



# **Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)**

**August 2010**

**Security Evaluations  
Oracle Corporation  
500 Oracle Parkway  
Redwood Shores, CA 94065**

**Evaluated Configuration for Oracle Enterprise Manager 10g Grid Control  
Release 5 (10.2.0.5)  
Issue 2.1**

**August 2010**

**Author: Trang Huynh**

**Contributors: Petra Manche, Jeremy Powell**

*The contributions of the many authors of the precursors to this document are acknowledged.*

Copyright © 2009, Oracle Corporation. All rights reserved. This documentation contains proprietary information of Oracle Corporation; it is protected by copyright law. Reverse engineering of the software is prohibited. If this documentation is delivered to a U.S. Government Agency of the Department of Defense, then it is delivered with Restricted Rights and the following legend is applicable:

**RESTRICTED RIGHTS LEGEND**

Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of DFARS 252.227-7013, Rights in Technical Data and Computer Software (October 1988).

Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065.

The information in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. Oracle Corporation does not warrant that this document is error free.

Oracle is a registered trademark and Oracle Enterprise Manger, PL/SQL are trademarks or registered trademarks of Oracle Corporation. Other names may be trademarks of their respective owners.

# Contents

1	Introduction.....	5
1.1	Intended Audience.....	6
1.2	Organization.....	6
1.3	Format.....	7
1.4	Delivery of the TOE.....	7
1.5	Electronic Delivery of the TOE.....	7
1.6	Electronic Delivery of the Oracle Database 11g Release 1 (11.1.0.7).....	9
1.7	Verification of TOE version.....	10
2	Overview of Security Functionality.....	12
2.1	Identification and Authentication.....	12
2.2	Privileged-based Access Control.....	12
2.3	Auditing.....	14
2.4	Data Transfer Protection.....	14
2.5	Compliance Management.....	14
2.6	Security Function Management.....	15
3	Evaluated Configuration Requirements.....	16
3.1.1	Operating System.....	16
3.1.2	Java Virtual Machine.....	16
3.1.3	Database Repository.....	17
3.1.4	Application Server.....	17
4	Host Configuration.....	20
4.1	Operating Systems.....	20
4.1.1	Oracle Enterprise Linux Version 4 (Update 5) and Red Hat Enterprise Linux AS (Release 5).....	20
4.1.2	SuSE Linux Enterprise Server 10 SP1.....	20
5	Oracle Enterprise Manager Configuration.....	21
5.1	Oracle Enterprise Manager 10g Grid Control.....	22
5.1.1	Oracle Management Service (OMS).....	22
5.1.2	Oracle Management Repository.....	22
5.1.3	Oracle Management Agent.....	22
5.1.4	Enterprise Manager Command Line Interface (EMCLI).....	23
5.1.5	Configuring the Evaluated Configuration.....	25
5.1.5.1	Configuring Identification and Authentication.....	25
5.1.5.2	Configuring Compliance Management.....	25
5.1.5.3	Configuring Audit Logging.....	25

5.1.5.4	Configuring Privileged-based Access Control.....	26
5.1.5.5	Configuring Secure Communication between OMS and Agent.....	26
5.1.5.6	Configuring Secure Communication between OMS and Repository.....	30
5.1.5.7	Configuring HTTPS for Web GUI.....	31
5.1.5.8	Configuring FIPS 140-2 Mode.....	31
5.1.5.9	Disabling the WSDL Web Services Interface.....	32
<i>A</i>	TOE Components.....	35
A.1	OMS Components.....	35
A.1	Agent Components.....	46
<i>B</i>	Errata.....	51
B.1	Privileges.....	51
B.2	Return Codes.....	53
B.3	Password guidelines/suggestions.....	56
<i>C</i>	References.....	57

# 1 Introduction

The Target of Evaluation (TOE) is the Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) (Grid Control).

The TOE is hosted on the following platforms, which is required by the TOE for support:

- For the targets (Oracle Management Agents):
  - Oracle Enterprise Linux Edition Version 4 (Update 5)
  - Red Hat Enterprise Linux AS (Release 5)
  - SuSE Linux Enterprise Server 10 SP 1
  - Java Runtime Environment 1.4.2
- For the OMS (Oracle Management Service)
  - Oracle Application Server 10.1.2.3
- For the repository (Oracle Management Repository)
  - Oracle Database 11g (11.1.0.7)
- For the Command Line Interface
  - Oracle Enterprise Linux Edition Version 4 (Update 5)
  - Red Hat Enterprise Linux AS (Release 5)
  - SuSE Linux Enterprise Server 10 SP 1
  - Java Runtime Environment 1.4.2

The Evaluation Assurance Level for the TOE is EAL4 augmented with ALC\_FLR.3.

This *Evaluated Configuration for Enterprise Manager 10g Grid Control Release 5* document (which hereafter referred to as *Evaluated Configuration Document*) describes how to install, administer, and use the TOE in CC-compliant configuration. This guide is an extension to the *Oracle Enterprise Manager Grid Control Installation and Configuration Guide 10g Release 5 (10.2.0.5)*, [ICG], *Oracle Enterprise Manager Administration 10g Release 5 (10.2.0.5)*, [EMADMIN], and the *Oracle Enterprise Manager Grid Control 10g Release 5 Security Deployment*, [SD]. This guide explains the manner in which the TOE must be configured along with the host operating system and network services so as to provide the security functionality and assurance as required under the Common Criteria for Information Technology Security Evaluation [CC].

In addition, the operational environment of Grid Control, such as operating systems, must also be set up according to this document and/or other related documents that this document refers to.

The assumptions and procedures stated in the document are all (by and large) intended to remove potential vulnerabilities or attack paths from the TOE in its environment.

Note: This guide supersedes any other guidance documentation in case of conflicting statements.

## 1.1 Intended Audience

The intended audience for this document includes Common Criteria evaluators of the TOE, system integrators who will be integrating the TOE into systems, and accreditors of the systems into which the TOE has been integrated.

## 1.2 Organization

This document is composed of the following sections:

- Chapter 1* contains a brief introduction to the CC certification, the structure of this document, and delivery of the TOE.
- Chapter 2* provides an overview of the security functionality of the TOE;
- Chapter 3* describes the physical environment of the TOE and the operational environment, required to support the TOE;
- Chapter 4* describes the host operating system and all other operational environment configurations required to support the TOE;
- Chapter 5* describes the configuration of the TOE; and all TOE-related services and applications;
- Annex A* lists the software components installed as per chapter 5;
- Annex B* contains an errata that provides changes to the TOE's user guidance documentation;
- Annex C* lists the references that are used in this document

### 1.3 Format

Assertions (e.g., assumptions) for the physical, personnel, and connectivity are given identifiers to the left of each evaluation configuration requirement in bold Arial font, e.g., **[A-1]**. Mandatory evaluation configuration requirements use the words “must” and/or “shall” in each assertion.

Strongly recommended evaluation configurations use the words “should” in each assertion.

### 1.4 Delivery of the TOE

To determine that the physical media has not been tampered with, check that:

1. the original packaging material with Oracle logo is being used,
2. the way bill contains both the order reference and the tracking number previously announced by Oracle.
3. the CD envelopes in the package are sealed and that the correct version (10.2.0.5) has been shipped.

### 1.5 Electronic Delivery of the TOE

To receive electronic delivery of the TOE, complete the following steps:

4. If you do not always have a SHA-1 file hash tool, download an appropriate SHA-1 tool to verify SHA-1 checksums. SHA-1 tools are available for any platform.
5. Access the Oracle E-Delivery website at: <https://edelivery.oracle.com>
6. (*Optional*) Choose a language preference.
7. Check Continue.
8. Enter your user information and click the checkboxes to agree to the license terms and export restrictions, then click Continue.
9. Select Oracle Enterprise Manager in the Product Pack field, then select Linux x86-64 or Linux x86 from OS platform from the drop-down list.
10. Select the Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) from the results list, then click Continue.
11. Click the View Digest button. A popup window displays with all available checksum values (both MD5 and SHA-1). Note that you should only use the SHA-1 checksum for verification. Take a note of the SHA-1 checksum value provided for the desired download (depending on your OS platform).
12. Make sure that the certificate associated with the web page that displays the digest is signed by a trusted CA. If your browser does not display any error message regarding the certificate, then it is signed by a trusted CA already known to the browser (here:

Verisign). You can check this by moving the mouse pointer over the secure session system (lock) in the browser.

In case of verification errors, the displayed digest cannot be trusted.

13. Close the View Digest popup window.
14. Click the Download button for the desired download (depending on your OS platform) and save the selected .zip file to the desired disk location.
15. Verify that the checksum for your download matches the checksum shown on the Oracle download page. For example, to calculate the SHA-1 hash value of the download, execute the following command (a built-in tool in most Unix-based) operating systems):  
“shasum *file\_name.zip*”

Where *file\_name.zip* is the name of the file that was transferred. This will generate a hexadecimal number that can be compared to the checksum value you noted above. If differences exist, corruption to the download may have occurred and the download cannot be trusted.

### **1.5.1 For Patch and Critical Patch Updates (CPU)**

16. Access the Oracle patch set website: <https://metalink.oracle.com>
17. Click Login To metaLink. Note: First time users must first register by clicking Register For MetaLink.
18. Enter your user information and click Sign I.
19. Select the Patches and Updates tab and click Simple Search.
20. Search by Patch Number/name: 8968670
21. Click Go.
22. Verify the search results returned the Oracle Database Patch Set necessary to achieve the TOE (10.2.0.5) for your operating system platform.
23. Click View Readme to access and/or print (recommended) the patch set notes.
24. Contact Oracle Support to obtain the password in order to download the patch(es).
25. Follow steps 6-8 above to note the checksum, download the patch set, and verify the checksum of the download.
26. Repeat steps 16 to 25 for the Patch Numbers/names 8814764 and 9019231.  
Note: skip step 24 for patch # 9019231.

### **1.5.2 For Guidance Documents**

27. Download the documentation for the TOE in PDF format from Oracle's website <http://www.oracle.com/technetwork/indexes/documentation/index.html> or <http://www.oracle.com/technetwork/topics/security/oracle-common-criteria-095703.html>.
28. You can generate hash sums for the PDF documents in the same manner as described above for the installation file, and compare them to the hash sums published in the certification report for Oracle Enterprise Manager 10g Grid Control Release 5 (available at [https://www.bsi.bund.de/cln\\_174/ContentBSI/EN/Topics/Certification/certific.html](https://www.bsi.bund.de/cln_174/ContentBSI/EN/Topics/Certification/certific.html)).



29. Should the hash sum for a guidance document obtained from Oracle's website not match the published value, it may have been updated. Email [seceval\\_us@oracle.com](mailto:seceval_us@oracle.com) in order to obtain the version of the document that was subject to evaluation.

## 1.6 Electronic Delivery of the Oracle Database 11g Release 1 (11.1.0.7)

To receive electronic delivery of the Oracle Database, complete the following steps:

1. Access the Oracle E-Delivery website at: <https://edelivery.oracle.com>
2. (*Optional*) Choose a language preference.
3. Click Continue.
4. Enter your user information and click the checkboxes to agree to the license terms and export restrictions, then click Continue.
5. Select Oracle Database in the Product Pack field, then select Linux x86-64 or Linux x86 from OS platform from the drop-down list.
6. Select the Oracle Database 11g Release 1 (11.1.0.6) from the results list, then
7. Click the View Digest button. A popup window displays with all available checksum values (both MD5 and SHA-1). Note that you should only use the SHA-1 checksum for verification. Take a note of the SHA-1 checksum value provided for the desired download (depending on your OS platform).
8. Make sure that the certificate associated with the web page that displays the digest is signed by a trusted CA. If your browser does not display any error message regarding the certificate, than it is signed by a trusted CA already known to the browser (here: Verisign). You can check this by moving the mouse pointer over the secure session symbol (lock) in the browser.  
In cases of certificate verification errors, the displayed digest cannot be trusted.
9. Make sure that the certificate associated with the web page that displays the digest is signed by a trusted CA. If your browser does not display any error message regarding the certificate, than it is signed by a trusted CA already known to the browser (here: Verisign). You can check this by moving the mouse pointer over the secure session symbol (lock) in the browser.  
In cases of certificate verification errors, the displayed digest cannot be trusted
10. Close the View Digest popup window.
11. Click the Download button for the desired download (depending on your OS platform) and save the selected .zip file to the desired disk location.
12. Verify that the checksum for your download matches the checksum shown on the Oracle download page. For example, to calculate the SHA-1 hash value of the download, execute the following command (a built-in tool in most Unix-based operating systems):  
“`sha1sum file_name.zip`”

where *file\_name.zip* is the name of the file that was transferred. This will generate a hexadecimal number that can be compared to the checksum value you noted above. If

differences exist, corruption to the download may have occurred and the download cannot be trusted.

13. Access the Oracle patch set website at: <https://metalink.oracle.com>
14. Click Login To MetaLink. Note: First time users must first register by clicking Register For MetaLink.
15. Enter your user information and click Sign In.
16. Select the Patches and Updates tab and click Simple Search.
17. Search by Patch Number/Name: 6890831.
18. Click Go.
19. Verify the search results returned the Oracle Database Patch Set necessary to achieve the TOE (11.1.0.7) for your operating system platform.
20. Click View Readme to access and/or print (recommended) the patch set notes.
21. Follow steps 2-4 above to note the checksum, download the patch set, and verify the checksum of the download.
22. Repeat steps 13-21 for the Critical Patch Update July 2009 (patch number: 8290478), and either the patch 8514682 (64-bit) or patch 8596022 (32-bit).

## **1.7 Verification of TOE version**

### **Verifying the agent version:**

On the agent host, issue the following CLI command:

```
<agent_home>/bin/emctl status agent
```

The following information is expected to show up:

```
Agent Version:      10.2.0.5.0
```

### **Verifying the OMS version:**

On the OMS host, issue the following CLI command:

```
<oms_home>/bin/emctl status oms
```

The following information is expected to show up:

```
Oracle Enterprise Manager 10g Release 5 Grid Control
```

### **Verifying the patch level:**

On the OMS host, issue the following CLI command:

```
opatch lsinventory -oh $OMS_HOME
```

The following patch information is expected to be listed:

Patch 8968670

Patch 8814764

# 2 Overview of Security Functionality

This section provides an overview of the TOE security functions that were evaluated. For more detailed information of these security functions, see chapter 7 of [ST].

## 2.1 Identification and Authentication

The TOE enforces identification and authentication to determine the identity of a user requesting to gain access to the TOE via the Oracle Management Server (OMS)-provided GUI or the CLI. The TOE receives from the user credentials (user ID and password) and passes this information to the repository in the operational environment for verification. The repository returns an authentication decision to the TOE. The TOE then enforces the authentication decision by either granting or rejecting access to the user.

Another form of authentication performed by the TOE involves the use of agent registration passwords and agent keys. This authentication mechanism occurs when the agent wanting to establish connection with the Oracle Management Server (OMS). The mechanism is summarized below:

- Agent registration passwords: passwords that are defined by administrator and provided to the agents for use during installation (bootstrapping). When a new, otherwise unknown agent registers with the OMS, the OMS will verify that the agent provides a valid registration password.
- Agent keys: passwords defined for individually identified agents that are both stored in the OMS as attributes of the respective agent, and on the target host as part of the agent configuration. These passwords are negotiated during agent registration process which involves the agent and the OMS verify that the HTTPS headers exchanged between them contain this password.

## 2.2 Privileged-based Access Control

The TOE enforces privilege-based access control policy for administrators using the TOE GUI or CLI interface to manage targets. Users are granted with certain privileges and roles.

Roles allow users to group privileges and to grant these to users or other roles.

Privileges give users rights to perform certain management actions within Grid Control.

Together privileges and roles control the targets a user can manage and specific types of tasks the user can perform.

The following privileges may be provided to the authenticated users:

- SYSTEM privileges:
  - SUPER\_USER - provides all privileges and full access to all targets as well as enables user and role management capabilities.
- TARGET privileges:
  - CREATE\_TARGET – ability to create a target
  - CREATE\_PROPAGATING\_GROUP – ability of create privilege propagating groups. Privileges granted on a privilege propagating group will be automatically granted on the members of the group
  - VIEW\_TARGET – ability to view properties, inventory, and monitor information about a target
  - BLACKOUT\_TARGET – ability to create, edit, schedule, or stop a blackout on a target
  - MANAGE\_TARGET\_METRICS – ability to edit threshold for metric and policy setting, apply monitoring templates, or manage User Defined Metrics
  - CONFIGURE\_TARGET – ability to edit target properties or modify monitoring configuration
  - MANAGE\_TARGET\_ALERTS – ability to clear stateless alerts, manually re-evaluate alerts or acknowledge alerts for the target properties
  - FULL\_TARGET – ability to do all operations on the target, including delete the target
  - GROUP\_ADMINISTRATION – ability to administer group targets
  - EM\_MONITOR – ability to read related actions on target properties, inventory, and monitoring information.
- JOB privileges
  - VIEW\_JOB – ability to view, or do a create like on a job
  - FULL\_JOB – ability to view any report
- REPORT privileges
  - PUBLISH\_REPORT – ability to publish reports for public viewing
  - VIEW\_ANY\_REPORT – ability to view any report
  - VIEW\_REPORT – ability to view report definition and stored reports, generate on demand reports or do a create like
- TEMPLATE privileges
  - VIEW\_TEMPLATE – ability to view a template

- FULL\_TEMPLATE – ability to apply, modify, or delete a template

Note: Within the context of the evaluation, system privileges refer to privileges that can be only be assigned to the SUPER USER role. Likewise, target privileges refer to privileges that allow a user who is assigned to those privileges to perform the corresponding operations on the target (i.e., managed machine).

## 2.3 Auditing

The TOE generates audit records of security-relevant activities triggered by users.

The following types of events are audited:

- Authentication attempts
- Logon/logoff
- User management
- Security attribute management
- Job management
- File transfer
- Remote operations

Audit records generated contain the following information:

- Date and time of the event
- User identity (if application)
- Outcome of the event (success/failure)
- Name and IP address of the user's host system

In addition, authorized users may select and view the audit records.

## 2.4 Data Transfer Protection

The TOE provides protected communication between the OMS host and agents via the use of SSL/TLS. When an agent wants to communicate securely with the OMS, the agent first has to register itself through the use of the agent registration described above. Upon successful registration, the OMS generates the server certificate along with associated CA's and trusted certificates for the agent to download. The agent then uses that certificate to establish secure communication with the OMS.

For a recurring agent wanting to connect to the OMS securely, the agent will renegotiate the agent key and download a new wallet created by OMS.

## 2.5 Compliance Management

The TOE performs comparison between configurations of managed targets and baseline configurations defined by administrators. The TOE generates reports based on the results from the comparison. In addition, the TOE notifies administrators of any violations such as inappropriate settings and incorrect system configurations.

Violation alerts generated and sent to administrators contain identification of all the policies, violations as well as compliance scores of the target.

Compliance score is a combination of severity, importance, and the percentage of objects found to be non-compliant.

Compliance score indicates the percentage to which a target has been compliant with the goals defined by management policies. Compliance score also summarizes all existing defined policies into a useful metric that can be monitored showing the level of compliance of a target.

Severity refers to the seriousness of the violation and is consisted of the following levels:

- Critical – denotes a violation that needs immediate attention
- Warning – warns of serious consequences if the violation is not dealt with in a timely manner
- Informational – imparts knowledge about an object that is violating best practices

Importance denotes the impact of the policy violation against a target. A “High” importance level indicates that the system could be compromised if a security policy rule violation is ignored.

## **2.6 Security Function Management**

The TOE provided on the OMS administrative interfaces GUI and CLI to manage security functions of the TOE.

The following aspects are subject to management:

- Security attributes used for the enforcement of the privilege-based access control policy
- TSF data including restricting the ability to query, modify, and delete audit events to be recorded, definition of target configuration baselines to authorized administrators
- Management functions including audit management, security attribute management, baseline configuration management, and credential management of target objects
- SSL/TLS certificates
- Security roles

# 3

## Evaluated Configuration Requirements

This chapter describes the requirements for maintaining the security of the TOE in its evaluated configurations.

### 3.1 Software Requirements

The TOE shall only be used with the software applications listed in this section.

#### 3.1.1 Operating System

The TOE is evaluated on the following operating system platforms which have been Common Criteria certified at assurance level EAL4 with compliance to Controlled Access Protection Profile [CAPP].

- Oracle Enterprise Linux Version 4 Update 5
- Red Hat Enterprise Linux AS Release 5
- SuSE Linux Enterprise Server 10 SP1

A CC-compliant installation of Grid Control includes installation on one of the operating systems listed above.

Chapter 4 provides instructions for the installation and configuration for each of these respective operating system platforms.

#### 3.1.2 Java Virtual Machine

The TOE is evaluated on the following Java Virtual Machine (JVM). Only this JVM is acceptable for the deployment of the TOE in its evaluated configuration.

- Java Runtime Environment 1.4.2

The Java Runtime Environment is installed by default as part of the installation process of Grid Control. Therefore, no additional installation is required.



### 3.1.3 Database Repository

The TOE requires a database where the Management Repository can be created.

The evaluated version of Grid Control comes with an embedded Oracle Database 10g Release 1 (10.1.0.4). However, for the evaluated configurations, the following version of the Oracle Database is supported.

- Oracle Database 11g Release 1 (11.1.0.7). This version of the Oracle Database has been Common Criteria certified at assurance level EAL4.

Section 1.7 provides instructions for obtaining Common Criteria Certified Oracle Database 11g.

Section 5.1.2 provides instructions for the installation and configuration for Oracle Database.

### 3.1.4 Application Server

The TOE requires an application server where the Oracle Management Service (OMS) can be run. The following application server is supported in the evaluated configuration.

- Oracle Application Server 10.1.2.3

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

Chapter 4 provides instructions for the installation and configuration for Oracle Application Server

## 3.2 Physical Requirements

- [P-1]** The machine(s) providing the runtime environment or the TOE, and the database or the OMS Repository, are protected from physical access and modification.

## 3.3 Personnel Requirements

- [A-1]** Administrators responsible or the administration of the TOE are competent and trustworthy individuals who are not careless, willfully negligent, or hostile and also will follow the provided guidance

documentation to install, configuration, operate, and manage the TOE and its operational environment properly.

- [A-2]** Administrators responsible for the administration of the TOE must ensure that the systems hosting parts of the TOE are used solely for this purpose and configured properly (i.e., not running application software except as required) to prevent unauthorized access to the TOE and the security information it contains. This also includes prevention against unauthorized physical access and network-related attacks.

### **3.4 Connectivity Requirements**

- [C-1]** The machine(s) providing the runtime environment for the TOE, and the database for the OMS repository are protected from physical access and modification.
- [C-2]** The machines providing the runtime environment for the TOE are used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the operational environment.
- [C-3]** Target host (operating system) – the operating system hosting the managed targets and agents must restrict access to the agent and agent configuration data to authorized users.
- [C-4]** OMS host (Oracle Application Server) – the application server needs to protect the EMGC application, its configuration and other data against unauthorized access. It needs to provide a secure network connection to the repository and managed targets. The web server used to serve the web-based GUI to administrators needs to provide SSL/TLS-protected communications to remote users. Additionally, the IP address of the client machine (which is included in the audit records) is calculated by the OMS machine.
- [C-5]** Repository (Oracle Database) – the database needs to provide authentication decisions to the OMS, VPD, and other mechanisms to restrict access to the EMGC data stored in the database, and encryption of communication with the OMS. The database must restrict access to EMGC code and data, including audit records, to authorized users. Additionally, it needs to provide a reliable time source for audit record creation.
- [C-6]** X.509 certificates used for securing communications between the OMS and the agent are imported from the TOE's runtime environment. It is also

assumed that such runtime environment is responsible for securely generating and storing these certificates.

**[C-7]**

Managed target systems have sufficient protection measures and are configured to protect the agent software of the TOE from unauthorized tampering.

# 4

## Host Configuration

This chapter describes the configuration requirements for the operating system platforms and other required operational environment components.

### 4.1 Operating Systems

The TOE shall only be used with operating system platforms listed in this section, which have all met Common Criteria security requirements for assurance level EAL 4.

#### 4.1.1 Oracle Enterprise Linux Version 4 (Update 5) and Red Hat Enterprise Linux AS (Release 5)

The following instructions apply to both Oracle Enterprise Linux and Red Hat Enterprise Linux. These respective operating systems shall be installed and operated in the manner described in [ORHEL], [ECGR].

#### 4.1.2 SuSE Linux Enterprise Server 10 SP1

SuSE Linux Enterprise Server shall be installed and operated in a manner described in [SLES].

# 5

## Oracle Enterprise Manager Configuration

The TOE consists of software only. The TOE contains no hardware or firmware components and there are no hardware or firmware dependencies which affect the evaluation.

The TOE shall be installed, configured and maintained in accordance with this document with the instructions provided in this document.

The installation process for the Grid Control does not differ from the default process. Hence, the complete list of instructions found in the *Oracle Enterprise Manager Grid Control Installation Guide* version 10.2.0.5, [ICG] and *Oracle Enterprise Manager Grid Control 10g Release 5 Security Deployment*, [SD] applies. If necessary, *How to Install Grid Control 10.2.0.5.0 on Enterprise Linux Using the Existing Database (11g)* [ICGED] may also be used. However, the following is mandatory:

- The product and this document are obtained using the delivery method described in sections 1.5 and 1.6 of this document.
- This must be a new installation of Oracle Enterprise Manager Grid Control
- The Common Criteria certified version of Oracle Database 11g used as the Management Repository is obtained using the delivery method described in section 1.7.
- The installation process is to be performed by administrator of the underlying system
- Only Repository-Based Authentication is supported as the authentication mechanism for users of the OMS-provided CLI and GUI.
- The Web interface must be configured to use HTTPS.
- Additional management plug-ins are not part of the evaluated configuration.
- Administrators should be aware that providing an under-privileged user with privileged database access may be a risk and should necessarily be avoided.
- Administrators should use a strong password for the Agent Registration Password. See Appendix B.3 for guidelines/suggestions for strong password selection.
- Read access to the sso-wallet must be restricted to the agent installation user/administrator.

## 5.1 Oracle Enterprise Manager 10g Grid Control

The evaluated Grid Control is mainly consisted of the following software components which are shipped as part of the Grid Control distribution and will be installed during the installation process of Grid Control.

- Oracle Management Service
- Oracle Management Repository
- Oracle Management Agent
- Enterprise Manager Command Line Interface

### 5.1.1 Oracle Management Service (OMS)

The OMS is installed with and deployed on Oracle Application Server. As a result, when OMS gets installed, the installation procedure first installs Oracle Application Server. Specifically, the installation procedure installs the Oracle Application Server J2EE and Web Cache installation type. The OMS is deployed on its own OC4J container in this application instance.

The following sections describe modifications to be made to the Grid Control configuration to comply with CC requirements.

### 5.1.2 Oracle Management Repository

See section 1.7 for instructions to download the Common Criteria certified Oracle Database 11g Release 1 (11.1.0.7).

The Oracle Database 11g shall be installed and operated in the manner described in Oracle *Database Installation and Configuration Guide, 11g Release 1 (11.1)*, [ODICG] and *Evaluated Configuration for Oracle Database 11g Release 1 (11.1.0)*, [ODECD].

### 5.1.3 Oracle Management Agent

The Management agents can be installed via one of the - installation methods described in section 3.3.3 of [ICG]. The following steps describe steps to be executed on the Deployment page shown on the OMS-provided GUI.

Deployment -> Configure My Oracle Support Credentials

Deployment -> Download Agent (that downloads the agent software for the selected platform onto the OMS)

Deployment -> Install Agent (that installs the agent on the selected host via ssh.–

## 5.1.4 Enterprise Manager Command Line Interface (EMCLI)

EMCLI consists of the EMCLI Client and EMCLI Oracle Management Service Extension.

The EMCLI Client is a Java-based command-line program that sends EMCLI Verbs to the OMS.

The EMCLI OMS Extension is automatically installed with the OMS and serves as the communication conduit between the EMCLI Client and the OMS.

### Installing the EMCLI Client

1. Obtain the EMCLI Client kit (emclikit.jar).

You can download the EMCLI client kit from any 10.2 Grid Control installation at the following location:

```
HTTP(S)://host:port/em/console/emcli/download
```

The emclikit.jar file is physically located in the \$ORACLE\_HOME/sysman/jlib directory of the 10.2.0.5 Grid Control OMS home.

2. Set your JAVA\_HOME environment variable and ensure that it is part of your PATH. Make sure that this variable is set to the home of a JDK 1.4.1 or greater. For example:

```
setenv JAVA_HOME /usr/local/packages/j2sdk1.4.1_02
setenv PATH $JAVA_HOME/bin:$PATH
```

3. Enter the following command to ensure that you have the correct Java in your PATH:

```
which java
```

This should show the Java in \$JAVA\_HOME/bin.

4. Install the EMCLI Client. You can install the client portion of EMCLI in any directory either on the same system as the OMS or on any system in your network (download the `emclikit.jar` file to that system).

Go to the directory where you have installed `emclikit.jar`:

```
cd $HOME/<your emcli installation directory>
```

5. Enter the following command:

```
java -jar emclikit.jar client -install_dir=<emcli client dir>
```

After you have installed the EMCLI Client, you are ready to begin setting up the client.

### **Setting Up the EMCLI Client**

After the EMCLI Client is installed, you are ready to begin using EMCLI. At this point, you can run the EMCLI Client out of the installation directory location, or alternatively, you can add it to your `PATH`.

### **Running Setup**

You must run `setup` to connect the EMCLI Client to the OMS running the EMCLI Management Services. Running the `setup` Verb installs all available Verb-associated command-line help from the EMCLI Management Service. You must run `setup` each time you want to connect to a different OMS.

1. Understand the syntax of the `setup` Verb and its options by entering the following command or referring to the `setup` Verb in the verb reference chapter of this guide:

```
./emcli help setup
```

2. Enter the `setup` Verb with at least the minimum required parameters as shown in the following example:

```
./emcli setup -url=https://myworkstation.us.oracle.com:em_port/em  
-username=em_user
```

3. Enter your user password when prompted after the EMCLI client connects with the EMCLI Management Services.

After running the `setup` Verb, the message "Emcli Setup Successful" appears, and you are ready to begin using EMCLI.



## 5.1.5 Configuring the Evaluated Configuration

The following configuration steps must be performed to ensure with Common Criteria requirements:

### 5.1.5.1 Configuring Identification and Authentication

In the evaluated configuration, users of the OMS-provided CLI and GUI shall be authenticated by the Management Repository (i.e., Oracle Database) via the Repository-Based Authentication method. The following sections provide instructions to set up Repository-Based Authentication.

The default method of authentication for users of the OMS-provided CLI and GUI is Repository-Based Authentication. Thus, configuration for authentication is done at installation time of Grid Control.

For more details, see *Oracle® Enterprise Manager Grid Control Installation and Configuration Guide 10g Release 5 (10.2.0.5)*, [IGC].

### 5.1.5.2 Configuring Compliance Management

#### Setting up a mail server for notifications

Before Enterprise Manager can send e-mail notifications, you must first specify the Outgoing Mail (SMTP) servers to be used by the notification system. Once set, you can then define e-mail notifications for yourself or, if you have Super Administrator privileges, other Enterprise Manager administrators.

You specify the Outgoing Mail (SMTP) server on the Notification Methods page on 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.

Specify one or more outgoing mail server names, the mail server authentication credentials (User Name, Password, and Confirm Password), if required, 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. A message will be sent to this e-mail address if any problem is encountered during the sending of an e-mail notification.

### 5.1.5.3 Configuring Audit Logging

Auditable events to be audited are outlined in chapter 2. The following instructions show how to set up the audit system.

### **Enabling audit using emcli commands**

- `enable_audit`: Enables auditing for all user operations.
- `disable_audit`: Disables auditing for all user operations.
- `show_audit_actions_list`: Shows a list of the user operations being audited.
- `show_audit_settings`: Shows the audit status, operation list, externalization service details, and purges period details.

### **Enabling audit using PL/SQL**

1. Log in to the Enterprise Manager Management Repository as the `sysman` user. To turn on the audit function, enter the following commands:

```
SQL> exec mgmt_audit_admin.enable_audit;  
SQL> commit;
```

2. After enabling auditing, you must restart the Oracle Management Service to ensure that this change has taken effect.
3. You can then login to Enterprise Manager and perform other user operations.

## **5.1.5.4 Configuring Privileged-based Access Control**

There is no post-installation configuration needed to enable this feature of the TOE.

## **5.1.5.5 Configuring Secure Communication between OMS and Agent**

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 Management 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 and Oracle Management Services are authorized to load their data into this Enterprise Manager installation. TOE administrators are advised to use a strong password for the Agent Registration Password. See appendix B.3 for guidelines/suggestions for strong password selection.

### **Securing the Oracle Management Service**

The following instructions are for securing 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. Configure the agent management port on the OMS by specifying the cipher suite `SSL_RSA_WITH_3DES_EDE_CBC_SHA` in `$OMS_HOME/sysman/config/httpd_em.conf.template`, e.g, as follows:

```
<IfDefine SSL>
...
SSLProxyCipherSuite SSL_RSA_WITH_3DES_EDE_CBC_SHA

<VirtualHost ...

SSLCipherSuite SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSLProxyCipherSuite SSL_RSA_WITH_3DES_EDE_CBC_SHA
```

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

```
ORACLE_HOME/bin
```

5. Enter the following command:

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

6. You will be prompted for the Enterprise Manager Root Password. Enter the `SYSMAN` password.
7. You will be prompted for the Agent Registration Password, which is the password required for any Management Agent attempting to secure with the Management Service. Specify an Agent Registration Password for the Management Service.
8. When the operation is complete, restart the Management Service, the Oracle HTTP Server, and Oracle AS 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:https_upload_port/em
```

For example: `https://mgmthost1.acme.com:1159/em`

If the Management Service security has been enabled, your browser displays the Enterprise Manager Login page.

### **Managing OMS host certificate via EMCTL**

To manage the host certificate of the OMS, you can use the command:

```
emctl secure oms
```

This command contains the following parameter:

- `key_strength` - the key size used for generation of the host certificate which has valid values of 512, 1024, and 2048 bits. Default value is 512 bits.
- `cert_validity` – number of days the certificate is valid. Default value is 3,560 days.

Please note that when these parameters are omitted, the default values are 512 bits for `key_strength` and 3,650 days (10 years) for `cert_validation`.

### **Securing the Agent**

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

```
AGENT_HOME/bin
```

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 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
```

3. Stop the Management Agent:

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

4. Enter the following command:

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

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  
$PROMPT> emctl secure agent agent_registration_pwd
```

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 homepage.

### **5.1.5.6 Configuring Secure Communication between OMS and Repository**

Security for the Management Repository is enabled through the use of Oracle Advanced Security. Oracle Advanced Security ensures the security of data transferred to and from an Oracle database.

The following sections describe how to secure the Management Repository.

#### **Configuring Oracle Advanced Security for the Management Repository**

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
```

Detailed instructions to secure the Management Repository are available at the *Oracle Database Advanced Security Administrator's Guide* [ODASAG].

#### **Configuring the Management Service to Connect to a Secure Management Repository Database**

The following instructions describe how 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 in the Management Service home directory:

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

- 3) Using a text editor, add the entries described in the `emoms.properties` file.

The entries described in the table (table 4-4 [EMADMIN]) correspond to valid parameters you can set when you configure network data encryption for the Oracle Database.

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

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

### 5.1.5.7 Configuring HTTPS for Web GUI

To restrict HTTP access (in other words, enabling HTTPS access) to the Web GUI (Grid Control Console), issue the following command.

```
emctl secure lock -console
```

To restrict the agent to communicate via HTTPS, secure the agent upload port as follows:

```
emctl secure lock -upload
```

After issuing the above command, the expected output can be as follows:

```
$prompt> emctl secure lock
Oracle Enterprise Manager 10g Release 5 Grid Control
Copyright (c) 1996, 2009 Oracle Corporation. All rights reserved.
OMS Console is locked. Access the console over HTTPS ports.
```

### 5.1.5.8 Configuring FIPS 140-2 Mode

The evaluated configuration of Grid Control must be configured to run in FIPS 140-2 compliant mode which would result in limiting support to the following cipher suite for SSL Version 3 connections.

- SSL\_RSA\_FIPS\_WITH\_3DES\_EDE\_CBC\_SHA

Add the above cipher suite to the following file:

```
$AGENT_HOME/sysman/config/emd.properties
```

To enable the FIPS mode, follow the steps below:

1. Set the following parameter in `$AGENT_HOME/network/admin/sqlnet.ora`

```
SQLNET.SSLFIPS_140=TRUE
```

2. If the OMS certificate has been changed, re-secure the agent by issuing the command  

```
emctl secure agent
```
3. Generate an autologin wallet file (cwallet.sso) using orapki with `cert name = agent_hostname`
4. Add the `$AGENT_HOME/sysman/config/b64LocalCertificate.txt` to the wallet
5. Copy the wallet file to `$AGENT_HOME/sysman/config/server` location and restart the agent.

Note: read access to the sso-wallet must be restricted to the agent installation user/administrator.

### 5.1.5.9 Disabling the WSDL Web Services Interface

To disable WSDL Web Services interface, perform the following steps:

On the OMS host, in the file:

`$OMS_HOME/j2ee/OC4J_EM/applications/em/em/WEB-INF/web.xml`,  
remove/comment out the following mapping elements:

```
<servlet-mapping>
  <servlet-name>stateless Java web service -
  /webservices/externalAlertProcessorWebService</servlet-name>
  <url-pattern>/externalAlertProcessorWebService</url-pattern>
</servlet-mapping>

<servlet-mapping>
  <servlet-name>stateless Java web service -
  /webservices/alertAnnotationProcessorWebService</servlet-name>
  <url-pattern>/alertAnnotationProcessorWebService</url-pattern>
</servlet-mapping>

<servlet-mapping>
  <servlet-name>ManagementService</servlet-name>
  <url-pattern>/connector/ManagementService</url-pattern>
</servlet-mapping>
```



Restart the OMS.

This page is intentionally left blank.

## ANNEX

# A TOE Components

To obtain a list of TOE components installed on your platform, run the following command:

```
opatch lsinventory -detail -oh <path to OMS or agent>
```

The following files contain the list of components:

```
$ORACLE_HOME/inventory/ContentsXML  
$ORACLE_HOME/inventory/Components21
```

The following is an exemplary listing of all the software components installed on an SuSE Enterprise Linux following the installation described in chapter 5.

### **A.1 OMS Components**

Invoking OPatch 11.1.0.6.9

Oracle Interim Patch Installer version 11.1.0.6.9  
Copyright (c) 2009, Oracle Corporation. All rights reserved.

```
Oracle Home      : /u01/app/gc/oms10g  
Central Inventory : /u01/app/oraInventory  
  from            : /etc/oraInst.loc  
OPatch version   : 11.1.0.6.9  
OUI version      : 10.2.0.5.0  
OUI location     : /u01/app/gc/oms10g/oui  
Log file location : /u01/app/gc/oms10g/cfgtoollogs/opatch/opatch2010-01-04_19-52-07PM.log
```

Patch history file: /u01/app/gc/oms10g/cfgtoollogs/opatch/opatch\_history.txt

Lsinventory Output file location : /u01/app/gc/oms10g/cfgtoollogs/opatch/lsinv/lsinventory2010-01-04\_19-52-07PM.txt

-----  
Installed Top-level Products (2):

Enterprise Manager Patchset 10.2.0.5.0  
 Oracle Enterprise Manager Grid Console 10.2.0.3.0  
 There are 2 products installed in this Oracle Home.

Installed Products (311):

ADF BC OMS for OracleAS GC 10.2.0.2.0  
 ADF BC Repository for OracleAS GC 10.2.0.2.0  
 Advanced Queueing (AQ) API 10.1.0.2.0  
 Advanced Queueing (AQ) API Patch 10.1.0.5.0  
 Agent Required Support Files 10.1.0.2.0  
 Agent Required Support Files Patch 10.1.0.5.0  
 Apache Configuration for Oracle Java Server Pages 10.1.2.0.0  
 Apache Module for Oracle Distributed Authoring and Versioning 10.1.2.1.0  
 Apache Module for Oracle Distributed Authoring and Versioning Patch 10.1.2.3.0  
 Assistant Common Files 10.1.0.2.0  
 Assistant Common Files Patch 10.1.0.5.0  
 Authentication and Encryption 10.1.0.2.0  
 Authentication and Encryption Patch 10.1.0.5.0  
 Bali Share 1.1.18.0.0  
 Common component for Virtualization 10.2.0.5.0  
 Database SQL Scripts 10.1.0.2.0  
 Database SQL Scripts Patch 10.1.0.5.0  
 DataDirect Connect JDBC Drivers 10.1.2.0.2  
 DBJAVA Required Support Files 10.1.0.2.0  
 DBJAVA Required Support Files Patch 10.1.0.5.0  
 Discoverer EM Plugin - OMS portion 10.2.0.2.0  
 Discoverer EM plugin - Repository portion 10.2.0.2.0  
 Documentation Required Support Files 10.1.0.3.0  
 Enterprise Manager Agent 10.1.0.4.2  
 Enterprise Manager Agent for iAS Patch 10.1.2.3.0  
 Enterprise Manager Agent for OracleAS 10.0.2.0.1  
 Enterprise Manager Application Server Plugin -- Common Support 10.2.0.3.0  
 Enterprise Manager Application Server Plugin -- Common Support Patch 10.2.0.5.0  
 Enterprise Manager Application Server Plugin -- Management Service Support 10.2.0.3.0  
 Enterprise Manager Application Server Plugin -- Management Service Support Patch 10.2.0.5.0  
 Enterprise Manager Application Server Plugin -- Repository Support 10.2.0.3.0  
 Enterprise Manager Application Server Plugin -- Repository Support Patch 10.2.0.5.0  
 Enterprise Manager BPEL Process Analytics Plugin -- Management Service Plugin 10.2.0.2.0  
 Enterprise Manager BPEL Process Analytics Plugin -- Repository Plugin 10.2.0.2.0  
 Enterprise Manager BPEL Process Manager Plugin -- Management Service Plugin 10.2.0.2.0  
 Enterprise Manager BPEL Process Manager Plugin -- Repository Plugin 10.2.0.2.0  
 Enterprise Manager Collaboration Suite Plugin -- Management Service Support 10.2.0.3.0  
 Enterprise Manager Collaboration Suite Plugin -- Management Service Support Patch 10.2.0.5.0  
 Enterprise Manager Collaboration Suite Plugin -- Repository Support 10.2.0.3.0  
 Enterprise Manager Collaboration Suite Plugin -- Repository Support Patch 10.2.0.5.0  
 Enterprise Manager Common Core Files 10.2.0.3.0  
 Enterprise Manager Common Core Files Patch 10.2.0.5.0  
 Enterprise Manager Common Files 10.2.0.3.0  
 Enterprise Manager Common Files Patch 10.2.0.5.0  
 Enterprise Manager Database Plugin -- Management Service Support 10.2.0.3.0

Enterprise Manager Database Plugin -- Management Service Support Patch	10.2.0.5.0
Enterprise Manager Database Plugin -- Repository Support	10.2.0.3.0
Enterprise Manager Database Plugin -- Repository Support Patch	10.2.0.5.0
Enterprise Manager Downloadable Agent	10.2.0.3.0
Enterprise Manager Downloadable Agent Patch	10.2.0.5.0
Enterprise Manager Grid Control Core Files	10.2.0.3.0
Enterprise Manager Grid Control Core Files Patch	10.2.0.5.0
Enterprise Manager Integration B2B Plugin -- Management Service Plugin	10.2.0.2.0
Enterprise Manager Integration B2B Plugin -- Repository Plugin	10.2.0.2.0
Enterprise Manager Integration InterConnect Plugin -- Management Service Plugin	10.2.0.2.0
Enterprise Manager Integration InterConnect Plugin -- Repository Plugin	10.2.0.2.0
Enterprise Manager Minimal Integration	10.1.0.2.0
Enterprise Manager Patchset	10.2.0.5.0
Enterprise Manager plugin Common Files	10.1.0.2.0
Enterprise Manager plugin Common Files	10.1.0.5.0
Enterprise Manager Process Utility	10.0.2.0.1
Enterprise Manager Repository	10.2.0.3.0
Enterprise Manager Repository	10.2.0.5.0
Enterprise Manager Repository Core Files	10.2.0.3.0
Enterprise Manager Repository Core Files	10.2.0.5.0
Enterprise Manager Siebel Plugin -- Agent Support	10.2.0.3.0
Enterprise Manager Siebel Plugin -- Management Service Support	10.2.0.5.0
Enterprise Manager Siebel Plugin -- Repository Support	10.2.0.5.0
Extended Windowing Toolkit	3.3.18.0.0
Forms OMS Plugin	10.2.0.2.0
Forms Repository Plugin	10.2.0.2.0
HTTP Server Files	1.3.31.0.0
HTTP Server Files Patch	10.1.2.3.0
Installation Common Files	10.1.0.2.0
Installation Common Files Patch	10.1.0.4.2
Installer SDK Component	10.2.0.5.0
Java Naming and Directory Interface Libraries	10.1.0.2.0
Java Naming and Directory Interface Libraries	10.1.0.5.0
Java Runtime Environment	1.4.2.8.0
Java Security Configuration Assistant	10.1.2.0.2
JDBC Common Files	10.1.0.2.0
JDBC Common Files Patch	10.1.0.5.0
JDBC/OCI Common Files	10.1.0.2.0
JDBC/OCI Common Files for Instant Client	10.1.0.2.0
JDBC/OCI Common Files for Instant Client Patch	10.1.0.5.0
JDBC/OCI Common Files Patch	10.1.0.5.0
LDAP Required Support Files	10.1.2.1.0
LDAP Required Support Files Patch	10.1.2.3.0
Management Connector Framework	2.0.0.0.0
Microsoft Operations Manager Connector	10.2.0.5.0
Netca Configuration for Oracle Application Server	10.1.2.0.0
Netca Patch	10.1.0.5.0
OC4J for Oracle Enterprise Manager	10.0.2.0.1
OC4J for Oracle Enterprise Manager Patch	10.1.2.3.0
Oracle Advanced Security	10.1.0.2.0
Oracle Apache Modules	10.1.2.1.0
Oracle Apache Modules Patch	10.1.2.3.0
Oracle Application Server 10g	10.1.2.0.2

Oracle Application Server Core Products	10.1.2.0.0
Oracle Application Server High availability components (BR, AFC, DR)	10.1.2.1.0
Oracle Application Server High availability components for midtier	10.1.2.0.2
Oracle Application Server Instance	10.1.2.0.2
Oracle Application Server Instance Dialog	10.1.2.0.2
Oracle Application Server Middle Tier Products	10.1.2.1.0
Oracle Application Server Object in OID	10.1.2.0.2
Oracle Application Server Repository API	10.1.2.0.2
Oracle Application Server Single Sign On Registration	10.1.2.0.0
Oracle Application Server UNIX Configuration	2.2.20.0.0
Oracle Application Server Upgrade Assistant	10.1.2.1.0
Oracle Business Intelligence Beans (graph files)	10.1.2.65.0
Oracle Client Required Support Files	10.1.0.2.0
Oracle Client Required Support Files Patch	10.1.0.5.0
Oracle CM SDK and Oracle Files Plugin for Oracle EM Repository	10.2.0.2.0
Oracle CM SDK and Oracle Files Plugin for Oracle EM Repository	10.2.0.3.0
Oracle CM SDK and Oracle Files Plugin for Oracle Management Server	10.2.0.2.0
Oracle Code Editor	1.2.1.0.0I
Oracle Collaboration Suite Web Access Plugin for Oracle Management Server	10.2.0.2.0
Oracle Collaboration Suite Web Access Plugin Patch for Oracle Management Server	10.2.0.3.0
Oracle Configuration Manager	10.3.1.0.0
Oracle Configuration Manager Repeater	10.3.1.0.0
Oracle Content DB Plugin for Oracle EM Repository	10.2.0.3.0
Oracle Content DB Plugin for Oracle Management Agent	10.2.0.3.0
Oracle Content DB Plugin for Oracle Management Server	10.2.0.3.0
Oracle Content Services Plugin for Oracle Management Server	10.2.0.2.0
Oracle Core Required Support Files	10.1.0.2.0
Oracle Core Required Support Files	10.1.0.5.0
Oracle Delegated Administration Service	10.1.2.1.0
Oracle Delegated Administration Service Patch	10.1.2.3.0
Oracle Discussions Plugin for Oracle Management Server	10.2.0.2.0
Oracle Discussions Plugin for Oracle Management Server Patch	10.2.0.3.0
Oracle Display Fonts	10.1.2.0.0
Oracle Distributed Configuration Management	10.1.2.1.0
Oracle Distributed Configuration Management Patch	10.1.2.3.0
Oracle Distributed Software Assistant	10.1.2.0.2
Oracle Distributed Software Assistant Client	10.1.2.0.2
Oracle Distributed Software Assistant Client Patch	10.1.2.3.0
Oracle Distributed Software Assistant Common	10.1.2.0.2
Oracle Distributed Software Assistant Common Patch	10.1.2.3.0
Oracle Distributed Software Assistant Patch	10.1.2.3.0
Oracle Distributed Software Assistant Server	10.1.2.0.2
Oracle Distributed Software Assistant Server Patch	10.1.2.3.0
Oracle Dynamic Monitoring Service	10.1.2.1.0
Oracle Dynamic Monitoring Service Patch	10.1.2.3.0
Oracle Dynamic Services Core	10.1.2.0.0
Oracle Dynamic Services Midtier	10.1.2.0.0
Oracle Dynamic Services Midtier Common	10.1.2.0.0
Oracle Dynamic Services Server	10.1.2.0.0
Oracle EM agent	10.1.2.0.1
Oracle Email components for Enterprise Manager Grid Control Console (OMS)	10.2.0.2.0
Oracle Email components for Enterprise Manager Grid Control Console (OMS) Patch	10.2.0.3.0
Oracle Enterprise Manager Application Server Control	10.0.2.0.1

Oracle Enterprise Manager Application Server Control Patch	10.1.2.3.0
Oracle Enterprise Manager Grid Console	10.2.0.3.0
Oracle Enterprise Manager Grid Console Patch	10.2.0.5.0
Oracle Extended Windowing Toolkit	3.4.38.0.0
Oracle Globalization Support	10.1.0.2.0
Oracle Globalization Support Patch	10.1.0.5.0
Oracle Help For Java	4.2.6.1.0
Oracle Help for the Web	2.0.8.0.0
Oracle HTTP Server	10.1.2.1.0
Oracle Ice Browser	5.2.3.6.0
Oracle interMedia Java Advanced Imaging Taglib	10.1.2.1.0
Oracle Internet Directory Tools	10.1.2.1.0
Oracle Internet Directory Tools Patch	10.1.2.3.0
Oracle Java Object Cache	10.1.2.1.0
Oracle Java Object Cache Patch	10.1.2.3.0
Oracle Java Portal Development Kit	10.1.2.0.1
Oracle Java Tools	10.1.0.2.0
Oracle Java Tools Patch	10.1.0.5.0
Oracle JDBC Thin Driver for JDK 1.1	10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.2	10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.2 Patch	10.1.0.5.0
Oracle JDBC Thin Driver for JDK 1.4	10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.4	10.1.0.5.0
Oracle JDBC Thin Driver for JDK 1.4 for Instant Client	10.1.0.2.0
Oracle JDBC Thin Driver for JDK 1.4 for Instant Client Patch	10.1.0.5.0
Oracle JDBC/OCI Driver for JDK 1.1	10.1.0.2.0
Oracle JDBC/OCI Driver for JDK 1.2	10.1.0.2.0
Oracle JFC Extended Windowing Toolkit	4.2.33.0.0
Oracle JFC Extended Windowing Toolkit Patch	4.2.34.0.0
Oracle Locale Builder	10.1.0.2.0
Oracle Locale Builder Patch	10.1.0.5.0
Oracle LogLoader	10.1.2.1.0
Oracle Management Service	10.2.0.3.0
Oracle Management Service Patch	10.2.0.5.0
Oracle Mobile Collaboration Server Plugin for Oracle Management Server	10.2.0.2.0
Oracle Mobile Collaboration Server Plugin for Oracle Management Server Patch	10.2.0.3.0
Oracle Mod PL/SQL Gateway	10.1.2.0.0
Oracle Net	10.1.0.2.0
Oracle Net Configuration Assistant	10.1.0.2.0
Oracle Net Manager	10.1.0.3.0
Oracle Net Manager Patch	10.1.0.5.0
Oracle Net Patch	10.1.0.5.0
Oracle Net Required Support Files	10.1.0.2.0
Oracle Net Required Support Files Patch	10.1.0.5.0
Oracle Notification Service	10.1.2.1.0
Oracle Notification Service Patch	10.1.2.3.0
Oracle OC4J Module	10.1.2.1.0
Oracle OC4J Module Patch	10.1.2.3.0
Oracle One-Off Patch Installer	10.2.0.4.2
Oracle Portal Monitoring	10.1.2.0.1
Oracle Portal OMS	10.2.0.2.0
Oracle Portal Repository	10.2.0.2.0
Oracle Process Management Notification	10.1.2.1.0

Oracle Process Management Notification Patch	10.1.2.3.0
Oracle Property Inspector	4.1.21.0.0
Oracle RAC Required Support Files	10.1.0.2.0
Oracle RAC Required Support Files Patch	10.1.0.5.0
Oracle RAC Required Support Files-HAS	10.1.0.2.0
Oracle RAC Required Support Files-HAS Patch	10.1.0.5.0
Oracle Rules Manager	10.2.0.3.0
Oracle Rules Manager Patch	10.2.0.5.0
Oracle SOAP Client files	2.2.0.0.2a
Oracle SOAP Client files Patch	2.2.0.0.2b
Oracle SOAP Server	2.2.0.0.2a
Oracle SOAP Server Patch	2.2.0.0.2b
Oracle SSO OMS	10.2.0.2.0
Oracle SSO Repository	10.2.0.2.0
Oracle TopLink Runtime	10.1.3.1.0
Oracle UIX	2.2.20.0.0
Oracle Ultra Search Plugin for Oracle Management Service	10.2.0.2.0
Oracle Ultra Search Plugin for Oracle Management Service Patch	10.2.0.3.0
Oracle Universal Installer	10.2.0.5.0
Oracle Voice Mail and Fax Files Plugin for Oracle Management Server	10.2.0.2.0
Oracle Voice Mail and Fax Files Plugin for Oracle Management Server Patch	10.2.0.3.0
Oracle Wallet Manager	10.1.0.2.0
Oracle Wallet Manager Patch	10.1.0.5.0
Oracle Workflow OMS component for Grid Control	10.2.0.2.0
Oracle Workflow repository component for Grid Control	10.2.0.2.0
Oracle Workspaces Plugin for Oracle Management Server	10.2.0.2.0
Oracle Workspaces Plugin for Oracle Management Server Patch	10.2.0.3.0
Oracle XML SQL Utility	10.1.0.2.0
Oracle XML SQL Utility Patch	10.1.0.5.0
Oracle10g Real Application Clusters Common Files	10.1.0.2.0
Oracle10g Real Application Clusters Common Files Patch	10.1.0.5.0
OracleAgent Deployment	10.2.0.3.0
OracleAgent Deployment Patch	10.2.0.5.0
OracleAS Configuration for OC4J	10.1.2.1.0
OracleAS J2EE	10.1.2.1.0
OracleAS J2EE BULKOPS	11.0.0.0.0
OracleAS J2EE Patch	10.1.2.3.0
OracleAS Port Tunnel	10.1.2.1.0
OracleAS Port Tunnel Patch	10.1.2.3.0
OracleAS Single Sign On Server Common Patch	10.1.2.3.0
OracleAS Web Cache	10.1.2.1.0
OracleAS Web Services	10.1.2.1.0
Parser Generator Required Support Files	10.1.0.2.0
Parser Generator Required Support Files Patch	10.1.0.5.0
Patch of Oracle Application Server 10g	10.1.2.3.0
Patch of Oracle Application Server High availability components (BR, AFC, DR)	10.1.2.3.0
Patch of Oracle Application Server Object in OID	10.1.2.3.0
Patch of Oracle Application Server Repository API	10.1.2.3.0
Patch of Oracle Dynamic Services Core	10.1.2.3.0
Patch of Oracle Dynamic Services Midtier	10.1.2.3.0
Patch of Oracle Dynamic Services Midtier Common	10.1.2.3.0
Patch of Oracle EM agent	10.1.2.3.0
Patch of Oracle Java Portal Development Kit	10.1.2.3.0



Patch of Oracle Mod PL/SQL Gateway	10.1.2.3.0	
Patch of Oracle Portal Monitoring	10.1.2.3.0	
Patch of OracleAS Upgrade Assistant	10.1.2.3.0	
Patch of OracleAS Web Cache	10.1.2.3.0	
Patch of OracleAS Web Services	10.1.2.3.0	
Patch of Sun JDK	1.4.2.14.02	
Perl Interpreter	5.6.1.0.2d	
PL/SQL Required Support Files	10.1.0.2.0	
PL/SQL Required Support Files	10.1.0.5.0	
Platform Required Support Files	10.1.0.2.0	
Platform Required Support Files Patch	10.1.0.5.0	
Precompiler Required Support Files	10.1.0.2.0	
Precompiler Required Support Files Patch	10.1.0.5.0	
Provisioning Advisor Framework	10.2.0.3.0	
Provisioning Advisor Framework Common Files For Agent and OMS		10.2.0.5.0
Provisioning Advisor Framework Patch	10.2.0.5.0	
RDBMS Required Support Files	10.1.0.2.0	
RDBMS Required Support Files Patch	10.1.0.5.0	
regexp	2.1.9.0.0	
Remedy HelpDesk Connector	10.2.0.5.0	
Reports EM plugin - OMS portion	10.2.0.2.0	
Reports EM plugin - Repository portion	10.2.0.2.0	
Required Support Files	10.1.0.2.0	
Secure Socket Layer	10.1.0.2.0	
Secure Socket Layer	10.1.0.2.0	
Secure Socket Layer Patch	10.1.0.5.0	
SQL*Plus	10.1.0.2.0	
SQL*Plus	10.1.0.5.0	
SQL*Plus Required Support Files	10.1.0.2.0	
SQL*Plus Required Support Files Patch	10.1.0.5.0	
SQLJ Runtime	10.1.2.1.0	
SQLJ Runtime Patch	10.1.2.3.0	
SSL Required Support Files	10.1.0.2.0	
SSL Required Support Files for InstantClient	10.1.0.2.0	
SSL Required Support Files for InstantClient Patch	10.1.0.5.0	
SSL Required Support Files Patch	10.1.0.5.0	
Sun JDK	1.4.2.0.8a	
Sun JDK extensions	10.1.2.0.0	
Virtualization component for OMS	10.2.0.5.0	
Virtualization component for repository	10.2.0.5.0	
Visigenics ORB	3.4.0.0.0	
Visigenics ORB	3.4.0.0.0d	
Wireless EM OMS	10.2.0.2.0	
Wireless EM repository	10.2.0.2.0	
XDK Required Support Files	10.1.0.2.0	
XDK Required Support Files Patch	10.1.0.5.0	
XML Class Generator for Java	10.1.0.2.0	
XML Class Generator for Java Patch	10.1.0.5.0	
XML Parser for Java	10.1.0.2.0	
XML Parser for Java Patch	10.1.0.5.0	
XML Transx	10.1.0.2.0	
XML Transx Patch	10.1.0.5.0	
XSQL Servlet	10.1.0.2.0	

XSQL Servlet Patch 10.1.0.5.0  
There are 311 products installed in this Oracle Home.

Interim patches (11) :

Patch 8968670 : applied on Mon Jan 04 19:40:48 CET 2010

Unique Patch ID: 12034224

Created on 15 Dec 2009, 10:10:27 hrs PST8PDT

Bugs fixed:

8968670

Files Touched:

/oracle/sysman/emSDK/sec/audit/AuditManager.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/emSDK/sec/audit/AuditSessionHandler.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/emSDK/sec/auth/EMLoginService.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/emdrep/audit/AuditConfigManager.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/emdrep/audit/AuditCacheManager.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/eml/sec/audit/AuditSearchHandler\$1.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/eml/sec/audit/AuditSearchHandler\$AuditTimestampComparator.class -->  
ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/eml/sec/audit/AuditSearchHandler.class --> ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/eml/sec/audit/CustomAuditAttrResourceBundle.class -->  
ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/eml/sec/audit/CustomAuditAttrResourceBundleID.class -->  
ORACLE\_HOME/sysman/jlib/emCORE.jar  
/oracle/sysman/emdrep/audit/emcli/AuditOMSSideMsg.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/AuditOMSSideMsgID.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/EnableEMAuditingVerb.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/ShowAuditSettings.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/UpdateAuditSettings.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/DisableEMAuditingVerb.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/emdrep/audit/emcli/AuditClientSideMsg.class -->  
ORACLE\_HOME/sysman/emcli/clientsideext/standardclientside.jar  
auditDetails.uix --> ORACLE\_HOME/j2ee/OC4J\_EM/applications/em/em/sec/audit/auditDetails.uix  
audit\_admin\_pkgbody.sql -->  
ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/audit/audit\_admin\_pkgbody.sql  
audit\_admin\_pkgdef.sql -->  
ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/audit/audit\_admin\_pkgdef.sql  
audit\_externalization\_pkgbody.sql -->  
ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/audit/audit\_externalization\_pkgbody.sql  
audit\_data\_upgrade.sql -->  
ORACLE\_HOME/sysman/admin/emdrep/sql/core/10.3.0.0/audit/audit\_data\_upgrade.sql  
audit\_post\_creation.sql --> ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/audit/audit\_post\_creation.sql  
sdk\_audit\_pkgbody.sql --> ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/sdk/sdk\_audit\_pkgbody.sql  
sdk\_audit\_pkgdef.sql --> ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/sdk/sdk\_audit\_pkgdef.sql  
Patch Location in Inventory:  
/u01/app/gc/oms10g/inventory/oneoffs/8968670

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/8968670\_Dec\_15\_2009\_10\_10\_27

Patch 8814764 : applied on Mon Jan 04 15:51:57 CET 2010

Unique Patch ID: 12034223

Created on 14 Dec 2009, 03:52:14 hrs PST8PDT

Bugs fixed:

8814764

Files Touched:

/oracle/sysman/eml/creds/pdp/emcli/CreatePdpSettingVerb.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/eml/creds/pdp/emcli/DeletePdpSettingVerb.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/eml/creds/pdp/emcli/PdpOMSSideMsg.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
/oracle/sysman/eml/creds/pdp/emcli/PdpOMSSideMsgID.class -->  
ORACLE\_HOME/sysman/emcli/omssideext/standardomsside.jar  
credentials\_ui\_pkgbody.sql -->  
ORACLE\_HOME/sysman/admin/emdrep/sql/core/latest/credentials/credentials\_ui\_pkgbody.sql

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/8814764

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/8814764\_Dec\_14\_2009\_03\_52\_14

Patch 8321694 : applied on Mon Dec 21 22:23:45 CET 2009

Unique Patch ID: 11108984

Created on 20 Mar 2009, 04:46:24 hrs PST8PDT

Bugs fixed:

8321694

Files Touched:

/\_home.class --> ORACLE\_HOME/sysman/jlib/emcore\_emjsp.jar  
home.jsp --> ORACLE\_HOME/j2ee/OC4J\_EM/applications/em/em/home.jsp

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/8321694

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/8321694\_Mar\_20\_2009\_04\_46\_24

Patch 5649850 : applied on Mon Dec 21 22:23:24 CET 2009

Created on 19 Oct 2008, 23:01:26 hrs PST8PDT

Bugs fixed:

5649850

Files Touched:

/oracle/jdbc/pool/OracleConnectionPoolDataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14dms.jar  
/oracle/jdbc/pool/OraclePooledConnection.class --> ORACLE\_HOME/jdbc/lib/ojdbc14dms.jar  
/oracle/jdbc/xa/client/OracleXADataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14dms.jar  
/oracle/jdbc/pool/OracleImplicitConnectionFactory.class --> ORACLE\_HOME/jdbc/lib/ojdbc14dms.jar  
/oracle/jdbc/pool/OracleConnectionPoolDataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14.jar  
/oracle/jdbc/pool/OraclePooledConnection.class --> ORACLE\_HOME/jdbc/lib/ojdbc14.jar  
/oracle/jdbc/xa/client/OracleXADataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14.jar  
/oracle/jdbc/pool/OracleImplicitConnectionFactory.class --> ORACLE\_HOME/jdbc/lib/ojdbc14.jar  
/oracle/jdbc/pool/OracleConnectionPoolDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.jar  
/oracle/jdbc/pool/OracleConnectionPoolDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.zip  
/oracle/jdbc/pool/OracleConnectionPoolDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar

/oracle/jdbc/pool/OraclePooledConnection.class --> ORACLE\_HOME/jdbc/lib/classes12.jar  
/oracle/jdbc/pool/OraclePooledConnection.class --> ORACLE\_HOME/jdbc/lib/classes12.zip  
/oracle/jdbc/pool/OraclePooledConnection.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar  
/oracle/jdbc/xa/client/OracleXADataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.jar  
/oracle/jdbc/xa/client/OracleXADataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.zip  
/oracle/jdbc/xa/client/OracleXADataSource.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar  
/oracle/jdbc/pool/OracleImplicitConnectionFactory.class --> ORACLE\_HOME/jdbc/lib/classes12.jar  
/oracle/jdbc/pool/OracleImplicitConnectionFactory.class --> ORACLE\_HOME/jdbc/lib/classes12.zip  
/oracle/jdbc/pool/OracleImplicitConnectionFactory.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/5649850

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/5649850\_Oct\_19\_2008\_23\_01\_26

Patch 5883719 : applied on Mon Dec 21 22:22:52 CET 2009

Created on 5 Dec 2008, 05:54:42 hrs PST8PDT

Bugs fixed:

5883719

Files Touched:

/oracle/jdbc/driver/T4CConnection.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar

/oracle/jdbc/driver/T4CTTIOauthenticate.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/5883719

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/5883719\_Dec\_5\_2008\_05\_54\_42

Patch 7227700 : applied on Mon Dec 21 22:22:33 CET 2009

Created on 23 Jul 2008, 01:17:08 hrs US/Pacific

Bugs fixed:

7227700

Files Touched:

eusm.jar --> ORACLE\_HOME/jlib/eusm.jar

opm.jar --> ORACLE\_HOME/jlib/opm.jar

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/7227700

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/7227700\_Jul\_23\_2008\_01\_17\_08

Patch 5984608 : applied on Mon Dec 21 22:22:18 CET 2009

Created on 27 May 2007, 23:53:18 hrs US/Pacific

Bugs fixed:

5984608

Files Touched:

/oracle/jdbc/pool/OracleDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.jar

/oracle/jdbc/pool/OracleDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12.zip

/oracle/jdbc/pool/OracleDataSource.class --> ORACLE\_HOME/jdbc/lib/classes12dms.jar

/oracle/jdbc/pool/OracleDataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14.jar

/oracle/jdbc/pool/OracleDataSource.class --> ORACLE\_HOME/jdbc/lib/ojdbc14dms.jar

Patch Location in Inventory:

/u01/app/gc/oms10g/inventory/oneoffs/5984608

Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/5984608\_May\_27\_2007\_23\_53\_18

Patch 6672979 : applied on Mon Dec 21 22:22:02 CET 2009  
Created on 7 Feb 2008, 01:59:07 hrs US/Pacific  
Bugs fixed:  
6672979  
Files Touched:  
timezone.dat --> ORACLE\_HOME/oracore/zoneinfo/timezone.dat  
timezlrq.dat --> ORACLE\_HOME/oracore/zoneinfo/timezlrq.dat  
readme.txt --> ORACLE\_HOME/oracore/zoneinfo/readme.txt  
Patch Location in Inventory:  
/u01/app/gc/oms10g/inventory/oneoffs/6672979  
Patch Location in Storage area:  
/u01/app/gc/oms10g/.patch\_storage/6672979\_Feb\_7\_2008\_01\_59\_07

Patch 5336126 : applied on Mon Dec 21 22:21:46 CET 2009  
Created on 11 Nov 2008, 12:48:26 hrs US/Pacific  
Bugs fixed:  
5336126  
Files Touched:  
/oracle/core/ojdl/LogMessage\$InstanceId.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage\$MessageArgument.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/MessageType.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage\$InstanceId.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/LogMessage\$MessageArgument.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/LogMessage.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/MessageType.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/ODL11Formatter.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/AccessLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BaseTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BufferedLogFileReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BusStopLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/EOFParseException.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/FileSet.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/FileSetLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogContentHandler.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogFileReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogParser.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogReaderConstants.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogRecordImpl.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/MessageFormatFileSet.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/ODLTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/ODLTextLogReaderFactory.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/SAXParserDriver.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/SimpleTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/TextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/UnformattedTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/WebCacheLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/XMLParser\$CharBuf.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/XMLParser.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/oraclelog.dtd --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
Patch Location in Inventory:  
/u01/app/gc/oms10g/inventory/oneoffs/5336126  
Patch Location in Storage area:

/u01/app/gc/oms10g/.patch\_storage/5336126\_Nov\_11\_2008\_12\_48\_26

Patch 4417596 : applied on Mon Dec 21 22:21:22 CET 2009  
Created on 12 Nov 2008, 16:25:04 hrs PST8PDT  
Bugs fixed:  
4417596  
Files Touched:  
mod\_oc4j.so --> ORACLE\_HOME/Apache/Apache/libexec/mod\_oc4j.so  
Patch Location in Inventory:  
/u01/app/gc/oms10g/inventory/oneoffs/4417596  
Patch Location in Storage area:  
/u01/app/gc/oms10g/.patch\_storage/4417596\_Nov\_12\_2008\_16\_25\_04

Patch 5697416 : applied on Mon Dec 21 22:21:08 CET 2009  
Created on 9 Jul 2007, 06:10:08 hrs PST8PDT  
Bugs fixed:  
5697416  
Files Touched:  
uix2.jar --> ORACLE\_HOME/jlib/uix2.jar  
Patch Location in Inventory:  
/u01/app/gc/oms10g/inventory/oneoffs/5697416  
Patch Location in Storage area:  
/u01/app/gc/oms10g/.patch\_storage/5697416\_Jul\_9\_2007\_06\_10\_08

-----  
OPatch succeeded.

## **A.1 Agent Components**

Invoking OPatch 10.2.0.4.5

Oracle Interim Patch Installer version 10.2.0.4.5  
Copyright (c) 2008, Oracle Corporation. All rights reserved.

Oracle Home : /u01/app/agent10g  
Central Inventory : /u01/app/oraInventory  
from : /etc/oraInst.loc  
OPatch version : 10.2.0.4.5  
OUI version : 10.2.0.5.0  
OUI location : /u01/app/agent10g/oui  
Log file location : /u01/app/agent10g/cfgtoollogs/patch/patch2010-03-07\_20-14-46PM.log

Patch history file: /u01/app/agent10g/cfgtoollogs/patch/patch\_history.txt

Lsinventory Output file location : /u01/app/agent10g/cfgtoollogs/patch/lsinv/lsinventory2010-03-07\_20-14-46PM.txt

---

Installed Top-level Products (1):

Oracle Management Agent 10.2.0.5.0  
There are 1 products installed in this Oracle Home.

Installed Products (91):

ADF BC agent for OracleAS GC 10.2.0.3.0  
Agent Required Support Files 10.2.0.1.0  
Agent Required Support Files Patch 10.2.0.4.0  
Agent Virtualization 10.2.0.5.0  
Bali Share 1.1.18.0.0  
Common component for Virtualization 10.2.0.5.0  
DBJAVA Required Support Files 10.2.0.1.0  
DBJAVA Required Support Files Patch 10.2.0.4.0  
Discoverer EM plugin - agent portion 10.2.0.2.0  
Enterprise Manager Agent 10.2.0.5.0  
Enterprise Manager Agent Core Files 10.2.0.5.0  
Enterprise Manager Agent for Grid Control 10.2.0.5.0  
Enterprise Manager Application Server Plugin -- Agent Support 10.2.0.5.0  
Enterprise Manager Application Server Plugin -- Common Support 10.2.0.5.0  
Enterprise Manager BPEL Process Analytics Plugin -- Agent Plugin 10.2.0.2.0  
Enterprise Manager BPEL Process Manager Plugin -- Agent Plugin 10.2.0.2.0  
Enterprise Manager Collaboration Suite Plugin -- Agent Support 10.2.0.5.0  
Enterprise Manager Common Core Files 10.2.0.5.0  
Enterprise Manager Common Files 10.2.0.5.0  
Enterprise Manager Database Plugin -- Agent Support 10.2.0.5.0  
Enterprise Manager Integration B2B Plugin -- Agent Plugin 10.2.0.2.0  
Enterprise Manager Integration InterConnect Plugin -- Agent Plugin 10.2.0.2.0  
Enterprise Manager Siebel Plugin -- Agent Support 10.2.0.5.0  
Forms Services Management Agent Plugin 10.2.0.2.0  
Installation Common Files 10.2.0.1.0  
Installation Common Files Patch 10.2.0.4.0  
Installer SDK Component 10.2.0.5.0  
JDBC Common Files 10.2.0.1.0  
LDAP Required Support Files 10.2.0.1.0  
LDAP Required Support Files Patch 10.2.0.4.0  
Oracle Application Server Repository API 10.1.2.0.2  
Oracle CM SDK and Oracle Files Plugin for Oracle Management Agent 10.2.0.3.0  
Oracle Collaboration Suite Web Access Agent Plugin 10.2.0.2.0  
Oracle Configuration Manager 10.3.1.0.0  
Oracle Content DB Plugin for Oracle Management Agent 10.2.0.3.0  
Oracle Content Services Plugin for Oracle Management Agent 10.2.0.3.0  
Oracle Core Required Support Files 10.2.0.1.0  
Oracle Core Required Support Files Patch 10.2.0.4.0  
Oracle Discussions Plugin for Agent 10.2.0.3.0  
Oracle Dynamic Monitoring Service 10.1.2.1.0  
Oracle Dynamic Monitoring Service Patch 10.1.2.3.0  
Oracle Email components for Enterprise Manager Grid Control Agent 10.2.0.3.0  
Oracle Globalization Support 10.2.0.1.0

Oracle Globalization Support Patch	10.2.0.4.0	
Oracle JDBC Thin Driver for JDK 1.4	10.2.0.1.0	
Oracle JDBC Thin Driver for JDK 1.4 Patch	10.2.0.4.0	
Oracle JDBC/OCI Instant Client	10.2.0.1.0	
Oracle JDBC/OCI Instant Client Patch	10.2.0.4.0	
Oracle Management Agent	10.2.0.5.0	
Oracle Mobile Collaboration Server Plugin for Agent	10.2.0.3.0	
Oracle Net Required Support Files	10.2.0.1.0	
Oracle Net Required Support Files Patch	10.2.0.4.0	
Oracle Notification Service	10.1.2.1.0	
Oracle Notification Service (eONS) - native client library	11.2.0.0.2	
Oracle One-Off Patch Installer	10.2.0.4.2	
Oracle Portal agent	10.2.0.3.0	
Oracle RAC Required Support Files-HAS	10.2.0.1.0	
Oracle RAC Required Support Files-HAS Patch	10.2.0.4.0	
Oracle Recovery Manager	10.2.0.1.0	
Oracle Recovery Manager Patch	10.2.0.4.0	
Oracle SSO Agent	10.2.0.3.0	
Oracle Ultra Search Plugin for Oracle Management Agent	10.2.0.3.0	
Oracle Universal Installer	10.2.0.5.0	
Oracle Voice Mail and Fax Files Plugin for Agent	10.2.0.3.0	
Oracle Workflow Agent for Grid Control	10.2.0.3.0	
Oracle Workspaces Plugin for Agent	10.2.0.3.0	
OracleAS J2EE BULKOPS	11.0.0.0.0	
Parser Generator Required Support Files	10.2.0.1.0	
Perl Interpreter	5.8.3.0.2	
Platform Required Support Files	10.2.0.1.0	
Precompiler Required Support Files	10.2.0.1.0	
Precompiler Required Support Files Patch	10.2.0.4.0	
Provisioning Advisor Framework Common Files For Agent and OMS	10.2.0.5.0	
RDBMS Required Support Files	10.2.0.1.0	
RDBMS Required Support Files for Instant Client	10.2.0.1.0	
RDBMS Required Support Files for Instant Client Patch	10.2.0.4.0	
RDBMS Required Support Files Patch	10.2.0.4.0	
Reports Services EM Plugin - Agent portion	10.2.0.2.0	
Required Support Files	10.2.0.1.0	
Secure Socket Layer	10.2.0.1.0	
Secure Socket Layer Patch	10.2.0.4.0	
SQL*Plus Required Support Files	10.2.0.1.0	
SQL*Plus Required Support Files Patch	10.2.0.4.0	
SSL Required Support Files for InstantClient	10.2.0.1.0	
SSL Required Support Files for InstantClient Patch	10.2.0.4.0	
Sun JDK	1.5.0.17.0	
Wireless EM Agent	10.2.0.3.0	
XDK Required Support Files	10.2.0.1.0	
XDK Required Support Files Patch	10.2.0.4.0	
XML Parser for Java	10.2.0.1.0	
XML Parser for Java Patch	10.2.0.4.0	

There are 91 products installed in this Oracle Home.

Interim patches (4) :



Patch 9019231 : applied on Tue Mar 02 14:33:07 CET 2010  
Unique Patch ID: 12257821  
Created on 3 Mar 2010, 02:50:17 hrs PST8PDT  
Bugs fixed:  
9019231  
Files Touched:  
/nmehlev.o --> ORACLE\_HOME/sysman/lib/libnmehl.a  
ins\_emagent.mk --> ORACLE\_HOME/sysman/lib/libnmemso  
Patch Location in Inventory:  
/u01/app/agent10g/inventory/oneoffs/9019231  
Patch Location in Storage area:  
/u01/app/agent10g/.patch\_storage/9019231\_Mar\_3\_2010\_02\_50\_17

Patch 7568506 : applied on Thu Dec 10 10:03:07 CET 2009  
Created on 3 Dec 2008, 02:06:34 hrs US/Eastern  
Bugs fixed:  
7568506  
Files Touched:  
/oracle/dms/address/Optic.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/dms/collector/Ajp13Connector.class --> ORACLE\_HOME/lib/dms.jar  
Patch Location in Inventory:  
/u01/app/agent10g/inventory/oneoffs/7568506  
Patch Location in Storage area:  
/u01/app/agent10g/.patch\_storage/7568506\_Dec\_3\_2008\_02\_06\_34

Patch 5336126 : applied on Thu Dec 10 10:02:56 CET 2009  
Created on 11 Nov 2008, 12:48:26 hrs US/Pacific  
Bugs fixed:  
5336126  
Files Touched:  
/oracle/core/ojdl/LogMessage\$InstanceId.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage\$MessageArgument.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/MessageType.class --> ORACLE\_HOME/lib/dms.jar  
/oracle/core/ojdl/LogMessage\$InstanceId.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/LogMessage\$MessageArgument.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/LogMessage.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/MessageType.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/ODL11Formatter.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/AccessLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BaseTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BufferedLogFileReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/BusStopLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/EOFParseException.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/FileSet.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/FileSetLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogContentHandler.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogFileReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogParser.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogReaderConstants.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/LogRecordImpl.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/MessageFormatFileSet.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/ODLTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar

/oracle/core/ojdl/reader/ODLTextLogReaderFactory.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/SAXParserDriver.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/SimpleTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/TextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/UnformattedTextLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/WebCacheLogReader.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/XMLParser\$CharBuf.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/XMLParser.class --> ORACLE\_HOME/diagnostics/lib/ojdl.jar  
/oracle/core/ojdl/reader/oraclelog.dtd --> ORACLE\_HOME/diagnostics/lib/ojdl.jar

Patch Location in Inventory:

/u01/app/agent10g/inventory/oneoffs/5336126

Patch Location in Storage area:

/u01/app/agent10g/.patch\_storage/5336126\_Nov\_11\_2008\_12\_48\_26

Patch 6672979 : applied on Thu Dec 10 10:02:45 CET 2009

Created on 21 Apr 2008, 03:10:40 hrs PST8PDT

Bugs fixed:

6672979

Files Touched:

timezone.dat --> ORACLE\_HOME/oracore/zoneinfo/timezone.dat

timezlrq.dat --> ORACLE\_HOME/oracore/zoneinfo/timezlrq.dat

readme.txt --> ORACLE\_HOME/oracore/zoneinfo/readme.txt

Patch Location in Inventory:

/u01/app/agent10g/inventory/oneoffs/6672979

Patch Location in Storage area:

/u01/app/agent10g/.patch\_storage/6672979\_Apr\_21\_2008\_03\_10\_40

-----  
OPatch succeeded.

# B Errata

This section is intended to provide changes to the user guidance documentation that is provided as part of the evaluated Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) TOE.

## B.1 Privileges

The table below provides description of privileges implemented by the TOE, their associated actions and objects, and instructions on how to manage them via the OMS-provided GUI interface.

Privilege	Actions	Objects	Management
OPERATOR_TARGET	All actions related to: <ul style="list-style-type: none"> <li>• BLACKOUT_TARGET</li> <li>• MANAGE_TARGET_METRICS</li> <li>• CONFIGURE_TARGET</li> <li>• MANAGE_TARGET_ALERTS</li> </ul>	Target or Target Group	Setup → Administrators
FULL_TARGET	All management actions on: <ul style="list-style-type: none"> <li>• Privileges</li> <li>• OPERATOR_TARGET Actions</li> </ul>	Target or Target Group	Setup → Administrators
VIEW_TARGET	All read related actions on: <ul style="list-style-type: none"> <li>• Target properties</li> <li>• Inventory</li> <li>• Monitoring information</li> </ul>	Target or Target Group	Setup → Administrators
VIEW_ANY_TARGET	All read related actions on: <ul style="list-style-type: none"> <li>• Target properties</li> <li>• Inventory</li> <li>• Monitoring information</li> </ul>	All targets (implicit)	Setup → Administrators
EM_MONITOR	All read related actions on: <ul style="list-style-type: none"> <li>• Target properties</li> <li>• Inventory</li> </ul> Monitoring information	All Agent Targets and the Repository	Setup → Administrators

Privilege	Actions	Objects	Management
		Target (implicit)	
BLACKOUT_TARGET	Blackout actions: <ul style="list-style-type: none"> <li>• Create blackouts</li> <li>• Edit blackouts</li> <li>• Schedule blackouts</li> <li>• Stop blackouts</li> </ul>	Target or Target Group	Setup → Administrators
MANAGE_TARGET_ALERTS	Alert Management: <ul style="list-style-type: none"> <li>• Clear stateless alerts</li> <li>• Manually re-evaluate alerts</li> <li>• Acknowledge alerts</li> </ul>	Target or Target Group	Setup → Administrators
MANAGE_TARGET_METRICS	Metric Management <ul style="list-style-type: none"> <li>• Edit threshold, metric, or policy settings</li> <li>• Apply monitoring templates</li> <li>• Manage user defined metrics</li> </ul>	Target or Target Group	Setup → Administrators
CONFIGURE_TARGET	Target Configuration: <ul style="list-style-type: none"> <li>• Delete target</li> <li>• Configure target credentials</li> </ul>	Target or Target Group	Setup → Administrators
CREATE_TARGET	Create a target	Target or Target Group (implicit)	Setup → Administrators
CREATE_PROPAGATING_GROUP	Create a propagating group	Propagating Groups (implicit)	Setup → Administrators
GROUP_ADMINISTRATION	Group Administration <ul style="list-style-type: none"> <li>• Add membership</li> <li>• Delete membership</li> <li>• Modify user privileges of targets in group</li> <li>• If group is privilege propagating, then also all actions of FULL_TARGET</li> </ul>	Target Group	Targets → Groups → Select Group → Members
VIEW_JOB	Limited job management: <ul style="list-style-type: none"> <li>• View a job</li> <li>• Create-Like jobs</li> </ul>	Job	Jobs → Create Job → Access
FULL_JOB	Full job management: <ul style="list-style-type: none"> <li>• Submit jobs</li> <li>• Modify jobs</li> </ul>	Job	Jobs → Create Job → Access

Privilege	Actions	Objects	Management
	<ul style="list-style-type: none"> <li>• Create-Like jobs</li> <li>• Delete jobs</li> </ul>		
PUBLISH_REPORT	Publish report	Report	Setup → Administrators
VIEW_REPORT	Read Reports: <ul style="list-style-type: none"> <li>• View report definition</li> <li>• View stored reports</li> <li>• Generate reports</li> <li>• Create-Like</li> </ul>	Reports	Reports → Edit Report → Access
VIEW_TEMPLATE	View Template	Template	Setup → Monitoring Template → Edit Template → Access
FULL_TEMPLATE	Template Management: <ul style="list-style-type: none"> <li>• Apply templates to targets</li> <li>• Modify templates</li> <li>• Delete templates</li> </ul>	Template	Setup → Monitoring Template → Edit Template → Access
SUPER_USER	Security Management: <ul style="list-style-type: none"> <li>• Assignment and revocation of roles</li> <li>• Assignment and revocation of privileges</li> <li>• Modification of OMS host certificate</li> </ul>	All objects (implicit)	Setup → Administrators

## B.2 Return Codes

This section provides return codes for the specified EM CLI functions.

- create\_privilege\_delegation\_setting
  - 0 – Success
  - 223 – The supplied options are syntactically incorrect
- clear\_credential
  - 0 – Success
  - 1 – The specified target type does not exist.
  - 2 – The specified target does not exist.
  - 3 – The specified credential set does not exist.

- 4 – Insufficient privileges.
- 223 - The supplied options are syntactically incorrect
- collect\_metric
  - 0 – success
  - 1 – agent unreachable
  - 2 – metric retrieval failure
  - 3 – target error
  - 4 – target type error
  - 5 – missing metric name
  - 6 – conflicting metric names
  - 7 – insufficient privilege
  - 8 – collection error
- enable\_audit
  - 0 – Success.
  - 223 - The supplied options are syntactically incorrect
  - SQL errors if user is not SUPER\_USER or the repository owner, or SYSMAN
- export\_report
  - 0 – Success
  - 23 – report does not exist
  - 24 – illegal report parameter
  - 25 – illegal system report
  - SQL errors if user is not privileged
- disable\_audit
  - 0 – Success.
  - 223 - The supplied options are syntactically incorrect
  - SQL errors if user is not SUPER\_USER or the repository owner, or SYSMAN
- grant\_privs
  - 0 – Success.
  - 2 – User does not exist
  - 3 – Invalid privilege
  - 4 – Invalid target
  - 5 – Invalid GUID
  - 6 – Invalid group
  - 7 – invalid job
  - 8 – Grant failed
  - 223 - The supplied options are syntactically incorrect
- grant\_roles
  - 0 – Success.
  - 2 – User does not exist.
  - 7 – Role does not exist.
- login
  - 0 – Success.
  - 1 – Cannot establish an OMS connection storage area
  - 2 – Cannot establish an OMS connection

- 3 – Login failed.
- 4 – Invalid License.
- 5 – Already logged in.
- 223 - The supplied options are syntactically incorrect
- logout
  - 0 – Success.
  - 1 – Cannot establish an OMS connection storage area.
  - 2 – Cannot establish an OMS connection.
- revoke\_privs
  - 0 – Success.
  - 2 – User does not exist.
  - 218 – Invalid state
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged to revoke privilege
- revoke\_roles
  - 0 – Success.
  - 2 – User does not exist.
  - 7 – Role does not exist
  - 218 – Invalid state
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged to revoke privilege
- update\_db\_password
  - 0 – Success.
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged
- update\_host\_password
  - 0 – Success.
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged
- update\_audit\_settings
  - 0 – Success.
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged
- update\_target\_password
  - 0 – Successful
  - 223 – The supplied options are syntactically incorrect
  - SQL errors if user is not privileged

### ***B.3 Password guidelines/suggestions***

At a minimum, passwords must be no longer than 30 characters. However, for greater security, follow these additional guidelines:

- Make the password between 10 and 30 characters and numbers.
- Use mixed case letters and special characters in the password. (See Oracle Database Security Guide for more information.)
- Use the database character set for the password's characters, which can include the underscore (\_), dollar (\$), and number sign (#) characters.
- Do not use an actual word for the entire password.



# C

## References

- [CC] *Common Criteria for Information Technology Security Evaluation*, Version 3.1, CCMB-2006-09-001, September 2006.
- [ECGOEL] *Common Criteria EAL4+ Evaluated Configuration Guide for Oracle Enterprise Linux 4 U4 and U5*, August 23, 2007; v1.3, Available from <http://www.oracle.com/technology/deploy/security/seceval/pdf/OEL-CAPP-EAL4-Configuration-Guide-v1.3.pdf>
- [ECGR] *Common Criteria EAL4+ Evaluated Configuration Guide for Red Hat Enterprise Linux 5 on HP Hardware*, May 31, 2007; v2.3. Available from <http://h71028.www7.hp.com/enterprise/downloads/RHEL5-CC-EAL4-HP-Configuration-Guide.pdf>
- [EMADMIN] *Oracle® Enterprise Manager Administration 10g Release 5 (10.2.0.5)*, Oracle Corporation.
- [ICG] *Oracle® Enterprise Manager Grid Control Installation and Configuration Guide 10g Release 5 (10.2.0.5)*, Oracle Corporation.
- [ICGED] *How to Install Grid Control 10.2.0.5.0 on Enterprise Linux Using the Existing Database (11g)*, Oracle Corporation.
- [ODECD] *Evaluated Configuration for Oracle Database 11g Release 1 (11.1.0)*, Oracle Corporation. July 2009.
- [ODICG] *Oracle Database Installation and Configuration Guide, 11g Release 1 (11.1)*, Oracle Corporation.
- [SD] *Oracle Enterprise Manager Grid Control 10g Release 5 Security Deployment*,

[SLES] *Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server on IBM Hardware*. Klaus Weidner, January 17, 2005; v1.20. Available from <http://download.boulder.ibm.com/ibmdl/pub/software/dw/library/os-ltc-security/IBM-SLES-EAL4-Configuration-Guide.pdf>.

[ST] *Oracle Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) Security Target*, Oracle Corporation.