Oracle® Enterprise Manager

Advanced Configuration

10*g* Release 1 (10.1)

Part No. B12013-03

August 2004

ORACLE®

Oracle Enterprise Manager Advanced Configuration, 10*g* Release 1 (10.1)

Part No. B12013-03

Primary Author: Peter LaQuerre

Contributor: Jerry Abramson, Murali Bhoopathy, Tina Boisvert, Yuen Chan, Gang Chen, Phil Choi, Sudip Datta, Erik DeMember, Nestor Dutko, Kondayya Duvvuri, Gary Gilchrist, Leslie Gloyd, Jackie Gosselin, Scott Grover, Nicole Haba, Ana Hernandez, Anita Holser, Narain Jagathesan, PJ (Eunhei Jang), Dana Joly, Vitaliy Khizder, Dennis Lee, Tania Le Voi, Conrad Lo, Jaydeep Marfatia, Lan Nguyen, Ravi Pinnamaneni, Dhaval Shah, Sridhar Reddy, Bert Rich, Mariliyn Roncati, Jonathan Stone, Anila Thomas, Venkat Tummalapalli, Steve Viavant, Jim Viscusi, Julie Wong

Contents

2 Starting and Stopping Enterprise Manager Components

3 Grid Control Common Configurations

4 Enterprise Manager Security

5 Configuring Enterprise Manager for Firewalls

6 Configuring Application Service Level Management

7 Locating and Configuring Enterprise Manager Log Files

8 Maintaining and Troubleshooting the Repository

9 Reconfiguring the Management Agent and Management Service

10 Migrating from Previous Versions of Enterprise Manager

11 Configuring Notifications

12 Additional Configuration Tasks

Index

Send Us Your Comments

Oracle Enterprise Manager Advanced Configuration, 10*g* Release 1 (10.1)

Part No. B12013-03

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, please indicate the title and part number of the documentation and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: nedc-doc_us@oracle.com
- FAX: (603) 897-3317. Attn: Oracle Enterprise Manager 10*g*
- Postal service:

  Oracle Corporation
  Oracle Enterprise Manager 10*g* Documentation
  1 Oracle Drive
  Nashua, NH 03062
  USA

If you would like a reply, please give your name, address, telephone number, and electronic mail address (optional).

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This guide describes advanced configuration tasks you can perform after you have installed Oracle Enterprise Manager and have started using the software. These tasks are optional and provide additional functionality for specific types of Oracle Enterprise Manager customers.

Intended Audience

This guide is written for system administrators who want to configure the advanced features of Oracle Enterprise Manager 10*g*. You should already be familiar with Oracle and the administrative tasks you want to perform.

You should also be familiar with the operation of your specific UNIX or Windows system. Refer to the documentation for your platform-specific documentation, if necessary.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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. 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 additional information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation JAWS, a Windows screen reader, 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, JAWS 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.

Related Documents

For more information about Oracle Enterprise Manager 10*g*, see the following resources:

- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Concepts*
- The Enterprise Manager online help, which is available by clicking the **Help** link at the top of any page in the Oracle Enterprise Manager 10*g* Grid Control Console.

Note: To obtain the latest Oracle Enterprise Manager 10*g* documentation, refer to the Enterprise Manager documentation page on the Oracle Technology Network (OTN):

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

Conventions

This section describes the conventions used in the text and code examples of this document. It describes:

- Conventions in Text
- Conventions in Code Examples

Conventions in Text

The following table describes conventions used in the body of the document.

Convention	Meaning	Example
Bold	Bold typeface indicates terms that are defined in the text or terms that appear in a glossary, or both.	When you specify this clause, you create an **index-organized table**.
Italics	Italic typeface indicates book titles or emphasis.	*Oracle Database Concepts* Ensure that the recovery catalog and target database do *not* reside on the same disk.
`UPPERCASE monospace (fixed-width font)`	Uppercase monospace typeface indicates elements supplied by the system. Such elements include parameters, privileges, datatypes, RMAN keywords, SQL keywords, SQL*Plus or utility commands, packages and methods, as well as system-supplied column names, database objects and structures, usernames, and roles.	You can specify this clause only for a `NUMBER` column. You can back up the database by using the `BACKUP` command. Query the `TABLE_NAME` column in the `USER_TABLES` data dictionary view. Use the `DBMS_STATS.GENERATE_STATS` procedure.

Convention	Meaning	Example
lowercase monospace (fixed-width font)	Lowercase monospace typeface indicates executables, filenames, 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, usernames and roles, program units, and parameter values. **Note:** Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.	Enter `sqlplus` to open SQL*Plus. The password is specified in the `orapwd` file. Back up the datafiles and control files in the `/disk1/oracle/dbs` directory. The `department_id`, `department_name`, and `location_id` columns are in the `hr.departments` table. Set the `QUERY_REWRITE_ENABLED` initialization parameter to `true`. Connect as `oe` user. The `JRepUtil` class implements these methods.
lowercase monospace (fixed-width font) italic	Lowercase monospace italic font represents placeholders or variables.	You can specify the *parallel_clause*. Run `U`*old_release*`.SQL` where *old_release* refers to the release you installed prior to upgrading.

Conventions in Code Examples

Code examples illustrate SQL, PL/SQL, SQL*Plus, or other command-line statements. They are displayed in a monospace (fixed-width) font and separated from normal text as shown in this example:

```
SELECT username FROM dba_users WHERE username = 'MIGRATE';
```

The following table describes typographic conventions used in code examples and provides examples of their use.

Convention	Meaning	Example
[ ]	Brackets enclose one or more optional items. Do not enter the brackets.	`DECIMAL (`*digits* `[ ,` *precision* `])`
< >	Angle brackets in command syntax denote an item for which you can substitute a real value. Do not enter the angle brackets.	`<host>:<port>:<oracle_sid>`
{ }	Braces enclose two or more items, one of which is required. Do not enter the braces.	`{ENABLE | DISABLE}`
|	A vertical bar represents a choice of two or more options within brackets or braces. Enter one of the options. Do not enter the vertical bar.	`{ENABLE | DISABLE}` `[COMPRESS | NOCOMPRESS]`
...	Horizontal ellipsis points indicate either: ■ That we have omitted parts of the code that are not directly related to the example ■ That you can repeat a portion of the code	`CREATE TABLE ... AS` *subquery*`;` `SELECT` *col1*`,` *col2*`, ... ,` *coln* `FROM employees;`
. . .	Vertical ellipsis points indicate that we have omitted several lines of code not directly related to the example.	
Italics	Italicized text indicates placeholders or variables for which you must supply particular values.	`CONNECT SYSTEM/`*system_password* `DB_NAME =` *database_name*

Convention	Meaning	Example

`UPPERCASE`	Uppercase typeface indicates elements supplied by the system. We show these terms in uppercase in order to distinguish them from terms you define. Unless terms appear in brackets, enter them in the order and with the spelling shown. However, because these terms are not case sensitive, you can enter them in lowercase.	`SELECT last_name, employee_id FROM employees;`
		`SELECT * FROM USER_TABLES;`
		`DROP TABLE hr.employees;`

`lowercase`	Lowercase typeface indicates programmatic elements that you supply. For example, lowercase indicates names of tables, columns, or files.
	Note: Some programmatic elements use a mixture of UPPERCASE and lowercase. Enter these elements as shown.
		`SELECT last_name, employee_id FROM employees;`
		`sqlplus hr/hr`
		`CREATE USER mjones IDENTIFIED BY ty3MU9;`

1

Introduction to Enterprise Manager Advanced Configuration

This chapter introduces you to Enterprise Manager advanced configuration and provides some 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:

1.1 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.

1.2 Understanding the Enterprise Manager Directory Structure

Before you perform maintenance and advanced configuration tasks, you should 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 the Database Control During and After the Oracle Database 10g Installation

1.2.1 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 two Oracle home directories:

- The Management Service home directory
- The Management Agent home directory

1.2.1.1 About the Oracle Management Service Home Directory

The Oracle Management Service is a J2EE application that is installed and deployed using Oracle Application Server. As a result, when you install the Oracle Management Service, the installation procedure first installs Oracle Application Server. Specifically, the installation procedure installs the Oracle Application Server J2EE and Web Cache installation type, which is used to deploy the Oracle Management Service.

The installation procedure installs the Enterprise Manager components within the Oracle Application Server Home, including:

- The Oracle Management Service
- Optionally, the Oracle Management Repository

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*

1.2.1.2 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 proper privileges, the Management Agent is installed in a subdirectory of the Oracle Application Server home directory.

1.2.1.3 Summary of the Important Directories in the Management Service Home

Figure 1–1 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 1–1 Important Oracle Management Service Installation Directories

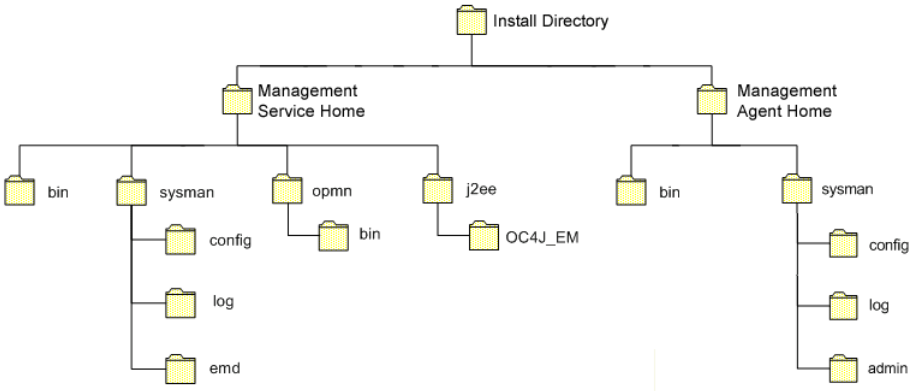


Table 1–1 describes in more detail the Management Service directories shown in Figure 1–1. In the table, ORACLE_HOME refers to the Management Service home directory in which the Oracle Management Service is installed and deployed.

Table 1–1 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. 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 1–1 (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. 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.

1.2.2 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 1–1).

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.

1.2.2.1 Summary of the Important Directories in the Management Agent Home

Table 1–2 describes some of the important subdirectories inside the AGENT_HOME directory.

Table 1–2 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. This directory serves as the Oracle Home for the Management Agent. Later in this document, this directory is referred to as the AGENT_HOME. 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 1-4.
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. 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.

1.2.2.2 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
```

1.2.3 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.

See Also: "Starting and Stopping Oracle Enterprise Manager 10g Grid Control" on page 2-10

"Locating and Configuring Enterprise Manager Log Files" on page 7-1

1.2.4 Understanding the Enterprise Manager Directories Installed with Oracle Database 10*g*

When you install Oracle Database 10*g*, you also install the Oracle Enterprise Manager 10*g* Database Control Console. The Database Control Console 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 the Database Control 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 example, if the database host name is `mgmt1.acme.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.acme.com_db42/sysman/log`

  See Also: "Locating and Configuring Enterprise Manager Log Files" on page 7-1

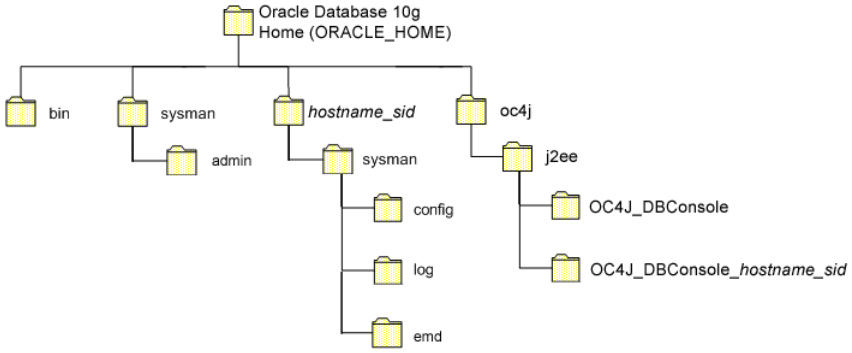
  If a *hostname_sid* directory does not exist in the Oracle Database 10*g* home directory, then the Oracle Enterprise Manager 10*g* Database Control Console was never configured for the database instance.

  See Also: "Configuring the Database Control During and After the Oracle Database 10g Installation" on page 1-7

In addition, the files required to deploy the Database Control as a J2EE application are installed into the `ORACLE_HOME/oc4j/j2ee` directory structure. The Database Control 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 Control deployed in the Oracle home.

Figure 1–2 summarizes the location of the important Enterprise Manager directories in a typical Oracle Database 10*g* home directory.

Figure 1–2 Important Enterprise Manager Directories in an Oracle Database 10g Installation



1.2.5 Tip for Identifying the Oracle Home When Using the emctl Command

When you install Grid Control, Oracle Application Server, or Oracle Database 10*g*, you 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. You 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. You 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
```

1.2.6 Configuring the Database Control During and After the Oracle Database 10*g* Installation

The following sections describe how the Oracle Enterprise Manager 10*g* Database Control Console is configured during the Oracle Database 10*g* installation. These sections also describe how you can configure the Database Control after the installation:

- Configuring the Database Control During Installation
- Configuring the Database Control with DBCA
- Configuring the Database Control with EMCA
- Using EMCA with Real Application Clusters

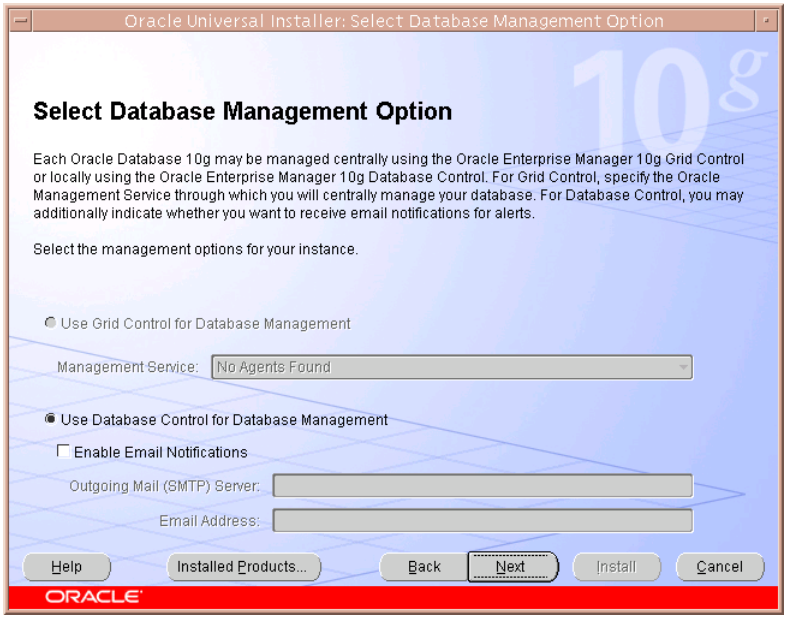
- EMCA Troubleshooting Tips

1.2.6.1 Configuring the Database Control 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 10*g* Database Control Console.

Figure 1–3 shows the Management Options page, which allows you to select your database management options while installing Oracle Database 10*g*.

Figure 1–3 Selecting Your Management Options While Installing Oracle Database 10g



To select the 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 the Database Control.

For most of the Oracle Database 10*g* installation types, you must choose either the Database Control or the 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 the Database Control:

- 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 the Database Control during the Oracle Database 10*g* installation, no *hostname_sid* directory is created in the resulting Oracle home directory (Figure 1–2).

1.2.6.2 Configuring the Database Control with DBCA

The primary method for configuring an existing Oracle Database 10*g* database so it can be managed with the Database Control 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 Control:

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 > Programs > Oracle -** ***home_name*** **> Configuration and Migration Tools > 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 1–4) and select the following options:
   - **Configure the Database with Enterprise Manager**
   - **Use Database Control for Database Management**
6. Optionally, select the options for enabling email 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 Control.

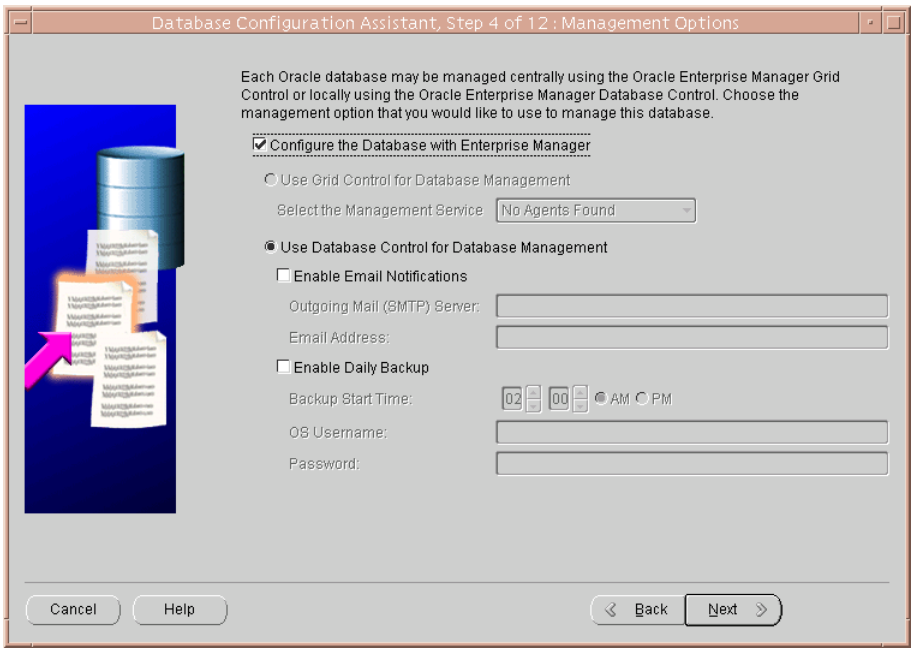
   After DBCA reconfigures the database, a new subdirectory appears in the Oracle home. This directory is named using the following format and contains Database Control configuration and state files specific to the database you just configured:

   ```
   hostname_sid
   ```

   For example:

   ```
   mgmthost1.acme.com_myNewDB
   ```

Figure 1–4 Management Options Page in DBCA



1.2.6.3 Configuring the Database Control with EMCA

When you use DBCA to configure Oracle Database 10*g*, DBCA provides a graphical user interface to help you select the Database Control options and to configure other aspects of your database.

However, if you want to use the operating system command-line to configure the Database Control, you can use the Enterprise Manager Configuration Assistant (EMCA).

To configure Database Control 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 1–3:

   ```
   $PROMPT> ./emca
   ```

   Depending upon the arguments you include on the EMCA command line, EMCA prompts you for the information required to configure the Database Control.

   For example, enter the following command to configure the Database Control so it will perform automatic daily backups of your database:

   ```
   $PROMPT> ./emca -b
   ```

Table 1–3 EMCA Command-Line Arguments

Argument	Description
-a	Use this option to configure the Database Control when you are using Automatic Storage Management to store the database files.
-b	Use this option to specify the automatic daily backup options. If you use this argument, EMCA prompts you for default backup settings that Enterprise Manager uses to automatically back up your critical database files. **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 when you use the `-b` option. You can modify these settings later using the Maintenance page in the Database Control. For more information, see the Database Control online help.
-c	Use this option to configure the Database Control for a clustered database, as opposed to a single-instance database.
-e *node_name*	Use this option to remove the Database Control for a specified node in a clustered database. Running the emca command does not remove the instance; it only removes the Database Control so you will no longer be able to manage the instance with Enterprise Manager. When removing the Database Control from a node, be sure to run the emca command before you delete the instance, and be sure to run the command from an different node and not the node from which you are removing the Database Control. Note that this option can be used only in a Real Application Clusters environment so you do not need to use the `-c` option on the command line.
-f *input_file_path*	Use this option to specify the path to an input file for EMCA to use as it configures the Database Control. For more information, see "Using an Input File for EMCA Parameters" on page 1-13.
-h	Use this option to display the online help for the EMCA utility. The help screens lists the options described in this table, as well as the parameters you will be prompted for, based on the options you select at the command line.
-m	Use this option to configure the database so it can be centrally managed by the Oracle Enterprise Manager 10*g* 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 installing the database.

Table 1–3 (Cont.) EMCA Command-Line Arguments

Argument	Description
-n *node_name*	Use this option to configure the Database Control for the specified node in a clustered database. Running the emca command does not create the instance; it only configures the Database Control so you can manage the instance with Enterprise Manager. When configuring the Database Control for a node, be sure to run the emca command after you create the instance and be sure to run the command from an existing node and not the newly created instance for which you are configuring the Database Control. Note that this option can be used only in a Real Application Clusters environment so you do not need to use the `-c` option on the command line.
-r	When you use this option, EMCA configures the database so it uses the Database Control, but it does not create the Management Repository. Use this option when the Management Repository has been created, but the Database Control has not been configured.
-s	Use this option to run EMCA in silent mode. EMCA will perform the operations without prompting for additional information. This option requires that you enter each of the required parameters on the command line, or that you enter the required parameters in an input file, using the -f argument on the emca command line. You can view a list of the available parameters by entering `emca -h` at the command line.
-x *SID* -x *DB_name*	Use this option to remove the Database Control for the specified database. For example, you might use this argument to remove the Database Control from a database you are planning to delete. In such a scenario, you should remove the Database Control before the database is physically deleted. Note that this option deletes only the Database Control for the database. It does not remove the database or any data files. When you use this argument in a Real Application Clusters environment, you must use it with the `-c` option and you should provided the name of the database and not the SID. For example: `$PROMPT> ./emca -c -x CRSdb42`
-RMI_PORT	Use this option to specify the RMI port for the Database Control. For example: `$PROMPT> ./emca -r -RMI_PORT 6201` For more information, see Section 1.2.6.6
-JMS_PORT	Use this option to specify the JMS port for the Database Control. `$PROMPT> ./emca -r -JMS_PORT 6201` For more information, see Section 1.2.6.6

Table 1–3 (Cont.) EMCA Command-Line Arguments

Argument	Description
-AGENT_PORT	Use this option to specify the Management Agent port for the Database Control. `$PROMPT> ./emca -r -AGENT_PORT 6201` **Note:** Use the `-AGENT_PORT` argument only when you are configuring Database Control for the first time. For more information, see Section 1.2.6.6
-DBCONSOLE_HTTP_PORT	Use this option to specify the port you use to display the Database Control Console in your Web browser. `$PROMPT> ./emca -r -DBCONSOLE_PORT 6201` For more information, see Section 1.2.6.6

1.2.6.4 Using an Input File for EMCA Parameters

Instead of answering a series of prompts when you run EMCA, you can use the `-f` 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
HOST=mgmthost1
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 -f input_file_path
```

For example, to configure the Database Control to perform daily backups, create an input file similar to the one shown in Example 1–1 and enter the following command at the operating system prompt:

```
$PROMPT> ./emca -b -f input_file_path
```

Example 1–1 EMCA Input File that Configures the Database Control for Automatic Backup and Creates the Management Repository

```
PORT=1521
SID=DB
HOST=mgmthost2
DBSNMP_PWD=dow31224
SYSMAN_PWD=squN3243
HOST_USER=johnson
HOST_USER_PWD=diTf32of
BACKUP_HOUR=5
BACKUP_MINUTE=5
NO_ARCHIVE=YES
LISTENER=LISTENER
SYS_PWD=qlKj4352
```

1.2.6.5 Using EMCA with Real Application Clusters

Oracle Real Application Clusters 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.

When you use EMCA to configure the Database Control for Real Application Clusters, you configure the Database Control for each instance in the cluster. After you create a new instance, you can run EMCA to configure a Database Control for that instance.

The following arguments to the EMCA command line utility can be used in a Real Application Clusters environment:

- `emca -c`, which you use to identify the fact that you are using EMCA in a Real Application Clusters environment. For example, enter `emca -c` to configure a Real Application Clusters database, create the Management Repository without enabling automatic daily backups. This option is also required when you are removing the Database Control with the `-x` option.
- `emca -e`, which you use to remove the Database Control for a specficied node.
- `emca -n`, which you use to configure the Database Control for a specified node.
- `ecma -x`, which you use to remove the Database Control from a specified database.

For more information, see Table 1–3, which describes each of the EMCA command-line options.

1.2.6.6 Specifying the Ports Used By the Database Control

When you initially install Oracle Database 10*g* or configure the Database Control with EMCA, the Database Control uses a set of default system ports. For example, by default, you access Database Control using port 5500, as in:

`http://`*`host.domain`*`:5500/em`

To use ports other than the default ports, use the following EMCA command-line arguments when you initially configure the Database Control with EMCA.

> **Note:** You can also use the following EMCA command-line arguments to configure Database Control after you have installed and configured the Oracle Database 10*g*. However, changing the port numbers of an existing Database Control will also reconfigure other Database Control default settings. Any configuration changes you have made to the Database Control will be lost.

The following list summarizes the EMCA command-line arguments that control the standard Database Control port assignments:

- -DBCONSOLE_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 the Database Control.

- -JMS_PORT <port_number>

  This port used by the OC4J Java Message Service (JMS), which is part of the J2EE software required by the Database Control.

- -AGENT_PORT <port_number>

  Caution: Use the `-AGENT_PORT` argument only when you are configuring Database Control for the first time. Do not attempt to change the `AGENT_PORT` after the Database Control is initially configured and started.

  If you attempt to change the `AGENT_PORT` after the Database Control has been configured and started, the database will show up as down in the Database Control Console. See the *Oracle Enterprise Manager 10g Database Control Release 10.1.0.3 Readme* for information about correcting the problem.

  This port is used by the Database Control Management Agent, which is monitoring and administering the database for the Database Control.

  See Also: Section 1.2.6.3 for a complete list of the EMCA comand-line arguments

1.2.6.7 EMCA Troubleshooting Tips

The following sections describe some troubleshooting tips to consider when using EMCA to configure the Database Control:

- Using EMCA When the Management Repository Already Exists
- Using EMCA After Changing the Database Listener Port

1.2.6.7.1 Using EMCA When the Management Repository Already Exists Sometimes, if you create a custom database and later use EMCA to add the capability to manage the database with the Database Control, you receive the following error:

```
Repository already exists. Fix the error(s) and run EM configuration assistant
again.
```

This error is generated when EMCA discovers that the SYSMAN database user and a corresponding Oracle Management Repository already exists in the database. As a result, EMCA is unable to create a new Oracle Management Repository for the Database Control.

There are several options for addressing this issue:

- If the database has been upgraded from a previous database version to Oracle Database 10*g*, then it likely contains a previous version of the Oracle Management Repository. As a result, you must drop the existing repository and run EMCA again to create a new Oracle Management Repository for Oracle Database 10*g*.
- If you created the database as part of the Oracle Database 10*g* installation procedure, or by using the Oracle Database 10*g* Database Configuration Assistant (DBCA), the database you created may already include the Oracle Management Repository schema. This would happen if you selected the options for configuring Enterprise Manager when you created the database.

  In this case, you can use the `-r` argument on the EMCA command line to prevent EMCA from re-creating the Management Repository:

  ```
  $PROMPT> ./emca -r
  ```

- If you are unsure of the origin of the Management Repository, or if you want to remove the existing Management Repository data and start with a new repository,

drop the existing repository and run EMCA again to create a new Management Repository for Oracle Database 10*g*.

1.2.6.7.2 Using EMCA After Changing the Database Listener Port If you change the listener port of the database after you have configured the Database Control, the database status will appear as down. To reconfigure the Database Control so it uses the new listener port, run the EMCA command using the `-r` comand-line argument.

Note: When you reconfigure the Database Control using EMCA any configuration changes you have made to the Database Control will be lost.

1.3 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

1.3.1 Enabling Enterprise Manager Accessibility Mode

Enterprise Manager takes advantage of user interface development technologies that improve the responsiveness 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 Control 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 Control (if you are modifying an Oracle Database 10*g* installation).

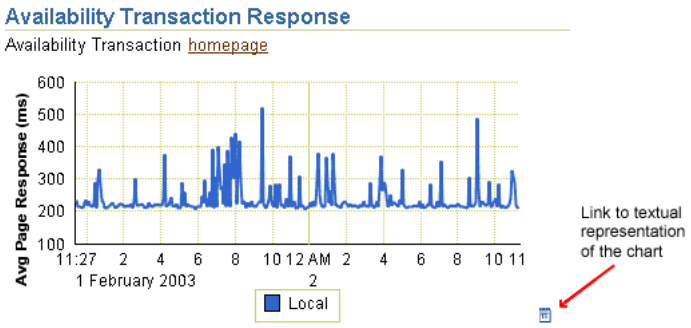
1.3.2 Providing Textual Descriptions of Enterprise Manager Charts

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 1–5 shows an example of the icon that displays beneath Enterprise Manager charts when you have enabled the textual representation of charts.

Figure 1–5 Icon Representing the Textual Representation of a 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. Uncomment 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 Control (if you are modifying an Oracle Database 10*g* installation).

2

Starting and Stopping Enterprise Manager Components

To start and stop the Management Service, the Management Agent, the Grid Control Console, the Application Server Control Console, and the Database Control, you use the Enterprise Manager command-line utility (`emctl`).

The capabilities of the command-line utility can be broken down into the following categories:

- Controlling the Oracle Management Agent
- Controlling the Oracle Management Service
- Controlling the Application Server Control
- Controlling the Database Control on UNIX
- Starting and Stopping Oracle Enterprise Manager 10g Grid Control
- Additional Management Agent Commands

2.1 Controlling the Oracle Management Agent

The following sections describe how to use the Enterprise Manager command-line utility (`emctl`) to control the Oracle Management Agent:

- Starting, Stopping, and Checking the Status of the Management Agent on UNIX
- Starting and Stopping the Management Agent on Windows
- Checking the Status of the Management Agent on Windows

2.1.1 Starting, Stopping, and Checking the Status of the Management Agent on UNIX

To start, stop, or check the status of the Management Agent on UNIX systems:

1. Change directory to the *AGENT_HOME*`/bin` directory.
2. Use the appropriate command described in Table 2–1.

   For example, to stop the Management Agent, enter the following commands:

```
$PROMPT> cd AGENT_HOME/bin
$PROMPT> ./emctl stop agent
```

Table 2–1 Starting, Stopping, and Checking the Status of the Management Agent

Command	Purpose
emctl start agent	Starts the Management Agent

Table 2–1 (Cont.) Starting, Stopping, and Checking the Status of the Management Agent

Command	Purpose
emctl stop agent	Stops the Management Agent
emctl status agent	If the Management Agent is running, this command displays status information about the Management Agent, including the Agent Home, the process ID, and the time and date of the last successful upload to the Management Repository (Example 2–1).

Example 2–1 Checking the Status of the Management Agent

```
$PROMPT> ./emctl status agent
Oracle Enterprise Manager 10g Release 10.1.0.2.0
Copyright (c) 2002, 2003 Oracle Corporation.  All rights reserved.
---------------------------------------------------------------
Version           : 10.1.0.2.0
Agent Home        : /private/oracle/EM_40_SH10/agent
Agent Process ID  : 8102
Parent Process ID : 8095
Agent URL         : http://usunnab08.us.oracle.com:1813/emd/main/
Started at        : 2003-01-29 12:11:39
Started by user   : oracle
Last Reload       : 2003-01-29 12:45:10
Last successful upload                       : 2003-01-30 11:08:27
Total Megabytes of XML files uploaded so far :    25.21
Number of XML files pending upload           :        0
Size of XML files pending upload(MB)         :     0.00
Available disk space on upload filesystem    :    76.87%
---------------------------------------------------------------
Agent is Running and Ready
$PROMPT>
```

2.1.2 Starting and Stopping the Management Agent on Windows

When you install the Oracle Management Agent on a Windows system, the installation procedure creates three new services in the Services control panel.

The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using. For example, on Windows 2000, locate the Services Control panel by selecting **Settings** and then **Administrative Tools** from the **Start** menu.

> **Note:** The `emctl` utility described in Section 2.2.1 is available in the `bin` subdirectory of the Oracle home where you installed the Management Agent; however, Oracle recommends that you use the Services control panel to start and stop the Management Agent on Windows systems.

Table 2–2 describes the Windows services that you use to control the Management Agent.

Table 2–2 Summary of Services Installed and Configured When You Install the Management Agent on WIndows

Component	Service Name Format	Description

Oracle Management Agent	`Oracle<agent_home>Agent`
	For example:
	`OracleOraHome1Agent`
		Use this Service to start and stop the Application Server Control for the Oracle Application Server instance that was installed and configured to deploy the Management Service J2EE application.

Oracle SNMP Peer Encapsulator	`Oracle<oracle_home>SNMPPeerEncapsulator`
	For example:
	`OracleOraHome1PeerEncapsulator`
		Use this service only if you are using the advanced features of the Simple Network Management Protocol (SNMP).
		For more information, see the *Oracle SNMP Support Reference Guide*

Oracle Peer SNMP Master Agent	`Oracle<oracle_home>SNMPPeerMasterAgent`
	For example:
	`OracleOraHome1PeerMasterAgent`
		Use this service only if you are using the advanced features of the Simple Network Management Protocol (SNMP).
		For more information, see the *Oracle SNMP Support Reference Guide*

Note: If you are having trouble starting or stopping the Management Agent on a Windows NT system, try stopping the Management Agent using the following command emctl command:

```
$PROMPT> <AGENT_HOME>/bin/emctl istop agent
```

After stopping the Management Agent using the emctl istop agent command, start the Management Agent using the Services control panel.

This problem and solution is applies only to the Windows NT platform, not to other Windows platforms, such as Windows 2000 or Windows XP systems.

2.1.3 Checking the Status of the Management Agent on Windows

To check the status of the Management Agent on Windows systems:

1. Change directory to the following location in the AGENT_HOME directory:

   AGENT_HOME/bin

2. Enter the following emctl command to check status of the Management Agent:

   ```
   $PROMPT> ./emctl status agent
   ```

   If the Management Agent is running, this command displays status information about the Management Agent, including the Agent Home, the process ID, and the

time and date of the last successful upload to the Management Repository (Example 2–1).

2.2 Controlling the Oracle Management Service

The following sections describe how to control the Oracle Management Service:

- Controlling the Management Service on UNIX
- Controlling the Management Service on Windows

2.2.1 Controlling the Management Service on UNIX

There are two methods for starting and stopping the Oracle Management Service on UNIX systems. You can use the Oracle Process Management and Notification (OPMN) utility, or you can use a set of `emctl` commands.

The following sections describe these two approaches to controlling the Management Service, as well as information about starting and stopping OracleAS Web Cache, which is also required by the Grid Control Console:

- Using OPMN to Start and Stop the Management Service
- Using emctl to Start, Stop, and Check the Status of the Oracle Management Service
- Starting and Stopping Oracle Application Server Web Cache

2.2.1.1 Using OPMN to Start and Stop the Management Service

One method of starting and stopping the Management Service by using the Oracle Process Management and Notification (OPMN) utility. The OPMN utility (`opmnctl`) is a standard command used to start and stop components of the Oracle Application Server instance.

The Management Service is a J2EE application running in an Oracle Application Server Containers for J2EE (OC4J) instance within the application server. As a result, the following command will start all the components of the Oracle Application Server instance, including the OC4J_EM instance and the Management Service application:

```
$PROMPT> cd opmn/bin
$PROMPT> ./opmnctl startall
```

Similarly, the following command will stop all the components of the Oracle Application Server instance:

```
$PROMPT> ./opmnctl stopall
```

If you want to start only the components necessary to run the Management Service, you can use the Enterprise Manager command-line utility.

2.2.1.2 Using emctl to Start, Stop, and Check the Status of the Oracle Management Service

To start, stop, or check the status of the Management Service with the Enterprise Manager command-line utility:

1. Change directory to the `ORACLE_HOME/bin` directory in the Management Service home.
2. Use the appropriate command described in Table 2–3.

   For example, to stop the Management Service, enter the following commands:

```
$PROMPT> cd bin
$PROMPT> ./emctl stop oms
```

Table 2–3 Starting, Stopping, and Checking the Status of the Management Service

Command	Purpose
emctl start oms	Starts the Oracle Application Server components required to run the Management Service J2EE application. Specifically, this command starts OPMN, the Oracle HTTP Server, and the OC4J_EM instance where the Management Service is deployed. **Note:** The `emctl start oms` command does not start Oracle Application Server Web Cache. For more information, see "Starting and Stopping Oracle Application Server Web Cache" on page 2-5.
emctl stop oms	Stops the Management Service. Note that this command does not stop the other processes that are managed by the Oracle Process Manager and Notification Server (OPMN) utility. To stop the other Oracle Application Server components, such as the Oracle HTTP Server and Oracle Application Server Web Cache, see "Starting and Stopping Oracle Enterprise Manager 10g Grid Control" on page 2-10.
emctl status oms	Displays a message indicating whether or not the Management Service is running.

2.2.1.3 Starting and Stopping Oracle Application Server Web Cache

By default, when you install Oracle Enterprise Manager 10*g*, the Grid Control Console is configured to use Oracle Application Server Web Cache.

> **See Also:** *Oracle Application Server Web Cache Administrator's Guide* for more information about Oracle Application Server Web Cache

Oracle Application Server Web Cache not only improves the performance of the Grid Control Console, but also makes it possible to measure the end-user performance of the Enterprise Manager Web application.

> **See Also:** Chapter 6, "Configuring Application Service Level Management" for more information about End-User Performance Monitoring and the Enterprise Manager Web Application

To view the Grid Control Console using Oracle Application Server Web Cache, you access the Grid Control Console using the standard port number assigned during the Oracle Enterprise Manager 10*g* installation procedure. You can find this default port number (usually 7777) in the `setupinfo.txt` file, which is copied to the following directory during the Enterprise Manager installation procedure:

```
AS_HOME/Apache/Apache
```

If Oracle Application Server Web Cache is not running, you will receive an error message, such as the following, if you try to access the Grid Control Console using the default port number:

```
HTTP 500 - Internal server error
```

To start Oracle Application Server Web Cache:

1. Change directory to the `ORACLE_HOME/opmn/bin` directory in the Management Service home.
2. Use the appropriate command described in Table 2–4.

   For example, to stop Oracle Application Server Web Cache, enter the following commands:

```
$PROMPT> cd opmn/bin
$PROMPT> ./opmnctl stopproc ias-component=WebCache
```

Table 2–4 Starting, Stopping, and Checking the Status of Oracle Application Server Web Cache

Command	Purpose
`opmnctl startproc ias-component=WebCache`	Starts Oracle Application Server Web Cache.
`opmnctl stopproc ias-component=WebCache`	Stops Oracle Application Server Web Cache.
`opmnctl status`	Displays a message showing the status of all the application server components managed by OPMN, including Oracle Application Server Web Cache.

2.2.2 Controlling the Management Service on Windows

When you install the Oracle Management Service on a Windows system, the installation procedure creates three new services in the Services control panel.

The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using. For example, on Windows 2000, locate the Services control panel by selecting **Settings** and then **Administrative Tools** from the **Start** menu.

> **Note:** The `emctl` utility described in Section 2.2.1 is available in the `bin` subdirectory of the Oracle home where you installed the Management Service; however, Oracle recommends that you use the Services control panel to start and stop the Management Service on Windows systems.

Table 2–5 describes the Windows services that you use to control the Oracle Management Service.

Table 2–5 Summary of Services Installed and Configured When You Install the Oracle Management Service on WIndows

Component	Service Name Format	Description

Application Server Control	`Oracle<oracle_home>ASControl`
	For example:
	`OracleOraHome1ASControl`
		Use this Service to start and stop the Application Server Control for the Oracle Application Server instance that was installed and configured to deploy the Management Service J2EE application.

Table 2–5 (Cont.) Summary of Services Installed and Configured When You Install the Oracle Management Service on WIndows

Component	Service Name Format	Description

Oracle Process Management and Notification (OPMN)	`Oracle<oracle_home>ProcessManager`
	For example:
	`OracleOraHome1ProcessManager`
		Use this service to start and stop all the components of the Oracle Application Server instance that was installed and configured to deploy the Management Service J2EE application.
		Use this service to start and stop the Management Service and all its related components, including OC4J, Oracle HTTP Server, and OracleAS Web Cache, which by default must be running in order for you to access the Grid Control Console.

2.3 Controlling the Application Server Control

The Application Server Control is a component of Oracle Enterprise Manager 10*g* that is installed as part of any Oracle Application Server installation. The following sections describe how to start and stop the Application Server Control:

- Starting and Stopping the Application Server Control on UNIX
- Starting and Stopping the Application Server Control on Windows

> **See Also:** *Oracle Application Server 10g Administrator's Guide* for more information about using `emctl` to control the Application Server Control Console and for information on starting and stopping the Application Server Control Console on Windows

2.3.1 Starting and Stopping the Application Server Control on UNIX

To control the Application Server Control Console on UNIX systems, you use the emctl command-line utility that is available in the `IAS_HOME/bin` directory after you install Oracle Application Server.

To start the Application Server Control Console, change directory to the `IAS_HOME/bin` directory and then enter the following command:

```
$PROMPT> ./emctl start iasconsole
```

To stop the Application Server Control Console, enter the following command:

```
$PROMPT> ./emctl stop iasconsole
```

2.3.2 Starting and Stopping the Application Server Control on Windows

To start or stop the Application Server Control on Windows systems:

1. Open the Services control panel.

   For example, on Windows NT, select **Start > Settings > Control Panel** and then double-click the Services icon.

   On Windows 2000, select **Start > Administrative Tools > Services**.

2. Locate the Application Server Control in the list of services.

The name of the service is usually consists of "Oracle," followed by the name of the home directory you specified during the installation, followed by the word "ASControl." For example, if you specified `AS10g` as the Oracle Home, the Service name would be:

```
OracleAS10gASControl
```

3. After you locate the service, you can use the Services control panel to start or stop the Application Server Control service.

   By default, the Application Server Control service is configured to start automatically when the system starts.

2.4 Controlling the Database Control on UNIX

The Oracle Enterprise Manager 10*g* Database Control Console is a component of Oracle Enterprise Manager 10*g* that is installed as part of any Oracle Database 10*g* installation.

To control the Database Control, you use the `emctl` command-line utility that is available in the `ORACLE_HOME/bin` directory after you install Oracle Database 10*g*.

2.4.1 Starting the Database Control on UNIX

To start the Database Control, as well the Management Agent and the Management Service associated with the Database Control:

1. Set the following environment variables to identify the Oracle home and the system identifier (SID) for the database instance you want to manage:
   - ORACLE_HOME
   - ORACLE_SID
2. Change directory to the `ORACLE_HOME/bin` directory.
3. Enter the following command:

```
$PROMPT> ./emctl start dbconsole
```

2.4.2 Stopping the Database Control on UNIX

To stop the Database Control, as well the Management Agent and the Management Service associated with the Database Control:

1. Set the following environment variables to identify the Oracle home and the system identifier (SID) for the database instance you want to manage:
   - ORACLE_HOME
   - ORACLE_SID
2. Change directory to the `ORACLE_HOME/bin` directory.
3. Enter the following command:

```
$PROMPT> ./emctl stop dbconsole
```

2.4.3 Starting and Stopping the Database Control on Windows

To start or stop the Database Control on Windows systems:

1. Open the Services control panel.

For example, on Windows NT, select **Start > Settings > Control Panel** and then double-click the Services icon.

On Windows 2000, select **Start > Administrative Tools > Services**.

2. Locate the Database Control in the list of services.

   The name of the service is usually consists of "Oracle," followed by the name of the home directory you specified during the installation and the database system identifier (SID), followed by the word "DBControl." For example, if you specified `DBd10g` as the Oracle Home, the Service name would be:

   ```
   OracleDB10gDBControl
   ```

3. After you locate the service, you can use the Services control panel to start or stop the Database Control service.

   By default, the Database Control service is configured to start automatically when the system starts.

2.5 Guidelines for Starting Multiple Enterprise Manager Components on a Single Host

Oracle Enterprise Manager 10*g* components are used to manage a variety of Oracle software products. For example, each time you install Oracle Application Server 10g (9.0.4) instance, you also install an Application Server Control. Similarly, each time you install Oracle Database 10*g*, you install a Database Control. In addition, if you want to centrally manage your system with Database Control, the Management Agent is also installed on each host you monitor.

In most cases, in a production environment, you will want to distribute your database and application server instances among multiple hosts to improve performance and availability of your software resources. However, in rare cases where you must install multiple application servers or databases on the same host, consider the following guidelines.

When you start Application Server Control, the Management Agent, or the Database Control, Enterprise Manager immediately begins gathering important monitoring data about the host and its managed targets. Keep this in mind when you develop a process for starting the components on the host.

Specifically, consider staggering the startup process so that each Enterprise Manager process has a chance to start before the next process begins its startup procedure.

For example, suppose you have installed OracleAS Infrastructure 10*g*, the J2EE and Web Cache application server installation type, and the Management Agent on the same host. When you start up all the components (for example, after a restart of the system), use a process such as the following:

1. Use the `opmnctl startall` command to start all the OPMN-managed processes in the OracleAS Infrastructure 10*g* home directory.
2. Wait 15 seconds.
3. Use the emctl start iasconsole command to start the Application Server Control in the OracleAS Infrastructure 10*g* home directory.
4. Wait 15 seconds.
5. Use the `opmnctl startall` command to start all the OPMN-managed processes in the J2EE and Web Cache home directory.

6. Wait 15 seconds.
7. Use the `emctl start iasconsole` command to start the Application Server Control in the J2EE and Web Cache home directory.
8. Wait 15 seconds.
9. Use the `emctl start agent` command to start the Management Agent for the host.

Using a staggered startup procedure such as the preceding example will ensure that the processes are not in contention for resources during the CPU-intensive startup phase for each component.

2.6 Starting and Stopping Oracle Enterprise Manager 10*g* Grid Control

As described in the previous sections, you use separate commands to control the Oracle Management Service, Oracle Management Agent, and the Oracle Application Server components on which the Grid Control depends.

The following sections describe how to stop and start all the Grid Control components that are installed by the Oracle Enterprise Manager 10*g* Grid Control Console installation procedure.

You can use this procedure to start all the framework components after a system reboot or to shutdown all the components before bringing the system down for system maintenance.

2.6.1 Starting Grid Control and All Its Components

The following procedure summarizes the steps required to start all the components of the Grid Control. For example, use this procedure if you have restarted the host computer and all the components of the Grid Control have been installed on that host.

To start all the Grid Control components on a host, use the following procedure:

1. If your Oracle Management Repository resides on the host, change directory to the Oracle Home for the database where you installed the Management Repository and start the database and the Net Listener for the database:
   a. Set the ORACLE_HOME environment variable to the Management Repository database home directory.
   b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).
   c. Start the Net Listener:

      ```
      $PROMPT> $ORACLE_HOME/bin/lsnrctl start
      ```

   d. Start the Management Repository database instance:

      ```
      ORACLE_HOME/bin/sqlplus /nolog
      SQL> connect SYS as SYSDBA
      SQL> startup
      SQL> quit
      ```

      See Also: *Oracle Database Administrator's Guide* for information about starting and stopping an Oracle Database

2. Start the Oracle Management Service:

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

> **See Also:** "Controlling the Oracle Management Service" on page 2-4

3. Start OracleAS Web Cache:

```
$PROPMT> $ORACLE_HOME/opmn/bin/opmnctl startproc ias-component=WebCache
```

4. Change directory to the home directory for the Oracle Management Agent and start the Management Agent:

```
$PROMPT> AGENT_HOME/bin/emctl start agent
```

> **See Also:** "Controlling the Oracle Management Agent" on page 2-1

> **Note:** Be sure to run the `emctl start agent` command in the Oracle Management Agent home directory and not in the Management Service home directory.

5. Optionally, start the Application Server Control Console, which is used to manage the Oracle Application Server instance that is used to deploy the Management Service:

```
$PROMPT> $ORACLE_HOME/bin/emctl start iasconsole
```

> **See Also:** "Controlling the Application Server Control" on page 2-7

2.6.2 Stopping Grid Control and All Its Components

The following procedure summarizes the steps required to stop all the components of the Grid Control. For example, use this procedure if you have installed all the components of the Grid Control on the same host you want to shut down or restart the host computer.

To stop all the Grid Control components on a host, use the following procedure:

1. Stop the Oracle Management Service:

```
$PROMPT> $ORACLE_HOME/bin/emctl stop oms
```

> **See Also:** "Controlling the Oracle Management Service" on page 2-4

2. If necessary, stop the Application Server Control Console, which is used to manage the Oracle Application Server instance used to deploy the Management Service:

```
$PROMPT> $ORACLE_HOME/bin/emctl stop iasconsole
```

> **See Also:** "Controlling the Application Server Control" on page 2-7

3. Stop all the Oracle Application Server components, such as the Oracle HTTP Server the OracleAS Web Cache:

```
$PROMPT> $ORACLE_HOME/opmn/bin/opmnctl stopall
```

See Also: *Oracle Application Server 10g Administrator's Guide*

4. Change directory to the home directory for the Oracle Management Agent and stop the Management Agent:

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

See Also: "Controlling the Oracle Management Agent" on page 2-1

Note: Be sure to run the `emctl stop agent` command in the Oracle Management Agent home directory and not in the Oracle Application Server home directory.

---

5. If your Oracle Management Repository resides on the same host, change directory to the Oracle Home for the database where you installed the Management Repository and stop the database and the Net Listener for the database:
   a. Set the ORACLE_HOME environment variable to the Management Repository database home directory.
   b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).
   c. Stop the database instance:

```
$PROMPT> ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

See Also: *Oracle Database Administrator's Guide* for information about starting and stopping an Oracle Database

   d. Stop the Net Listener:

```
$PROMPT> $ORACLE_HOME/bin/lsnrctl stop
```

2.7 Additional Management Agent Commands

The following sections describe additional `emctl` commands you can use to control the Management Agent:

- Uploading and Reloading Data to the Management Repository
- Specifying New Target Monitoring Credentials
- Listing the Targets on a Managed Host
- Controlling Blackouts

2.7.1 Uploading and Reloading Data to the Management Repository

Under normal circumstances, the Management Agent uploads information about your managed targets to the Management Service at regular intervals.

However, there are two Enterprise Manager commands that can help you force an immediate upload of data to the Management Service or a reload of the target definitions and attributes stored in the Management Agent home directory.

To use these commands, change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_HOME\bin` directory (Windows) and enter the appropriate command as described in Table 2–6.

Table 2–6 Manually Reloading and Uploading Management Data

Command	Purpose
emctl upload	Use this command to force an immediate upload of the current management data from the managed host to the Management Service. Use this command instead of waiting until the next scheduled upload of the data.
emctl reload	This command is for use by Oracle Support. This command can be used when manual edits are made to the Management Agent configuration (.XML) files. For example, if changes are made to the `targets.xml` file, which defines the attributes of your managed targets, this command will upload the modified target information to the Management Service, which will then update the information in the Management Repository. **Note:** Oracle does not support manual editing of the `targets.xml` files unless the procedure is explicitly documented or you are instructed to do so by Oracle Support.

2.7.2 Specifying New Target Monitoring Credentials

To monitor the performance of your database targets, Enterprise Manager connects to your database using a database username and password. This username and password combination is referred to as the database monitoring credentials.

> **Note:** The instructions in this section are specific to the monitoring credentials for a database target, but you can use this procedure for any other target type that requires monitoring credentials. For example, you can use this procedure to specify new monitoring credentials for your Oracle Management Service and Management Repository.
>
> For more information about the monitoring credentials for the Management Repository, see "Changing the SYSMAN Password" on page 8-7.

When you first add an Oracle9i Database target, or when it is added for you during the installation of the Management Agent, Enterprise Manager uses the DBSNMP database user account and the default password for the DBSNMP account as the monitoring credentials.

When you install Oracle Database 10*g*, you specify the DBSNMP monitoring password during the database installation procedure.

As a result, if the password for the DBSNMP database user account is changed, you must modify the properties of the database target so that Enterprise Manager can continue to connect to the database and gather configuration and performance data.

Similarly, immediately after you add a new Oracle Database 10*g* target to the Grid Control, you may need to configure the target so it recognizes the DBSNMP password that you defined during the database installation. Otherwise, the Database Home page may display no monitoring data and the status of the database may indicate that there is a metric collection error.

You can modify the Enterprise Manager monitoring credentials by using the Oracle Enterprise Manager 10*g* Grid Control Console or by using the Enterprise Manager command-line utility (`emctl`).

2.7.2.1 Using the Grid Control Console to Modify the Monitoring Credentials

To modify the password for the DBSNMP account in the Oracle Enterprise Manager 10*g* Grid Control Console:

1. Click the **Targets** tab in the Grid Control Console.
2. Click the **Database** subtab to list the database targets you are monitoring.
3. Select the database and click **Configure**.

   Enterprise Manager displays the Configure Database: Properties page.
4. Enter the new password for the DBSNMP account in the **Monitor Password** field.
5. Click **Test Connection** to confirm that the monitoring credentials are correct.
6. If the connection is successful, continue to the end of the Database Configuration wizard and click **Submit**.

2.7.2.2 Using the Enterprise Manager Command Line to Modify the Monitoring Credentials

To enter new monitoring credentials with the Enterprise Manager command-line utility:

1. Change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_HOME\bin` directory (Windows).
2. Enter the following command to specify new monitoring credentials:

   ```
   $PROMPT>./emctl config agent credentials [Target_name[:Target_Type]]
   ```

   To determine the correct target name and target type, see "Listing the Targets on a Managed Host" on page 2-14.

   Example 2–2 shows an example of the prompts and the output you receive from the command.

Example 2–2 Modifying the Database Monitoring Credentials

```
$PROMPT>./emctl config agent credentials emrep10.acme.com:oracle_database
Oracle Enterprise Manager 10g Release 10.1.0.2.0
Copyright (c) 2002, 2003 Oracle Corporation.  All rights reserved.
Name = emrep10.us.oracle.com, Type = oracle_database
Want to change for "UserName" (y/n):n
Want to change for "password" (y/n):y
Enter the value for "password" :*******
EMD reload completed successfully
```

2.7.3 Listing the Targets on a Managed Host

There are times when you need to provide the name and type of a particular target you are managing. For example, you must know the target name and type when you are setting the monitoring credentials for a target.

To list the name and type of each target currently being monitored by a particular Management Agent:

1. Change directory to the AGENT_HOME/bin directory (UNIX) or the AGENT_HOME\bin directory (Windows).
2. Enter the following command to specify new monitoring credentials:

```
$PROMPT>./emctl config agent listtargets  [AGENT_HOME]
```

Example 2–3 shows the typical output of the command.

Example 2–3 Listing the Targets on a Managed Host

```
./emctl config agent listtargets
Oracle Enterprise Manager 10g Release 10.1.0.2.0
Copyright (c) 2002, 2003 Oracle Corporation.  All rights reserved.
[usunnab08.us.oracle.com, host]
[LISTENER_usunnab08.us.oracle.com, oracle_listener]
[EnterpriseManager.usunnab08.us.oracle.com_HTTP Server, oracle_apache]
[EnterpriseManager.usunnab08.us.oracle.com_home, oc4j]
[EnterpriseManager.usunnab08.us.oracle.com_Web Cache, oracle_webcache]
[EnterpriseManager.usunnab08.us.oracle.com, oracle_ias]
[EnterpriseManager.usunnab08.us.oracle.com_OC4J_EM, oc4j]
[EnterpriseManager.usunnab08.us.oracle.com_OC4J_Demos, oc4j]
[EM_Repository, oracle_emrep]
[usunnab08.us.oracle.com:1813, oracle_emd]
[EM Website, website]
[emrep10.us.oracle.com, oracle_database]
```

2.7.4 Controlling Blackouts

Blackouts allow Enterprise Manager users to suspend management data collection activity on one or more managed targets. For example, administrators use blackouts to prevent data collection during scheduled maintenance or emergency operations.

> **See Also:** The "Systems Monitoring" chapter in Oracle Enterprise Manager Concepts for more information about Enterprise Manager blackouts

You can control blackouts from the Oracle Enterprise Manager 10*g* Grid Control Console or from the Enterprise Manager command-line utility (emctl). However, if you are controlling target blackouts from the command line, you should not attempt to control the same blackouts from the Grid Control Console. Similarly, if you are controlling target blackouts from the Grid Control Console, do not attempt to control those blackouts from the command line.

> **See Also:** "Creating, Editing, and Viewing Blackouts" in the Enterprise Manager online help for information about controlling blackouts from the Grid Control Console

From the command line, you can perform the following blackout functions:

- Starting Immediate Blackouts
- Stopping Immediate Blackouts
- Checking the Status of Immediate Blackouts

Note: When you start a blackout from the command line, any Enterprise Manager jobs scheduled to run against the blacked out targets will still run. If you use the Grid Control Console to control blackouts, you can optionally prevent jobs from running against blacked out targets.

To use the Enterprise Manager command-line utility to control blackouts:

1. Change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_HOME\bin` directory (Windows).
2. Enter the appropriate command as described in Table 2–7.

Note: When you start a blackout, you must identify the target or targets affected by the blackout. To obtain the correct target name and target type for a target, see "Listing the Targets on a Managed Host" on page 2-14.

Table 2–7 Summary of Blackout Commands

Blackout Action	Command
Set an immediate blackout on a particular target or list of targets	`emctl start blackout <Blackoutname> [<Target_name>[:<Target_Type>]]....[-d <Duration>]` Be sure to use a unique name for the blackout so you can refer to it later when you want to stop or check the status of the blackout. The `-d` option is used to specify the duration of the blackout. Duration is specified in `[days] hh:mm where:` ■ days ■ indicates number of days, which is optional ■ hh ■ indicates number of hours ■ mm ■ indicates number of minutes If you do not specify a target or list of targets, Enterprise Manager will blackout the local host target. All monitored targets on the host are not blacked out unless a list is specified or you use the `-nodelevel` argument, which is described below. If two targets of different target types share the same name, you must identify the target with its target type.
Stop an immediate blackout	`emctl stop blackout <Blackoutname>`
Set an immediate blackout for all targets on a host	`emctl start blackout <Blackoutname> [-nodeLevel] [-d <Duration>]` The `-nodeLevel` option is used to specify a blackout for all the targets on the host; in other words, all the targets that the Management Agent is monitoring, including the Management Agent host itself. The `-nodeLevel` option must follow the blackout name. If you specify any targets after the `-nodeLevel` option, the list is ignored.
Check the status of a blackout	emctl status blackout `[<Target_name>[:<Target_Type>]]....`

Use the following examples to learn more about controlling blackouts from the Enterprise Manager command line:

- To start a blackout called "bk1" for databases "db1" and "db2," and for Oracle Listener "ldb2," enter the following command:

  ```
  $PROMPT> emctl start blackout bk1 db1 db2 ldb2:oracle_listener -d 5 02:30
  ```

  The blackout starts immediately and will last for 5 days 2 hours and 30 minutes.

- To check the status of all the blackouts on a managed host:

  ```
  $PROMPT> emctl status blackout
  ```

- To stop blackout "bk2" immediately:

  ```
  $PROMPT> emctl stop blackout bk2
  ```

- To start an immediate blackout called "bk3" for all targets on the host:

  ```
  $PROMPT> emctl start blackout bk3 -nodeLevel
  ```

- To start an immediate blackout called "bk3" for database "db1" for 30 minutes:

  ```
  $PROMPT> emctl start blackout bk3 db1 -d 30
  ```

- To start an immediate blackout called "bk3" for database "db2" for five hours:

  ```
  $PROMPT> emctl start blackout bk db2 -d 5:00
  ```

3

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.

This chapter presents the common configurations 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 server load balancers, Oracle Real Application Clusters, and Oracle Data Guard.

This chapter contains the following sections:

3.1 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 example, 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 4, "Enterprise Manager Security" for information about securing the connections between Grid Control components
>
> Chapter 5, "Configuring Enterprise Manager for Firewalls" for information about configuring firewalls between Grid Control components

Besides providing a description of common configurations, 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.

3.2 Summary of the Grid Control Architecture and Components

The Grid Control architecture consists of the following software components:

- The Oracle Management Agent
- The Oracle Management Service
- The Oracle Management Repository
- The Oracle Enterprise Manager 10*g* Grid Control Console

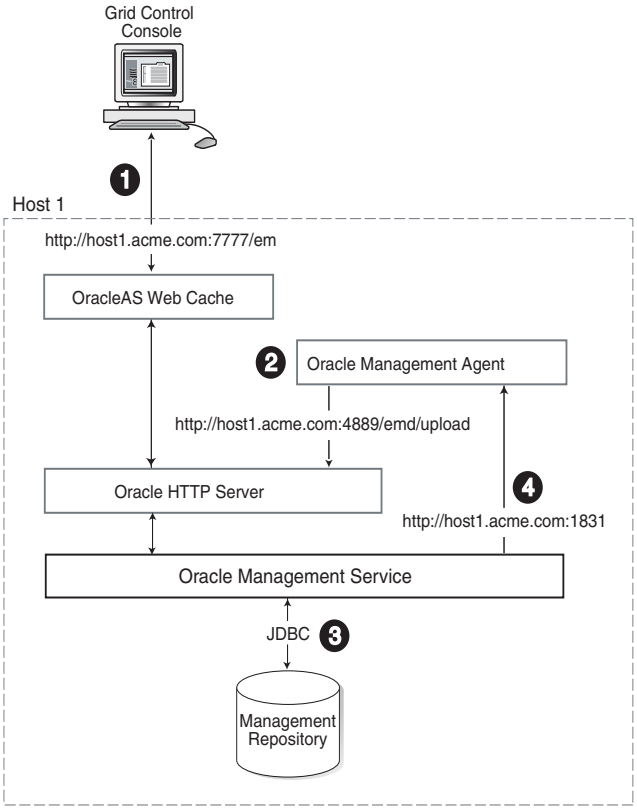
> **See Also:** *Oracle Enterprise Manager Concepts* for more information about each of the Grid Control components

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.

3.3 Deploying Grid Control Components on a Single Host

Figure 3–1 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 3–1 Grid Control Components Installed on a Single Host



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 of the managed targets on the host, including the Management Service and the Management Repository database) via 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 1-1 for more information about the AGENT_HOME directory

3. The Management Service uses JDBC connections to load data into the repository database and to retrieve information from the repository so it can be displayed in the Grid Control Console. The 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 9-7 for more information on modifying the repository connection information in the `emoms.properties` file

4. The Management Service sends data to the Management Agent via 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:

   ```
   URL_EMD=http://host1.acme.com:1831/emd/main/
   ```

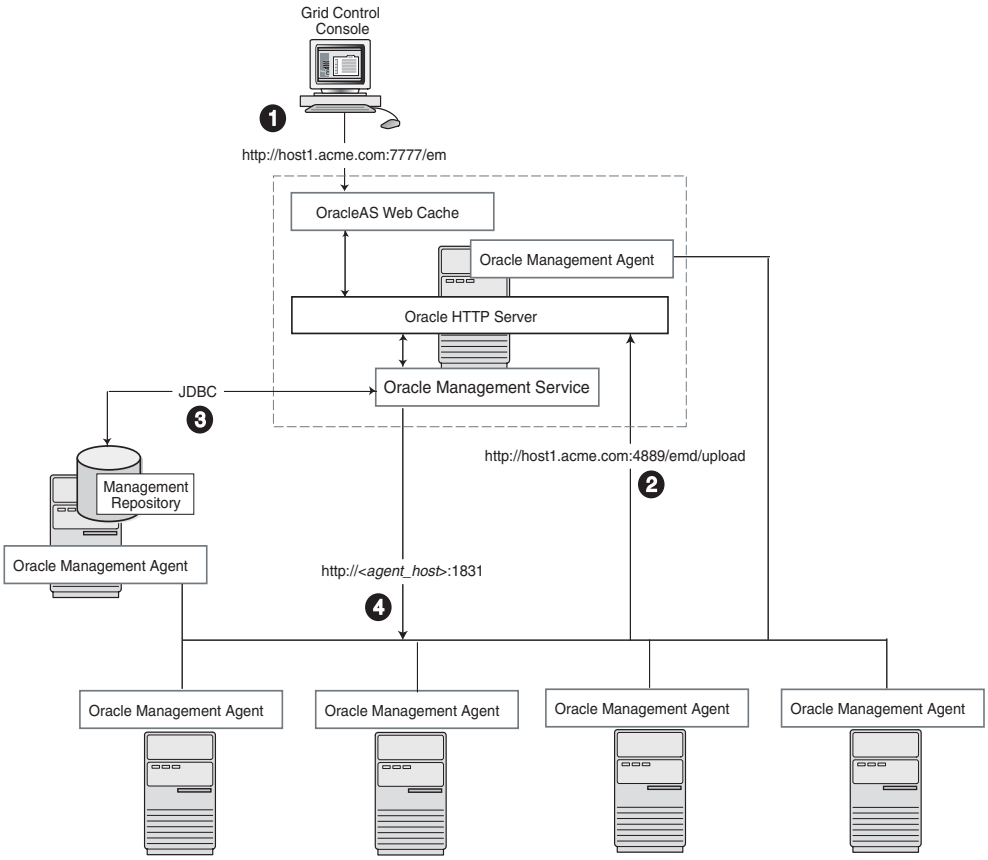
   In addition, by default, the name of the Management Agent as it appears in the Grid Control Console consists of the Management Agent host name and the port used by the Management Agent URL.

3.4 Managing Multiple Hosts and Deploying a Remote Management Repository

Installing all the Grid Control components on a single host is a 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. Such a configuration is shown in Figure 3–2.

Figure 3–2 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 via 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 3.3.
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 via 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 repository database and to retrieve information from the 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 via 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 3.3, the Management Agent includes a built-in HTTP listener so no Oracle HTTP Server is required on the Management Agent host.

3.5 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:

- Determining When To Use Multiple Management Service Installations
- Understanding the Flow of Management Data When Using Multiple Management Services

3.5.1 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 and balanced. 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

3.5.1.1 Monitoring the Load on Your Management Service Installations

To keep the workload evenly distributed, you should always be aware of how many Management Agents are configured for each Management Service and monitor the load on each Management Service.

At any time, you can view list of Management Agents and Management Services on the **Management System** tab of the Grid Control Console.

Use the charts on the Management System tab to monitor:

- Loader backlog (files)

  The Loader is part of the Management Service that pushes metric data into the 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 summed 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 backlog

  The Notification 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 you may want to consider adding another Management Service, reducing the number of notification rules, and verifying that all rules and notification methods are useful and valid.

3.5.1.2 Monitoring the Response Time of the Enterprise Manager Web Application Target

The information on the Management System tab can help you determine the load being placed on your Management Service installations. More importantly, you should also 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. Review the Availability Transaction Response chart to view 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 Service Level 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 via 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.

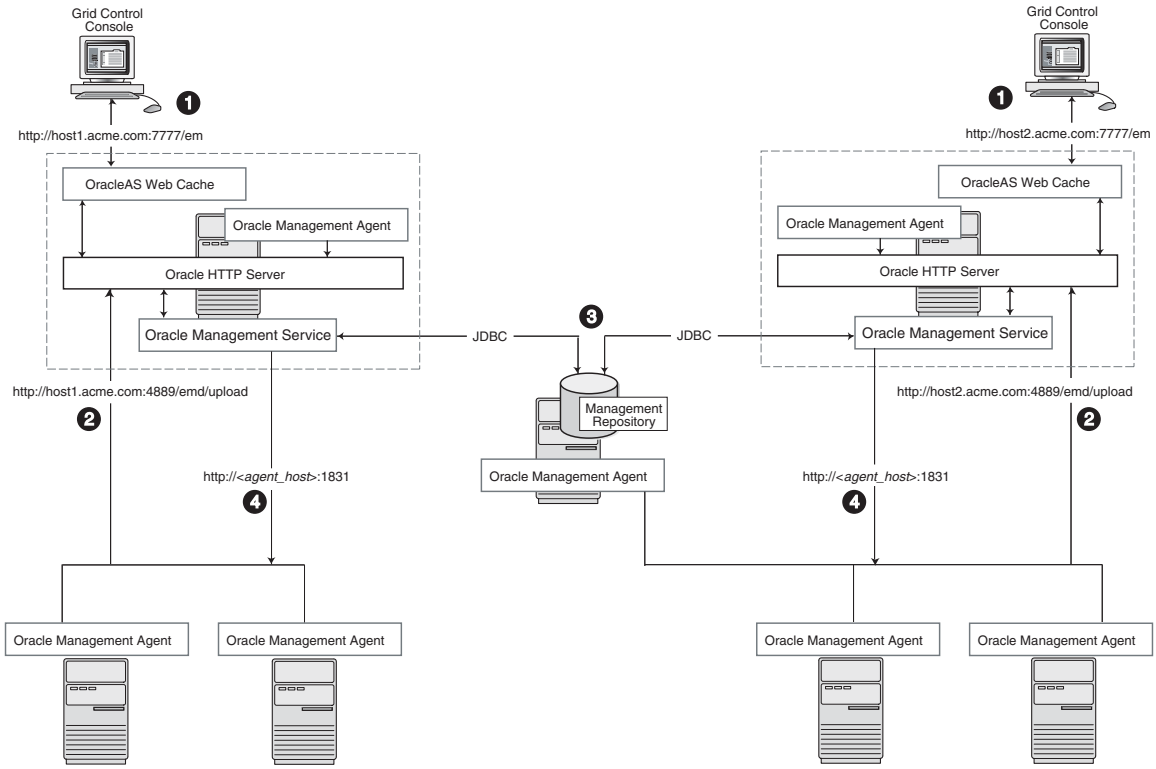
Consider adding additional Management Service installations if the response time of all pages is increasing over time or if the response time is unusually high for specific popular pages within the Grid Control Console.

Notes: You can use Application Service Level Management and Web Application targets to monitor your own Web applications. For more information, see Chapter 6, "Configuring Application Service Level Management"

3.5.2 Understanding the Flow of Management Data When Using Multiple Management Services

Figure 3–3 shows a typical environment where an additional Management Service has been added to improve the performance of the Grid Control environment.

Figure 3–3 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 hostname and port in the URL, the Grid Control Console obtains data from the Management Service (via 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 via Oracle HTTP Server, bypassing OracleAS Web Cache.

3. Each Management Service communicates via 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 via the unique Management Agent URL assigned to each Management Agent.

   As described in Section 3.3, 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.

3.6 High Availability Configurations

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.

One way to protect your Grid Control components is to use high availability software deployment techniques, which usually involve the deployment of hardware server load balancers, Oracle Real Application Clusters, and Oracle Data Guard.

Note: The following sections do not provide a comprehensive set of instructions for configuring Grid Control for high availability. The examples here are shown only to provide examples of some common configurations of Grid Control components. These examples are designed to help you understand some of your options when you deploy Grid Control in your environment.

For a complete discussion of configuring Oracle products for high availability, refer to *Oracle High Availability Architecture and Best Practices*

Refer to the following sections for more information about common Grid Control configurations that take advantage of high availability hardware and software solutions:

- Load Balancing Connections Between Management Agent and the Management Service
- Load Balancing Connections Between the Grid Control Console and the Management Service
- Configuring the Management Repository for High Availability

3.6.1 Load Balancing Connections Between 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, you should be aware that 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 re-attempts to send the information later.

To protect against the situation where a Management Service is unavailable, you can use a server load balancer between the Management Agents and the Management Services.

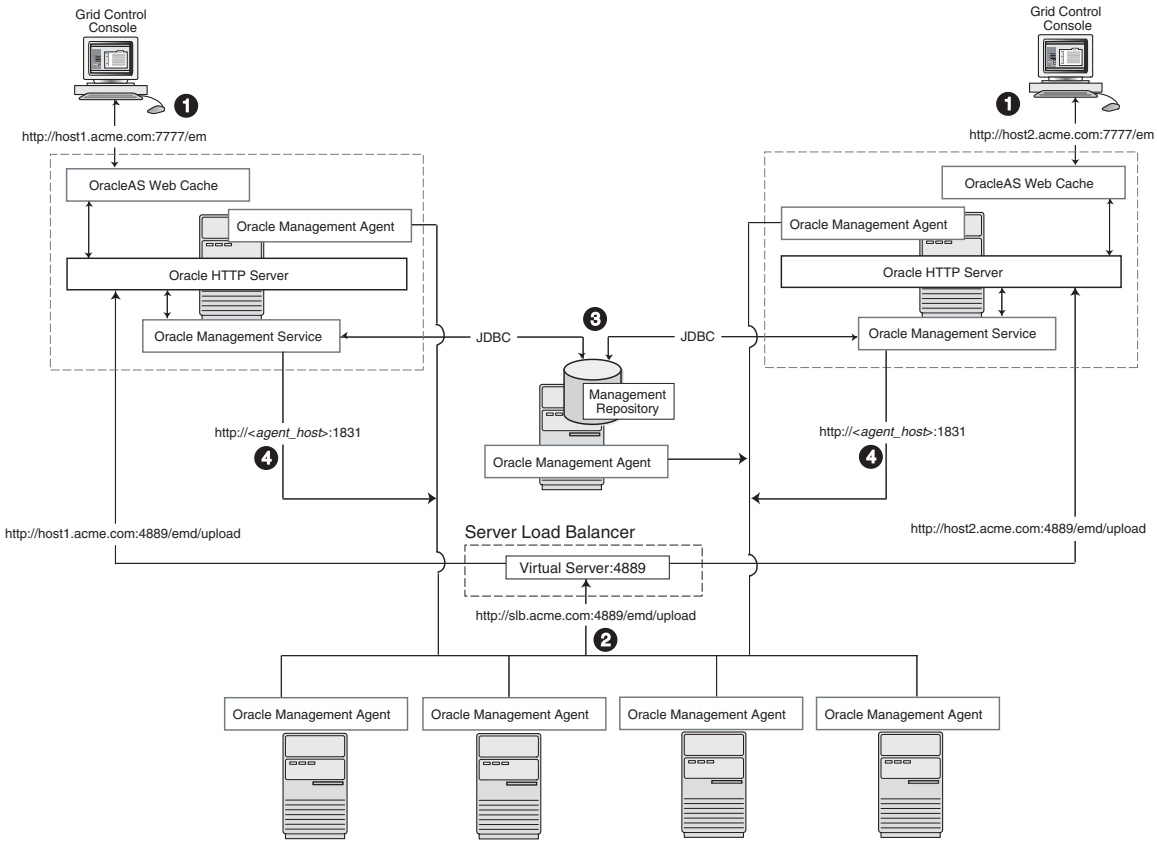
However, if you decide to implement such a configuration, be sure to review the following sections carefully before proceeding:

- Understanding the Flow of Data When Load Balancing the Upload of Management Data
- Configuring a Server Load Balancer for Management Agent Data Upload
- Important Considerations When Load Balancing the Upload of Management Data

3.6.1.1 Understanding the Flow of Data When Load Balancing the Upload of Management Data

Figure 3–4 shows a typical scenario where a set of Management Agents upload their data to a server load balancer, which redirects the data to one of two Management Service installations.

Figure 3–4 Load Balancing Between the Management Agent and the Management Service



In this example, only the upload of Management Agent data is routed through the server load balancer. The Grid Control Console still connects directly to a single Management Service via the unique Management Service upload URL.

When you load balance the upload of Management Agent data to multiple Management Service installations, the data is directed along the following paths:

1. Administrators can use one of two URLs to access the Grid Control Console just as they do in the multiple Management Service configuration defined in Section 3.5.
2. Each Management Agent uploads its data to a common server 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 server load balancer. The server load balancer routes the request to any one of a number of available servers that provide the requested service.

> **Caution:** Before deploying a server load balancer for the upload of Management Agent data, be sure to review Section 3.6.1.3, "Important Considerations When Load Balancing the Upload of Management Data"

3. Each Management Service communicates via JDBC with a common Management Repository, just as they do in the multiple Management Service configuration defined in Section 3.5.

4. Each Management Service communicates directly with each Management Agent via HTTP, just as they do in the multiple Management Service configuration defined in Section 3.5.

3.6.1.2 Configuring a Server Load Balancer for Management Agent Data Upload

This section describes some guidelines for configuring a server load balancer to balance the upload of data from Management Agents to multiple Management Service installations.

Specifically, you should use the administration tools that are packaged with your server load balancer to configure a virtual pool that consists of the hosts and the services that each host provides. In the case of the Management Services pool, specify the hostname and agent upload port. To insure a highly available Management Service, you should have two or more Management Services defined within the virtual pool.

Declare the pool such that any new connection between a Management Agent and the virtual pool member is persistent. This relationship is maintained and the Management Agent will upload to that the Management Service till the persistence period has elapsed or the Management Service is deemed to be inaccessible.

Modify the REPOSITORY_URL property in the `emd.properties` file located in the `sysman/config` directory of the Management Agent home directory. The hostname and port specified must be that of the server load balancer virtual service.

> **See Also:** "Configuring the Management Agent to Use a New Management Service" on page 9-1 for more information about modifying the REPOSITORY_URL property for a Management Agent

This configuration allows the Management Agent to make a permanent connection to a Management Service unless for some reason that Management Service becomes unavailable. In that event, the server load balancer will connect the agent to any surviving Management Service, based on the policies configured in the load balancer (for example, Round Robin or Least Loaded).

> **See Also:** Your Server Load Balancer documentation for more information on configuring virtual pools and load balancing policies

3.6.1.3 Important Considerations When Load Balancing the Upload of Management Data

The Grid Control architecture requires that collected monitoring data be loaded in chronological order. The Management Service, upon receipt of data, stores it temporarily in a local file and acknowledges receipt to the Management Agent. The Management Service then loads the data in a background thread in chronological order.

Should the data stored locally by the Management Service not get uploaded to the Management Repository, and the Management Agent attempts to upload the collected data to another Management Service, the new Management Service may upload data for data points more recent than was previously sent to the other host. As a result, the older data may never get loaded into the Management Repository and simply be discarded. This could result in potential holes in historic data.

To minimize this potential, you can:

- Carefully monitor the amount of data pending and waiting to be loaded into the Management Repository.

You can monitor this metric using the **Management System** tab in the Grid Control Console. If the loader backlog grows over time, consider adding additional Management Service installations to reduce the chance of losing data that is being uploaded to the Management Service installations.

See Also: "Monitoring the Load on Your Management Service Installations" on page 3-6

- Configure the server load balancer so that you maintain session affinity between each Management Agent and its Management Service.

  Session affinity assures you that no management data will be lost because no data will be uploaded to the Management Service and no data will be loaded into the Management Repository if the Management Service is suddenly unavailable. The Management Agent will wait until the assigned Management Service is available before it restarts the upload of data to the Management Service.

3.6.2 Load Balancing Connections Between the Grid Control Console and the Management Service

Using a server 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.

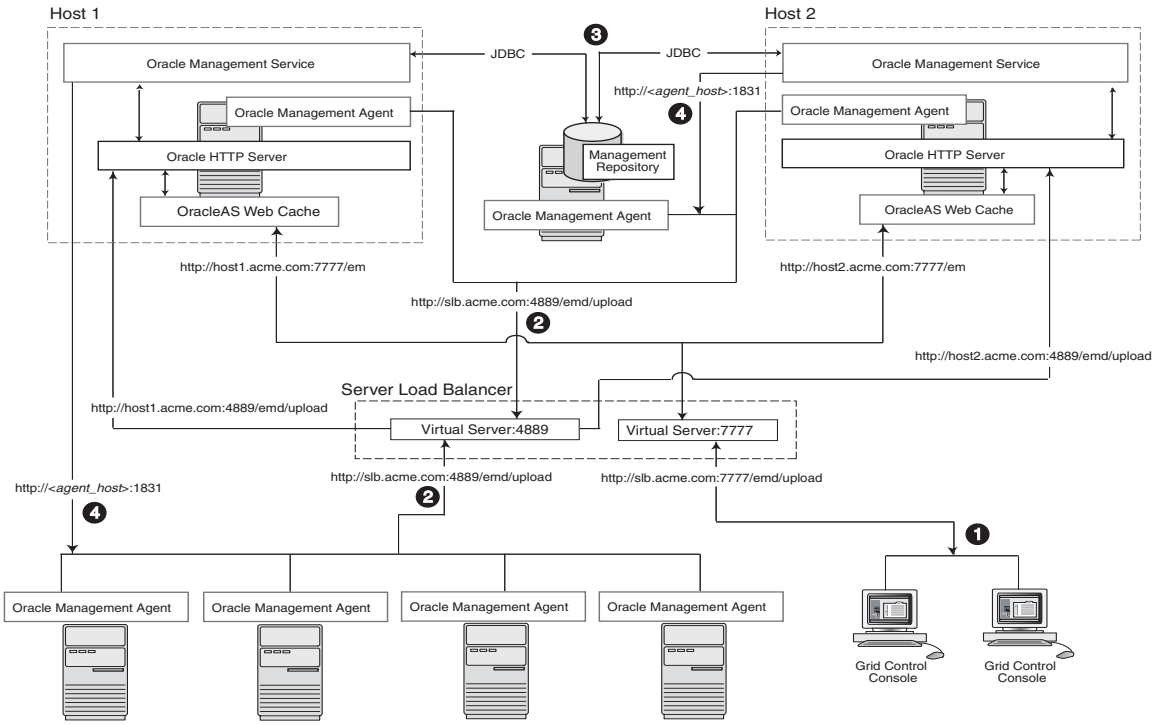
The following sections provide more information about this configuration:

- Understanding the Flow of Data When Load Balancing the Grid Control Console
- Configuring a Server Load Balancer for the Grid Control Console
- Configuring Oracle HTTP Server When Using a Load Balancer for the Grid Control Console

3.6.2.1 Understanding the Flow of Data When Load Balancing the Grid Control Console

Figure 3–5 shows a typical configuration where a server load balancer is used between the Management Agents and multiple Management Services, as well as between the Grid Control Console and multiple Management Service.

Figure 3–5 Load Balancing Between the Grid Control Console and the Management Service



In this example, a single server 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 server 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 server load balancer virtual service. The virtual service redirects the browser to one of the Management Service installations. Depending upon the hostname and port selected by the server load balancer from the virtual pool of Management Service installations, the Grid Control Console obtains the management data via 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 server load balancer URL as described in Section 3.6.1.

> **Caution:** Before deploying a server load balancer for the upload of Management Agent data, be sure to review Section 3.6.1.3, "Important Considerations When Load Balancing the Upload of Management Data"

3. Each Management Service communicates via JDBC with a common Management Repository, just as they do in the multiple Management Service configuration defined in Section 3.5.
4. Each Management Service communicates directly with each Management Agent via HTTP, just as they do in the multiple Management Service configuration defined in Section 3.5.

3.6.2.2 Configuring a Server Load Balancer for the Grid Control Console

Use the administration tools that are packaged with your server load balancer to configure a virtual pool that consists of the hosts and the services that each host provides. In the case of the Management Services pool, specify the hostname and default OracleAS Web Cache port. To insure a highly available Management Service, you should have two or more Management Services defined within the virtual pool.

The load balancer parcels the work to any number of Management Service processes that it has in its virtual pool. This provides a method for constant communication to the Grid Control Console in the event of the failure of a Management Service.

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 server load balancer. The monitor defines:

- The HTTP request that is to be sent to a Management Service
- The expected result in the event of success
- The 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`.

3.6.2.3 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 hostname, back to the client browser. The browser then uses that URL, which includes the Oracle HTTP Server hostname, 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 server load balancer.

To prevent the browser from bypassing the load balancer when a URL is redirected, edit the `ServerName` directive defined in the Oracle HTTP Server configuration file. This directive will be found in one of two places:

- If you have enabled Enterprise Manager Framework Security and you are running the Management Service in a secure environment (using HTTPS and SSL), the `ServerName` directive you must change is located in the following configuration file:

  ```
  ORACLE_HOME/Apache/Apache/conf/ssl.conf
  ```

- If you have not enabled Enterprise Manager Framework Security and you are running in an environment that is not secure (using HTTP), the `ServerName` directive you must change is located in the following configuration file:

  ```
  ORACLE_HOME/Apache/Apache/conf/httpd.conf
  ```

Change the `ServerName` directive so it matches the name of the server load balancer virtual service that you configured in Section 3.6.2.2.

See Also: *Oracle HTTP Server Administrator's Guide*

3.6.3 Configuring the Management Repository for High Availability

When you configure Grid Control for high availability, there are several ways to configure the Management Repository to prevent the loss of management data stored in the database.

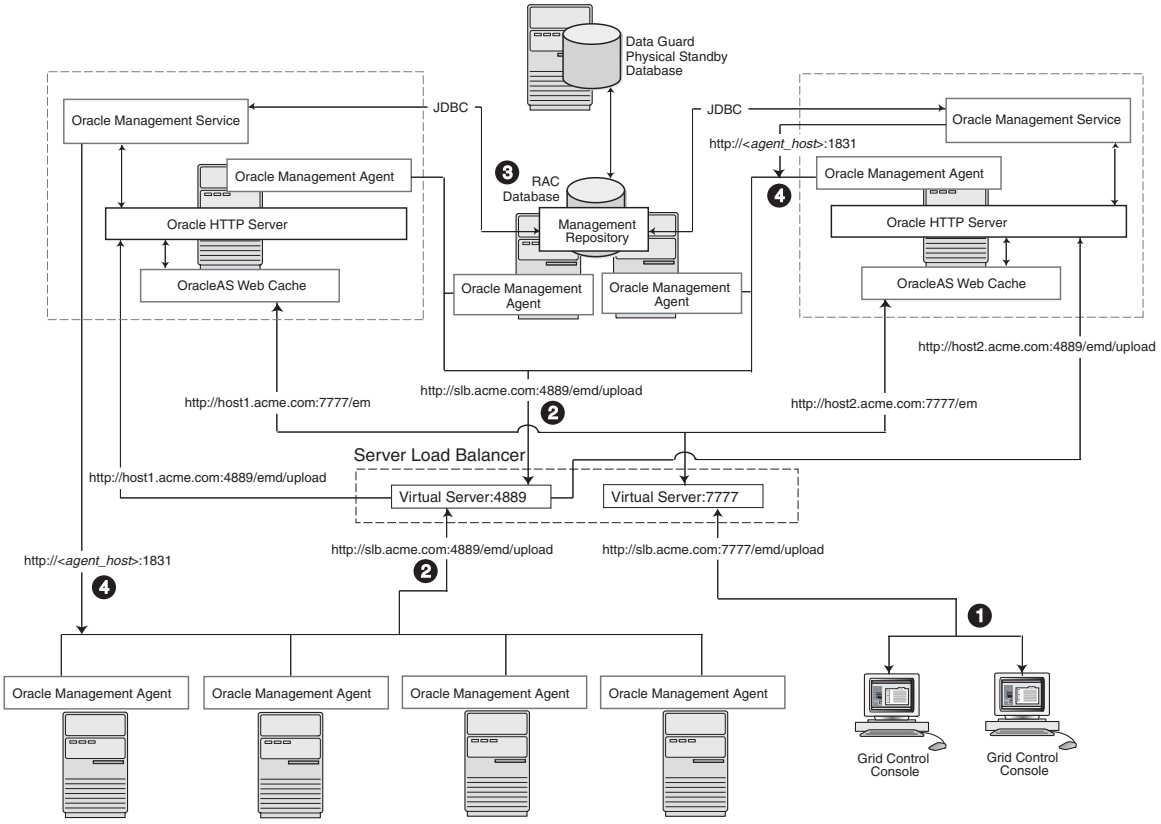
The following sections describe a typical configuration designed to safeguard your Management Repository:

- Understanding the Flow of Data When Configuring the Management Repository for High Availability
- Installing the Management Repository into a Real Applications Clusters (RAC) Instance
- Specifying the Size of the Management Repository Tablespaces in a RAC Database
- Configuring the Management Service to Use Oracle Net Load Balancing and Failover

3.6.3.1 Understanding the Flow of Data When Configuring the Management Repository for High Availability

Figure 3–6 shows a typical Grid Control high availability configuration, where server load balancers are balancing the load on the multiple Management Service installations and the Management Repository is protected by Oracle Real Application Clusters and Oracle Data Guard.

Figure 3–6 Grid Control High Availability Configuration



When you use install the Management Repository in a RAC database and incorporate Oracle Data Guard into the configuration, 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 server load balancer virtual service as described in Section 3.6.2.
2. Each Management Agent uploads its data to a common server load balancer URL as described in Section 3.6.1.

   Caution: Before deploying a server load balancer for the upload of Management Agent data, be sure to review Section 3.6.1.3, "Important Considerations When Load Balancing the Upload of Management Data"

3. Each Management Service communicates via JDBC with a common Management Repository, which is installed in a Real Application Clusters instance. Each Management Service uses the same database connection information, defined in the `emoms.properties` file, to load data from its 0s 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.

   See Also: "Configuring the Management Service to Use Oracle Net Load Balancing and Failover" on page 3-18 for information about configuring the connection to a Management Repository that is installed in a RAC database

   In addition, the Management Repository is also protected by Oracle Data Guard. Note that only physical Data Guard is supported for protecting the Management Repository.

   See Also: *Oracle Data Guard Concepts and Administration*

4. Each Management Service communicates directly with each Management Agent via HTTP, just as they do in the multiple Management Service configuration defined in Section 3.5.

3.6.3.2 Installing the Management Repository into a Real Applications Clusters (RAC) Instance

To install the Management Repository into a RAC instance, use the following procedure:

1. Install the Oracle9*i* Database Release 2 (9.2) software and create a RAC database.
2. Begin installing Grid Control, using the **Enterprise Manager 10g Grid Control Using an Existing Database** installation option.
3. When you are prompted for a database system identifier (SID) and port, specify the SID for one of the RAC instances.
4. After the Grid Control installation is complete, modify the Management Service connection string to take advantage of client failover in the event of a RAC host outage.

See Also: "Configuring the Management Service to Use Oracle Net Load Balancing and Failover" on page 3-18

3.6.3.3 Specifying the Size of the Management Repository Tablespaces in a RAC Database

When you install the Management Repository into a RAC database instance, you cannot set the size of the required Enterprise Manager tablespaces. You can, however, specify the name and location of data files to be used by the Management Repository schema. The default sizes for the initial data file extents depend on using the AUTOEXTEND feature and as such are insufficient for a production installation. This is particularly problematic when storage for the RAC database is on a raw device.

If the RAC database being used for the repository is configured with raw devices there are two options for increasing the size of the repository. You can create multiple raw partitions, with the first one equal to the default size of the tablespace as defined by the installation process. Alternatively, you can create the tablespace using the default size, create a dummy object that will increase the size of the tablespace to the end of the raw partition, then drop that object. Regardless, if raw devices are used, disable the default space management for these objects, which is to auto-extend.

3.6.3.4 Configuring the Management Service to Use Oracle Net Load Balancing and Failover

When you use a RAC cluster, a standby system, or both to provide high availability for the Management Repository, the Management Service can be configured to use an Oracle Net connect string that will take advantage of redundancy in the repository. Correctly configured, the Management service process will continue to process data from Agents even during a database node outage.

To configure the Management Service to take advantage of this feature:

1. Use a text editor to open the following configuration file in the Management Service home directory:

   ```
   ORACLE_HOME/sysman/config/emoms.properties
   ```

2. Locate the following entry in the `emoms.properties` file:

   ```
   oracle.sysman.eml.mntr.emdRepConnectDescriptor=
   ```

3. Edit the entry so it includes references to the individual nodes within the RAC database.

   The following example shows a connect string that supports a two-node RAC configuration. Note the backslash (\) before each equal sign (=), which is required when you are entering the connect string within the `emoms.properties` configuration file:

   ```
   oracle.sysman.eml.mntr.emdRepConnectDescriptor=(DESCRIPTION\=(ADDRESS_
   LIST\=(FAILOVER\=ON)(ADDRESS\=(PROTOCOL\=TCP)(HOST\=haem1.us.oracle.com)(PORT\=
   1521))(ADDRESS\=(PROTOCOL\=TCP)(HOST\=haem2.us.oracle.com)(PORT\=1521)))(CONNEC
   T_DATA\=(SERVICE_NAME\=em10)))
   ```

   See Also: "Enabling Advanced Features of Oracle Net Services" in the *Oracle9i Net Services Administrator's Guide* for more information about using the FAILOVER parameter and other advanced features within a database connect string

4

Enterprise Manager Security

This chapter describes how to configure Oracle Enterprise Manager Security. Specifically, this chapter contains the following sections:

4.1 About Oracle Enterprise Manager Security

Oracle Enterprise Manager provides tools and procedures to help you ensure that you are managing your Oracle environment in a secure manner. Oracle Enterprise Manager security can be divided into these categories:

- Security for the Oracle Enterprise Manager 10*g* Grid Control Console
- Security for the Oracle Enterprise Manager 10*g* Application Server Control Console

  See Also: *Oracle Application Server 10g Administrator's Guide* for information about securing the Oracle Enterprise Manager 10*g* Application Server Control Console

- Security for the Oracle Enterprise Manager 10*g* Database Control Console

The following sections describe the security features that apply to these categories.

4.1.1 Oracle Enterprise Manager Security Model

The goals of Oracle Enterprise Manager security are:

- To be sure that only users with the proper privileges have access to critical monitoring and administrative data.

  This goal is met by requiring username and password credentials before users can access the Enterprise Manager consoles. This includes access to the Oracle Enterprise Manager 10*g* Grid Control Console, the Oracle Enterprise Manager 10*g*

Database Control Console, and the Oracle Enterprise Manager 10*g* Application Server Control Console.

- To be sure that all data transferred between Enterprise Manager components is transferred in a secure manner and that all data gathered by each Oracle Management Agent can be transferred only to the Oracle Management Service for which the Agent is configured.

  This goal is met by enabling Enterprise Manager Framework Security. Enterprise Manager Framework Security automates the process of securing the Enterprise Manager components installed and configured on your network.

  See Also: "About Enterprise Manager Framework Security" on page 4-4

4.1.2 Classes of Users and Their Privileges

Oracle Enterprise Manager supports different classes of Oracle users, depending upon the environment you are managing and the context in which you are using Oracle Enterprise Manager 10*g*.

The types of users supported by Enterprise Manager vary depending upon the Enterprise Manager product you are using. For example:

- The Grid Control Console provides support for creating and managing Enterprise Manager administrator accounts.

  The Enterprise Manager administrators you create and manage in the Grid Control Console are granted privileges and roles to log in to the Grid Control Console and to manage specific target types and to perform specific management tasks.

  The default super administrator for the Grid Control Console is the SYSMAN user, which is a database user associated with the Oracle Management Repository. You define the password for the SYSMAN account during the Enterprise Manager installation procedure.

- Oracle Application Server administrators use the Oracle Application Server administrator account (`ias_admin`) to log in to the Application Server Control Console.

- You use the `ias_admin` account to manage the components of a specific Oracle Application Server instance. You define the password for the `ias_admin` account during the Oracle Application Server installation procedure.

- Oracle Database 10*g* administrators can use the SYS, SYSTEM, or SYSMAN database user accounts to log in to the Database Control.

  The SYSMAN database user is the default super administrator for managing Oracle Database 10*g*. You define the password for the SYSMAN account during the Oracle Database 10*g* installation procedure.

4.1.3 Resources Protected

By restricting access to privileged users and providing tools to secure communications between Oracle Enterprise Manager 10*g* components, Enterprise Manager protects critical information in the Oracle Management Repository.

The Management Repository contains management data that Enterprise Manager uses to help you monitor the performance and availability of your entire enterprise. This data provides you with information about the types of hardware and software you

have deployed, as well as the historical performance and specific characteristics of the applications, databases, applications servers, and other targets that you manage.

The Management Repository also contains information about the Enterprise Manager administrators who have the privileges to access the management data.

4.1.4 Authorization and Access Enforcement

Authorization and access enforcement for Enterprise Manager is controlled as follows:

- When you use the Grid Control Console, you create and manage Enterprise Manager administrator accounts. The SYSMAN super administrator can assign specific privileges and roles to each of the additional administrators. These privileges and roles control the targets an administrator can manage and the specific types of tasks the administrator can perform.

  See Also: "About Administrators and Roles" in the Enterprise Manager online help

- When you use the Application Server Control Console, access to the Console is restricted to administrators who use the `ias_admin` administrator's account. The `ias_admin` account is set up automatically and you assign a password for the account during the Oracle Application Server installation procedure.

  See Also: *Oracle Application Server 10g Administrator's Guide* for more information about the `ias_admin` account

- When you use the Oracle Enterprise Manager 10*g* Database Control Console, access and authorization for the Database Control is limited to specific database users who have been granted management privileges by the SYS, SYSTEM, or SYSMAN user.

  See Also: "About Administrators and Roles" in the Enterprise Manager online help

4.1.5 Leveraging Oracle Application Server Security Services

As a Web-based application, Enterprise Manager relies on industry-standard technologies to provide secure access to the Oracle Enterprise Manager 10*g* Grid Control Console, Database Control, and Application Server Control Console.

When you configure security for the Oracle Enterprise Manager 10*g* Grid Control Console, Enterprise Manager Framework Security provides secure communications between the components of your Enterprise Manager installation. However, you should also use the security services of your Oracle HTTP Server to be sure access to the Grid Control Console is secure.

See Also: "Configuring Security for Grid Control" on page 4-4 for more information about the Enterprise Manager Framework Security

Oracle HTTP Server Administrator's Guide for information about configuring security for your Oracle HTTP Server.

Enterprise Manager deploys the Application Server Control Console and Database Control within a single, standalone Oracle Application Server Containers for J2EE (OC4J) instance. As a result, when you configure security for the Application Server

Control Console, or for the Database Control, Enterprise Manager uses the standard security services of OC4J to protect your management data.

> **See Also:** "Configuring Security for the Enterprise Manager Application Server Control" on page 4-17

4.1.6 Leveraging Oracle Identity Management Infrastructure

Oracle Enterprise Manager 10*g* takes advantage of Oracle Identity Management in two ways:

- First, you can configure the Grid Control Console so it uses Oracle Application Server Single Sign-On. Administrators can then use their Single Sign-On credentials to log in to the Grid Control Console.

  Similarly, you can configure the Oracle Enterprise Manager 10*g* Database Control Console so it uses Oracle Application Server Single Sign-On credentials.

  > **See Also:** *Oracle Application Server Single Sign-On Administrator's Guide* for general information about Oracle Application Server Single Sign-On
  >
  > "Configuring Enterprise Manager for Use with Oracle Application Server Single Sign-On" on page 4-20

- Second, you can take advantage of the Enterprise User Security features of the Oracle database. Enterprise User Security provides single sign-on (SSO) or single password authentication for your database users.

  > **See Also:** "Managing Enterprise User Security" in the *Oracle Advanced Security Administrator's Guide*
  >
  > "Configuring Enterprise Manager for Use with Enterprise User Security" on page 4-24

4.2 Configuring Security for Grid Control

This section contains the following topics:

4.2.1 About Enterprise Manager Framework Security

Enterprise Manager Framework Security provides safe and secure communication channels between the components of Enterprise Manager. For example, Framework Security provides secure connections between your Oracle Management Service and its Management Agents.

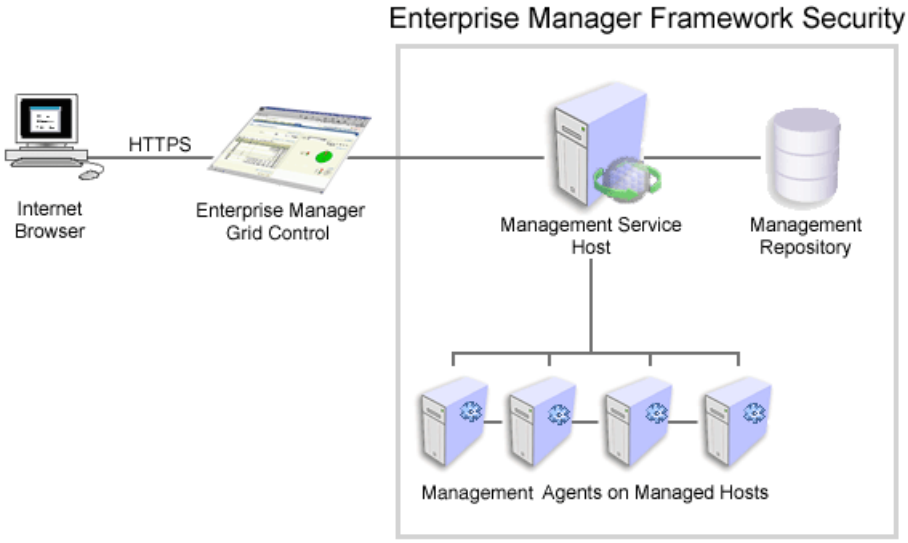
See Also: *Oracle Enterprise Manager Concepts* for an overview of Enterprise Manager components

Enterprise Manager Framework Security works in concert with—but does not replace—the security features you should enable for your Oracle HTTP Server. Oracle HTTP Server is part of the Oracle Application Server instance that is used to deploy the Management Service J2EE Web application.

See Also: *Oracle Application Server 10g Security Guide*

Figure 4–1 shows how Enterprise Manager Framework Security provides security for the connections between the Enterprise Manager components. However, the secure HTTPS connection between your browser and the Grid Control Console should be configured like any other Web application by using the security features of your Oracle HTTP Server.

Figure 4–1 Enterprise Manager Framework Security



Enterprise Manager Framework Security implements the following types of secure connections between the Enterprise Manager components:

- HTTPS and Public Key Infrastructure (PKI) components, including signed digital certificates, for communications between the Management Service and the Management Agents.

  See Also: *Oracle Security Overview* for an overview of Public Key Infrastructure features, such as digital certificates and public keys

- Oracle Advanced Security for communications between the Management Service and the Management Repository.

  See Also: *Oracle Advanced Security Administrator's Guide*

4.2.2 Overview of the Steps Required to Enable Enterprise Manager Framework Security

To enable Enterprise Manager Framework Security, you must configure each of the Enterprise Manager components in a specific order. The following list outlines the process for securing the Management Service and the Management Agents that upload data to the Management Service:

1. Use the `opmnctl stopall` command to stop the Management Service, the Oracle HTTP Server, and the other components of the Oracle Application Server that are used to deploy the Management Service.
2. Use `emctl secure oms` to enable security for the Management Service.
3. Restart the Management Service, the Oracle HTTP Server, OracleAS Web Cache, and the other application server components using the `opmnctl startall` command.
4. For each Management Agent, stop the Management Agent, use the `emctl secure agent` command to enable security for the Agent, and restart the Management Agent.
5. After security is enabled for all the Management Agents, use the `emctl secure lock` command to restrict HTTP Access to the Management Service. This will ensure that all data gathered from the Management Agents is uploaded over a secure HTTPS connection.

The following sections describe how to perform each of these steps in more detail.

4.2.3 Enabling Security for the Oracle Management Service

To enable Enterprise Manager Framework Security for the Management Service, you use the `emctl secure oms` utility, which is located in the following subdirectory of the Management Service home directory:

```
$ORACLE_HOME/bin
```

The `emctl secure oms` utility performs the following actions:

- Generates a Root Key within your Management Repository. The Root Key is used during distribution of Oracle Wallets containing unique digital certificates for your Agents.
- Modifies your Oracle HTTP Server to enable an HTTPS channel between your Management Service and Management Agents, independent from any existing HTTPS configuration that may be present in your Oracle HTTP Server.
- Enables your Management Service to accept requests from Management Agents using Enterprise Manager Framework Security.

To run the `emctl secure oms` utility you must first choose an Agent Registration Password. The Agent Registration password is used to validate that future installation sessions of Oracle Management Agents are authorized to load their data into this Enterprise Manager installation.

To enable Enterprise Manager Framework Security for the Oracle Management Service:

1. Change directory to the following directory in the Management Service home:

   ORACLE_HOME`/opmn/bin`

2. Stop the Management Service, the Oracle HTTP Server, and the other application server components using the following command:

   ```
   $PROMPT> ./opmnctl stopall
   ```

3. Change directory to the following directory in the Management Service home:

   ORACLE_HOME/bin

4. Enter the following command:

   ```
   $PROMPT> ./emctl secure oms
   ```

   Enterprise Manager prompts you for the Enterprise Manager Root Password.

5. Enter the password for the SYSMAN administrator account used for the Management Repository.

   Enterprise Manager prompts you to specify an Agent Registration Password, which is a new password that will be required for any Management Agents that attempt to connect to the Management Service.

6. Specify an Agent Registration Password for the Management Service.

   Enterprise Manager prompts you to confirm the hostname of the Management Service.

7. Enter the fuly qualified name of the host (including the domain) where the Management Service resides.

   The `emctl secure` utility reconfigures the Management Service to enable Framework Security. Example 4–1 shows a sample of the output you should receive from the `emctl secure oms` command.

8. When the operation is complete, restart the Management Service, the Oracle HTTP Server, and OracleAS Web Cache:

   ```
   $PROMPT> cd $ORACLE_HOME/opmn/bin
   $PROMPT> ./opmnctl startall
   ```

9. After the Management Service restarts, test the secure connection to the Management Service by browsing to the following secure URL using the HTTPS protocol:

   https://*hostname.domain*:4888/

   For example:

   ```
   https://mgmthost1.acme.com:4888/
   ```

   If the Management Service security has been enabled, your browser displays the Oracle Application Server Welcome page.

   The 4888 port number is the default secure port used by the Management Agents to upload data to the Management Service. This port number may vary if the default port is unavailable.

   See Also: "Viewing a Summary of the Ports Assigned During the Application Server Installation" on page 5-10

Caution: While the `emctl secure oms` command provides immediate HTTPS browser access to the Grid Control Console via the secure Management Agent upload port, it does not enable security for the default OracleAS Web Cache or Oracle HTTP Server ports that your administrators use to display the Grid Control Console.

To enable security for users who access the Grid Control through OracleAS Web Cache and the default Oracle HTTP Server ports, refer to *Oracle Application Server 10g Security Guide*.

Example 4–1 Sample Output of the emctl secure oms Command

```
$PROMPT> ./emctl secure oms
Oracle Enterprise Manager 10g Release 10.1.0.2.0.
Copyright (c) 1996, 2003 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root Password :
Enter Agent Registration password :
Enter a Hostname for this OMS : hsunnab14.us.oracle.com
Checking Repository...   Done.
Checking Repository for an existing Enterprise Manager Root Key...   Done.
Generating Enterprise Manager Root Key (this takes a minute)...   Done.
Fetching Root Certificate from the Repository...   Done.
Generating Registration Password Verifier in the Repository...   Done.
Generating Oracle Wallet Password for Enterprise Manager OMS...   Done.
Generating Oracle Wallet for Enterprise Manager OMS...   Done.
Generating Oracle Wallet for iAS HTTP Server...   Done.
Updating HTTPS port in emoms.properties file...   Done.
Generating Oracle Wallet Distribution Service...   Done.
Generating HTTPS Virtual Host for Enterprise Manager OMS...   Done.
```

Note: Alternatively, you can enter the `emctl secure oms` command all on one line, but if you enter the command on one line, the passwords you enter will be displayed on the screen as you type:

$PROMPT> emctl secure oms *sysman_pwd agent_reg_pwd*

4.2.4 Enabling Security for the Oracle Management Agent

When you install the Management Agent on a host, you must identify the Management Service that will be used by the Management Agent. If the Management Service you specify has been configured to take advantage of Enterprise Manager Framework Security, you will be prompted for the Agent Registration Password and Enterprise Manager Framework Security will be enabled for the Agent during the installation.

Otherwise, if the Management Service has not been configured for Enterprise Manager Framework Security, then security will not be enabled for the Management Agent. In those cases, you can later enable Enterprise Manager Framework Security for the Management Agent.

To enable Enterprise Manager Framework Security for the Management Agent, you use the `emctl secure agent` utility, which is located in the following directory of the Management Agent home directory:

AGENT_HOME/bin (UNIX)
AGENT_HOME\bin (Windows)

The `emctl secure agent` utility performs the following actions:

- Obtains an Oracle Wallet from the Management Service that contains a unique digital certificate for the Management Agent. This certificate is required in order for the Management Agent to conduct SSL communication with the secure Management Service.
- Obtains an Agent Key for the Management Agent that is registered with the Management Service.
- Configures the Management Agent so it is available on your network over HTTPS and so it uses the Management Service HTTPS upload URL for all its communication with the Management Service.

To enable Enterprise Manager Framework Security for the Management Agent:

1. Ensure that your Management Service and the Management Repository are up and running.
2. Change directory to the following directory:

   ```
   AGENT_HOME/bin (UNIX)
   AGENT_HOME\bin (Windows)
   ```

3. Stop the Management Agent:

   ```
   $PROMPT> ./emctl stop agent
   ```

4. Enter the following command:

   ```
   $PROMPT> ./emctl secure agent (UNIX)
   $PROMPT> emctl secure agent (Windows)
   ```

   The `emctl secure agent` utility prompts you for the Agent Registration Password, authenticates the password against the Management Service, and reconfigures the Management Agent to use Enterprise Manager Framework Security.

   Note: Alternatively, you can enter the command all on one line, but if you enter the command on one line, the password you enter will be displayed on the screen as you type:

   ```
   $PROMPT> ./emctl secure agent agent_registration_pwd (UNIX)
   $PROMPT> emctl secure agent agent_registration_pwd (Windows)
   ```

   Example 4–2 shows sample output of the `emctl secure agent` utility.

5. Restart the Management Agent:

   ```
   $PROMPT> ./emctl start agent
   ```

6. Confirm that the Management Agent is secure by checking the Management Agent home page.

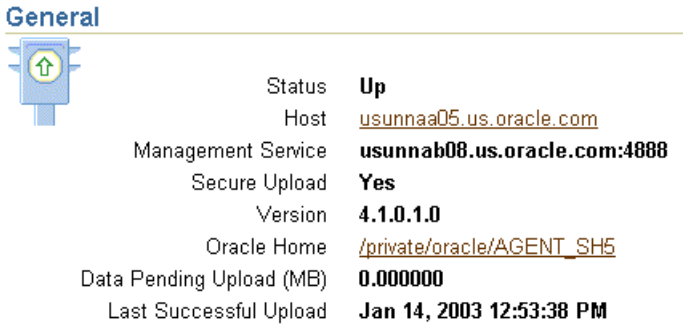
   In the General section of the Management Agent home page (Figure 4–2), the **Secure Upload** field indicates whether or not Enterprise Manager Framework Security has been enabled for the Management Agent.

   See Also: "Checking the Status of an Oracle Management Agent" in the Enterprise Manager online help

Example 4–2 Sample Output of the emctl secure agent Utility

```
$PROMPT> ./emctl secure agent
Oracle Enterprise Manager 10g Release 10.1.0.2.0.
Copyright (c) 1996, 2003 Oracle Corporation.  All rights reserved.
Enter Agent Registration password :
Requesting an HTTPS Upload URL from the OMS...   Done.
Requesting an Oracle Wallet and Agent Key from the OMS...   Done.
Check if HTTPS Upload URL is accessible from the agent...   Done.
Configuring Agent for HTTPS...   Done.
EMD_URL set in /private/oracle/agent/sysman/config/emd.properties
$PROMPT>
```

Figure 4–2 Secure Upload Field on the Management Agent Home Page



4.2.5 Enabling Security with Multiple Management Service Installations

If you already have a secure Management Service running and you install an additional Management Service that uses the same Management Repository, you will need to enable Enterprise Manager Framework Security for the new Management Service. This task is executed using the same procedure that you used to secure the first Management Service, by running the `emctl secure oms` utility.

Because you have already established at least one Agent Registration Password and a Root Key in your Management Repository, they must be used for your new Management Service. Your secure Management Agents can then operate against either Management Service.

All the registration passwords assigned to the current repository are listed on the Registration Passwords page in the Oracle Enterprise Manager 10*g* Grid Control Console.

See Also: "Managing Agent Registration Passwords" on page 4-12

If you install a new Management Service that uses a new Management Repository, the new New Management Service is considered to be a distinct enterprise. There is no way for the new Management Service to partake in the same security trust relationship as another Management Service that uses a different Management Repository. Secure Management Agents of one Management Service will not be able to operate against the other Management Service.

4.2.6 Restricting HTTP Access to the Management Service

By default, when you enable Enterprise Manager Framework Security on your Oracle Management Service there are no default restrictions on HTTP access. Any Oracle

Management Agent can access the Grid Control Console and Management Service using HTTP or HTTPS connections.

However, it is important that only secure Management Agent installations that use the Management Service HTTPS channel are able to upload data to your Management Repository.

To restrict access so Management Agents can upload data to the Management Service only over HTTPS:

1. Stop the Management Service, the Oracle HTTP Server, and the other application server components:

   ```
   $PROMPT> cd $ORACLE_HOME/opmn/bin
   $PROMPT> ./opmnctl stopall
   ```

2. Change directory to the following location in the Management Service home:

   ```
   $ORACLE_HOME/bin
   ```

3. Enter the following command to prevent Management Agents from uploading data to the Management Service over HTTP:

   ```
   $PROMPT> emctl secure lock
   ```

4. Restart the Management Service, the Oracle HTTP Server, and the other application server components:

   ```
   $PROMPT> cd $ORACLE_HOME/opmn/bin
   $PROMPT> ./opmnctl startall
   ```

5. Verify that you cannot access the Management Agent upload URL using the HTTP protocol:

   For example, navigate to the following URL:

   ```
   http://hostname.domain:4889/em/upload
   ```

   You should receive an error message similar to the following:

   ```
   Forbidden
   You don't have permission to access /em/upload on this server
   ```

6. Verify that you can access the Management Agent using the HTTPS protocol:

   For example, navigate to the following URL:

   ```
   https://hostname.domain:4888/em/upload
   ```

   You should receive the following message, which confirms the secure upload port is available to secure Management Agents:

   ```
   Http XML File receiver
   Http Recceiver Servlet active!
   ```

To remove the restriction for HTTPS uploads from the Management Agents, repeat the preceding procedure, but replace the emctl secure lock command with the following command:

```
$PROMPT> emctl secure unlock
```

Caution: The `emctl secure lock` command does not prevent users from accessing the Oracle Enterprise Manager 10*g* Grid Control Console over HTTP. It restricts non-secure access only for Management Agents that attempt to upload data to the Management Service using the upload URL, which is usually:

```
http://hostname.domain:4889/em/upload
```

To restrict HTTP access to the Oracle Enterprise Manager 10*g* Grid Control Console, configure your Oracle HTTP Server and OracleAS Web Cache as described in the Oracle Application Server documentation.

See Also: *Oracle HTTP Server Administrator's Guide*

4.2.7 Managing Agent Registration Passwords

Enterprise Manager uses the Agent Registration password to validate that installations of Oracle Management Agents are authorized to load their data into the proper Oracle Management Service.

You create the registration password when you use `emctl secure oms` to configure security for the Oracle Management Service installation.

4.2.7.1 Using the Grid Control Console to Manage Agent Registration Passwords

After you enable security for your Enterprise Manager components, you can use the Grid Control Console to manage your existing registration passwords or create additional registration passwords:

1. Click **Setup** at the top of any Grid Control Console page.
2. Click **Registration Passwords**.

   Enterprise Manager displays the Registration Passwords page (Figure 4–3). After you enable security for the Management Service, the registration password you created when you ran the `emctl secure oms` command appears in the Registration Passwords table.
3. Use the Registration Passwords page to change your registration password, create additional registration passwords, or remove registration passwords associated with the current Management Repository.

Figure 4–3 Managing Registration Passwords in the Grid Control Console

When you create or edit an Agent Registration Password on the Registration Passwords page, you can determine whether the password is persistent and available for multiple agents or to be used only once or for a predefined period of time.

For example, if an administrator requests to install a Management Agent on a particular host, you can create a one-time-only password that the administrator can use to install and configure one Management Agent.

On the other hand, you can create a persistent password that an administrator can use for the next two weeks before it expires and the administrator must ask for a new password.

4.2.7.2 Using emctl to Change the Agent Registration Password

To change an existing Agent Registration Password, use the following `emctl` command:

```
$PROMPT> emctl secure setpwd sysman_password new_Install_Password
```

Note that the `emctl secure setpwd` command requires that you provide the password of the Enterprise Manager super administrator user, `sysman`, to authorize the resetting of the Agent Registration Password.

If you change the Agent Registration Password, you must communicate the new password to other Enterprise Manager administrators who need to install new Management Agents, enable Enterprise Manager Framework Security for existing Management Agents, or install additional Management Services.

As with other security passwords, you should change the Agent Registration Password on a regular and frequent basis to prevent it from becoming too widespread.

4.2.8 Enabling Security for the Management Repository Database

This section describes how to enable Security for the Oracle Management Repository. This section includes the following topics:

- About Oracle Advanced Security and the sqlnet.ora Configuration File

- Configuring the Management Service to Connect to a Secure Management Repository Database
- Enabling Oracle Advanced Security for the Management Repository
- Enabling Security for the Management Agent that is Monitoring a Secure Management Repository or Database

4.2.8.1 About Oracle Advanced Security and the sqlnet.ora Configuration File

You enable security for the Management Repository by using Oracle Advanced Security. Oracle Advanced Security ensures the security of data transferred to and from an Oracle database.

> **See Also:** *Oracle Advanced Security Administrator's Guide*

To enable Oracle Advanced Security for the Management Repository database, you must make modifications to the `sqlnet.ora` configuration file. The `sqlnet.ora` configuration file is used to define various database connection properties, including Oracle Advanced Security parameters.

The sqlnet.ora file is located in the following subdirectory of the Database home:

ORACLE_HOME`/network/admin`

After you have enabled Security for the Management Repository and the Management Services that communicate with the Management Repository, you must also configure Oracle Advanced Security for the Management Agent by modifying the `sqlnet.ora` configuration file in the Management Agent home directory.

> **See Also:** "Enabling Security for the Management Agent that is Monitoring a Secure Management Repository or Database" on page 4-17

It is important that both the Management Service and the Management Repository are configured to use Oracle Advanced Security. Otherwise, errors will occur when the Management Service attempts to connect to the Repository. For example, the Management Service might receive the following error:

```
ORA-12645: Parameter does not exist
```

To correct this problem, be sure both the Management Service and the Management Repository are configured as described in the following sections.

Note: The procedures in this section describe how to manually modify the `sqlnet.ora` configuration file to enable Oracle Advanced Security. Alternatively, you can make these modifications using the administration tools described in the *Oracle Advanced Security Administrator's Guide*.

4.2.8.2 Configuring the Management Service to Connect to a Secure Management Repository Database

If you have enabled Oracle Advanced Security for the Management Service database—or if you plan to enable Oracle Advanced Security for the Management Repository database—use the following procedure to enable Oracle Advanced Security for the Management Service:

1. Stop the Management Service:

   ```
   $PROMPT> ORACLE_HOME/bin/emctl stop oms
   ```

2. Locate the following configuration file in the Management Service home directory:

   ORACLE_HOME/network/admin/emoms.properties

3. Using a text editor, add the entries described in Table 4–1 to the `emoms.properties` file.

   The entries described in the table correspond to valid parameters you can set when you configure network data encryption for the Oracle Database.

   > **See Also:** "Configuring Network Data Encryption and Integrity for Oracle Servers and Clients" in the *Oracle Application Server 10g Administrator's Guide*

4. Save your changes and exit the text editor.
5. Restart the Management Service.

   > **See Also:** "Starting and Stopping Oracle Enterprise Manager 10g Grid Control" on page 2-10

Table 4–1 Oracle Advanced Security Properties in the Enterprise Manager Properties File

Property	Description
oracle.sysman.emRep.dbConn.enableEncryption	Defines whether or not Enterprise Manager will use encryption between Management Service and Management Repository. Possible values are TRUE and FALSE. The default value is FALSE. For example: `oracle.sysman.emRep.dbConn.enableEncryption=true`
oracle.net.encryption_client	Defines the Management Service encryption requirement. Possible values are REJECTED, ACCEPTED, REQUESTED, REQUIRED. The default value is REQUESTED. In other words, if the database supports secure connections, then the Management Service uses secure connections, otherwise the Management Service uses insecure connections. For example: `oracle.net.encryption_client=REQUESTED`

Table 4–1 (Cont.) Oracle Advanced Security Properties in the Enterprise Manager Properties File

Property	Description
oracle.net.encryption_types_client	Defines the different types of encryption algorithms the client supports. Possible values should be listed within parenthesis. The default value is `( DES40C )`. For example: `oracle.net.encryption_types_client= ( DES40C )`
oracle.net.crypto_checksum_client	Defines the Client's checksum requirements. Possible values are REJECTED, ACCEPTED, REQUESTED, REQUIRED. The default value is REQUESTED. In other words, if the server supports checksum enabled connections, then the Management Service uses them, otherwise it uses normal connections. For example: `oracle.net.crypto_checksum_client=REQUESTED`
oracle.net.crypto_checksum_types_client	This property defines the different types of checksums algorithms the client supports. Possible values should be listed within parentheses. The default value is (MD5). For example: `oracle.net.crypto_checksum_types_client= ( MD5 )`

4.2.8.3 Enabling Oracle Advanced Security for the Management Repository

To be sure your database is secure and that only encrypted data is transferred between your database server and other sources, review the security documentation available in the Oracle Database 10*g* documentation library.

See Also: *Oracle Advanced Security Administrator's Guide*

The following instructions provide an example of how you can confirm that Oracle Advanced Security is enabled for your Management Repository database and its connections with the Management Service:

1. Locate the `sqlnet.ora` configuration file in the following directory of the database Oracle Home:

   ```
   ORACLE_HOME/network/admin
   ```

2. Using a text editor, look for the following entries (or similar entries) in the `sqlnet.ora` file:

   ```
   SQLNET.ENCRYPTION_SERVER = REQUESTED
   SQLNET.CRYPTO_SEED = "abcdefg123456789"
   ```

> **See Also:** "Configuring Network Data Encryption and Integrity for Oracle Servers and Clients" in the *Oracle Application Server 10g Administrator's Guide*

3. Save your changes and exit the text editor.

4.2.8.4 Enabling Security for the Management Agent that is Monitoring a Secure Management Repository or Database

After you have enabled Oracle Advanced Security for the Management Repository, you must also enable Advanced Security for the Management Agent that is monitoring the repository:

1. Locate the `sqlnet.ora` configuration file in the following directory inside the home directory for the Management Agent that is monitoring the Management Repository:

   AGENT_HOME`/network/admin (UNIX)`
   AGENT_HOME`\network\admin (Windows)`

2. Using a text editor, add the following entry to the `sqlnet.ora` configuration file:

   ```
   SQLNET.CRYPTO_SEED = "abcdefg123456789"
   ```

   > **See Also:** "Configuring Network Data Encryption and Integrity for Oracle Servers and Clients" in the *Oracle Application Server 10g Administrator's Guide*

3. Save your changes and exit the text editor.
4. Restart the Management Agent.

   > **See Also:** "Controlling the Oracle Management Agent" on page 2-1

4.3 Configuring Security for the Enterprise Manager Application Server Control

When you install Oracle Application Server 10*g* Release 2 (9.0.4), the installation procedure also installs and configures Oracle Enterprise Manager 10*g* Application Server Control, which you use to manage your application server instances.

> **See Also:** "Introduction to Administration Tools" in the *Oracle Application Server 10g Administrator's Guide* for more information about using the Application Server Control Console

The Application Server Control Console relies on several underlying technologies, including a version of the Oracle Management Agent that is designed to provide monitoring data to the Application Server Control Console.

By default, you access the Application Server Control Console through your Web browser using the non-secure, HTTP protocol. In addition, communications between the local Oracle Management Agent and the Application Server Control Console are transferred over an insecure HTTP connection.

To secure the communications between the Management Agent and the Application Server Control, and to provide HTTPS access to the Application Server Control Console, Enterprise Manager provides the `emctl secure em` command-line utility.

The `emctl secure em` utility enables HTTPS and Public Key Infrastructure (PKI) components, including signed digital certificates, for communications between the Application Server Control and the local Management Agent.

> **Caution:** Before you use the `emctl secure agent` command to secure the Application Server Control Console, be sure to stop the Application Server Control Console.

To configure security for the Application Server Control, use the following procedure:

1. Stop the Application Server Control Console by entering the following command in the `IAS_HOME/bin` directory:

   ```
   $PROMPT> ./emctl stop iasconsole
   ```

2. Enter the following command in the `ORACLE_HOME/bin` directory:

   ```
   $PROMPT> ./emctl secure em
   ```

   Enterprise Manager secures the Application Server Control Console. Sample output of the `emctl secure em` command is shown in Example 4–3.

3. Start the Application Server Control Console by entering the following command in the `IAS_HOME/bin` directory:

   ```
   $PROMPT> ./emctl start iasconsole
   ```

4. Test the security of the Application Server Control Console by entering the following URL in your Web browser:

   ```
   https://hostname:port/
   ```

   For example:

   ```
   https://mgmthost1:1812/
   ```

Example 4–3 Sample Output from the emctl secure em Command

```
$PROMPT> ./emctl secure em
Oracle Enterprise Manager 9.0.4
Copyright (c) 2002, 2003 Oracle Corporation.  All rights reserved.
Generating Standalone Console Root Key (this takes a minute)...   Done.
Fetching Standalone Console Root Certificate...   Done.
Generating Standalone Console Agent Key...   Done.
Generating Oracle Wallet for the Standalone Console Agent...   Done.
Configuring Agent for HTTPS...   Done.
EMD_URL set in /dsk01/oracle/appserver1/sysman/config/emd.properties
Generating Standalone Console Java Keystore...   Done.
$PROMPT>
```

4.4 Configuring Security for the Database Control

This section describes the architecture and configuration of security for the Oracle Enterprise Manager 10*g* Grid Control.

> **See Also:** *Oracle Database Security Guide* for an overview of Oracle Database 10*g* security features

Oracle strongly recommends that you use the Secure Socket Layer (SSL) protocol and HTTPS for all connections to Enterprise Manager and that you use a valid digital security certificate.

To configure security for the Database Control:

1. Stop the Database Control by entering the following command in the `ORACLE_HOME/bin` directory (UNIX) or the `ORACLE_HOME\bin` (Windows):

   ```
   $PROMPT> ./emctl stop dbconsole (UNIX)
   $PROMPT> emctl stop dbconsole (Windows)
   ```

   See Also: "Controlling the Database Control on UNIX" on page 2-8

   "Starting and Stopping the Database Control on Windows" on page 2-8

2. Change directory to the `ORACLE_HOME/bin` directory or the `ORACLE_HOME\bin` (Windows) and enter the following emctl command

   ```
   $PROMPT> ./emctl secure dbconsole (UNIX)
   $PROMPT> emctl secure dbconsole (Windows)
   ```

   Enterprise Manager prompts you for the Enterprise Manager Root Password.

3. Enter the password for the SYSMAN database user.

   Enterprise Manager prompts you to specify an Agent Registration Password, which is a new password that will be required for any Management Agents that attempt to connect to the Management Service.

4. Specify an Agent Registration Password for the Management Service.

   Enterprise Manager prompts you to confirm the hostname of the Management Service.

5. Enter the name of the host where the Management Service resides.

   The `emctl secure` utility reconfigures the Management Service to enable Framework Security. If the Management Service is up and running, Enterprise Manager restarts the Management Service.

   When the operation is complete, communications between the Enterprise Manager components is secure.

   In addition, you can access the Grid Control Console using the HTTPS protocol.

6. Start the Database Control by entering the following command in the `ORACLE_HOME/bin` directory or the `ORACLE_HOME\bin` (Windows):

   ```
   $PROMPT> ./emctl start dbconsole (UNIX)
   $PROMPT> emctl start dbconsole (Windows)
   ```

   See Also: "Controlling the Database Control on UNIX" on page 2-8

7. Test the security of the Database Control by entering the following URL in your Web browser:

   ```
   https://hostname:port/em
   ```

   For example:

   ```
   https://dbhost1:1820/em
   ```

Note: Alternatively, you can enter the `emctl secure dbconsole` command all on one line, but if you enter the command on one line, the passwords you enter will be displayed on the screen as you type:

$PROMPT> emctl secure dbconsole *sysman_pwd agent_reg_pwd*

4.5 Configuring Enterprise Manager for Use with Oracle Application Server Single Sign-On

If you are currently using Oracle Application Server Single Sign-On to control access and authorization for your enterprise, you can extend those capabilities to the Grid Control Console.

By default, when you navigate to the Grid Control Console, Enterprise Manager displays the Enterprise Manager login page. However, you can configure Enterprise Manager so it uses Oracle Application Server Single Sign-On to authorize your Grid Control Console users. Instead of seeing the Enterprise Manager login page, Grid Control Console users will see the standard Oracle Application Server Single Sign-On login page. From the login page, administrators can use their Oracle Application Server Single Sign-On credentials to access the Oracle Enterprise Manager 10*g* Grid Control Console.

The following sections describe how to configure Enterprise Manager as a OracleAS Single Sign-On Partner Application:

- Configuring Enterprise Manager to Use the Single Sign-On Logon Page
- Registering Single Sign-On Users as Enterprise Manager Administrators
- Grid Control as a Single Sign-On Partner Application
- Bypassing the Single Sign-On Logon Page

4.5.1 Configuring Enterprise Manager to Use the Single Sign-On Logon Page

To configure the Grid Control Console for use with Oracle Application Server Single Sign-On:

1. Set the ORACLE_HOME environment variables to the Management Service home directory.

   For example:

   ```
   $PROMPT> setenv ORACLE_HOME /dev01/oracle/em10g_GridControl
   ```

2. Change directory to the bin directory of the Management Service Oracle home:

   ```
   $PROMPT> cd $ORACLE_HOME/opmn/bin
   ```

3. Stop the Management Service, the Oracle HTTP Server, and the other components of the application server:

   ```
   $PROMPT> ./opmnctl stopall
   ```

4. Change directory to the bin directory of the Management Service Oracle home:

   ```
   $PROMPT> cd $ORACLE_HOME/bin
   ```

5. Enter the following command at the operating system prompt:

```
$PROMPT> ./emctl config oms sso -host ssoHost -port ssoPort -sid ssoSid  -pass
ssoPassword -das http://ssohost:port/
```

For example:

```
$PROMPT> ./emctl config oms sso -host sshost1.acme.com -port 1521 -sid asdb
-pass Ch22x5xt -das http://ssohost1.acme.com:7777
```

Table Table 4–2 describes the arguments on the `emctl config oms sso` command line.

Example 4–4 shows the typical output generated by the `emctl config oms sso` command.

6. Restart the Management Service, Oracle HTTP Server, and the other application server components:

```
$PROMPT> cd $ORACLE_HOME/opmn/bin
$PROMPT> ./opmnctl startall
```

7. Go the Grid Control Console URL.

For example:

```
http://mgmthost1.acme.com:7777/em
```

The browser is redirected to the standard Single Sign-On Logon page.

Table 4–2 Arguments for the emctl sso Command

Argument	Description
-host	The name of the host computer where the Oracle Application Server Single Sign-On server resides. Be sure to use the fully-qualified host name.
-port	The port for the Oracle Application Server Single Sign-On database. For example, 1521.
-sid	The system identifier (SID) for the Oracle Application Server Single Sign-On database.
-pass	The password for the Oracle Application Server Single Sign-On schema (`orasso`). The orasso schema password is randomized when the Oracle Application Server infrastructure is installed. To obtain the password, see "Obtaining the Single Sign-On Schema Password" in the *Oracle Application Server Single Sign-On Administrator's Guide*.
-das	The URL containing the host and port for the Delegated Administration Service (DAS). Generally, the DAS hostname and port are the same as the hostname and port of the Oracle Application Server Single Sign-On server. For example: `http://mgmthost1.acme.com:7777`

Example 4–4 Sample Output of the emctl config oms sso Command

```
$PROMPT> ../opmn/bin/opmnctl stopall
opmnctl: stopping opmn and all managed processes...
$PROMPT> ./emctl config oms sso -host mgmthost1.acme.com -port 1521 -sid asdb
-pass E9p36Yst -das http://mgmthost1.acme.com:7777
Oracle Enterprise Manager 10g Release 10.1.0.2.0.
Copyright (c) 1996, 2003 Oracle Corporation.  All rights reserved.
/private/oracle/em10gRel5a/Apache/Apache/conf/httpd.conf has already been
set to enable SSO.
```

```
/private/oracle/em10gRel5a/sysman/config/emoms.properties has been modified.
Registering to SSO server, please wait...
Parameters passed to SSO registration tool :
param0:-oracle_home_path param1:/private/oracle/em10gRel5a param2:-host
param3:mgmthost1.acme.com param4:-port param5:1521 param6:-sid param7:asdb
param8:-schema param9:orasso param10:-pass param11:E9p36Yst param12:-site_name
param13:ssohost2.acme.com:7777 param14:-success_url
param15:http://ssohost2.acme.com:7777/osso_login_success param16:-logout_url
param17:http://ssohost2.acme.com:7777/osso_logout_success param18:-cancel_url
param19:http://ssohost2.acme.com:7777/ param20:-home_url
param21:http://ssohost2.acme.com:7777/ param22:-config_mod_osso param23:TRUE
param24:-u param25:oracle param26:-sso_server_version param27:v1.2
-DinstallType=
-DoldOracleHome=
-DoldOHSUser=root
Check /private/oracle/em10gRel5a/sso/log/ssoreg.log for the result of registration
$PROMPT> ../opmn/bin/opmnctl startall
opmnctl: starting opmn and all managed processes...
$PROMPT>
```

4.5.2 Registering Single Sign-On Users as Enterprise Manager Administrators

After you have configured Enterprise Manager to use the Single Sign-On logon page, you can register any Single Sign-On user as an Enterprise Manager administrator:

1. Go the Grid Control Console URL.

   For example:

   ```
   http://mgmthost1.acme.com:7777/em
   ```

   The browser is redirected to the standard Single Sign-On Logon page.

2. Enter the credentials for a valid Single Sign-On user.

   If the Single Sign-On user is not an Enterprise Manager administrator, the browser is redirected to a modified version of the Enterprise Manager logon page (Figure 4–4).

3. Log in to Enterprise Manager as a Super Administrator.

4. Click **Setup** and then click **Administrators** to display the Administrators page.

   > **See Also:** "Creating, Editing, and Viewing Administrators" in the Enterprise Manager online help

   Because Enterprise Manager has been configured to use Single Sign-On, the first page in the Create Administrator wizard now offers you the option of creating an administrator based on a registered Oracle Internet Directory user (Figure 4–5).

5. Select **Oracle Internet Directory** and advance to the next page in the wizard.

6. Enter the name and email address of the Oracle Internet Directory user, or click the flashlight icon to search for a user name in the Oracle Internet Directory.

7. Use the rest of the wizard pages to define the roles, system privileges, and other characteristics of the Enterprise Manager administrator and then click **Finish**.

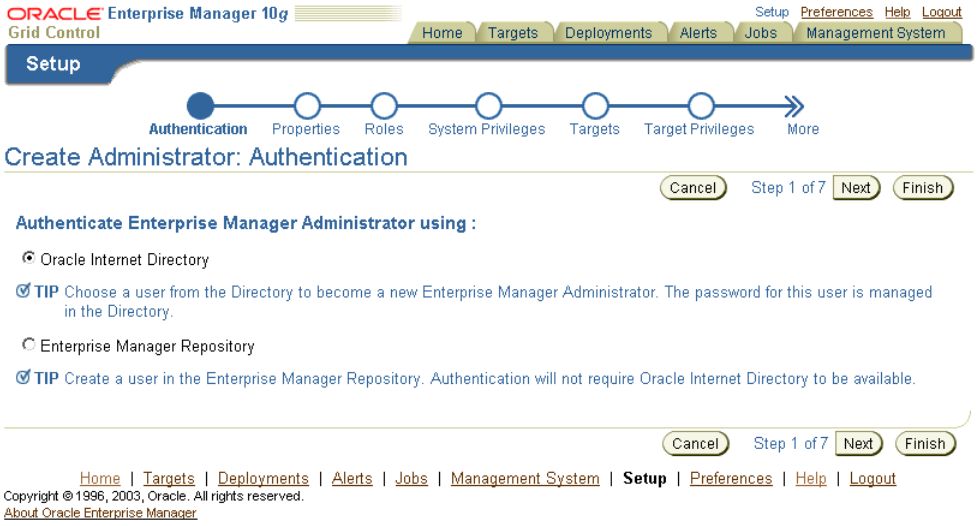
   Enterprise Manager displays a summary page that lists the characteristics of the administrator account.

8. Click **Finish** to create the new Enterprise Manager administrator.

The OID user is now included in the list of Enterprise Manager administrators. You can now verify the account by logging out of the Grid Control Console and logging back in using the OID user credentials on the Single Sign-On logon page.

Figure 4–4 Modified Enterprise Manager Logon Page When Configuring SSO

Figure 4–5 Create Administrator Page When SSO Support Is Enabled



4.5.3 Grid Control as a Single Sign-On Partner Application

The `emctl config oms sso` command adds the Oracle Enterprise Manager 10*g* Grid Control Console as an Oracle Application Server Single Sign-On partner application. Partner applications are those applications that have delegated authentication to the Oracle Application Server Single Sign-On Server.

To see the list of partner applications, navigate to the following URL:

`http://`*`hostname`*`:`*`port`*`/pls/orasso/orasso.home`

For example:

```
http://ssohost1.acme.com:7777/pls/orasso/orasso.home
```

4.5.4 Bypassing the Single Sign-On Logon Page

After you configure Enterprise Manager to use the Single Sign-On logon page, you can bypass the Single Sign-On page at any time and go directly to the Enterprise Manager logon page by entering the following URL:

```
http://hostname.domain:port/em/console/logon/logon
```

For example:

```
http://mgmthost1.acme.com:7777/em/console/logon/logon
```

4.6 Configuring Enterprise Manager for Use with Enterprise User Security

Enterprise User Security enables you to create and store Oracle9i database information as directory objects in an LDAP-compliant directory server. For example, an administrator can create and store enterprise users and roles for the Oracle9i database in the directory, which helps centralize the administration of users and roles across multiple databases.

> **See Also:** "Enterprise User Security Configuration Tasks and Troubleshooting" in the *Oracle Advanced Security Administrator's Guide*

If you currently use Enterprise User Security for all your Oracle9i databases, you can extend this feature to Enterprise Manager. Configuring Enterprise Manager for use with Enterprise User Security simplifies the process of logging in to database targets you are managing with the Oracle Enterprise Manager 10*g* Grid Control Console.

To configure Enterprise Manager for use with Enterprise User Security:

1. Ensure that you have enabled Enterprise User Security for your Oracle Management Repository database, as well as the database targets you will be managing with the Grid Control Console.
2. Stop the Oracle Management Service.

   > **See Also:** "Controlling the Oracle Management Service" on page 2-4

3. Change directory to the `IAS_HOME/sysman/config` directory and open the `emoms.properties` file with your favorite text editor.
4. Add the following entry in the `emoms.properties` file:

   ```
   oracle.sysman.emSDK.sec.DirectoryAuthenticationType=EnterpriseUser
   ```

5. Save and close the `emoms.properties` file.
6. Start the Management Service.

The next time you use the Oracle Enterprise Manager 10*g* Grid Control Console to drill down to a managed database, Enterprise Manager will attempt to connect to the database using Enterprise User Security. If successful, Enterprise Manager will connect you to the database without displaying a login page. If the attempt to use Enterprise User Security fails, Enterprise Manager will prompt you for the database credentials.

4.7 Additional Security Considerations

After you enable security for the Enterprise Manager components and framework, thee are additional security considerations. This section provides the following topics:

- Responding to Browser-Specific Security Certificate Alerts
- Configuring Beacons to Monitor Web Applications Over HTTPS

4.7.1 Responding to Browser-Specific Security Certificate Alerts

This section describes how to respond to browser-specific security alert dialog boxes when you are using Enterprise Manager in a secure environment.

The security alert dialog boxes described in this section should appear only if you have enabled Enterprise Manager Framework Security, but you have not completed the more extensive procedures to secure your Oracle HTTP Server properly.

> **See Also:** *Oracle Application Server 10g Security Guide*

This section contains the following topics:

- Responding to the Internet Explorer Security Alert Dialog Box
- Responding to the Netscape Navigator New Site Certificate Dialog Box
- Preventing the Display of the Internet Explorer Security Information Dialog Box

4.7.1.1 Responding to the Internet Explorer Security Alert Dialog Box

If you enable security for the Management Service, but you do not enable the more extensive security features of your Oracle HTTP Server, you will likely receive a Security Alert dialog box similar to the one shown in Figure 4–6 when you first attempt to display the Grid Control Console using the HTTPS URL in Internet Explorer.

> **Note:** The instructions in this section apply to Internet Explorer 5.5. The instructions may vary for other supported browsers.

Figure 4–6 Internet Explorer Security Alert Dialog Box

When Internet Explorer displays the Security Alert dialog box, use the following instructions to install the certificate and avoid viewing this dialog box again in future Enterprise Manager sessions:

1. In the Security Alert dialog box, click **View Certificate**.

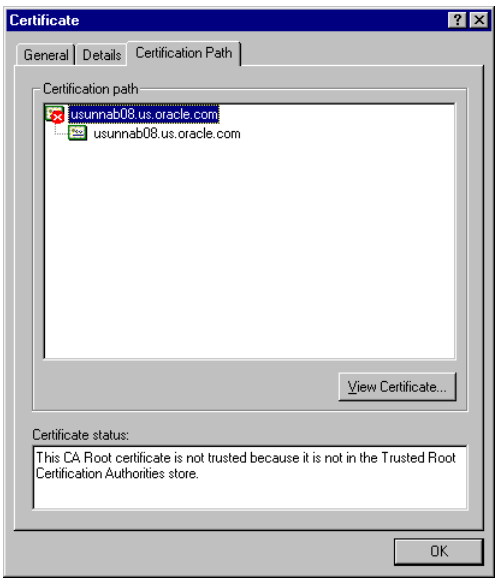
Internet Explorer displays the Certificate dialog box.

2. Click the **Certificate Path** tab and select the first entry in the list of certificates as shown in Figure 4–7.
3. Click **View Certificate** to display a second Certificate dialog box.
4. Click **Install Certificate** to display the Certificate Import wizard.
5. Accept the default settings in the wizard, click **Finish** when you are done, and then click **Yes** in the Root Certificate Store dialog box.

   Internet Explorer displays a message box indicating that the Certificate was imported successfully.
6. Click **OK** to close each of the security dialog boxes and click **Yes** on the Security Alert dialog box to continue with your browser session.

   You should no longer receive the Security Alert dialog box in any future connections to Enterprise Manager when you use this browser.

Figure 4–7 Certificate Path Tab on the Internet Explorer Certificate Dialog Box



4.7.1.2 Responding to the Netscape Navigator New Site Certificate Dialog Box

If you enable security for the Management Service, but you do not enable the more extensive security features of your Oracle HTTP Server, you will likely receive a New Site Certificate dialog box similar to the one shown in Figure 4–8 when you first attempt to display the Grid Control Console using the HTTPS URL in Netscape Navigator.

> **Note:** The instructions in this section apply to Netscape Navigator 4.79. The instructions may vary for other supported browsers.

When Netscape Navigator displays the New Site Certificate dialog box, use the following instructions to install the certificate and avoid viewing this dialog box again in future Enterprise Manager sessions:

1. Review the instructions and information on each wizard pages; click **Next** until you are prompted to accept the certificate.
2. Select **Accept this certificate forever (until it expires)** from the list of options.
3. On the last screen of the wizard, click **Finish** to close the wizard and continue with your browser session.

   You should no longer receive the New Site Certificate dialog box when using the current browser.

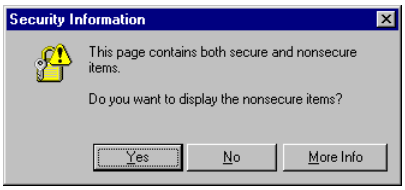
Figure 4–8 Netscape Navigator New Site Certificate Dialog Box

4.7.1.3 Preventing the Display of the Internet Explorer Security Information Dialog Box

After you enable Security for the Management Service, you may receive a dialog box similar to the one shown in Figure 4–9 whenever you access certain Enterprise Manager pages.

> **Note:** The instructions in this section apply to Internet Explorer 6.0. The instructions may vary for other supported browsers.

Figure 4–9 Internet Explorer Security Information Dialog Box



To stop this dialog box from displaying:

1. Select **Internet Options** from the Internet Explorer **Tools** menu.
2. Click the **Security** tab.
3. Select **Internet** and then click **Custom Level**.

   Internet Explorer displays the Security Settings dialog box.

4. Scroll down to **Miscellaneous** settings and enable the **Display Mixed Content** option.

4.7.2 Configuring Beacons to Monitor Web Applications Over HTTPS

Oracle Beacons provide application performance availability and performance monitoring. They are part of the Application Service Level Management features of Enterprise Manager.

> **See Also:** "About Application Service Level Management" in the Enterprise Manager Online Help

When a Beacon is used to monitor a URL over SSL (using an HTTPS URL), the Beacon must be configured to recognize the Certificate Authority that has been used by the Web site where that URL resides.

> **See Also:** "The Public Key Infrastructure Approach to Security" in *Oracle Security Overview* for an overview of Public Key Infrastructure features, such as Certificate Authorities

The Beacon software is preconfigured to recognize most commercial Certificate Authorities that are likely to be used by a secure Internet Web Site. However, you may encounter Web Sites that, although available over HTTPS, do not have a Certificate that has been signed by a commercial Certificate Authority recognized by the Beacon.

In those cases, for example, if you attempt to use the Test section of the Beacon Performance page to test the HTTP Response of the secure URL, the following error appears in the **Status Description** column of the Response Metrics table on the URL Test Page:

```
javax.net.ssl.SSLException: SSL handshake failed:
X509CertChainIncompleteErr--https://mgmtsys.acme.com/OracleMyPage.Home
```

> **See Also:** "Using Beacons to Monitor Remote URL Availability" in the Enterprise Manager online help

To correct this problem you must allow the Beacon to recognize the Certificate Authority that was used by the Web Site to support HTTPS. You must add the Certificate of that Certificate Authority to the list of Certificate Authorities recognized by Beacon.

To configure the Beacon to recognize the Certificate Authority:

1. Obtain the Certificate of the Web Site's Certificate Authority, as follows:
   a. In Microsoft Internet Explorer, connect to the HTTPS URL of the Web Site you are attempting to monitor.
   b. Double-click the lock icon at the bottom of the browser screen, which indicates that you have connected to a secure Web site.

      The browser displays the Certificate dialog box, which describes the Certificate used for this Web site. Other browsers offer a similar mechanism to view the Certificate detail of a Web Site.
   c. Click the **Certificate Path** tab and select the first entry in the list of certificates as shown in Figure 4–7.
   d. Click **View Certificate** to display a second Certificate dialog box.

e. Click the **Details** tab on the Certificate window.

f. Click **Copy to File** to display the Certificate Manager Export wizard.

g. In the Certificate Manager Export wizard, select **Base64 encoded X.509 (.CER)** as the format you want to export and save the certificate to a text file with an easily-identifiable name, such as `beacon_certificate.cer`.

h. Open the certificate file using your favorite text editor.

   The content of the certificate file will look similar to the content shown in Example 4–5.

2. Update the list of Beacon Certificate Authorities, as follows:

   a. Locate the `b64InternetCertificate.txt` file in the following directory of Agent Home of the Beacon host:

      agent_home`/sysman/config/`

      This file contains a list of Base64 Certificates.

   b. Edit the `b64InternetCertificate.txt` file and add the contents of the Certificate file you just exported to the end of the file, taking care to include all the Base64 text of the Certificate including the BEGIN and END lines.

3. Restart the Management Agent.

   After you restart the Management Agent, the Beacon detects your addition to the list of Certificate Authorities recognized by Beacon and you can successfully monitor the availability and performance of the secure Web site URL.

Example 4–5 Sample Content of an Exported Certificate

```
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAwIBAgIQTs4NcImNY3JAs5edi/5RkTANBgkqhkiG9w0BAQQFADCB
... base64 certificate content...
-----END CERTIFICATE-----
```

5

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 3 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

5.1 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 9, "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 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.

5.2 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

5.2.1 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 7777. 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 7777:

```
http://mgmthost.acme.com:7777/em
```

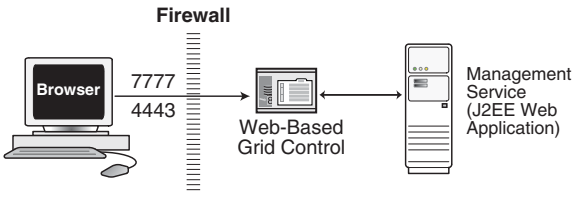
On the other hand, if you have enabled security for your Oracle HTTP Server, you are likely using the default secure port for the server, which is usually port 4443. If you are accessing the Grid Control Console using the following URL and port, then you must configure the firewall to allow the Grid Control Console to receive HTTP traffic over port 4443:

```
https://mgmthost.acme.com:4443/em
```

See also: *Oracle Application Server 10g Security Guide*

Figure 5–1 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 5–1 Firewall Between Your Browser and the Grid Control Console



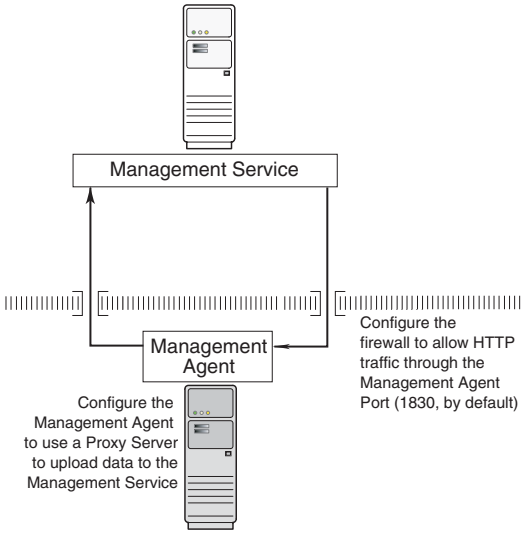
5.2.2 Configuring the Management Agent on a Host Protected by a Firewall

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 service on the Management Agent port, which is 1830 by default, regardless of whether or not Enterprise Manager Framework Security has been enabled.

Figure 5–2 illustrates the connections the Management Agent must make when it is protected by a firewall.

Figure 5–2 Configuration Tasks When the Management Agent is Behind a Firewall



5.2.2.1 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 two lines
#REPOSITORY_PROXYHOST=
#REPOSITORY_PROXYPORT=
```

3. 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 two lines
REPOSITORY_PROXYHOST=proxyhostname.domain
REPOSITORY_PROXYPORT=proxy_port
```

   For example:

```
REPOSITORY_PROXYHOST=proxy42.acme.com
REPOSITORY_PROXYPORT=80
```

4. Save your changes and close the `emd.properties` file.
5. Stop and start the Management Agent.

> **See Also:** "Controlling the Oracle Management Agent" on page 2-1

5.2.2.2 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 Agent does not change when you enable Enterprise Manager Framework Security. For more information, see "Configuring Security for Grid Control" on page 4-4

In addition, administrators can change the Management Agent port after the installation.

> **See Also:** "Chapter 9, "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.
>
> "Configuring Security for Grid Control" on page 4-4 for information about Enterprise Manager Framework Security

5.2.3 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:

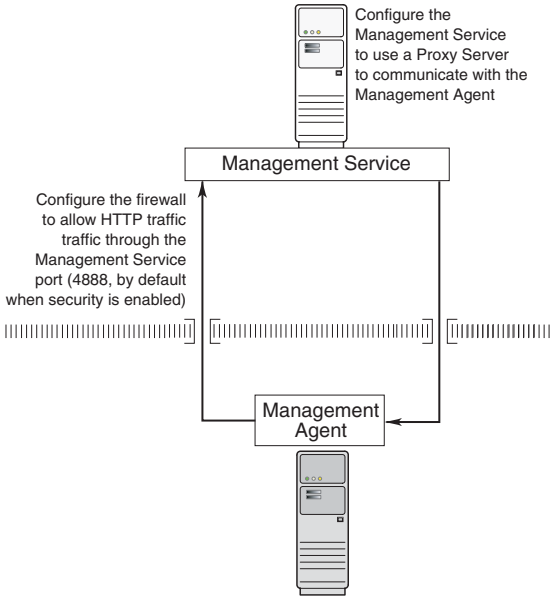
- Configure the Management Service to use a proxy server for its communications to the Management Agents.
- Configure the firewall to allow incoming HTTP traffic from the Management Agents on the repository upload port.

  If you have enabled Enterprise Manager Framework Security, the upload URL uses port 4888; if you have *not* enabled Enterprise Manager Framework Security, the upload port is 4889.

  > **See also:** "Enabling Security for the Oracle Management Service" on page 4-6

Figure 5–3 illustrates the connections the Management Service must make when it is protected by a firewall.

Figure 5–3 Configuration Tasks When the Management Service is Behind a Firewall



5.2.3.1 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 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, ...
   ```

   For example:

   ```
   proxyHost=proxy42.acme.com
   proxyHost=80
   dontProxyFor=.acme.com, .acme.us.com
   ```

   The `dontProxyFor` property identifies specific URL domains for which the proxy will not be used.

   See Also: "About the dontProxyfor Property" on page 5-6 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
   ```

5.2.3.2 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
```

5.2.3.3 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 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 to the 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 4888 HTTPS port.

> **See Also:** "Configuring Security for Grid Control" on page 4-4 for information about Enterprise Manager Framework Security

Administrators can also change the upload port after the installation.

> **See Also:** Chapter 9, "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

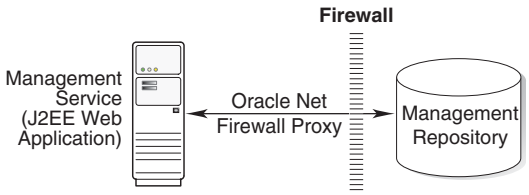
5.2.4 Firewalls Between the Management Service and the Management Repository

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 Advanced Security Administrator's Guide*

Figure 5–4 shows a typical configuration of a firewall between the Management Service and the Management Repository.

Figure 5–4 Firewall Between the Management Service and the Management Repository



5.2.5 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.

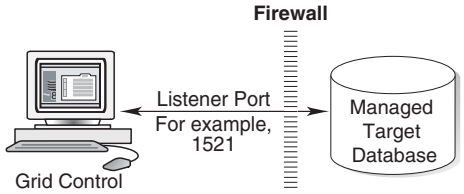
Specifically, to perform any administrative activities on the managed database, you must be sure that the firewall is configured to allow the Oracle Management Service to communicate with the database through the Oracle Listener port.

You can obtain the Listener port by reviewing the Listener home page in the Grid Control Console.

See Also: *Oracle Advanced Security Administrator's Guide*

Figure 5–5 shows a typical configuration of a firewall between Grid Control and the Management Repository.

Figure 5–5 Firewall Between Grid Control and a Managed Database Target



5.2.6 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 5-3

"Configuring the Management Service on a Host Protected by a Firewall" on page 5-5

- 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 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

5.2.7 Configuring Firewalls to Allow ICMP and UDP Traffic for Beacons

Oracle Beacons provide application performance availability and performance monitoring. They are part of the Application Service Level Management features of Enterprise Manager.

See Also: "About Application Service Level Management" in the Enterprise Manager Online Help

Enterprise Manager uses the industry-standard Internet Control Message Protocol (ICMP) and User Datagram Protocol (UDP) to transfer data between 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.

See Also: "Configuring Beacons to Monitor Web Applications Over HTTPS" on page 4-28

5.2.8 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

5.3 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

6

Configuring Application Service Level Management

This chapter describes how to configure Application Service Level Management (also known as Application Performance Management). Application Service Level Management is a feature available to users of the Oracle Enterprise Manager 10*g* Grid Control Console.

This chapter contains the following sections:

6.1 Before You Begin Configuring Application Service Level Management

Before you configure Application Service Level Management, you should:

- Be familiar with the concepts of systems monitoring and Application Service Level Management, as described in Oracle Enterprise Manager Concepts and in the Enterprise Manager online help.
- Review the Enterprise Manager Web Application target, which is created automatically when you install the Oracle Management Service.

> **See Also:** "Application Service Level Management" in *Oracle Enterprise Manager Concepts*
>
> "About Application Service Level Management" in the Enterprise Manager online help

6.2 Summary of Application Service Level Management Configuration Tasks

The configuration tasks in this chapter allow you to take advantage of four distinct features of Application Service Level Management. Each of these features is available from the Web Application target home page (Figure 6–1).

Figure 6–1 Web Application Target Home Page

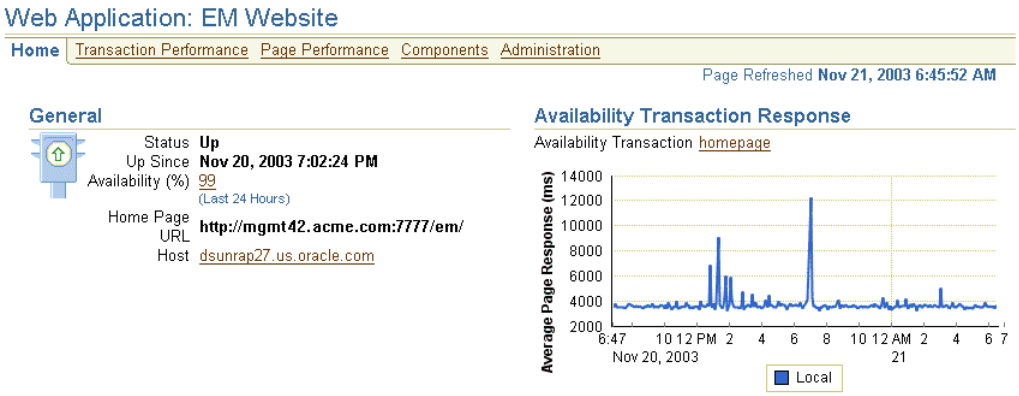


Table 6–1 describes each of the four major Application Service Level Management features and how they can be accessed from the Web Application target home page.

Table 6–1 Summary of the Application Service Level Management Configuration Tasks

Feature	Description	Requirements	Reference to Configuration Information
Transaction Performance Monitoring	Allows you to use the Transaction Performance page to: ▪ Proactively monitor business transactions ▪ Use Beacons to model the performance of various end user communities Click **Manage Transactions** on the Transaction Performance page and play back your transactions to review performance data.	Microsoft Internet Explorer 5.5 or later for creating and playing back transactions.	"Basic Configuration of Transaction Performance Monitoring" on page 6-4

Table 6–1 (Cont.) Summary of the Application Service Level Management Configuration Tasks

Feature	Description	Requirements	Reference to Configuration Information
Interactive Tracing for Business Transactions	Allows you to click **Manage Transactions** on the Transaction Performance page and use the **Play with Trace** button so you can: ▪ Diagnose performance problems at the transaction level ▪ Interactively trace transactions and analyze breakout of J2EE server activity times (servlet/JSP, EJB, JDBC time), including individual SQL statements.	Microsoft Internet Explorer 5.5 or later for creating and playing back transactions Oracle Application Server 10*g* (9.0.4) for playing back a transaction with trace to view J2EE server activity times	"Configuring Business Transaction Tracing" on page 6-4
End-User Response Time Monitoring	Allows you to use the Page Performance page to: ▪ Understand real end-user page response times within your application ▪ Assess the user impact of performance problems ▪ Analyze end user response times by by page, domain, region, visitors, and Web server.	Oracle Application Server Web Cache (9.0.2, 9.0.3, or 9.0.4)	"Configuring End-User Performance Monitoring" on page 6-6
Middle-Tier URL Performance	Allows you to use the Page Performance page to: ▪ Diagnose root cause of performance problems ▪ View historical tracing of J2EE middle tier activity ▪ View breakouts of J2EE server processing times (servlet, JSP, EJB, JDBC times), including individual SQL statements ▪ Correlate server activity to other Web Application component metrics ▪ View the full URL processing call stack.	Oracle Application Server 10*g* (9.0.4)	"Configuring OC4J for Middle-Tier URL Performance Monitoring" on page 6-14

6.3 Configuring Transaction Performance Monitoring

Configuring Transaction Performance Monitoring involves three levels of configuration:

- Basic configuration, in which you create a Web Application target and Enterprise Manager automatically begins monitoring your application based on the home page URL you provide when you create the target
- Advanced configuration, in which you optionally identify multiple remote Beacons and transactions to more accurately measure the availability and performance of you application
- Transaction tracing configuration, in which you configure Oracle Application Server Containers for J2EE (OC4J) so you can analyze the performance of the servlets, JSPs, EJB, and JDBC components that comprise your Web application

The following sections describe these configuration levels in more detail.

6.3.1 Basic Configuration of Transaction Performance Monitoring

To begin monitoring a Web application with Enterprise Manager:

1. Install an Oracle Management Agent on each of the host computers where your Web application components reside.

   This step is required so you can manage all the components of your Web Application with the Oracle Enterprise Manager 10*g* Grid Control Console. For example, if your Web application depends upon a back-end database as a data source, install the Management Agent on the database host so you can manage the database from the Grid Control Console.

2. Create a new Web Application target in the Oracle Enterprise Manager 10*g* Grid Control Console.

   See Also: "Creating Web Application Targets" in the Enterprise Manager online help

3. As you create this new Web Application target, add each of the managed targets that comprise the Web application.

   For example, be sure to include components such as the Oracle HTTP Server and the OC4J instance you used to deploy your application. Also include any backend databases you are using as a data source and the Oracle Application Server Web Cache instance you are using to improve the performance of your Web application.

   See Also: "About Beacons" in the Enterprise Manager online help

As soon as the Web Application appears in your list of managed targets, Enterprise Manager begins monitoring your application using the Local Beacon that is provided with the Management Agent you identified as the Monitoring Agent when you created the Web Application target.

This Local Beacon uses the home page URL you provided when you created the Web Application target to check the availability and performance of the application at periodic intervals.

Note: If the home page URL you provided while creating the Web Application target uses the HTTPS protocol, you must configure the Local Beacon so it can monitor the URL over the secure HTTPS protocol. For more information, see Section 4.7.2 on page 4-28

You can see the results of the home page URL transaction by viewing the Web Application home page, which includes a chart that shows the average response time of the home page URL each time it is run by the Local Beacon (Figure 6–1).

6.3.2 Advanced Configuration of Transaction Performance Monitoring

By default, when you first create a Web Application target, the Local Beacon attempts to access the application's home page URL at periodic intervals. When the Beacon successfully accesses this URL, Enterprise Manager considers your Web application available to your users.

> **See Also:** "About Web Application Availability" in the Enterprise Manager online help

Beyond the default home page URL and Local Beacon, you can customize your Web application as follows:

- To obtain more detailed information about the performance of pages other than the home page URL, you can create additional transactions to measure the availability and performance of specific pages or features of your application.

  You create additional transactions by using the **Manage Transactions** link on the Administration page of the Web Application target home page.

  > **See Also:** "Creating Transactions" in the Enterprise Manager online help

- To monitor the availability and performance of your application from multiple locations on your Intranet or on the Internet, you can identify additional Beacons to run your availability transactions.

  You add additional Beacon targets to the Grid Control Console by selecting **Beacon** from the **Add** drop-down list on the Agent home page. Use the **Manage Beacons** link on the Administration page of the Web Application target home page to identify which Beacon targets are used to monitor your Web application.

  > **See Also:** "Using Beacons to Monitor Web Application Availability" in the Enterprise Manager online help

6.3.3 Configuring Business Transaction Tracing

When you use transactions to monitor your Web application, some of the transactions you create often involve application components such as servlets, Java Server Pages (JSPs), Enterprise Java Beans (EJBs), and JDBC connections. Often, the best way to solve a performance problem is to trace these more complex transaction and analyze the time spent processing each back-end application component.

Enterprise Manager provides a mechanism for tracing these transactions. Use the **Manage Transactions** link on the Administration page on the Web Application target home page to create your transactions and to trace the transactions as they are processed by the servlets, JSPs, EJBs, or JDBC connections of your application.

However, before you can take advantage of transaction tracing, you must first enable tracing for the OC4J instance used to deploy the application.

To enable tracing for an OC4J instance:

1. Navigate to the OC4J Home page in the Oracle Enterprise Manager 10*g* Application Server Control Console.
2. Click **Administration** to display the Administration page.
3. On the Administration page, click **Server Properties**.
4. In the Command Line Options section of the Server Properties page, click **Tracing Properties**.

   Enterprise Manager displays the Tracing Properties page.
5. Select the three check boxes to enable general, interactive, and historical tracing.

   Click **Help** for more information about enabling OC4J tracing.

> **See Also:** "Enabling OC4J Tracing" in the Enterprise Manager online help

6. Click **Apply**.

   Enterprise Manager prompts you to restart the OC4J instance.

7. Click **Yes** to restart the instance.

6.4 Configuring End-User Performance Monitoring

After you have performed the basic configuration tasks for Transaction Performance Monitoring, you can then configure End-User Performance Monitoring.

> **See Also:** "Basic Configuration of Transaction Performance Monitoring" on page 6-4

The following steps describe how to enable End-User Performance Monitoring after you have configured Transaction Performance Monitoring in the Grid Control Console. Specifically, this procedure assumes you have created a Web Application target that includes at least one instance of Oracle Application Server Web Cache.

> **Note:** To enable End-User Performance Monitoring for a Web Application target, you must be using Oracle Application Server Web Cache to improve the performance of your Web application and the Oracle Application Server Web Cache instance you are using must be listed as a managed target in the Grid Control Console.
>
> In addition, you must include the Oracle Application Server Web Cache target as a component of the Web Application target you created in the section "Basic Configuration of Transaction Performance Monitoring" on page 6-4.

The procedure you use to enable End-User Performance Monitoring depends upon the version of Oracle Application Server Web Cache you are using. The following sections provide more information:

- Configuring End-User Performance Monitoring Using Oracle Application Server Release 2 (9.0.4)
- Configuring End-User Performance Monitoring Using Earlier Versions of Oracle Application Server Web Cache
- Configuring End-User Performance Monitoring Using Standalone Oracle Application Server Web Cache

6.4.1 Configuring End-User Performance Monitoring Using Oracle Application Server Release 2 (9.0.4)

The following sections describe how to configure and start End-User Performance Monitoring:

- Configuring Oracle Application Server Web Cache 9.0.4 for End-User Performance Monitoring
- Starting and Stopping End-User Performance Monitoring

> **See Also:** "Overview of Configuring End-User Performance Monitoring" in the Enterprise Manager online help

6.4.1.1 Configuring Oracle Application Server Web Cache 9.0.4 for End-User Performance Monitoring

End-User Performance Monitoring uses data from Oracle Application Server Web Cache to gather statistics about the performance of pages within your Web applications. As a result, you must configure Oracle Application Server Web Cache so it logs your Oracle Application Server Web Cache activity and that the data is in the correct format.

When Oracle Application Server Web Cache is properly configured, End-User Performance Monitoring can begin collecting the end-user performance data and load it into the Oracle Management Repository. After the data is collected and loaded into the repository, the performance data can be viewed on the End-User Performance page of the Web Application home page in the Oracle Enterprise Manager 10*g* Grid Control Console.

> **See Also:** "Configuring End-User Performance Monitoring" in the *Oracle Application Server Web Cache Administrator's Guide*

To configure the Oracle Application Server Web Cache Manager:

1. Navigate to the Web Application home page in the Grid Control Console and click **Administration**.

   Enterprise Manager displays the Web Application Administration page.

2. Click **Configure Web Application Web Caches**.

   Enterprise Manager displays the Configure Web Application Web Caches page.

3. Click **Configure Logging**.

   A new browser windows opens. It displays the OracleAS Web Cache Welcome page.

4. Click **Log on to Web Cache Manager**.

   OracleAS Web Cache displays a dialog box so you can log in to OracleAS Web Cache Manager.

5. Log in to the Oracle Application Server Web Cache Manager.

   > **See Also:** *Oracle Application Server Web Cache Administrator's Guide* for information about the default passwords for Oracle Application Server Web Cache

   You can also log in to the OracleAS Web Cache Manager using the `ias_admin` username and password you selected during the Oracle Application Server installation.

6. Enable OracleAS Web Cache logging for End-User Performance Monitoring:

   a. Select **Logging and Diagnostics > End-User Performance Monitoring** in the OracleAS Web Cache Manager navigator frame.

      You can enable monitoring for a particular cache or for an entire site.

   b. To enable monitoring for a particular cache, select the cache from the Cache-Specific End-User Performance Monitoring section and click **Enable**.

Be sure to enable the cache that you are using as a front-end to your Web application.

c. To enable monitoring for the entire site, select the site from the Site-Specific End-User Performance Monitoring section and click **Enable**.

7. Configure Oracle Application Server Web Cache to use the Web Cache Log Format (WCLF):

   a. Select **Logging and Diagnostics > Access Logs** in the OracleAS Web Cache Manager navigator frame.

   b. In the Cache-Specific Access Log Configuration table, click **Edit Selected** and enable the access log for your selected cache.

   c. In the Site-Specific Access Log Configuration table, make sure that the Format style of the selected Site Name is `WCLF` and that it is enabled.

8. Click **Apply Changes** at the top of the Web Cache Manager window and restart OracleAS Web Cache by clicking **Restart** on the Web Cache Manager Cache Operations page.

9. Close the Web Cache Manager browser window and return to the Configure Web Application Web Caches page in the Grid Control Console.

6.4.1.2 Starting and Stopping End-User Performance Monitoring

After you configure Oracle Application Server Web Cache for End-User Performance Monitoring, you can then start collecting end-user performance data:

1. Navigate to the Web Application home page in the Grid Control Console and click **Administration**.

2. Click **Configure Web Application Web Caches** in the Monitoring of End-User Response Time section of the page.

   Enterprise Manager displays the Configure Web Application Web Caches page.

3. For the Web Cache you are using to improve the performance of your Web application, select the check box in the **Collecting** column of the table.

4. In the **Interval (minutes)** column, enter the interval at which Enterprise Manager will collect performance data.

To stop collecting end-user performance data:

1. Navigate to the Configure Web Application Web Caches page.

2. Clear the check box in the Collecting column of the table and click **Apply**.

6.4.2 Configuring End-User Performance Monitoring Using Earlier Versions of Oracle Application Server Web Cache

If you are managing an earlier version of the Oracle Application Server using the Oracle Enterprise Manager 10*g* Grid Control Console, you can monitor your Web applications with End-User Performance Monitoring, but you cannot configure your Oracle Application Server Web Cache instance from within the Grid Control Console.

Instead, you configure End-User Performance Monitoring for Oracle Application Server Web Cache 9.0.2 and 9.0.3 by running the `chronos_setup` script on the computer that hosts your Oracle HTTP Server.

Note: Before you can enable End-User Performance Monitoring, you should have already configured Transaction Performance Monitoring, as described in the section "Basic Configuration of Transaction Performance Monitoring" on page 6-4.

In addition, the Oracle Application Server Web Cache instance you are using for your Web application must be included as a component of the Web Application target you created.

6.4.2.1 About the chronos_setup Configuration Script

Before you begin, consider the following:

- The `chronos_setup` script is installed in the `bin` directory of your Management Agent home when you install the Management Agent using the instructions in *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*.
- You must run the `chronos_setup` script as an operating system user with the privilege to write to the document root of your Oracle HTTP Server.
- If you have trouble running the script, run it with no arguments to display the help text.

To enable End-User Performance Monitoring for Oracle Application Server Web Cache 9.0.2 or Oracle Application Server Web Cache 9.0.3, you must run the `chronos_setup` script three times, each time with a different argument:

- Once to configure the document root for each Web server in your Web site
- Once to configure Oracle Application Server Web Cache
- Once to start collecting response time data

The following sections describe each step of enabling End-User Performance Monitoring for Oracle Application Server Web Cache 9.0.2 or Oracle Application Server Web Cache 9.0.3.

6.4.2.2 Configuring the Document Root for Each Web Server

When you run the `chronos_setup` script with the `webserver` argument, the script:

- Creates a new directory inside the document root. The directory is called:

  ```
  oracle_smp_chronos
  ```

- Installs two files into the oracle_smp_chronos directory:

  ```
  oracle_smp_chronos.js
  oracle_smp_chronos.gif
  ```

The `oracle_smp_chronos.js` must be installed in the document root of each Web server that serves content for your Web site.

Note: If you have more than one document root, you must run the `chronos_setup` script on each document root.

For example, if Oracle Application Server Web Cache and your Web server are on different machines and an Oracle Management Agent is present on the Web server machine, you must run the `chronos_setup` script with the `webserver` option on the Web Server host to configure the document root for the remote Web server.

If Oracle Application Server Web Cache and your Web server are installed on different machines and you have no plans to install a Management Agent or to monitor the Web server, you will need to create a directory called `oracle_smp_chronos` under the Web server document root directory, and using FTP, place the `oracle_smp_chronos.js` file in the `oracle_smp_chronos` directory.

To configure the document root for each Web server:

1. Change directory to the `/bin` directory in the Management Agent home directory.

   For example:

   ```
   $PROMPT> cd AGENT_HOME/bin
   ```

2. Make sure you have write access to the Web server document root directory and then run the script as follows:

   ```
   $PROMPT> ./chronos_setup webserver location_of_the_webserver_DocumentRoot
   ```

   An example of a Document Root is as follows:

   ```
   $ORACLE_HOME/Apache/Apache/htdocs
   ```

   To find the location of the document root:

   - Log in to the Oracle Application Server Release 2 (9.0.2) Enterprise Manager Web site and navigate to the Oracle HTTP Server Home Page. The document root is displayed in the General section of the HTTP Server Home Page.

     OR

   - Use a text editor or a command-line search utility to search for the term `DocumentRoot` in the following Oracle HTTP Server configuration file:

     ```
     $ORACLE_HOME/Apache/Apache/conf/httpd.conf
     ```

6.4.2.3 Configuring Oracle Application Server Web Cache for End-User Performance Monitoring

To configure Oracle Application Server Web Cache for End-User Performance Monitoring, you run the `chronos_setup` script with the `webcache` argument. The script sets up Oracle Application Server Web Cache for End-User Performance Monitoring, and stops and restarts Oracle Application Server Web Cache automatically.

To configure Oracle Application Server Web Cache for End-User Performance Monitoring:

1. Make sure you have write access to the Oracle Application Server Web Cache directory.

   For example, if Web Cache is installed in an Oracle Application Server home directory, you will need access to the `IAS_HOME/webcache` directory.

2. Change directory to the `/bin` directory in the Management Agent home directory.

   For example:

   ```
   $PROMPT> cd /private/agent_home/bin
   ```

3. Run the script as follows:

   ```
   $PROMPT> ./chronos_setup webcache webcache_installation_directory
   ```

Note: After running `chronos_setup`, if you cannot restart Oracle Application Server Web Cache, back out of the configuration process by copying the following files back to their original name and location:

- `internal.xml<timestamp>`
- `webcache.xml<timestamp>`

6.4.2.4 Starting End-User Performance Monitoring

To start End-User Performance Monitoring, you run the `chronos_setup` script with the `collection` argument. The script creates a collection file for the specified target and restarts the agent.

To start End-User Performance Monitoring:

1. Log in as the user who installed the Management Agent so you have write access to the following directory:

   ```
   AGENT_HOME/sysman/emd/collection
   ```

2. Change directory to the `/bin` directory in the Management Agent home directory.

   For example:

   ```
   $PROMPT> cd AGENT_HOME/bin
   ```

3. Locate the name of the Oracle Application Server Web Cache target.

   You can locate the name of the target in one of three ways:

   - From the Oracle Enterprise Manager 10*g* Grid Control Console, locate the Oracle Application Server Web Cache target on the Targets tab. The name listed in the first column of the Target table is the name you must enter as an argument to the `chronos_setup` script. Note the use of spaces and underscores.
   - Search the contents of the targets.xml configuration file, which lists all the targets managed by the Management Agent. Locate the Oracle Application Server Web Cache entry in the file and use the NAME attribute for the Web Cache target. The targets.xml file is located in the following directory of the Management Agent home:

     ```
     AGENT_HOME/sysman/emd/targets.xml
     ```

   - Use the `emctl config agent listtargets` command to list the target names and target types currently being monitored by the Management Agent.

     See Also: "Listing the Targets on a Managed Host" on page 2-14

4. Start the collection for the Oracle Application Server Web Cache target by running the script as follows:

   ```
   $PROMPT> ./chronos_setup collection webcache_targetname
   ```

   Note: If the name of the Oracle Application Server Web Cache target includes spaces, you must use quotation marks around the name.

See Also: "Creating Web Application Targets" in the Enterprise Manager online help

6.4.3 Configuring End-User Performance Monitoring Using Standalone Oracle Application Server Web Cache

Oracle Application Server Web Cache is available as a standalone download from the Oracle Technology Network (OTN). The standalone version of Oracle Application Server Web Cache allows you to improve the performance and reliability of your Web server even if you are not using Oracle Application Server.

If you are using standalone Oracle Application Server Web Cache with a third-party Web server, you can still manage Oracle Application Server Web Cache using the Oracle Enterprise Manager 10*g* Grid Control Console. As a result, you can also use End-User Performance Monitoring to monitor the Web applications that your users access through Oracle Application Server Web Cache.

Configuring End-User Performance Monitoring for standalone Oracle Application Server Web Cache involves the following steps, which are described in the following sections:

- Installing Standalone Oracle Application Server Web Cache
- Configuring Standalone Oracle Application Server Web Cache
- Enabling End-User Performance Monitoring for Standalone Oracle Application Server Web Cache

6.4.3.1 Installing Standalone Oracle Application Server Web Cache

To install the standalone version of Oracle Application Server Web Cache:

1. Navigate to the Oracle Technology Network (OTN):

   ```
   http://otn.oracle.com/software/content.html
   ```

2. Locate and select the Oracle Application Server Web Cache download option and follow the links for your operating system.
3. Use the instructions on the OTN Web site to download Oracle Application Server Web Cache.
4. Use the instructions in the Web Cache readme file to install Oracle Application Server Web Cache in its own Oracle Home.

6.4.3.2 Configuring Standalone Oracle Application Server Web Cache

End-User Performance Monitoring uses data from Oracle Application Server Web Cache to gather statistics about the performance of pages within your Web applications. As a result, Enterprise Manager obtains End-User Performance Monitoring data only when Oracle Application Server Web Cache is configured to improve the performance and reliability of your Web server.

See Also: *Oracle Application Server Web Cache Administrator's Guide* for complete instructions for configuring Oracle Application Server Web Cache

Specifically, you must perform the following Oracle Application Server Web Cache configuration tasks:

1. Change the default listening port of your HTTP Server (for example, 7777) to a new port number (for example, 7778) and restart the HTTP Server.

   See Also: "Specifying Listening Addresses and Ports" in the Enterprise Manager online help if you are using Oracle HTTP Server and managing the server with Enterprise Manager

   Oracle HTTP Server Administrator's Guide for information about modifying the `httpd.conf` file if you are not managing the server with Enterprise Manager

2. Start Oracle Application Server Web Cache and its administration tools.
3. Configure Oracle Application Server Web Cache so it receives requests on the default port previously assigned to your Web server (for example, 7777).
4. Configure Oracle Application Server Web Cache so it so it sends cache misses to your newly defined Web server default port number (for example, 7778), which is also referred to as the origin server.
5. Create an Oracle Application Server Web Cache *site* and map the site to your origin server.
6. Apply the changes and restart Oracle Application Server Web Cache.
7. Test the installation to be sure Oracle Application Server Web Cache and your Web server are working properly.

6.4.3.3 Enabling End-User Performance Monitoring for Standalone Oracle Application Server Web Cache

After you have installed and configured Oracle Application Server Web Cache and tested the configuration to be sure your Web site data is being cached, you can then enable End-User Performance Monitoring.

The procedure for enabling End-User Performance Monitoring is similar to the procedures documented earlier in this chapter; however, the steps vary depending upon the version of standalone Oracle Application Server Web Cache you are using.

To enable End-User Performance Monitoring for standalone Oracle Application Server Web Cache:

1. Perform the basic configuration tasks to enable Transaction Performance Monitoring.

   Basic configuration of Transaction Performance Monitoring involves adding the Oracle Application Server Web Cache target and creating a Web Application target.

   See Also: "Basic Configuration of Transaction Performance Monitoring" on page 6-4

2. Use the Oracle Application Server Web Cache Manager to configure End-User Performance Monitoring, and use the Grid Control to start End-User Performance Monitoring, as described in "Configuring End-User Performance Monitoring Using Oracle Application Server Release 2 (9.0.4)" on page 6-6.

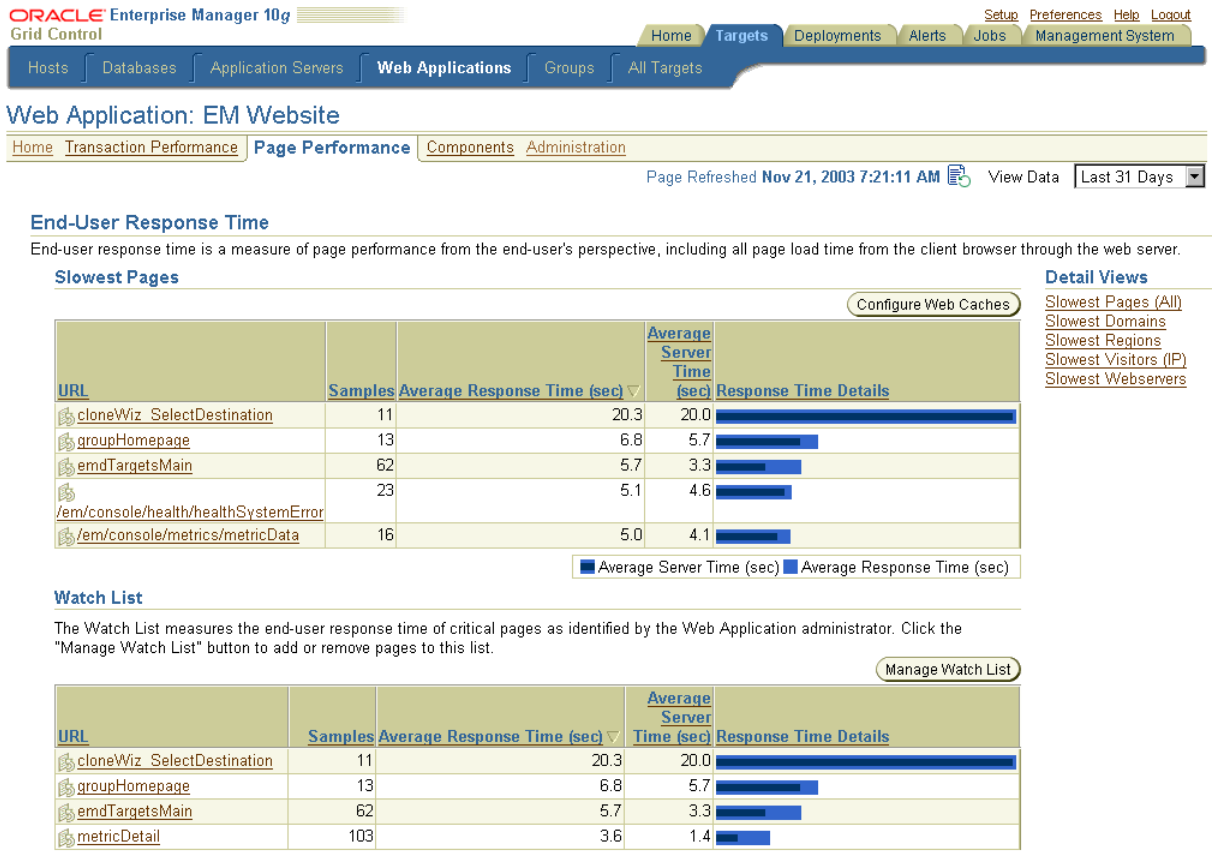
6.4.4 Confirming that End-User Performance Monitoring is Enabled

When End-User Performance Monitoring is properly enabled, you will see response time data on the Page Performance tab of the Web Application home page as shown in Figure 6–2.

However, note that it may take some time for Enterprise Manager to gather and display the end-user monitoring data. You must also be sure that enough users are accessing your Web application so that enough end-user performance data can be gathered and stored in the Oracle Management Repository.

> **See Also:** "Verifying and Troubleshooting End-User Performance Monitoring" in the Enterprise Manager online help for more information about confirming that End-User Performance Monitoring is configured and operating correctly.

Figure 6–2 End-User Performance Data on the Web Application Home Page



6.5 Configuring OC4J for Middle-Tier URL Performance Monitoring

When combined with the tracing features of OC4J, Application Performance Management can gather critical middle-tier performance data about your Web application. Enterprise Manager displays this performance data on the Web Application Performance Page, just below the End-User Performance Monitoring data.

This feature can be instrumental when you are diagnosing application server and back-end performance issues.

See Also: "About Monitoring Page Performance" in the Enterprise Manager online help

Before you can begin collecting middle-tier URL performance data and before this data can appear on the Web Application Page Performance page, you must first enable the logging and tracing capabilities of the OC4J instance that you used to deploy your application.

For more information, see the following:

- Configuring OC4J Tracing for Middle-Tier URL Monitoring
- Additional Configuration for Monitoring UIX Applications

6.5.1 Configuring OC4J Tracing for Middle-Tier URL Monitoring

To configure OC4J tracing so you can begin collecting middle-tier URL performance data:

1. Navigate to the Web Application home page and click **Administration**.
2. Click **Configure Web Application OC4Js**.

   Enterprise Manager displays the Configure Web Application OC4Js page.
3. For the OC4J instance that you used to deploy your application, select the check box in the **Collecting** column.
4. In the **Interval (minutes)** column, enter the interval at which to collect OC4J tracing data.

   The recommended interval setting is 60 minutes.
5. Click **Enable Logging**.

   Enterprise Manager opens another browser window and displays the Tracing Properties page for the OC4J instance in the Application Server Control.

   If you are prompted to log in to the Application Server Control Console, enter the credentials for the `ias_admin` adminstrator's account.
6. Select the following options on the Tracing Properties page:
   - **Enable JDBC/SQL Performance Details**
   - **Enable Interactive Trace**
   - **Enable Historical Trace**

   You can use the default values for most of the tracing properties. However, Oracle recommends that you set the **Frequency to Generate Trace File (seconds)** field to `3600` seconds (equivalent to 60 minutes).

   Note: Modifying the value in the **Trace File Directory** field is not supported.
7. Click **Apply**.

   If this is the first time you are enabling OC4J tracing for this application server, Enterprise Manager displays a message stating that the `transtrace` application is being deployed. The Application Server Control then prompts you to restart the OC4J instance.

8. Click **Yes** to restart the instance and enable the tracing properties.
9. Return to the Grid Control Console.

   Middle-Tier Performance data should begin to appear on the Web Application Page Performance page as soon as data for the OC4J instance is collected and uploaded into the Management Repository.

6.5.2 Additional Configuration for Monitoring UIX Applications

If you used Oracle User Interface XML (UIX) to build your application, there is an additional configuration step you must perform before you can monitor the middle-tier URLs of your application.

> **See Also:** Your JDeveloper documentation for information on using UIX to develop Web applications

Before you can monitor the middle-tier URLs of your UIX application, you must do the following:

1. Enable tracing for the OC4J instance you used to deploy your application, as described in "Configuring OC4J Tracing for Middle-Tier URL Monitoring" on page 6-15.
2. Locate the following configuration file in the Application Server home directory where you deployed your UIX application:

   `$ORACLE_HOME/j2ee/`*`OC4J_instance_name`*`/config/oc4j.properties`

   For example, if you deployed your application in the OC4J instance called "home," locate the following configuration file:

   `$ORACLE_HOME/j2ee/home/config/oc4j.properties`

3. Open the `oc4j.properties` file using your favorite text editor and add the following line to the end of the file:

   ```
   oracle.dms.transtrace.dollarstrippingenabled=true
   ```

4. Save your changes and close the `oc4j.properties` file.
5. Restart the OC4J instance.

7

Locating and Configuring Enterprise Manager Log Files

When you install the Oracle Management Agent or the Oracle Management Service, Enterprise Manager automatically configures the system to save certain informational, warning, and error information to a set of log files.

Log files can help you troubleshoot potential problems with an Enterprise Manager installation. They provide detailed information about the actions performed by Enterprise Manager and whether or not any warnings or errors occurred.

This chapter not only helps you locate and review the contents of Enterprise Manager log files, but also includes instructions for configuring the log files to provide more detailed information to help in troubleshooting or to provide less detailed information to save disk space.

This chapter contains the following sections:

7.1 Locating and Configuring Management Agent Log and Trace Files

The following sections provide information on the log and trace files for the Oracle Management Agent:

7.1.1 About the Management Agent Log and Trace Files

Oracle Management Agent log and trace files store important information that support personnel can later use to troubleshoot problems. The Management Agent uses three types of log files:

- The Management Agent log file (`emagent.log`)

  The Agent saves information to the log file when the Agent performs an action (such as starting, stopping, or connecting to a Management Service) or when the

Agent generates an error (for example, when the Agent cannot connect to the Management Service).

- The Management Agent trace file (`emagent.trc`)

  The Management Agent trace file provides an advanced method of troubleshooting that can provide support personnel with even more information about what actions the Agent was performing when a particular problem occurred.

- The Management Agent startup log file (`emagent.nohup`)

  The Management Agent saves information to the startup log file when there is a problem starting the agent. This file is updated by the Management Agent Watchdog Process. When the Watchdog Process logs any problems it finds to this file.

  See Also: "About the Management Agent Watchdog Process" on page 9-4

In addition, Enterprise Manager also provides a log file and a trace file for the fetchlets, which are software programs used by the Management Agent for certain data-gathering tasks:

- `emagentfetchlet.log`
- `emagentfetchlet.trc`

7.1.2 Locating the Management Agent Log and Trace Files

The Management Agent log files are stored in the following directory when you install the Management Agent:

```
AGENT_HOME/sysman/log/
```

See Also: Chapter 1, "Introduction to Enterprise Manager Advanced Configuration" for information about locating the Agent home directory.

7.1.3 About Management Agent Rollover Files

Both the Management Agent log file and the Management Agent trace file are designed to increase in size over time as information is written to the files. However, they are also designed to reach a maximum size. When the files reach the predefined maximum size, the Management Agent renames (or rolls) the logging or trace information to a new file name and starts a new log or trace file. This process keeps the log files from growing too large.

To be sure you have access to important log or trace file information, the Management Agent will rollover the log and trace files four times by default. When it rolls the log or trace file over the fourth time, the Agent deletes the oldest rollover file.

As a result, you will often see a total of four log files and four trace files in the log directory. The following example shows three archived trace files and the current trace file in the `AGENT_HOME/sysman/log` directory:

```
emagent.trc
emagent.trc.1
emagent.trc.2
emagent.trc.3
```

7.1.4 Controlling the Size and Number of Management Agent Log and Trace Files

You can control how large the log file and the trace file can get before the Management Agent creates a rollover file. You can also control how many rollover files are created before the Management Agent deletes any logging or tracing data.

To control the size and number of Management Agent Log and Trace Files:

1. Stop the Management Agent.

   See Also: "Starting, Stopping, and Checking the Status of the Management Agent on UNIX" on page 2-1

2. Locate the `emd.properties` file, which is located in the following directory:

   ```
   AGENT_HOME/sysman/config/ (UNIX)
   AGENT_HOME\sysman\config (Windows)
   ```

3. Use a text editor to open the `emd.properties` file.
4. Use the information in Table 7–1 to locate and modify the Agent logging and tracing properties in the `emd.properties` file.
5. Restart the Management Agent.

Table 7–1 Management Agent Log and Trace File Properties

Property	Purpose	Example
`LogFilewithPID`	When set to TRUE, this property appends the process ID of the Management Agent to the log file name. This makes it easier to identify the process ID of the Management Agent you are monitoring.	`LogFilewithPID=true`
`LogFileMaxSize`	When the Agent log file reaches this size (in kilobytes), the Management Agent copies the logging data to a new rollover file and creates a new `emagent.log` logging file.	`LogFileMaxSize=4096`
`LogFileMaxRolls`	By the default, the Agent will rollover the log file four times before it deletes any logging data. The number of rollover files is controlled by this property.	`LogFileMaxRolls=4`
`TrcFileMaxSize`	When the Agent trace file reach this size (in kilobytes), the Management Agent copies the logging data to a new rollover file and creates a new `emagent.trc` logging file.	TrcFileMaxSize=4096
TrcFileMaxRolls	By the default, the Agent will rollover the trace file four times before it deletes any tracing data. The number of rollover files is controlled by this property.	TrcFileMaxRolls=4

7.1.5 Controlling the Contents of the Management Agent Trace File

To modify the amount of information saved in the Management Agent trace file:

1. Stop the Management Agent.

   See Also: "Starting, Stopping, and Checking the Status of the Management Agent on UNIX" on page 2-1

2. Locate the `emd.properties` file, which is located in the following directory:

   AGENT_HOME`/sysman/config`

3. Open the `emd.properties` file using your favorite text editor and look for the following entries near the bottom of the file:

   ```
   tracelevel.main=WARN
   tracelevel.emdSDK=WARN
   tracelevel.emdSDK.util=WARN
   tracelevel.ResMonitor=WARN
   tracelevel.Dispatcher=WARN
   tracelevel.ThreadPool=WARN
   tracelevel.pingManger=WARN
   .
   .
   .
   ```

   Each of these properties controls the level of logging detail for the various subcomponents of the Management Agent.

4. Modify the amount of information that is included in the trace file by replacing the WARN value for each property to one of the values shown in Table 7–2.

   Note: The values described in Table 7–2 are case-sensitive.

5. Restart the Management Agent.

Table 7–2 Enterprise Manager Component Tracing Levels

Level	Purpose
ERROR	Include only critical errors in the trace file. This setting generates the least amount of tracing data. The trace file will likely grow at a relatively slow rate when you select this logging level.
WARN	Include warning information, in addition to critical errors.
INFO	Include informational messages, in addition to warning and critical error information.
DEBUG	Include debugging information, as well as informational tracing, warning, and critical errors. This setting generates the greatest amount of tracing data. **Note:** The trace file will likely grow at a relatively fast rate when you select this logging level.

7.1.6 Controlling the Size and Number of Fetchlet Log and Trace Files

Like the Management Agent log and trace files, the Management Agent fetchlet log and trace files are designed to reach a maximum size before the Management Agent renames (or rolls) the information to a new file name and starts a new log or trace file.

To control the maximum size of the Management Agent fetchlet log and trace files, as well as the number of rollover files:

1. Stop the Management Agent.

   See Also: "Starting, Stopping, and Checking the Status of the Management Agent on UNIX" on page 2-1

2. Locate the `emagentlogging.properties` file in the following directory:

   `AGENT_HOME/sysman/config`

3. Open the `emagentlogging.properties` file with a text editor and modify the entries described in Table 7–3.

4. Restart the Management Agent.

Table 7–3 Management Agent Servlet Log and Trace File Properties

Property	Purpose	Example
log4j.appender.emagentlogAppender.MaxFileSize	When the fetchlet log file reaches this size, the Management Agent copies the logging data to a new rollover file and creates a new `emagentfetchlet.log` file.	log4j.appender.emagentlogAppender.MaxFileSize=20000000
log4j.appender.emagentlogAppender.MaxBackupIndex	This optional property indicates how many times the Management Agent will rollover the fetchlet log file to a new file name before deleting logging data. **Note:** Because the log file does not contain as much data as the trace file, it is usually not necessary to create more than one rollover file. As a result, this entry is not included in the properties file by default.	log4j.appender.emagentlogAppender.MaxBackupIndex=1
log4j.appender.emagenttrcAppender.MaxFileSize	When the fetchlet trace file reaches this size, the Management Agent copies the logging data to a new rollover file and creates a new `emagentfetchlet.trc` log file.	log4j.appender.emagenttrcAppender.MaxFileSize=5000000
log4j.appender.emagenttrcAppender.MaxBackupIndex	This property indicates how many times the Management Agent will rollover the trace file to a new file name before deleting tracing data.	log4j.appender.emagenttrcAppender.MaxBackupIndex=10

7.1.7 Controlling the Contents of the Fetchlet Trace File

By default, the Management Agent will save all critical and warning messages generated by the Management Agent fetchlets to the `emagentfetchlet.trc` file. However, you can adjust the amount of logging information that the fetchlets generate.

To change the amount of tracing information generated by the Management Agent fetchlets:

1. Stop the Management Agent.

   See Also: "Starting, Stopping, and Checking the Status of the Management Agent on UNIX" on page 2-1

2. Locate the `emagentlogging.properties` file in the following directory:

   `AGENT_HOME/sysman/config`

3. Open the `emagentlogging.properties` file with a text editor and locate the following entry:

   ```
   log4j.rootCategory=WARN, emagentlogAppender, emagenttrcAppender
   ```

4. Change the value of the `log4j.rootCategory` parameter to one of the values shown in Table 7–2.

   Note: The the values described in Table 7–2 are case-sensitive.

5. Restart the Management Agent.

7.2 Locating and Configuring Management Service Log and Trace Files

The following sections describe how to locate and configure the Management Service log files:

- Locating the Management Service Log and Trace Files
- Controlling the Size and Number of Management Service Log and Trace Files
- Controlling the Contents of the Management Service Trace File

7.2.1 About the Management Service Log and Trace Files

Oracle Management Service log and trace files store important information that support personnel can later use to troubleshoot problems. The Management Service uses two types of log files:

- The Management Service log file (`emoms.log`)

  The Oracle Management Service saves information to the log file when the Management Service performs an action (such as starting or stopping) or when the Management Service generates an error.

- The Management Service trace file (`emoms.trc`)

  The Management Service trace file provides an advanced method of troubleshooting that can provide support personnel with even more information about what actions the Management Service was performing when a particular problem occurred.

7.2.2 Locating the Management Service Log and Trace Files

The Management Service log and trace files are stored in the following directory inside the Oracle Application Server Home where the Oracle Management Service is installed and deployed:

```
AS_HOME/sysman/log/
```

7.2.3 Controlling the Size and Number of Management Service Log and Trace Files

The Management Service log and trace files increases in size over time as information is written to the files. However, the files are designed to reach a maximum size. When the files reach the predefined maximum size, the Management Service renames (or rolls) the logging information to a new file name and starts a new log or trace file. This process keeps the log and trace files from growing too large.

As a result, you will often see multiple log and trace files in the Management Service log directory. The following example shows one archived log file and the current log file in the `AS_HOME/sysman/log` directory:

```
emoms.log
emoms.log.1
```

To control the maximum size of the Management Service log and trace files, as well as the number of rollover files:

1. Stop the Management Service.

   See Also: "Controlling the Oracle Management Service" on page 2-4

2. Locate the `emomslogging.properties` file in the following directory:

   ```
   AS_HOME/sysman/config
   ```

3. Open the `emomslogging.properties` file with a text editor and modify the entries described in Table 7–4.
4. Restart the Management Service.

Table 7–4 Management Service Log File Properties in the emomslogging.properties File

Property	Purpose	Example
log4j.appender.emlogAppender.MaxFileSize	When the Management Service log file reaches this size, the Management Service copies the logging data to a new rollover file and creates a new `emoms.log` log file.	log4j.appender.emlogAppender.MaxFileSize=20000000
log4j.appender.emlogAppender.MaxBackupIndex	This optional property indicates how many times the Management Service will rollover the log file to a new file name before deleting logging data. **Note:** Because the log file does not contain as much data as the trace file, it is usually not necessary to create more than one rollover file. As a result, this entry is not included in the properties file by default.	log4j.appender.emlogAppender.MaxBackupIndex=1
log4j.appender.emtrcAppender.MaxFileSize	When the Management Service trace file reaches this size, the Management Service copies the logging data to a new rollover file and creates a new `emoms.trc` log file.	log4j.appender.emtrcAppender.MaxFileSize=5000000
log4j.appender.emtrcAppender.MaxBackupIndex	This property indicates how many times the Management Services will rollover the trace file to a new file name before deleting tracing data.	log4j.appender.emtrcAppender.MaxBackupIndex=10

7.2.4 Controlling the Contents of the Management Service Trace File

By default, the Management Service will save all critical and warning messages to the `emoms.trc` file. However, you can adjust the amount of logging information that the Management Service generates.

To change the amount of logging information generated by the Management Service:

1. Stop the Management Service.

   See Also: "Controlling the Oracle Management Service" on page 2-4

2. Locate the `emomslogging.properties` file in the following directory:

   ```
   AS_HOME/sysman/config
   ```

3. Open the `emomslogging.properties` file with a text editor and locate the following entry:

   ```
   log4j.rootCategory=WARN, emlogAppender, emtrcAppender
   ```

4. Modify the value of the `log4j.rootCategory` parameter to one of the values shown in Table 7–2.

   Note: The the values described in Table 7–2 are case-sensitive.

5. Restart the Management Service.

8

Maintaining and Troubleshooting the Repository

This chapter describes maintenance and troubleshooting techniques for maintaining a well-performing Management Repository.

Specifically, this chapter contains the following sections:

8.1 Management Repository Deployment Guidelines

To be sure that your management data is secure, reliable, and always available, consider the following settings and configuration guidelines when you are deploying the Management Repository:

- Install a RAID-capable Logical Volume Manager (LVM) on the system where the Management Repository resides. At a minimum the operating system must support disk mirroring and stripping. Configure all the repository data files with some redundant configuration.
- Use Real Application Clusters to provide the highest levels of availability for the repository.
- If you use Enterprise Manager to alert administrators of errors or availability issues in a production environment, be sure that the Grid Control components are configured with the same level of availability. At a minimum, consider using Oracle Data Guard to mirror the Management Repository database. Configure the Data Guard environment for no data loss.

  See Also: *Oracle High Availability Architecture and Best Practices*

  Oracle Data Guard Concepts and Administration

- You should configure your database to use at least three redo logs no less than 100MB each in size.

- Oracle strongly recommends that archive logging be turned on and that a comprehensive backup strategy be in place prior to an Enterprise Manager implementation going live in a production environment. The backup strategy should include both incremental and full backups as required.

  See Also: *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for information about the database initialization parameters required for Management Repository

- If you are using an Oracle9i database with Partitioning, you should manually analyze three specific tables in the Management Repository each time the number of targets you manages changes significantly.

  See Also: "Requirement to Manually Analyze Specific Management Repository Tables" on page 8-5

8.2 Management Repository Data Retention Policies

When the various components of Enterprise Manager are configured and running efficiently, the Oracle Management Service gathers large amounts of raw data from the Agents running on your managed hosts and loads that data into the Management Repository. This data is the raw information that is later aggregated, organized, and presented to you in Enterprise Manager Console.

After the Oracle Management Service loads information into the Repository; Enterprise Manager aggregates and purges the data over time.

The following sections describe:

- The default aggregation and purging policies used to maintain data in the Management Repository
- How you can modify how long the data is retained before it is aggregated and then purged from the repository

8.2.1 Management Repository Default Aggregation and Purging Policies

Enterprise Manager aggregates your management data by hour and by day to minimize the size of the Management Repository. Before the data is aggregated, each data point is stored in a raw data table. Raw data is rolled up, or aggregated, into a one-hour aggregated metric table. One-hour records are then rolled up into a one-day table.

After Enterprise Manager aggregates the data, the data is then considered eligible for purging. A certain period of time has to pass for data to actually be purged. This period of time is called the retention time.

The raw data, with the highest insert volume, has the shortest default retention time, which is set to 7 days. As a result, 7 days after it is aggregated into a one-hour record, a raw data point is eligible for purging.

One-hour aggregate data records are purged 31 days after they are rolled up to the one-day data table. The highest level of aggregation, one day, is kept for 365 days.

The default data retention policies are summarized in Table 8–1.

Table 8–1 Default Repository Purging Policies

Aggregate Level	Retention Time
Raw metric data	7 days
One-hour aggregated metric data	31 days
One-day aggregated metric data	365 days

Note: When you delete a target, Enterprise Manager automatically deletes all historical metric data in the next repository purge interval.

If you have configured and enabled Application Service Level Management, Enterprise Manager also gathers, saves, aggregates, and purges response time data. The response time data is purged using policies similar to those used for metric data. The Application Service Level Management purging policies are shown in Table 8–2.

Table 8–2 Default Repository Purging Policies for Application Performance Management Data

Aggregate Level	Retention Time
Raw response time data	24 hours
One-hour aggregated response time data	7 days
One-hour distribution response time data	24 hours
One-day aggregated response time data	31 days
One-day distribution aggregated response time data	31 days

8.2.2 Management Repository Default Aggregation and Purging Policies for Other Management Data

Besides the metric data and Application Performance Monitoring data, other types of Enterprise Manager data accumulates over time in the Management Repository. These other types of data, such as severities, availability records, and string metric history are retained indefinitely.

For example, the last availability record for a target will also remain in the repository indefinitely, so the last known state of a target is preserved.

8.2.3 Modifying the Default Aggregation and Purging Policies

The Enterprise Manager default aggregation and purging policies were designed to provide the most available data for analysis while still providing the best performance and disk-space requirements for the repository. As a result, you should not modify these policies to improve performance or increase your available disk space. Modifying these default policies can affect the performance of the repository and have adverse reactions on the scalability of your Enterprise Manager installation.

However, if you plan to extract or review the raw or aggregated data using data analysis tools other than Enterprise Manager, you may want to increase the amount of

raw or aggregated data available in the repository. You can accomplish this by increasing the retention times for the raw or aggregated data.

To modify the default retention time for each level of management data in the repository, you must insert additional rows into the MGMT_PARAMETERS table in the repository database. Table 8–3 shows the parameters you must insert into the MGMT_PARAMETERS table to modify the retention time for each of the raw data and aggregate data tables.

Table names that contain "_RT_" indicate tables used for Application Performance Monitoring response time data. In the **Table Name** column, replace *datatype* with one of the three response time data types: DOMAIN, IP, or URL.

Table 8–3 Parameters for Modifying Default Data Retention Times in the Management Repository

Table Name	Parameter in MGMT_ PARAMETERS Table	Default Retention Value
MGMT_METRICS_RAW	mgmt_raw_keep_window	7 days
MGMT_METRICS_1HOUR	mgmt_hour_keep_window	31 days
MGMT_METRICS_1DAY	mgmt_day_keep_window	365 days
MGMT_RT_METRICS_RAW	mgmt_rt_keep_window	24 hours
MGMT_RT_*datatype*_1HOUR	mgmt_rt_hour_keep_window	7 days
MGMT_RT_*datatype*_1DAY	mgmt_rt_day_keep_window	31 days
MGMT_RT_*datatype*_DIST_1HOUR	mgmt_rt_dist_hour_keep_window	24 hours
MGMT_RT_*datatype*_DIST_1DAY	mgmt_rt_dist_day_keep_window	31 days

For example, to change the default retention time for the table MGMT_METRICS_RAW from seven days to 14 days:

1. Use SQL*Plus to connect to the repository database as the Management Repository user.

   The default Management Repository user is `sysman`.

2. Enter the following SQL to insert the parameter and change the default value:

```
INSERT INTO MGMT_PARAMETERS (PARAMETER_NAME, PARAMETER_VALUE)
VALUES ('mgmt_raw_keep_window','14');
```

Similarly, to change from the default retention time for all of the MGMT_RT_*datatype*_1DAY tables from 31 days to 100 days:

1. Use SQL*Plus to connect to the repository database as the Management Repository user.

   The default Management Repository user is `sysman`.

2. Enter the following SQL to insert the parameter and change the default value:

```
INSERT INTO MGMT_PARAMETERS (PARAMETER_NAME, PARAMETER_VALUE)
VALUES ('mgmt_rt_day_keep_window', '100');
```

8.2.4 Modifying Data Retention Policies When Targets Are Deleted

By default, when you delete a target from the Grid Control Console, Enterprise Manager automatically deletes all target data, including raw metric data and aggregated data, from the Management Repository.

However, deleting raw and aggregated metric data for database and other data-rich targets is a resource consuming operation. Targets can have hundreds of thousands of rows of data and the act of deleting this data can degrade performance of Enterprise Manager for the duration of the deletion, especially when several targets are deleted at once.

To avoid this resource-consuming operation, you can prevent Enterprise Manager from performing this task each time you delete a target. When you prevent Enterprise Manager from performing this task, the metric data for deleted targets is not purged as part of target deletion task; instead, it is purged as part of the regular purge mechanism, which is more efficient.

In addition, Oracle strongly recommends that you do not add new targets with the same name and type as the deleted targets within 24 hours of target deletion. Adding a new target with the same name and type will result in the Grid Control Console showing data belonging to the deleted target for the first 24 hours.

To disable raw metric data deletion:

1. Use SQL*Plus to connect to the repository as the Management Repository user.

   The default repository user is SYSMAN. For example:

   ```
   SQL> connect sysman/oldpassword;
   ```

2. To disable metric deletion, run the following SQL.

   ```
   SQL> EXEC MGMT_ADMIN.DISABLE_METRIC_DELETION();
   SQL> COMMIT;
   ```

To enable metric deletion at a later point, run the following SQL:

1. Use SQL*Plus to connect to the repository as the Management Repository user.

   The default repository user is SYSMAN. For example:

   ```
   SQL> connect sysman/oldpassword;
   ```

2. To enable metric deletion, run the following SQL.

   ```
   SQL> EXEC MGMT_ADMIN.ENABLE_METRIC_DELETION();
   SQL> COMMIT;
   ```

8.3 Requirement to Manually Analyze Specific Management Repository Tables

If the Management Repository is stored in an Oracle9i database and the Partitioning option is enabled, Oracle strongly recommends that you manually analyze three specific tables in the database on a regular basis:

- MGMT_METRICS_RAW
- MGMT_METRICS_1HOUR
- MGMT_METRICS_1DAY

This requirement does not apply to Oracle Database 10*g*. To determine if Partitioning is available in your Oracle9i database, connect to the database using SQL*Plus and enter the following query:

```
SQL> SELECT VALUE FROM V$OPTION WHERE PARAMETER='Partitioning';
```

If the query returns "TRUE," then partitioning is enabled in the database and you should use the following guidelines when deciding when to analyze these tables:

- The analysis should be done after the number of targets in the EM has after you stabilized.

  For example, after you first install the Grid Control Console, there will be a period of time when you are actively adding new targets to manage. After you have deployed the Oracle Enterprise Manager 10*g* Grid Control, and after you have added most of the targets that you plan to manage, you should perform the table analysis.

- Thereafter, you should perform the analysis of the tables each time a large number of targets is added to the Grid Control Console installation.

  The statistics generated by the analysis should stay valid as long as the number of targets and collections for the targets stays the same. In other words, the manual analysis should be required only when the number of targets managed changes significantly.

Before analyzing the tables, you must stop the Enterprise Manager rollup DBMS job. You can restart the rollup job after the table analysis has completed. If the rollup job is allowed to run during the analysis, the rollup job will cause the analysis to fail by invalidating all the SQL cursors used in the analysis.

Example 8–1 shows a SQL*Plus session that demonstrates how to stop and restart the rollup job and perform the analysis on the tables.

Example 8–1 Stopping the rollup DBMS Job and Manually Analyzing Selected Management Repository Tables with SQL-Plus

```
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.4.0 - Production
With the Partitioning, Real Application Clusters, Oracle Label Security, OLAP
and Oracle Data Mining options
JServer Release 9.2.0.4.0 - Production

SQL> exec emd_maintenance.remove_em_dbms_jobs;

PL/SQL procedure successfully completed.

SQL> exec dbms_stats.gather_table_stats('SYSMAN','MGMT_METRICS_1DAY',NULL,
DBMS_STATS.AUTO_SAMPLE_SIZE, FALSE,'FOR ALL
COLUMNS',NULL,'GLOBAL',FALSE,NULL,NULL,NULL);

PL/SQL procedure successfully completed.

SQL> exec dbms_stats.gather_table_stats('SYSMAN','MGMT_METRICS_1HOUR',NULL,
DBMS_STATS.AUTO_SAMPLE_SIZE, FALSE,'FOR ALL
COLUMNS',NULL,'GLOBAL',FALSE,NULL,NULL,NULL);

PL/SQL procedure successfully completed.

SQL> exec dbms_stats.gather_table_stats('SYSMAN','MGMT_METRICS_RAW',NULL,
DBMS_STATS.AUTO_SAMPLE_SIZE, FALSE,'FOR ALL
```

```
COLUMNS',NULL,'GLOBAL',FALSE,NULL,NULL,NULL);

PL/SQL procedure successfully completed.

SQL> exec emd_maintenance.submit_em_dbms_jobs

PL/SQL procedure successfully completed.
```

8.4 Changing the SYSMAN Password

The SYSMAN account is the default super user account used to set up and administer Enterprise Manager. It is also the database account that owns the objects stored in the Oracle Management Repository. From this account, you can set up additional administrator accounts and set up Enterprise Manager for use in your organization.

The SYSMAN account is created automatically in the Management Repository database during the Enterprise Manager installation. You also provide a password for the SYSMAN account during the installation.

> **See Also:** *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for information about installing Enterprise Manager

If you later need to change the SYSMAN database account password, use the following procedure:

1. Shut down all the Oracle Management Service instances that are associated with the Management Repository.

   > **See Also:** "Controlling the Oracle Management Service" on page 2-4

2. In the Grid Control Console, click the **All Targets** tab, and then click **All Targets**.
3. Select the **Management Services and Repository** target and click **Configure**.

   Enterprise Manager displays the OMS and Repository target properties page.
4. Enter the new password in the **Repository password** field and click **OK**.

   > **See Also:** "Specifying New Target Monitoring Credentials" on page 2-13

5. Change the password of the SYSMAN database account using the following SQL*Plus commands:

   ```
   SQL>connect sysman/oldpassword;
   SQL>alter user sysman identified by newpassword;
   ```

6. For each Management Service associated with the Management Repository, locate the `emoms.properties` configuration file.

   The `emoms.properties` file can be found in the following directory of the Oracle Application Server Home where the Oracle Management Service is installed and deployed:

   ```
   IAS_HOME/sysman/config/
   ```

7. Locate the following entries in the `emoms.properties` file:

```
oracle.sysman.eml.mntr.emdRepPwd=ece067ffc15edc4f
oracle.sysman.eml.mntr.emdRepPwdEncrypted=TRUE
```

8. Enter your new password in the first entry and enter FALSE in the second entry.

   For example:

   ```
   oracle.sysman.eml.mntr.emdRepPwd=new_password
   oracle.sysman.eml.mntr.emdRepPwdEncrypted=FALSE
   ```

9. Save and exit the `emoms.properties` file and restart each Management Service associated with the Management Repository.

10. After the Oracle Management Service has started, check the contents of the `emoms.properties` file to be sure the password you entered has been encrypted.

    For example, the entries should appear as follows:

    ```
    oracle.sysman.eml.mntr.emdRepPwd=ece067ffc15edc4f
    oracle.sysman.eml.mntr.emdRepPwdEncrypted=TRUE
    ```

8.5 Dropping and Recreating the Management Repository

This section provides information about dropping the repository from your existing database and recreating the management repository after you install Enterprise Manager.

8.5.1 Dropping the Management Repository

To recreate the Management Repository, you first remove the Enterprise Manager schema from your repository database. You accomplish this task using the `-action drop` argument to the `RepManager` script, which is described in the following procedure.

To remove the Management Repository from your database:

1. Locate the `RepManager` script in the following directory of the Oracle Application Server Home where you have installed and deployed the Oracle Management Service:

   ```
   IAS_HOME/sysman/admin/emdrep/bin
   ```

2. At the command prompt, enter the following command:

   ```
   $PROMPT> RepManager repository_host repository_port repository_SID
   -sys_password password_for_sys_account -action drop
   ```

   In this syntax example:

   - *`repository_host`* is the machine name where the repository database is located
   - *`repository_port`* is the repository database listener port address, usually 1521 or 1526
   - *`repository_SID`* is the repository database system identifier
   - *`password_for_sys_account`* is the password of the SYS user for the database. For example, `change_on_install`.
   - `-action drop` indicates that you want to drop the repository.

Alternatively, you can use a connect descriptor to identify the database on the RepManager command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521)) (CONNECT_DATE=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action drop
```

> **See Also:** "Establishing a Connection and Testing the Network" in the *Oracle Database Net Services Administrator's Guide* for more information about connecting to a database using connect descriptors

8.5.2 Recreating the Management Repository

The preferred method for creating the Management Repository is to create the repository during the Enterprise Manager installation procedure, which is performed using Oracle Universal Installer.

> **See Also:** *Oracle Enterprise Manager Grid Control Installation and Basic Configuration* for information about installing Enterprise Manager

However, if you need to recreate the repository in an existing database, you can use the `RepManager` script, which is installed when you install the Oracle Management Service. Refer to the following sections for more information:

- Using the RepManager Script to Create the Management Repository
- Using a Connect Descriptor to Identify the Management Repository Database

8.5.2.1 Using the RepManager Script to Create the Management Repository

To create a repository in an existing database:

1. Review the hardware and software requirements for the Management Repository as described in *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*. and review the section "Management Repository Deployment Guidelines" on page 8-1.
2. Locate the `RepManager` script in the following directory of the Oracle Management Service home directory:

   ```
   ORACLE_HOME/sysman/admin/emdrep/bin
   ```

3. At the command prompt, enter the following command:

   ```
   $PROMPT> ./RepManager repository_host repository_port repository_SID
   -sys_password password_for_sys_account -action create
   ```

In this syntax example:

- *`repository_host`* is the machine name where the repository database is located
- *`repository_port`* is the repository database listener port address, usually 1521 or 1526
- *`repository_SID`* is the repository database system identifier

- *password_for_sys_account* is the password of the SYS user for the database. For example, change_on_install.

Enterprise Manager creates the repository in the database you specified in the command line.

8.5.2.2 Using a Connect Descriptor to Identify the Management Repository Database

Alternatively, you can use a connect descriptor to identify the database on the RepManager command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action create
```

> **See Also:** "Establishing a Connection and Testing the Network" in the *Oracle Database Net Services Administrator's Guide* for more information about connecting to a database using a connect descriptor

The ability to use a connect string allows you to provide an address list as part of the connection string. The following example shows how you can provide an address list consisting of two listeners as part of the RepManager command line. If a listener on one host becomes unavailable, the second listener can still accept incoming requests:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=
(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCP)(HOST=host1)(PORT=1521)
(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521)
(CONNECT_DATE=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action create
```

> **See Also:** *Oracle High Availability Architecture and Best Practices*
>
> "Configuring the Management Service to Use Oracle Net Load Balancing and Failover" on page 3-18

8.6 Troubleshooting Management Repository Creation Errors

Oracle Universal Installer creates the Management Repository using a configuration step at the end of the installation process. If the repository configuration tool fails, note the exact error messages displayed in the configuration tools window, wait until the other configuration tools have finished, exit from Universal Installer, and then use the following sections to troubleshoot the problem.

8.6.1 "Package Body Does Not Exist" Error While Creating the Repository

If the creation of your Management Repository is interrupted, you may receive the following when you attempt to create or drop the Management Repository at a later time:

```
SQL> ERROR:
ORA-00604: error occurred at recursive SQL level 1
ORA-04068: existing state of packages has been discarded
ORA-04067: not executed, package body "SYSMAN.MGMT_USER" does not exist
```

```
ORA-06508: PL/SQL: could not find program unit being called
ORA-06512: at "SYSMAN.SETEMUSERCONTEXT", line 5
ORA-06512: at "SYSMAN.CLEAR_EMCONTEXT_ON_LOGOFF", line 4
ORA-06512: at line 4
```

To fix this problem, see "General Troubleshooting Techniques for Creating the Repository" on page 8-11.

8.6.2 "Server Connection Hung" Error While Creating the Repository

If you receive an error such as the following when you try to connect to the repository database, you are likely using an unsupported version of the Oracle Database:

```
Server Connection Hung
```

To remedy the problem, upgrade your database to the supported version as described in *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*.

8.6.3 General Troubleshooting Techniques for Creating the Repository

If you encounter an error while creating the Management Repository, drop the repository by running the `-drop` argument to the RepManager script.

See Also: "Dropping the Management Repository" on page 8-8

If the RepManager script drops the repository successfully, try creating the repository again.

If you encounter errors while dropping the repository, do the following:

1. Connect to the database as SYSDBA using SQL*Plus.
2. Check to see if the SYSMAN database user exists in the repository database.

   For example, use the following command to see if the SYSMAN user exists:

   ```
   prompt> SELECT username FROM DBA_USERS WHERE username='SYSMAN';
   ```

3. If the SYSMAN user exists, drop the user by entering the following SQL*Plus command:

   ```
   prompt> DROP USER SYSMAN CASCADE;
   ```

4. Check to see if the following triggers exist:

   ```
   SYSMAN.EMD_USER_LOGOFF
   SYSMAN.EMD_USER_LOGON
   ```

   For example, use the following command to see if the EMD_USER_LOGOFF trigger exists in the database:

   ```
   prompt> SELECT trigger_name FROM ALL_TRIGGERS
           WHERE trigger_name='EMD_USER_LOGOFF';
   ```

5. If the triggers exist, drop them from the database using the following commands:

   ```
   prompt> DROP TRIGGER SYSMAN.EMD_USER_LOGOFF;
   prompt> DROP TRIGGER SYSMAN.EMD_USER_LOGON;
   ```

9

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

9.1 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

9.1.1 Configuring the Management Agent to Use a New Management Service

When you install the Management Agent on a managed host, you associate the 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 Agent requires no changes to the Management Service. The reconfigured Agent will begin communicating with the new Management Service after the Agent is restarted.

To associate the Management Agent with a new Management Service after you have installed the Agent:

1. Stop the Management Agent.

See Also: "Controlling the Oracle Management Agent" on page 2-1

2. Locate the `emd.properties` file in the 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/
   ```

8. Restart the Management Agent.

9.1.2 Changing the Management Agent Port

The Oracle 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 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 Agent port.

To change the Management Agent port:

1. Stop the Management Agent.

   See Also: "Controlling the Oracle Management Agent" on page 2-1

2. Locate the `emd.properties` file in the 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 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.

9.1.3 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 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 the this value is exceeded, the Management Agent stops collected 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.

   See Also: "Controlling the Oracle Management Agent" on page 2-1

2. Locate the `emd.properties` file in the 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 9–1.
4. Save your changes and exit the file.
5. Restart the Management Agent.

Table 9–1 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 repository reduces the amount of collected data in the upload directory.

Table 9–1 (Cont.) Properties for Controlling the Disk Space Used by the Management

Property	Explanation
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. The Management Agent will be 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.

9.1.4 About the Management Agent Watchdog Process

The Oracle 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` script located in the following directory of the Management Agent home directory:

```
AGENT_HOME/bin/emwd
```

You can identify the watchdog process by using the following command UNIX systems:

```
$PROMPT> ps -ef | grep emwd
```

9.1.5 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
- Troubleshooting Management Agent Time Zone Problems
- Troubleshooting Oracle Management Service Time Zone Problems

9.1.5.1 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
```

9.1.5.2 Troubleshooting Management Agent Time Zone Problems

Sometimes, during the Management Agent installation, the time zone detected by the 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 the an error similar to the following:

```
Could not determine agent time zone. Please refer to 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 9–2, depending upon which Enterprise Manager product you are using.

Table 9–2 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`

> **See Also:** "Locating and Configuring Management Agent Log and Trace Files" on page 7-1 for more information about the Oracle Management Agent log files

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 this `emctl config agent getTZ` command.

   This is the time zone of the host computer.

3. Use a 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 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.

9.1.5.3 Troubleshooting Oracle Management Service Time Zone Problems

Section 9.1.5.2 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 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 9–2, 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 9-5 for instructions on changing the time zone assigned to the Management Agent

9.2 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 Repository
- Configuring the Management Service to Use a New Port

9.2.1 Configuring the Management Service to Use a New 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 of the Oracle Application Server Home where the Oracle Management Service is installed and deployed:

```
IAS_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.

9.2.1.1 Changing the Repository Properties in the emoms.properties File

To associate the Oracle Management Service with a new repository, you must modify the repository properties saved in the `emoms.properties` configuration file:

1. Stop the Management Service.

   See Also: "Controlling the Oracle Management Service" on page 2-4

2. Locate the `emoms.properties` file in the following directory of the Oracle Application Server Home where you installed and deployed the Management Service:

   ```
   AS_HOME/sysman/config/
   ```

3. Edit the `emoms.properties` file by updating the appropriate values for the properties described in Table 9–3.

   Example 9–1 shows sample entries in the `emoms.properties` file.

4. Restart the Management Service.

Table 9–3 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. The default value is `sysman`, but when you open the file you will notice that the value for this property is an encrypted string. Remove the encrypted string and enter the management password for the new Management Repository.

Table 9–3 (Cont.) Repository Properties in the emoms.properties File

Property	Description
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.
emdRepPwdEncrypted	This property must be set to FALSE so you can manually modify the management password (`emdRepPwd`) property. For more information, see "About Changing the Repository Password" on page 9-8.

Example 9–1 Sample Repository Properties in the emoms.properties File

```
oracle.sysman.eml.mntr.emdRepUser=SYSMAN
oracle.sysman.eml.mntr.emdRepPwd=sysman
oracle.sysman.eml.mntr.emdRepPwdEncrypted=false
oracle.sysman.eml.mntr.emdRepSID=oemrep1
oracle.sysman.eml.mntr.emdRepServer=system12.mycompany.com
oracle.sysman.eml.mntr.emdRepPort=1521
```

9.2.1.2 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. For this reason, when you edit the `emoms.properties` file after the Management Service has been started at least once, you will notice that the `emdRepPwdEncrypted` property is set to TRUE.

As a result, to modify the repository password, you must do the following:

1. Stop the Management Service.
2. Open the `emoms.properties` file.
3. Change the `emdRepPwdEncrypted` property to FALSE.
4. Change the `emdRepPwd` property to the new password.
5. Save the changes and close the `emoms.properties` file.
6. Restart the Management Service.

   When the Management Service starts, it opens the `emoms.properties` file, encrypts the password, and changes the `emdRepPwdEncrypted` property to TRUE.

9.2.2 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.

> **See Also:** "Controlling the Oracle Management Service" on page 2-4

2. Locate the following `httpd_em.conf` file located in the following directory in the Oracle Application Server home directory where you installed and deployed the Management Service:

   ```
   AS_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. Locate the `emoms.properties` file in the same `sysman/config` directory.
6. 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
   ```

7. Restart the Management Service.
8. Reconfigure each 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 9-1

10

Migrating from Previous Versions of Enterprise Manager

This chapter discusses the migration procedure used to move from a previous version of Oracle Enterprise Manager to the new Oracle Enterprise Manager 10*g* environment. This chapter contains the following topics:

10.1 Overview of the Enterprise Manager Migration Process

This chapter describes how to migrate from the following versions of Enterprise Manager:

- Oracle Enterprise Manager Release 2.2
- Oracle Enterprise Manager Release 9.0.1
- Oracle Enterprise Manager Release 9.2

Migrating your existing Enterprise Manager framework to the Oracle Enterprise Manager 10*g* environment involves two steps:

- Making targets within your managed environment monitorable using the new framework by installing Oracle Enterprise Manager 10*g* Management Agents on hosts that are running your managed targets
- Migrating information about users, privileges, groups, and preferred credentials from the old management repository to the new Oracle Enterprise Manager 10*g* Management Repository.

Once you have completed migrating to the new framework, you may wish to change the default metric thresholds for groups of managed targets within your enterprise.

See Also: "Configuring Metric Thresholds" on page 10-8

10.2 Requirements for Migrating from Previous Versions of Enterprise Manager

Before beginning the migration process, ensure that the following list of requirements is satisfied:

- The previous version of complete Enterprise Manager Framework (Release 2.2, 9.0.1, or 9.2) must be up and running, including the Enterprise Manager Console, Oracle Management Server, Repository, and Intelligent Agents. The migration procedure uses the Job system in the previous version of Enterprise Manager to deploy the Oracle Enterprise Manager 10*g* Management Agents.
- The Oracle Enterprise Manager 10*g* Grid Control Console must be installed and running ona network host. Specifically, the Management Service must be up and running and available to the Oracle Enterprise Manager 10*g* Management Agents that you will install on your managed hosts.
- You must have the credentials for the Enterprise Manager Administrator Account for both the previous version of Enterprise Manager, as well as for Oracle Enterprise Manager 10*g*. Account read/write privileges are required for any machine currently running the Release 2.2, 9.0.1 or 9.2 Intelligent Agent.
- You must have the Database User and Password for the previous version of the Enterprise Manager Repository Database, as well as for the Oracle Enterprise Manager 10*g* Management Repository database.
- You must have 375 Megabytes of free disk space on each host where an Management Agent is to be installed.
- You must have installed the latest system and software patches for the Oracle Enterprise Manager 10*g* environment. Note that the system and software patch requirements for the Oracle Enterprise Manager 10*g* Grid Control Console are significantly different from previous versions of Enterprise Manager.

See Also: *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*

10.3 The Oracle Enterprise Manager 10*g* Migration Process

Migrating from a previous version of Enterprise Manager to the Oracle Enterprise Manager 10*g* Grid Control is a two-stage process. The following sections describe each stage in the process:

- Deploying and Configuring Oracle Enterprise Manager 10g Management Agents
- Migrating Management Repository Data

10.3.1 Deploying and Configuring Oracle Enterprise Manager 10*g* Management Agents

Deploying Oracle Enterprise Manager 10*g* Management Agents on machines running targets managed by an older version of Enterprise Manager makes these targets monitorable via Oracle Enterprise Manager 10*g*. To simplify and automate Management Agent deployment, a Tcl script is provided that is submitted as a job from an Enterprise Manager Release 2.2, Release 9.0.1, or Release 9.2 Job system. The deployment script (`agentIntallJob.tcl`) can be found in the Oracle Enterprise Manager 10*g* home directory at the following location:

```
%ORACLE_HOME/sysman/agent_download/agentInstallJob.tcl
```

Deployment of the Oracle Enterprise Manager 10*g* Management Agent is carried out in two phases:

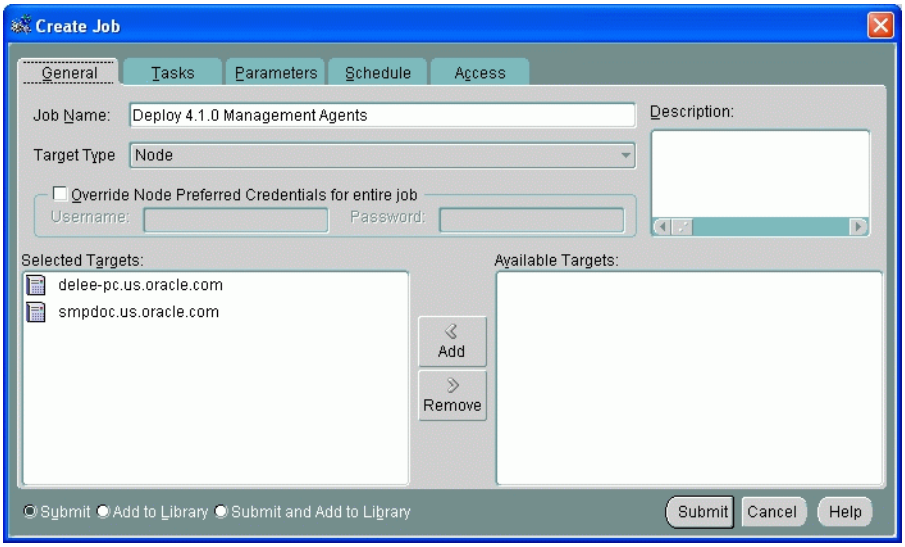
- Deploying the Oracle Enterprise Manager 10g Management Agents Using the Release 2.2, Release 9.0.1, or Release 9.2 Job System

- Configuring the Oracle Enterprise Manager 10g Management Agents for Use with the Oracle Enterprise Manager 10g Job System (UNIX Systems Only)

10.3.1.1 Deploying the Oracle Enterprise Manager 10*g* Management Agents Using the Release 2.2, Release 9.0.1, or Release 9.2 Job System

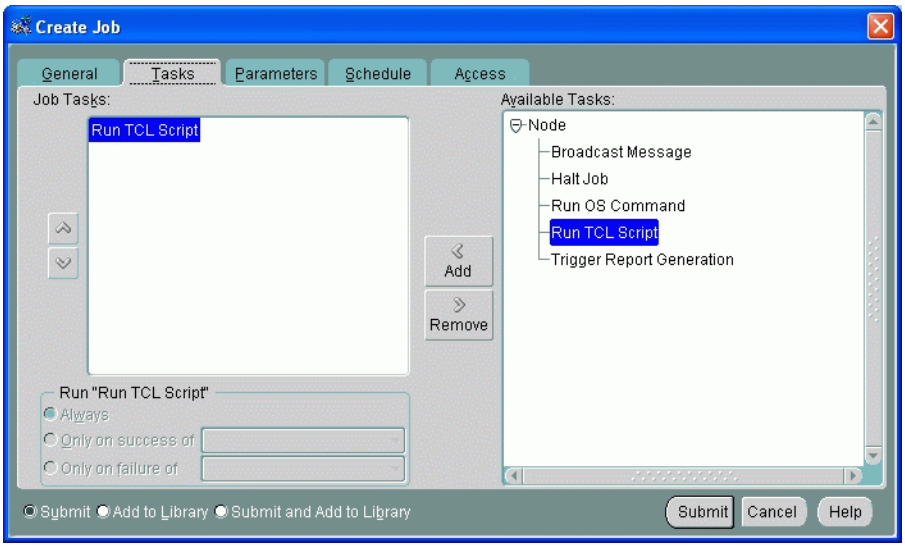
The `agentInstallJob.tcl` script must be run as a Tcl job from an Enterprise Manager Release 2.2, Release 9.0.1, or Release 9.2 Console. As shown in Figure 10–1, you define the job by choosing a "Node" target type and then selecting the machines on which the Oracle Enterprise Manager 10*g* Management Agents are to be installed.

Figure 10–1 Selecting Machines for Management Agent Deployment



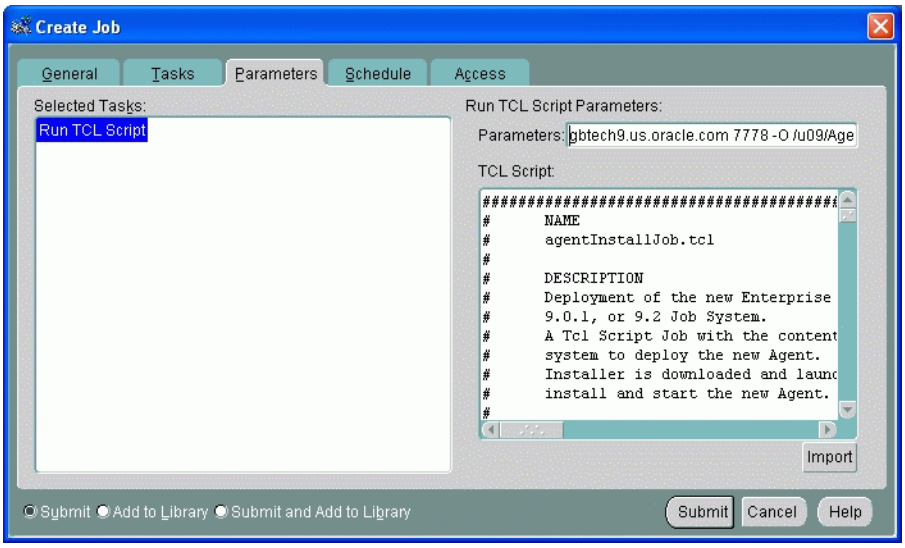
Once you have selected where the Management Agents are to be deployed, you need to define an installation task using `agentInstallJob.tcl`. As shown in Figure 10–2, select the "Run TCL Script" task.

Figure 10–2 Choosing the Run TCL Script Task



The next step involves defining the functional core of the job. As shown in Figure 10–3, you need to copy the content of the `agentInstallJob.tcl` script into the text entry area using either the Import function or manually copying and pasting the entire script into the TCL Script text entry area.

Figure 10–3 Copying agentInstallJob.tcl and Specifying Job Parameters



In addition to importing the script content, you must specify operational parameters required by the script to install the Oracle Enterprise Manager 10*g* Management Agent. As shown in Figure 10–3, you enter these parameters in the **Run TCL Script Parameters** field. The parameters are:

- The Oracle Management Service host

  Example: `mgmthost1.acme.com`

- HTTP Port Number

  Example: `7778`

- Directory Type (-o or -f)

  Usage:

  -o Identical installation directory structure on all machines.

  -f Different installation directory structure on various machines (specified in text file)

- Directory Argument

  Example: `/u09/agent/agent_41`

Example 10–1 and Example 10–2 show the format and syntax used to specify these parameters in the **Run TCL Script Parameters** field.

Example 10–1 Same Installation Directory Structure on All Machines

```
mgmthost1.acme.com 7778 -o /u09/Agent/Agent_41
```

Example 10–2 Different Installation Directory Structure on Different Machines

```
mgmthost1.acme.com 7778 -f hostname_lookup.txt
```

10.3.1.1.1 More About the Directory Type Parameter The Directory Type parameter offers two options either "-o" or "-f" plus the Directory Argument which consists of either a default directory (-o option) or host lookup file (-f option). As mentioned in the previous section, the "-o" option specifies that the same Management Agent home directory structure be created on all machines where the Management Agent is to be installed. For example, if the `agentInstallJob.tcl` job is submitted against MACHINE1, MACHINE2, and MACHINE3 using the following job parameters:

```
mgmthost1.acme.com 7778 -o /u09/agent/agent_41
```

The `agentInstallJob.tcl` script will create the `/u09/agent/agent_41` directory on each of the three machines. Once created, this directory is used by the Oracle Universal Installer (OUI) as an installation staging area. This directory eventually becomes the Oracle Enterprise Manager 10*g* Management Agent Home.

> **Note:** The agentInstallJob.tcl job runs OUI in silent mode to perform the actual Management Agent installation operations.

In contrast, the "-f" option specifies that different installation/Agent Home directory structures be created for specific machines. Before creating a TCL job with this option you must first create a flat text file listing each machine name and corresponding directory for that host. The flat file MUST reside in the Oracle Enterprise Manager 10*g* Management Service Home in the following directory:

```
OMS_HOME/sysman/agent_download
```

In the following example, the lookup file parsed by the TCL job is named hostname_ lookup.txt.

```
mgmthost1.acme.com 7778 -f hostname_lookup.txt
```

When a TCL job is submitted using the "-f" option, the job first obtains the name of the target machine by executing the "hostname" command. The result is then compared against entries in the hostname lookup file. If the hostname is found in the file, the associated directory structure is used. If the hostname is not found, then the directory structure specified for the "wildcard" character is used. The wildcard can be used as a default entry in case the TCL job cannot locate a particular hostname within the file. A wildcard entry is designated by a "*" and must be the last entry as the file is parsed from top to bottom.

Example 10–3 shows the format for a sample hostname lookup file. In the example, you have 20 machines in your enterprise where you want Oracle Enterprise Manager 10*g* Management Agents installed. You want the same Agent Home directory structure created on all machines except HOST1, HOST2, and HOST3.

Example 10–3 Sample Hostname Lookup File

```
HOST1/oracle_home1/agent/agent_install
HOST2/ora_host2/agent_install
HOST3/orahome_host3/agent/install
*/ora_agent/agent/install
```

The TCL job (submitted to HOST2) runs the hostname command and receives HOST2 as the output. This output is then cross-referenced with all entries within the hostname_lookup.txt file. Since HOST2 is an entry in the hostname_lookup.txt file, the TCL job knows to create the Oracle Enterprise Manager 10*g* Management Agent Home in `/ora_host2/agent_install`. HOST1, HOST2, and HOST3 will have unique

directories. The Management Agent home directory for the remaining 17 machines will be `/ora_agent/agent/install`.

Because the TCL job, or more specifically OUI, creates files and directories on the target machines, full read/write privileges for the Enterprise Manager administrator account running the job are required. When the installation is compete the new Oracle Enterprise Manager 10*g* Management Agent is started automatically and begins retrieving host, database, and listener information. This information is then uploaded via HTTP or HTTPS to the new Enterprise Manager 10*g* management repository where it becomes available to the Grid Control for viewing.

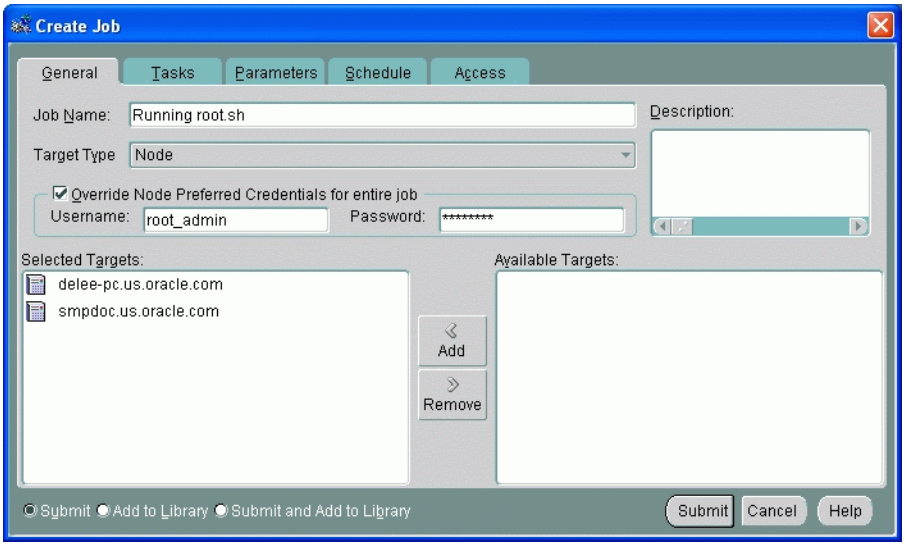
10.3.1.2 Configuring the Oracle Enterprise Manager 10*g* Management Agents for Use with the Oracle Enterprise Manager 10*g* Job System (UNIX Systems Only)

Once the Oracle Enterprise Manager 10*g* Management Agents are operational, you need to configure each Management Agent for use with the new Oracle Enterprise Manager 10*g* job system. This step consists of running the `root.sh` script on each machine where the Management Agent is installed. This script is located in the Management Agent Home of the host machine. Specifically, the root.sh script grants root privileges to the Oracle Enterprise Manager 10*g* Management Agent. Therefore, the root user and password for that machine are required in order to run root.sh.

As with the agentInstallJob.tcl script you can automate this task by running the `root.sh` script using the Enterprise Manager Release 2.2, Release 9.0.1, or Release 9.2 Job system. To do this, you create an "OS command" job that executes "root.sh" on all machines requiring Management Agent configuration. As shown in the Figure 10–4, preferred credentials should be overridden by the root user and password of the target host.

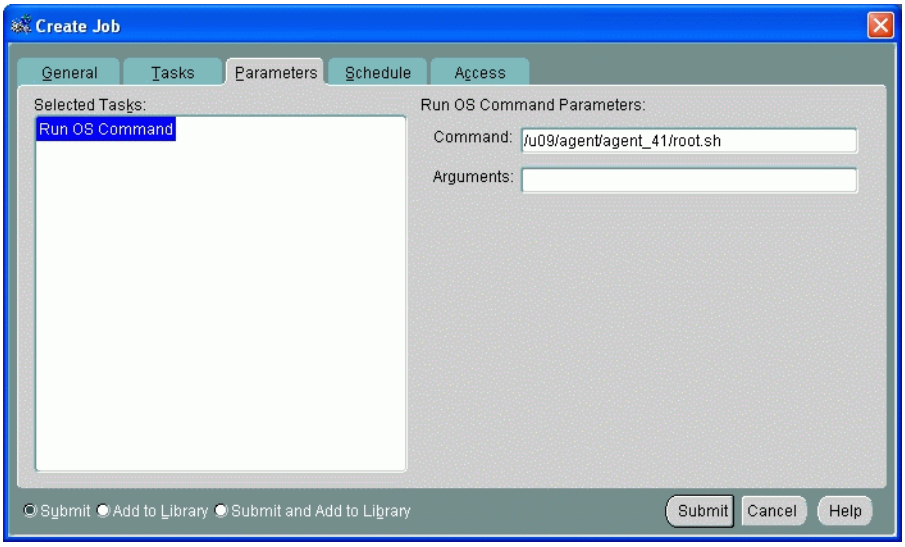
> **Note:** The Preferred Credential Override is available with Enterprise Manager Release 9.2 systems only. For older versions of Enterprise Manager, you must run the job as a user with preferred credentials allowing root access.

Figure 10–4 Overriding Preferred Credentials



On the job Parameters page (Figure 10–5), specify "root.sh" in the **Command** field as shown in the following figure and submit the job for execution. You must specify the full path to the root.sh script. For example: `/u09/agent/agent_41/root.sh`

Figure 10–5 Command Parameters



The Oracle Enterprise Manager 10*g* Management Agent can be up and running when `root.sh` is executed and does not need to be restarted after the configuration process has been completed.

> **Note:** In previous releases of Enterprise Manager, job system configuration was part of the Intelligent Agent install. With the Enterprise Manager 10*g* release, this configuration is now a separate step due to architectural differences between the old and new frameworks.

10.3.2 Migrating Management Repository Data

Once the Oracle Enterprise Manager 10*g* Management Agents have been deployed and configured, the next step is to migrate information about users, privileges, groups, and preferred credentials from the original Management Repository to the Oracle Enterprise Manager 10*g* Management Repository.

> **Note:** Privileges, group membership, and preferred credentials are migrated for databases, listeners, and hosts only.

Both Enterprise Manager 9*i* and Oracle Enterprise Manager 10*g* save and encrypt all administrator accounts and preferred credentials in the repository. In order to migrate all of these accounts over to Enterprise Manager 10*g*, you must run the Migration Utility from the Enterprise Manager 10*g* home. This command line utility can be found in the following directory:

```
%EM_HOME%\bin\repo_mig
```

The Migration Utility requires the repository user and password for both the original Management Repository database and for the new Oracle Enterprise Manager 10*g*

Management Repository database. You execute the utility and specify operational parameters using the following format:

```
repo_mig -preview|-migrate source_user/source_pwd@source_service dest_user/dest_
pwd@dest_service
```

where:

- -preview: Generates a preliminary migration report without carrying out the migration.
- -migrate: Performs migration of groups, administrators, target privileges, and preferred credentials of hosts, databases, and listeners.
- source_user: Source OEM repository user name
- source_pwd: Source OEM repository password
- source_service: Source OEM repository service. For example, Host:Port:SID
- dest_user: Destination OEM repository user name
- dest_pwd: Destination OEM repository password
- dest_service: Destination OEM repository service. (Host:Port:SID)

Once the migration is complete, the account information is then saved and encrypted. The passwords on all of the accounts will remain the same.

10.4 Configuring Metric Thresholds

As mentioned previously, migration only involves transferring users, privileges, groups, and preferred credentials to the Enterprise Manager 10*g* framework; any event test thresholds that existed in your previous version of Enterprise Manager will not be transferred.

Enterprise Manger 10*g* provides out-of-the-box monitoring that simplifies a critical but potentially time-consuming task of setting up monitoring for managed targets. As you add targets to Enterprise Manager, options are automatically provided to monitor the target at a recommended or at a minimum level. Each level of monitoring consists of a set of metrics and predefined thresholds that are based on Oracle recommendations for those levels. You may choose to use these Oracle recommendations, or you can change these thresholds to suit your particular needs.

> **See Also:** The Enterprise Manager online help for specific information on modifying metric thresholds

10.4.1 Copying Metric Thresholds to Multiple Targets

Your Enterprise Manager 10*g* installation may be monitoring a very large number of targets, making it inconvenient to manually change metric threshold values for each monitored target. Enterprise Manager 10*g* provides an easy way to copy metric thresholds from one target to any number of targets as long as they are the same target type: You simply set new metric thresholds for a single target and then have Enterprise Manager propagate these settings to all other targets of the same type.

To copy metric thresholds, select the Manage Metrics link (located in the Related Links section) from any target home page that offers this capability and follow the instructions given on the web page. For more information about metric threshold settings, see Enterprise Manager 10*g* online help.

11

Configuring Notifications

The notification system can, in addition to notifying administrators, automate responses to alerts by executing operating system commands (including scripts) and PL/SQL procedures. This capability allows you to implement specific IT practices in response to specific alerts. For example, if an alert is generated when monitoring the operational (up/down) status of a database, you may want the notification system to automatically open an in-house trouble-ticket using an OS script so that the appropriate IT staff can respond in a timely manner.

By using Simple Network Management Protocol (SNMP) traps, the Enterprise Manager notification system also allows you to access SNMP-enabled third-party applications such as HP OpenView. Some administrators may want to send third-party applications a notification when a certain metric has exceeded a threshold.

Specifically, this chapter contains the following sections:

11.1 Setting Up Notifications

Notifications are configured using Notification Methods and Notification Rules.

- Notification Methods are the mechanisms by which alerts are sent. Enterprise Manager superusers can setup e-mail notifications by configuring the 'e-mail' notification method. Most likely this would already have been setup as part of the Oracle Management Service installation.

  Enterprise Manager superusers can also define other custom notification methods. For example, alerts may need to be forwarded to a 3rd party trouble-ticketing system. Assuming APIs to the third-party trouble-ticketing system are available, a custom notification method can be created to call a custom OS script that has the

appropriate APIs. The custom notification method can be named in a user-friendly fashion, for example, "Log trouble ticket". Once that's defined, any time an administrator needs to send alerts to the trouble-ticketing system, he merely needs to invoke the now globally available notification method called "Log trouble ticket".

Custom notification methods can be defined based on any custom OS script, any custom PL/SQL procedure, or by sending SNMP traps.

- A notification rule is a user-defined rule that instructs Enterprise Manager on how alerts should be sent. Specifically, in each rule, you can specify the alert conditions you're interested in and the notification methods that should be used for sending these alerts. For example, you can set up a rule such that when any database goes down, e-mail should be sent and the "log trouble ticket" notification method should be called. Or you can define another rule such that when the CPU or Memory Utilization of any host reach critical severities, SNMP traps should be sent to another management console. During notification rule creation, you specify the targets you are interested in, their monitored metrics and severity conditions (clear, warning, critical), and the associated notification method.

11.2 Managing Notification Methods

Notification Methods allow you to define different mechanisms for sending notifications. These include e-mail, SNMP traps, or running custom scripts, or all three. Once defined, these methods can then be used with Notification Rules for sending notifications to administrators as a result of alert occurrences.

Through the Notification Methods page, you can:

- Set up the outgoing mail servers if you plan to send e-mail notifications through notification rules
- Create other custom notification methods using OS and PL/SQL scripts and SNMP traps.

11.2.1 Setting Up a Mail Server for Notifications

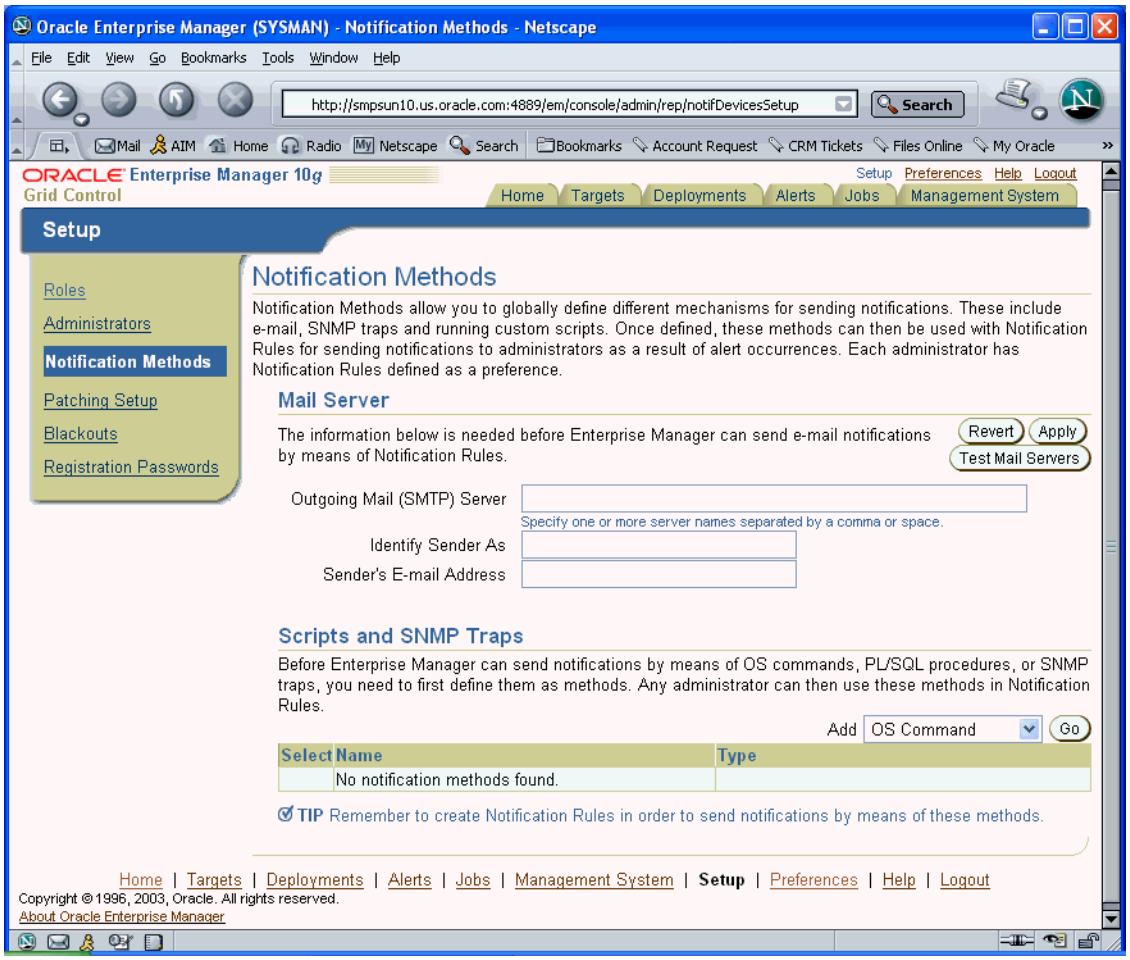
Before Enterprise Manager can send e-mail notifications using Notification Rules, you must first set up the Outgoing Mail (SMTP) servers using the Notification Methods page (Figure 11–1). Display the Notification Methods page by clicking **Setup** on any page in the Grid Control Console and clicking **Notification Methods** in the vertical navigation bar. Only privileged users can configure SMTP servers.

Specify one or more outgoing mail (SMTP) server names, the name you want to appear as the sender of the notification messages, and the e-mail address you want to use to send your e-mail notifications. This address, called the Sender's Mail Address, must be a valid address on each mail server that you specify. This e-mail address will be notified by the mail server of any problem encountered during the sending of an e-mail notification. See Example 11–1.

Example 11–1 Mail Server Settings

```
Outgoing Mail (SMTP Server) smtp01.oracle.com, smtp02.oracle.com
Identify Sender As Enterprise Manager Notifications
Sender's Mail Address mgmt_rep@oracle.com
```

Figure 11–1 Defining a Mail Server



> **Note:** The e-mail address you specify on this page is not the e-mail address to which the notification is sent. You will have to specify the e-mail address (where notifications will be sent) from the Preferences General page. For information on specifying e-mail addresses for e-mail notification, see Specifying E-mail address for E-mail Notifications.

After configuring the e-mail server, click **Test Mail Servers** to verify your e-mail setup. You should verify that an e-mail message was received by the e-mail account specified in the **Sender's E-mail Address** field.

Defining multiple mail servers will improve the reliability of e-mail notification delivery and spread the load across multiple systems. The Management Service makes use of each mail server to send e-mails and the behavior is controlled by the following parameters found in the $ORACLE_HOME/sysman/config/emoms.properties file.

Example 11–2 Management Service Parameters

```
# The maximum number of emails that can be sent in a single connection to an
# email server
# em.notification.emails_per_connection=20
#
# The maximum number of emails that can be sent in a minute
```

```
# em.notification.emails_per_minute=250
```

Based on the defaults in Example 11–2, the first mail server is used to send 20 e-mails before the Management Service switches to the next mail server which is used to send another 20 e-mails before switching to the next mail server. This prevents one mail server from becoming overloaded and should improve overall reliability and throughput.

11.2.2 Custom Notification Methods using Scripts and SNMP Traps

You can create other custom notification methods based on OS scripts, PL/SQL procedures, or SNMP traps. Any administrator can then use these methods in Notification Rules.

11.2.2.1 Adding a Notification Method based on an OS Command

You can specify an Operating System command or script that will be called in Notification Rules. The OS Command is run as the user who started the Management Service. The OS command (or script) must exist and be placed on each Management Service host machine that connects to the Management Repository.

> **Note:** Notification methods based on OS commands must be configured by an administrator with superuser privileges before users can choose to select one or more of these OS command methods while creating/editing a notification rule.

The following information is required for each OS command notification method:

- Name
- Description

  Both Name and Description should be clear and intuitive so that the function of the method is clear to other administrators.

- OS Command

You must enter the full path of the OS command or script in the OS command field (for example, `/u1/bin/myscript.sh`). For environments with multiple Management Services, the path must be exactly the same on each machine that has a Management Service. Command line parameters can be included after the full path (for example, /u1/bin/myscript.sh arg1 arg2).

To define a notification method based on an OS command, perform the following steps.

1. Create an OS command on the repository host machine.

   Create an OS Command on each Management Service machine that connects to the Management Repository. The OS Command should be an absolute path name and must be the same on each Management Service host machine, for example, /u1/bin/logSeverity.sh. The command is run by the user who started the Management Service. If an error is encountered during the running of the OS Command, the Notification System can be instructed to retry the sending of the notification to the OS Command by returning an exit code of 100. The procedure is initially retried after one minute, then two minutes, then three minutes and so on, until the notification is a day old, at which point it will be purged.

Example 11–3 shows the parameter in emoms.properties that controls how long the OS Command can execute without being killed by the Management Service. This is to prevent OS Commands from running for an inordinate length of time and blocking the delivery of other notifications. By default the command is allowed to run for 30 seconds before it is killed.

Example 11–3 Parameter in emoms.properties File

```
# The amount of time in seconds after which an OS Command started by the
# Notification System will be killed if it has not exited
# em.notification.os_cmd_timeout=30
```

2. Add this OS command as a notification method that can be called in Notification Rules. See "Adding a Notification Method based on an OS Command" on page 11-4.
3. Define a notification rule (choose the targets and conditions for which you want to be notified), and associate the OS command with the rule. See "Creating Your Own Notification Rules" on page 11-17.

Example 11–4 shows an example of the required information.

Example 11–4 OS Command Notification Method

```
Name Trouble Ticketing
Description Notification method to log trouble ticket for a severity occurrence
OS Command /private/mozart/bin/logTicket.sh
```

> **Note:** There can be more than one OS Command configured per system.

Information about the metrics in alert can be made available to your OS notification method. See "Passing Metric Severity Information" on page 11-8 for more details.

11.2.2.2 Adding a Notification Method Based on a PL/SQL Procedure

Before setting up the method, the procedure must be created on the repository database. Using the database account of the repository owner (such as SYSMAN).

The procedure must have the following signature:

PROCEDURE p(severity IN MGMT_NOTIFY_SEVERITY)

> **Note:** The notification method based on a PL/SQL procedure must be configured by an administrator with superuser privileges before a user can select it while creating/editing a notification rule.

Information about the metrics in alert can be made available to your PL/SQL procedure. See "Passing Metric Severity Information" on page 11-8 for more details.

Next, create a notification method based on your PL/SQL procedure. The following information is required when defining the method:

- Name
- Description
- PLSQL Procedure

You must enter a fully qualified procedure name (for example, OWNER.PKGNAME.PROCNAME) and ensure that the owner of the Management Repository has execute privilege on the procedure.

To define a notification method based on a PL/SQL procedure, perform the following steps.

1. Create the PL/SQL procedure on the repository database using the following procedure specification:

   PROCEDURE p(severity IN MGMT_NOTIFY_SEVERITY)

   If an error is encountered during the running of the procedure, the Notification System can be instructed to retry the sending of the notification to the procedure by raising a user defined exception that uses the error code -20000. See the example above. The procedure initially retried after one minute, then two minutes, then three minutes and so on, until the notification is a day old, at which point it will be purged.

2. Add this PLSQL procedure as a notification method that can be called in Notification Rules. See "Adding a Notification Method Based on a PL/SQL Procedure" on page 11-5.

   Make sure to use a fully qualified name that includes the schema owner, package name and procedure name. The procedure will be executed by the repository owner and so the repository owner must have execute permission on the procedure.

3. Associate the PL/SQL procedure with a notification rule.

An example of the required information is shown in Example 11–5.

Example 11–5 PL/SQL Procedure Required Information

```
Name Cleanup error log
Description Notification method to clean up the error log table
PLSQL Procedure mgmt_rep.log_util.cleanup_log
```

There can be more than one PL/SQL-based method configured per system.

For information about the severity types that relate to a target's availability, and how metric severity information is passed to the PLSQL procedure, see "Passing Metric Severity Information" on page 11-8 for more details.

11.2.2.3 Adding a Notification Method Based on an SNMP Trap

Enterprise Manager supports integration with third-party management tools through the SNMP. For example, you can use SNMP to notify a third-party application that a selected metric has exceeded its threshold.

The trap is an SNMP Version 1 trap and is described by the MIB definition shown at the end of this chapter. See "Management Information Base (MIB)" on page 11-21.

For more comprehensive configuration information, see the documentation specific to your platform; SNMP configuration differs from platform to platform.

Note: Notification methods based on SNMP traps must be configured by an administrator with superuser privileges before any user can then choose to select one or more of these SNMP trap methods while creating/editing a notification rule.

You must provide the name of the host (machine) on which the SNMP master agent is running and other details as shown in the following example. In Example 11–6, the SNMP host will receive your SNMP traps.

Example 11–6 SNMP Trap Required Information

```
Name HP OpenView Console
Description Notification method to send trap to HP OpenView console
SNMP Trap Host Name machine1.us.oracle.com
SNMP Host Port 162
SNMP Community public
This SNMP host will receive your SNMP traps.
```

Note: A Test Trap button exists for you to test your setup.

Metric severity information will be passed as a one-line message in the SNMP trap.

An example SNMP Trap is shown in Example 11–7. All information is in one line which is sent as a variable embedded in the SNMP Trap.

Example 11–7 SNMP Trap

```
Tue Oct 28 05:00:02 2003

Command: 4
   Enterprise: 1.3.6.1.4.1.111.15.2
   Agent: 138.1.6.200
   Generic Trap: 6
   Specific Trap: 1
   Time Stamp: 8464:39.99
   Count: 11

Name: 1.3.6.1.4.1.111.15.1.1.1.2.1
   Kind: OctetString
   Value: "mydatabase"

Name: 1.3.6.1.4.1.111.15.1.1.1.3.1
   Kind: OctetString
   Value: "Database"

Name: 1.3.6.1.4.1.111.15.1.1.1.4.1
  Kind: OctetString
  Value: "myhost.com"

Name: 1.3.6.1.4.1.111.15.1.1.1.5.1
   Kind: OctetString
   Value: "Owner's Invalid Object Count"

Name: 1.3.6.1.4.1.111.15.1.1.1.6.1
   Kind: OctetString
   Value: "Invalid Object Owner"

Name: 1.3.6.1.4.1.111.15.1.1.1.7.1
   Kind: OctetString
   Value: "SYS"

Name: 1.3.6.1.4.1.111.15.1.1.1.8.1
   Kind: OctetString
   Value: "28-OCT-2003 04:59:10 (US/Eastern GMT)"
```

```
Name: 1.3.6.1.4.1.111.15.1.1.1.9.1
   Kind: OctetString
   Value: "Warning"

Name: 1.3.6.1.4.1.111.15.1.1.1.10.1
   Kind: OctetString
   Value: "12 object(s) are invalid in the SYS schema."

Name: 1.3.6.1.4.1.111.15.1.1.1.11.1
   Kind: OctetString
   Value: "Database Metrics"

Name: 1.3.6.1.4.1.111.15.1.1.1.12.1
   Kind: OctetString
   Value: "SYSMAN"
```

11.2.3 Passing Metric Severity Information

Passing metric severity attributes (severity level, type, notification rule, rule owner, or rule owner, and so on) to PL/SQL procedures or OS commands/scripts allows you to customize automated responses to alerts. For example, if an OS script opens a trouble ticket for an in-house support trouble ticket system, you will want to pass severity levels (critical, warning, and so on) to the script to open a trouble ticket with the appropriate details and escalate the problem.

11.2.3.1 Passing Information to an OS Script or Executable

The notification system passes severity information to an OS script or executable using system environment variables. Conventions used to access environmental variables vary depending on the operating system:

- UNIX: $ENV_VARIABLE
- Windows:%ENV_VARIABLE%

The notification system sets the following environment variables before calling the script. The script can then use any or all of these variables within the logic of the script.

Table 11–1 Environment Variables

Environment Variable	Description
TARGET_NAME	Name of the target on which the severity occurred.
TARGET_TYPE	Type of target on which the severity occurred. Targets are defined as any monitorable service.
HOST	Name of the machine on which the target resides.
METRIC	Metric generating the severity.
KEY_VALUE	For metrics that monitor a set of objects, the KEY_VALUE indicates the specific object that triggered the severity. For example for the Tablespace Space Used (%) metric that monitors tablespace objects, the KEY_VALUE is 'USERS' if the USERS tablespace triggered at warning or critical severity.
KEY_VALUE_NAME	For metrics that monitor a set of objects, the KEY_VALUE_NAME indicates the type of object monitored. For example for the Tablespace Space Used (%) metric that monitors tablespace objects, the KEY_VALUE_NAME is 'Tablespace Name'.
TIMESTAMP	Time when the severity occurred.

Table 11–1 (Cont.) Environment Variables

Environment Variable	Description
SEVERITY	Type of severity. For example, severity types that relate to a target's availability are: ■ UP ■ DOWN ■ UNREACHABLE CLEAR ■ UNREACHABLE START ■ BLACKOUT END ■ BLACKOUT START Other metrics can have any of the following severities: ■ WARNING ■ CRITICAL ■ CLEAR ■ METRIC ERROR CLEAR ■ METRIC ERROR START
MESSAGE	Message for the alert that provides details about what triggered the condition.
RULE_NAME	Name of the notification rule that resulted in the severity.
RULE_OWNER	Name of the Enterprise Manager administrator who owns the rule.

Your script may reference some or all of these variables.

Example 11–8 shows an OS command script appending environment variable entries to a log file.

Example 11–8 logs a severity occurrence to a file server. If the file server is unreachable then an exit code of 100 is returned to force the Oracle Management Service Notification System to retry the notification

Example 11–8 Sample OS Command Script

```
#!/bin/ksh

LOG_FILE=/net/myhost/logs/severity.log
if test -f $LOG_FILE
then
echo $TARGET_NAME $MESSAGE $TIMESTAMP >> $LOG_FILE
else
   exit 100
fi
```

Example 11–9 shows an OS script that logs alert information to the file 'alertmsg.txt'. The file is saved to the /u1/results directory.

Example 11–9 Alert Logging Script

```
#!/usr/bin/sh
echo "Alert logged:" > /u1/results/alertmsg.txt
echo "\n" >> /u1/results/alertmsg.txt
echo "target name is " $TARGET_NAME >> /u1/results/alertmsg.txt
echo "target type is " $TARGET_TYPE >> /u1/results/alertmsg.txt
```

```
echo "target is on host " $HOST >> /u1/results/alertmsg.txt
echo "metric in alert is " $METRIC >> /u1/results/alertmsg.txt
echo "metric index is " $KEY_VALUE >> /u1/results/alertmsg.txt
echo "timestamp is " $TIMESTAMP >> /u1/results/alertmsg.txt
echo "severity is " $SEVERITY >> /u1/results/alertmsg.txt
echo "message is " $MESSAGE >> /u1/results/alertmsg.txt
echo "notification rule is " $RULE_NAME >> /u1/results/alertmsg.txt
echo "rule owner is " $RULE_OWNER >> /u1/results/alertmsg.txt
exit 0
```

Example 11–10 shows a script that sends an alert to an HP OpenView console from Enterprise Manager Grid Control. When a metric alert is triggered, the Enterprise Manager Grid Control displays the alert. The HP OpenView script is then called, invoking opcmsg and forwarding the information to the HP OpenView management server.

Example 11–10 HP OpenView Script

```
/opt/OV/bin/OpC/opcmsg severity="$SEVERITY" app=OEM msg_grp=Oracle msg_
text="$MESSAGE" object="$TARGET"
```

11.2.3.2 Passing Information to a PL/SQL Procedure

The notification system passes severity information to a PL/SQL procedure using the MGMT_NOTIFY_SEVERITY object. An instance of this object is created for every alert. When an alert occurs, the notification system calls the PL/SQL procedure associated with the notification rule and passes the populated object to the procedure. The procedure is then able to access the fields of the MGMT_NOTIFY_SEVERITY object that has been passed to it.

Table 11–2 lists all metric severity attributes that can be passed:

Table 11–2 Metric Severity Attributes

Attribute	Datatype	Additional Information
target_name	VARCHAR2(64)	Name of the target on which the severity occurred.
target_type	VARCHAR2(64)	Type of target on which the severity occurred. Targets are defined as any monitorable service.
timezone	VARCHAR2(64)	The target's regional timezone
host_name	VARCHAR2(128)	Name of the machine on which the target resides.
metric_name	VARCHAR2(64)	Metric generating the severity.
metric_description	VARCHAR2(128)	Meaningful description of the metric that can be understood by other administrators.
metric_column	VARCHAR2(64)	For table metrics, the metric column contains the name of the column in the table that is being defined. If the metric that is being defined is not a table metric, the value in this column is a single space.

Table 11–2 (Cont.) Metric Severity Attributes

Attribute	Datatype	Additional Information
key_value	VARCHAR2(256)	For metrics that monitor a set of objects, the KEY_VALUE indicates the specific object that triggered the severity. For example for the Tablespace Space Used (%) metric that monitors tablespace objects, the KEY_VALUE is 'USERS' if the USERS tablespace triggered at warning or critical severity.
key_value_name	VARCHAR2(512)	For metrics that monitor a set of objects, the KEY_VALUE_NAME indicates the type of object monitored. For example for the Tablespace Space Used (%) metric that monitors tablespace objects, the KEY_VALUE_NAME is 'Tablespace Name'.
key_value_guid	VARCHAR2(256)	GUID associated with a composite key value name.
collection_timestamp	DATE	The time when the target status change was last detected and logged in the management repository.
severity_code	NUMBER	Numeric code identifying the severity level. See Severity Code table below.
message	VARCHAR2(4000)	An optional message that is generated when the alert is created that provides additional information about the alert condition.
severity_guid	RAW(16)	Severity global unique identifier.
metric_guid	RAW(16)	Metric global unique identifier.
target_guid	RAW(16)	Target global unique identifier.
rule_owner	VARCHAR2(64)	Name of the Enterprise Manager administrator who owns the rule.
rule_name	VARCHAR2(132)	Name of the notification rule that resulted in the severity.

When a severity occurs for the target, the notification system creates an instance of the MGMT_NOTIFY_SEVERITY object and populates it with values from the severity. The severity codes in Table 11–3 have been defined as constants in the MGMT_GLOBAL package and can be used to determine the type of severity in the severity_code field of the MGMT_NOTIFY_SEVERITY object. See Example 11–11.

Table 11–3 Severity Codes

Name	Datatype	Value
G_SEVERITY_COMMENT	NUMBER(2)	10
G_SEVERITY_CLEAR	NUMBER(2)	15
G_SEVERITY_WARNING	NUMBER(2)	20
G_SEVERITY_CRITICAL	NUMBER(2)	25
G_SEVERITY_UNREACHABLE_CLEAR	NUMBER(3)	115
G_SEVERITY_UNREACHABLE_START	NUMBER(3)	125
G_SEVERITY_BLACKOUT_END	NUMBER(3)	215
G_SEVERITY_BLACKOUT_START	NUMBER(3)	225

Table 11–3 (Cont.) Severity Codes

Name	Datatype	Value
G_SEVERITY_ERROR_END	NUMBER(3)	315
G_SEVERITY_ERROR_START	NUMBER(3)	325
G_SEVERITY_NO_BEACONS	NUMBER(3)	425
G_SEVERITY_UNKNOWN	NUMBER(3)	515

Example 11–11 PL/SQL Procedure Using a Severity Code

```
CREATE TABLE alert_log (target_name VARCHAR2(64),
alert_msg VARCHAR2(4000),
occured DATE);

PROCEDURE LOG_CRITICAL_ALERTS(severity IN MGMT_NOTIFY_SEVERITY)
IS
BEGIN
-- Log all critical severities
   IF severity.severity_code = MGMT_GLOBAL.G_SEVERITY_CRITICAL
   THEN
   BEGIN
   INSERT INTO alert_log (target_name, alert_msg, occured)
   VALUES (severity.target_name, severity.message,
   severity.collection_timestamp);
   EXCEPTION
   WHEN OTHERS
   THEN
   -- If there are any problems then get the notification retried
   RAISE_APPLICATION_ERROR(-20000, 'Please retry');
  END;
  COMMIT;
   END IF;
END LOG_CRITICAL_ALERTS;
```

11.3 Notification Rules

Notification rules allow you to choose the targets and conditions for which you want to receive notifications from Enterprise Manager. The methods for sending notifications include e-mail, SNMP traps, or running custom scripts, or all three.

After you set up your notification methods, you can define the rules that Enterprise Manager will use when sending notifications. When you define the notification rules, you can choose to make them 'public' to share them with other administrators, or to keep them 'private' for your own use. When logged into the Enterprise Manager Grid Control, you can see both types of rules:

1. Click the **Preferences** global link.
2. In the Notification section of vertical navigational bar, you can click **My Rules** to access all the rules that you have defined.
3. In the same navigational bar, you can click **Public Rules** to access all rules defined by other administrators that have been made public.

An Administrator with superuser privileges can see all rules (private and public).

11.4 Default Notification Rules

When you installed the Oracle Management Service, you would have been given an option to receive e-mail notifications for critical alerts. If you chose this option, then some default notification rules would have been created that covered the availability and critical states for the more common target types. If an e-mail address for the SYSMAN user was specified, then these rules would also be configured to send e-mail for these conditions.

Table 11–4 lists all the default notification rules. These are all owned by the SYSMAN user and are public rules.

Table 11–4 Default Notification Rules

Name	Description	Target Type	Send Notification on the Following Availability States	Send Notification on the Following Metrics and their CRITICAL and WARNING States
Application Server Availability and Critical/Warning States	System-generated notification rule for monitoring Application Servers' availability, and critical and warning metric statuses.	Application Servers	Down Unreachable Start Unreachable End	Metric Label: CPU Usage (%) Metric Name: ResourceUsage Metric Column: Cpu.component Metric Label: Response Time (seconds) Metric Name: Response Metric Column: Timing.sec
OC4J Availability and Critical/Warning States	System-generated notification rule for monitoring OC4J instance's availability, and critical and warning metric statuses.	OC4J	Down Unreachable Start Unreachable End	Metric Label: CPU Usage (%) Metric Name: ResourceUsage Metric Column: Cpu.components Metric Label: Request Processing Time for the OC4J Instance (seconds) Metric Name: oc4j_instance_ rollup Metric Column: processRequest.time Metric Label: Active Sessions for the OC4J Instance Metric Name: oc4j_instance_ rollup Metric Column: session.active

Table 11–4 (Cont.) Default Notification Rules

Name	Description	Target Type	Send Notification on the Following Availability States	Send Notification on the Following Metrics and their CRITICAL and WARNING States
HTTP Server Availability and Critical/Warning States	System-generated notification rule for monitoring HTTP Server's availability, and critical and warning metric statuses.	Oracle HTTP Server	Down Unreachable Start Unreachable End	Metric Label: CPU Usage (%) Metric Name: ResourceUsage Metric Column: cpu.component Metric Label: Request Processing Time (seconds) Metric Name: ohs_server Metric Column: request.currentProcessingTime Metric Label: Active HTTP Connections Metric Name: ohs_server Metric Column: connection.active Metric Label: Percentage of Busy Processes Metric Name: ohs_server Metric Column: busyProcesses.currentPercentage
Web Cache Availability and Critical/Warning States	System-generated notification rule for monitoring Web Cache's instance's availability, and critical and warning metric statuses.	Oracle Web Cache	Down Unreachable Start Unreachable End	Metric Label: CPU Usage (%) Metric Name: ResourceUsage Metric Column: cpu.component Metric Label: Hits (% if requests) Metric Name: HIST Metric Column: HIST__ COMPUTED__HIT_RATE

Table 11–4 (Cont.) Default Notification Rules

Name	Description	Target Type	Send Notification on the Following Availability States	Send Notification on the Following Metrics and their CRITICAL and WARNING States
Database Availability and Critical/Warning States	System-generated notification rule for monitoring Databases' availability, and critical and warning metric statuses.	Databases (single instance only)	Down Unreachable Start Unreachable End	Metric Name: Alert Log Metric Column: Archiver Hung Metric Name: Alert Log Metric Column: Data Block Corruption Metric Name: User Block Metric Column: Blocking Session Count Metric Name: User Wait Time Metric Column: User Wait Time (%) Metric Name: Database Limits Metric Column: Datafile Usage (%) Metric Name: Database Limits Metric Column: Lock Limit Usage (%) Metric Name: Database Limits Metric Column: Process Limit Usage (%) Metric Name: Database Limits Metric Name: Archive Area Metric Column: Used (%) Metric Column: Session Limit Usage (%) Metric Name: Problem Tablespace Metric Column: Tablespace Space Used (%) Metric Name: Problem Tablespace Metric Column: Segments Unable to Extend Count Metric Name: Problem Tablespace Metric Column: Segments Approaching MaxExtents
Listener Availability	System-generated notification rule for monitoring database Listeners' availability, and critical and warning metric statuses.	Listeners	Down Unreachable Start Unreachable End	N/A

Table 11–4 (Cont.) Default Notification Rules

Name	Description	Target Type	Send Notification on the Following Availability States	Send Notification on the Following Metrics and their CRITICAL and WARNING States
Host Availability and Critical/Warning States	System-generated notification rule for monitoring Hosts' availability, and critical and warning metric statuses.	Hosts	Down Unreachable Start Unreachable End	Metric Label: Average Disk I/O Service Time (ms) Metric Name: DiskActivity Metric Column: DiskActivityavserv Metric Label: Average I/O Wait Time (ms) Metric Name: DiskActivity Metric Column: DiskActivityavwait Metric Label: CPU in IO-Wait (%) Metric Name: Load Metric Column: cpuIOWait Metric Label: Disk Utilization (%) Metric Name: DiskActivity Metric Column: DiskActivitybusy Metric Label: Run Queue Length (5 minute average) Metric Name: Load Metric Column: cpuLoad Metric Column: swapUtil Metric Column: PctAvailable Metric Label: File System Space Available (%) Metric Name: Filesystems Metric Label: Memory Page Scan Rate (per second) Metric Name: Load Metric Column: pgScanRate Metric Label: CPU Utilization (%) Metric Name: Load Metric Column: cpuUtil Metric Label: Memory Utilization (%) Metric Name: Load Metric Column: MemUsedPct Metric Label: Network Interface Combined Utilization (%) Metric Name: Network Metric Label: Swap Utilization (%) Metric Name: Load Metric Column: totalThroughput

Table 11–4 (Cont.) Default Notification Rules

Name	Description	Target Type	Send Notification on the Following Availability States	Send Notification on the Following Metrics and their CRITICAL and WARNING States
Repository Operations Availability	System-generated notification rule for monitoring the availability of the DBMS jobs that are part of the Management Repository.	Oracle Management Service and Repository	Critical	Metric Name: DBMS_Job_Status Metric Column: jobUpDown
Agent Upload Problems	System-generated notification rule for monitoring Agents that may have problems uploading data to the Management Service.	Oracle Management Service and Repository	Critical	Metric Name: Targets_not_uploading Metric Column: targetCount
Agents Unreachable	System-generated notification rule for monitoring Agents that lose contact with the Management Service due to network problems, host problems or Agents going down.	Agents	Unreachable Start Unreachable End	N/A

11.5 Creating Your Own Notification Rules

To create your own notification rule:

1. From the Enterprise Manager Grid Control, click **Preferences**.
2. Click **My Rules** in the vertical navigation bar.

   If you are not logged in as an administrator with superuser privileges, you will see a link for **My Rules** instead of Notification Rules as in the case of an administrator with superuser privileges.
3. Click **Create**.

   Enterprise Manager displays the Create Notification Rule wizard. Follow the instructions in the wizard to create your notification rule.

   When you specify the notification rule properties, check **Make Public** in the Properties page of the wizard if you want other non-privileged users to be able to view and share that rule. For example, it allows other administrators to later specify that they should receive e-mail for this rule.

   When you specify the notification rule, you will only be able to choose from e-mail and SNMP traps. Specifying custom commands and PL/SQL procedures is an option which is only available to privileged users.

11.6 Getting Email Notifications

If you want to receive notifications by email, you will need to specify your e-mail address in the Preferences General page. In addition to defining notification e-mail

addresses, you associate the notification message format (long or short) to be used for each e-mail address.

Each e-mail address can have up to 132 characters; there is no upper bound with the number of e-mail addresses.

To add an e-mail address:

1. From the Grid Control Console, click **Preferences** at the top of the page. By default the General page is selected.
2. Click **Add Another Row** to create a new e-mail entry field in the **E-mail Addresses** table.
3. Specify the e-mail associated with your Enterprise Manager account. All e-mail notifications you receive from Enterprise Manager will be sent to the e-mail addresses you specify.

   For example, `user1@oracle.com`

   Select the message format for your e-mail address. The Long Format sends a HTML formatted e-mail that contains detailed information about an alert. Example 11–12 shows a typical notification that uses the long format.

   The Short Format (Example 11–13) sends a concise text e-mail that is limited to 155 characters thereby allowing the e-mail be received as an SMS message or page. The subject contains the severity type (for example, Critical) and the target name. The body contains the time the severity occurred and the severity message. Since the message length is limited to 155 character, some of this information may be truncated. If truncation has occurred there will be a series of dots at the end of the message.
4. Click Apply to save your e-mail address.

Example 11–12 Long E-mail Notification

```
Name=myhost.com
Type=Host
Host=myhost.com
Metric=Filesystem Space Available (%)
Mount Point =/usr
Timestamp=06-OCT-2003 16:27:05 US/Pacific
Severity=Warning
Message=Filesystem / has only 76.07% available space
Rule Name=Host Availability and Critical States
Rule Owner=SYSMAN
```

Example 11–13 Short E-mail notification

```
Subject is :
EM:Unreachable Start:myhost
Body is :
Nov 16, 2003 2:02:19 PM EST:Agent is Unreachable (REASON = Connection refused)
but the host is UP
```

11.6.1 Notification Schedules

Once you have defined your e-mail notification addresses, you will need to define a notification schedule. For example, if your e-mail addresses are user1@oracle.com, user2@oracle.com, user3@oracle.com, you can choose to use one or more of these e-mail addresses for each time period in your notification schedule.

A notification schedule is a rotating schedule used by Enterprise Manager to determine how to send e-mail notifications to administrators. Each administrator has exactly one notification schedule. When an alert needs to be e-mailed to an administrator, Enterprise Manager consults that administrator's notification schedule to determine the e-mail address to be used.

To define a notification schedule:

1. From the Enterprise Manager Grid Control, click **Preferences** at the top of the page. By default the General page is selected.
2. Click **Notification Schedule** in the vertical navigation bar.

   The Enterprise Manager Grid Control displays the Notification Schedule page.
3. Follow the directions on the Notification Schedule page to specify what times you should be notified by e-mail.

11.6.2 Using Out-of-Box Notification Rules

Enterprise Manager creates a comprehensive set of predefined notification rules for the most common target types. These default rules are adequate for most notification needs situations. See "Default Notification Rules" on page 11-13 for more information. If these rules meet your needs, you can choose to receive e-mail for them by selecting the rule from the Preferences Rules or Public Rules page, then click the **Assign Methods** button.

11.6.3 Creating Your Own Notification Rules

If you find that the default notification rules do not meet your needs, you can define your own custom rules. See "Notification Rules" on page 11-12.

The e-mail format is HTML. The target Name is a link to the target in the Grid Control. The metric name is a link to the metric in the Grid Control.

11.7 Configuring Methods for Rules

After you set up your notification method or methods and created rules, you can associate the rules with multiple notification methods.

1. From the Enterprise Manager Grid Control, click **Preferences** at the top of the page.
2. Click **Notification Rules** in the vertical navigation bar.

   The Enterprise Manager Grid Control displays the Notification Rules page. Any notification rules already created are listed in the **Notification Rules** table.
3. Select the radio button next to the rule for which you want to configure a method.
4. Click **Configure Methods**.
5. Specify the notification methods that should occur when metric severities are met.

   Choose the **Send Me E-mail** option and specify one or more e-mail addresses to which notifications will be sent; then choose a notification method from the list of notification methods.

Once you have defined your notification methods and have decided which notification rules to use (predefined or custom), you need to define the association between various methods and rules. If you have a large number of rules, methods, or both, Enterprise Manager provides an easy way to perform method-rule mapping.

"Assigning Methods to Rules" on page 11-20 and "Assigning Rules to Methods" on page 11-20 illustrate how to perform this mapping quickly and easily.

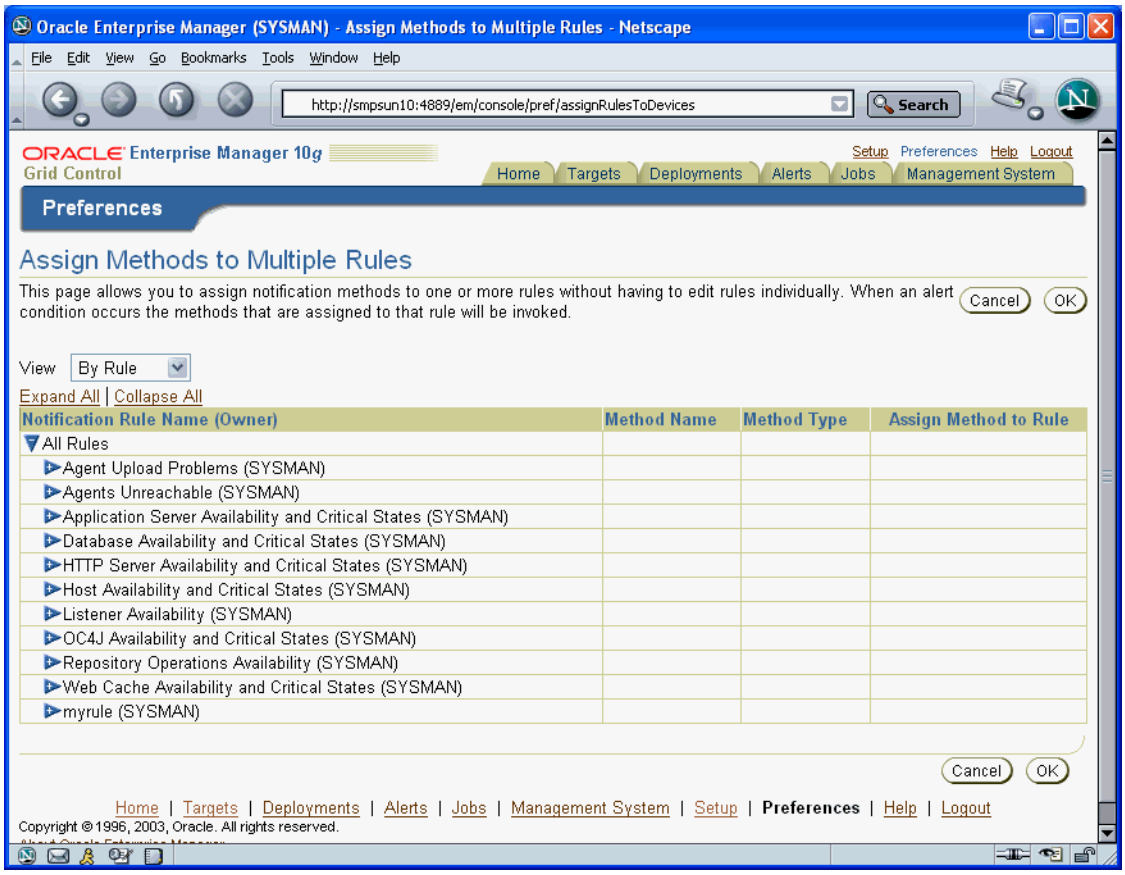
11.8 Assigning Methods to Rules

For each notification rule, you can assign one or more notification methods to be called as a result of alert occurrences.

1. From the Enterprise Manager Grid Control, click **Preferences** at the top of the page.
2. Click **Notification Rules** in the vertical navigation bar.

   The Enterprise Manager Grid Control displays the Notification Rules page. Any notification rules already created are listed in the **Notification Rules** table.
3. Click **Assign Methods to Multiple Rules**.
4. Perform your assignments.

Figure 11–2 Assigning Methods to Rules



11.9 Assigning Rules to Methods

For each notification method, you can associate one or more notification rules that will use that method to send notifications.

1. From the Enterprise Manager Grid Control, click **Preferences** at the top of the page.

2. Click **Notification Rules** in the vertical navigation bar.

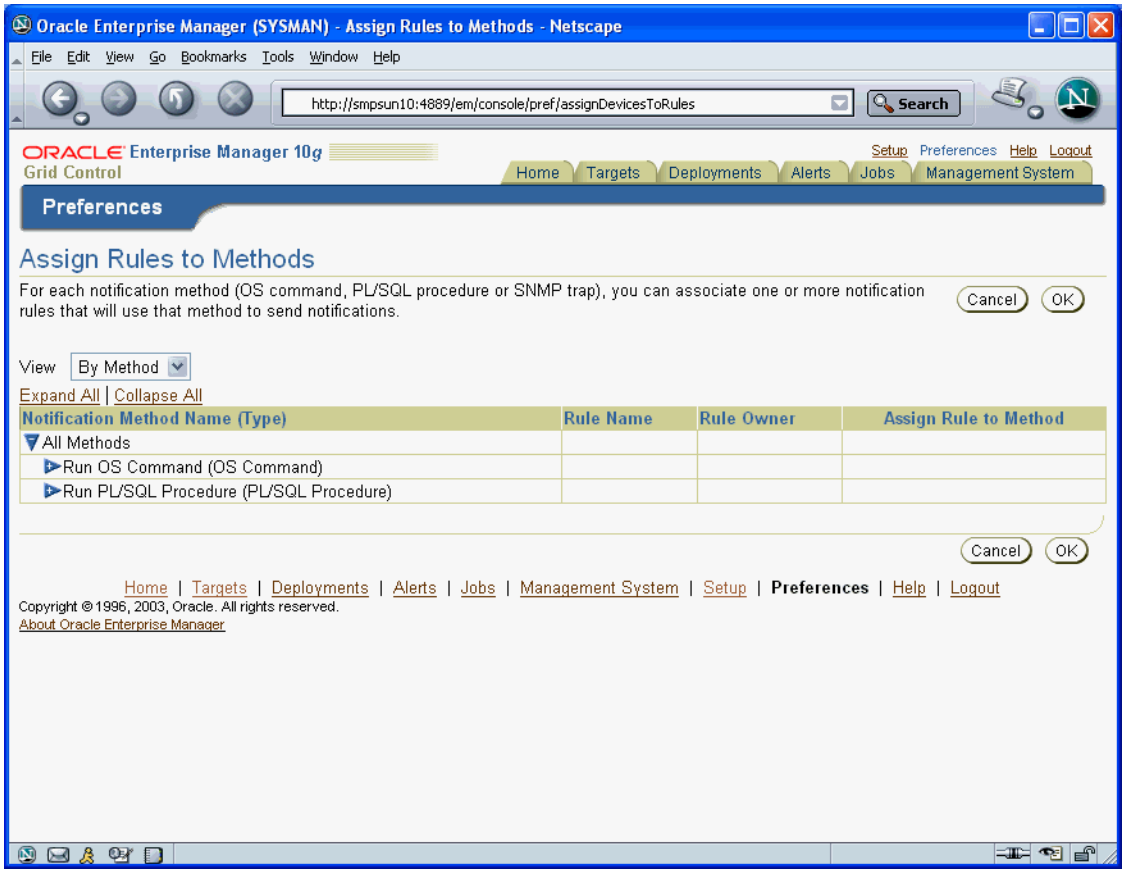
   The Enterprise Manager Grid Control displays the Notification Rules page. Any notification rules already created are listed in the **Notification Rules** table.

3. Click **Assign Methods to Multiple Rules**.

4. From the **View** menu, select **By Method**.

5. Perform your assignments.

Figure 11–3 Assign Rules to Methods



11.10 Management Information Base (MIB)

While SNMP allows Enterprise Manager to send information to third-party SNMP-enabled applications, there may be situations where you want SNMP-enabled applications to obtain information from Enterprise Manager. This is accomplished using management information base (MIB) variables. The following sections discuss Enterprise Manager MIB variables in detail.

11.10.1 About MIBs

A MIB is a text file, written in ASN.1 notation, which describes the variables containing the information that SNMP can access. The variables described in a MIB, which are also called MIB objects, are the items that can be monitored using SNMP. There is one MIB for each element being monitored. Each monolithic or subagent consults its respective MIB in order to learn the variables it can retrieve and their characteristics. The encapsulation of this information in the MIB is what enables

master agents to register new subagents dynamically — everything the master agent needs to know about the subagent is contained in its MIB. The management framework and management applications also consult these MIBs for the same purpose. MIBs can be either standard (also called public) or proprietary (also called private or vendor).

The actual values of the variables are not part of the MIB, but are retrieved through a platform-dependent process called "instrumentation". The concept of the MIB is very important because all SNMP communications refer to one or more MIB objects. What is transmitted to the framework is, essentially, MIB variables and their current values.

11.10.2 Reading the MIB Variable Descriptions

This section covers the format used to describe MIB variables. Note that the STATUS element of SNMP MIB definition, Version 2, is not included in these MIB variable descriptions. Since Oracle has implemented all MIB variables as CURRENT, this value does not vary.

11.10.2.1 Variable Name

Syntax
Maps to the SYNTAX element of SNMP MIB definition, Version 2.

Max-Access
Maps to the MAX-ACCESS element of SNMP MIB definition, Version 2.

Status
Maps to the STATUS element of SNMP MIB definition, Version 2.

Explanation
Describes the function, use and precise derivation of the variable. (For example, a variable might be derived from a particular configuration file parameter or performance table field.) When appropriate, incorporates the DESCRIPTION part of the MIB definition, Version 2.

Typical Range
Describes the typical, rather than theoretical, range of the variable. For example, while integer values for many MIB variables can theoretically range up to 4294967295, a typical range in an actual installation will vary to a lesser extent. On the other hand, some variable values for a large database can actually exceed this "theoretical" limit (a "wraparound"). Specifying that a variable value typically ranges from 0 to 1,000 or 1,000 to 3 billion will help the third-party developer to develop the most useful graphical display for the variable.

Significance
Describes the significance of the variable when monitoring a typical installation. Alternative ratings are Very Important, Important, Less Important, or Not Normally Used. Clearly, the DBA will want to monitor some variables more closely than others. However, which variables fall into this category can vary from installation to installation, depending on the application, the size of the database, and on the DBA's objectives. Nevertheless, assessing a variable's significance relative to the other variables in the MIB can help third-party developers focus their efforts on those variables of most interest to the most DBAs.

Related Variables
Lists other variables in this MIB, or other MIBs implemented by Oracle, that relate in some way to this variable. For example, the value of this variable might derive from

that of another MIB variable. Or perhaps the value of this variable varies inversely to that of another variable. Knowing this information, third-party developers can develop useful graphic displays of related MIB variables.

Suggested Presentation
Suggests how this variable can be presented most usefully to the DBA using the management application: as a simple value, as a gauge, or as an alarm, for example.

11.10.2.2 MIB Definition

Example 11–14 shows a typical MIB definition used by Enterprise Manager.

Example 11–14 MIB Definition

```
ORACLE-ENTERPRISE-MANAGER-4-MIB DEFINITIONS ::= BEGIN

IMPORTS
TRAP-TYPE
FROM RFC-1215
DisplayString
FROM RFC1213-MIB
OBJECT-TYPE
FROM RFC-1212
enterprises
FROM RFC1155-SMI;

oracle OBJECT IDENTIFIER ::= { enterprises  111 }

oraEM4 OBJECT IDENTIFIER ::= { oracle  15 }

oraEM4Objects OBJECT IDENTIFIER ::= { oraEM4  1 }

oraEM4AlertTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF OraEM4AlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information on alerts generated by Oracle Enterprise Manager. This table
is not queryable; it exists only to document the variables included in the
oraEM4Alert trap.  Each trap contains a single instance of each variable in the
table."
    ::= { oraEM4Objects  1 }

oraEM4AlertEntry OBJECT-TYPE
    SYNTAX  OraEM4AlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information about a particular Oracle Enterprise Manager alert."
    INDEX   { oraEM4AlertIndex }
    ::= { oraEM4AlertTable  1 }

OraEM4AlertEntry ::=
    SEQUENCE {
        oraEM4AlertIndex
            INTEGER,

        oraEM4AlertTargetName
   DisplayString,
```

```
        oraEM4AlertTargetType
   DisplayString,

        oraEM4AlertHostName
   DisplayString,

        oraEM4AlertMetricName
   DisplayString,

        oraEM4AlertKeyName
   DisplayString,

        oraEM4AlertKeyValue
   DisplayString,

        oraEM4AlertTimeStamp
   DisplayString,

        oraEM4AlertSeverity
   DisplayString,

        oraEM4AlertMessage
   DisplayString,

        oraEM4AlertRuleName
   DisplayString

        oraEM4AlertRuleOwner
   DisplayString
    }

oraEM4AlertIndex OBJECT-TYPE
    SYNTAX  INTEGER
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Index of a particular alert, unique only at the moment an alert is
generated."
    ::= { oraEM4AlertEntry  1 }

oraEM4AlertTargetName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the target to which this alert applies."
    ::= { oraEM4AlertEntry  2 }

oraEM4AlertTargetType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The type of the target to which this alert applies."
    ::= { oraEM4AlertEntry  3 }

oraEM4AlertHostName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
```

```
    DESCRIPTION
     "The name of the host on which this alert originated."
    ::= { oraEM4AlertEntry  4 }

oraEM4AlertMetricName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the metric which generated this alert."
    ::= { oraEM4AlertEntry  5 }

oraEM4AlertKeyName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the key-column, if present, for the metric which generated this
alert."
    ::= { oraEM4AlertEntry  6 }

oraEM4AlertKeyValue OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The value of the key-column, if present, for the metric which generated this
alert."
    ::= { oraEM4AlertEntry  7 }

oraEM4AlertTimeStamp OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The time at which this alert was generated."
    ::= { oraEM4AlertEntry  8 }

oraEM4AlertSeverity OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The severity of the alert e.g. Critical."
    ::= { oraEM4AlertEntry  9 }

oraEM4AlertMessage OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The message associated with the alert."
    ::= { oraEM4AlertEntry  10 }

oraEM4AlertRuleName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the notification rule that caused this notification."
```

```
    ::= { oraEM4AlertEntry  11 }

oraEM4AlertRuleOwner OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The owner of the notification rule that caused this notification."
    ::= { oraEM4AlertEntry  12 }

oraEM4Traps OBJECT IDENTIFIER ::= { oraEM4  2 }

oraEM4Alert TRAP-TYPE
    ENTERPRISE  oraEM4Traps
    VARIABLES   { oraEM4AlertTargetName, oraEM4AlertTargetType,
                  oraEM4AlertHostName, oraEM4AlertMetricName,
                  oraEM4AlertKeyName, oraEM4AlertKeyValue, oraEM4AlertTimeStamp,
                  oraEM4AlertSeverity, oraEM4AlertMessage,
                  oraEM4AlertRuleName, oraEM4AlertRuleOwner }
    DESCRIPTION
     "The variables included in the oraEM4Alert trap."
    ::= 1


END
```

12

Additional Configuration Tasks

This chapter contains the following sections:

12.1 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:

12.1.1 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.

12.1.2 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.

12.2 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 Concepts Guide*

When you use Enterprise Manager to monitor your Oracle software installations, Enterprise Manager takes advantage of information saved in the Universal Installer inventory.

As it gathers information about the configuration of your host computer, by default, Enterprise Manager assumes that you have one Oracle Universal Installer inventory on the host. Specifically, Enterprise Manager recognizes the inventory that Oracle Universal Installer uses when you run the Universal Installer on the host.

However, in some cases, you may have more than one inventory. For example, you may have worked with Oracle Support to clone your Oracle software installations. For those cases, you can use the following procedure to be sure that Enterprise Manager can track and manage the software information in multiple inventories on the same host.

> **Caution:** Enabling support for multiple inventories is optional and available only for advanced users who are familiar with the Oracle Universal Installer inventory architecture and who have previously worked with multiple inventories on a managed host. This procedure is not required for hosts where normal installations have been performed.

To set up Enterprise Manager so it can read multiple inventories on a host:

1. Locate the `OUIinventories.add` file in the following directory:

   ```
   AGENT_HOME/sysman/config/
   ```

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, but Enterprise Manager does collect the configuration information for the other inventories.

12.3 Manually Configuring a Database Target for Complete Monitoring

When you first discover an Oracle Database 10*g* 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.

> **See Also:** "Specifying New Target Monitoring Credentials" on page 2-13

Besides setting the monitoring credentials, no other configuration tasks are required in order to monitor an Oracle Database 10*g* target.

However, when you monitor an Oracle9i 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 Oracle9i 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 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;
   ```

7. Connect as SYS 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 agent by entering the following command:

```
$PROMPT> ./emctl agent reload
```

15. Using Grid Control, return to the Database home page and verify that the Bad SQL and Top SQL Report metrics are now being gathered.

12.4 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.

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W