

Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-in Installation Guide

Release 13c (13.1.1.0.0)

E68921-01

February 2016

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:

- [Section 1, "Introduction to Enterprise Manager Plug-in for Oracle GoldenGate"](#)
- [Section 2, "Preparing to Deploy"](#)
- [Section 3, "Deploying the Plug-in"](#)
- [Section 4, "Creating the Oracle Wallet"](#)
- [Section 5, "Configuring Oracle GoldenGate to Run with Oracle Enterprise Manager"](#)
- [Section 6, "Starting the Oracle GoldenGate Instances"](#)
- [Section 7, "Creating SSH Key Named Credentials"](#)
- [Section 8, "Setting the Preferred Credentials"](#)
- [Section 9, "Monitoring High Availability Feature"](#)
- [Section 10, "Verifying and Validating the Plug-in Deployment"](#)
- [Section 11, "Adding Instances for Monitoring"](#)
- [Section 12, "Configuring Instance-Level Security"](#)
- [Section 13, "Using the Enterprise Manager Plug-in for Oracle GoldenGate"](#)
- [Section 14, "Troubleshooting"](#)
- [Section 15, "Upgrading"](#)
- [Section 16, "Known Issues"](#)
- [Section 17, "Undeploying the Enterprise Manager Plug-in for Oracle GoldenGate"](#)
- [Section 18, "Documentation Accessibility"](#)

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 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.
- Start, stop, and kill individual processes.
- Modify existing configuration files.
- View error logs, Oracle GoldenGate error logs, report files, and discard files.
- Audit user access of privileged EM Plug-in features and instance level security for user creation.

2 Preparing to Deploy

This section contains the following topics:

- [Section 2.1, "Supported Platforms"](#)
- [Section 2.2, "Supported Releases"](#)
- [Section 2.3, "Meeting the Prerequisites"](#)

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 12c agent and later instances can run.

The system monitoring plug-in for Oracle GoldenGate is not supported on the following platforms:

- HP NonStop
- IBM System z
- IBM z/OS (supported with change in OEM and CORE configuration)
- IBM i (AS400)(supported with change in OEM and CORE configuration)

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 13c Release 1 (13.1.0.0) and later.
- Oracle GoldenGate versions supported include:
 - Oracle GoldenGate Monitor Agent 12c (12.1.3.0.4) and later is required 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 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 omsOracleHome/plugins/oracle.fmw.gg.oms.plugin_13.1.1.0.0/metadata/versionmgmt/feature_version.xml file as follows:

```
<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 12c (12.1.2.0.1) and later or Oracle GoldenGate 11g Release 11.2.1.0.17 and later to support monitoring by Enterprise Manager Cloud Control.
 - Oracle GoldenGate Monitor Agent 12c (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 12c installation location.
 - Oracle Enterprise Manager (OEM) Cloud Control 13c Release 1 (13.1.0.0) and later (Oracle Management Service and Oracle Management agent).
- An Oracle Management agent must be installed on each system to be monitored which are hosting Oracle GoldenGate instances.

- Verify that Java JRE 1.7.0_80 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 data store used to store monitoring data.
 - Start the monitor or jAgent agent that collects monitoring data to pass to the OEM 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 "Downloading Plug-Ins" chapter in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details to download the plug-in.

3 Deploying the Plug-in

You can deploy plug-ins to any 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* for steps to deploy the plug-in.

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. Deploy the Plug-in on Management server. 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. Click **Oracle GoldenGate** then click **Deploy on** and finally click **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.

3.2 Deploying the Plug-in to Management Agent

Follow the steps to deploy the plug-in to management agent once you have completed the plug-in deployment on management server.

1. Click **Setup** in the upper right corner, then click **Extensibility**, and finally **Plug-ins**.

2. In the Plug-ins page, expand the **Middleware** folder.
3. Click **Oracle GoldenGate**, then click **Deploy on**, and finally click **Management Agent...** to start the deployment process.
4. Select the version of plug-in and click on **Continue**.
5. Select all the EM Agents where you want to install plug-in.
6. Click on **Continue** and **Deploy**.

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 OGG_AGENT_ORA_HOME 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 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 monitor or jAgent 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 data store that will persist monitoring data:

```
GGSCI> CREATE DATASTORE
```

4. If this is the initial start of Oracle GoldenGate since monitoring has been enabled, create the sub-directories using the GGSCI> CREATE SUBDIRS command.

5. 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
```

6. Start the Oracle GoldenGate Manager process:

```
GGSCI> START MANAGER
```

7. 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.

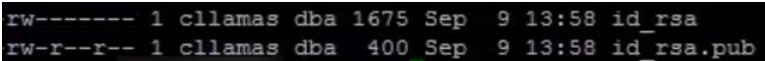
7 Creating SSH Key Named Credentials

Follow the steps below to create SSH Key named credentials:

1. Generate keys on your server using the ssh-keygen utility.

A directory with the name .ssh is created and two files are included in the directory.

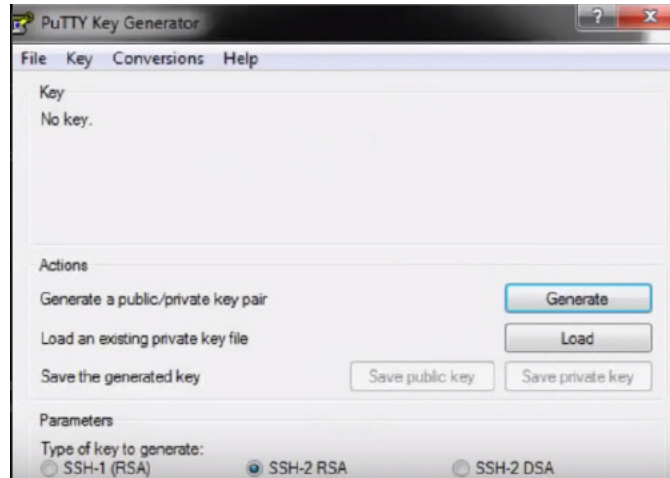
Figure 1 Files Created in .ssh Directory



```
rw----- 1 cllamas dba 1675 Sep  9 13:58 id_rsa
rw-r--r-- 1 cllamas dba  400 Sep  9 13:58 id_rsa.pub
```

2. Use the client (for example, Putty Key Generator) to generate the Private key and the Public key.

Figure 2 Generating Keys



3. Save both the Public and the Private key.
4. In the Putty Key Generator dialog use the **Export OpenSSH Key** under **Conversions** to convert the key.
5. Save the converted key.
6. In the Putty Key Generator dialog, select the OpenSSH key, copy, and paste the contents in a file called **authorized keys** using the command `vi authorized keys`

Figure 3 Selecting the Public Key to Copy

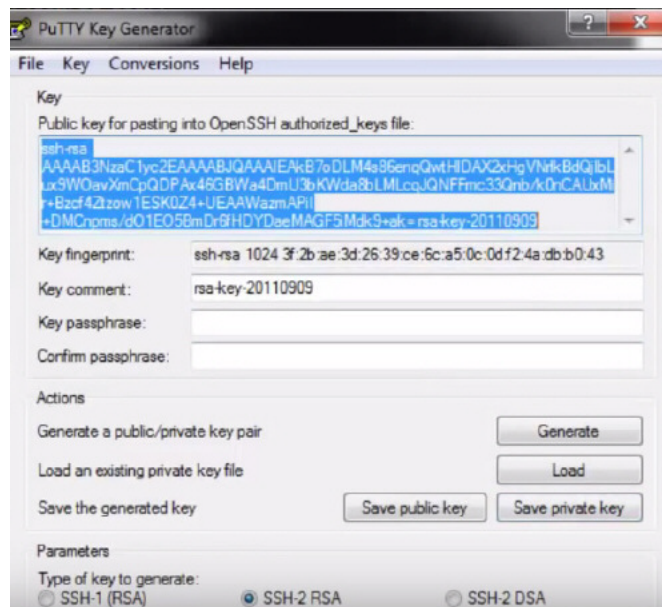


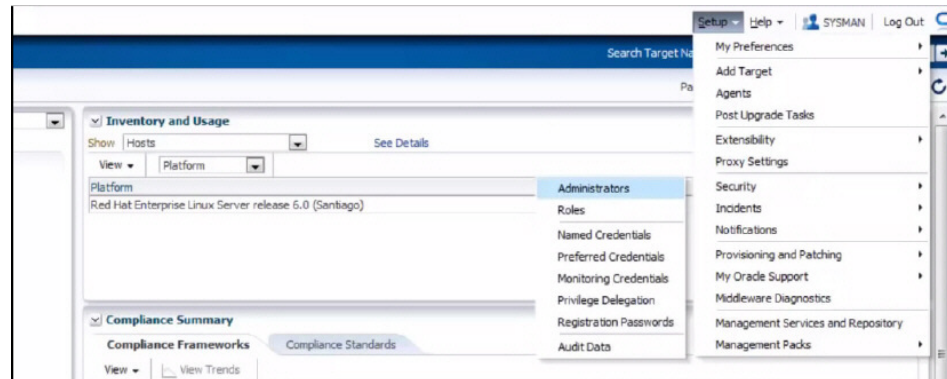
Figure 4 Creating authorized key File

```
$ vi authorized keys
```

7. Save the file.

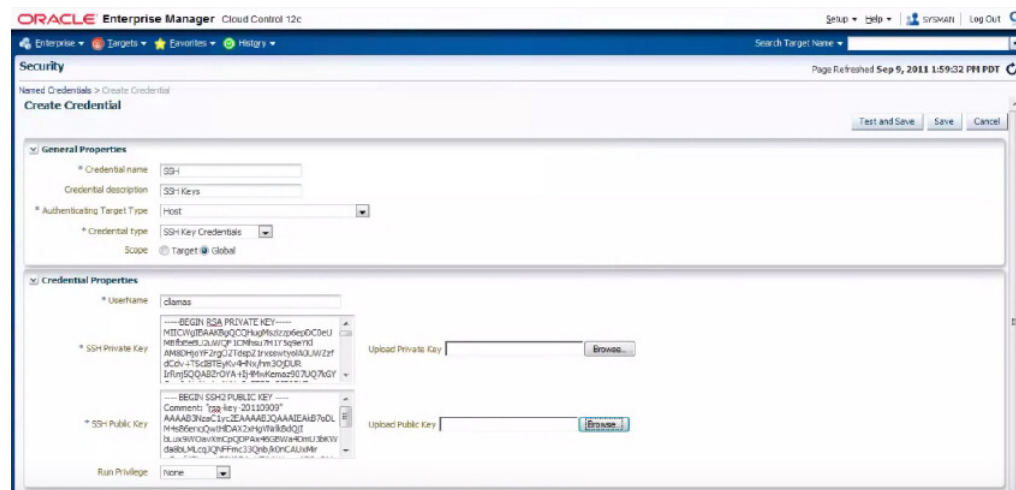
8. Use the Putty agent to load the key that you just generated.
9. You can now login to the server using the key.
10. To create a named credentials, In the EnterPrise Manager Cloud Control, from the **Setup** menu click **Security** and then **Named Credentials**.

Figure 5 Setting up Named Credentials



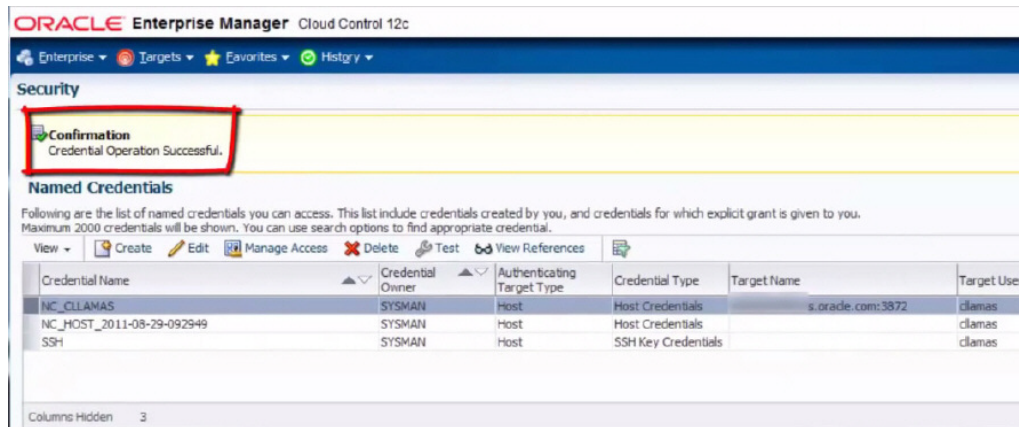
11. Click **Create** in the Named Credentials dialog box.
12. Select **Host** in the drop down for Authenticating Target Type.
13. Select **SSH Key Credentials** in the drop down for Credential type.
14. Select **Global** as scope if the same SSH key is used for all the targets.
15. In the Credential Properties section, upload the open SSH public key and the private key.

Figure 6 Uploading Private and Public Keys



16. Click on the **Add Grant** button and set the access privilege for the user.
17. Click on the **Change Privilege** button and in the dialog box that is displayed, select Full from the drop down list.
18. Click the **Test And Save** button to check the connection.
19. A confirmation message is displayed if the operation is successful.

Figure 7 Confirmation Dialog

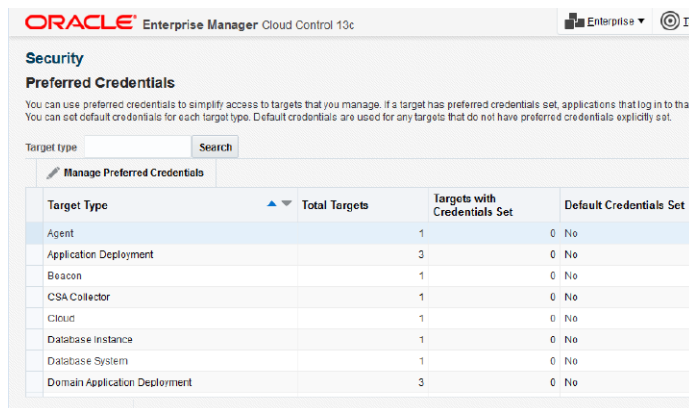


8 Setting the Preferred Credentials

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, use the search box to narrow down the Target Type, or scroll down to select a Target Type from the list. Once selected, click on the Manage Preferred Credentials button below the search box.

Figure 8 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 `myhost` 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. To Set the Administration credential, the username is added in the `config.properties` file of Oracle GoldenGate instance and the password is defined at the time of the Oracle Wallet creation.

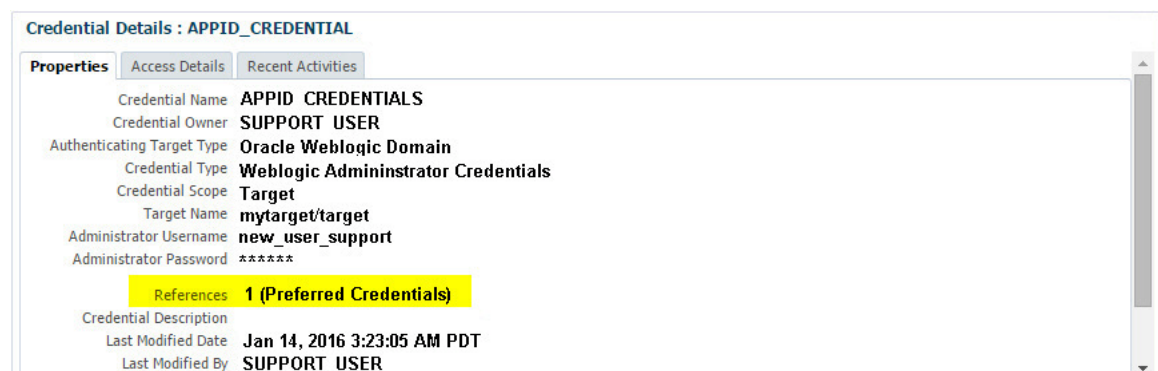
Note: If Oracle GoldenGate Core setup is done on a different system which is not running the OMS and EM Agent, you need to provide the OMS host credential for `host credential set`, and not the Oracle GoldenGate Core system credentials.

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.

Figure 9 Preferred Credentials Configured



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.

Repeat host credentials for the other GoldenGate target types:

- Oracle GoldenGate Manager
- Oracle GoldenGate Extract
- Oracle GoldenGate Replicat

9 Monitoring High Availability Feature

The following procedure explains the monitoring of High Availability features for Oracle GoldenGate Management Pack. For the High Availability feature to properly function with Oracle GoldenGate plug-in, virtual IP (not the physical IP) of the Oracle GoldenGate host should be provided at the time of Oracle GoldenGate target discovery.

There can be two scenarios where High Availability is required:

1. Oracle GoldenGate instance is failed over from one node to another in the cluster. In this scenario, the existing **Master** Agent will continue monitoring the Oracle GoldenGate instance in a seamless manner and **Host Name** parameter in Oracle GoldenGate Manager page will display physical host name of the new node.
2. Current Master agent stops functioning. In such scenario, any of the other EM Agent which is currently running, should have been marked as **Slave** for this Oracle GoldenGate instance. When the current **Master** agent stops functioning, any of these **Slave** agents will be assigned as **Master** for the Oracle GoldenGate instance, and monitoring will continue.

This procedure uses both the Oracle Enterprise Manager Cloud Control portal and a console connection.

1. Start Oracle Enterprise Manager Cloud Control.
2. Login using the provided credentials. The user must have 'sysman' privilege.
3. In the page that is displayed, click **Manage Cloud Control** under Setup menu and then click **Agents**.

All the agents are listed under Agents page.

4. Click **GoldenGate** under **Targets** menu.
5. In the GGSCI console, type the command `info all` to view the current status of the processes. All the processes are displayed as running.
6. From the **Setup** menu click **Add target** and then **Configure Auto Discovery**. Select the host and click on **Discovery Modules** to provide credentials details by selecting Goldengate discovery. See, [Appendix 11](#)
7. Click **Discovered Targets** for a particular Agent Host Name. The dialog box lists all the Targets on Hosts, select a particular host. In the next screen click **Promote** to promote the particular process. A Confirmation dialog is displayed when the promotion process is completed.
8. In the **Manage Agents** screen, click **Submit**. A confirmation dialog box is displayed.

This page is displayed after successful completion of promotion of the targets. It includes the recently promoted Oracle GoldenGate instance with a list of all EM agents where Oracle GoldenGate plug-in is deployed.

The agent through which these targets were discovered and promoted, is shown as **Master** for this Oracle GoldenGate instance. All other agents are marked as **None**, which means that they are not associated with this Oracle GoldenGate instance. You can select any number of these agents as **Slave**, and click on **Submit** button which saves the changes.

If you do not want to make any such changes, you can click the **Oracle GoldenGate Home** button and navigate to the GoldenGate plug-in home page.

9. Click **GoldenGate** under **Targets** menu.
10. Select the **Data Pump** process.
11. In the **Extract:DPUMP** screen, click on the **Stop** button. Click **Yes** in the confirmation dialog to stop the process. Click **Close** on the process complete dialog box.
12. From the **Targets** menu click **GoldenGate**. The **DPUMP** process is displayed as stopped. Click on the **Refresh** button to refresh the screen if the process is still shown as running.
13. Click on the **DPUMP** process. In the next screen **Extract:DPUMP**, click on the **Start** button. Select **Normal** on the confirmation dialog box and click **Start**.
14. Click **Close** when the process complete dialog is displayed.
15. Click **OGG Home** to go back to the home page. All the processes are displayed as running.
16. Click on the **Manage Agents** tab. Under the Agents name, one is displayed as **Master** and the other is displayed as **None**. Use the drop down list and change the Status from **None** to **Slave**.
17. Click **Submit**. In the confirmation dialog box click **OK**.
18. From the **Setup** menu click **Manage Cloud Control** and then **Agents**. In the **Agents** screen that is displayed, click **Targets**. In the next screen click **OGG Home**.
All the processes are displayed as running.
19. Use the console to stop the running processes using the `stop *` command.
20. Next, stop the **JAgent** process using the `stop jagent` command.
21. Type **Y** to confirm the action.
22. Stop the **MANAGER** process using the `stop manager` command.
23. Type **Y** to confirm the action.
24. In the console, use the command `info all` to view the current status of the processes. All the processes are displayed as stopped.
25. Next, start the **MANAGER** process using `start manager` command.
26. Start the other processes using `start *` command.
27. Start the **JAgent** process using `start jagent` command.
28. In the management portal, refresh the **OGG Home** tab to view the updated status of the processes. It can take few moments for the screen to update. All the processes are displayed as running.

29. Click on the **DPUMP** process in the **Extract:DPUMP** screen and stop the process. Click **Yes** in the confirmation dialog box. Click **Close** in the process complete dialog box.
30. Use the console to view the status of all the processes `info all`.
All the processes are shown as running.
31. In the Enterprise Manager portal, Click on **OGG Home**. All the processes are shown as running.
32. Using the console, stop the running processes through the console using the `stop *` command.
33. Stop the **JAgent** and **MANAGER** process as mentioned previously. Type **Y** to confirm the actions.
34. Use the command `info all` to view the current status of the processes. All the processes are displayed as stopped.
35. Start the processes using `start *` command.
36. Start the **MANAGER** and **JAgent** process.
37. In the console, type the command `info all` to view the current status of the processes. All the processes are displayed as running.
38. In the portal, click on the **Refresh** button to update the status of the processes. All the processes are displayed as running.
39. In the **OGG Home** Tab, click the **DPUMP** process.
40. In the **Extract:DPUMP** screen, click **Stop**. Click **Yes** in the confirmation dialog. Click **Close** to Complete the process.

10 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.

11 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, click **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, click **Add Target**, then click **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*.

12 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, click **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**.

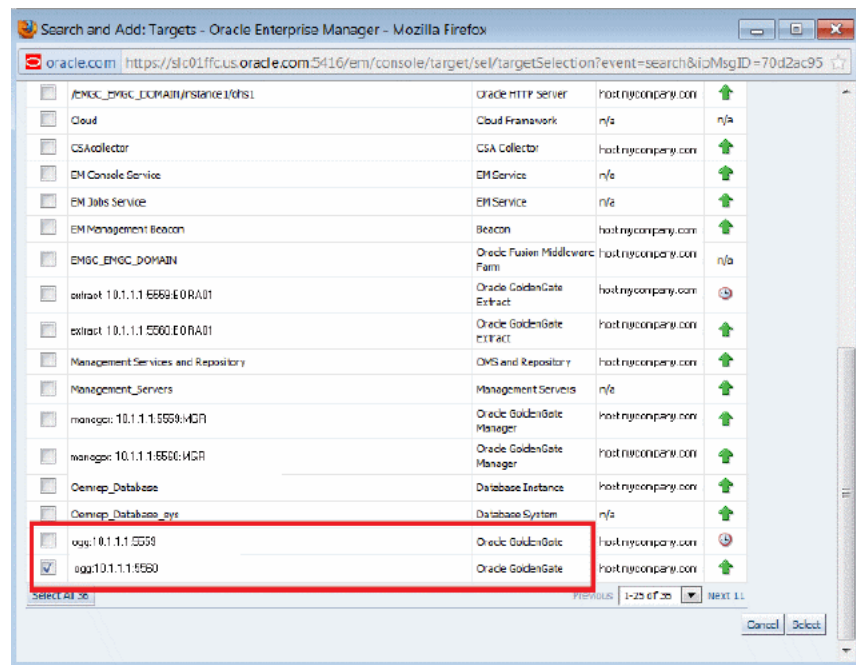
These two roles are required for full functionality and multi-version support.

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 10 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 10 Selecting 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 11.

Figure 11 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 target

Name Type

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

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 12](#)).

Figure 12 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

- 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 13](#)).

Figure 13 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

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

13 Using the Enterprise Manager Plug-in for Oracle GoldenGate

This section contains these topics:

- [Section 13.1, "Using Audit Logging"](#)
- [Section 13.2, "Monitoring Metrics"](#)
- [Section 13.3, "Sending Email for Metric Alerts"](#)

13.1 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:

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

13.1.1 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 discard file: OGG_VIEW_DISCARD
- View `ggstderr.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_DISCARD;OGG_VIEW_GGSERRLOG;OGG_
EDIT_PARAM"
```

13.1.2 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 click **Security**, and finally **Audit Data**.
2. On the Audit Data page (Figure 15), click the **Operations** drop-down menu and look for operations starting with **OGG**. Figure 14 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 14 Selecting Oracle GoldenGate Operations to Audit

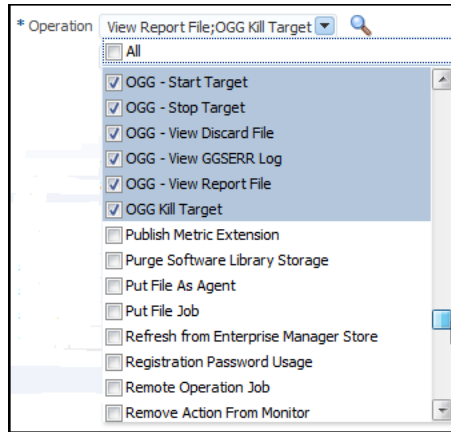



Figure 15 Audit Data Page

Timestamp	Operation	Status	Administrator	Upstream Component Type	Message	Session
Feb 2, 2016 10:30:22...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	AC2DC338756CA76
Jan 30, 2016 01:36:59...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	9EB60A8CC7D4AE1
Jan 30, 2016 01:04:53...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	71F224AB1A407715
Jan 29, 2016 10:25:49...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	5A8AD81ADA7B99F
Jan 29, 2016 03:30:21...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	9EB60A8CC7D4AE1
Jan 29, 2016 12:10:45...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	5A8AD81ADA7B99F
Jan 29, 2016 10:47:19...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	71F224AB1A407715

Audit Record Details

General | Client Information | OMS Information | Operation Specific Information

Operation Timestamp: Feb 2, 2016 10:30:22 AM (Timezone -08:00)
 Administrator: SYSMAN
 Authentication Type: Repository
 Operation: Enterprise Manager Login
 Status: Success
 Message: SYSMAN Logged on successfully
 Normalized Timestamp: Feb 2, 2016 06:30:21 PM (Timezone +09:00)

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 16). 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 16 Audit Record Details

Audit Record Details	
General	Client Information OMS Information Operation Specific Information
Operation Timestamp	Sep 12, 2014 12:04:41 PM (Timezone -07:00)
Administrator	SYSMAN
Authentication Type	Repository
Operation	Enterprise Manager Login
Status	Success
Message	SYSMAN Logged on successfully
Normalized Timestamp	Sep 12, 2014 07:04:41 PM (Timezone +00:00)

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*.
-

13.2 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	<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 <i>SEND group-name STATUS</i> 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 <code>SEND group GETLAG</code>.</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>
Start Time	<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>
Version	<p>Indicates the version of Oracle GoldenGate that the selected Oracle GoldenGate Instance represents.</p> <p>Valid values: X.x.x (major, minor, and maintenance version levels), for example 11.1.1</p>
Working Directory	<p>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.</p> <p>Valid values: The full path name of the directory</p>

13.3 Sending Email for Metric Alerts

You can configure Enterprise Manager to send email to administrators when a metric alert threshold is reached. See https://docs.oracle.com/cd/E24628_

01/doc.121/e24473/incident_mgmt.htm#EMADM14304 for more information on how to set up an email alert.

14 Troubleshooting

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

14.1 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

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

15 Upgrading

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.

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 "Downloading Plug-Ins" chapter at http://docs.oracle.com/cd/E63000_01/EMADM/plugin_mgr.htm#EMADM13097 in the *Oracle Enterprise Manager Cloud Control Administrator's Guide* at http://docs.oracle.com/cd/E63000_01/EMADM/ for details on how to download the plug-in.

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.

15.1 Upgrading to the Newest Version

The following example demonstrates how to upgrade the Enterprise Manager Plug-in for Oracle GoldenGate from version 12.1.0.4.0 to the latest version:

1. Copy the emkey using the command `OMS_HOME/bin/emctl config emkey -copy_to_repos`.
2. Stop the OMS using the command `OMS_HOME /bin/emctl stop oms -all`
3. Download the Enterprise Manager Plug-in for Oracle GoldenGate version 13.1
4. Find the plug-in location at `/em_linux64.bin -invPtrLoc OMS_HOME/oraInst.loc PLUGIN_LOCATION=/net/machine name/scratch/user/opar`.
5. In the dialog box, deselect the check box and click **Next**. Click Yes in the confirmation box that appears.

Figure 17 Oracle Enterprise Manager Cloud Control 13c Installation Step 1

The screenshot shows the 'My Oracle Support Details' window for Oracle Enterprise Manager Cloud Control 13c. The title bar indicates 'Step 1 of 10'. On the left, a navigation pane lists steps: My Oracle Support Details (selected), Software Updates, Prerequisite Checks, Installation Types, Installation Details, Configuration Details, Shared Location Details, Review, Install Progress, and Finish. The main area prompts the user to provide an email address for security updates. It includes a text field for 'Email:' with a note 'Easier for you if you use your My Oracle Support email address/username.' Below this is a checkbox labeled 'I wish to receive security updates via My Oracle Support' and a text field for 'My Oracle Support Password:'. At the bottom, there are buttons for '< Back', 'Next >', 'Install', and 'Cancel'. A 'Help' button is located in the bottom left corner.

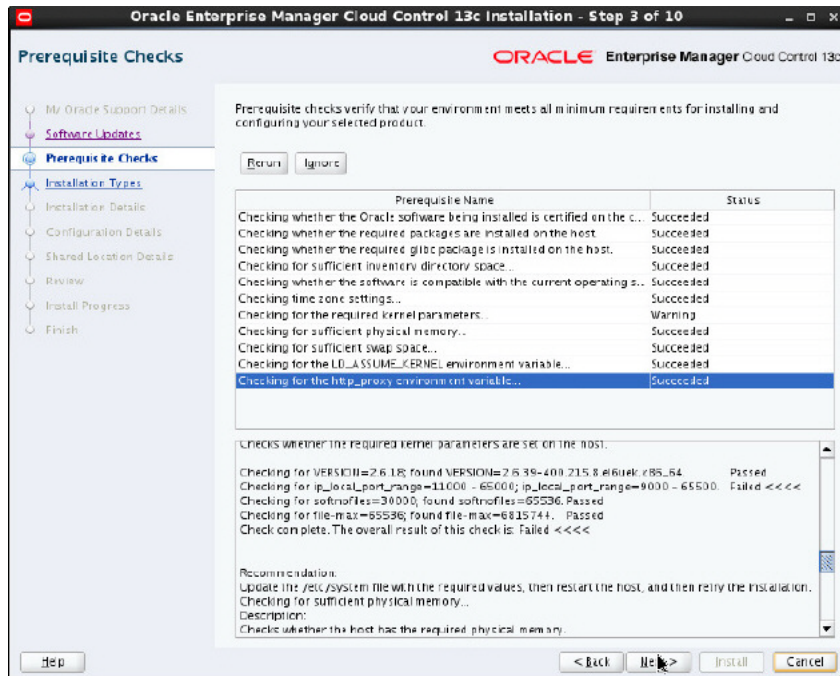
6. Click **Skip** in the dialog box that appears and click **Next**.

Figure 18 Oracle Enterprise Manager Cloud Control 13c Installation Step 2

The screenshot shows the 'Software Updates' window for Oracle Enterprise Manager Cloud Control 13c. The title bar indicates 'Step 2 of 10'. The navigation pane on the left is the same as in Step 1, with 'Software Updates' now selected. The main area shows three radio button options: 'Skip' (selected), 'Search for Updates (Prerequisites, Critical Patches, Interim Patches, Plug-ins, etc.)', and 'Local Directory'. The 'Skip' option is highlighted with a yellow box. The 'Search for Updates' option has sub-options for 'Local Directory' and 'My Oracle Support (Requires Internet Connection)'. The 'My Oracle Support' option includes text fields for 'User Name' and 'Password', and a 'Search for Updates' button. At the bottom, there are buttons for '< Back', 'Next >', 'Install', and 'Cancel'. A 'Help' button is in the bottom left corner. A 'Messages:' section is visible at the bottom of the main area.

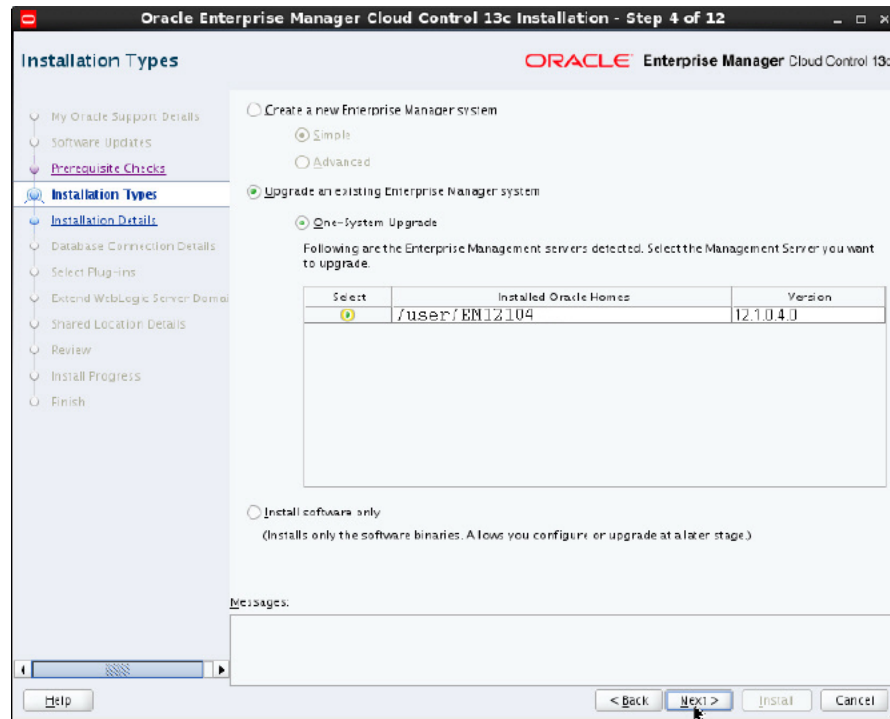
7. Click **Next** in the dialog box that appears.

Figure 19 Oracle Enterprise Manager Cloud Control 13c Installation Step 3



8. Select **One System Upgrade** in the dialog box that appears and click **Next**.

Figure 20 Oracle Enterprise Manager Cloud Control 13c Installation Step 4



9. Enter the new **Middleware Home Location** in the dialog box that appears and click Next.

Figure 21 Oracle Enterprise Manager Cloud Control 13c Installation Step 5

The screenshot shows the 'Installation Details' window for Oracle Enterprise Manager Cloud Control 13c. The window title is 'Oracle Enterprise Manager Cloud Control 13c Installation - Step 5 of 12'. On the left, a navigation pane lists the installation steps: My Oracle Support Details, Software Updates, Prerequisite Checks, Installation Types, **Installation Details**, Database Connection Details, Select Plug-ins, Extend WebLogic Server Domain, Shared Location Details, Review, Install Progress, and Finish. The main area contains two input fields: 'Middleware Home Location' with the value '/u002/EM131000' and a 'Browse...' button, and 'Host Name' with the value 'myhost.us.example.com'. At the bottom, there is a 'Messages' section and a row of buttons: 'Help', '< Back', 'Next >', 'Upgrade', and 'Cancel'.

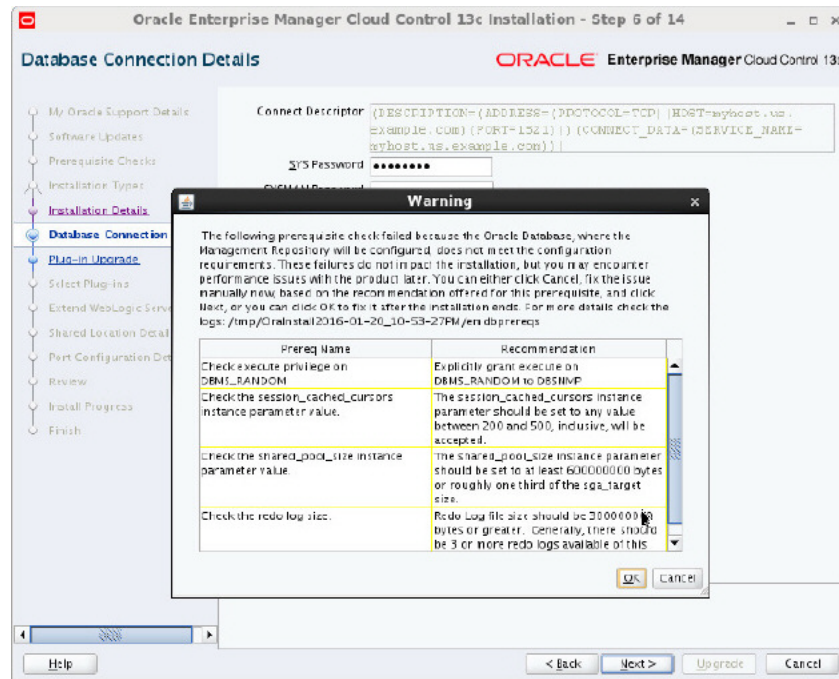
10. Enter the database password and Click Next.

Figure 22 Oracle Enterprise Manager Cloud Control 13c Installation Step 6

The screenshot shows the 'Database Connection Details' window for Oracle Enterprise Manager Cloud Control 13c. The window title is 'Oracle Enterprise Manager Cloud Control 13c Installation - Step 6 of 12'. The navigation pane on the left is the same as in Step 5, but 'Database Connection Details' is now selected. The main area contains a 'Connect Descriptor' text area with the value '(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=myhost.us.example.com)(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=my103c.us.example.com))'. Below this are two password fields: 'SYS Password' and 'SYSMAN Password', both masked with asterisks. There are two checked checkboxes: 'Confirm that you have backed up the Management Repository.' and 'Disable DDMP jobs'. At the bottom, there is a 'Messages' section and a row of buttons: 'Help', '< Back', 'Next >', 'Upgrade', and 'Cancel'.

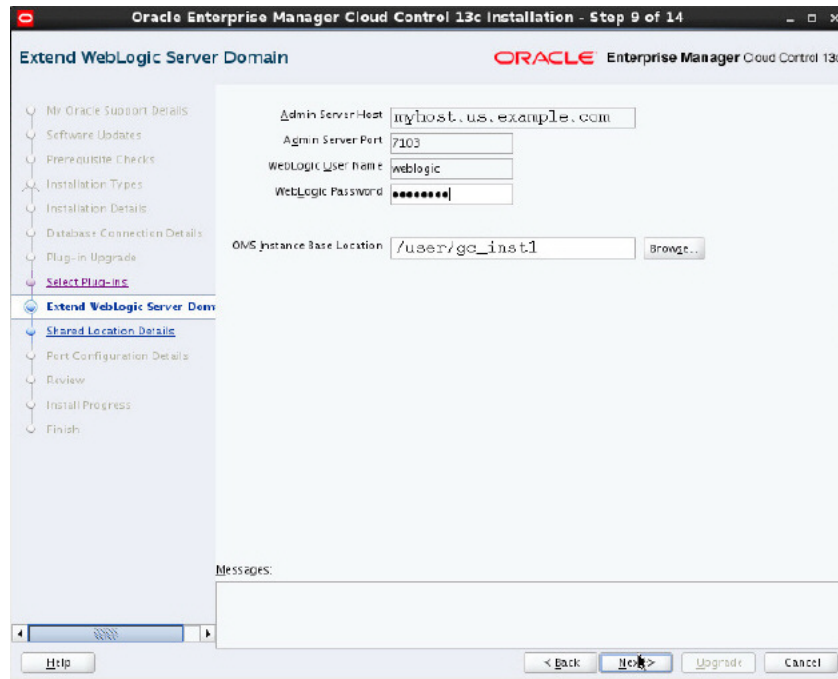
11. Click OK in dialog box that appears.

Figure 23 Oracle Enterprise Manager Cloud Control 13c Installation Step 6 - warning



12. Click Next in the dialog boxes that appear till you see **Extend WebLogic Server Domain**.
13. Enter the **WebLogic Password** and the new **OMS Instance Base Location** and click **Next** to continue.

Figure 24 Oracle Enterprise Manager Cloud Control 13c Installation Step 9



14. Click **Upgrade** in the dialog box that appears.
15. Deselect the check boxes for additional plug-in installation and click **Next**.

15.2 Upgrading Oracle Management Agents

See the "Upgrading Oracle Management Agents" chapter at http://docs.oracle.com/cd/E63000_01/EMUPG/upgrading_agents.htm#EMUPG185 for more information on how to upgrade the Oracle Management agents.

16 Known Issues

This chapter describes the known issues you might encounter when you install and configure the Enterprise Manager Plug-in for Oracle GoldenGate.

16.1 Download Failure

When downloading the Enterprise Manager Plug-in for Oracle GoldenGate as previously described, you may encounter an error when the download is 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
```

16.2 Upgrading the Monitor Agent

To upgrade Oracle GoldenGate Monitor Agent 12c version 12.1.3.0.4 to 12.2.1.0.0 for Enterprise Manager Plug-in, use the command `touch cfg_templates/oggmon.properties && ./upgradeToMonitorAgent1221.sh` instead of `./upgradeToMonitorAgent1221.sh` command.

16.3 Undeploying and redeploying the same version of Enterprise Manager Plug-in

Undeploying and redeploying the Enterprise Manager Plug-in version 13.1.1.0.0 can cause some unexpected error and is not recommended.

After undeploy and redeploy, if you navigate to Oracle GoldenGate home page from the Enterprise Manager Plug-in for Oracle GoldenGate interface and click on Extract, you can get an error as shown in the following image.

Figure 25 Error displayed while undeploying and redeploying the same version



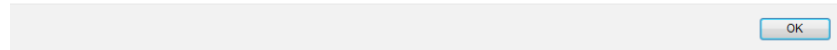
16.4 Oracle Application Development Framework (ADF) Error while Monitoring Oracle GoldenGate Instances

Clicking on **Log** and **Configuration** tab within the Enterprise Manager interface can cause ADF error while monitoring Oracle GoldenGate instances on Linux.

You can close the browser and login again to recover from the error.

Figure 26 ADF Error in Enterprise Manager Interface

ADF_FACES-60097:For more information, please see the server's error log for an entry beginning with: ADF_FACES-60096:Server Exception during PPR, #20



17 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_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 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.

Oracle GoldenGate System Monitoring Plug-in Installation Guide , 13c (13.1.1.0.0)
E68921-01

Copyright © 2014, 2016, 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, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

