-exverify] [-remotePlatform <platform id (linux:46,
solaris:453, msplats:912>] [-obPassword <obfuscated password>] [-silent]
[-localPlatformGrp <unix,win>] [help]
```

***Example G–4 Usage of the sshConnectivity.ch Script to Set Up SSH on Local UNIX Platforms (Linux, Solaris, HP-UX, and IBM AIX)***

```
./sshConnectivity.sh -user <username> -hosts <space separated
hostlist> | -hostfile <absolute path of cluster configuration file>
[-remotePlatform <platform id (linux:46, solaris:453, msplats:912>]
[-shared] [-confirm]
```

For example,

```
./sshConnectivity.sh -user pjohn -hosts sidtest1
./sshConnectivity.sh -user alhammel -hosts zeke2 -remotePlatform 453
```

***Example G–5 Usage of the sshConnectivity.ch Script to Set Up SSH on Local Microsoft Windows Platforms***

```
./sshConnectivity.sh -user
<username> -localPlatformGrp win -asUser <user for which the setup needs to
be done on the local machine, for example, SYSTEM> [-asUserGrp <group that the
specified asUser belongs to>] -sshLocalDir <Windows style full
path of dir where keys should be generated on the local machine for
asUser> -hosts <space separated hostlist> | -hostfile <absolute path of
cluster configuration file> [-remotePlatform <platform id (linux:46,
solaris:453, msplats:912>] [-shared] [-confirm]
```

For example,

1. Go to the Cygwin BASH prompt and execute `cd /`
2. Execute `mkdir .ssh`
3. Now, execute the script as follows:

   ```
   ./sshConnectivity.sh -user alhammel -localPlatformGrp win -asUser SYSTEM
   -asUserGrp root -sshLocalDir C:\cygwin\.ssh -hosts scrat2
   ```

**Note:** Specify all the paths in double quotation marks (" ").

### Parameter Description

- *-user*

  This is the user on remote hosts.

- *-hosts*

  This specifies space-separated remote hosts list.

- *-hostfile*

  You can specify the host names either through the `-hosts` option, or by specifying the absolute path of a cluster configuration file. A sample of the host file content is as follows:

  ```
  scrat02 scrat02int 10.1.0.0 scrat02v -
  scrat06 scrat06int 10.1.0.1 scrat06v -
  ```

**Note:** The first column in each row of the host file will be used as the host name.

- *-localPlatformGrp*

  Specify this option if the local platform is Microsoft Windows. The default value of this option is `unix`.

- *-remotePlatform*

  You must specify this option is the remote platform is not the same as the local platform. Here, you must specify the platform ID of the remote platform. You can find the platform IDs of the supported platforms in the `platforminfo.properties` file.

> **Caution:** When you are executing this script on a Microsoft Windows OMS machine, ensure it is executed from within the Cygwin `BASH` shell. This script will fail to execute if run from outside this location.

## G.2.3 Installing Management Agent Using 10.2.0.3 or higher Enterprise Manager Grid Control

SSH Setup is required if you are installing a Management Agent using Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) or higher, but you do not have to set it up manually.

In Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) or higher, the Agent Deploy application sets up and drops the SSH connectivity automatically, but if the Management Agent is going to be on a Microsoft Windows operating systems, then you need to install and configure Cygwin on that host.

Therefore, if you are installing a Management Agent using Enterprise Manager 10g Grid Control Release 3 (10.2.0.3) or higher, then you do not have to set up the SSH connectivity manually, but have to install Cygwin for Microsoft Windows hosts. So you do not have to run the SSH script (sshUserSetup.ssh/sshUserSetupNT.ssh, sshConnectivity.sh) before starting with the Agent Deploy application.

For information about setting up SSH for Microsoft Windows, see Appendix G.2.1.2, "Setting Up SSH Server (SSHD) on Microsoft Windows (Only For 10.2.0.1 and 10.2.0.3 Enterprise Manager Grid Control)".

## G.2.4 Setting Up the Timezone Variable on Remote Hosts

This section lists the steps you must follow to set up the timezone environment variable on remote hosts.

To verify if the timezone environment variable (TZ) is accessible by the SSH server on the remote hosts, execute the following command from the OMS host:

```
ssh -l <user_name> -n <remote_node> 'echo $TZ'
```

If this command does not return the TZ environment variable value, you must set the TZ variable and ensure this is accessible by the SSH server. You can set the TZ environment variable on remote hosts in the following sections:

### G.2.4.1 Set the TZ variable and Restart the SSH Daemon

If the shell being used is BASH, add the following line to the `.bashrc` file in the home directory of the user (being used) for `ssh` access:

```
export TZ=<your machine's timezone>
```

If you are using a CSH shell, then add the following line to the `.cshrc` file in that directory:

```
setenv TZ <your machine's timezone>
```

1. Depending on the shell that is present on the host, set the TZ variable by executing the following command:

   ```
   For a CSH Shell, specify:
   setenv TZ PST8PDT
   ```

2. Restart the SSH daemon by executing:

   ```
   sudo /etc/init.d/sshd restart
   ```

3. Now, execute the following command from the OMS home to verify if the SSH server can access the TZ variable.

   ```
   ssh -l <user_name> -n <node_name> 'echo $TZ'
   ```

#### G.2.4.2 Set the TZ Variable in the "Shell rc" File

The timezone variable must be set in the `rc` file of the shell that the host is using.

For example, if the host is using a BASH shell, go to the user's home directory (`$HOME`) and add the following to the `~/.bashrc` file to set the TZ variable:

```
TZ=PST8PDT; export TZ
```

If the host is using a CSH shell, go to `$HOME` and add the following to the `~/.cshrc` file:

```
setenv TZ PST8PDT
```

Now, execute the following command from the OMS home to verify if the SSH server can access the TZ variable.

```
ssh -l <user_name> -n <node_name> 'echo $TZ'
```

> **Note:** If `sshd` is not set up on remote box for `TZ`, you can pass this variable in the Additional Parameters text box using the `-z` option for default software source location (for install or upgrade) and the `s_timezone=<timezone>` option for a nondefault software location.
>
> Note that this will perform the installation of agents on all remote nodes with the same timezone value that you specify in the Additional Parameters text box. See Appendix H, "Additional Parameters for Agent Deploy Application" for more information.

### G.2.5 Dropping SSH Connection

For dropping SSH connection for 10.2.0.1 and 10.2.0.2 release, do the following on the Oracle Management Service machine:

1. For UNIX operating systems, remove the $HOME/.ssh folder (use the rm -rf $HOME/.ssh command). In the 10.2.0.1 release, $HOME is the home directory of the user who runs sshConnectivity.sh/sshUserSetup.sh.

2. For Windows operating systems, in the cygwin bash prompt, go to $HOME folder (use the cd $HOME command).

   > **Note:** If $HOME value has spaces, for example, C:\Documents and Settings\foo\, make sure that you type the value of $HOME in double-quotes. For example:
   >
   > ```
   > cd "C:\Documents and Settings\foo"
   > ```

3. Remove the .ssh folder as follows:

   ```
   rm -rf .ssh
   ```

4. Navigate to C:\cygwin, which is the default folder where agentpush assumes you installed cygwin. If cygwin is installed in folder X, go to folder X. Remove the .ssh folder.

   > **Note:** The sub-key value of ' SOFTWARE->Cygnus Solutions->Cygwin -> mounts v2->/' is the installation directory of cygwin, by default. If you have changed it manually, go to that folder and remove the .ssh folder.

For Enterprise Manager 10.2.0.3.0 or higher, SSH is setup and dropped by the application itself. Dropping the SSH setup will bring back the previous existing setup, if any.

If SSH was set up by the user, by running sshConnectivity.sh and the application has used this existing setup, the user will need to follow the steps explained above for dropping SSH connection for 10.2.0.1 and 10.2.0.2 release. Dropping the SSH setup will not bring back any existing SSH setup.

### G.2.6 Checking if SSH Connection is Removed

To check if SSH connection is removed, do the following:

1. Run the following command on the Oracle Management Service machine:

   ```
   ssh -l username <remote node> date
   sshConnectivity.sh/sshUserSetup.sh/sshUserSetupNT.sh
   ```

   where username is the value of the -user option used while running and remote node is one of the nodes used in the -hosts argument while running. For example:

   ```
   sshConnectivity.sh/sshUserSetup.sh/sshUserSetupNT.sh
   This command should NOT show date output. This command must stop for password
   conformation to proceed.
   For Example:
   $ssh -l john mybox.mydomain.com 'date'
   The authenticity of host 'mybox.mydomain.com (111.222.333.444)' can't be
   established.
   RSA key fingerprint is ec:52:5d:63:bc:85:07:ef:fe:5b:74:d3:6b:18:04:1c.
   Are you sure you want to continue connecting (yes/no)?
   ```

The above message ensures that the SSH connection is dropped from the Oracle Management Service to the remote node.

## G.3 Validate All Command Locations

The properties files located at `<omshome>/sysman/prov/resources/` comprises the default locations of commands that are required for successful execution of certain application programming interfaces (APIs), for example, the `ping` executable.

Such command locations can vary between machines and platforms. Run the `Validatepaths` script to verify whether the command locations in the properties file are correct. This script provides a list of commands that are not found in the default locations.

Run the following command to execute this script:

```
./validatePaths -dirloc oms/sysman/prov/resources/
In the preceding example (of the ping executable), if the executable is present in
/usr/sbin/ping, which is not the default location, you must specify this value in
the userpaths.properties file by specifying PING_PATH=/usr/sbin/ping.
```

The properties files that are loaded by the Agent Deploy application are the following:

- *platforminfo.properties*

  Contains a list of files that need to be loaded for each platform. These files specify the paths for the commands. For example, `/bin/ping`.

  - `Paths.properties`

    This file contains the arguments that need to be passed everytime the commands listed in this file are executed.

  - `sPaths.properties`

    This is a generic file that contains the paths for all commands that need to be executed, regardless of the platform.

  - `ssPaths_<platform>.properties`

    This is a platform-specific file and contains the commands that need to be executed for that platform. For example, `ssPaths_sol.properties`.

    **Caution:** On Microsoft Windows platforms, the path to the `cygwin` binaries is hardcoded in the `ssPaths_msplats.properties` file. If you install `cygwin` at a location other than `c:\cygwin` (default location), it can cause the agent installation to fail.

    To work around this issue, you must either install `cygwin` in the default directory (`c:\cygwin`), or update this properties file with the correct path to the `cygwin` binaries.

    You can look into the following remote registry key to find out the correct Cygwin path:

    ```
    HKEY_LOCAL_MACHINE\SOFTWARE\Cygnus Solutions\Cygwin\mounts v2\/
    ```

  - `userPaths.properties`

    This file lists all the variables that are used to specify the command paths. You must uncomment the variables that you want to use, and specify appropriate values.

**Caution:** The files that comprise each properties file are loaded in the ascending order of their precedence. This means that values you specify in the last file that is loaded will override the values for the same property in the previous files.

For example, the `platforminfo.properties` file comprises `paths.properties`, `spaths.properties`, `ssPaths.properties`, and `userPaths.properties`.

If the default location for the ping executable in `sPaths.properties` file is `usr/bin/ping`, and you specified an alternative location in the ssPaths.properties file as `usr/sbin/ping`, the value in the latter file takes precedence over the others.

**Note:** If you want to include other command variables, you can either choose to specify these variables in any of these `s*Paths.properties/userPaths.properties` files, or create another properties file and specify its name in `platforminfo.properties`.

Ensure these files are part of the `platforminfo.properties` file. If they are not, Agent Deploy ignores the paths to the executables that you have specified in these files and attempts to run the executables from their default locations.

Sample property files are provided at the end of this appendix under Sample Properties Files.

- `system.properties`

  This file contains properties that help you control the activity and performance of the application. For example:

  - `oracle.system.prov.threadpoolsize`

    Number of threads that get created in the application and work in parallel to execute commands on remote hosts. The default threadpool size value that is set for Agent Deploy is 32. You can specify an appropriate value for the threadpool size in this property.

    For example `oracle.sysman.prov.threadpoolsize=128`.

  - `oracle.sysman.prov.threadpoolmaxsize`

    Number of threads that can increase dynamically depending on the workload.

    The default value used in the application is 256 (`oracle.sysman.prov.threadpoolmaxsize=256`). You can specify an appropriate maximum value for the threadpool size in this property.

- `ignoreMessages.txt`

  If there are error messages displayed in the error stream that you know can be ignored in the setup, you can update these messages in the `ignoreMessages.txt` file.

  Generally, if the error stream contains data when you execute any command, it is assumed that the command failed. But the data in the error stream may not always correspond to the error. So, to ignore such error messages, you must add these messages (including the banner) to the `ignoreMessages.txt` file.

```
Consider the following example:
When you run /usr.local/bin/sudo on a remote machine, it writes the following
messages on to the error stream:
Administrator. It usually boils down to these two things:
#1) Respect the privacy of others.
#2) Think before you type.

Password:
This essentially, is just a warning to the user and does not constitute the
failure of the executed command.
Such error messages can be added to the ignore_Message.txt file.
```

> **Note:** The data format for these files mandates only one property per line. You must specify the property values in the format: `variable=value`.

### G.3.1 Location of Properties File

You can view the following properties files at `<OMS_HOME>/sysman/prov/resources/`:

- platformInfo.properties
- Paths.properties
- sPaths.properties
- ssPaths_sol.properties
- userPaths.properties
- system.properties
- ignoreMessages.txt

### G.3.2 Location of Installation Logs

See Appendix B, "Installation and Configuration Log Files" for more information on the various installation and configuration logs that are created, and their locations.

## G.4 Verify User Credentials

Ensure the user installing the agent is the same as the user that has installed Oracle Application Server and/or Oracle Collaboration Suite. You must also ensure the user has `SUDO` privileges that are required to execute the `root.sh` script (UNIX platforms only).

You can either select **Run Root.sh** in Agent Deploy that will execute the `root.sh` script (on UNIX platforms only) automatically at the end of the installation, or choose not to select this option, but run this script manually at the end of the installation.

This script must be run after the installation is complete in order to discover all the targets.

**Note:** Agent Deploy application uses `sudo` to run the `root.sh` script. You must specify the *invoking user's password* here. If `/etc/sudoers` is configured in such a way that `sudo` never prompts for a password, then a directory with the host password as the title gets created in the invoking users home directory. To avoid this, ensure that you configure /etc/sudoers file such that running a command using sudo always prompt for a password.

## G.5 Prerequisite Checks Executed by Agent Deploy

The Agent Deploy application runs a local prerequisite check (on the machine running the Management Service) and remote prerequisite checks on all the remote hosts before proceeding with the installation process.

**WARNING: Do not attempt to view the prerequisite check status while the prerequisite checks are still in progress. If you do so while the checks are still in progress, the application will display an error.**

### G.5.1 Prerequisite Checks Executed on the Local Host

Table G–2 lists the connectivity prerequisite checks that are run on the local (Oracle Management Service) host.

*Table G–2 Connectivity Prerequisite Check*

| Check if | Description |
|---|---|
| Nodes are active | Verifies if the remote nodes are accessible. |
| SSH Server is up | Verifies if there is an SSH Server Daemon running on all remote hosts, since the installation process will require SSH. |
| SSH is set | Verifies if the user name specified in the installation details page has the SSH on all the remote hosts. |
| Installation directory is writable on the remote hosts | Verifies if the installation base directory that you have specified is writable. |

### G.5.2 Prerequisite Checks Executed on Remote Hosts

Table G–3 lists the prerequisite checks that are executed by Agent Deploy for each installation type.

*Table G–3 Prerequisite Checks for a New Installation of Management Agent*

| Prerequisite Check for | Description | New Installation | Shared Agent Installation | Upgrade |
|---|---|---|---|---|
| Certified Versions | Checks if the operating system on remote hosts is certified. | Yes | Yes | Yes |
| Packages | Checks if the minimum required packages are available on remote hosts | Yes | No | Yes |
| Disk Space | Checks if the minimum required disk space is available. | Yes | No | Yes |

*Table G–3 (Cont.) Prerequisite Checks for a New Installation of Management Agent*

| Prerequisite Check for | Description | New Installation | Shared Agent Installation | Upgrade |
|---|---|---|---|---|
| Agent Targets | Checks for targets on remote hosts that cannot be monitored by the agent.<br>Targets that have been installed by another user cannot be monitored by the agent that you are going to install. | Yes | Yes | Yes |
| Oracle Home Location | Verifies if the specified Oracle home (`<install_base_dir/agent10g>`) is empty. | Yes | Yes | Yes |
| Existing Agent Installations | Checks for any existing agent installations on the remote hosts. | Yes | No | No |
| Write Permissions for Base Directory | Checks if the installation base directory on all remote hosts have write permissions. | Yes | No | No |
| Inventory Check | Checks if the user credentials that you have specified have write permissions on the central inventory of each remote host. | Yes | Yes | Yes |
| Upgrade Agent Existence Check | Determines the existence of an agent (10.1) that can be upgraded on the remote hosts. | No | No | Yes |
| Write Permissions for Upgrade Agent | Checks if the installation base directory on all remote hosts have write permissions. | No | No | Yes |
| NFS Agent Existence Check | Checks for any existing agent installations on the remote hosts. | No | Yes | No |
| Write Permissions for NFS Agent | Checks if the installation base directory, `EMSTATE` directory, and the NFS location are writable from all the remote hosts. | No | Yes | No |
| Time Zone ENV Check (UNIX Only) | Checks if the Timezone (TZ) environmental variable is set on the remote hosts. | Yes | Yes | Yes |

*Table G–3 (Cont.) Prerequisite Checks for a New Installation of Management Agent*

| Prerequisite Check for | Description | New Installation | Shared Agent Installation | Upgrade |
|---|---|---|---|---|
| Software Existence Check | Ensures the alternative software that you have specified is valid.<br>Note: This check is executed only if you have selected a nondefault (Another Location) software location for the agent installation. | Yes | | |

### G.5.3 Skipping Prerequisite Checks

You can choose to skip the prerequisite check that is run by the Agent Deploy application. To do so, follow these steps:

1. Navigate to the <OMSHOME>/sysman/prov/agentpush directory.
2. Open the `agentpush.properties` file.
3. Change the value of `oracle.sysman.prov.agentpush.step2` to "false", that is `oracle.sysman.prov.agentpush.step2=false`.

> **Note:** On Microsoft Windows, do not open the `agentpush.properties` file using Microsoft Word software. Open it using other text editors such as VIM or Notepad.

## G.6 Troubleshooting Failed Prerequisite Checks

This section details the possible errors that you may encounter when the prerequisite checks are executed, and the appropriate user actions to be taken to resolve the errors.

### G.6.1 Prerequisite Check Errors and Resolutions on Local Host

Table G–4 lists the most common reasons for prerequisite check failures, and the corresponding user actions to be performed to resolve them.

*Table G–4 Prerequisite Check Errors and Resolutions on Local Host*

| Prerequisite Check | Reason for Failure | User Action[1] |
|---|---|---|
| Nodes are active | Nodes are not accessible. | ■ Ensure all the nodes are active.<br>■ Remove the nodes that are not accessible from the nodes list. |

*Table G–4 (Cont.) Prerequisite Check Errors and Resolutions on Local Host*

| Prerequisite Check | Reason for Failure | User Action[1] |
|---|---|---|
| SSH Server is up | SSH daemon on one or more nodes is not up. | ■ Try to start the SSH daemon on the failed nodes.<br>■ Remove the failed nodes from the node list. |
| SSH is set | SSH is not set up from the local host to the failed nodes for the specified user credentials. | ■ Set up the SSH for the specified user credentials between the Management Service and remote hosts using the `sshUserSetup.sh` script. See Section G.2, "SSH (Secure Shell) Setup" for more information.<br>■ Remove the failed nodes from the nodes list. |
| Installation directory is writable on the remote hosts | Installation base directory that you have specified is not writable, or cannot be created on the failed nodes. | ■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host:<br>`[ssh -l <user> <host> "chmod +w -R <dir>"]`<br>■ Remove failed nodes from the nodes list. |

[1] Where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

## G.6.2 Prerequisite Check Errors and Resolutions on Remote Hosts

Table G–5 lists the most common reasons for prerequisite check failures on remote hosts, and the corresponding user actions to be performed to resolve them.

*Table G–5 Reasons for Prerequisite Check Failure and Corresponding User Actions*

| Prerequisite Check | Reason for Failure | User Action[1] |
|---|---|---|
| Certified Versions | The failed host may have an operating system or version that is not certified to deploy the agent on that machine. | ■ Exit the current installation and retry the agent installation without the failed hosts.<br>■ Upgrade the failed node to an operating system or version that is certified before proceeding with the installation. |
| Packages | The failed hosts may not comprise the recommended minimum packages required to deploy the agent. | Click **Fix and Retry** in the Prorate Details page. Agent Deploy performs an automatic packages fix using YUM or RPMs. During the process, it returns to the Installation Details page and prompts you to specify valid or alternative values where required, and then reruns the prerequisite checks. |
| Disk Space | This check may fail if the required minimum disk space for the installation is not found on the remote hosts. | ■ Increase the disk space on the failed hosts.<br>■ Remove the failed nodes from the nodes list. |
| Agent Targets | The failed nodes may have some targets that were installed by a different user, and hence cannot be monitored by the agent. | ■ Remove the targets that cannot be monitored from the failed hosts.<br>■ Continue with the installation because the failure message is only a warning (though not recommended). |
| Port | ■ The specified port is not valid, or is not available.<br>■ You have not specified any port and there is no available port in the default range. | ■ Ensure the specified port is not blocked on the failed hosts.<br>■ In the Installation Details page, leave the Port value blank.<br>■ If the default ports are either blocked or not available, remove the failed nodes from the nodes list. |

*Table G–5 (Cont.) Reasons for Prerequisite Check Failure and Corresponding User*

| Prerequisite Check | Reason for Failure | User Action[1] |
|---|---|---|
| Oracle Home Location | The `<install_base_dir>/agent10g` already exists and is not empty. | ■ Clean up the `<install_base_dir>/agent10g` directory.<br>■ Specify an alternative installation base directory.<br>■ Remove the failed nodes from the nodes list. |
| Existing Agent Installations | An agent already exists on the failed remote hosts that is registered with the central inventory. | ■ Uninstall the existing agent and retry the prerequisite checks.<br>■ Continue with the installation because the failure message is only a warning (though not recommended). |
| Write Permissions for Base Directory | The installation base directory is not writable. | ■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host:<br>`[ssh -l <user> <host> "chmod +w -R <dir>"]`<br>■ Remove failed nodes from the nodes list. |
| Inventory Check | The specified user credential does not have write permissions on the central inventory. | Change the central inventory permission settings to render the central inventory and its subdirectories writable. Complete the following steps to resolve this issue:<br>**1.** Log in to the local host (machine running the Oracle Management Service).<br>**2.** Change the directory to:<br>`<HOME>/sysman/prov/agentpush/resources/fixup`<br>**3.** For each failed host, run the following script:<br>`./fixOraInvPermissions.sh <install user> <install group> <failed host name> <inventory location>.`<br>As this script must be run as `root` (using `sudo`) on the failed remote host, you are prompted to specify the `sudo` password. |
| Upgrade Agent Existence Check | A Management Agent release 10.1 is not present in the remote hosts on which you want to perform the agent upgrade. | Exit the upgrade process. |
| Write Permissions for Upgrade Agent | The installation base directory is not writable. | ■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host:<br>`[ssh -l <user> <host> "chmod +w -R <dir>"]`<br>■ Remove failed nodes from the nodes list. |
| NFS Agent Existence Check | An agent already exists on the remote hosts that is registered with the central inventory. | ■ Uninstall the existing agent and retry the prerequisite checks.<br>■ Continue with the installation since the failure message is only a warning (though not recommended). |

*Table G–5 (Cont.) Reasons for Prerequisite Check Failure and Corresponding User*

| Prerequisite Check | Reason for Failure | User Action[1] |
|---|---|---|
| Write Permissions 'for NFS Agent | ■ The installation base directory is not writable.<br>■ The NFS location is not accessible.<br>■ The `EMSTATE` directory is not writable. | ■ Include write permissions on the failed nodes by executing the following command on the failed hosts from the local (OMS) host:<br>`[ssh -l <user> <host> "chmod +w -R <dir>"]`<br>■ Remove failed nodes from the nodes list. |
| Time Zone ENV Check | The TZ environment variable is not set on the remote hosts. | Recommended<br>■ Specify the time zone in the Additional Parameters section (using the -z option) of the Installation Details page.<br>Optional<br>■ Set the TZ environment variable. Shut down and restart SSH on all remote hosts.<br>■ Update with the TZ environment variable on all remote hosts. |
| Software Existence Check | The alternative software location that you have specified is not valid. | ■ Revert to the default software source location.<br>■ Change the alternative software location to a valid location (having `./stage/product.xml`). |

[1] Where there are multiple user actions listed, you can choose to perform the action that is most appropriate.

## G.7 Commands and Arguments Executed to Run Agent Deploy Plugins

The Agent Deploy application makes use of plugins to perform certain functions (for example, collect installation logs from targets). These plugins execute certain commands from the local (OMS) node (for example, `mkdir`, `scp`, and `unzip`), while others are executed from the remote nodes (for example, `zip`).

Table G–6 provides a list of commands that are executed on local and remote nodes.

*Table G–6 Commands Executed on Local (OMS) and Remote Nodes*

| Commands Executed on Local Node (OMS) | Commands Executed on Remote Nodes |
|---|---|
| PING_PATH | RSH_PATH |
| SH_PATH | SSH_PATH |
| SHELL_PATH | RCP_PATH |
| SHELL_ARGS | SCP_PATH |
| TAR_PATH | SSH_ARGS |
| TAR_EXTRACT_ARGS | SCP_ARGS |
| TAR_MTIME_ARGS | RCP_ARGS |
| MKDIR | UNZIP_PATH |
| | UNZIP_ARGS |

## G.8 Sample Properties Files

A sample of each property file in the `platforminfo.properties` file is provided as follows:

### platforminfo.properties

Contains the mapping between platform ID and the files to be loaded for that platform.

```
# Copyright (c) 2005, Oracle. All rights reserved.

#unix
-1=Paths.properties,sPaths.properties,userPaths.properties
#linux x86
46=Paths.properties,sPaths.properties,userPaths.properties
#solaris sparc
453=Paths.properties,sPaths.properties,ssPaths_sol.properties,userPaths.properties
#ms_plats
-3=Paths.properties,ssPaths_msplats.properties
#windows nt
912=Paths.properties,ssPaths_msplats.properties
#HP-UIX
2=Paths.properties,sPaths.properties,ssPaths_hpuix.properties,userPaths.properties
#AIX
610=Paths.properties,sPaths.properties,ssPaths_aix.properties,userPaths.properties
```

### Paths.properties

This is a generic file.

```
# Copyright (c) 2005, 2006, Oracle. All rights reserved.

SSH_ARGS=-o FallBackToRsh=no  -o PasswordAuthentication=no  -o
StrictHostKeyChecking=yes
SCP_ARGS=-p -o FallBackToRsh=no  -o PasswordAuthentication=no  -o
StrictHostKeyChecking=yes
UNZIP_ARGS=-o
ZIP_ARGS=-r
ZIP_EXCLUDE_ARGS=-x
ZIP_INCLUDE_ARGS=-i
```

### sPaths.properties

This is a UNIX-specific file.

```
# Copyright (c) 2006, Oracle. All rights reserved.

TRUE=/bin/true
SSH_PATH=/usr/bin/ssh
SCP_PATH=/usr/bin/scp
RSH_PATH=/usr/bin/rsh
RCP_PATH=/usr/bin/rcp
RCP_ARGS=-p
SH_PATH=/bin/sh
SH_ARGS=-c
KSH_PATH=/usr/bin/ksh
PING_ARGS=-c 1 -w
PING_PATH=/bin/ping
ZIP_PATH=/usr/bin/zip
UNZIP_PATH=/usr/bin/unzip
TAR_PATH=/bin/tar
TAR_CREATE_ARGS=cvf
TAR_EXTRACT_ARGS=xvfm
TAR_EXCLUDE_ARGS=-X
TAR_INCLUDE_ARGS=-T
TAR_MTIME_ARGS=-m
CAT_PATH=/bin/cat
```

```
CP_PATH=/bin/cp
CP_ARGS=-p
MV_PATH=/bin/mv
MV_ARGS=-f
MKDIR_PATH=/bin/mkdir
MKDIR_ARGS=-p
RMDIR_PATH=/bin/rmdir
RMDIR_PARENTS_ARGS=-p
RMDIR_ARGS=--ignore-fail-on-non-empty
RM_PATH=/bin/rm
RM_F_ARGS=-f
RM_RF_ARGS=-rf
LN_PATH=/bin/ln
LN_ARGS=-fs
XARGS_PATH=/usr/bin/xargs
LS_PATH=/bin/ls
LS_ARGS=-A
CHMOD_PATH=/bin/chmod
CHOWN_PATH=/bin/chown
DF_PATH=/bin/df
DF_ARGS=-k
DF_COL_NAME=Available
SUDO_PATH=/usr/local/bin/sudo
SUDO_K_ARGS=-K
SUDO_S_ARGS=-S
TOUCH_PATH=/bin/touch
HOSTNAME_PATH=/bin/hostname
HOSTNAME_ARGS=-f
DATE_PATH=/bin/date
DATE_ARGS=+%s
SSH_KEYGEN_PATH=/usr/bin/ssh-keygen
SSH_KEYGEN_ARGS=-t rsa
SSH_KEYGEN_ARGS_KEYFILE=-f
SSH_KEYGEN_ARGS_PASSPHRASE=-N
SSH_HOST_KEY_LOC=/etc/ssh
PATH_EXISTS_FLAG=-e
FILE_EXISTS_FLAG=-f
DIR_EXISTS_FLAG=-d
DIR_WRITABLE_FLAG=-w
SLINK_EXISTS_FLAG=-h
SCRATCHPATH=/tmp

#{0} REMOTESHELL
#{1} NODE
#{2} LOGINSHELL
#{3} CMD

#KEY0=$REMOTESHELL $NODE $LOGINSHELL '$CMD;echo :EXITCODE:$? '
KEY0={0} {1} {2} ''{3};echo :EXITCODE:$? ''
#KEY1=$REMOTESHELL $NODE $LOGINSHELL '$CMD'
KEY1={0} {1} {2} ''{3}''
#KEY2=$LOGINSHELL '$CMD'
KEY2={2} ''{3}''
#KEY3=$REMOTESHELL $NODE $CMD
KEY3={0} {1} {3}
#KEY4=$LOGINSHELL '$CMD NODE'
KEY4={2} ''{3} {1}''


#{0} REMOTESHELLPATH
```

```
#{1} REMOTESHELLARGS
#{2} NODE
#{3} LOGINSHELLPATH
#{4} LOGINSHELLARGS
#{5} CMD

#KEY10=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#''$C
MD;echo :EXITCODE:$?''
KEY10={0}#{1}#{2}#{3}#{4}#''{5};echo :EXITCODE:$?''

#KEY11=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#''$C
MD''
KEY11={0}#{1}#{2}#{3}#{4}#''{5}''

#KEY12=$LOGINSHELLPATH#$LOGINSHELLARGS#''$CMD''
KEY12={3}#{4}#''{5}''

#KEY13=$REMOTESHELLPATH#$REMOTESHELLARGS#$NODE#$CMD
KEY13={0}#{1}#{2}#{5}

#KEY15=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$LOGINSHELLPATH#$LOGINSHELLARGS#$CMD
KEY15={0}#{1}#{2}#{3}#{4}#{5}

#{0} ENV
#{1} PATH
#{2} ARGS
#{3} LOGINSHELL
#{4} FLAGS

#CMD0=$PATH $ARGS
CMD0={1} {2}

#CMD1=$ENV $PATH $ARGS
CMD1={0} {1} {2}

#CMD2=if [[ $FLAGS $PATH ]] ; then exit 0; else exit 1; fi
CMD2=if [[ {4} {1} ]] ; then exit 0; else exit 1; fi

#CMD3=if [[ $FLAGS $PATH ]] ; then echo :EXITCODE:0; else echo :EXITCODE:1; fi
CMD3=if [[ {4} {1} ]] ; then echo :EXITCODE:0; else echo :EXITCODE:1; fi

#CMD4=$PATH $ARGS $LOGINSHELL '$ENV $PATH $ARGS'
CMD4={0} {1} {2} ''{3} {4} {5}''

#CMD5=$PATH $ARGS $LOGINSHELL '$ENV $PATH $ARGS'
CMD5={0} {1} {2} ''{3} {4} {5};echo :EXITCODE:$?''

#CMD2=$CMD1 && $CMD1
#CMD2={0} {1} {2}
#CMD3=$CMD1 $LOGINSHELL $CMD1
#CMD6=( $CMD1 && $CMD1 )
#CMD7= $CMD1 | $CMD1
```

### ssPaths_sol.properties (Solaris-specific file)

```
# Copyright (c) 2005, Oracle. All rights reserved.

SH_PATH=/bin/bash
SH_ARGS=-c
KSH_PATH=/usr/bin/ksh
RMDIR_ARGS=
#the date should be in the format of year:month:date:hour:minute:second
DATE_ARGS=-u +%y:%m:%d:%H:%M:%S
PING_PATH=/usr/sbin/ping
PING_ARGS=
SSH_PATH=/usr/local/bin/ssh
SSH_KEYGEN_PATH=/usr/local/bin/ssh-keygen
SCP_PATH=/usr/local/bin/scp
TAR_EXCLUDE_ARGS=X
TAR_INCLUDE_ARGS=-I
DF_COL_NAME=avail
SSH_HOST_KEY_LOC=/usr/local/etc
```

### ssPaths_msplats.properties (Microsoft Windows-specific file)

```
# Copyright (c) 2005, 2006, Oracle. All rights reserved.

FALSE=C:/cygwin/bin/false.exe
#SSH_PATH=C:\\Program Files\\OpenSSH\\bin\\ssh.exe
#SCP_PATH=C:\\Program Files\\OpenSSH\\bin\\scp.exe
SSH_PATH=C:/cygwin/bin/ssh.exe
SCP_PATH=C:/cygwin/bin/scp.exe
PING_ARGS=-n 5 -w
PING_PATH=C:\\WINDOWS\\system32\\ping.exe
LS_PATH=C:/cygwin/bin/ls.exe
LS_ARGS=-A
MKDIR_PATH=C:/cygwin/bin/mkdir.exe
MKDIR_ARGS=-p
ZIP_PATH=C:/cygwin/bin/zip.exe
UNZIP_PATH=C:/cygwin/bin/unzip.exe
DATE_PATH=cmd.exe /c date
DATE_ARGS=/T
TIME_PATH=cmd.exe /c time
TIME_ARGS=/T
TOUCH_PATH=C:/cygwin/bin/touch.exe
HOSTNAME_PATH=C:/WINDOWS/system32/hostname.exe
MV_PATH=cmd.exe /c move
MV_ARGS=/Y
#MV_PATH=C:/cygwin/bin/mv.exe
#MV_ARGS=
SH_PATH=
SH_ARGS=
RMDIR_PATH=cmd.exe /c rmdir
#RM_PATH=C:/cygwin/bin/rm.exe
#RM_F_ARGS=-f
#RM_RF_ARGS=-rf
RM_PATH=cmd.exe /c del
RM_F_ARGS=/F /Q
RM_RF_ARGS=/S /Q
RM_ERR1=Could not find
CHMOD_PATH=C:/cygwin/bin/chmod.exe
CHOWN_PATH=C:/cygwin/bin/chown.exe
CP_PATH=cmd.exe /c copy
CP_ARGS=/Y
PATH_EXISTS_FLAG=-e
FILE_EXISTS_FLAG=-f
DIR_EXISTS_FLAG=-d
DIR_WRITABLE_FLAG=-w
SCRATCHPATH=C:/tmp
MORE_PATH=cmd.exe /c more
SHELL_PATH=C:/cygwin/bin/sh.exe
SHELL_ARGS=-c
```

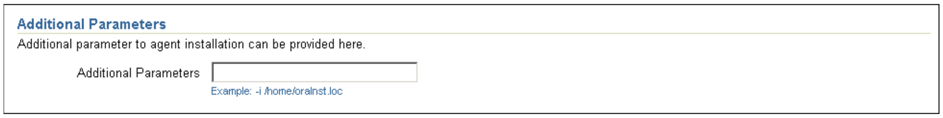
```
CMD_PATH=C:/WINDOWS/system32/cmd.exe
CMD_ARGS=/c
SSH_HOST_KEY_LOC=C:/Program Files/OpenSSH/etc

#{0} REMOTESHELLPATH
#{1} REMOTESHELLARGS
#{2} NODE
#{3} LOGINSHELLPATH
#{4} LOGINSHELLARGS
#{5} CMD

#KEY1=$REMOTESHELLPATH#$REMOTESHELLARGS#NODE#$CMD
#KEY1={0}#{1}#{2}#\"{5}\"
KEY11={0}#{1}#{2}#{5}

#{0} ENV
#{1} PATH
#{2} ARGS
#{3} LOGINSHELL
#{4} FLAGS

#CMD2=if [ $FLAGS $PATH ] ; then exit 0; else exit 1; fi
CMD2=if [ {4} {1} ] ; then exit 0; else exit 1; fi
```

H

# Additional Parameters for Agent Deploy Application

The additional parameters that you specify during the agent installation using the Agent Deploy application depend on the software source location that you have selected.

*Figure H–1 Additional Parameters Section of the Installation Details Page*



Additional Parameters

Additional parameter to agent installation can be provided here.

Additional Parameters

Example: -i /home/oralnst.loc

If you select the default source software location, you must specify additional parameters that are supported by the `agentDownLoad` script. See Table H–1 for a list of parameters supported by this script.

If you select an alternative location, you must specify additional parameters that are supported by Oracle Universal Installer (OUI). See Table H–2 for a list of parameters supported by OUI.

Also, if you cloning a Management Agent using the Agent Clone Wizard, you must specify additional parameters that are supported by OUI. See Table H–2 for a list parameters supported by OUI.

> **Note:** If the same parameters that you specify here are also specified independently (from the command-line option), the value of the parameters that you specify here take precedence over the other.
>
> For example, if the installation base directory is specified independently, and `-b` option is specified here, the latter value (`-b`) is used in the installation.

## H.1 Additional Parameters Supported by agentDownload Script

Table H–1 lists the possible parameters that you can specify if you select the default (Management Service) location. If you are decide to specify more than one parameter, then separate them with a white space.

***Table H–1 Parameters Supported by agentDownload Script***

| Parameters | Description |
|---|---|
| -t | No value required. Do not start the agent after installation or upgrade. |
| -c | Cluster node list. Used during installation only. Nodes should be specified in double-quotation marks, separated by commas. For example, `-c "node1,node2,node3"` |
| -b | Installation base directory location. For example, -b `/home/OracleHomes/agent/` |
| -d | No value required. Do not initiate automatic target discovery. |
| -i | Inventory pointer location file. For example, `-i/etc/oraInst.loc` |
| -n | Cluster name. For example, `-n CLUSTER1` |
| -p | File location for static port for agent. For example, `-p /home/config/staticports.ini`<br>The template file for the `-p` option follows:<br>`# staticports.ini Template File`<br>`# This file is a template for specifying port numbers at installation time.`<br>`# To specify a port number, uncomment the appropriate line (remove #) and`<br>`# replace "port_num" with the desired port number.`<br>`# You can then launch Oracle Universal Installer with special options to use this file.`<br>`# Please refer to Enterprise Manager Grid Control 10gR2 Installation Guide for instructions.`<br>`# Enterprise Manager`<br>`#Enterprise Manager Central Agent Port=port_num` |
| -v | Inventory location. Instead of using the -i parameter to point to a file that has the inventory location details, you can use -v parameter to directly pass the inventory location. Therefore, this is an alternative to -i. |
| -z | Timezone environment variable value (`-z <timezone>`). For example, `-z PST8PDT`. |

**Note:** Use the -z option to specify the time zone, but the Agent Deploy application discovers a TZ environment variable already set on the remote host, this TZ value will take precedence over the -z value that you specify.

You can verify if the TZ environment variable has been set on the remote host by executing the following command:

```
ssh -l <user_name> -n <remote_node> 'echo $TZ'
```

The <user name> argument is the ID that you are using for the agent installation, and <remote host> is the host on which you want to install the agent.

If you are installing the agent from a nondefault software location, you must specify the timezone environment variable using the following command:

```
s_timeZone=<timezone>
For example, s_timezone=PST8PDT
```

## H.2 Additional Parameters Supported by Oracle Universal Installer

Table H–2 lists the possible parameters that you can specify if you select an alternative software source (nondefault) location. If you are decide to specify more than one parameter, then separate them with a white space.

*Table H–2 Parameters Supported by Oracle Universal Installer*

| Parameter | Description |
|---|---|
| -clusterware oracle.crs, <crs version> | Version of the installed Oracle Clusterware. |
| -crslocation <path> | For cluster installs, specifies the path to the CRS home location. Specifying this overrides CRS information obtained from the central inventory. |
| -invPtrLoc <full path of oraInst.loc> | Linux only. To point to a different inventory location. The orainst.loc file contains:<br>inventory_loc=<location of central inventory><br>inst_group=<group of the user that is installing the agent> |
| INVENTORY_LOCATION <location> | Inventory location. Instead of using the -invPtrLoc parameter to point to a file that has the inventory location details, you can use INVENTORY_LOCATION parameter to directly pass the inventory location. Therefore, this is an alternative to -invPtrLoc. |
| -jreLoc <location> | Path where the Java Runtime Environment is installed. OUI cannot be run without this. |
| -logLevel <level> | Filter log messages that have a lesser priority level than <level>. Valid options are: severe, warning, info, config, fine, finer, finest, basic, general, detailed, trace. The use of basic, general, detailed, and trace is deprecated. |
| -paramFile <location of file> | Location of oraparam.ini file to be used by Oracle Universal Installer. |
| -responseFile <Path> | Response file and path to use. |

*Table H–2 (Cont.) Parameters Supported by Oracle Universal Installer*

| Parameter | Description |
|---|---|
| -sourceLoc <location of products.xml> | Software source location. |
| -cfs | Oracle home specified is on the cluster file system (shared). This is mandatory when '-local' is specified so that Oracle Universal Installer can register the home appropriately into the inventory. |
| -debug | Get debug information from OUI. |
| -executeSysPrereqs | Execute system prerequisite checks and exits. |
| -force | Allow silent mode installation into a non-empty directory. |
| -help | Display the usage of all preceding options. |
| -ignoreSysPrereqs | Ignore the results of the system prerequisite checks. |
| -local | Perform the operation on the local node irrespective of the cluster nodes specified. |
| -printmemory | Log debug information for memory usage. |
| -printtime | Log debug information for time usage. |
| -updateNodeList | Update the node list for this home in the OUI inventory. |

# I

# Oracle Reserved Words

This appendix provides a complete list of Oracle reserved words.

## I.1 List of Oracle Reserved Words

In addition to the reserved words in Table I–1, Oracle also uses system-generated names beginning with *SYS_* for implicitly generated schema objects and subobjects. Oracle discourages you from using this prefix in the names you explicitly provide to your schema objects and subobjects to avoid possible conflicts in name resolution.

***Table I–1 List of Oracle Reserved Words***

| Oracle Reserved Words and Keywords | | |
|---|---|---|
| ACCESS | ACCOUNT | ACTIVATE |
| ADD | ADMIN | ADVISE |
| AFTER | ALL | ALL_ROWS |
| ALLOCATE | ALTER | ANALYZE |
| AND | ANY | ARCHIVE |
| ARCHIVELOG | ARRAY | AS |
| ASC | AT | AUDIT |
| AUTHENTICATED | AUTHORIZATION | AUTOEXTEND |
| AUTOMATIC | BACKUP | BECOME |
| BEFORE | BEGIN | BETWEEN |
| BFILE | BITMAP | BLOB |
| BLOCK | BODY | BY |
| CACHE | CACHE_INSTANCES | CANCEL |
| CASCADE | CAST | CFILE |
| CHAINED | CHANGE | CHAR |
| CHAR_CS | CHARACTER | CHECK |
| CHECKPOINT | CHOOSE | CHUNK |
| CLEAR | CLOB | CLONE |
| CLOSE | CLOSE_CACHED_OPEN_CURSORS | CLUSTER |
| COALESCE | COLUMN | COLUMNS |

*Table I–1 (Cont.) List of Oracle Reserved Words*

| Oracle Reserved Words and Keywords | | |
|---|---|---|
| COMMENT | COMMIT | COMMITTED |
| COMPATIBILITY | COMPILE | COMPLETE |
| COMPOSITE_LIMIT | COMPRESS | COMPUTE |
| CONNECT | CONNECT_TIME | CONSTRAINT |
| CONSTRAINTS | CONTENTS | CONTINUE |
| CONTROLFILE | CONVERT | COST |
| CPU_PER_CALL | CPU_PER_SESSION | CREATE |
| CURRENT | CURRENT_SCHEMA | CURREN_USER |
| CURSOR | CYCLE | |
| DANGLING | DATABASE | DATAFILE |
| DATAFILES | DATAOBJNO | DATE |
| DBA | DBHIGH | DBLOW |
| DBMAC | DEALLOCATE | DEBUG |
| DEC | DECIMAL | DECLARE |
| DEFAULT | DEFERRABLE | DEFERRED |
| DEGREE | DELETE | DEREF |
| DESC | DIRECTORY | DISABLE |
| DISCONNECT | DISMOUNT | DISTINCT |
| DISTRIBUTED | DML | DOUBLE |
| DROP | DUMP | EACH |
| ELSE | ENABLE | END |
| ENFORCE | ENTRY | ESCAPE |
| EXCEPT | EXCEPTIONS | EXCHANGE |
| EXCLUDING | EXCLUSIVE | EXECUTE |
| EXISTS | EXPIRE | EXPLAIN |
| EXTENT | EXTENTS | EXTERNALLY |
| FAILED_LOGIN_ATTEMPTS | FALSE | FAST |
| FILE | FIRST_ROWS | FLAGGER |
| FLOAT | FLOB | FLUSH |
| FOR | FORCE | FOREIGN |
| FREELIST | FREELISTS | FROM |
| FULL | FUNCTION | GLOBAL |
| GLOBALLY | GLOBAL_NAME | GRANT |
| GROUP | GROUPS | HASH |
| HASHKEYS | HAVING | HEADER |
| HEAP | IDENTIFIED | IDGENERATORS |

*Table I–1 (Cont.) List of Oracle Reserved Words*

| Oracle Reserved Words and Keywords | | |
|---|---|---|
| IDLE_TIME | IF | IMMEDIATE |
| IN | INCLUDING | INCREMENT |
| INDEX | INDEXED | INDEXES |
| INDICATOR | IND_PARTITION | INITIAL |
| INITIALLY | INITRANS | INSERT |
| INSTANCE | INSTANCES | INSTEAD |
| INT | INTEGER | INTERMEDIATE |
| INTERSECT | INTO | IS |
| ISOLATION | ISOLATION_LEVEL | KEEP |
| KEY | KILL | LABEL |
| LAYER | LESS | LEVEL |
| LIBRARY | LIKE | LIMIT |
| LINK | LIST | LOB |
| LOCAL | LOCK | LOCKED |
| LOG | LOGFILE | LOGGING |
| LOGICAL_READS_PER_CALL | LOGICAL_READS_PER_SESSION | LONG |
| MANAGE | MASTER | MAX |
| MAXARCHLOGS | MAXDATAFILES | MAXEXTENTS |
| MAXINSTANCES | MAXLOGFILES | MAXLOGHISTORY |
| MAXLOGMEMBERS | MAXSIZE | MAXTRANS |
| MAXVALUE | MIN | MEMBER |
| MINIMUM | MINEXTENTS | MINUS |
| MINVALUE | MLSLABEL | MLS_LABEL_FORMAT |
| MODE | MODIFY | MOUNT |
| MOVE | MTS_DISPATCHERS | MULTISET |
| NATIONAL | NCHAR | NCHAR_CS |
| NCLOB | NEEDED | NESTED |
| NETWORK | NEW | NEXT |
| NOARCHIVELOG | NOAUDIT | NOCACHE |
| NOCOMPRESS | NOCYCLE | NOFORCE |
| NOLOGGING | NOMAXVALUE | NOMINVALUE |
| NONE | NOORDER | NOOVERRIDE |
| NOPARALLEL | NOPARALLEL | NOREVERSE |
| NORMAL | NOSORT | NOT |
| NOTHING | NOWAIT | NULL |
| NUMBER | NUMERIC | NVARCHAR2 |

*Table I–1 (Cont.) List of Oracle Reserved Words*

| Oracle Reserved Words and Keywords | | |
|---|---|---|
| OBJECT | OBJNO | OBJNO_REUSE |
| OF | OFF | OFFLINE |
| OID | OIDINDEX | OLD |
| ON | ONLINE | ONLY |
| OPCODE | OPEN | OPTIMAL |
| OPTIMIZER_GOAL | OPTION | OR |
| ORDER | ORGANIZATION | OSLABEL |
| OVERFLOW | OWN | PACKAGE |
| PARALLEL | PARTITION | PASSWORD |
| PASSWORD_GRACE_TIME | PASSWORD_LIFE_TIME | PASSWORD_LOCK_TIME |
| PASSWORD_REUSE_MAX | PASSWORD_REUSE_TIME | PASSWORD_VERIFY_FUNCTION |
| PCTFREE | PCTINCREASE | PCTTHRESHOLD |
| PCTUSED | PCTVERSION | PERCENT |
| PERMANENT | PLAN | PLSQL_DEBUG |
| POST_TRANSACTION | PRECISION | PRESERVE |
| PRIMARY | PRIOR | PRIVATE |
| PRIVATE_SGA | PRIVILEGE | PRIVILEGES |
| PROCEDURE | PROFILE | PUBLIC |
| PURGE | QUEUE | QUOTA |
| RANGE | RAW | RBA |
| READ | READUP | REAL |
| REBUILD | RECOVER | RECOVERABLE |
| RECOVERY | REF | REFERENCES |
| REFERENCING | REFRESH | RENAME |
| REPLACE | RESET | RESETLOGS |
| RESIZE | RESOURCE | RESTRICTED |
| RETURN | RETURNING | REUSE |
| REVERSE | REVOKE | ROLE |
| ROLES | ROLLBACK | ROW |
| ROWID | ROWNUM | ROWS |
| RULE | SAMPLE | SAVEPOINT |
| SB4 | SCAN_INSTANCES | SCHEMA |
| SCN | SCOPE | SD_ALL |
| SD_INHIBIT | SD_SHOW | SEGMENT |
| SEG_BLOCK | SEG_FILE | SELECT |
| SEQUENCE | SERIALIZABLE | SESSION |

*Table I–1 (Cont.) List of Oracle Reserved Words*

| Oracle Reserved Words and Keywords | | |
|---|---|---|
| SESSION_CACHED_CURSORS | SESSIONS_PER_USER | SET |
| SHARE | SHARED | SHARED_POOL |
| SHRINK | SIZE | SKIP |
| SKIP_UNUSABLE_INDEXES | SMALLINT | SNAPSHOT |
| SOME | SORT | SPECIFICATION |
| SPLIT | SQL_TRACE | STANDBY |
| START | STATEMENT_ID | STATISTICS |
| STOP | STORAGE | STORE |
| STRUCTURE | SUCCESSFUL | SWITCH |
| SYS_OP_ENFORCE_NOT_NULL$ | SYS_OP_NTCIMG$ | SYNONYM |
| SYSDATE | SYSDBA | SYSOPER |
| SYSTEM | TABLE | TABLES |
| TABLESPACE | TABLESPACE_NO | TABNO |
| TEMPORARY | THAN | THE |
| THEN | THREAD | TIMESTAMP |
| TIME | TO | TOPLEVEL |
| TRACE | TRACING | TRANSACTION |
| TRANSITIONAL | TRIGGER | TRIGGERS |
| TRUE | TRUNCATE | TX |
| TYPE | UB2 | UBA |
| UID | UNARCHIVED | UNDO |
| UNION | UNIQUE | UNLIMITED |
| UNLOCK | UNRECOVERABLE | UNTIL |
| UNUSABLE | UNUSED | UPDATABLE |
| UPDATE | USAGE | USE |
| USER | USING | VALIDATE |
| VALIDATION | VALUE | VALUES |
| VARCHAR | VARCHAR2 | VARYING |
| VIEW | WHEN | WHENEVER |
| WHERE | WITH | WITHOUT |
| WORK | WRITE | WRITEDOWN |
| WRITEUP | XID | YEAR |
| ZONE | | |

# Index