

Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In Installation Guide

Release 12.1.0.2.0

E27804-05

September 2014

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

- [Oracle GoldenGate Description and Features](#)
- [Platforms Supported](#)
- [Versions Supported](#)
- [Prerequisites](#)
- [Downloading the Plug-in](#)
- [Deploying the Plug-in](#)
- [Creating the Oracle Wallet](#)
- [Configuring Oracle GoldenGate to Run with Oracle Enterprise Manager](#)
- [Starting the Oracle GoldenGate Instances](#)
- [Configure the Management Agent to Deploy the Plug-in](#)
- [Verifying and Validating the Plug-in](#)
- [Adding Instances for Monitoring](#)
- [Instance-Level Security](#)
- [Enabling Audit Logging](#)
- [Metrics](#)
- [Upgrading the Plug-in](#)
- [Undeploying the Plug-in](#)

1 Oracle GoldenGate Description and Features

The Enterprise Manager Plug-in for Oracle GoldenGate extends Oracle Enterprise Manager Cloud Control to support for monitoring and managing Oracle GoldenGate processes. By deploying the plug-in 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.
- 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.

1.1 What's New in Oracle GoldenGate Plug-in Release 12.1.0.2.0

The following features are included for Release 12.1.0.2.0:

- Control Extract and Replicate target types by:
 - Initiating start, stop, and kill commands
 - Editing parameter and include files.
- Access report and discard files to understand processing and diagnose problems.
- Audit logging enabled to collect process operations and file access. Messages are recorded into the server log.
- Partially view `ggserr.log` file content within Enterprise Manager Cloud Control and download the complete file to your local system.

2 Platforms Supported

The Oracle GoldenGate Plug-in supports monitoring of all platforms where both Oracle GoldenGate Release 11.2.1 or later and Oracle Enterprise Manager Cloud Control 12c agent or 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>

3 Versions Supported

The Oracle GoldenGate plug-in supports the following product versions:

- Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3) and later.
- Oracle GoldenGate versions supported include:
 - Oracle GoldenGate 12c (12.1.2.1.0) is supported and is the minimum version required to support START, STOP, KILL, and EDIT features.
 - Oracle GoldenGate 12c (12.1.2.0.1).
 - Oracle GoldenGate 12c (12.1.2.0.0).
 - Oracle GoldenGate 11g Release 2 (11.2.1.0.10) and later.

Note: Oracle GoldenGate 11g Release 2 (11.2.1.0.10) and later is supported. However, some features in the Oracle GoldenGate Plug-in user interface are only supported by newer versions of Oracle GoldenGate replication and the Oracle GoldenGate agent. If the feature is not supported, then the interface will not present the feature to the user.

For example, if the release of the Oracle GoldenGate agent does not support process control, then the user interface will not display START, STOP, and KILL buttons for processes being monitored by that agent.

4 Prerequisites

The following prerequisites must be met before you can use the Oracle GoldenGate plug-in:

- [Set Environment Variables to Point to the Java Installation](#)
- [Software Requirements](#)
- [Configure Each Oracle GoldenGate Instance](#)

4.1 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 bash shell):

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

4.2 Software Requirements

- The following must be installed and running:
 - Oracle Golden Gate 12c (12.1.2.0.1) and later or Oracle GoldenGate 11g Release 11.2.1.0.10 or 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 Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or later (Oracle Management Service and Oracle Management Agent)
- An Oracle Management Agent must be installed on each system hosting an Oracle GoldenGate instance that will be monitored.
- Verify that Java 7.0 or later 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
```

Output would look like this:

```
$ java -version
java version "1.7.0_25"
Java(TM) SE Runtime Environment (build 1.7.0_25-b16)
Java HotSpot(TM) 64-Bit Server VM (build 23.25-b01, 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, refer to the *Configuring Software Library* chapter in the *Enterprise Manager Cloud Control Administrator's Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/softwarelib.htm#BABHFAIH

4.3 Configure Each Oracle GoldenGate Instance

- For each Oracle GoldenGate instance:
 - 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.

- Create the Oracle Wallet to store passwords using the steps listed in [Creating the Oracle Wallet](#).
- 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](#)

- 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.

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* for details to download the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#CJGBEAHJ

6 Deploying the Plug-in

You can deploy plug-ins to an 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* for steps to deploy the plug-in:

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/plugin_mgr.htm#CJGCDHFG

For detailed instructions for deploying the Oracle GoldenGate plug-in, see Doc ID 1469108.1 in My Oracle Support:

<https://support.oracle.com>

6.1 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 Oracle GoldenGate plug-in from the downloads page:

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

The plug-in 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 plug-in 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 plug-in is deployed, an **Oracle GoldenGate** item will appear under **Targets** in Enterprise Manager Cloud Control.

7 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 Oracle GoldenGate installation directory.

Note: Oracle GoldenGate 12c (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 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 (**Note:** 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
```

8 Configuring Oracle GoldenGate to Run with Oracle Enterprise Manager

To configure your Oracle GoldenGate instance to work with the Oracle Enterprise Manager, you set property values for the hosts, ports, and monitoring type.

To configure monitoring for Oracle Enterprise Manager, navigate to the Oracle GoldenGate installation 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. This 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
```

9 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 GoldenGate Monitor 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.

10 Configure 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 Oracle GoldenGate plug-in:

1. In Enterprise Manager Cloud Control, click **Setup**, then **Security**, and finally **Preferred Credentials**.
2. On the Preferred Credentials page, select the **Host** target type and click **Manage Preferred Credentials**.
3. In the Host Preferred Credentials page, in the Target Credentials section, for the host that is running the Management Agent where the plug-in has to be deployed, specify the JAgent user name and password.
4. After setting the credentials, on the same page, click **Test**. If your test runs successfully, then your credentials are set correctly.
5. Run the OS Command job for the Management Agent where the plug-in has to be deployed:
 - Log in to Enterprise Manager Cloud Control.
 - Click **Enterprise**, then **Job**, and finally **Activity**.
 - In the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.
 - 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.

11 Verifying and Validating the Plug-in

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

http://docs.oracle.com/cd/E24628_01/doc.121/e24473/discovery.htm#CBAFHEHC

After waiting a few minutes for the plug-in 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.

12 Adding Instances for Monitoring

After successfully deploying the plug-in, 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. Highlight the Agent Host Name and click **Edit Parameters** to enter the information needed to connect to the Oracle GoldenGate Agent:
 - 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.
 - RMI port - The Remote Method Invocation port to use for the connection
4. Click **Ok**.

13 Instance-Level Security

Enterprise Manager provides instance-level security flexibility to provide target-level privileges to admin users. For example, if an Oracle GoldenGate (OGG) plug-in 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 finally **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 role:
 - **Properties:** enter the required credentials for the new user.
 - **Roles:** select one or more roles from the Available Roles list and click **Move** to add them to the new user. Once you have selected the roles, click **Next**.

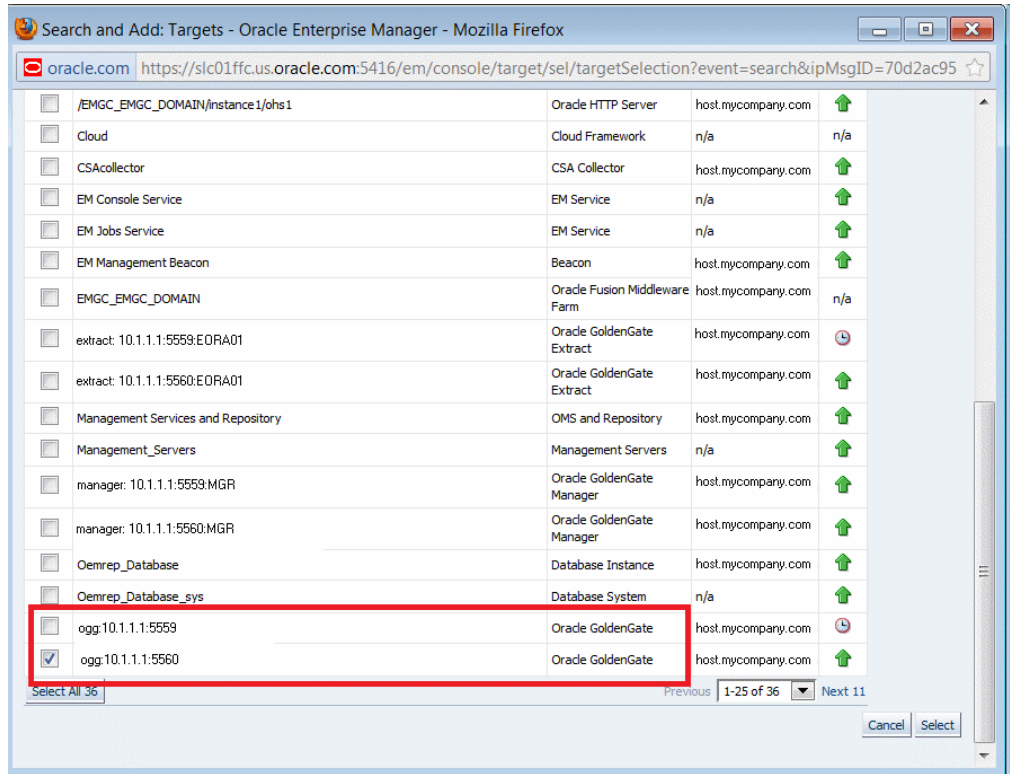
Note: Make sure that you do not select any 'ALL' roles in this step (for example, `EM_ALL_ADMINISTRATOR`, `EM_ALL_OPERATOR`, etc.). Otherwise, the user role you are creating will be entitled to all OGG instances.

3. On the Target Privileges page, scroll down to the Target Privileges section. Click **Add**.
4. 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 or extract/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. Once you have selected the instances, click **Select** to save the changes.

Figure 1 Select Oracle GoldenGate Targets



- After you click **Select** from the Add Targets window, the Target Privileges window will refresh to show your selection as shown in Figure 2. You should be able to see the selected Oracle GoldenGate instance in the list.

Figure 2 Updated Target Privileges

Target Privileges

Target Privileges give the Administrator the right to perform particular actions on targets. Table below shows privileges on the targets which would be granted to Use "Grant to All" button to assign privileges to all targets. Use "Grant to Selected" button to assign privileges to multiple targets. Privileges for the selected targ

Name Type

Select	Name	Type
<input type="checkbox"/>	ogg:10.1.1.1:5560	Oracle GoldenGate

- 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.

Privilege Name	Description
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.

7. Click **Continue**.
8. 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).
9. To test the instance-level security:
 - Log in as the newly created/edited user. 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](#)).
 - Log out and log in as root. From the Targets menu, click **GoldenGate**. Confirm that ALL the managed OGG instances are being shown up in this page (see [Figure 4](#)).

Figure 3 Instance-Level Security Test for New User

Oracle GoldenGate			
Status	All	Lag	All
Customize			
Target Name	Target Type	Status	Lag (Sec)
▽ 10.1.1.1:5560	Oracle GoldenGate	↑	
EORA01	Extract	↑	0
MGR	Manager	↑	
RORA01	Replicat	↑	0

Figure 4 Instance-Level Security Test for Root User

Oracle GoldenGate			
Status	All	Lag	All
Customize			
Target Name	Target Type	Status	Lag (Sec)
▼ 10.1.1.1:5559	Oracle GoldenGate		
EORA01	Extract		
MGR	Manager		
RORA01	Replicat		0
▼ 10.1.1.1:5560	Oracle GoldenGate		
EORA01	Extract		0
MGR	Manager		
RORA01	Replicat		0

14 Enabling Audit Logging

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

- [Enabling Audit Logging](#)
- [Searching and Viewing Audit Logs](#)

14.1 Enabling Audit Logging

To enable or disable an audit for a specific action, run the following commands from the oms/bin directory:

```
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:

- 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 discard file: OGG_VIEW_DISCARD
- 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 Oracle GoldenGate plug-in:

```
emcli update_audit_settings -operations_to_enable="OGG_START_TARGET;OGG_STOP_TARGET;OGG_KILL_TARGET;OGG_VIEW_REPORT;OGG_VIEW_DISCARD;OGG_VIEW_GGSERRLOG;OGG_EDIT_PARAM"
```

14.2 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

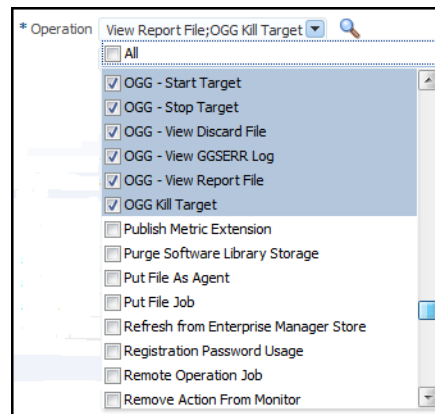
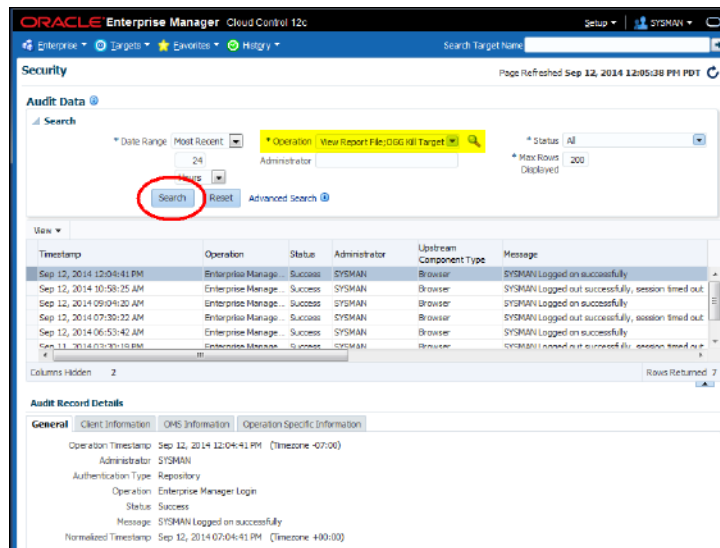


Figure 6 Audit Data Page




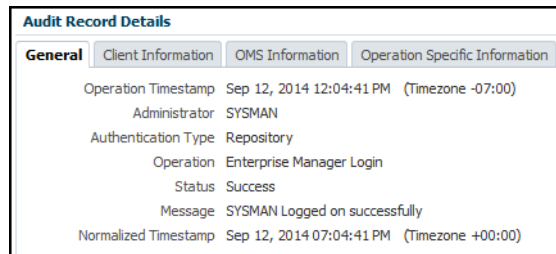
3. Check or uncheck the actions as needed. Audit logs are searchable only for the actions checked in this Operations drop-down menu. You can filter the results with various other criteria (date range, status, etc.) available on the Audit Data page.
4. Click the **Search** button .
5. To view the audit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

- "Configuring Auditing Framework" in the *Oracle® Enterprise Manager Cloud Control Getting Started Guide*:

http://docs.oracle.com/cd/E24628_01/install.121/e39876/configuring_auditing_fmwrk.htm

- "Configuring the Audit Data Export Service" in the *Oracle® Enterprise Manager Cloud Control Security Guide*:

http://docs.oracle.com/cd/E24628_01/doc.121/e36415/sec_features.htm#EMSEC12909

15 Metrics

The following processes are monitored by the Oracle GoldenGate plug-in:

- **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	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>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 byte 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.</p> <p>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:</p> <ul style="list-style-type: none"> ■ The values of the RBA (relative byte address) ■ The file sequence number ■ The time stamp
Delta Deletes	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
Delta Discards	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: Positive integer.</p>
Delta Executed DDLs	<p>Valid for Extract and Replicat</p> <p>Shows the count of executed data definition language (DDL) operations that were processed by the selected Oracle GoldenGate process since the last sample time.</p> <p>Valid values: Positive integer</p>
Delta Ignores	<p>Valid for Extract</p> <p>Shows the number of data manipulation language (DML) operations that through an error were configured to be ignored since the last sample time.</p> <p>Valid values: Positive integer</p>
Delta Inserts	<p>Valid for Extract and Replicat</p> <p>Shows the number of data manipulation language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process since the last sample.</p> <p>Valid values: A positive integer</p>

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

Metric	Description
Delta Operation Per Second	<p>Valid for Extract and Replicat</p> <p>Shows the number of operations (per second) that were processed by the selected Oracle GoldenGate process since the last sample.</p> <p>Valid values: A positive integer</p>
Delta Operations	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
Delta Row Fetch Attempts	<p>Valid for Extract</p> <p>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.</p> <p>Valid values: Positive integer</p>
Delta Row Fetch Failures	<p>Valid for Extract</p> <p>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</p> <p>Valid values: Positive integer</p>
Delta Truncates	<p>Valid for Extract and Replicat</p> <p>Shows the number of TRUNCATE operations that were processed by the selected Oracle GoldenGate process in its current run session since the last sample.</p> <p>Valid values: A positive integer</p>
Delta Updates	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
End of File	<p>Valid for Extract and Replicat</p> <p>Shows whether or not the selected process has reached the end of the input from its data source (transaction log or trail file).</p> <p>Valid values: TRUE (at end of file) or FALSE</p>
Lag (sec)	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: The lag time, in seconds</p>
Last Checkpoint Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when the last checkpoint was written by the process.</p> <p>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.</p>

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

Metric	Description
Last Operation Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log.</p> <p>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</p>
Last Processed Timestamp	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>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</p>
Message	<p>Valid for Extract and Replicat</p> <p>The message includes the following information:</p> <ul style="list-style-type: none"> ■ 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	<p>Valid for Extract and Replicat</p> <p>Name of the selected object.</p> <p>Valid values: Name of the object as displayed in the Oracle GoldenGate Monitor interface.</p>
Seconds Since Last OGG Checkpoint	<p>Valid for Extract and Replicat</p> <p>Time (in seconds) since the last OGG checkpoint.</p>
Start Time	<p>Valid for Extract and Replicat</p> <p>Shows the time that an Oracle GoldenGate component received its startup information after it has been created.</p> <p>Valid values: 64-bit Julian GMT time stamp in microseconds</p>
Status	<p>Valid for Extract and Replicat</p> <p>Shows the run status of the selected process.</p> <p>Valid values: Starting, Running, Stopped, Abended, or Aborted.</p>
Total Deletes	<p>Valid for Extract and Replicat</p> <p>Shows the total number of DELETE operations that were processed by the selected Oracle GoldenGate process in its current run session.</p> <p>Valid values: A positive integer</p>

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

Metric	Description
Total Discards	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: Positive integer.</p>
Total Executed DDLs	<p>Valid for Extract and Replicat</p> <p>Shows the total number of Data Definition Language (DDL) operations that were processed by the selected Oracle GoldenGate process in its current run session.</p> <p>Valid values: Positive integer</p>
Total Ignores	<p>Valid for Extract</p> <p>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.</p> <p>Valid values: Positive integer</p>
Total Inserts	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
Total Operations	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
Total Row Fetch Attempts	<p>Valid for Extract</p> <p>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.</p> <p>Valid values: Positive integer</p>

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

Metric	Description
Total Row Fetch Failures	<p>Valid for Extract</p> <p>Shows the total number of row fetches that the selected process was unable to perform in its current run session.</p> <p>Valid values: Positive integer</p>
Total Truncates	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>
Total Updates	<p>Valid for Extract and Replicat</p> <p>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.</p> <p>Valid values: A positive integer</p>

Table 2 Metrics Used for the Manager Process

Metric	Description
Host Name	<p>Shows the name of the host system.</p> <p>Valid values: The fully qualified DNS name of the host, or its IP address</p>
Manager Port	<p>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).</p> <p>Valid values: The port number for the Manager process, as specified in the Manager parameter file</p>
Message	<p>The message includes the following information:</p> <ul style="list-style-type: none"> ■ Message code number of an event message from the Oracle GoldenGate error log. <p>Valid values: The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651.</p> ■ Message Date: Timestamp of an event message from the Oracle GoldenGate log. <p>Valid values: A date-time value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format)</p> ■ Message Text: Text of an event message from the Oracle GoldenGate error log. <p>Valid values: A text string from the message.</p>

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

16 Upgrading the Plug-in

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

To upgrade the Oracle GoldenGate plug-in to the newest version:

1. Log in to Enterprise Manager Cloud Control.
2. From the Setup, select **Extensibility**, then **Plug-ins**.
3. From the Actions menu, select **Check Updates**, which should download the new version.

Note: If you experience downloading problems, see [Known Issue: Download Failure](#).

4. Select the plug-in from the list and click **Deploy On**, then **Management Agent**.
5. Once deployed to the Management agent, select the plug-in from the list and click **Deploy On**, then **Management Server**.
6. Once deployed to both Management Agent and Management Server, click the Refresh icon to reload the page. Verify that the latest version of the plug-in is installed.

You can also import the Oracle GoldenGate plug-in from the Enterprise Manager CLI (EM CLI):

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. Once you have imported the plug-in, you can now update it on the Oracle Management Service without removing the existing version of a plug-in from the OMS instance before upgrading to the latest version. The steps are same to deploy the plug-in from Cloud Control as described above.

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

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

16.1 Known Issue: Download Failure

When downloading the Oracle GoldenGate plug-in as described above, 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
```

17 Undeploying the Plug-in

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

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

18 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 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.

Copyright © 2014, 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 is software or related documentation that 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 America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware 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.