Oracle® GoldenGate Enterprise Manager Plug-In

System Monitoring Installation Guide

Release 12*c* (12.1.0.3.0)

E62429-05

March 2018

This document provides a brief description of the Enterprise Manager Plug-in for Oracle GoldenGate, details on the releases the plug-in supports, prerequisites for deploying the plug-in, and step-by-step instructions on how to configure Oracle GoldenGate for the Enterprise Manager Plug-in for Oracle GoldenGate. The following topics are discussed:

1 Introduction to Enterprise Manager Plug-in for Oracle GoldenGate

The Enterprise Manager Plug-in for Oracle GoldenGate extends the Oracle Enterprise Manager (EM) Cloud Control to support for monitoring and managing Oracle GoldenGate processes. By deploying the it in your Cloud Control environment, you gain the following features:

- Visually monitor current Oracle GoldenGate metrics and historical trends.

- Generate automatic alerts and incidents when thresholds are breached.

ORACLE®

- Start and stop individual processes.

- Modify existing configuration files.

- View error logs, report files, and discard files.

- Audit user access of privileged Plug-in features.

2 Preparing to Deploy

This section contains the following topics:

2.1 Supported Platforms

The Enterprise Manager Plug-in for Oracle GoldenGate supports monitoring of all platforms where both Oracle GoldenGate Release 11.2.1 and later and Oracle Enterprise Manager Cloud Control 12*c* agent and later instances can run.

The Oracle GoldenGate agent has a local dependency on the Enterprise Manager agent. Therefore, the system monitoring plug-in for Oracle GoldenGate is not supported on the following platforms:

- HP NonStop

- IBM System z

- IBM z/OS

- IBM i (AS400)

See the Certifications tab on My Oracle Support for details:

https://support.oracle.com

2.2 Supported Releases

The Enterprise Manager Plug-in for Oracle GoldenGate supports the following product releases:

- Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4.0) and later.

- Oracle GoldenGate versions supported include:

  - Oracle GoldenGate Monitor Agent 12*c* (12.1.3.0.3) and later is required and is the minimum version required to support Start, Stop, Kill, and Edit features.

  - Oracle GoldenGate 12*c* (12.1.2.0.1).

  - Oracle GoldenGate 12*c* (12.1.2.0.0).

  - Oracle GoldenGate 11*g* Release 2 (11.2.1.0.10) and higher.

  - Support for non-core Oracle GoldenGate. If you want to use a particular version of Oracle GoldenGate (for example, version 11.2.1.0.23) other than the default version, then add a `<MinOGGCoreVersion>` entry for each `<Feature>` element in the `feature_version.xml` file as shown below:

    ```
    <Document>
    ```

```
<VersionCacheResetSchedule>
    <Interval>1</Interval>
    <TimeUnit>Hour</TimeUnit>
</VersionCacheResetSchedule>
<FeatureList>
    <Feature>
        <FeatureName>ExecuteCommands</FeatureName>
        <MinPluginOMSVersion>12.1.0.4.0</MinPluginOMSVersion>
        <MinPluginEMAgentVersion>.0</MinPluginEMAgentVersion>
        <MinOGGCoreVersion>11.2.1.0.23</MinOGGCoreVersion>
    </Feature>
    <Feature>
        <FeatureName>ViewLogs</FeatureName>
        <MinPluginOMSVersion>12.1.0.4.0</MinPluginOMSVersion>
        <MinPluginEMAgentVersion>.0</MinPluginEMAgentVersion>
        <MinOGGCoreVersion>11.2.1.0.23</MinOGGCoreVersion>
    </Feature>
    <Feature>
        <FeatureName>ViewEditConfig</FeatureName>
        <MinPluginOMSVersion>12.1.0.4.0</MinPluginOMSVersion>
        <MinPluginEMAgentVersion>.0</MinPluginEMAgentVersion>
        <MinOGGCoreVersion>11.2.1.0.23</MinOGGCoreVersion>
    </Feature>
</FeatureList>
</Document>
```

2.3 Meeting the Prerequisites

The following prerequisites must be met before you can deploy and use the Enterprise Manager Plug-in for Oracle GoldenGate:

- Section 2.3.1, "Software Requirements"

- Section 2.3.2, "Verify Your Environment Meets Certification Requirements"

- Section 2.3.3, "Set Environment Variables to Point to the Java Installation"

- Section 2.3.4, "Configure Each Oracle GoldenGate Instance"

- Section 2.3.5, "Downloading the Plug-in"

2.3.1 Software Requirements

- The following must be installed and running:

    - Oracle GoldenGate 12*c* (12.1.2.0.1) and later or Oracle GoldenGate 11*g* Release 11.2.1.0.17 and later to support monitoring by Enterprise Manager Cloud Control.

        Note: Oracle Enterprise Manager does *not* support monitoring of Oracle GoldenGate release 11.1.1 and earlier.

    - Oracle GoldenGate Monitor Agent 12*c* (12.1.3.0.4) and later; the installation location you chose is referred to as OGG_AGENT_ORA_HOME in this document. This location is not necessarily the Oracle GoldenGate 12*c* installation location.

    - Oracle Enterprise Manager (OEM) Cloud Control 12*c* Release 4 (12.1.0.4.0) and later (Oracle Management Service and Oracle Management agent).

- You must apply the OEM Patch 20460402 before deploying or upgrading Enterprise Manager Plug-in for Oracle GoldenGate found at

  https://support.oracle.com/

- An Oracle Management agent must be installed on each system hosting an Oracle GoldenGate instance that will be monitored.

- Verify that Java SE, JDK 7u85 and greater is installed on each system where Oracle GoldenGate is installed. To verify your Java version, navigate to the Oracle GoldenGate installation directory and run the following command:

```
Shell> java -version
```

The version is displayed and should be similar to the following:

```
java version "1.7.0_85"
Java(TM) SE Runtime Environment (build 1.7.0_85-b18)
Java HotSpot(TM) Client VM (build 25.25-b02, mixed mode)
```

If this does not return a 1.7 version of Java, check that the PATH environmental variable includes java.exe and java.

If you need the latest version of Java, you can download it from:

http://www.oracle.com/technetwork/java/javase/downloads/

- You can download either the Java Development Kit (JDK) or Java Runtime Environment (JRE).

- For the Windows x64 platform, you must use the x64 version of JDK or Enterprise Manager will not be able to load the Java agent.

- To configure the Software Library, see the "Configuring Software Library" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

2.3.2 Verify Your Environment Meets Certification Requirements

Make sure that you are installing your product on a supported hardware or software configuration. For more information, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

Oracle has tested and verified the performance of your product on all certified systems and environments; whenever new certifications occur, they are added to the proper certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

2.3.3 Set Environment Variables to Point to the Java Installation

Perform the following steps to ensure that your environment is ready for monitoring:

> **Note:** If you set the LD_LIBRARY_PATH for monitoring for Oracle GoldenGate Release 11.1.1 instances, you must remove the setting when monitoring 11.2.1 and later instances.

- For **Windows**:

  1. Set the JAVA_HOME variable to the location of the Java installation.

  2. Set the PATH variable to the jre\bin of the Java installation location:

```
. . .;%JAVA_HOME%\jre\bin
```

- For **Oracle Solaris** and **Linux**:

  1. Set the `JAVA_HOME` environment variable to the location of the Java installation.

  2. Set the `PATH` environment variable to the `jre/bin` directory of the Java installation.

  For example (using the `bash` shell):

  ```
  export JAVA_HOME=<PATH to JDK installation>
  export PATH = $PATH:$JAVA_HOME/jre/bin
  ```

2.3.4 Configure Each Oracle GoldenGate Instance

For each Oracle GoldenGate instance:

1. Enable monitoring by navigating to the Oracle GoldenGate installation directory and editing the `GLOBALS` parameter file.

   ```
   Shell> ./ggsci
   GGSCI> EDIT PARAMS ./GLOBALS
   ```

   Add the `ENABLEMONITORING` parameter to the `GLOBALS` parameters and save the file. The parameter will be activated when you start the Manager after configuring the Oracle GoldenGate instance.

2. Create the Oracle Wallet to store passwords using the steps listed in Creating the Oracle Wallet.

3. Configure the Oracle GoldenGate instances for monitoring by Oracle Enterprise Manager by following the steps listed in Configuring Oracle GoldenGate to Run with Oracle Enterprise Manager

4. Follow the steps listed in Starting the Oracle GoldenGate Instances to:

   - Create the database used to store monitoring data.

   - Start the Oracle GoldenGate agent that will gather monitoring data to pass to the Oracle Management agent.

2.3.5 Downloading the Plug-in

You can download plug-ins in online or offline mode. *Online* refers to an environment where you have Internet connectivity to the Enterprise Manager Store. *Offline* refers to an environment where you do not have Internet connectivity. See the `Managing Plug-ins` chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3 Deploying the Plug-in

You can deploy plug-ins to an y Oracle Management Services (OMS) instance in graphical interface or command line interface. While the graphical interface mode enables you to deploy one plug-in at a time, the command line interface mode enables you to deploy multiple plug-ins at a time, thus saving plug-in deployment time and downtime, if applicable. See the `Managing Plug-ins` chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3.1 Importing the Plug-in Archives Manually

If you have downloaded the plug-in manually, then you will need to import the plug-in into Oracle Enterprise Manager Cloud Control:

1. Download the Enterprise Manager Plug-in for Oracle GoldenGate from the Downloads page:

   http://www.oracle.com/technetwork/middleware/goldengate/downloads/

   It is located in the Management Pack for Oracle GoldenGate section.

2. Set up the Enterprise Manager Command Line (EM CLI) utility. From the **Setup** menu, click **Command Line Interface**. Follow the instructions outlined on the Enterprise Manager Command Line Interface Download page.

3. Import the plug-in archive:

   ```
   emcli login -username=<your user ID> -password=<password>
   emcli sync
   emcli import_update -file=<path to *.opar file you downloaded>
   ```

4. Once you have imported the plug-in archive, log in to Enterprise Manager Cloud Control and complete the deployment:

   a. Click **Setup** (in the upper right corner), then **Extensibility**, and finally **Plug-ins**.

   b. On the Plug-ins page, expand the Middleware folder.

   c. Select **Oracle GoldenGate**. Click **Deploy on**, then select **Management Servers...** to start the deployment process.

   d. Enter the **Repository SYS password** and click **Continue**.

      A series of prerequisite system checks will begin. As each system check completes, click **Next** to continue to the next check.

   e. Once the prerequisite checks are complete, click **Next** and then **Deploy**.

   Note: Deployment usually takes about 10 minutes to complete. During that time, all connected users will be disconnected from Enterprise Manager. Even though the confirmation page displays, clicking Show Status will display "This webpage is not available" while deployment of the plug-in progresses.

   ---

   f. Check the status of Enterprise Manager Plug-in for Oracle GoldenGate deployment. After 10 minutes, you can check the status through the `emcli` command:

   ```
   emcli login -username=<your user ID> -password=<password>
   emcli sync
   emcli get_plugin_deployment_status -plugin_id=oracle.fmw.gg -omslocal
   ```

   Note: If you have not enabled the `-omslocal` flag, then make sure you specify the host and all the necessary credentials.

Once the Enterprise Manager Plug-in for Oracle GoldenGate is deployed, an **Oracle GoldenGate** item will appear under **Targets** in Enterprise Manager Cloud Control.

4 Creating the Oracle Wallet

Perform the following steps to create the Oracle Wallet and to add the password that the Oracle Management agent will use to connect to the Oracle GoldenGate agent to receive metric values:

1. Navigate to the navigate to the `OGG_AGENT_ORA_HOME` directory.

   > **Note:** Oracle GoldenGate 12*c* (12.1.2.0.0) introduced the storing of passwords for extract and replicats in Oracle Wallets. However, both the Oracle GoldenGate core replication and Oracle GoldenGate Monitor Agent (JAgent) wallets cannot reside in the same location. If both Oracle GoldenGate core and JAgent are using the Oracle Wallet then Oracle GoldenGate core must use a non-default location. This configuration can be set by using the `GLOBALS` parameter `WALLETLOCATION`.

2. Run the appropriate `pw_agent_util` script using the runtime argument that specifies you will be using only the Java agent (and not Oracle GoldenGate Monitor Server):

   - On Windows, go to the command line and enter:

     ```
     Shell> pw_agent_util.bat -jagentonly
     ```

   - On UNIX, enter the following command:

     ```
     Shell>./pw_agent_util.sh -jagentonly
     ```

   If a wallet does not exist, then one is created.

3. Next, the utility prompts you to enter the Oracle Enterprise Manager agent password:

   ```
   Please create a password for Java Agent:
   ```

   It then prompts you to confirm the password:

   ```
   Please confirm password for Java Agent:
   ```

   If a wallet already exists in the `dirwlt` directory, a message is returned and the utility stops. If this happens, run the utility to create the Jagent password by entering one of the following (the command options are not case sensitive):

   - On Windows, go to the command line and enter:

     ```
     Shell> pw_agent_util.bat -updateAgentJMX
     ```

   - On UNIX, enter the following command:

     ```
     Shell> ./pw_agent_util.sh -updateAgentJMX
     ```

5 Configuring Oracle GoldenGate to Run with Oracle Enterprise Manager

You must configure your Oracle GoldenGate instance to work with the EM by setting property values for the hosts, ports, and monitoring type.

To configure monitoring for EM, navigate to the `OGG_AGENT_ORA_HOME` directory and edit the `cfg/Config.properties` file with the following settings:

1. Set the property that determines the monitoring type to Oracle Enterprise Manager:

   ```
   agent.type.enabled=OEM
   ```

2. Ensure that the port you assign to the `jagent.rmi.port` property is free and available:

   - For UNIX, run:

     ```
     netstat -anp | grep [port_number]
     ```

     For example:

     ```
     netstat -anp | grep 5559
     ```

   - For Windows, run:

     ```
     netstat -an|findstr [port_number]
     ```

     For example:

     ```
     netstat -an|findstr 5559
     ```

3. Set the Remote Method Invocation (RMI) port for the Oracle Enterprise Manager agent. The default is **5559**.

   ```
   jagent.rmi.port=[port_number]
   ```

4. Set the property that identifies the host of the Jagent. This should be the host of the Oracle GoldenGate instance. The value may be a name or an IP address.

   ```
   jagent.host=[Oracle_GoldenGate_host_name]
   ```

5. Set the port of the Jagent. The default for this property is **5555**.

   ```
   jagent.jmx.port=[port_number]
   ```

6. Set the user name for the connection to the Jagent.

   ```
   jagent.username=[user_name]
   ```

7. Set the SSL value for the connection to **false**:

   ```
   jagent.ssl=false
   ```

6 Starting the Oracle GoldenGate Instances

Use the following steps to start Oracle GoldenGate and the Oracle GoldenGate agent. For more information on the `GGSCI` commands used in this section, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

1. Navigate to the Oracle GoldenGate installation directory.

2. Start a `GGSCI` session:

   ```
   Shell> ./ggsci
   ```

3. If this is the first start for Oracle GoldenGate since monitoring has been enabled, create the database that will persist monitoring data:

   ```
   GGSCI> CREATE DATASTORE
   ```

4. If you just added the `GLOBALS` parameter to enable monitoring, you must stop and restart running Oracle GoldenGate Manager processes to activate the new setting:

   ```
   GGSCI> STOP MANAGER
   ```

5. Start the Oracle GoldenGate Manager process:

   ```
   GGSCI> START MANAGER
   ```

6. Start the Oracle GoldenGate agent:

   ```
   GGSCI> START JAGENT
   ```

   > **Note:** The Oracle Wallet must be successfully created and the password entered before the agent is started.

7 Configuring the Management Agent to Deploy the Plug-in

Follow the steps below to set the preferred credentials on all agents where you want to deploy the Enterprise Manager Plug-in for Oracle GoldenGate:

1. In Enterprise Manager Cloud Control, click **Setup**, then **Security**, and **Preferred Credentials**.

2. On the Preferred Credentials page, search for and select your host from the Target Type column then click **Manage Preferred Credentials**.

   The Preferred Credentials page appears and is divided into two sections:

   Default Preferred Credentials:
   These credentials are set as default for the selected target type. When set, these credentials are applicable to all the targets of this type, for which credentials are not specifically provided.

   Target Preferred Credentials:
   These credentials are specific to the individual targets. They are provided if the selected target requires separate credential values than those set for its target type by default. Setting target credentials overrides the default credentials for that target.

3. In the Target Credentials section, for the host that is running the Management agent where the Enterprise Manager Plug-in for Oracle GoldenGate has to be deployed, select the host name and click **Set**

   The Select Named Credential dialog box appears.

4. Enter the values for host credential as follows:

   These values set host credentials of the EM agent so that the Enterprise Manager Plug-in for Oracle GoldenGate can communicate with it. For example, if the EM agent is on host slc0045 and this machine is accessible using credentials X1 and X2

and X1 was used to install the EM agent, then you must use the X1 as the host credentials.

There are two Oracle GoldenGate Preferred Credentials; they are the Oracle GoldenGate host credential and the administration credential. This username is added in the `config.properties` file of Oracle GoldenGate agent and the password is defined at the time of the Oracle Wallet creation.

5. Click **Save**.

   The credentials are saved as named credentials, making them available for use later. The Select Named Credential dialog box closes and a confirmation message appears on the Security page.

6. Click **Test** to ensure that there are no errors. If your test runs successfully, then your credentials are set correctly.

7. Run the OS Command job for the Management agent where the Enterprise Manager Plug-in for Oracle GoldenGate has to be deployed:

   a. Log in to Enterprise Manager Cloud Control.

   b. Click **Enterprise**, then **Job**, and finally **Activity**.

   c. In the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.

   d. Enter the details required in the following pages, and click **Submit** to run the job. If the job runs successfully, then your credentials are set correctly.

8 Verifying and Validating the Plug-in Deployment

Before verifying and validating the Enterprise Manager Plug-in for Oracle GoldenGate, you must promote the GoldenGate target that is found during auto-discovery. Refer to the "Discovering, Promoting, and Adding Targets" section in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

After waiting a few minutes for the Enterprise Manager Plug-in for Oracle GoldenGate to start collecting data, use the following steps to verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click the **Oracle GoldenGate** target link from the All Target page. The Oracle GoldenGate Home Page appears.

2. Verify that no metric collection errors are reported by clicking **Monitoring and then Metric Collection Errors** from the Target menu.

3. Ensure that reports can be seen and no errors are reported by clicking **Information Publisher Reports** in the Target menu and viewing reports for the Oracle GoldenGate target type.

4. Ensure that configuration data can be seen by clicking **Configuration** and then **Last Collected** in the Target menu. If configuration data does not immediately appear, click **Refresh** in the Latest Configuration page.

9 Adding Instances for Monitoring

After successfully deploying the Enterprise Manager Plug-in for Oracle GoldenGate, follow these steps to add the plug-in target to Enterprise Manager Cloud Control for central monitoring and management:

1. From the **Setup** menu, select **Add Target** and then **Configure Auto Discovery**.

2. Click on the GoldenGate Discovery Module to display the **Configure Target Discovery for Target Types** screen.

3. Select the agent host name and click **Edit Parameters**.

   The Edit Parameters: GoldenGate Discovery dialog appears.

4. Enter the information needed to connect to the Oracle GoldenGate agent as follows:

   - JAgent Username - Valid user name for the connection. This name is specified in the `Config.properties` file.

   - JAgent Password - Password for the user, which is set during the Oracle Wallet creation.

   - JAgent RMI Port - The Remote Method Invocation port to use for the connection.

   - JAgent Host Name - Enter the Cluster Virtual IP (VIP) for your high availability cluster environment (HA/RAC) instead of Physical IP of your Oracle GoldenGate machine; for all other environments, use the default, localhost.

     For HA/RAC environments, when the targets are promoted, the host property of the targets is updated with VIP. When these targets are relocated or failed over to another node, they are still accessible using the same monitoring details because the EM agent continues monitoring the OGG instance irrespective of where OGG instance is actually running.

5. Click **Ok** when finished. Target discovery has been configured on this host.

6. Click **Discover Now** to discover targets immediately.

7. After the discovery job executes, you can check for discovered hosts that may contain potential targets. You can do this two ways:

   - Select the job in the Host Discovery page, then click **View Discovered Targets**; or

   - From the Setup menu, select **Add Target**, then select **Auto Discovery Results**.

8. Select a target to promote, then click **Promote**. A promotion wizard for this target type opens. .

9. Select the **Targets on Hosts** tab, and choose one or several OGG targets to promote.

10. Check the target type home page to verify that the target is promoted as an Cloud Control target. Once a target is successfully promoted, the Management Agent installed on the target host begins collecting metric data on the target.

    For more information about discovering, promoting, and adding targets, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

10 Configuring Instance-Level Security

Enterprise Manager provides instance-level security flexibility to provide target-level privileges to admin users. For example, if an Enterprise Manager Plug-in for Oracle GoldenGate is managing three OGG instances (for example, OGG1, OGG2, and

OGG3), a user can be granted privileges to any of these instances and their sub-targets (that is, their OGG processes).

For granting target-level access:

1. Log in as a super admin (for example, `sysman`). From the **Setup** menu, select **Security**, and then **Administrators**.

2. On the Administrators page, click **Edit** to modify access for an existing user. Click **Create/Create Like** to create a new user and to assign the appropriate user roles.

3. On the Properties tab, enter the required credentials for the new user.

4. Click **Next**.

   The Create Administrator *userName*: Roles page appears. This screen allows you to assign roles to the named user by moving the role from the Available Roles column to the Selected Roles column.

5. Select one or more roles from the Available Roles list and click the **Move** arrow to add them to the new user. At a minimum, you must select the **EM_BASIC_ SUPPORT_REP** role in addition to the preselected roles.

   The role privileges are as follows:

RM Role Name	Edit/View Parameter	View Report	View Discard
EM_ALL_ADMINISTRATOR	Yes	No	No
EM_ALL_OPERATOR	Yes	No	No
EM_ALL_VIEWER	No	No	No
PUBLIC	No	No	No
EM_PLUGIN_USER	No	No	No

   > **Note:** Make sure that you do not select any 'ALL' roles in this step (for example, EM_ALL_ADMINISTRATOR, EM_ALL_OPERATOR, etc.), because the user role you are creating will be entitled to all OGG instances.

   EM supports object level access control so administrators can be given roles for specific targets only, see the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

6. Click **Next**.

   The Target Privileges page appears.

7. Select the Target Privileges tab, scroll down to the Target Privileges section and select the **Execute Command Anywhere** and **Monitor Enterprise Manager** roles, and then click **Add**.

   These two roles are required for full functionality and multi-version support.

8. Scroll below the Privileges Applicable to All Targets table to the Target Privileges section. This section gives the Administrator the right to perform particular actions on targets.

9. Click **Add**.

The Search and Add: Targets page appears in a new browser window.

**10.** From the list of instances, select the instances you want to give access to the user.

> **Note:** Only the Oracle GoldenGate instances are being assigned, not the Manager, Extract, or Replicat processes.

Figure 1 shows an example of two Oracle GoldenGate instances (with port numbers 5559 and 5560, respectively). Access to only one of them (with port number 5560) is being assigned to this user.
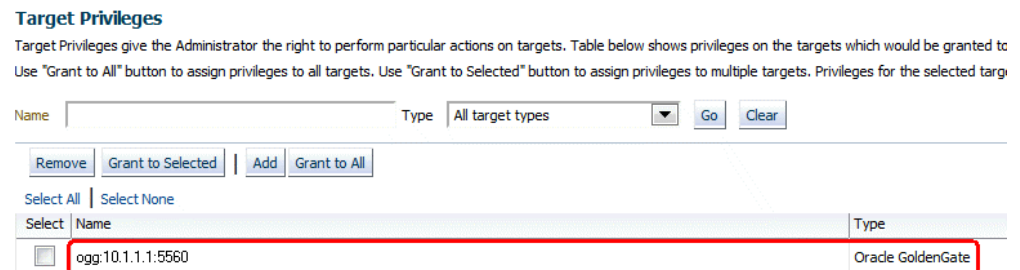
Figure 1 Select Oracle GoldenGate Targets
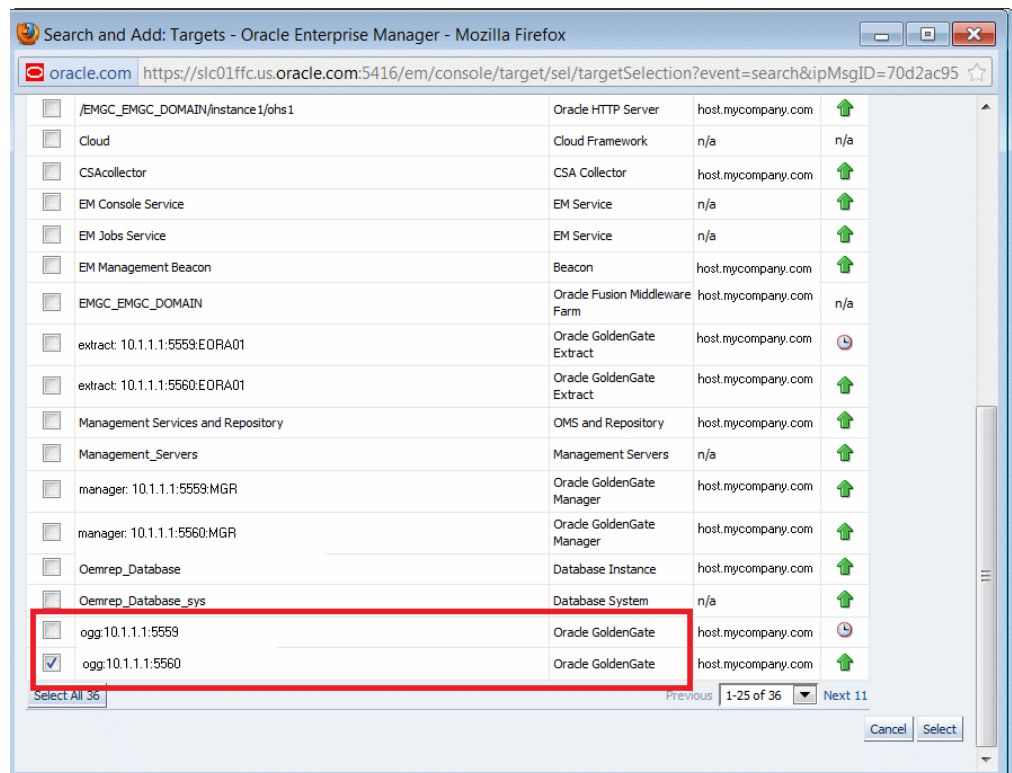
11. Click **Select** to save the changes.

You are returned to the Add Targets page and the Target Privileges list is refreshed to show your selection as shown in Figure 2.

Figure 2 Updated Target Privileges

12. To set the required privileges for the target, click the **Edit Individual Privileges** link in the right-most column for each target.

Select from the following privileges:

Privilege Name	Description
Full	Ability to do all operations on the target, including delete the target.
View contents of OGG report file	Ability to view content of the report files for OGG targets.
View contents of OGG discard file	Ability to view content of the discard files for OGG targets.
Run OGG command	Ability to run OGG commands (`Start`, `Stop`, `Kill`) for OGG targets.
Edit OGG parameter file	Ability to edit parameter files for OGG targets.
Connect Target	Ability to connect and manage target.

You should *not* select both the Full and Connect Target privileges because Full includes Connect Target so it in effect disables Connect Target. Use Connect Target without the Full privilege.

13. Click **Continue**.

14. To complete the process, click **Review** to review your user's privileges and then click **Finish**. The user should now have access to the selected instance(s).

These privileges are automatically assigned from top to bottom in the hierarchy. For example, if the 'Run OGG Command' privilege is assigned to an OGG instance, it is automatically assigned to all its child processes. However, you can also provide process specific privileges. Suppose the 'Edit OGG parameter file' privilege is assigned to a process, it is specific to that process and is be assigned to other processes in the instance.

15. Test the instance-level security to confirm that all edited processes are operating whit the assigned privileges:

    a. Log in as the newly created/edited user.

    b. From the Targets menu, click **GoldenGate**. On the Oracle GoldenGate page, confirm that only those OGG instances are visible for which access was granted to the user (see Figure 3).

Figure 3   Instance-Level Security Test for New User

c. Log out and log in as `root`.

d. From the Targets menu, click **GoldenGate**. Confirm that ALL the managed OGG instances are being shown up in this page (see Figure 4).

Figure 4   Instance-Level Security Test for Root User

For more information about security, see the *Oracle Enterprise Manager Cloud Control Security Guide*.

11 Using the Enterprise Manager Plug-in for Oracle GoldenGate

This section contains these topics:

■ Section 11.1, "Using Audit Logging"

■ Section 11.2, "Monitoring Metrics"

11.1 Using Audit Logging

For all Oracle GoldenGate actions (for example, Start and Stop processes) and file access (for example, parameter, report, and discard), messages are logged to the server log file for auditing purposes. For details to enable and view the audit log:

11.1.1 Enabling Audit Logging

To enable or disable an audit for a specific action, run the following commands from the `oms/bin` directory by entering the values you want to use for each setting:

```
emcli update_audit_settings
  -audit_switch="ENABLE|DISABLE"
  -operations_to_enable="name_of_operations_to_enable"
  -operations_to_disable="name_of_operations_to_disable"
  -externalization_switch="ENABLE|DISABLE"
  -directory="directory_name"
  -file_prefix="file_prefix"
  -file_size="file_size"
  -data_retention_period="data_retention_period"
```

One or more logging options can be enabled or disabled. The operations that can be logged and their `-operations_to_enable` flag follow and are prepended with OGG to indicate Oracle GoldenGate:

- Start OGG process: `OGG_START_TARGET`

- Stop OGG process: `OGG_STOP_TARGET`

- Kill OGG process: `OGG_KILL_TARGET`

- View report file: `OGG_VIEW_REPORT`

- View `ggserr.log` contents: `OGG_VIEW_GGSERRLOG`

- Edit parameter file: `OGG_EDIT_PARAM`

Options can be combined and separated by a semicolon (;). For example, to enable all audit logging for the Enterprise Manager Plug-in for Oracle GoldenGate:

```
emcli update_audit_settings -operations_to_enable="OGG_START_TARGET;OGG_STOP_
TARGET;OGG_KILL_TARGET;OGG_VIEW_REPORT;OGG_VIEW_GGSERRLOG;OGG_EDIT_PARAM"
```

11.1.2 Searching and Viewing Audit Logs

A Cloud Control user with Super Administrator privileges has the access to search for and view an audit log. To view an audit log from Cloud Control:

1. As a user with Super Administrator privileges, click the **Setup** menu, then select **Security**, and finally **Audit Data**.

2. On the Audit Data page (Figure 6), click the **Operations** drop-down menu and look for operations starting with **OGG**. Figure 5 shows an example of the OGG operations.

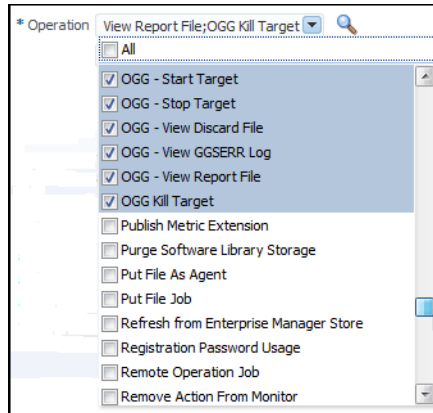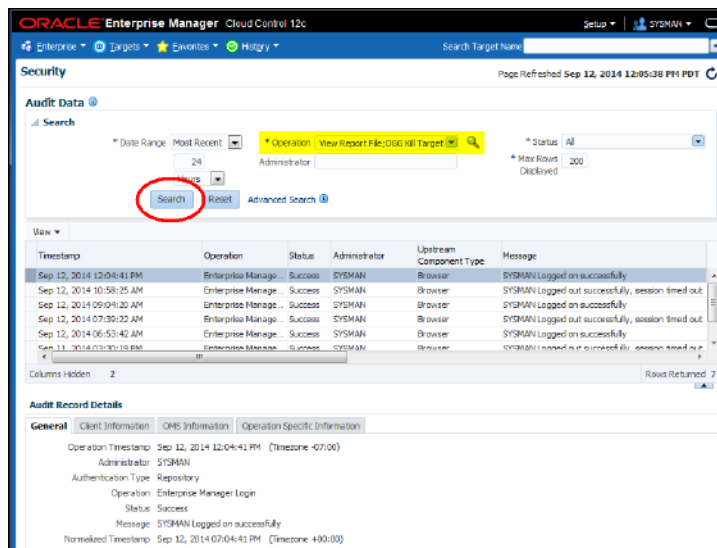> **Note:** If you deselect the **All** item, then all audit data items will be deselected as well.

Figure 5   Selecting Oracle GoldenGate Operations to Audit

Figure 6   Audit Data Page

3. Check or uncheck the actions as needed. Audit logs are searchable only for the actions checked in this Operations drop-down menu. You can filter the results with various other criteria (date range, status, etc.) available on the Audit Data page.

4. Click the **Search** button ![Search].

5. To view the audit log, select an audit log from the search results list.

6. Once selected, you can view audit log information in the Audit Record Details region (Figure 7). The Audit Record Details will update automatically for each audit log you select. Click the tabs for specific information:

   ■ General

   ■ Client Information

   ■ OMS Information

   ■ Operation Specific Information

Figure 7   Audit Record Details

> **Note:** For additional information about the auditing functionality of Enterprise Manager, refer to these documents:
>
> - See the "Configuring Auditing Framework" section of *Oracle Enterprise Manager Cloud Control Getting Started Guide*.
>
> - "Configuring the Audit Data Export Service" in the *Oracle Enterprise Manager Cloud Control Security Guide*.

11.2 Monitoring Metrics

The following processes are monitored by the Enterprise Manager Plug-in for Oracle GoldenGate:

- **Extract** - An Extract process picks up changes from transaction logs and writes them to a trail. That trail is picked up by a Replicat and the changes are written to the target database. If the Replicat is across the network, then the trail is across the network. If the network is down the changes will be lost.

  Best practice is to always write the changes to a trail that is local to the Extract. Another Extract is set up as a "data pump". It resides in the same location and reads data from the local trail and passes it across the network. In this way, the changes will not be lost if the network is down.

- **Replicat** - The Replicat process runs on the target system, reads the trail on that system, and applies the operations to the target database.

  > **Note:** Data Manipulation Language (DML) operations (adds, updates, deletes) are applied. Data Definition Language (DDL) operations are replicated only for the Oracle and Teradata databases.

- **Manager** - The Manager process is the administrative process of an Oracle GoldenGate instance. It controls all of the other Oracle GoldenGate processes in the instance. Part of its role is to generate information about critical monitoring events, which it passes to the agent.

Table 1 lists and describes the metrics used for the Extract and Replicat processes. Table 2 lists and describes the metrics used for the Manager process.

Table 1   Metrics Used for Extract and Replicat Processes

Metric	Description
Checkpoint Position	**Valid for Extract and Replicat**
	Shows a composite representation of the checkpoints that were persisted to disk most recently by Extract or Replicat. The value is captured by the monitoring agent when the attribute is published, right after the checkpoint gets persisted.
	Extract creates read and write checkpoints, and Replicat creates only read checkpoints. Each individual checkpoint within the composite Checkpoint Position consists of the RBA (relative bye address) of a record in the transaction log or trail (depending on the process and whether it is a read or write checkpoint) and the sequence number of the log or trail file that contains the record. There can be a series of read checkpoints in multiple data source log files (such as Extract from Oracle Real Application Cluster), and/or multiple write checkpoints such as in Extract configurations with multiple trail files.
	Valid values: Different databases use different representations of the position of a record in the log. Therefore, instead of numeric values, Checkpoint Position is published as a string of text characters encoded in UTF8. For each individual checkpoint within Checkpoint Position, the following are shown the way that they are returned by the GGSCI SEND <group-name> STATUS command:
	■ The values of the RBA (relative byte address)
	■ The file sequence number
	■ The time stamp
Delta Deletes	**Valid for Extract and Replicat**
	Shows the number, since the metric was last reported, of DELETE operations that were processed by the selected Oracle GoldenGate process in its current run session.
	Valid values: A positive integer
Delta Discards	**Valid for Extract and Replicat**
	Shows the number, since the metric was last reported, of DISCARD operations that were processed by the selected Oracle GoldenGate process in its current run session. The records are written to the discard file that is associated with the process.
	Valid values: Positive integer.
Delta Executed DDLs	**Valid for Extract and Replicat**
	Shows the count of executed data definition language (DDL) operations that were processed by the selected Oracle GoldenGate process since the last sample time.
	Valid values: Positive integer
Delta Ignores	**Valid for Extract**
	Shows the number of data manipulation language (DML) operations that through an error were configured to be ignored since the last sample time.
	Valid values: Positive integer
Delta Inserts	**Valid for Extract and Replicat**
	Shows the number of data manipulation language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process since the last sample.
	Valid values: A positive integer

Table 1   (Cont.) Metrics Used for Extract and Replicat Processes

Metric	Description
Delta Operation Per Second	**Valid for Extract and Replicat** Shows the number of operations (per second) that were processed by the selected Oracle GoldenGate process since the last sample. **Valid values:** A positive integer
Delta Operations	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) INSERT, UPDATE, DELETE, AND TRUNCATE operations that were processed by the selected Oracle GoldenGate process since the last sample. **Valid values:** A positive integer
Delta Row Fetch Attempts	**Valid for Extract** Shows the number of row fetch attempts that were processed by the selected Oracle GoldenGate process since the last sample. A fetch must be done occasionally to obtain row values when the information is incomplete or absent in the transaction log. **Valid values:** Positive integer
Delta Row Fetch Failures	**Valid for Extract** Shows the number of row fetch failures that were processed by the selected Oracle GoldenGate process since the last sample. A fetch must be done occasionally to obtain row values when the information is incomplete or absent in the transaction log **Valid values:** Positive integer
Delta Truncates	**Valid for Extract and Replicat** Shows the number of TRUNCATE operations that were processed by the selected Oracle GoldenGate process in its current run session since the last sample. **Valid values:** A positive integer
Delta Updates	**Valid for Extract and Replicat** Shows the number of UPDATE (including primary key updates) operations that were processed by the selected Oracle GoldenGate process in its current run session since the last sample. **Valid values:** A positive integer
End of File	**Valid for Extract and Replicat** Shows whether or not the selected process has reached the end of the input from its data source (transaction log or trail file). **Valid values:** TRUE (at end of file) or FALSE
Lag (sec)	**Valid for Extract and Replicat** Shows the time difference between the Last Operation Timestamp and the Last Processed Timestamp. This attribute represents the true lag between the Oracle GoldenGate process and its data source. This lag value should match the value that is returned from the GGSCI command SEND <group> GETLAG. **Valid values:** The lag time, in seconds
Last Checkpoint Timestamp	**Valid for Extract and Replicat** Shows the time when the last checkpoint was written by the process. **Valid values:** Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM ǀ PM}, for example: 01/14/2011 09:36:32 AM.

Table 1 (Cont.) Metrics Used for Extract and Replicat Processes

Metric	Description
Last Operation Timestamp	**Valid for Extract and Replicat** Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log. **Valid values:** Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example:01/14/2011 09:36:32 AM
Last Processed Timestamp	**Valid for Extract and Replicat** Shows the time when a valid record was returned to the selected process. For Extract, this time value is assigned when the record is processed after the container transaction commits (not the time when the record is read from the transaction log). For a Data Pump or Replicat, this time value is returned immediately, because all transactions in the trail are known to be committed. **Valid values:** Date time value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example: 01/14/2011 09:36:32 AM

Message	**Valid for Extract and Replicat**
	
	The message includes the following information:
	
	■ Message code number of an event message from the Oracle GoldenGate error log.
	
	    Valid values: The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651.
	
	■ Message Date: Timestamp of an event message from the Oracle GoldenGate log.
	
	    Valid values: A datetime value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format)
	
	■ Message Text: Text of an event message from the Oracle GoldenGate error log.
	
	    Valid values: A text string from the message.

Name	**Valid for Extract and Replicat** Name of the selected object. **Valid values:** Name of the object as displayed in the Oracle GoldenGate Monitor interface.
Seconds Since Last OGG Checkpoint	**Valid for Extract and Replicat** Time (in seconds) since the last OGG checkpoint.
Start Time	**Valid for Extract and Replicat** Shows the time that an Oracle GoldenGate component received its startup information after it has been created. **Valid values:** 64-bit Julian GMT time stamp in microseconds
Status	**Valid for Extract and Replicat** Shows the run status of the selected process. **Valid values:** Starting, Running, Stopped, Abended, or Aborted.
Total Deletes	**Valid for Extract and Replicat** Shows the total number of DELETE operations that were processed by the selected Oracle GoldenGate process in its current run session. **Valid values:** A positive integer

Table 1   (Cont.) Metrics Used for Extract and Replicat Processes

Metric	Description
Total Discards	**Valid for Extract and Replicat** Shows the total number of operations that were discarded by the selected Oracle GoldenGate process in its current run session. The records are written to the discard file that is associated with the process. **Valid values:** Positive integer.
Total Executed DDLs	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) operations that were processed by the selected Oracle GoldenGate process in its current run session. **Valid values:** Positive integer
Total Ignores	**Valid for Extract** Shows the total number of Data Manipulation Language (DML) operations that were ignored by the process in its current run session. Errors are included in the Total Ignores metric. **Valid values:** Positive integer
Total Inserts	**Valid for Extract and Replicat** Shows the total number of Data Manipulation Language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process in its current run session. The statistic reflects the total operations performed on all of the tables that are specified in the parameter file for that process. **Note:** If any tables are mapped to targets in the Extract configuration, the statistics will reflect the total operations for all of the targets. **Valid values:** A positive integer
Total Operations	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) INSERT, UPDATE, DELETE, and TRUNCATE operations that were processed by the selected Oracle GoldenGate process in this current run session. **Valid values:** A positive integer
Total Row Fetch Attempts	**Valid for Extract** Shows the total number of row fetches that the selected process performed in its current run session. A fetch must be done sometimes to obtain row values when the information is incomplete or absent in the transaction log. **Valid values:** Positive integer

Table 1 (Cont.) Metrics Used for Extract and Replicat Processes

Metric	Description
Total Row Fetch Failures	**Valid for Extract** Shows the total number of row fetches that the selected process was unable to perform in its current run session. **Valid values:** Positive integer
Total Truncates	**Valid for Extract and Replicat** Shows the total number of TRUNCATE operations that were processed by the selected Oracle GoldenGate process in its current run session. The statistic reflects the total operations performed on all of the tables that are specified in the parameter file for that process. Note: if any tables are mapped to targets in the Extract configuration, the statistics will reflect the total operations for all of the targets. **Valid values:** A positive integer
Total Updates	**Valid for Extract and Replicat** Shows the total number of UPDATE (including primary key updates) operations that were processed by the selected Oracle GoldenGate process in its current run session. The statistic reflects the total operations performed on all of the tables that are specified in the parameter file for that process. **Note**: If any tables are mapped to targets in the Extract configuration, the statistics will reflect the total operations for all of the targets. **Valid values:** A positive integer

Table 2 Metrics Used for the Manager Process

Metric	Description
Host Name	Shows the name of the host system. **Valid values**: The fully qualified DNS name of the host, or its IP address
Manager Port	Shows the port on which the Manager process of the Instance is running on its local system. The default port number is 7809, but a different port could be specified for this Manager and can be identified by viewing the Manager parameter file or by issuing the INFO MANAGER command in GGSCI (if Manager is running). **Valid values:** The port number for the Manager process, as specified in the Manager parameter file
Message	The message includes the following information: ■ Message code number of an event message from the Oracle GoldenGate error log. **Valid values:** The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651. ■ Message Date: Timestamp of an event message from the Oracle GoldenGate log. **Valid values:** A date-time value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format) ■ Message Text: Text of an event message from the Oracle GoldenGate error log. **Valid values:** A text string from the message.

Table 2   (Cont.) Metrics Used for the Manager Process

Metric	Description
Start Time	Shows the time that an Oracle GoldenGate component received its startup information after it has been created.
	Valid values: 64-bit Julian GMT time stamp in microseconds
Version	Indicates the version of Oracle GoldenGate that the selected Oracle GoldenGate Instance represents.
	Valid values: X.x.x (major, minor, and maintenance version levels), for example 11.1.1
Working Directory	Shows the directory that contains the Manager executable file for the selected Oracle GoldenGate Instance. This is the home directory of the Oracle GoldenGate installation.
	Valid values: The full path name of the directory

12 Troubleshooting

This section describes how to solve issues that may arise when using the Enterprise Manager Plug-in for Oracle GoldenGate.

12.1 Correcting ADFC Error on Windows 64-Bit Machines

When on the Enterprise Manager Plug-in for Oracle GoldenGate home page and selecting a target, it is possible that an ADFC exception can result on Windows 64-bit machines. To correct this issue, execute following command:

```
emctl load policies -plugin_id "oracle.fmw.gg" -policies_file
"middleware_home/plugins/goldengate_plugin_home
/metadata/security/jaznpolicy/jazn-data.xml"
```

Where *middleware_home* is where you installed your Oracle

12.2 Locating EM Log Files

The EM log files that help in troubleshooting the Enterprise Manager Plug-in for Oracle GoldenGate. This section details how to locate these log files.

Discovery related error details log file: `ogg_so_logs.log.0`
This file is in the $AGENT_STATE_DIR/sysman/emd/ directory. For example:

```
/scratch/prod/view_storage/prod_em4_2/work/agentStateDir/sysman/emd/ogg_so_l
ogs.log.0
```

EM Agent error details log file: `emagent.log`
This file is in the $AGENT_STATE_DIR/sysman/log/ directory. For example:

```
/scratch/prod/view_storage/prod_em4_2/work/agentStateDir/sysman/log/gcagent.log
```

Enterprise Manager Plug-in for Oracle GoldenGate user interface error details log file: `emoms.log`
This file is in the $T_WORK/ user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/sysman/log/ directory. For example:

```
$oracle/work/user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1
/sysman/log/emoms.log
```

Oracle Management Services log file: `EMGC_OMS1.out`

This file is in the `$T_WORK/user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/logs/` directory. For example:

```
/net/slczqy/scratch/prod/view_storage/prod_em4_2/work/user_projects/domain s/EMGC_
DOMAIN/servers/EMGC_OMS1/logs/EMGC_OMS1.out
```

13 Upgrading the Enterprise Manager Plug-in for Oracle GoldenGate

The Self Update feature allows you to expand the Enterprise Manager capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available using the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download.

See the "Updating Cloud Control" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for detailed steps for updating a plug-in.

13.1 Upgrading to the Newest Version

To upgrade the Enterprise Manager Plug-in for Oracle GoldenGate to the newest version:

1. Install the Oracle Enterprise Manager 12.1.0.4.0 release. For installation and upgrade instructions, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

2. (Optional) Oracle recommends that you backup your repository and export your first management server configuration prior to upgrading.

3. Log in to Enterprise Manager Cloud Control.

4. From the Setup menu, select **Extensibility**, then **Plug-ins**.

5. Locate the **Middleware** folder, and then click the adjacent arrow to expand it.

6. Select **Oracle GoldenGate**.

7. Select **Check Updates** then **OK** to confirm that you want to start a job that will find any updates.

   You are returned to the Plug-ins page.

8. Ensure that **Oracle GoldenGate** is selected and click **Check Updates** to retrieve the list of updates that generated.

9. Locate **Plug-in** in the list and select it.

10. Search for **GoldenGate** using the Search Description control to narrow the list of updates.

11. Select the update with the Available status then click **Download** to download the file.

12. Click **Select** in the Schedule Download dialog to immediately download the file.

13. Click **OK** in the Confirmation dialog once the file is successfully downloaded.

You are returned to the Plug-ins page.

14. Ensure that **Oracle GoldenGate** is selected.

15. Click **Deploy On**, then **Management Server** to deploy the update to your server.

    The Deploy Plug-ins on Management Servers: Plug-ins wizard starts.

16. Ensure that the version in the To Deploy column is correct and click **Next** to check the prerequisites.

17. Click **Next** then verify the repository SYS named credentials. You can add new credentials by selecting **New** and providing details for the new SYS credential.

18. Select the required check box indicating that you are aware that your repository should be backed up then click **Next**.

19. Review the deployment information for accuracy then click **Deploy** to continue.

    The deployment begins and you are advanced to the Confirmation step.

20. Click **OK** to exit the wizard and Enterprise Manager Cloud Control.

21. Log back in to Enterprise Manager Cloud Control.

22. From the Setup menu, select **Extensibility**, then **Plug-ins**.

23. Locate the **Middleware** folder, and then click the adjacent arrow to expand it.

24. Select **Oracle GoldenGate**.

    The On Management Server column displays the update version that you just deployed on it and the Management Agent with Plug-in column is zero (0).

25. Click **Deploy On**, then **Management Agent** to deploy the update to your agent.

    The Deploy Plug-in on Management Agent wizard starts listing the Oracle GoldenGate version and supported target versions.

26. Ensure the correct Oracle GoldenGate version is selected and click **Continue**.

27. Select the Management Agent you want to deploy then click **Continue**.

28. Ensure that are no errors from the prerequisite checks then click **Next**.

29. Review the deployment information for accuracy and ensure that the agent Status is a green arrow indicating that the agent is running, and then click **Deploy**.

    The deployment begins and you are advanced to the Confirmation step.

30. Click **Show Status** to exit the wizard and ensure that the deployment completes.

31. From the Setup menu, select **Extensibility**, then **Plug-ins**.

32. Locate the **Middleware** folder, and then click the adjacent arrow to expand it.

33. Select **Oracle GoldenGate**.

    The On Management Server column displays the update version that you just deployed on it and the Management Agent with Plug-in column is 1.

34. From the Targets menu, select **GoldenGate** to verify the deployment for both the servers and agents.

13.2 Upgrading While Retaining Existing Versions

You can import the Enterprise Manager Plug-in for Oracle GoldenGate from the EM command line interface (CLI) and update it on the Oracle Management Service without removing the existing version of the plug-in from the Oracle Management Server instance before upgrading to the latest version using the following steps:

1. Log in to Enterprise Manager Cloud Control.

2. From the Setup menu, select **Command Line Interface**. Follow the instructions on the page to download (if needed) and launch EM CLI.

3. Import the plug-in to Enterprise Manager Cloud Control with the following command:

   ```
   emcli import_update -file=your_opar_file_absolute_path -omslocal
   ```

4. Use the steps Section 13.1, "Upgrading to the Newest Version" to deploy your server and agent.

14 Known Issues

This section contains any known issues and resolutions.

14.1 Download Failure

When downloading the Enterprise Manager Plug-in for Oracle GoldenGate as previously described, you may encounter an error when the download it initiated. The output would look like this:

```
Downloading file in staging directory
/scratch/aime/WORKEM12104/mw2587/gcinst2587/em/EMGC_
OMS1/sysman/stage/034148593e245c3de050f00a82634a7f ...
Staging directory cleaned up.
Download failed: Exception: Error downloading file: Server returned invalid
response. Status Code = 200, Response Text = [OK | <results>
   <error>
       <id>10-013</id>
       <message>Choose valid parameters.</message>
   </error>
</results>
]
```

To solve this problem:

1. Clean up in the self update location. For example:

   ```
   Middlewarehome/gcinst/em/EMGC_OMS1/sysman/cache/selfupdate
   ```

2. Check whether Enterprise Manager is pointing to *staging* or *production*. If it is pointing to staging, then run the following command to point to production:

   ```
   emctl set property -sysman_pwd welcome1 -name oracle.sysman.emSDK.core.mos.mos_
   url -value https://support.oracle.com
   ```

15 Undeploying the Enterprise Manager Plug-in for Oracle GoldenGate

See the "Managing Plug-Ins" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for steps to undeploy the Enterprise Manager Plug-in for Oracle GoldenGate:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mngr.htm

16 Documentation Accessibility

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

Access to Oracle Support

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