

Oracle® Enterprise Manager

Grid Control Release Notes for AIX 5L Based Systems (64-Bit)

10g Release 5 (10.2.0.5)

E14642-03

November 2009

Oracle Enterprise Manager Grid Control is a management solution that provides a centralized, integrated framework for managing different versions of Oracle products and some third-party products in the enterprise. Grid Control automates day-to-day maintenance requirements such as software installation, patching, upgrading, workload balancing, and security for an enterprise grid.

This Release Notes document is one of the documents that are bundled with the 10.2.0.5 Grid Control Patch Set. The document provides information about the patch set and procedures that help you patch your previous releases of Grid Control and (or) Management Agent - that is, any 10.2.0.x.x installation - and upgrade it to the 10.2.0.5 release.

Note: This document helps you only patch any previous releases of Grid Control and (or) Management Agent, that is any 10.2.0.x.x installation, and upgrade it to the 10.2.0.5 release. If you do not have a previous release, but want to have a 10.2.0.5 environment, then first install the 10.2.0.1 base release, then use this patch set to upgrade it to 10.2.0.5. For information about installing Grid Control, refer to the installation guides available at:

<http://www.oracle.com/technology/documentation/oem.html>

This document contains the following sections:

- [Patch Set Documentation](#)
- [New Features Included In the Patch Set](#)
- [Pre-Upgrade Tasks](#)
- [Installation Procedure](#)
- [Post-Installation Tasks](#)
- [De-Installation Of A Patch Set](#)
- [Known Issues](#)
- [Documentation Accessibility](#)

1 Patch Set Documentation

There are two documents related to this release of Enterprise Manager Grid Control:

- *Oracle Enterprise Manager Grid Control Release Notes, 10g Release 5 (10.2.0.5)* (this document)

This document provides a list of new features included in this patch set, instructions to install or de-install the patch set, and a list of known issues in this release.

- *Oracle Enterprise Manager Grid Control List of Bugs Fixed, 10g Release 5 (10.2.0.5)*

This document provides a list of all generic bugs related to Grid Control that have been fixed in this release.

Both of these documents are available on Oracle Technology Network (OTN) and My Oracle Support (formerly MetaLink).

To find these documents on OTN, access the following URL. From the table, click View Library. On the Enterprise Manager documentation library page, click the Documentation tab, and from the Release Notes section, access the documents.

<http://www.oracle.com/technology/documentation/oem.html>

To find these documents on My Oracle Support, access the following URL.

<http://metalink.oracle.com>

From the top-left corner of the main page, click Knowledge. From the Browser Knowledge list, select Enterprise Manager Grid Control, and in Search Knowledge, specify the note numbers that relate to these documents, and click Search. Use Note 803053.1 for the Release Notes and Note 807697.1 for the List of Bugs Fixed document.

You can also find this document on the Oracle Technology Network (OTN) Web site:

<http://www.oracle.com/technology/index.html>

2 New Features Included In the Patch Set

Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) contains a significant number of new features and enhancements. See the "New in Enterprise Manager Grid Control 10g Release 5" section in the *Enterprise Manager Concepts* book for a detailed overview of what's new in this latest release.

To find this document on OTN, access the following URL:

http://download.oracle.com/docs/cd/B16240_01/doc/nav/portal_booklist.html

You will find links to Adobe PDF and HTML versions of *Enterprise Manager Concepts* in the "Getting Started" section of the Web page.

3 Pre-Upgrade Tasks

This section describes the tasks to be performed before beginning the upgrade.

Warning: There is no mechanism provided for de-installing patch sets. If you are concerned about being able to de-install a patch set, Oracle recommends that you back up your software installation before applying the patch set. See [Section 6, "De-Installation Of A Patch Set"](#) for more information.

3.1 Steps To Complete Before Upgrading

Complete the following checks before upgrading to Oracle Enterprise Manager Grid Control version 10.2.0.5.0.

1. Oracle recommends that you back up the ORACLE_HOME that will be upgraded using this Patch Set.

In the case of a Management Repository, Oracle recommends that you back up the repository database before applying the Patch set because the Patch Set makes changes to the repository that cannot be rolled back. You should also back up the Oracle Inventory directory.

2. Make sure that you meet the product pre-requisites (operating system patches, packages etc.) for 10.2.0.5.0 patch set.

For information about platform-specific package and kernel requirements, refer to the *Enterprise Manager Grid Control Installation and Basic Configuration Guide* available at the following URL:

<http://www.oracle.com/technology/documentation/oem.html>

The above URL takes you to the Enterprise Manager documentation library page, and from the table, click **View Library**. On the following page, click the *Documentation* tab, and then click the name of the document you want to access.

3.1.1 Oracle Management Service (OMS) Pre-Upgrade Tasks

Complete the following before upgrading your Oracle Management Service (OMS) instances.

Note: All patches that apply to OMS should have ORACLE_HOME set to <OMS_HOME>.

1. Ensure that the shared pool size is set in your Grid Control repository database as per your infrastructure. Minimum size for the shared pool is 512 MB. For information about the fixed initialization parameter values, refer to the pre-installation requirements described in the *Enterprise Manager Grid Control Installation and Basic Configuration Guide* available at:

<http://www.oracle.com/technology/documentation/oem.html>

The above URL takes you to the Enterprise Manager documentation library page. From the table, click **View Library**. On the following page, click the *Documentation* tab, then click the name of the document you want to access.

2. If the secure key was exported from the repository, it must be put back into the repository before beginning the upgrade. To check if the key is outside of the repository, use this command:

```
$ <OMS_HOME>/bin/emctl status emkey
```

If the output reports the following, the key has been exported from the repository, and must be re-imported:

"The EM Key is configured properly"

Import the key using this command:

```
$ <OMS_HOME>/bin/emctl config emkey -copy_to_repos
```

After the upgrade has completed, see [Section 5.2, "Oracle Management Service Post-Installation Tasks"](#) later in this document to re-export the key.

3. The script *preinstall.pl*, which can be found in the top-level directory of the extracted patch set, must be run as *Perl preinstall.pl <OMS_HOME>* before upgrading if the one-off patch #7214697 was applied in the OMS_HOME before the upgrade.

If the one-off patch was not applied, running the script is not required.

Note: If you do not find the generic script *preinstall.pl* after extracting the software, you can download it from either OTN or My Oracle Support Note 464674.1.

Note: Refer to upgrade checklist Note 464674.1 on My Oracle Support. This note is updated frequently with the latest checklist information.

3.1.2 Grid Control Repository Pre-Upgrade Tasks

Complete the following before upgrading the Grid Control Repository database.

Note: All OMS patches that must connect to the Grid Control repository (SYSMAN schema) should invoke database connections from *<OMS_HOME>/bin/sqlplus*.

1. Verify that the Partitioning Option is enabled in the database housing the Grid Control Repository (SYSMAN schema).

Connect to the database as SYSDBA and run the following query to see if the Partitioning Option is installed:

```
SQL> CONNECT / AS SYSDBA;
SQL> SELECT value
FROM v$option
WHERE parameter = 'Partitioning';
```

The return value should be TRUE.

Note: No additional partitioning license is required for the database housing the Grid Control Repository, as it is a basic Grid Control requirement.

2. Note that the minimal version of EMDIAG to use is 2009.0706 for 10.2.0.5. If an older version is currently installed, upgrade to 2009.0706 (or higher). For more information on EMDIAG, and how to download and upgrade it, see the following Note on My Oracle Support:

421053.1: EMDiagkit Download and Master Index

3. The SYSMAN schema objects should be in a VALID status. To verify the objects' status, log on to the repository database as the SYSMAN user and execute the following:

```
SQL> CONNECT SYSMAN;
SQL> SELECT object_name, object_type
FROM user_objects
WHERE status != 'VALID';
```

If invalid objects are found in the SYSMAN schema, recompile them using the *admin_recompile_invalid.sql* script as shown below. The script is available in the <OMS_HOME>/sysman/admin/emdrep/sql/core/latest/admin directory on the OMS host.

```
SQL> @admin_recompile_invalid.sql SYSMAN
```

To verify that all objects in the SYSMAN schema are in the VALID state after running the script, execute the query again.

4. Ensure that the DBMS PL/SQL packages (owned by SYS) are in a VALID state:

```
SQL> SELECT object_name, object_type
FROM all_objects
WHERE status != 'VALID'
AND object_name LIKE 'DBMS%';
```

Any packages marked as INVALID will need to be recompiled again using the following commands:

- If the package itself is invalid:

```
SQL> ALTER PACKAGE <name> COMPILE;
```

- If the package body is invalid:

```
SQL> ALTER PACKAGE <name> COMPILE BODY;
```

5. If the repository database is configured with the UTF8 character set, the value of the NLS_LENGTH_SEMANTICS needs to be set to BYTE. To verify this in the database:

```
SQL> SELECT value
FROM nls_database_parameters
WHERE parameter='NLS_LENGTH_SEMANTICS';
```

If the value is not set to BYTE, change it by running this command:

```
SQL> ALTER SYSTEM SET NLS_LENGTH_SEMANTICS=BYTE SCOPE=both;
```

6. Both the SYSMAN and DBSNMP users require access to the DBMS_RANDOM package in the database. If EXECUTE privileges have not been granted to this package to both users, it will have to be granted before running the upgrade.

To check for the privilege in the database for SYSMAN, connect to the database as SYS and execute the following (note that you must do the same for the DBSNMP user):

```
SQL> CONNECT AS SYS;
SQL> SELECT grantee, grantor, owner, table_name
FROM DBA_TAB_PRIVS
WHERE table_name = 'DBMS_RANDOM'
AND privilege = 'EXECUTE'
AND grantee IN
(
SELECT DISTINCT granted_role
FROM DBA_ROLE_PRIVS
START WITH grantee = 'SYSMAN'
CONNECT BY PRIOR granted_role=grantee
UNION ALL
SELECT 'SYSMAN'
FROM dual
WHERE ROWNUM = 1
UNION ALL
SELECT 'PUBLIC'
FROM dual
WHERE ROWNUM = 1
);
```

If the EXECUTE privilege was not granted to the SYSMAN user, grant it using this command:

```
SQL> GRANT EXECUTE ON DBMS_RANDOM TO sysman;
```

Repeat each of these steps for the DBSNMP user.

7. Data Guard only:

If Data Guard is being used, you must upgrade the repository on the primary Data Guard database, and not on a standby database. The upgrade changes will then be propagated to all standby databases.

Use the following query to determine if the database you intend to upgrade is the primary database:

```
SQL> CONNECT / AS SYSDBA;
SQL> SELECT count(*)
FROM v$archive_dest
WHERE target='STANDBY'
AND register='YES';
```

If the query result is >0, the database is a Data Guard primary database.

Next, ensure that the primary database is in FORCE LOGGING mode before beginning the upgrade. This will force all index maintenance commands to be propagated to all standby databases.

Use the following query to check whether FORCE LOGGING is enabled:

```
SQL> SELECT FORCE_LOGGING FROM v$database;
```

If the query returns with YES, force logging is enabled. If not, force the database into logging mode as follows:

```
SQL> ALTER DATABASE FORCE LOGGING;
```

8. All database jobs, including DBMS_JOBS and DBMS_SCHEDULER jobs, must be stopped prior to the upgrade. Connect to the database as SYSMAN and execute the following to stop all DBMS_JOBS:

```
SQL> CONNECT SYSMAN;
SQL> EXECUTE emd_maintenance.remove_em_dbms_jobs;
SQL> COMMIT;
```

Next, stop all DBMS_SCHEDULER jobs. Before doing so however, note the current value of the *job_queue_processes* parameter for each of the database instances hosting the repository to reinstate the values after the upgrade. Use the following query to get this value:

```
SQL> SELECT a.instance_name AS sid, b.value AS jobqueue
FROM gv$instance a, gv$parameter b
WHERE a.inst_id = b.inst_id
AND b.name='job_queue_processes';
```

When you have all current parameter values, stop the jobs with the following. Note that you will set the value for *job_queue_processes* to "0":

```
SQL> ALTER SYSTEM SET job_queue_processes=0 SID='*';
SQL> EXECUTE dbms_scheduler.set_scheduler_attribute('SCHEDULER_
DISABLED', 'TRUE');
```

9. If the site was upgraded from 10.2.0.4, the DBMS_JOB called MGMT_CNTR_TT.clean_up_old_ticket_recs must be removed:

```
SQL> CONNECT SYSMAN;
SQL> SELECT job
FROM user_jobs
WHERE what = 'MGMT_CNTR_TT.clean_up_old_ticket_recs';
SQL> EXECUTE dbms_job.remove(<the job id>);
SQL> COMMIT;
```

10. If the version of the repository database is either 9i or 10gR1, and the *session_cached_cursors* parameter is specified at the database level, the following error might be reported while loading data into the repository:

ORA-01801: date format is too long for internal buffer

To resolve this issue, use either of these two procedures:

- Set the *session_cached_cursors* parameter to zero in either *init.ora* or *spfile.ora*, then bounce the database. This parameter cannot be changed dynamically.
- Apply the following patch to the database:

3944226 - APPSST: ORA-01801: DATE FORMAT IS TOO LONG FOR
INTERNAL BUFFER

3.2 Apply Critical Patches Before Upgrading

Oracle strongly recommends that all critical patches be applied before upgrading to the latest release. A list of the latest critical patches is available in the following My Oracle Support Note:

https://metalink2.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=853691.1

Note: All patches that apply to OMS should have ORACLE_HOME set to <OMS_HOME>.

3.3 Notes On Solaris 10.2.0.1.0 And Decunix 10.2.0.2 Management Agents

The Solaris 10.2.0.1 and Decunix 10.2.0.2 Management Agents should not be deployed. Instead, deploy agents with minimum version of 10.2.0.2 for Solaris and 10.2.0.5 for Decunix by downloading the complete agent bits from Oracle Technology Network. Visit the following link for instructions on downloading and installing the full agent:

http://www.oracle.com/technology/software/products/oem/htdocs/agentdownload_script_readme.pdf

Also see My Oracle Support (formerly MetaLink) Note 784629.1 for additional details.

4 Installation Procedure

This section describes the installation procedure.

4.1 Extracting The Software

For upgrading to Enterprise Manager Grid Control 10.2.0.x.x to 10.2.0.5, you must manually download and extract the 10.2.0.5 Patch Set.

You can download the 10.2.0.5 Patch Set from Oracle Technology Network (OTN) at:

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

Note: Mass Agent patching is an exception. For Mass Agent patching, refer to [Section 4.4.2, "Upgrading Management Agent \(Standalone or Cluster\) - Multiple Hosts At A Time"](#).

Note: Verify that the file size of your downloaded patch set software matches the file size displayed on Oracle Technology Network (OTN). After downloading the software, run the cksum command against the downloaded file to ensure that the file size of the downloaded software is the same as the file size on OTN. For information about verifying the platform and file size, refer to the verifying downloaded software steps described in the *Enterprise Manager Grid Control Installation and Basic Configuration Guide*.

To download and extract the Patch Set:

1. Download the p3731593_102050_<platform name>.zip patch set installation archive to any directory that may or may not be an Oracle Home directory.
2. Enter the following command to unzip and extract the installation files:

```
$ unzip p3731593_102050_<platform name>.zip
```

This extracts the files to the "3731593" directory.

Important: The same Patch Set can be used for upgrading Oracle Management Service, Grid Control Repository (sysman schema), and Management Agent. The procedures are described in the following sections.

4.2 Upgrading Oracle Management Service

The pre-installation tasks can be broadly categorized based on the following types of upgrade that you can perform:

- Upgrading First Oracle Management Service and repository
- Upgrading Additional Oracle Management Services
- Upgrading Management Agent

4.2.1 Upgrading The Oracle Management Service And Repository

To upgrade multiple Oracle Management Services (OMS), shut down all the OMS's, apply the 10.2.0.5 patch set to any one of the OMSs so that the associated Management Repository (sysman schema) is also upgraded, then apply the patch set to the rest of the Oracle Management Services.

Note: This Patch set will upgrade only the Grid Control repository (sysman schema) and not the database, which contains the Grid Control repository.

Be sure that you first upgrade the Oracle Management Service (OMS), and then the Management Agent before upgrading the database that contains the Grid Control repository.

The steps to be taken before upgrading the first OMS are:

- While applying the OMS patch set, leave the repository database and listener instance running.
- Make sure that you follow all the pre-installation tasks as mentioned in the above Section 3.1 before going ahead with upgrade process.
- **Shut down all OMS instances attached to the Grid Control repository, from the respective Oracle homes in their respective hosts. Also stop the Application Server components that run in each Oracle home directory of the Oracle Management Service (OMS).**

Note: If you have multiple Oracle Management Services then you must stop all the OMS instances. When you upgrade the first OMS, the Patch Set also upgrades the Grid Control repository, and since the other OMS instances connect to the same Grid Control repository, they must also be stopped.

Stopping the Management Agents is not mandatory, and as a result, there may be an increase in the number of Agent-related log files. However, this is harmless and can be ignored.

To stop all the Grid Control components on a host, follow these steps:

1. Stop the Oracle Management Service (OMS) by running the following command from the Oracle home directory of the OMS, where `$ORACLE_HOME` is the Oracle home directory of the Oracle Management Service:

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

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

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

3. Stop all the application server components, such as Oracle HTTP Server and OracleAS Web Cache by running the following command from the Oracle home directory of the OMS.

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

4. Wait for four to five minutes to ensure that all the OPMN processes are stopped and TCP ports are released.
5. Set the Oracle_Home to your Oracle home directory of the Oracle Management Services before applying the patch set.

- Apply the 10.2.0.5 Patch Set either interactively by executing the runInstaller or silently by using the response file.

After you have upgraded the first OMS and the Grid Control repository (sysman schema) to version 10.2.0.5, the first OMS starts up automatically and you must then patch the unpatched OMS's to version 10.2.0.5.

Warning: Do not start an OMS that has not been patched to version 10.2.0.5.

For example, assume there are four version 10.2.0.2 Oracle Management Services labeled OMS A, B, C, and D. In the previous section, all four OMS's are down and you decide to patch OMS B first. After you patch OMS B to version 10.2.0.5, the Enterprise Manager Repository is also patched and OMS B is now up and running. However OMS A, C, and D remain down.

You can then patch OMS A, C, and D in parallel or in serial to version 10.2.0.5 but you must not bring up the unpatched version of those OMS's at any time prior to patching them to version 10.2.0.5.

4.2.2 Oracle Management Service Upgrade Flow

The following sections describe the upgrade flow for the OMS.

4.2.2.1 Interview Phase

This phase consists of the following four steps:

1. Oracle Configuration Manager Installation (OCM)

In this step, the installer collects information to install Oracle Configuration Manager (OCM) into the existing ORACLE_HOME location. Email address is mandatory for OCM to get configured.

On this screen, provide an email address to be used in configuring the Configuration Manager software. Preferably, this address should be a My Oracle Support (formerly MetaLink) user name; if it is, and the corresponding My Oracle Support password is entered, you will be able to access detailed configuration management features and security updates through the My Oracle Support (formerly MetaLink) dashboard. If no email address is provided, you will need to confirm that you do not wish to be informed of security issues that can be identified by OCM.

The installation process will automatically determine if a connection to Oracle can be created, or if proxy server information is required to make the connection to Oracle.

If you have not chosen to configure OCM during the interview phase then follow the steps below after the OMS upgrade is successful to manually configure the OCM.

a. Execute one of the following commands according to your choice:

Typical configuration:

```
$ORACLE_HOME/ccr/bin/setupCCR
```

If you want to configure while specifying a particular Customer Support Identifier (CSI), for My Oracle Support user accounts containing more than one CSI:

```
$ORACLE_HOME/ccr/bin/setupCCR <CSI>  
[<MyOracleSupportUserName>] [<Country-Code>]
```

For more information about using setupCCR, use the setupCCR -help command.

b. Provide the requested information when prompted.

c. Setup then installs and configures OCM.

d. When setup is complete, OCM gathers configuration information for ORACLE_HOME, and uploads this information to Oracle for use while supporting your site.

e. If you want to check the status of OCM, run the following command:

```
$ORACLE_HOME/ccr/bin/emCCR status
```

2. Product specific pre-requisite checks

The OUI performs the product specify check for example Packages, Operating system certification, and so on, on the host where the Oracle Management Service resides.

3. Enter your SYS password of the Database in which the Grid Control Repository resides

In this step, OUI picks up the repository connection details from the configuration files and then prompts for the SYS password of the repository database.

4. Enter your Application server instance password

The `ias_admin` user is the administrative user for Oracle Application Server instances. The password that you specify here is required to access the application server and to deploy the new features.

This password is same as the SYSMAN password that you specified when you first installed the Grid Control in your environment.

Note: After installing the Grid Control in your environment, if you change the SYSMAN password, `ias_admin` password will not be changed.

To change the `ias_admin` password, go to the Oracle home directory of Oracle Management Service and run the following command:

```
$ORACLE_HOME/bin/emctl set password <Old ias_admin password> <New ias_admin Password>
```

Note: If you don't remember the old `ias_admin` password, follow the instructions from Document ID 280587.1 on My Oracle Support (formerly MetaLink) at <http://metalink.oracle.com>.

4.2.2.2 Copy And Relink Phase

In this phase, the installer copies all necessary files and performs relink operations. It also prompts you to run `root.sh` as a root user.

Note: After the `root.sh` script runs successfully (as a root user), you return to the command prompt without any confirmation message. This is an expected behavior of the script in Enterprise Manager 10g Grid Control Release 5 (10.2.0.5).

4.2.2.3 Configuration Phase

In this phase, the installer does the following:

1. **OMS Oneoff Patch Application:** This assistant applies the Oracle Management Service related one-off patches
2. **Updates the Repository:** This assistant upgrades the Grid Control repository (sysman schema) to 10.2.0. release. If the repository has already been upgraded to 10.2.0.5 release and this is an additional OMS being patched, then the configuration phase does not update the Grid Control repository

Note: If the Repository Upgrade Assistant fails during the 10.2.0.5 OMS patch set install, then do not click *Retry*.

1. If the following error message is present in the log, then the repository upgrade is going on from another OMS patch set install:

STATUS - 2 : Repository Upgrade is already running from another OMS install. Wait until upgrade finishes.

Execute the below SQL query to find the Repository Upgrade status.

```
select status from sysman.mgmt_versions where  
component_name='_UPGRADE_';
```

Wait until the status shows '4' which indicates that the upgrade is complete without any errors. Then click *Retry* to continue with Install.

2. If the following error message is present in the log, then the repository upgrade has failed:

*SEVERE: oracle.sysman.top.oms:Repository Upgrade is failed with errors.
Rectify the errors and retry the install.*

For additional details on configuration issues, you may refer to these log files available in the following location, where \$ORACLE_HOME is the Oracle home directory of the OMS:

`$ORACLE_HOME/cfgtoollogs/cfgfw`

For additional details on repository failures, you may refer to the log files available in the following location, where \$ORACLE_HOME is the Oracle home directory of the OMS:

`$ORACLE_HOME/sysman/log/emrepmgr.log.10.2.0.5.0`

`$ORACLE_HOME/sysman/log/emrepmgr.log.10.2.0.5.0.errors`

If you cannot identify the repository issues, contact Oracle Support. If the errors from the schema upgrade were analyzed and rectified, then the following can be executed to allow the installer to continue upon *Retry*:

1. Log in to the database as SYSMAN
2. Execute `emd_maintenance.set_comp_status(' _UPGRADE_', EMD_MAINTENANCE.G_STATUS_CONFIGURED_READY);`
3. Exit SQLplus
4. Click *Retry* on the installer. The installer should continue. Alternately, you can exit the Installer and execute the *runConfig* command to run the failed configuration tools.

Go to the `<OMS_ORACLE_HOME>/oui/bin` directory and run the command below:

```
For UNIX: ./runConfig.sh ORACLE_HOME=<OMS_  
ORACLE_HOME> ACTION=patchsetConfigure  
MODE=perform COMPONENT_  
XML={oracle.sysman.top.oms.10_2_0_5_0.xml}  
RERUN=true
```

```
For Windows: runConfig.bat ORACLE_HOME=<OMS_  
ORACLE_HOME> ACTION=patchsetConfigure  
MODE=perform COMPONENT_  
XML={oracle.sysman.top.oms.10_2_0_5_0.xml}  
RERUN=true
```

3. **Performs OMS Patch Configuration** -- This configuration assistant redeploys the Enterprise Manager Application and starts the Oracle Management Service
4. **Performs Enterprise Manager Command Line Interface (EMCLI)**
Configuration: This step will setup EMCLI in secure mode on the Oracle Management Service machine with sysman credentials.

If Enterprise Manager is registered with a Single Sign-On Server, then this step will fail to setup EMCLI. In this case, setup EMCLI after the upgrade with the following command after setting ORACLE_HOME environment variable to the OMS home:

```
<ORACLE_HOME>/bin/emcli setup -ssouser=<SSOUsername>  
-url=<Grid Control URL> -licans=yes -trustall  
-dir=<ORACLE_HOME>/sysman/emcli/setup -noautologin  
-nocertvalidate
```

In case Enterprise Manager is NOT registered with a Single Sign-On Server and if this assistant fails, then setup EMCLI after the upgrade as follows.

Set the ORACLE_HOME environment variable to the OMS home and then run the following command:

```
<ORACLE_HOME>/bin/emcli setup -user=sysman -url=<Grid  
Control URL> -licans=yes -trustall -dir=<ORACLE_  
HOME>/sysman/emcli/setup -noautologin -nocertvalidate
```

For example:

```
/scratch/OracleHomes/sonly/oms10g/bin/emcli setup  
-user=sysman -url=https://abc.us.oracle.com:443  
-licans=yes -trustall  
-dir=/scratch/OracleHomes/sonly/oms10g/sysman/emcli/setup  
-noautologin -nocertvalidate
```

If EMCLI is already configured at <OMS_HOME>/sysman/emcli/setup, this step will skip the configuration.

After the upgrade process is successfully completed, you can run the EMCLI verbs from the Oracle home directory of the OMS (\$ORACLE_HOME/bin/emcli).

5. **Configures Oracle Configuration Manager:** This step configures OCM if you have provided the required email address or My Oracle Support (formerly MetaLink) credentials. As part of the configuration, the necessary directories are created and files are instantiated in order to configure CCR. If there are problems during this configuration operation, then the configuration will not be performed. To configure OCM at a later time, you can invoke \$ORACLE_HOME/ccr/bin/setupCCR after the installation process has completed.

4.3 Installing An Additional OMS After Upgrade

You cannot perform an additional 10.2.0.1 OMS install using the 10.2.0.5 OMS repository. You can however install additional 10.2.0.1 OMS with the following workaround if the repository is already upgraded to 10.2.0.5. To do this, complete the following steps:

1. Convert the repository version to 10.2.0.1 from 10.2.0.5 by using the following SQL statement:

```
UPDATE sysman.mgmt_versions SET version = '10.2.0.1.0'
where component_name='CORE'; commit;
```

2. Invoke the Installer from the 10.2.0.1 DVD and choose the Additional Management Service option.
3. Provide the repository credentials for the Specify Database Configuration Screen and click Next, then stop here. (Do not proceed with the install.)
4. Update the repository version to 10.2.0.5 by using the following SQL statement:

```
UPDATE sysman.mgmt_versions SET version = '10.2.0.5.0'
where component_name='CORE'; commit;
```

5. Click **Next** to proceed with the installation from where it was previously stopped.
6. Once the base install has completed, both the Agent and the OMS must be shut down immediately by executing the commands below:

Run the command from the Oracle home directory of Management Agent:

```
$ORACLE_HOME/bin/emctl stop agent
```

Run the command from the Oracle home directory of Oracle Management Service (OMS):

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

7. Patch the OMS to 10.2.0.5 using the 10.2.0.5 Patch Set. Refer to Pre-installation Tasks Specific to the Upgrade Type in this document for more information on how to patch the OMS to version 10.2.0.5.
8. Once the OMS has been patched to 10.2.0.5 successfully, it will start automatically.
9. From the Oracle home directory of Management Agent, restart the Management Agent:

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

4.4 Upgrading Management Agent

The Management Agent can be upgraded in two ways - either one host at a time using Oracle Universal Installer, or many hosts at a time using Patch Wizard from Grid Control.

4.4.1 Upgrading Management Agent - One Host At A Time

To upgrade Management Agents, one host at a time, using OUI, follow these steps:

1. Login to the specific host where the Management Agent is running.
2. Change directory to the Oracle home directory for the Management Agent and stop the Management Agent. For cluster Agent, stop the Agent on all cluster nodes.

```
$ORACLE_HOME/bin/emctl stop agent
```

3. Ensure that `$ORACLE_HOME` is set to the Oracle home directory of the Management Agent that is intended for patching.
4. Extract the software as per section 4.1 and then run the `./runInstaller` executable from the 3731593/Disk1 subdirectory or the 3822442/Disk1 directory and proceed with the upgrade.

Note: If you forget to shut down the Management Agent before invoking the `runInstaller`, follow the steps below on Unix platform:

1. Go to the Oracle home directory of the Management Agent `<ORACLE_HOME>`
2. Move `jdk<timestamp>` to `<AGENT_HOME>/jdk`
For example on a Unix platform: `mv jdk2009-01-23_04-51-03-AM/jdk`
3. Change directory to the Oracle home directory for the Management Agent and stop the Management Agent.
`$ORACLE_HOME/bin/emctl stop agent`
4. Again go to the Oracle home directory of the Management Agent `<ORACLE_HOME>/jdk`
5. Move `jdk` to `jdk<timestamp>`
6. Go to the OUI screen and click the **Retry** button to continue with the Management Agent upgrade. Then OUI proceeds with the copying of files and subsequent relinking operation.

Once the Management Agent upgrade is done successfully, remove the `jdk<timestamp>` from the Oracle home directory of the Management Agent.

The OUI proceeds with the copying of files and subsequent relinking operation. It also prompts you to run `root.sh` as a root user.

4.4.2 Upgrading Management Agent (Standalone or Cluster) - Multiple Hosts At A Time

To upgrade Management Agents, multiple hosts at a time using Patch Wizard from Grid Control, use either of the following two methods:

- Method 1 - By Distributing the Full Patch Set to a Number of Hosts
- Method 2 - By Staging the Patch Set and Distributing Scripts to a Number of Hosts

You can choose one of the methods for mass patching of Management Agents. Method 1 is based on a "push" technique in which the entire set of patch binaries is transferred to all the targets. Method 2 is based on a "pull" technique in which only a script is transferred to the targets and the patch is then installed over HTTP.

However for Method 1, you can choose to pre-stage the patch set binary in a mounted location accessible from all the Agent hosts that need to be upgraded. This will avoid network traffic of copying the patch set binary on all the hosts. Since there is no requirement to transfer the entire set of patch binaries in Method 2, it is the recommended method for large number of targets, whereas Method 1 is more suitable for a limited number of targets.

On Microsoft Windows, note that for Method 2, the *wget* executable needs to be installed on the target machines and present in the PATH environment variable.

■ **Method 1 - By Distributing the Full Patch Set to a Number of Nodes**

If pre-staging is not selected, this method copies the patch to the Oracle home directory of the Management Agent of the selected targets and runs a script to apply the patch. The script creates blackouts, shuts down the Management Agent before applying the Patch Set, applies the Patch Set, clears the blackouts after applying the Patch Set, and then restarts the Management Agent. It is advisable to choose a reasonable number of nodes so that the network is not overloaded.

1. Login to Enterprise Manager Grid Control using SYSMAN credentials. Click Targets and check if the Agent target to be upgraded is up and running.
2. If you have already upgraded the OMS to version 10.2.0.5, click the **Deployments** tab, then click the **Patch Agent** link. (For versions of OMS 10.2.0.3 or earlier, click **Deployments**, then **Patch Oracle Software**.) Provide the patch number 3822442 and select the correct platform and the 10.2.0.5 release. If you do not see the patch set for the 10.2.0.5 release, do the following:
 - Click **Setup** from the top-right corner of the Grid Control console. Then select **Patching Setup** from the panel to the left. Provide the My Oracle Support (formerly MetaLink) credentials and click **Apply**.
 - This will schedule the job "Refresh From My Oracle Support". Once this job runs successfully, it will ensure that the latest information about releases is downloaded from My Oracle Support.
3. You can then select a number of targets to apply the patch against. After selecting the target, select the **Use default patching script** or **Provide custom script** option.
4. On the Oracle Configuration Manager (OCM) screen, provide an email address to be used in configuring the configuration manager software. Preferably, this address should be a My Oracle Support user name; if it is, and the corresponding My Oracle Support password is entered, you will be able to access detailed configuration management features and security updates through the My Oracle Support dashboard. If no email address is provided, you will need to confirm that you do not wish to be informed of security issues that can be identified by OCM.
5. You must execute the *root.sh* script as root for agents on any flavor of Unix platform. For running *root.sh* from the Patch Wizard, you must select the *Custom Post Command/Script*, select *Run Privilege sudo*, use *Run As value* as root and provide *Custom Post Command/Script* value as *%emdroot%/root.sh*. If Sudo is not installed on the target box then this step will not work. In this case *root.sh* will not run and you must manually run the *root.sh* on all the targets from the Oracle home directory of the Management Agent.

For 10.2.0.4 Agents, if you have configured PowerBroker for the PDP settings and have configured the patching user to allow running commands as root, you can execute the Custom Post Command/Script with PowerBroker privilege delegation. For this, you select **Run**

Privilege PAM, use *Run As* value as root, provide a Profile if needed and provide Custom Post Command/Script value as `%emdroot%/root.sh`.

■ **Method 2 - By Staging the Patch Set and Distributing Scripts to a Number of Nodes**

This method copies the script to the selected number of hosts and runs a script to apply the Patch Set from the above staged location. It is advisable to choose a reasonable number of nodes so that the network is not overloaded.

Note: For Microsoft Windows target machines, patching through this method requires `wget.exe` to be in the PATH environment variable and to be present in Oracle home directory of Management Agent (`ORACLE_HOME/bin`). If `wget.exe` is not in the PATH of the target machine, add it to the PATH and make sure it is present in the Oracle home directory of the Management Agent (`ORACLE_HOME/bin`). Bounce the Management Agent by executing the following:

```
$ORACLE_HOME/bin/emctl stop agent
$ORACLE_HOME/bin/emctl start agent
```

Perform the following steps on the OMS host:

1. Navigate to the following location where `<ORACLE_HOME>` is the Oracle home directory of the Oracle Management Service (OMS):

```
cd <ORACLE_HOME>/sysman/agent_download/
```

2. Create a directory:

```
mkdir -p patchset/10.2.0.5.0/<platform name>
```

3. You can then stage the Patch Set by either copying from a DVD or by extracting the contents of the My Oracle Support (formerly MetaLink) patch 3731593.
4. Copy the `p3731593_102050_<platform name>.zip` from the DVD or My Oracle Support patch to an empty, temporary directory.
5. Extract the contents of the ZIP file to that same temporary directory.
6. Now navigate to the `3731593/Disk1` directory or the `3822442/Disk1` directory and copy its contents to the newly created directory in step (2):

To navigate:

```
cd 3731593/Disk1
```

To copy the contents to the newly created directory in step (2):

```
cp -r * <ORACLE_HOME>/sysman/agent_
download/patchset/10.2.0.5.0/<platform name>
```

Here, `$ORACLE_HOME` is the Oracle home directory of the Oracle Management System (OMS) and "platform name" is one of the following:

Table 1 *Descriptions of Platform Names*

Platform Name	Description
linux	Linux
x86_64	Linux X86_64
ppc64	Linux on power PC
linux390	z/Linux
ia64linux	IA64 Linux
solaris	Solaris 64 bit
solarisx86	Solaris-x86
hpux	HP-UX
decunix	HP Tru64 UNIX
hpunix	HP 64 bit
hpi	HP-UX-Itanium
aix	AIX5L
macosx	MACOSX
vms	VMS
windows_ia64	Microsoft Windows (64-bit IA)
windows_x64	Microsoft Windows (64-bit AMD64)
win32	Microsoft Windows 32 bit

The above-mentioned operation stages the contents of the Patch Set in the OMS host.

Note: For an environment with multiple OMS servers, repeat steps 1 through 6 for each OMS server.

7. After this happens, follow these steps:

- (a) Login to Enterprise Manager Grid Control using SYSMAN credentials. Click **Targets** and check to see that the Agent targets to be upgraded are up and running on the host.
- (b) If you have already upgraded the OMS to version 10.2.0.5, click the Deployments tab, then click the Patch Agent link. (For versions of OMS 10.2.0.3 or earlier, click Deployments, then Patch Oracle Software.) Provide the patch number 3731596 and select the correct platform and the 10.2.0.5 release. If you do not see the patch set for 10.2.0.5 release, do the following:
 - Click **Setup** from the top-right corner of the Grid Control console, then select **Patching Setup** from the panel to the left. Provide the My Oracle Support (formerly MetaLink) credentials and click **Apply**.
 - This will schedule the job "Refresh From My Oracle Support". Once this job runs successfully, it will ensure that the latest information about releases is downloaded from My Oracle Support.

(c) You can then select a number of targets to apply the patch. After selecting the target, select the **Use default patching script** or **Provide custom script** option.

(d) On the Oracle Configuration Manager (OCM) screen, provide an email address to be used in configuring the configuration manager software. Preferably, this address should be a My Oracle Support (formerly MetaLink) user name; if it is, then if the corresponding My Oracle Support password is entered, you will be able to access detailed configuration management features and security updates through the My Oracle Support dashboard. If no email address is provided, you will need to confirm that you do not wish to be informed of security issues that can be identified by OCM.

(e) You must execute the *root.sh* script as root for agents on any flavor of Unix platform. For running *root.sh* from the Patch Wizard, you must select the *Custom Post Command/Script*, select *Run Privilege sudo*, use *Run As value* as root and provide *Custom Post Command/Script* value as *%emdroot%/root.sh*. If Sudo is not installed on the target box then this step will not work. In this case *root.sh* will not run and you must manually run the *root.sh* on all the targets from the Oracle Home directory of the Management Agent. For 10.2.0.4 Agents, if you have configured PowerBroker for the PDP settings and have configured the patching user to allow running commands as root, you can execute the Custom Post Command/Script with PowerBroker privilege delegation. For this, you select **Run Privilege PAM**, use *Run As value* as root, provide a Profile if needed and provide Custom Post Command/Script value as *%emdroot%/root.sh*.

5 Post-Installation Tasks

This section describes the post installation tasks to be performed.

5.1 Post Installation Tasks In General

If you had upgraded multiple Oracle Management Services (OMS) by applying the patch set to one of the OMS's first, and then subsequently upgraded the remaining OMS's, the OMS restarts automatically once the upgrade is complete. If the Agents are shutdown prior to the OMS upgrade, they must be restarted manually.

5.2 Oracle Management Service Post-Installation Tasks

This section describes post-upgrade OMS tasks.

1. During the installation process, the OMS post-configuration tool tries to set up EMCLI in the OMS home. This step may fail if the OMS is not started quickly enough, or if the OMS instances have been configured with a software load balancer working on a different UI port than the default 7777 and 4444 ports.

The EMCLI setup is not part of the core EM upgrade, and can therefore be ignored or aborted without any functional impact on Grid Control. At any time after the upgrade, the setup command can be re-run for EMCLI to re-configure it with the command line tool.

The EMCLI command to re-run the setup is:

```
$ emcli setup -user=sysman -licans=yes -trustall -noautologin  
-nocertvalidate -url=https://<host>:<port> -dir=$ORACLE_  
HOME/sysman/emcli/setup
```

If an SLB is used, the host and port used by the SLB for the UI connections has to be used for the URL parameter.

2. Re-export the emkey out of the repository using EMCTL:

```
$ emctl config emkey -remove_from_repos
```

Make sure to have a backup of this file, as this file is CRUCIAL for the securing of the repository and new Agents.

If a large number of Agents are unreachable, there may be an insufficient number connections configured in the OMS.

3. Check the database connections for the receivers.

On large systems with more than 500 Agents, the default number of connections the OMS uses to receive files might not be enough. Note that CPU and memory resources as well as available database processes should be checked before increasing the number of database connections for OMS receiver threads.

If the number of 'Busy' errors in relation to the number of total files received is too high, the default size of 25 connections might be insufficient. To determine if the system is affected by this, run the following EMDIAG test:

```
$ repvfy verify repository -test 28 -details
```

Note: EMDIAG version 2009.0706 or higher required for this test to be available.

This test will return a factor to be used to increase the number of connections for the data receivers on the OMS server.

If the database limits imposed by the 'sessions' and 'processes' parameters in the database permit it, the following parameter in the *emoms.properties* file in the *\$ORACLE_HOME/sysman/config* directory can be changed:

```
oracle.sysman.emRep.dbConn.maxConnForReceiver=<number>;
```

Note: Do not increase the number of connections to more than 60.

5.3 Grid Control Repository Database Post-Installation Tasks

This section describes post-upgrade Grid Control Repository database tasks.

1. Re-enable all database jobs, including DBMS_JOBS and DBMS_SCHEDULER jobs, that were stopped prior to the upgrade.

Note that you must set the value of *job_queue_processes* to its pre-upgrade value.

```
SQL> CONNECT SYSMAN;  
SQL> EXECUTE emd_maintenance.submit_em_dbms_jobs;
```

```
SQL> COMMIT;
SQL> ALTER SYSTEM SET job_queue_processes=<original_value> SID='*';
SQL> EXEC dbms_scheduler.set_scheduler_attribute('SCHEDULER_
DISABLED', 'FALSE');
```

2. Data Guard only:

If logging was forced on before the upgrade in configurations with Data Guard, undo the FORCE LOGGING change:

```
SQL> CONNECT / AS SYSDBA;
SQL> ALTER DATABASE NO FORCE LOGGING;
```

5.4 Agent Post-Installation Tasks

This section describes post-upgrade Agent tasks.

After upgrading the Agent software, a backup of the JDK directory will be present in the ORACLE_HOME. This contains the previous version of the JDK installed in the Agent ORACLE_HOME.

Example:

```
$ ls -ld jdk*
drwxr-xr-x 6 oraha dba 4096 Jan 28 10:15 jdk
drwxr-x-- 7 oraha dba 4096 Jan 26 12:31 jdk2009-01-28_10-14-39-AM
```

When the Agent has been verified and validated, this JDK backup directory can be removed from the file system.

5.5 Apply Critical Patches

For updated information about the critical patch list, or for information about any post-upgrade patches that must be applied, refer to the following Note on My Oracle Support:

https://metalink2.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=853691.1

6 De-Installation Of A Patch Set

There is no mechanism provided for de-installing Patch Sets. If you are concerned about being able to revert to the environment that existed before applying the Patch Set, then Oracle recommends that you back up your software installation before applying the Patch Set.

After applying the Patch Set, at any point if you want to revert to your old environment, then restore the backed-up software installation following these steps (in the order designated):

- Restore the \$ORACLE_HOME directory that was backed up
- Restore the repository database that was backed up
- Restore the Oracle Inventory that was backed up

Contact Oracle Support Services if you encounter any problems.

7 Known Issues

This section lists the known issues pertaining to this patch set release.

7.1 Installation And Upgrade Known Issues

This section addresses installation and upgrade known issues.

7.1.1 Installation Known Issues Specific To Agent Push

This section covers issues that are related to the Agent push deployment process.

For more information about Management Agent deployment, refer to the Management Agent Deployment Best Practices document available at:

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

7.1.1.1 IgnoreMessages.txt Is Not Picked Up By Remote Infrastructure If Edited With Word/WordPad

ignoreMessages.txt is not picked up by the remote infrastructure if it is edited with text editors like Microsoft Word or WordPad. If it is, the Agent Deploy application results in an application error.

Use text editors like NotePad or vi to edit the *ignoreMessages.txt* available at `<OMS_HOME>/sysman/prov/resources`. Be sure to back up the file before modifying it.

(Bug 5727231)

7.1.2 Secure UI Traffic Not Working Due To Software Load Balancer Not Being Configured

If you have a software load balancer configured in your environment, you might not be able to access the Grid Control secure URL (https). You must set the port correctly by issuing the following command:

```
./emctl secure oms -slb_console_port <port number>
```

(Bug 7624103)

7.1.3 Ignore Error When Upgrading Version 10.2.x RAC Agent to Version 10.2.0.5

When upgrading a version 10.2.0.x RAC agent to version 10.2.0.5, the following error may display:

oracle.ops.mgmt.cluster.InvalidNodeListException: PRKC-1035 : Node names for this cluster could not be retrieved

This error is harmless and can be ignored.

(Bug 8333551)

7.2 Database Management Known Issues

This section discusses known issues related to Database Management.

7.2.1 Data Masking Fails If Using Substring format With Multi-byte Characters

The Substring format uses character semantics; that is, it calculates lengths using characters. It returns a sub-string beginning at the specified 'Start Position' and contains 'Length' characters. As a result the byte-length of the returned string may not be the same as its character-length. This can happen when a column contains multi-byte characters.

For example, suppose a column of type VARCHAR2(10) contains five Korean characters, which are two bytes long. We mask this column using:

1. Substring format: with Start Position 1 and Length 3
2. Random Digits format: with Start Length 5 and End Length 5

The character-length of the string returned by the Substring format is 3 whereas the byte-length is 6. If we combine this sub-string with the random number from the second format, the total length becomes 11 bytes, which exceeds the column size and the masking operation fails.

(Bug 6967557)

7.2.2 Synchronize And Data Masking Jobs Fail After OMS Upgrade From Grid Control Version 10.2.0.4 To 10.2.0.5

A Synchronize or Data Masking job may fail with an error after upgrading the OMS from Grid Control version 10.2.0.4 to 10.2.0.5. Version 10.2.0.5 of the Change Management Pack and the Data Masking Pack requires that the Agent be upgraded to at least the 10.2.0.5 version. If you are unable to upgrade the Agent, an alternative solution is to patch the file in the Agent home. To do this, copy the latest version of this file from the Grid Control home to the Agent home. The file in both homes can be found in the following location:

`$ORACLE_HOME/sysman/admin/scripts/db/reorg/reorganize.pl`

(Bug 7564680)

7.2.3 Patch Must Be Applied If Converting To RAC Using Data Guard

Using Data Guard, you can reduce the downtime when converting a database to RAC. To use this functionality, you must apply the patch for bug 7569643 in the RAC database home.

7.2.4 Database Replay Should Be Invoked At The Database Instance Level Only

Database Replay can be invoked from the RAC database level or from the database instance level. At present, Oracle recommends that you start Database Replay at the database *instance* level only. Any database capture or replay operation will always involve all RAC database instances regardless which link you use.

(Bug 7654001)

7.2.5 RAC Provisioning Requires A 10.2.0.5 Agent

The Agent must be upgraded to version 10.2.0.5 to perform RAC provisioning or the Extend cluster deployment procedures.

(Bug 7716981)

7.2.6 Shared RAC Patching For Windows Not Supported

The *Patch Oracle RAC database - All nodes* deployment procedure for 10.2.0.4 Windows patch set application is not supported in Grid Control 10.2.0.5 out-of-the-box.

(Bug 7678502)

7.2.7 Ignore Patching Validation Errors Thrown When Oracle Clusterware Version Is Higher Than RAC Version

When a newer release of Oracle Clusterware is used with an older release of the RAC (for example, Clusterware version is 11.1.0.7 and RAC version is 10.2.0.4), the *Run prerequisite checks* can fail with a reported error when attempting to patch RAC. Such errors can be safely ignored; the patch set application will complete successfully.

(Bug 8203997)

7.2.8 Support Workbench Link Is Incorrectly Displayed On The Database Home Page If Agent Version Is Prior To 10.2.0.5

When monitoring an Oracle 11g RAC database using a Grid Control 10.2.0.4 or earlier Agent, or when monitoring an Oracle 10g RAC database, an active incident link might be visible on the target homepage. Clicking on this link leads to a non-functioning Support Workbench that reports, *There was a communication problem with the emagent*. Support Workbench is only supported when monitoring an Oracle 11g database using a Grid Control 10.2.0.5 Agent.

(Bug 7669788)

7.2.9 Job Scheduling Does Not Work In Support Workbench

Job scheduling does not work for Support Workbench in this release. When trying to schedule a task, such as generating or uploading a package, the following error message will appear: *ORA-20400: The specified job type is not valid*. The workaround is to run these tasks immediately instead of scheduling them.

(Bug 7757702)

7.2.10 Advanced Search Does Not Work In Support Workbench

The advanced search feature of Support Workbench does not work in this release.

(Bug 7856945)

7.2.11 Viewing/Searching Database ODL Alert Log Displays No Results

The file *ojdl.jar* is required by the Agent to read the alert log in ODL format for an Oracle 11g database target. However, the *ojdl.jar* is not installed in the correct location during the Agent installation process. As a result, a symbolic link of *ojdl.jar* in *\$ORACLE_HOME/sysman/jlib* pointing to *\$ORACLE_HOME/diagnostics/lib* must be created, where *\$ORACLE_HOME* is the Enterprise Manager Agent Oracle home.

For example, on Linux and Unix platforms, you would need to type the following:

```
cd $ORACLE_HOME/sysman/jlib
ln -s ../../diagnostics/lib/ojdl.jar
```

On platforms where symbolic links are not supported, call Oracle Support for workaround instructions.

(Bug 7827793)

7.2.12 Errors In Modifying Resource Plan For Database Instance

For a database resource plan's threshold, the default value of each threshold is 'UNLIMITED'. The user can change the value to any non-zero digit, but after the change, the user cannot change it back to 'UNLIMITED' and cannot change it to zero or leave it blank.

(Bug 7508127)

7.2.13 Deadlock In Delete Target B/W MGMT_BSLN_DATASOURCES And MGMT_BSLN_BASELINES

Deleting different targets in close succession can cause deadlocks in the sessions performing the deletions.

(Bug 6699780)

7.2.14 Database Performance Page Requires Adobe Flash Player Plugin

The database performance page requires the Adobe Flash Player plugin (version 9 or above) to be installed in your browser. The URL for the downloading the plugin is <http://www.adobe.com/products/flashplayer/>.

7.2.15 Managing Oracle Streams With Enterprise Manager

Grid Control provides improved support for Streams Management. An RDBMS patch may need to be applied on the target database to enable improved monitoring from Enterprise Manager. Details of this are documented in Oracle Support Note 784021.1.

7.2.16 LPAR Statistics Metric Deprecated

The *LPAR Statistics* metric on the AIX and Linux on PowerPC releases of Grid Control has been deprecated in the 10.2.0.5 version of Grid Control. It has been replaced by two separate metrics on AIX and Linux on PowerPC respectively:

1. LPAR Statistics on AIX
2. LPAR Statistics on Linux PowerPC

Any custom reports using the *LPAR Statistics* metric would need to be updated accordingly.

(Bug 7626803)

7.3 Host Management Known Issues

This section discusses known issues related to host administration.

7.3.1 IP Address May Not Be Available If IPV6 Is Enabled On Windows Hosts

On machines with IPv6 interfaces enabled, the IP address may not be displayed on the Host homepage. For such cases, follow the steps documented by Microsoft to disable IPv6 (available at

<http://www.microsoft.com/technet/network/ipv6/ipv6faq.mspx>).

After disabling IPv6, restart the Enterprise Manager Agent. The IP address will now be displayed on the Host homepage.

(Bug 7708518)

7.4 Oracle Management Service and Management Agent Known Issues

This section addresses the known issues related to Oracle Management Service (OMS) and Management Agent.

7.4.1 Metric Errors Occur For WebLogic/WebSphere Targets After Agent Upgrade

A metric error occurs after Agent upgrade for WebLogic Server or WebSphere targets.

For WebLogic targets, go to the Monitoring Configuration Link in the Related Links Section and update the value of "Jar Path". For WebLogic 9.x and 10.x targets, this value must point to a directory which contains the *wljmxclient.jar* and *wlclient.jar* files. For WebLogic 8 this must point to a directory containing the *weblogic.jar* file.

For WebSphere targets, go to Monitoring Configuration Link and update the property "WebSphere Home". This must point to WebSphere Install home.

(Bug 7680968)

7.4.2 Healthcheck Metric Collections: Agent Installation Does Not Ship GIM*.MSG Message Files

When the Healthcheck metric fails to be collected with the Agent 10.2.0.x, the output in the emagent.trc file appears as seen below:

```
2007-05-09 09:27:04 Thread-27 ERROR fetchlets.healthCheck: GIM-00104: file not found
```

The *gimus.msg* and *gimus.msb* files should be present in the directory *\$AGENT_HOME/rdbms/mesg*. However the files are not shipped with the Agent software distribution. This causes the Agent to display a generic error messages stack similar to the above example.

Refer to the My Oracle Support (formerly MetaLink) Note 430993.1 for the solution to this problem.

(Bug 7448650)

7.4.3 get_reports EMCLI Command Lists External Report Title Instead Of Internal Report Title

When Create Like is performed on an out-of-the-box report that ships with Enterprise Manager, the get_reports EMCLI command lists the external report title rather than the internal report title.

The workaround is to change the out-of-the-box report title to a different title, then issue the get_reports command. Changing the report title will cause the internal and external report titles to match.

(Bug 7656498)

7.4.4 Unable To Configure Remedy Connector After Deleting Existing Connector And Redeploying

The configure icon on the Management Connectors page does not show as a link after you register a connector because the EMKEY is not present in the repository.

You can copy the key to the repository before registering the connector and remove the key from the repository after the registration. To do this, follow these steps:

1. Copy the key to the repository:

```
emctl config emkey -copy_to_repos
```

2. Register the connector

3. Remove the key from the repository

```
emctl config emkey -remove_from_repos
```

(Bug 7758176)

7.4.5 Repeating Job Abruptly Stops Scheduling

A repeating job abruptly stops scheduling when the agent monitoring the job's target is started and the job has already skipped executions because the agent was down. Only customers with security-hardened systems (EM key is removed from the EM repository) will experience this issue.

To address this issue, edit the schedule of the job (shift the schedule by a minute, for example), save the changes, and then edit the job again to restore the original schedule. Alternatively, you can create the job again and submit it.

(Bug 7568252)

7.4.6 Issue With Metric Collection For Windows Tools Permissions Agent Metric

A Windows metric (*Windows Tools Permissions* agent metric) is executed on a non-Windows platform and reports the following error:

Error writing input stream for OS fetchlet

When this occurs, the *Windows Tools Permission* policy cannot be evaluated. Both the metric and the policy are not applicable on non-Windows platforms so the error can be ignored.

(Bug 8318835)

7.5 Client Side Monitoring Known Issues

This section addresses the client side monitoring known issues.

7.5.1 Oracle Forms JAR Download Utility Does Not Support Proxy

The beacon cannot download Oracle Forms JAR files from the Forms server when HTTP proxy is used to access the Oracle Forms server. The playback of forms transactions will fail with a connection error.

To address this issue, manually copy the Forms JAR files from the Forms server to the beacon host as follows:

1. If you are running standalone forms application, login to the system on which the Forms server has been installed. Locate the *frmall.jar* (if you are

using Forms 10.1 or later) or *f90all.jar* (if are using Forms 9.0.4 or later) under the *\$FORMS_HOME/forms/java* directory.

2. If you are running Oracle Applications, login to the system on which the Oracle Application server has been deployed. Locate the following files:

\$JAVA_TOP/oracle/apps/fnd/jar/fndforms.jar

\$JAVA_TOP/oracle/apps/fnd/jar/fndewt.jar

3. Login to the system on which the beacon has been deployed. Find out the Agent state directory by looking into *emd.properties* located in *\$ORACLE_HOME/sysman/config/* (*agentStateDir* property). Copy the JAR file(s) to *<agent_state_dir>/forms_jars_<host_name>_<port>* directory. If your forms server is *https://my.formshost.com/*, then the directory name would be *forms_jars_my.formshost.com_443*. No Agent restart is needed. The beacon should find the JAR files next time the forms transaction runs.

(Bug 7669541)

7.6 Provisioning Known Issues

The following sections discuss known provisioning known issues.

7.6.1 Application Server Provisioning And Patching Features Not Enabled By Provisioning And Patch Automation Pack For Middleware

If you own the *Provisioning and Patch Automation Pack for Middleware*, you will need to explicitly enable the license for *Provisioning and Patch Automation Pack* for using the Application Server Provisioning and Patching Deployment features. Refer to the *Enterprise Manager Licensing Information* documentation for details on the features covered by the *Provisioning and Patch Automation Pack for Middleware*.

(Bug 7662804, 7704419)

7.6.2 Staging Of Image Fails If The Staging Server Is An SLES10 Machine With "Sudo" Version 1.6 Or Higher In Bare Metal Provisioning

Staging of a default or single server image of the operating system fails if the *sudo* application on the staging server is version 1.6 or higher (for example, *sudo-1.6.8p12-18.2*). This can be fixed by ensuring that the *PERL5LIB* environment variable is included in the *Defaults_env_keep* section in the */etc/sudoers* file.

(Bug 7691716)

7.6.3 Editing Components and Images In The Software Library Created Using An Older Version of Enterprise Manager Is Not Supported In Bare Metal Provisioning

Operating system components and images that were created using an older version of Enterprise Manager, such as Enterprise Manager version 10.2.0.3 or 10.2.0.4, cannot be edited. However, these components and images can be staged and used for provisioning on bare metal machines.

(Bug 7665151)

7.6.4 Additional Operating System Users Specified During Default Or Single Server Image Creation Cannot Be Used As Agent Install User

Additional users added during image creation using the Bare Metal Provisioning (BMP) application cannot be used as an agent install user/agent home owner.

The user specified when creating the *Assignment* for the image will take precedence over users specified during image creation as an agent install user.

(Bug 7758344)

7.6.5 Pre-Install CVU For Clusterware Fails In Initial Provisioning

The *Pre-Install CVU Check* step is not supported for Grid Control versions 10.2.0.1 and 11.1.0.6 clusterware shiphomes on the AIX 6.1 platform. You must disable the step *Pre-Install CVU Check* if you are provisioning RAC on an AIX 6.1 machine.

(Bug 8403389)

7.6.6 Prereq Must Be Present To Check Whether User Has Required Capabilities

If the NIS credentials are supplied for provisioning in the AIX platform, then the CRS root scripts fail. A prerequisite to prevent this will be added in the next release.

(Bug 7758299)

7.6.7 Incorrect Text Description for Forms and Reports Source Selection

The 904 Forms and Reports provisioning procedure allows provisioning based on the existing installed Home. The user interface of the procedure allows the selection of an installed Home using a target selector which displays all existing Oracle Application Server installations. However the target selector has a text description *Source Host* associated with it, which incorrectly indicates that the host of the source installation must be selected instead of the installation itself.

(Bug 7713415)

7.6.8 Extend Cluster Deployment Procedure Fails At the Verify Prerequisite Checks Step

On some operating systems, if a user executes the *Extend Cluster Deployment Procedure* on an Oracle RAC database that uses ASM storage, the step *Verify Prerequisite Checks* (under the Prerequisites and Fix-ups phase) may fail on the reference node with the message *Invalid entry point found*.

To address this issue, verify that the prerequisites have executed successfully on the new nodes and then ignore and continue with the deployment procedure execution.

The same issue may be seen at the *Verify Prerequisite Checks* step (under the Operating System user checks for RAC phase). Perform the verification specified above and then ignore and continue with the deployment procedure execution.

(Bug 8438698)

7.6.9 Oracle RAC Provisioning Fails If Gold Image Was Created Using Different DBA Group

When using gold images to deploy Oracle RAC using the Oracle Clusterware and RAC deployment procedure, the procedure may fail during database creation with the error OS Authentication error. One primary cause of this failure is because of a group mismatch between the source Oracle Home used to create the database gold image and the target Oracle Home that the gold image is being used to create.

Ensure that the user using the gold image for provisioning belongs to the same primary group as that of the gold image source Oracle Home user.

(Bug 8444916)

7.7 Middleware Management Known Issues

This section addresses known issues in middleware management support.

7.7.1 Data Source Metrics Are Not Available For OC4J 10.1.3

The datasource metrics that Grid Control displayed for OC4J 10.1.2 are no longer available for OC4J 10.1.3.

(Bug 7637391, 7637391)

7.7.2 Configuration Files Not Getting Collected For WebLogic Server 8.x Administration Server

The Configuration Files tab on the Last Collected Configuration page does not actually display any WebLogic Server configuration files. To correct this problem, specify the "Domain Home" in the "Monitoring Configuration" page of the WebLogic Administration Server.

(Bug 7574570)

7.7.3 WebLogic Server Upgrade From 8.1 SP6 To 10.0 Does Not Support New Features

When upgrading from 8.1 SP6 to 10.0, the WebLogic Server home page in Grid Control still shows as version 8.1. None of the new features will be available after an in-place upgrade of WebLogic from 8.1 to 10.0.

The Monitoring Configuration link in Grid Control still displays version 8.1 and the *weblogic.jar* location from the 8.1 install location, even after refreshing the Domain from the WebLogic Server domain home page in Grid Control.

Since automatic discovery of WebLogic is not supported, you must manually update the Version and "Jar Path" properties via the Monitoring Configuration page and restart the Agent.

(Bug 7584224)

7.7.4 Configuration Files Not Getting Collected For WebLogic Server 8.x Administration Server

The Configuration Files tab on the Last Collected Configuration page does not actually display any WebLogic Server configuration files. To correct this problem, specify the "Domain Home" in the "Monitoring Configuration" page of the WebLogic Administration Server.

(Bug 7574570)

7.7.5 WebLogic Server Upgrade From 8.1 SP6 to 10.0 Does Not Support New Features

After upgrading from WebLogic Server version 8.1 to version 10.0, the new management features will not be available by default. To enable them, the Version and "Jar Path" properties must be manually updated via the Monitoring Configuration page. Re-start the Agent after making these updates.

(Bug 7584224)

7.7.6 Agent Cannot Trace WebLogic Server Status After Manual Restart

When a WebLogic Admin server is restarted manually, Enterprise Manager Grid Control cannot monitor the WebLogic server after restart. The status will always be displayed as *Down*.

The workaround is to restart the agent which is monitoring the WebLogic target.

(Bug 8221486)

7.7.7 Metric Error for WebLogic/WebSphere Targets After Agent Upgrade

A metric error occurs after Agent upgrade for WebLogic Server or WebSphere targets.

For WebLogic targets, go to the Monitoring Configuration Link in the Related Links Section and update the value of "Jar Path". For WebLogic 9.x and 10.x targets, this value must point to a directory which contains the *wljmxclient.jar* and *wlclient.jar* files. For WebLogic 8 this must point to a directory containing the *weblogic.jar* file.

For WebSphere targets, go to Monitoring Configuration Link and update the property "WebSphere Home". This must point to WebSphere Install home.

(Bug 7680968)

7.7.8 BPEL Target With Latest Agent Contains Alerts For BPEL Partner

If you using Oracle Management Agent 10g Release 5 (10.2.0.5) to monitor BPEL 10.1.3.3 or 10.1.3.4, a metric collection error will occur on the home pages.

To resolve this issue, follow the workaround described in My Oracle Support (formerly MetaLink) note 735128.1.

(Bug 7830296)

7.7.9 Oracle Service Bus Provisioning Not Supported If WebLogic Server Is Discovered Using Remote Agent

Remote monitoring of a WebLogic Server target requires that the Management Agent be installed on the WebLogic Server host. Ensure the Agent exists on the host before running the Oracle Service Bus Provisioning deployment procedure.

(Bug 7597773)

7.7.10 Oracle Service Bus 2.6 End Point URI Metric Missing For Business Service

The Endpoint URI metric for the Business Service is not available when monitoring OSB 2.6 targets. This is a known issue in that OSB release. The metric is available in the OSB 3.0 release however.

(Bug 7611127)

7.8 Third-Party Application Server Monitoring Known Issues

This section addresses third-party application server monitoring known issues.

7.8.1 Discovery Of IBM WebSphere Application Server Fails On Grid Control Version 10.2.0.4 With Agent Version 10.2.0.5

Discovery of IBM WebSphere Application Server fails using OMS version 10.2.0.4 with Agent version 10.2.0.5. The same behavior is evident when the OMS is version 10.2.0.5 and the Agent is version 10.2.0.4.

You must apply patch for bug 6829159 or upgrade the OMS to version 10.2.0.5 to resolve this issue.

(Bug 7634145)

7.9 Other Known Issues

This section addresses SOA Management Pack known issues.

7.9.1 Siebel Workflow And Other Newly Enabled Targets Shown In Metric Collection (Error) State After UpdateNow Completes

After the UpdateNow operation has completed during upgrading the OMS and the Agent from 10.2.0.4 to 10.2.0.5, newly enabled Siebel Workflow targets will be enabled. However, both the Workflow Component group and the newly enabled components will be shown in a metric collection (error) state. On the *Monitoring Configuration* page, the Workflow Component Group will have empty passwords.

To address this issue, re-enter the Siebel password for the newly added target and the Workflow component group targets in the *Monitoring Configuration* page of the respective components. Bounce the Agent to resolve the status of the affected components.

(Bug 7719976)

7.9.2 Siebel Workflow Target Link Disabled After Grid Control Is Upgraded

After upgrading to this patch set, the link to the Workflow target may not be visible in the *General* section of the Siebel Enterprise Home page. To refresh the details and view the link, click **Update Now**.

(Bug 7670650)

8 Documentation Accessibility

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

<http://www.oracle.com/accessibility/>

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should

appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711.

Oracle Enterprise Manager Grid Control Release Notes, 10g Release 5 (10.2.0.5) for AIX 5L Based Systems (64-Bit)
E14642-03

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.