Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In User Guide

(13.4.1.0)
F24283-02
September 2020

Oracle Enterprise Manager Oracle GoldenGate System Monitoring Plug-In User Guide, (13.4.1.0)

F24283-02

Primary Author: Oracle Corporation

Contents

Preface

1 Overview

2 Setting Up Enterprise Manager Plug-In for Oracle GoldenGate

3 Setting the Credentials

4 Monitoring Oracle GoldenGate Targets

5 Managing Events, Alerts, and Incidents

6 Audit Logging

7 Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service

Preface

This document describes how to set up the Enterprise Manager Plugin for Oracle GoldenGate and use the plug-in to discover and monitor Oracle GoldenGate targets.

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`.

Accessible Access to Oracle Support

Oracle customers who 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:

- Cloud Control's Adminstrator's Guide
- Security Overview in *Oracle Enterprise Manager Cloud Control Security Guide.*
- Upgrading Oracle Management Agents
- Introduction to Oracle GoldenGate Monitor

  in *Installing and Configuring Oracle GoldenGate Monitor.*
- Introduction to Oracle GoldenGate in *Oracle Fusion Middleware Understanding Oracle GoldenGate.*
- Deploying the Enterprise Manager Plug-in in *Oracle GoldenGate System Monitoring Plug-In Installation and Upgrade Guide.*
- Oracle Fusion Middleware 12c (12.2.1.4.0) Interoperability and Compatibility in *Understanding Interoperability and Compatibility* 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 Overview

The Oracle GoldenGate extends the Oracle Enterprise Manager (EM) Cloud Control to support for monitoring and managing Oracle GoldenGate processes including the following:

1.1 Custom Screens

The Oracle GoldenGate Enterprise Manager Plug-In includes custom screens for:

- Customizing the display on the home page. This allows you to:
  - Indicate that certain Oracle GoldenGate instances should or should not be displayed on the home page.
  - Change the order of instances displayed.
  - Define an alternate display name.
  - Add a description for an instance.
- Promoting Oracle GoldenGate targets. To simplify the promotion of Oracle GoldenGate instances that may include many processes, a custom screen displays all of the processes defined for an instance and allows you to promote all or a subset in a single action
- Support high availability is enabled through the **Manage Agent** tab.

2 Setting Up Enterprise Manager Plug-In for Oracle GoldenGate

After deploying the Enterprise Manager plug-in, there are a number of tasks that you must complete before you begin to use the plug-in to monitor the Oracle GoldenGate instances.

This topic details the following:

Topics

2.1 Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager

To configure your Oracle GoldenGate instances:

1. Configure the Oracle GoldenGate monitoring agent to run with Oracle Enterprise Manager. See Installing and Configuring Oracle GoldenGate Monitor Agent in *Installing and Configuring Oracle GoldenGate Monitor Agent* to configure the agent for the Oracle Enterprise Manager.

   You need to do this configuration only for Oracle GoldenGate classic instance and is not required for Oracle GoldenGate microservices architecture (MA).
2. Create the Oracle Wallet to store passwords using the steps listed in Creating the Oracle Wallet.

2.1.1 Creating 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.

This is applicable for the Oracle GoldenGate classic instance only as the Oracle GoldenGate monitoring agent is used by classic instance.
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 monitoring agent wallets cannot reside in the same location. If both Oracle GoldenGate core and the Oracle GoldenGate monitoring agent 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 doesn't 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 Oracle GoldenGate Monitoring Agent 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`

2.2 Discovering an Oracle GoldenGate Enterprise Manager Plug-in Processes

Discovery is a process, where an agent identifies pre-defined target types, registers them in the Oracle GoldenGate Enterprise Manager Plug-in, and collects their target properties and initial configuration data. The agent then sends this data to the Oracle Management Service (OMS), which processes the data and loads it into the Management Repository. After the targets are discovered, Oracle GoldenGate Enterprise Manager Plug-in can access data about the targets on the UI to monitor and manage the instances under a single roof.

The Oracle GoldenGate Enterprise Manager supports the following target types for Classic and Microservices (MA) instances. For more information about monitoring these target types, see Monitoring Oracle GoldenGate Targets.

Table 2-1 Target Types Supported

Target Type	Description	Classic (Supported-Yes/No)	Microservices(Supported - Yes/No)
Oracle GoldenGate	Oracle GoldenGate target type represents an Oracle GoldenGate classic instance. It's the parent target of Manager, Extract, and Replicat targets. It shows the cumulative status of all the processes in the Oracle GoldenGate instance excluding the Initial Load processes.	Yes. See Oracle GoldenGate.	No
Extract	The Extract target type enables the static extraction of data records from one database and loads those records to a trail file.	Yes	Yes. See Extract and Replicat.
Replicat	The Replicat target type reads the data from trail and applies the data to the target database.	Yes	Yes. See Extract and Replicat.
Manager	The Manager target type instantiates the Oracle GoldenGate processes, allocates port numbers, and performs file maintenance. This target type is a controller process.	Yes. See Manager.	No

Table 2-1 (Cont.) Target Types Supported

Target Type	Description	Classic (Supported-Yes/No)	Microservices(Supported - Yes/No)
Service Manager	The Service Manager target type is the central hub from where you can start and stop deployments, Administration Server, Distribution Server, Performance MetricsServer, and Receiver Server.	No	Yes. See Service Manager.
Administration Server	The Administration Server target type supervises, administers, manages, and monitors processes within an Oracle GoldenGate deployment.	No	Yes. See Administration Server.
Deployment	The Deployment target type enables connection with the Service Manager that helps in controlling all other services in Microservices.	No	Yes. See Deployment.
Performance Metrics Server	The Performance Metrics Server target type uses the metrics service to collect and store instance deployment performance results. This metrics collection and repository is separate from the administration layer information collection.	No	Yes

Table 2-1 (Cont.) Target Types Supported

Target Type	Description	Classic (Supported-Yes/No)	Microservices(Supported - Yes/No)
Distribution Server	The Distribution Server target type is a service that functions as a networked data distribution agent in support of conveying and processing data and commands in a distributed deployment. It is a high performance application that is able to handle multiple commands and data streams from multiple source trail files, concurrently.	No	Yes. See Distribution Server
Receiver Server	The Receiver Server target type is the central control service that handles all incoming trail files. It interoperates with the Distribution Server and provides compatibility with the classic architecture pump for remote classic deployments.	No	Yes. See Receiver Server.

This topic describes the following:

- Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances
- Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance
- Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance

2.2.1 Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances

Ensure to upload the SSL certificate to the Oracle Enterprise Manager Agent:

- Go to the *EMAgent* location and run the `emctl` command for uploading the certificate. For example:

  ```
  ./emctl secure add_trust_cert_to_jks -password welcome -trust_certs_loc
        /<certification location>/rootCA_Cert.pem -alias <alias name of the
  certification>
  ```

  This command adds the certificate to the following: `$EMAGENT_BASE_LOCATION/sysman/config/montrust/AgentTrust.jks`.

2.2.2 Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance

Ensure that the plug-in has already been imported to the Enterprise Manager Cloud Control and deployed to the management agent.

To discover a Classic Instance of the Oracle GoldenGate Enterprise Manager Plug-in:

1. After logging in to the Oracle GoldenGate Enterprise Manager Plug-in, on the main page, select **Setup**, click **Add Target**, and then select **Configure Auto Discovery** to display the **Setup Discovery** page.
2. In **Setup Discovery** page, on the **Targets** tab, select a target and then click **Discovery Modules** to configure the discovery modules.
3. In the **Discovery Module** page that is displayed, select the **Oracle GoldenGate Classic** check box.
4. Click **Edit Parameters** to display the **Edit Parameters: Oracle GoldenGate** dialog box.
5. Enter the following information required to connect to the Oracle GoldenGate agent:
   - **Monitor Agent Host Name**: Enter the hostname of the Oracle GoldenGate instance or Cluster Virtual IP (VIP) of high availability cluster environment (HA/RAC). For example, `<`*`agenthost`*`>.us.oracle.com`. The Monitor agent is a secure tunnel way, and therefore, these agent details are required to connect the Enterprise Manager and Oracle GoldenGate.

     > **Note:**
     >
     > To monitor multiple Oracle GoldenGate instances where individual Oracle Enterprise Manager agent is installed on each of the same host as Oracle GoldenGate, do not use `LOCALHOST`.

     > **Note:**
     >
     > For HA/RAC environments, when the targets are promoted, the host property of the targets is updated with Virtual IP. When these targets are relocated or failed over to another node, they are still accessible using the same monitoring details. This is because the Enterprise Manager agent continues to monitor the Oracle GoldenGate instance irrespective of where the Oracle GoldenGate instance is actually running.

   - **Monitor Agent User Name**: Enter the Monitor agent user name. Enter the user credential that you have used while configuring the Monitor agent.
   - **Monitor Agent Password**: Enter the Monitor agent password.
   - **Monitor Agent Port**: Enter the port number of the agent host. For example, `5559`.

6. Click **OK** when finished in the **Edit Parameters** page.
7. Click **OK** to go back to the **Setup Discovery** page.
8. Select the target host, click **Discovered Targets**, and then click **Discover Now** to discover targets, and click **Yes** in the **Discover Now** confirmation dialog box.
9. After the discovery is successful, click **Close** in the **Confirmation** dialog box.
10. To view the discovery logs in case of an error occurrence, select the target, click **Diagnostic Details**, select **Oracle GoldenGate Classic**, and the click **Log from Agent**.

You need to promote these discovered targets now. See Promoting Oracle GoldenGate Targets.

2.2.3 Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance

Ensure that the plug-in has already been imported to the Enterprise Manager Cloud Control and deployed to the management agent.

You can discover Oracle GoldenGate Microservices target as well as secure Microservices targets. See Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances.

To discover a Microservices Instance of the Oracle GoldenGate Enterprise Manager Plug-in:

1. After logging in to the Oracle GoldenGate Enterprise Manager Plug-in, on the main page, select **Setup**, click **Add Target**, and then select **Configure Auto Discovery** to display the **Setup Discovery** page.
2. In **Setup Discovery** page, on the **Targets** tab, select a target and then click **Discovery Modules** to configure the discovery modules.
3. In the **Discovery Module** page that is displayed, select the **Oracle GoldenGate Microservices** check box.
4. Click **Edit Parameters** to display the **Edit Parameters: Oracle GoldenGate** dialog box.
5. Enter the following information required to connect to the Oracle GoldenGate agent:
   - **Service Manager Host Name**: Enter the host name of the machine on which the Service Manager Service is installed. For example: `*adsvrmgr*.us.oracle.com`.
   - **Service Manager User Name**: Enter the User Name which you have entered while installing the service manager.
   - **Service Manager Password**: Enter the Service Manager Password.
   - **Service Manager Port**: Enter the port number of the host. For example, `8050`.
6. Click **OK** when finished in the **Edit Parameters** page.
7. Click **OK** to go back to the **Setup Discovery** page.
8. Select the target host and then click **Discover Now** to discover targets, and click **Yes** in the **Discover Now** confirmation dialog box.

9. After the discovery is successful, click **Close** in the **Confirmation** dialog box.
10. To view the discovery logs in case of an error occurrence, select the target, click **Diagnostic Details**, select **Oracle GoldenGate Microservices**, and the click **Log from Agent**.

You need to promote these discovered targets now. See Promoting Oracle GoldenGate Targets.

2.3 Promoting Oracle GoldenGate Targets

Once the targets are discovered successfully, you need to promote them in order to view and monitor the targets. After the targets are promoted, they are displayed on the **OGG Home** page.

To promote Oracle GoldenGate targets:

1. In the **Targets on Host** page click **Discovered Targets** to view a list of discovered targets.
2. From this list, select a target that you want to promote, and then click **Promote** to display the **Custom Promotion for GoldenGate Targets** page. In this page, you can deselect the processes, which are not required for promotion.

   > **Note:**
   >
   > When you select any target, its parent targets are auto selected.

3. Click **Promote** in the **Custom Promotion for GoldenGate Targets** page.
4. Click **Yes** in the **Confirmation** dialog box if you want to manage agents.
5. After the promotion is sucessfully completed, click **Close** to display the **Manage EM Agents for OGG instance** page.
6. Select the **Target Name** and then click **Submit**.

   An **Information** box is displayed indicating that the changes are submitted successfully.
7. Click **OGG Home** to display all the targets that are promoted.

   Once a target is successfully promoted, the target is displayed on the **Home** page, and the Management Agent installed on the target host begins collecting metric data on the target. See Target Metrics Available on OGG Home Page.

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

2.4 Verifying and Validating the Plug-in Deployment

Before verifying and validating the Enterprise Manager Plug-In for Oracle GoldenGate, you must promote the Oracle GoldenGate target that is found during auto-discovery.

For more details, see Discovering, Promoting, and Adding Targets in the *Enterprise Manager Cloud Control Administrator's Guide*.

To verify and validate that Enterprise Manager is properly monitoring the plug-in target:

1. Click **Oracle GoldenGate target** 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 the configuration data can be seen. If configuration data doesn't immediately appear, click **Refresh** on the Latest Configuration page.

2.5 Configuring 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. Select the User for whom you need to modify the access.
4. Ensure that you have the target types Host, Agent, Oracle GoldenGate (in case of a classic instance), and Oracle GoldenGate Service Manager (in case of a Microservices instance)
5. Click **Edit** to modify access for an existing user.
6. Click **Create/Create Like** to create a new user and to assign the appropriate user roles to display the **Properties** tab.
7. 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.
8. 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.

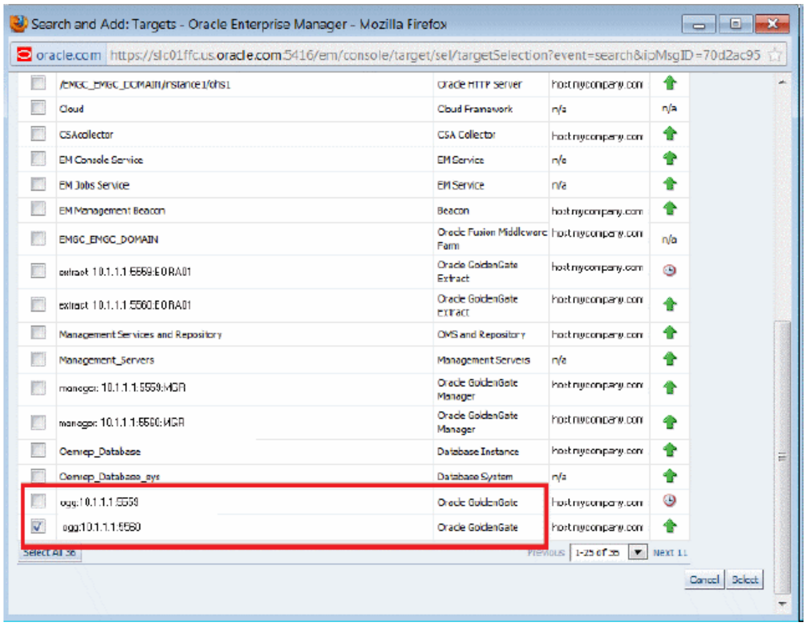
Enterprise Manager (EM) supports object-level access control so administrators can be given roles for specific targets only. See Creating Roles for Systems Infrastructure Administration in the *Enterprise Manager Cloud Control Administrator's Guide*.

9. Click **Next** to open the Target Privileges page.
10. 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.
11. 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.
12. Ensure to add the targets Host (in case of classic) or Agent (MA) appropriately based on the the instnaces.
13. 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.



Search and Add: Targets - Oracle Enterprise Manager - Mozilla Firefox

oracle.com https://slc01ffc.us.oracle.com:5416/em/console/target/sel/targetSelection?event=search&ipMsgID=70d2ac95

□	/EMGC_EMGC_DOMAIN/instance1/ohs1	Oracle HTTP Server	host.mycompany.com	↑
□	Cloud	Cloud Framework	n/a	n/a
□	CSAcollector	CSA Collector	host.mycompany.com	↑
□	EM Console Service	EM Service	n/a	↑
□	EM Jobs Service	EM Service	n/a	↑
□	EM Management Beacon	Beacon	host.mycompany.com	↑
□	EMGC_EMGC_DOMAIN	Oracle Fusion Middleware Farm	host.mycompany.com	n/a
□	extract 10.1.1.1:5559:EORA01	Oracle GoldenGate Extract	host.mycompany.com	◷
□	extract 10.1.1.1:5560:EORA01	Oracle GoldenGate Extract	host.mycompany.com	↑
□	Management Services and Repository	OMS and Repository	host.mycompany.com	↑
□	Management_Servers	Management Servers	n/a	↑
□	manager: 10.1.1.1:5559:MGR	Oracle GoldenGate Manager	host.mycompany.com	↑
□	manager: 10.1.1.1:5560:MGR	Oracle GoldenGate Manager	host.mycompany.com	↑
□	Oemrep_Database	Database Instance	host.mycompany.com	↑
□	Oemrep_Database_sys	Database System	n/a	↑
□	ogg:10.1.1.1:5559	Oracle GoldenGate	host.mycompany.com	◷
☑	ogg:10.1.1.1:5560	Oracle GoldenGate	host.mycompany.com	↑

14. 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.

15. Click the **Edit Individual Privileges** link under the **Manage Target Privilege Grants** Column, which is the third-last column from the right, 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`, and `Resume`) for OGG targets. You can also select these control operations from the **Target** drop-down list in the Oracle GoldenGate Home page. Select a control operation to display a confirmation dialog box. Once you click Yes in the confirmation dialog box, the action is sent to Oracle GoldenGate Core for execution. The dialog box refreshes automatically to check the progress of the command. An Error or Success of the command is displayed in the same dialog box. When you click **OK**, the Home page is refreshed with the latest status of the target.
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* .

16. Click **Continue**.

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

    The user now has access to the selected instance(s). The priviliges available for all targets are:

    - Edit any OGG Parameter File
    - Run any OGG command
    - View contents of any OGG discard file
    - View contents of any OGG report file

    These privileges are automatically assigned from top to bottom in the hierarchy. For example, if the *Run any 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 any 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.

18. 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 Overview in the *Cloud Control Security Guide*.

2.5.1 Authorizing Users with Permissions

As an administrator user, you can provide the following permissions to the users: Editing an Oracle GoldenGate parameter file, running an Oracle GoldenGate command, viewing the contents of any Oracle GoldenGate discard file, and viewing contents of any Oracle GoldenGate report file.

To provide permissions to the users:

1. Log in as a super admin (for example, `sysman`).

   The super admin user can create Named Credentials for the Monitoring Agent (in case of classic instances) and Monitoring Credentials for Service Manager Agent (in case of MA instances). The super admin user grants permissions to the users. The user, after logging in to the Enterprise Manager Cloud Control with the new user credentials can then set the corresponding credentials based on the type of instances
2. Select **Setup, Security, Administrators** to open the Administrators page.
3. Click **Edit** to modify access for an existing user.
4. Click **Next** to display the **Privileges applicable to all Targets** page to view all the four permissions.
5. Select the required permission and click **Submit**.

> **Note:**
>
> - The buttons are disabled for the users if they don't have the required permission. For example, if the user doesn't have Edit Parameters permission, then the **Edit** button in the Configuration tab for all the targets is disabled.
> - If the users are already logged-in and their permissions are changed by the super administrator, then new permissions are reflected in the user interface (UI) once the logged-in user refreshes the page.
> - If you happen to remove permissions for a logged-in user who has the command privileges, then when the user clicks any of the command buttons, such as Start, Stop, Kill, or Resume, then an error message is displayed that says that the user doesn't have sufficient permissions.

2.6 Monitoring the 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 in 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. Select **Setup, Add target, Configure Auto Discovery**.
6. Select the host and click **Discovery Modules** to provide credentials details by selecting Goldengate discovery.

   See Discovering an Oracle GoldenGate Enterprise Manager Plug-in Processes.
7. 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 to display a confirmation dialog box (that says **Do You Want to Manage Agents now?**) when the promotion process is completed.

   b. In the confirmation dialog box, click **Yes** to **Manage Agents**.

   > **Note:**
   >
   > You can bypass the **Manage Agents** page that displays a confirmation page. By bypassing this page, the promotion of the Oracle GoldenGate targets happens quickly.

8. Click **Submit** from the **Manage Agents** page to display a confirmation page. However, this is an optional step.

   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 the changes.

   If you don't want to make any such changes, you can click **Oracle GoldenGate Home** and navigate back to the Oracle GoldenGate plug-in home page.

   After the process promotion, you can see the promoted target in the Oracle GoldenGate Home page.

9. If you want to start, stop, or kill the process, then navigate to the corresponding process page and then select appropriate controls.

10. Click **Targets**, select **GoldenGate**, and then select the process, which you want to either start or stop.

    You can select any of the processes, such as Extract, Replicat, or Data Pump to start or stop.

    The status of the Oracle GoldenGate processes is reflected according to the option you selected (**Start/Stop/Kill**) and it gets reflected in both the **OGG Home** page as well as **Process Details** page. Click **Refresh** to view the updates.

3 Setting the Credentials

This topic details the following:

- Credentials - Overview
- **Different Credential Sets for Oracle GoldenGate**
- Setting the Preferred Credentials for Oracle GoldenGate Classic Instances
- Setting Credentials for Oracle GoldenGate Microservices Instance

For more information on setting credentials, watch the Setting Credentials in Oracle GoldenGate Enterprise Manager Plug-in video.

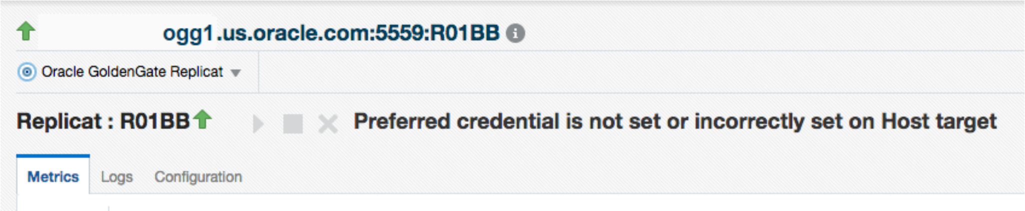
3.1 Credentials — Overview

The Enterprise Manager Credential subsystem enables the Enterprise Manager Administrators to store credentials in a secure manner — as preferences or operation credentials. The credentials can then be used to perform different system management activities, such as real-time monitoring, patching, provisioning, and other target administrative operations.

You need to set the Preferred Credentials for Oracle GoldenGate classic instance and set the Monitoring Credentials for Oracle GoldenGate microservices (MA) instance.

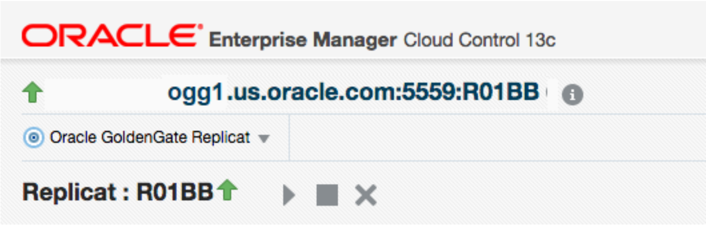
Before setting credentials, you can notice that the process action buttons are grayed out:

Figure 3-1 Action Buttons are not active



Preferred credential is not set or incorrectly set on Host target

Figure 3-2 Action Buttons are active


ORACLE Enterprise Manager Cloud Control 13c
ogg1.us.oracle.com:5559:R01BB
Oracle GoldenGate Replicat
Replicat : R01BB

3.2 Different Credential Sets for Oracle GoldenGate

Preferred credentials are used to simplify access to the managed targets by storing target login credentials in the Management Repository. Preferred credentials are required for performing the administrative tasks for the Oracle GoldenGate classic instances.

Preferred credentials are set on a per-user basis, thus ensuring the security of the managed enterprise environment. The credentials are hierarchical in nature. For example, if credentials are provided for Oracle GoldenGate target type, then by default, they are applicable to its child target types as well, which means that they are applicable for Oracle GoldenGate Extract, Manager, or Replicat processes. Preferred Credentials are of the following types: Host Credential and OGG Admin Credentials.

Host Credential
Host Credential is the credential to login to the Enterprise Manage Agent host machine.

OGG Admin Credentials
OGG Admin Credentials is the credentials of Oracle GoldenGate Monitoring Agent. The username is defined in the `config.properties` in the Oracle GoldenGate Monitoring Agent installation.

3.2.1 Monitoring Credentials

Monitoring credentials are required to perform the administrative tasks for the Oracle GoldenGate microservices instances.

The monitoring credentials are hierarchical in nature. For example, if credentials are provided for Oracle GoldenGate Service Manager target type, then by default, they are applicable to its child target types as well, such as Oracle GoldenGate Administration/ Distribution/Receiver Server. For monitoring credential, use the same credential that can access Service Manager on Oracle GoldenGate microservices instances.

3.3 Setting the Credentials for Oracle GoldenGate Classic Instance

To create preferred credentials:

1. Navigate to the **Setup** menu, select **Security**, then select **Preferred Credentials**.
2. On the **Preferred Credentials** page, type **goldengate** in search box, then click **Search**.
3. Under the **Target Type** column, click **Oracle GoldenGate** to highlight the row, then click **Manage Preferred Credential**
4. On the **Oracle GoldenGate Preferred Credentials** page, you can create both the Default Preferred Credentials as well as the Target Preferred Credentials.

   If you want to set a preferred credential for Oracle GoldenGate, which is applicable for all Oracle GoldenGate targets, then go to **Default Preferred Credentials**.

If you want to set a preferred credential for Oracle GoldenGate applicable only to a specific Oracle GoldenGate target, then go to **Target Preferred Credentials**.

5. Under **Default Preferred Credentials**, select the **Host Credentials** credential set, and click **Set** to display the **Select Named Credential** dialog box. Create new or use existing credential that can be used to login to the EM Agent host machine.
6. Under Default Preferred Credentials, select **OGG Admin Credentials** credential set, and click **Set** to display the **Select Named Credential** dialog box. Create new credential by entering the same JAgent credential that was used to discover this GoldenGate instance, or use an existing one.
7. Under **Target Preferred Credentials**, click on a target with **Host Credentials** credential set, then click **Test** by wrench icon. It brings up the **Test Named Credential** page. Keep the Test Type as **Basic**, and click **Test** button. Ensure all targets with **Host Credentials** credential set are tested with successful results.

3.4 Setting Credentials for Oracle GoldenGate Microservices Instance

To set the monitoring credentials for Oracle GoldenGate microservices (MA) instance:

1. Navigate to the **Setup** menu, select **Security**, and then select **Monitoring Credentials** to display the **Security > Monitoring Credentials** page.
2. Type **goldengate service** in the search box, then click **Search**.
3. Select the Oracle GoldenGate Service Manager Target Type.
4. Click **Manage Monitoring Credentials** to display the **Oracle GoldenGate Monitoring Credentials** page.
5. Select the Target Name and click **Set Credentials** to display the **Enter monitor credentials** dialog box.
6. Enter the service manager Username, Password, and Confirm Password, and click **Save**. (same Service Manager credential that was used to discover this GoldenGate instance).

   The Monitoring Credentials are set and this information is indicated on the screen.

> **Note:**
>
> The Monitoring Credentials should only be set for GoldenGate microservices instance. Do not use Monitoring Credentials for classic instance. To set Monitoring Credentials for multiple targets, you can use `emcli create_credential_set` verb with the `-monitoring` option.

4 Monitoring Oracle GoldenGate Targets

After you have set the credentials for the targets, you can monitor them. For a few targets, such as the Extract and Replicat, the **Start**, **Stop**, and **Kill** buttons are enabled, using which, you can manage the targets by performing the start and stop operations.

To view the target details:

1. In the Oracle GoldenGate Enterprise Manager Plug-in, click **Targets** and then select **GoldenGate** to display the **OGG Home** tab.
2. Click the target name to view correspond target details, such as metrics, logs, and configurations.

If the process is up, then the status of the target types is indicated as Up by an **Up** arrow, if not the status of the target types is also down. This topic describes the target types for Microservices and Classic instances.

4.1 Start and Stop a Target

You can use the start, stop, or kill the Extract or Replicat targets, for which the credentials have been set.

To start, stop, or kill the targets:

1. Go to the **OGG Home** page.

   (Optional) Enter the result of the step here.
2. Select either the Extract or Replicat Process.
3. Click one of the following: **Start**, **Stop**, or **Kill**.

4.2 Metrics Tab

The **Metrics** tab on the Targets page enable you to monitor metrics and to alert users about specific metric results.

For more information about the target-specific metrics that are dispayed on the OGG Home page, see Target Metrics Available on OGG Home Page.

4.3 Log Tab

For targets, such as Extract and Replicat, the **Log** tab contains the following: **Report**, **Discards**, and **GGS Error Log**.

- **Report**: The **Report** tab contains a list of reports generated for the selected target type. The files have an extension of `.rpt`. These report files contain details of the targets, such as target directories, database versions, parameters they run on, and recovery parameters.

- **Discards**: If there are any discard files specified in the parameter files and the file exists in Oracle GoldenGate Core, then these files are also displayed in the **Discards** tab as a list of Discard Files. You can specify the names of the folder, files, or file extensions of your choice. The default discard files are read from the `dirrpt` folder, for example, `dirrpt/processName*.dsc`. Note that the file name is an absolute path of the discard file or path related to the `OGGCORE` location and file extension can be any of the following: `.txt`, `.discard`, or `.dsc`. You can specify multiple discard files as follows:

  ```
  DISCARDFILE dirrpt/File1.txt, APPEND, MEGABYTES
  DISCARDFILE dirdat/File2.txt, APPEND, MEGABYTES
  ```

- **GGS Error Log**: The **GGSERR log** tab shows the file contents of the `ggserr.log` file.

4.4 Configuration Tab

The **Configuration** tab displays the entire parameter file in view mode. At runtime, new tabs get added on the **Configuration** tab for the Oracle GoldenGate properties file. There can be multiple such tabs for these files. You can modify the content of the property and parameter files.

To modify the files on the **Configuration** tab:

1. In the **Configuration** tab, click **Edit** to reopen the parameter file in an edit mode.
2. Click the filename (hyperlink) in the parameter file to create a new tab next to the parameter tab. The tab title is displayed as the `include/obey` file name.

   > **Note:**
   >
   > The absolute path to the file is displayed at the bottom of the tab. The content of the existing `include/obey` file is displayed in new tab. If the file doesn't exist (for example, user-typed new file name in editing mode) the empty tab is displayed with a warning message above the text area.

3. Click **Save** after you have made the chages. If you haven't modified any content, then no action is taken.

If you want to revert the changes to the parameter configuration files, then click **Reload**. Changes made to the parameters file in the text area is discarded.

If you want to verify whether the property (or parameter) file is edited, then:

1. Edit the properties file from the Oracle GoldenGate Enterprise Manager Plug-In user interface and save it.
2. Go to the Oracle GoldenGate Core and check for these changes.
3. Add or remove content from the Oracle GoldenGate side and click **Refresh** on the Oracle GoldenGate Enterprise Manager Plug-In side.

   Existing properties files are displayed in the Oracle GoldenGate Enterprise Manager Plug-In UI.

4.5 Supported Target Types

This topic lists the target types supported in Classic and Microservices instances.

4.5.1 Target Types Supported in Classic

The target types supported in Oracle GoldenGate Enterprise Manager Classic instances are as follows:

- Oracle GoldenGate
- Extract and Replicat
- Manager

4.5.1.1 Oracle GoldenGate

Oracle GoldenGate target type represents an Oracle GoldenGate classic instance. It's the parent target of Manager, Extract, and Replicat targets.

The Oracle GoldenGate target displays the collective status of all the processes available in Oracle GoldenGate excluding the Initial Load processes. The following is an example that illustrates how the collective status of this target works: there may be 5 Extract and Replicat processes and 2 Initial Load processes in Oracle GoldenGate, out of which, only 2 are discovered and promoted in the Oracle Enterprise Manager. This means that a subset of the Oracle GoldenGate processes is being monitored in the Enterprise Manager. However, the Oracle GoldenGate target displays the collective status of all the processes available in Oracle GoldenGate, and does not display only the status of the processes that are monitored in the Enterprise Manager.

4.5.1.2 Extract and Replicat

You can view detailed metrics of Extract, logs, and configuration of extract on an Extract page; and view detailed metrics of Replicat, logs, and configuration of Replicat on a Replicat page.

For more information, see the Extract and the Replicat target types, see Extract and Replicat.

4.5.1.3 Manager

The Manager process controls all the Oracle GoldenGate processes in the classic instance. Part of its role is to generate information about critical monitoring events, which it passes to the agent. For target types Replicat, Extract, and Manager, you can control the process though start, stop, kill, and resume actions.

This topic discusses the Manager process for Oracle GoldenGate Enterprise Manager Plug-in Classic instance.

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

Metric	Description
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

4.5.2 Target Types Supported in Microservices

The target types supported in Oracle GoldenGate Enterprise Manager Microservices instances are as follows:

- Administration Server
- Extract and Replicat
- Service Manager
- Deployment
- Distribution Server
- Receiver Server
- Performance Metrics Server

4.5.2.1 Administration Server

You can use the Administration Server page to manage Extract and Replicat processes and to monitor the metrics of these processes.

4.5.2.2 Extract and Replicat

On the Extract target and Replicat target pages, you can view the respective Oracle GoldenGate process metrics, set alerts for these metrics, view logs, configuration files, and monitor historical trends.

The following table lists the metrics used to monitor the Extract and Replicat processes. Metrics are fetched every 60 seconds by default from the targets. However, you can change the fetch frequency.

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 of DELETE operations that were processed by the selected Oracle GoldenGate process since the last fetched value. **Valid values:** A positive integer
Delta Discards	**Valid for Extract and Replicat** Shows the DISCARD operations that were processed by the selected Oracle GoldenGate process since the last fetched value. **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 fetched value. **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 fetched value. **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 fetched value. **Valid values:** A positive integer
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 fetched value. **Valid values:** A positive integer
Delta Operations	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) and Data Manipulation Language (DML) INSERT, UPDATE, DELETE, AND TRUNCATE operations that were processed by the selected Oracle GoldenGate process since the last fetched value. **Valid values:** A positive integer

Metric	Description
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 fetched value. **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 fetched value. **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 fetched value. **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 fetched value. **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. **Note:** End of File metrics value 0 means FALSE. For the alert template, ensure to use the stored metric values 0 and 1, where 0 means FALSE and 1 means TRUE. **Note:** For the alert template, ensure to use the stored metric value in milliseconds (since Unix Epoch) to all the following metrics: last_checkpoint_ts, last_processed_ts, last_operation_ts, start_time, last_checkpoint_ts, last_processed_ts, last_operation_ts, start_time.
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 theOracle GoldenGate process and its data source. This lag value should match the value that is returned from the GGSCI command SEND *group*GETLAG . **Valid values:** The lag time, in seconds
Last Checkpoint Timestamp	**Valid for Extract and Replicat** Shows the time when the last checkpoint was written by the process. **Valid values:** Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM | PM}, for example: 01/14/2011 09:36:32 AM.

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

Metric	Description
Total Discards	**Valid for Extract and Replicat** Shows the total number of operations that were discarded by the selected Oracle GoldenGate process in its current run session. The records are written to the discard file that is associated with the process. **Valid values:** Positive integer.
Total Executed DDLs	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) operations that were processed by the selected Oracle GoldenGate process in its current run session. **Valid values:** Positive integer
Total Ignores	**Valid for Extract** Shows the total number of Data Manipulation Language (DML) operations that were ignored by the process in its current run session. Errors are included in the Total Ignores metric. **Valid values:** Positive integer
Total Inserts	**Valid for Extract and Replicat** Shows the total number of Data Manipulation Language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process in its current run session. The statistic reflects the total operations performed on all of the tables that are specified in the parameter file for that process. **Note:** If any tables are mapped to targets in the Extract configuration, the statistics will reflect the total operations for all of the targets. **Valid values:** A positive integer
Total Operations	**Valid for Extract and Replicat** Shows the total number of Data Definition Language (DDL) and Data Manipulation Language (DML) 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
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

Metric	Description
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

4.5.2.3 Service Manager

The **Service Manager** page lists all the Oracle GoldenGate Miscroservices Architecture deployments.

The **Service Manager** page lists the following for each deployment:

- **Service Name**: Name of the service, for example: `distsrvr:8062`
- **Service Type**, such as Administration Server, Distribution Server, Performance Metrics Server, or Receiver Server
- **Port -** Port number
- **Status** - This is the status of the service type.

4.5.2.4 Deployment

Following are the details that you can view for each deployment.

Details	Description
Status	Status of target deployment. For example, **running**.
GoldenGate Home	The Oracle GoldenGate home that is created on a host computer is the directory that you choose to install the product. This read-only directory contains binary, executable, and library files for the product. The default directory path is: `/ogg_install_location`.
GoldenGate Etc Home	The location in which your deployment configuration files are stored including parameter files. The default directory path is: `/ogg_deployment_location/etc`.
GoldenGate Conf Home	The location in which each deployment information and configuration artifacts are stored. The default directory path is: `/ogg_deployment_location/etc/conf`.
GoldenGate SSL Home	The location in which each deployment security artifacts (certificates, wallets) are stored. The default directory path is: `/ogg_deployment_location/etc/ssl`.
GoldenGate Var Home	The location in which each deployment logging and reporting processing artifacts are stored. The default directory path is: `/ogg_deployment_location/var`.
GoldenGate Data Home	The location in which each deployment data artifacts (trail files) are stored. The default directory path is: `/ogg_deployment_location/var/lib/data`.
Managed by Service Manager	Indicates whether the deployment is managed by the Service Manager. Valid values: **true** or **false**.

4.5.2.5 Distribution Server

The Distribution Server displays the distribution path, and the details of each path, such as status, time taken for data movement, source and target path details, and the database name.

Path Details	Description
Distribution Server Path Name	Path Name of the Distribution Server
Status	Status of the Distribution Server. Valid values are: • Running • Stopped
Processing Lag	Time (number of seconds) taken to move the data from source to target.
Source	Complete path name of the Distribution server.
Target	Complete path name of the Receiver server.
DB Name	Name of the database from which the Extract target is fetching the data from.
Extract	Name of the Extract target (to which the data is fetched into) the Distribution server is connected to.

4.5.2.6 Receiver Server

The Receiver Server displays the receiver path, and the details of each path, such as status, time taken for data movement, source and target path details, and the database name.

Path Details	Description
Receiver Server Path Name	Path Name of the Receiver Server
Status	Status of the Receiver Server. Valid values are: • Running • Stopped
Processing Lag	Time (number of seconds) taken to move the data from source to target.
Source	Complete path name of the Distribution server.
Target	Complete path name of the Receiver server.
DB Name	Name of the database from which the Extract target is fetching the data from.
Extract	Name of the Extract target (to which the data is fetched into) the Receiver server is connected to.

4.6 Target Metrics Available on OGG Home Page

After the target is promoted, you can view its details on the **OGG Home** page. For each process in the instance, the Oracle GoldenGate Enterprise Manager Plug-In Home page displays the target details:

- Target name

- Target types as follows: Manager, Extract, Replicat (in case of Oracle GoldenGate classic instance), or Service Manager, Deployment, Administration Server, Performance Metrics Server, Distribution Server, Receiver Server, Extract, Replicat (in case of Oracle GoldenGate Microservices instance).
- Status
- Lag (in seconds)
- Lag Trend
- Sparkline graphs that display lag trends
- Total operations
- Delta operations
- Delta operations per second
- Incidents
- Time elapsed since last Oracle GoldenGate checkpoint
- Timestamp of last Oracle GoldenGate checkpoint
- Viewing summary of all Oracle GoldenGate instances on a single, customizable web page
- In depth examination into dozens of metric values and metric history.
- Automated notifications and ticket creation through incidents.

4.7 Elements for Monitoring Targets

Table 4-1 Elements Available for Monitoring Targets

Element	Description
All Metrics	Display all of the metrics defined for the target.
Metrics and Collections Settings	Displays the metric thresholds and collection interval for the target.
Metrics Collection Errors	Displays the details about the errors encountered while obtaining target metrics. This helps to get the detail of the metric that do not represent the performance of the target accurately.
Status History	Displays information about target outages. This information is essential for troubleshooting target related incidents. For more information, see Viewing Target Status and Availability History in *Enterprise Manager Cloud Control Middleware Management Guide* and Monitoring Oracle GoldenGate Targets.
Incident Manager	Displays details about the various events, related to the GoldenGate target, that negatively impact any hardware or software component. These events require user action. The details provided by this section, such as the incident summary, severity, target, or target type, are essential for troubleshooting.
Alert History	Displays a complete alert history of the target.

For more information about these various elements, see Monitoring and Managing Targets in the *Enterprise Manager Cloud Control Administrator's Guide*.

5

Managing Events, Alerts, and Incidents

For more information about managing events, incidents, and problems, see Managing Events, Incidents, and Problems in the *Enterprise Manager Cloud Control Administrator's Guide*. For a list of common elements available for all the targets, see Elements for Monitoring Targets.

5.1 Events

An event is a significant occurrence that indicates a potential problem. When a metric threshold value is reached, a metric alert is raised. A metric alert is a type of event. An alert can also be generated for various target availability states.

Event Types

Typically, key event types used in Enterprise Monitoring are:

- **Metric Alert**: A metric alert event is generated when an alert occurs for a metric on a specific target or metric on a target and object combination, such as *Lag Exceeding a Specified Threshold Value*.
- **Target Availability**: The Target Availability Event represents a target's availability status. For example: Up, Down, Agent Unreachable, or Blackout. For more information on all the targets available in Oracle GoldenGate, see Supported Target Types.

5.2 Metric Data and Alerts

Metric data refers to the collection of data that changes frequently. You can create alerts on the metric data. Oracle GoldenGate delivers predefined metric types and default collection times for each target type.

To view the metric data for a target, click the **Target** drop-down, select **Monitoring**, and then click **All Metrics**. The following are the metric data for Oracle GoldenGate Extract and/or for Replicat targets:

- Checkpoint Position
- Name
- Status
- Start Time
- End of File
- Lag (Sec)
- Total Inserts
- Delta Inserts
- Total Deletes
- Delta Deletes

- Total Truncates
- Delta Truncates
- Total Operations
- Delta Operations
- Delta Operation Per seconds
- Total Executed DDLs
- Delta Executed DDLs
- Total Discards
- Delta Discards
- Total Ignores
- Delta Ignores
- Last OGG Checkpoint Timestamp
- Last Processed Timestamp
- Delta Row Fetch Attemps
- Delta Row Fetch Failures
- Total Row Fetch Failures

For more information on the metric data, see Extract and Replicat. The metric data collected is saved to the Management Repository and is compared to the predefined thresholds for each target. If a threshold is reached, then the system generates an alert. The Incidents are displayed on each of the target's homepage.

5.3 Incidents and Alerts

An incident is a unit containing a single, or closely correlated set of events that identify an issue that needs administrator attention. Although incidents can correspond to a single event, incidents more commonly correspond to groups of related events.

Incidents indicates a potential problem; either a warning or critical threshold for a monitored metric has been crossed.
The Oracle Enterprise Manager provides various options to respond to Incidents. Administrators can be notified automatically when an alert triggers and can set up corrective actions to resolve an alert condition automatically.

You can set metric alerts and also generate alerts for various target availability states. This topic details the following:

- Setting Metric Alerts and Incidents for Extract and Replicat
- Setting Incidents and Alerts for Oracle GoldenGate Target Availability

5.3.1 Setting Metric Alerts and Incidents for Extract and Replicat

For more information on how a metric alert can be set for Oracle GoldenGate target, see the video on Setting Incidents and Email Alerts in the GoldenGate Enterprise Manager Plug-in.
If you want to set alerts of metric status values, the following are the status values for Extract and Replicat.

- Registered - 2
- Starting - 3
- Running - 7
- Stopping - 8
- Stopping Forcefully - 9
- Stopped - 10
- Stopped Forcefully - 11
- Abended - 12
- Killed - 13
- Unresponsive - 16

For a list of metrics used to monitor Extract and Replicat, see Extract and Replicat.
Oracle recommends to set alerts for target availability to monitor the status of the targets.

5.3.2 Setting Incidents and Alerts for Oracle GoldenGate Target Availability

You need to set alerts on Target Availability of Oracle GoldenGate targets to get notified when there are any issues with these targets.

This includes occurrences when the Enterprise Manager is unable to retrieve status of Oracle GoldenGate targets, or is unable to communicate with the Oracle GoldenGate Monitor Agent in case of Oracle GoldenGate classic targets.
To set incidents and alerts for target availability:

1. On the Home page, click **Setup**, select **Incidents**, and then click **Incident Rule** to display the **Incident Rules - All Enterprise Rules** page.
2. Click **Create Rule Set...**.
3. Enter a **Name**, for example **Incident management rule set for Target Availability** and click **Save**.
4. In the **Target** area, select **All Targets of types**, and select the target type from the adjacent drop-down.
5. In the **Rules** area, click **Create...** to display the **Select Type of Rule to Create** dialog box.
6. Select **Incoming events and updates to events** and click **Continue** to display the **Create New Rule: Select Events** page.
7. Select **Target Availability** from the **Type** drop-down list and click **Next** to display the **Create New Rule: Add Actions** page.
8. Click **Add** to display the **Add Conditional Actions** page, select **Always execute the actions**.
9. Under **Send Notifications**, expand **Basic Notifications**, and enter email IDs in **E-mail To** and **E-mail Cc** to assign recepients for notifications. These email IDs can belong to the users of the Enterprise Manager.
10. Click **Continue** to view the **Action Summary** in the **Create New Rule: Select Events** page.

11. Click **Next** to display the **Create New Rule: Specify Name and Description** page, where a new Rule, for example, **rule 166** is displayed. You can either specify a rule name or click **Next** to accept the pre-specified name to display the **Create New Rule: Review** page.
12. Click **Continue** and then click **Save** to save the new rule.
    In this example, a rule 166 has been successfully created and added to the current rule set. **Incident management rule set for Target Availability** is the incident rule set that has been set on Target Availability of the selected targets, which will trigger alert and send emails to the recepients specified in case of issues or events with these targets.

For more information, see Using Incident Management in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

5.4 Alerts on Home Page

The Oracle GoldenGate Home page displays all the incidents that are generated. An alert is generated when a metric threshhold is reached. The most recent alerts are listed first.

See Incident Manager in Elements for Monitoring Targets.
To view the alerts on the **OGG Home** page:

1. On the **OGG Home** page, click the number (Critical or Warning) under **Incidents** to display the **Incident Manager**.
2. Click an alert message to view all the details about the selected metric in the alert.

For more information, see Using Incident Management in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

6 Audit Logging

This chapter describes how to enable logs for auditing and how to view audit logs in the Enterprise Manager.

6.1 Enabling 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 GoldenGate 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 (;). The following is the command to enable all audit logging for the Enterprise Manager Plug-In for Oracle GoldenGate.

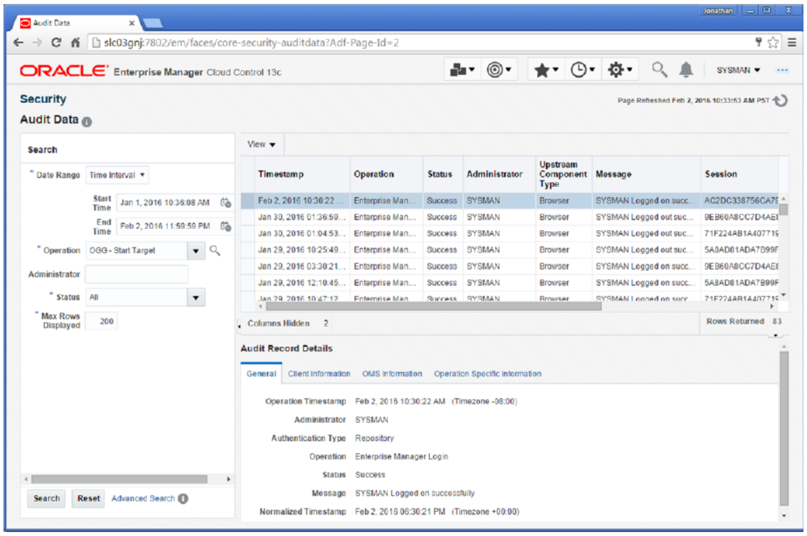
```
emcli update_audit_settings -
operations_to_enable="OGG_START_TARGET;OGG_STOP_TARGET;OGG_KILL_TARGET;OGG_VIEW_R
EPORT;OGG_VIEW_DISCARD;OGG_VIEW_GGSERRLOG;OGG_EDIT_PARAM"
```

6.2 Viewing the 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.


Audit Data
slc03gnj:7802/em/faces/core-security-auditdata?Adf-Page-Id=2
Jonathan
ORACLE Enterprise Manager Cloud Control 13c
SYSMAN
Security
Audit Data
View
Search
Reset
Advanced Search

Page Refreshed Feb 2, 2016 10:33:53 AM PST

Search

* Date Range	Time Interval
Start Time	Jan 1, 2016 10:36:08 AM
End Time	Feb 2, 2016 11:59:59 PM
* Operation	OGG - Start Target
Administrator	
* Status	All
* Max Rows Displayed	200

Timestamp	Operation	Status	Administrator	Upstream Component Type	Message	Session
Feb 2, 2016 10:30:22 ...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	AC2DC338756CA79
Jan 30, 2016 01:36:59...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	9EB60A8CC7D4AE8
Jan 30, 2016 01:04:53...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	71F224AB1A407719
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...	9EB60A8CC7D4AE8
Jan 29, 2016 12:10:45...	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	5A8AD81ADA7B99F
Jan 29, 2016 10:47:12	Enterprise Man	Success	SYSMAN	Browser	SYSMAN Logged on succ	71F224AB1A407719

Columns Hidden 2

Rows Returned 83

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 +00:00)

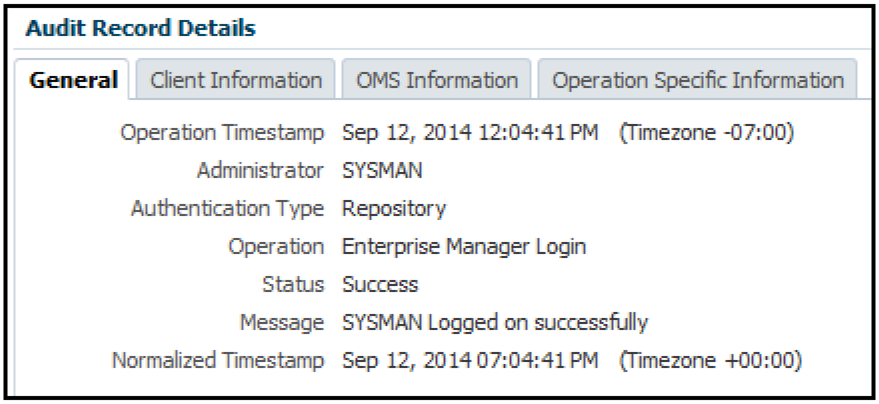
2. Select your search criteria, such as date range, operations, or status.

   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** to display the search results in a grid format.

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.



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)

For additional information about the auditing feature in Enterprise Manager, see Configuring the Audit Data Export Service in the *Enterprise Manager Cloud Control Security Guide*.

7

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

- About Hybrid Cloud Monitoring
- Installing the Monitor Agent on Cloud Device to Configure the Oracle GoldenGate Monitoring Agent
- Creating an Inventory Location for Non Oracle Users
- Configuring Oracle GoldenGate Monitoring Agent in the Provisioning Environment
- Installing the Hybrid Cloud Gateway Agent
- Configuring the EM Hybrid Cloud
- Configuring the SOCKS Proxy Setup

7.1 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*.

7.2 Installing the Monitor Agent on Cloud Device to Configure the Oracle GoldenGate Monitoring Agent

You must install the monitor agent on your cloud device to configure the Oracle GoldenGate Monitoring Agent:

1. Provide the latest release file, which is `fmw_12.2.1.4.0_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.

7.3 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.

7.4 Configuring Oracle GoldenGate Monitoring Agent in the Provisioning Environment

You must configure the Oracle GoldenGate Monitoring Agent 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.

> **Note:**
>
> The `create datastore` command is required only you want to monitor the Oracle GoldenGate instances prior to the Oracle GoldenGate 12.3 release.

The GGSCI should show both the manager and Oracle GoldenGate Monitoring Agent processes.

7.5 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.

7.6 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.

7.7 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

8
Troubleshooting

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

Topics

8.1 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.

8.2 Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files

Following are the Oracle GoldenGate Enterprise Manager Plug-in log files (assuming that `ORACLE_HOME` is set to `/home/oracle/`) 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 Oracle GoldenGate Enterprise Manager Plug-in Agent connects with iAgent, the information is logged in this file.
For example:
`/home/oracle/oem/agent/agent_inst/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:
`/home/oracle/oem/agent/agent_inst/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:

```
/home/oracle/oem/gc_inst/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:

```
/home/oracle/oem/gc_inst/user_projects/domains/EMGC_DOMAIN/servers/
EMGC_OMS1/logs/EMGC_OMS1.out
```

8.3 Availability Error

For the Oracle GoldenGate Microservices targets, you need to set the monitoring credential correctly for getting the target status and other metrics, unlike the classic targets. In case of the classic targets, you do not have to set the preferred credentials to display the metrics.

The preferred credentials were only required to get logs and the **Configuration** tab. If the monitoring credentials are not set, then you need to first set them. If the credentials are set, then you need to check the following:

- whether the Enterprise Manager agent is up and running.
- If the agent is running, then you need to reset the credentials. To change the credentials:

1. Change the username.
2. Save the new username details.
3. Use the same username and password.

A

Enabling the Oracle GoldenGate Enterprise Manager Plug-in Accessibility Features

As a part of an effort to make the Oracle products, services, and supporting documentation accessible and usable to the disabled community, the Oracle GoldenGate Enterprise Manager Plug-in offers several features that make the management data available for users of assistive technology.

See Enabling the Enterprise Manager Accessibility Features in the *Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.