Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In Installation Guide

13*c* (13.2.1.0.0)

E77936-03

July 2017

Oracle Enterprise Manager Oracle GoldenGate System Monitoring Plug-In Installation Guide, 13*c* (13.2.1.0.0)

E77936-03

Primary Author: Oracle Corporation(contributor)

Contents

Preface

Topics

Audience

This document is intended for administrators who want to use the Enterprise Manager Plug-in for Oracle GoldenGate to monitor and manage Oracle GoldenGate processes.

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.

Related Documents

For more information, see the following documents:

- Intoduction to Plug-In Manager in *Oracle Enterprise Manager Cloud Control Administrator's Guide*
- Security Overview in *Oracle Enterprise Manager Cloud Control Security Guide*
- Upgrading Oracle Management Agents in *Oracle Enterprise Manager Cloud Control Upgrade Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Getting Started with Enterprise Manager Plug-In for Oracle GoldenGate

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.

Topics

1.1 What is Enterprise Manager Plug-In for Oracle GoldenGate

The Oracle GoldenGate Enterprise Manager Plug-In extends the Oracle Enterprise Manager (EM) Cloud Control to support 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.

1.2 Supported Platforms and Releases

This topic discusses the platforms and releases that are supported by Enterprise Manager Plug-In for Oracle GoldenGate.

Supported Platforms

- Make sure that you are installing your product on a supported hardware or software configuration.

  See the Certifications tab on My Oracle Support for details.
- 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.

- 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 13c Agent and later instances can run.
- DB2 z/OS and DB2 for I do *not* support the installation of the Enterprise Manager and EM Agent. Monitoring of Oracle GoldenGate instances is achieved through remote EM Agent and Oracle GoldenGate Monitor Agent installed on these operating systems (supported with changes in the OEM and Oracle GoldenGate configuration).
- For DB2 for i, the Java Platform Standard Edition (Java SE) Development Kit (JDK) 7 Update 2 or later is required to support Transport Layer Security (TLS) 1.2 specification (supported with changes in the OEM and Oracle GoldenGate configuration).
- Oracle GoldenGate for HP NonStop is *not* supported.

Supported Releases

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

- Enterprise Manager Cloud Control 13*c* Release 2 (13.2.0.0) and later.
- Oracle GoldenGate versions supported include:
  - Oracle GoldenGate Monitor Agent 12*c* (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 12*c* (12.1.2.0.1).
  - Oracle GoldenGate 12*c* (12.1.2.0.0).
  - Oracle GoldenGate 11*g* Release 2 (11.2.1.0.10) and higher.
  - Support for non-core Oracle GoldenGate.

    If you want to use a specific version of Oracle GoldenGate other than the default version, (for example, version 11.2.1.0.23) , then add a `MinOGGCoreVersion` entry for each `Feature` element in the `omsOracleHome/plugins/oracle.fmw.gg.oms.plugin_13.2.1.0.0/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>
```

1.3 Before You Begin with Enterprise Plug-In for Oracle GoldenGate

Oracle Enterprise Manager for Oracle GoldenGate has a number of prerequisites that must be performed before you can get started with deploying and using the product.

Software Requirements

- The following must be installed and running:
  - Oracle GoldenGate 12*c* (12.1.2.0.1) and later or Oracle GoldenGate 11*g* Release 11.2.1.0.17 and later to support monitoring by Enterprise Manager Cloud Control.
  - Oracle GoldenGate Monitor Agent 12*c* (12.1.3.0.4) and later; the installation location you chose is referred to as `OGG_AGENT_ORA_HOME` in this document. This location is not necessarily the Oracle GoldenGate 12*c* installation location.
  - Oracle Enterprise Manager (OEM) Cloud Control 13*c* Release 2 (13.2.0.0) and later (Oracle Management Service and Oracle Management agent).
- An Oracle Management agent must be installed on each system, which are hosting Oracle GoldenGate instances, and you wish to monitor.
- 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 doesn't return a 1.7 version of Java, check that the `PATH` environmental variable includes `java.exe` and `java`.

  If you require 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 is unable to load the Java agent.

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

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.

> **NOT_SUPPORTED:**
>
> Oracle has tested and verified the performance of your product on all certified systems and environments; whenever new certifications occur, they're 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.

Set Environment Variables to Point to the Java Installation

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

> **Caution:**
>
> 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.

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
```

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
```

Configure Oracle GoldenGate Instances

To configure your Oracle GoldenGate instances:

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 are 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 How do I Create the Oracle Wallet.
3. Use the steps listed in How do I Configure Oracle GoldenGate to Run with Oracle Enterprise Manager to configure the Oracle GoldenGate instances for monitoring by Oracle Enterprise Manager.
4. Use the steps listed in How do I Start 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.

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 don’t have Internet connectivity. See Downloading Plug-Ins in *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

2
Deploying the Plug-In

This section describes how to import the plug-in into Oracle Enterprise Manager Cloud Control and how to deploy the plug-in to the management agent.

Topics

2.1 How do I Import the Plug-in Archive

If you manually downloaded the plug-in, then you must manually import the plug-in archive into Oracle Enterprise Manager Cloud Control. This topic tells you how to complete this task.

To import the plug-in archive:

1. Go to OTN and download the Enterprise Manager Plug-In for Oracle GoldenGate from the Downloads page, located in the Management Pack for Oracle GoldenGate section.
2. Select **Setup, Command Line Interface** and follow the instructions outlined on the Enterprise Manager Command Line Interface Download page to set up the Enterprise Manager Command Line (EM CLI) utility.
3. Import the plug-in archive:

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

4. Log in to Enterprise Manager Cloud Control to complete the deployment:
   a. Select **Setup, Extensibility, Plug-ins** to open the Plug-ins page.
   b. Expand the Middleware folder.
   c. Select **Oracle GoldenGate, Deploy on, Management Servers...** to start the deployment process.
   d. Enter the **Repository SYS password** and click **Continue**.

      A series of prerequisite system checks begins. As each system check completes,
   e. Click **Next** after each system check completes to continue to the next check. Do this until all of the prerequisite checks are complete.
   f. Click **Next** and then **Deploy**.

> **Tip:**
>
> Deployment usually takes about 10 minutes to complete. During this time, all connected users are disconnected from Enterprise Manager. Even though the confirmation page displays, clicking **Show Status** displays *This webpage is not available*while deployment of the plug-in progresses.

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

> **Note:**
>
> If you haven't enabled the `-omslocal` flag, then make sure you specify the host and all the necessary credentials.

2.2 How do I Deploy the Plug-In to the Management Agent

Once you've completed the plug-in deployment on the management server, you must deploy the plug-in to the management agent. This topic tell you how to complete this task.

To deploy the plug-in to the management agent:

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

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

3

Setting Up Enterprise Manager Plug-In for Oracle GoldenGate

After deploying the Enterprise Manager plug-in, there are a number of tasks that must be completed before you can begin to use the plug-in to monitor your processes. This section shows you how to complete these tasks.

Topics

3.1 How do I Create the Oracle Wallet

You must perform the following steps to create the Oracle Wallet and to add the password that the Oracle Management agent uses to connect to the Oracle GoldenGate agent to receive metric values.
To create the Oracle Wallet:

1. Navigate to the `OGG_AGENT_ORA_HOME` directory.

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

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

- *Windows:* Go to the command line and enter `Shell> pw_agent_util.bat -jagentonly`
- *UNIX:* Enter the command `Shell>./pw_agent_util.sh -jagentonly`

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

3. Enter and confirm the Oracle Enterprise Manager agent password when you see this prompt:

```
Please create a password for Java Agent:

Please confirm password for Java Agent:
```

> **NOT_SUPPORTED:**
>
> If a wallet already exists in the `dirwlt` directory, a message is returned and the utility stops. If this happens go to the next step.

4. Optional: Run the utility to create the `JAgent` password by entering one of the following commands. (Note that the command options are not case sensitive):

> **Caution:**
>
> Only perform this step if the wallet already exists in the `dirwlt` directory.

- *Windows:* Go to the command line and enter: `Shell> pw_agent_util.bat -updateAgentJMX`
- *UNIX:* Enter the command `Shell> ./pw_agent_util.sh -updateAgentJMX`

3.2 How do I Configure Oracle GoldenGate to Run with Oracle Enterprise Manager

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

To configure monitoring for Oracle Enterprise Manager:

1. Navigate to the `OGG_AGENT_ORA_HOME` directory
2. Edit the `cfg/Config.properties` file:
   a. Set the property that determines the monitoring type to *Oracle Enterprise Manager:*

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

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

      UNIX,: `netstat -anp | grep [port_number]`

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

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

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

d. Set the property that identifies the host of the `JAgent`.

This is the host of the Oracle GoldenGate instance. The value may be a name or an IP address.

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

e. Set the port of the `JAgent`. The default for this property is *5555*.

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

f. Set the user name for the connection to the `JAgent`.

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

g. Set the SSL value for the connection to *false*.

```
jagent.ssl=false
```

3.3 How do I Start the Oracle GoldenGate Instances

This topic shows you how to start your Oracle GoldenGate and the monitor or JAgent agent using GGSCI commands.
For more details see, Oracle GoldenGate GGSCI Commands.

1. Navigate to the Oracle GoldenGate installation directory.
2. Start a GGSCI session:

```
Shell> ./ggsci
```

3. Create the data store that persists monitoring data if this is the first time you're starting Oracle GoldenGate after enabling monitoring,

```
GGSCI> CREATE DATASTORE
```

4. Create the sub-directories if this is the first time you're starting Oracle GoldenGate after enabling monitoring.

```
GGSCI> CREATE SUBDIRS
```

5. Stop and restart running Oracle GoldenGate Manager processes if you just added the `GLOBALS` parameter to enable monitoring.

   You must perform this step 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
```

> **Tip:**
>
> The Oracle Wallet must be successfully created and the password entered before starting the agent. See How do I Create the Oracle Wallet.

3.4 How do I Create SSH Named Credentials

This topic shows you how to create SSH Key named credentials.

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.

   ```
   rw- – – – – – – 1 cllamas dba 1675 Mar 21 13:58 id_rsa
   rw- r – – r – – 1 cllamas dba 400 Mar 21 13:58 id_rsa.pub
   ```

2. Use the client, such as Putty Key Generator, to generate the Private key and the Public key.
3. Save both the Public and Private keys.
4. Use the **Conversions, Export OpenSSH Key** in the Putty Key Generator dialog to convert the key.
5. Save the converted key.
6. Select the OpenSSH key in the Putty Key Generator dialog, then copy and paste the contents in a file called **authorized keys** using the command `vi authorized keys`.
7. Save the file.
8. Use the Putty agent to load the key that you just generated.
9. Log in to the server using the key.
10. Go to the Enterprise Manager Cloud Control.
11. Select **Setup, Security, Named Credentials** to open the Named Credentials dialog and create a named credentials.
12. Click **Create**.
    a. Select *Host* in the dropdown for **Authoring Target Type**.
    b. Select *SSH Key Credentials* in the dropdown for **Credential** type.
    c. Select Global as the scope if the same SSH Key is going to be used for all the targets.
    d. Go to the Credential Properties section and upload the open SSH public key as well as the private key.
    e. Click **Add Grant** and set the access privilege for the user.
    f. Click **Change Privilege** and in the dialog box that's displayed, select *Full* from the drop down list.
    g. Click **Test and Save** to check the connection.

       A confirmation message appears if the connection is successful.

(Optional) Enter the result of the procedure here.

3.5 How do I Set the Preferred Credentials

This topic shows you how to set the preferred credentials on all agents where you want to deploy Enterprise Manager Plug-In for Oracle GoldenGate.

To set the preferred credentials:

1. Go to Enterprise Manager Cloud Control and select **Setup, Security, Preferred Credentials** to open the Preferred Credentials page.
2. Select the required target type from the list.

   You can narrow your search by entering search criteria, or you can just scroll through the list of target types if there are not too many.
3. Click **Manage Preferred Credentials** to open the Preferred Credentials page.

   The Preferred Credentials page 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.
4. Go to the Target Credentials section and select the host name for the host that is running the Management agent where the Enterprise Manager Plug-In for Oracle GoldenGate has to be deployed. Click **Set** to open the Select Named Credential dialog.
5. Enter values for the host credential and the administration credential.
   - *Host Credential:* This sets host credentials of the EM agent so that the Enterprise Manager Plug-In for Oracle GoldenGate can communicate with it.

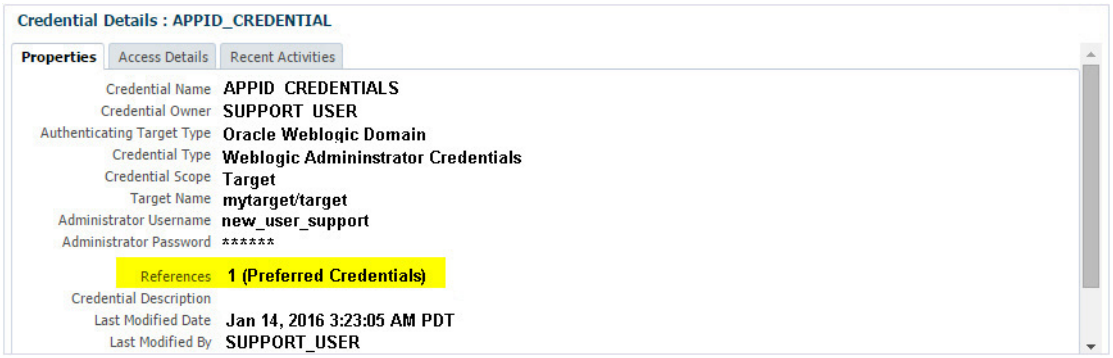
     For example, if the EM agent is on host `myhost` and this machine is accessible using credentials X1 and X2; and X1 was used to install the EM agent, then you must use the X1 as the host credentials.
   - *Administration Credential:* Set the Administration credential by adding the username to the `config.properties` file of the Oracle GoldenGate instance and defining the password when the Oracle Wallet is created.

   NOT_SUPPORTED:

   If Oracle GoldenGate Core setup is done on a different system, which isn't running the OMS and EM Agent, you must provide the OMS host credential for `host credential set`, and not the Oracle GoldenGate Core system credentials.
6. 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.

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



8. Run the OS Command job for the Management agent where the Enterprise Manager Plug-In for Oracle GoldenGate is deployed:
   a. Log in to Enterprise Manager Cloud Control.
   b. Click **Enterprise, Job, Activity** to open the Job Activity page.
   c. Select **OS Command** from the Create Job list, then 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.
9. Repeat host credentials for the other GoldenGate target types:
   - Oracle GoldenGate Manager
   - Oracle GoldenGate Extract
   - Oracle GoldenGate Replicat

3.6 How do I Monitor High Availability Features

This topic 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 must be provided at the time of Oracle GoldenGate target discovery.

There can be two scenarios where High Availability is required:

- *Oracle GoldenGate instance is failed over from one node to another in the cluster:* In this scenario, the existing Master Agent continues monitoring the Oracle GoldenGate instance in a seamless manner and the **Host Name** parameter oin the Oracle GoldenGate Manager page displays the physical host name of the new node.
- *Current Master Agent stops functioning:* In this scenario, the EM Agents that are currently running, must be marked as **Slave** for this Oracle GoldenGate instance. When the current Master Agent stops functioning, one of the **Slave** agents is assigned as **Master** for the Oracle GoldenGate instance, and monitoring continues.

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. Select **Setup, Manage Cloud Control, Agents** to open the Agents page.

   All the agents are listed on this page.
4. Select **Targets, GoldenGate** .
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. Select **Setup, Add target, Configure Auto Discovery**.
7. Select the host and click **Discovery Modules** to provide credentials details by selecting Goldengate discovery.

   See How do I Add Instances for Monitoring.
8. Click **Discovered Targets** for a particular Agent Host Name.

   The dialog lists all the targets on hosts, select a particular host.

   a. Click **Promote** to promote the particular process. A Confirmation dialog displays when the promotion process is completed.
9. Click **Submit** from the Manage Agents page. A confirmation dialog displays.

   This page displays after successful completion of the 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’re not associated with this Oracle GoldenGate instance. You can select any number of these agents as **Slave**, and click **Submit** to save he changes.

   If you don’t want to make any such changes, you can click **Oracle GoldenGate Home** and navigate back to the GoldenGate plug-in home page.
10. Click **Targets, GoldenGate** and then select the *Data Pump* process.
11. Click **Stop** on the Extract:DPUMP page. Click **Yes** in the confirmation dialog to stop the process. Click **Close** on the process complete dialog.
12. Select **Targets, GoldenGate** .

    The DPUMP process is displayed as stopped. Click **Refresh** to refresh the page if the process still shows as running.
13. Select the **DPUMP** process to open the Extract:DPUMP page.
14. Click **Start**. Select **Normal** on the confirmation dialog box and then click **Start**.
15. Click **Close** when the Process Complete dialog displays.

16. Click **OGG Home** to go back to the home page.

    All the processes are displayed as running.

17. Select the **Manage Agents** tab. .

    Note that in the list of Agents, one displays as *Master* and the other displays as *None*.

18. Using the dropdown list, change the **Status** from *None* to *Slave*.

19. Click **Submit**. In the confirmation dialog click **OK**.

20. Select **Setup, Manage Cloud Control, Agents** to open the Agents page.

21. Click **Targets** and then on the next page click **OGG Home**.

    All the processes display as running.

22. Go to the console to stop the running processes by using the `stop *` command.

23. Next, stop the *JAgent* process using the `stop jagent` command.

24. Type *Y* to confirm the action.

25. Stop the *MANAGER* process using the `stop manager` command.

26. Type *Y* to confirm the action.

27. In the console, use the command `info all` to view the current status of the processes.

    All the processes display as stopped.

28. Next, start the *MANAGER* process using the `start manager` command.

29. Start the other processes using the `start *` command.

30. Start the *JAgent* process using the `start jagent` command.

31. In the management portal, refresh the OGG Home tab to view the updated status of the processes.

    Note that it can take few moments for the page to update. All the processes display as running.

32. Select the *DPUMP* process on the Extract:DPUMP page and stop the process. box.

    Click **Yes** in the confirmation dialog. Click **Close** in the Process Complete dialog

33. Use the console to view the status of all the processes using the `info all` command.

    All the processes display as running.

34. In the Enterprise Manager portal, click **OGG Home**.

    All the processes display as running.

35. Go to the console and stop the running processes using the `stop *` command.

36. Stop the *JAgent* and *MANAGER* processes as mentioned previously.

    Type *Y* to confirm the actions.

37. Use the command `info all` to view the current status of the processes.

    All the processes display as stopped.

38. Start the processes using the `start *` command.
39. Start the *MANAGER* and *JAgent* processes.
40. In the console, type the command `info all` to view the current status of the processes.

    All the processes display as running.
41. In the portal, click **Refresh** to update the status of the processes.

    All the processes display as running.
42. Go to the OGG Home tab, and select the *DPUMP* process to open the Extract:DPUMP page.
43. Click **Stop**. Click **Yes** in the confirmation dialog.
44. Click **Close** to complete the process.

3.7 How do I Verify and Validate 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.

For more details, see Discovering, Promoting, and Adding Targets.

After waiting a few minutes for the Enterprise Manager Plug-In for Oracle GoldenGate to start collecting data, use these 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 to open the Oracle GoldenGate Home Page.
2. Select **Target, Monitoring and then Metric Collection Errors** to verify that no metric collection errors are reported.
3. Select **Target, Information Publisher Reports** to view reports for the Oracle GoldenGate target type, and ensure that no errors are reported.
4. Select **Target, Configuration, Last Collected** Ensure that configuration data can be seen. If configuration data doesn't immediately appear, click **Refresh** on the Latest Configuration page.

3.8 How do I Add Instances for Monitoring

After successfully deploying the Enterprise Manager Plug-In for Oracle GoldenGate, you must add the plug-in target to Enterprise Manager Cloud Control for central monitoring and management.

1. Select **Setup, Add Target, Configure Auto Discovery** .
2. Click on the GoldenGate Discovery Module to display the Configure Target Discovery for Target Types page.
3. Select the agent host name and click **Edit Parameters** to open the Edit Parameters: GoldenGate Discovery dialog.
4. Enter the information required 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 when you create the Oracle Wallet.
- **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 the 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're still accessible using the same monitoring details. This is 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, 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**.
   - Select **Setup, Add Target, Auto Discovery Results**.
8. Select a target to promote, then click **Promote** to open a promotion wizard for this target type.
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 a 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 details. see Discovering, Promoting, and Adding Targets

3.9 How do I Configure Instance-Level Security

Enterprise Manager provides instance-level security flexibility to provide target-level privileges to administrators. For example, if an Enterprise Manager Plug-In for Oracle GoldenGate is managing three Oracle GoldenGate (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).

To grant target-level access:

1. Log in as a super admin (for example, `sysman`).
2. Select **Setup, Security, Administrators** to open the Administrators page.
3. Click **Edit** to modify access for an existing user.
4. Click **Create/Create Like** to create a new user and to assign the appropriate user roles.

5. Select the Properties tab, enter the required credentials for the new user, and click **Next** to open the Create Administrator *userName*: Roles page.

   This page lets you to assign roles to the named user by moving the role from the **Available Roles** column to the **Selected Roles** column.

6. Select one or more roles from the **Available Roles** list and click **Move** 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. This table shows the different roles.

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

   Do not select any *ALL* roles in this step, such as `EM_ALL_ADMINISTRATOR`, `EM_ALL_OPERATOR`, and so on, else the user role you're creating will be entitled to all OGG instances.

   Enterprise Manager (EM) supports object-level access control so administrators can be given roles for specific targets only. See Creating Roles for Systems Infrastructure Administration in *Enterprise Manager Cloud Control Administrator's Guide*.

7. Click **Next** to open the Target Privileges page.

8. 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**.

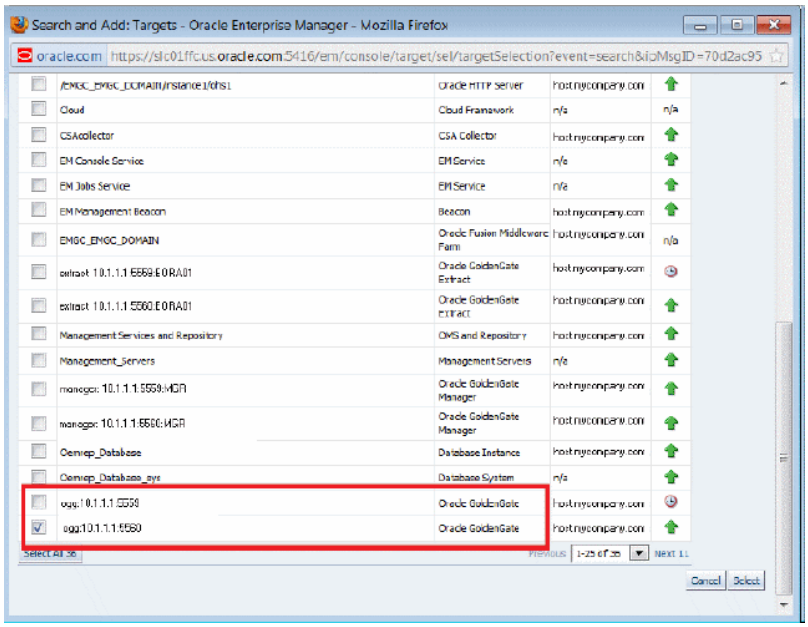
   These two roles are required for full functionality and multi-version support.

9. 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. Click **Add** to open the Search and Add: Targets page appears in a new browser window.

10. Select the instances you want the user to have access.

> **NOT_SUPPORTED:**
>
> You're only assigning Oracle GoldenGate instances at this time. You're not assigning *Manager, Extract*, or *Replicat* processes.

Here is an example of two Oracle GoldenGate instances (port numbers 5559 and 5560). Access to only one of them (port number 5560) is being assigned to this user.



11. Click **Select** to save the changes.

    You're returned to the Add Targets page and the Target Privileges list is refreshed to show your selection.

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

    Select from the following privileges:

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

    Don't select both the *Full* and *Connect Target* privileges because *Full* includes *Connect Target* .

13. Click **Continue**.

14. Click **Review** to review your user's privileges, then click **Finish**.

    The user now has 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's 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's specific to that process and is not assigned to other processes in the instance.

15. Test the instance-level security to confirm that all edited processes are operating with their assigned privileges:
    a. Log in as the newly created or edited user.
    b. Select **Targets, GoldenGate** to open the Oracle GoldenGate page.
    c. Confirm that only the OGG instances that you have access to are visible.
    d. Log out and log in again as `root`.
    e. Select **Targets, GoldenGate** to open the Oracle GoldenGate page.
    f. You should now see all the managed OGG instances.

For more details, see Security.

3.10 How do I Configure JAgent to Support Remote Monitoring Using JMX Server

You must configure the JAgent to support remote monitoring using JMX Server.

To configure the JAgent to support remote monitoring using JMX Server.

1. Edit the `Config.properties` file.
    a. Set `jagent.rmi.port` for OEM mode
    b. Set `jagent.jmx.port` for OGGMON mode
    c. Set `agent.type.enabled` = OEM or OGGMON
2. Optional: Add the following parameters only when Oracle GoldenGate and JAgent are running on cloud or within a firewall.
    a. The `jmx.enable.remote.monitoring` = true or false.
    b. The `jmx.broker.port` = default (any valid port number).
3. Set `jmx.enable.remote.monitoring` = true.
4. Set `jmx.broker.port` = any valid firewall enabled port.

   It uses two ports, either the `jagent.rmi.port` or `jagent.jmx.port` as the registry port depending on `agent.type.enabled` property, and `jmx.broker.port` as the communication port.
5. Optional: Enable SSH tunneling for the ports.
    a. `ssh -i opc_rsa -f opc@192.0.2.1 -L 9020:192.0.2.1:9020 -N`
    b. `ssh -i opc_rsa -f opc@192.0.2.1 -L 5559:192.0.2.1:5559 -N`
    c. `ssh -i opc_rsa -f opc@192.0.2.1 -L 7809:192.0.2.1:7809 -N`

   The IP 192.0.2.1 is the public IP address of the cloud device.

Important:

You must repeat the command sequence if the client system is restarted.

4

Using the Enterprise Manager Plug-In for Oracle GoldenGate

This section discusses how to enable, search, and interpret audit logs, how to monitor metrics, and how to alert users about specific metric results.

Topics

4.1 How do I Enable Audit Logging

Messages are automatically logged to the server log file for all Oracle GoldenGate actions, such as start and stop as well as for file access, such as parameter, report, and discard. This topic discusses how to enable these logs for auditing.
To enable or disable an audit for a specific action, run the following commands from the `oms/bin` directory. Enter 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"
```

You can enable or disable one or more operations using the `-operations_to_enable` flag. Here is a list of the Oracle GoldenGate operations and the values to use.

Operation	Value
Start Oracle GoldeGate process	`OGG_START_TARGET`
Stop Oracle GoldenGate process	`OGG_STOP_TARGET`
Kill Oracle GoldenGate 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`

Operations can be combined and separated by a semicolon (;). Here is how to enter the command to enable all audit logging for the Enterprise Manager Plug-In for Oracle GoldenGate.

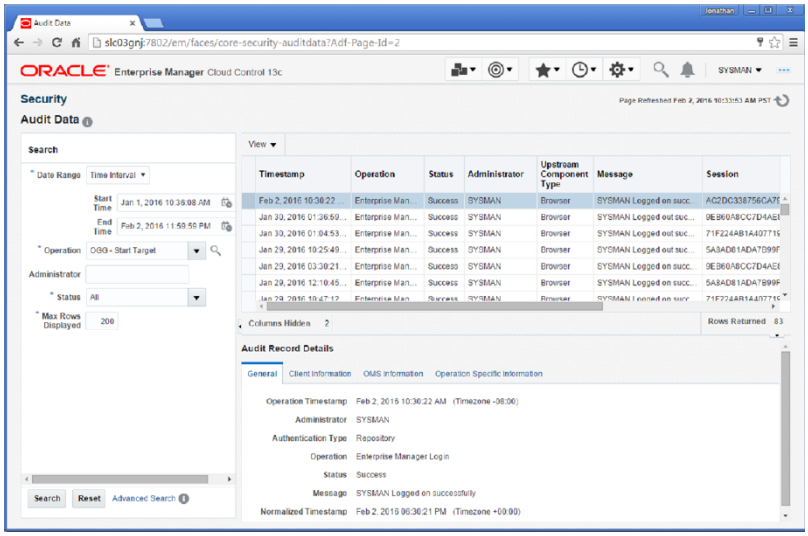
```
emcli update_audit_settings -
operations_to_enable="OGG_START_TARGET;OGG_STOP_TARGET;OGG_KILL_TARGET;OGG_VIEW_REPOR
T;OGG_VIEW_DISCARD;OGG_VIEW_GGSERRLOG;OGG_EDIT_PARAM"
```

4.2 How do I View Audit Logs

A Cloud Control user with Super Administrator privileges has the access to search for and view audit logs. This topic discusses how to search for and view a specific audit log using Cloud Control.

To view a specific audit log:

1. Select **Setup, Security, Audit Data** to open the Audit Data page.



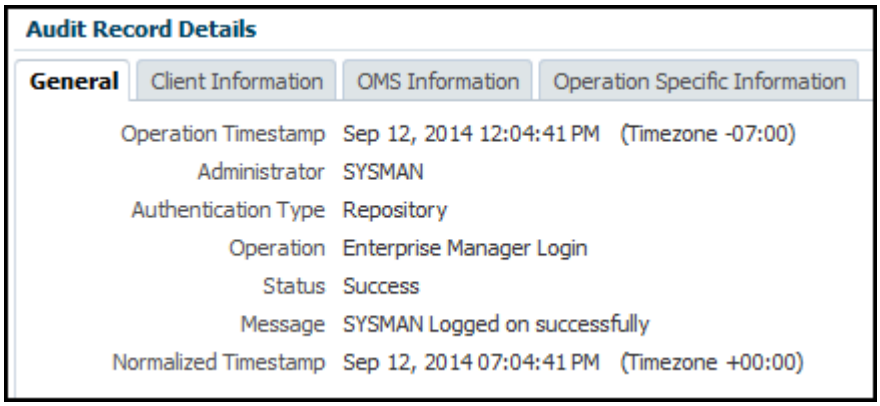
2. Select your search criteria, such as date range, operations, status, and so on.

   You can select specific operations from the **Operations** drop-down menu. For example, you can select all the operations that begin with OGG.

3. Click **Search** .

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

5. Once selected, you can view audit log information in the Audit Record Details region, as shown. The Audit Record Details are updated automatically for each audit log you select. Click the General, Client Information, CMS Information, and Operation Specific Information tabs for specific information.



For additional information about the auditing feature in Enterprise Manager, see Configuring Auditing Frameworkin *Enterprise Manager Cloud Control Getting Started Guide* and Configuring the Audit Data Export Servicein *Enterprise Manager Cloud Control Security Guide*.

4.3 How do I Monitor Processes

This topic discusses the metrics used to monitor the extract, replicat, and manager processes.
The following processes are monitored by Oracle GoldenGate Enterprise Manager 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 process and 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 are lost.

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

Here is a list of the metrics used for the Extract and Replicat processes.

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

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

Metric	Description
Last Checkpoint Timestamp	**Valid for Extract and Replicat** Shows the time when the last checkpoint was written by the process. **Valid values:** Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example: 01/14/2011 09:36:32 AM.
Last Operation Timestamp	**Valid for Extract and Replicat** Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log. **Valid values:** Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example:01/14/2011 09:36:32 AM
Last Processed Timestamp	**Valid for Extract and Replicat** Shows the time when a valid record was returned to the selected process. For Extract, this time value is assigned when the record is processed after the container transaction commits (not the time when the record is read from the transaction log). For a Data Pump or Replicat, this time value is returned immediately, because all transactions in the trail are known to be committed. **Valid values:** Date time value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example: 01/14/2011 09:36:32 AM
Message	**Valid for Extract and Replicat** The message includes the following information: • Message code number of an event message from the Oracle GoldenGate error log. **Valid values:** The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651. • Message Date: Timestamp of an event message from the Oracle GoldenGate log. **Valid values:** A datetime value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format) • Message Text: Text of an event message from the Oracle GoldenGate error log. **Valid values:** A text string from the message.
Name	**Valid for Extract and Replicat** Name of the selected object. **Valid values:** Name of the object as displayed in the Oracle GoldenGate Monitor interface.
Seconds Since Last OGG Checkpoint	**Valid for Extract and Replicat** Time (in seconds) since the last OGG checkpoint.
Start Time	**Valid for Extract and Replicat** Shows the time that an Oracle GoldenGate component received its startup information after it has been created. **Valid values:** 64-bit Julian GMT time stamp in microseconds

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

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

Here is a list of the metrics used for the Manager process.

Metric	Description
Host Name	Shows the name of the host system. **Valid values**: The fully qualified DNS name of the host, or its IP address
Manager Port	Shows the port on which the Manager process of the Instance is running on its local system. The default port number is 7809, but a different port could be specified for this Manager and can be identified by viewing the Manager parameter file or by issuing the INFO MANAGER command in GGSCI (if Manager is running). **Valid values:** The port number for the Manager process, as specified in the Manager parameter file
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

4.4 How do I Send Email Alerts

You can configure Enterprise Manager to send email to administrators when a metric alert threshold is reached.
See Sending Email for Metric Alerts in *Enterprise Manager Cloud Control Administrator's Guide* for details about how to set up an email alert.

5

Upgrading Enterprise Plugin for Oracle GoldenGate

This section discusses how to upgrade your Enterprise Plug-In for Oracle GoldenGate so that you can take advantage of the latest new features.

Topics

5.1 About Upgrading Using Self Update

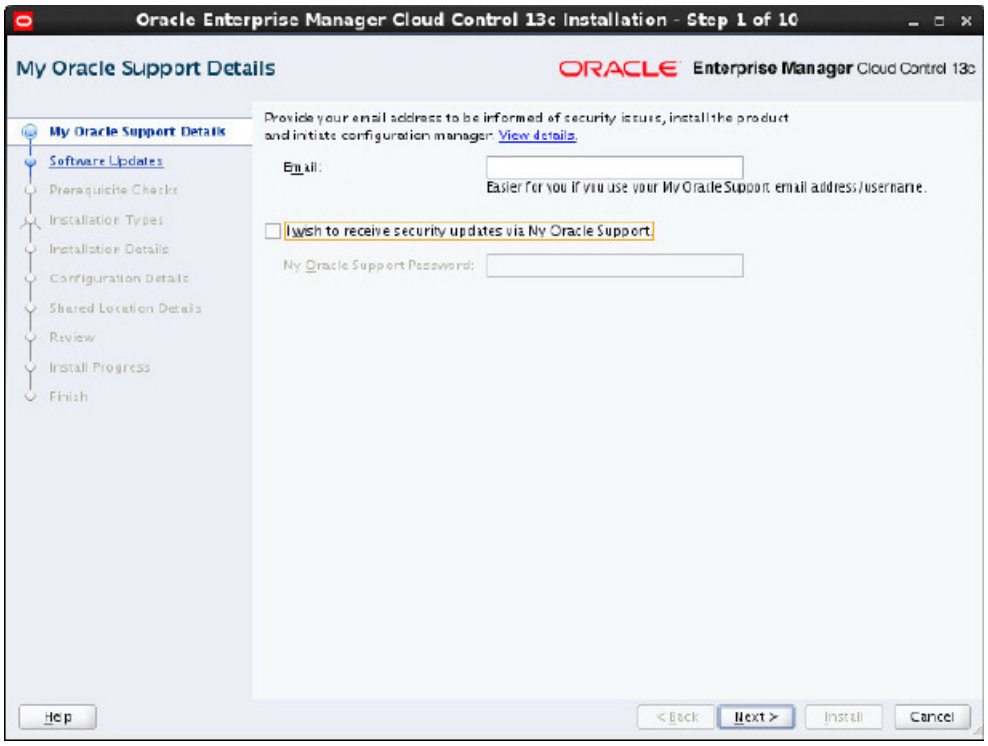
The Self Update feature allows you to expand the Enterprise Manager capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available using the Enterprise Manager Store, an external site that is periodically checked by Enterprise 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 Downloading Plug-Ins in *Enterprise Manager Cloud Control Administrator's Guide* for details on how to download the plug-in.

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

5.2 Upgrading to the Newest Version

Here is an example that demonstrates how to upgrade your Oracle GoldenGate Enterprise Manager Plug-In 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 Oracle GoldenGate Enterprise Manager Plug-In version 13.2.
4. Copy the 13.2 OPAR to a location, for example `OPAR_LOCATION`, and run the command `em_linux64.bin -invPtrLoc OMS_HOME/oraInst.loc PLUGIN_LOCATION=`*`OPAR_LOCATION`*.
5. In the dialog box, deselect the checkbox and then click **Next**. Click **Yes** in the confirmation box that appears.



6. Click **Skip**, then click **Next**.
7. Click **Next**.
8. Select **One System Upgrade**, then click **Next**.
9. Enter the new **Middleware Home Location**, then click **Next**.
10. Enter the database password, then click **Next**.
11. Read the warning, then click **OK** to close the dialog.
12. Click **Next** in the dialogs that appear until you see **Extend WebLogic Server Domain**.
13. Enter the **WebLogic Password** and the new **OMS Instance Base Location**, then click **Next** to continue.
14. Click **Upgrade** in the dialog box that appears.
15. Deselect the check boxes for additional plug-in installation and click **Next**.

5.3 Upgrading Oracle Management Agents

Starting with 13c Release 1, Enterprise Manager Cloud Control offers Agent Gold Images, in addition to the Agent Upgrade Console and EM CLI, to upgrade your Management Agents. Oracle recommends that you use Agent Gold Images to upgrade all your Management Agents, although you can use other upgrade approaches.
See Upgrading Oracle Management Agents in *Enterprise Manager Cloud Control Upgrade Guide* for details about how to upgrade the Oracle Management agents.

6

Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service

This section discusses using the Enterprise manager Cloud Control console to administer both your Oracle cloud and on-premises deployments.

Topics

6.1 About Hybrid Cloud Monitoring

You can use the Enterprise Manager Cloud Control console to administer both your on-premises and Oracle Cloud deployments.
Oracle Hybrid Cloud lets you as an on-premises Enterprise Manager administrator, monitor and manage cloud services using the same Oracle Enterprise Manager tools to monitor, provision, and maintain Oracle Databases, Engineered Systems, Oracle Applications, Oracle Middleware, and a variety of third-party systems. See Enabling Hybrid Cloud Management in *Enterprise Manager Cloud Control Administrator's Guide*.

6.2 Installing the Monitor Agent on Cloud Device to Configure the JAgent

You must install the monitor agent on your cloud device to configure the JAgent:

1. Provide the latest release file, which is `fmw_12.2.1.2.0_ogg_generic.jar`.
2. Copy the file into the cloud device.
3. Select **Monitor agent only** and provide the location for installation.

> **Note:**
>
> You must have permission to install in the mentioned location.

4. Once the installation is complete, go to *MON_AGENT_INST_LOC*/oggmon/ogg_agent directory.
5. Run the createMonitorAgentInstance.sh. Provide the Oracle GoldenGate core location, for example /u01/app/oracle/gghome when asked.

   Provide a new location /u02/data/Agent_Inst to create an agent instance for the monitor.
6. Go to the *AGENT_INST_LOC*/bin directory.
7. Run pw_agent_util.sh -jagentonly.
   - Create a password for Java Agent:
   - Confirm password for Java Agent:
8. Go to the *AGENT_INST_LOC*/cfg directory.
9. Modify the Config.properties file and change **agent.type = OEM** and save the file.

6.3 Creating an Inventory Location for Non Oracle Users

You must create a new inventory location for non Oracke users as they do not have direct access to Oracle GoldenGate Cloud Service POD machines through Oracle user. Without this access they're unable to push the Hybrid cloud agent from the Enterprise Cloud interface.
To create a new inventory location for the opc user:

1. Copy the createCentralInventory.sh script to the GGCS POD machine.
2. Login as an opc user then use the sudo su # command.
3. Create the inventory directory.

   Example: /u02/data/opcuser/oraInventory directory.
4. Run the create inventory script ./createCentralInventory1479193434142.sh inventory_location group_name.

   Example: ./createCentralInventory1479193434142.sh /u02/data/opcuser/oraInventory opc.
5. Change the permission of inventory folder from root to opc using the chown command.

   Example: chown opc /u02/data/opcuser/oraInventory.
6. Use Ctrl+D to come out from root user and change to opc user.
7. Create an emagent folder as opc user to push the Hybrid cloud agent.
8. Push the Hybrid cloud agent from Enterprise Manager interface.

The location of createCentralInventory.sh will be provided separately.

6.4 Configuring JAgent in the Provisioning Environment

You must configure the JAgent to work in the provisioning environment.

1. Go to `GGHOME` location and start the GGSCI console using the `./ggsci` command.
2. Use the `info-all` command to verify that only the `manager` process has stopped.
3. Use the `view param mgr` command to check the parameters in `MGR.prm` file and modify the port as needed
4. Exit the GGSCI console.
5. Create the `GLOBALS` file and provide the value as `ENABLEMONITORING` and save it in the `GGHOME` location.
6. Start the GGSCI console and use the `create datastore` command to create the datastore.

The GGSCI should show both the manager and JAgent processes.

6.5 Installing the Hybrid Cloud Gateway Agent

Install the EM Agent on the machine A, which is marked as a Hybrid Cloud Gateway Agent.

1. From the **Setup** menu, select **Add Target**, then **Add Target Manually**, and then select **Install Agent on Host**.
2. Add the Host Target. Enter the host name, for example *A*, and platform, for example *platform* = *Linux x86-64*. Click **Next**.
3. Add Installation base directory to a location on machine A.
4. Add Named Credential to Host credential of Machine A.
5. Don't add a value in the **Port** field. The system uses an available free port. Click **Next**.
6. Click **Deploy Agent**.

   Ignore any warning that is displayed.
7. Click **Continue On All Host**.
8. Run the `/usr/local/packages/aime/em/run_as_root /scratch/userID/emagentm/agent_13.1.0.0.0/root.sh` command to complete the installation.

6.6 Configuring the EM Hybrid Cloud

You must configure the Hybrid Cloud agent.

1. In the Enterprise Manager Plug-in for Oracle GoldenGate UI, select **Setup, Add Target, Add Target Manually, Install Agent on Host.**
2. Add the `Host Target`. Enter the host name and platform. Click **Next**.
3. Add the `Installation base directory`. It is the same location as in host provided in step 2.

   It's the same location as you provided in the previous step for the host .
4. Add the `Named Credential` to the host as provided in step 2.

   You must have privilege to the location provided in the previous step.

5. Don't provide the `port value`. The system allocates a free port. Click **Next**.
6. Click **Deploy Agent**.
7. Provide the details about the known error, which appears.

6.7 Configuring the SOCKS Proxy Setup

To configure the SOCKS proxy to work with the cloud device:

1. Login to the cloud or POD box using the credentials provided during the Hybrid agent installation.
2. Use this command to start the proxy server on the cloud device.

```
ssh -i private_key file -v -N -f -D listening IP Address:listening IP port GGCS Oracle User@GGCS IP Address
```

```
ssh -i opc_rsa -v -f -N -D 1080 USER@$_IP
```

```
ssh -i private_key file -v -N -f -D listening IP Address:listening IP port
```

- `-i`: Private Key File
- `-v`: Verbose Mode
- `-N`: No execution command on remote system
- `-f`: Run the proxy process in the background
- `-D`: Dynamic Port Forwarding
- `-C`: Compression

7
Troubleshooting

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

Topics

7.1 Correcting ADFC Error on Windows 64-Bit Machines

Selecting a target from the Oracle GoldenGate Enterprise Manager Plug-In home page may cause an ADFC exception 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"
```

> **Note:**
>
> `middleware_home` is where you installed Oracle Fusion Middleware products.

7.2 Locating EM Log Files

Following are the EM log files that can help you with troubleshooting the Oracle GoldenGate Enterprise Manager Plug-In.

Discovery related error details log file: **`ogg_so_logs.log.0`**
This file is in the `$AGENT_STATE_DIR/sysman/emd/` directory.
The `ogg_so_log` file contains discovery related errors, details about execute commands, and report/discard/config file operations. If there are any errors while the EM Agent connects with JAgent, the information is logged in this file.
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
```

Oracle GoldenGate Enterprise Manager Plug-In user interface error details log file: `emoms.log`

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

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

Oracle Management Services log file: `EMGC_OMS1.out`

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

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

8
Known Issues

This section describes the following known issues that you may encounter when you install and configure the Enterprise Manager Plug-In for Oracle GoldenGate.

Topics

8.1 Download Failure

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

```
Downloading file in staging directory
/scratch/aime/WORKEM12104/mw2587/gcinst2587/em/EMGC_OMS1/sysman/stage/
034148593e245c3de050f00a82634a7f ...
Staging directory cleaned up.
Download failed: Exception: Error downloading file: Server returned invalid
response. Status Code = 200, Response Text = [OK | <results>
   <error>
       <id>10-013</id>
       <message>Choose valid parameters.</message>
   </error>
</results>
]
```

To solve this problem:

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

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

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

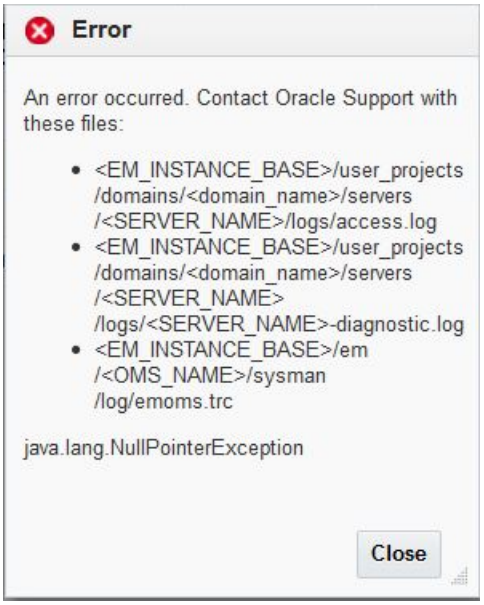
   ```
   emctl set property -sysman_pwd welcome1 -name
   oracle.sysman.emSDK.core.mos.mos_url -value https://support.oracle.com
   ```

8.2 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.

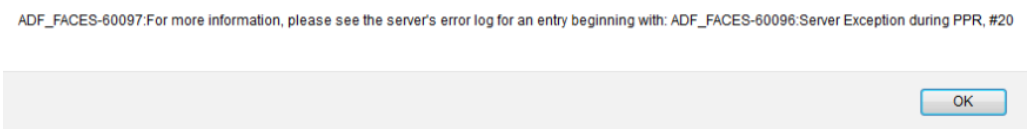
8.3 Undeploying and redeploying the same version of Enterprise Manager Plug-in

We do not recommend that you undeploy and redeploy the Enterprise Manager Plug-in version 13.2.1.0.0 as it can cause some unexpected errors. For example, if you navigate to Oracle GoldenGate home page from the Oracle GoldenGate Enterprise Manager Plug-In interface and click on Extract after you've undeployed and redeployed, you can get an error as shown.



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

If you select either the **Log** or **Configuration** tab within the Enterprise Manager interface while you are monitoring Oracle GoldenGate instances on Linux., it can cause thisADF error.



Click **OK**, then close the browser and login again to recover from the error.