

Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In User Guide



(13.2.3.0.0)

F19471-02

August 2019

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2018, 2019, Oracle and/or its affiliates. All rights reserved.

Primary Author: Oracle Corporation

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

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

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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

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

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	v
Documentation Accessibility	v
Related Documents	v
Conventions	vi

1 Overview

1.1 Home Page	1-1
1.2 Custom Screens	1-1

2 Setting Up Enterprise Manager Plug-In for Oracle GoldenGate

2.1 Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager	2-1
2.1.1 Creating the Oracle Wallet	2-1
2.2 Discovering Oracle GoldenGate Targets	2-2
2.3 Promoting Oracle GoldenGate Targets	2-4
2.4 Verifying and Validating the Plug-in Deployment	2-4
2.5 How do I Configure Instance-Level Security	2-5
2.5.1 Authorizing Users with Permissions	2-8
2.6 Monitoring the High Availability Features	2-8

3 Setting the Credentials

3.1 Credentials — Overview	3-1
3.1.1 Oracle GoldenGate Preferred Credentials	3-1
3.2 Credential Sets for Oracle GoldenGate	3-1
3.3 Setting Preferred Credentials for Oracle GoldenGate Classic Instance	3-2
3.4 Monitoring Credentials for Oracle GoldenGate Microservices	3-2

4 Using the Enterprise Manager Plug-In for Oracle GoldenGate

4.1	Enabling Audit Logging	4-1
4.2	Viewing the Audit Logs	4-2
4.3	Home Page Metrics	4-3
4.4	Monitoring Oracle GoldenGate Targets	4-4
4.4.1	Service Manager	4-5
4.4.2	Administration Server	4-5
4.4.3	Extract and Replicat	4-5
4.4.3.1	Starting, Stopping, or Killing Extract and Replicat Processes	4-10
4.4.3.2	Displaying Discard Files	4-10
4.4.3.3	Editing Files on the Configuration Tab	4-11
4.4.4	Manager	4-12
4.5	Monitoring Current Oracle GoldenGate Metrics and Historical Trends	4-13
4.6	Generating Automatic Alerts and Incidents When Thresholds are Breached	4-14
4.7	Creating an Incident Rule	4-14
4.8	Sending Email Alerts	4-16

5 Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service

5.1	About Hybrid Cloud Monitoring	5-1
5.2	Installing the Monitor Agent on Cloud Device to Configure the JAgent	5-1
5.3	Creating an Inventory Location for Non Oracle Users	5-2
5.4	Configuring JAgent in the Provisioning Environment	5-2
5.5	Installing the Hybrid Cloud Gateway Agent	5-3
5.6	Configuring the EM Hybrid Cloud	5-3
5.7	Configuring the SOCKS Proxy Setup	5-4

6 Troubleshooting

6.1	Correcting ADFC Error on Windows 64-Bit Machines	6-1
6.2	Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files	6-1
6.3	Availability Error	6-2

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 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*.
- [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 \(12.2.1.3.0\) Interoperability and Compatibility](#) in *Understanding Interoperability and Compatibility Guide*.
- [Oracle GoldenGate Plug-in for Oracle Enterprise Manager 13.2.3.0.0 Certifications](#)

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.
<i>italic</i>	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 Home Page

For each process in the instance, the Oracle GoldenGate Enterprise Manager Plug-In Home page displays:

- Target name
- Target types as follows: Manager, Extract, Replicat (in case of Oracle GoldenGate classic instance), or Service Manager, Administration Server, Performance Metric Server, Distribution Server, Receiver Server, Extract, Replicat (in case of Oracle GoldenGate MA instance), and Deployment.
- Process status
- The lag in seconds
- 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.

1.2 Custom Screens

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

- Customizing the display on the home page. This allows the 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
- To support high availability, the **Manage Agent** tab was added to home screen.

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

- [Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager](#)
- [Discovering Oracle GoldenGate Targets](#)
- [Promoting Oracle GoldenGate Targets](#)
- [Verifying and Validating the Plug-in Deployment](#)
- [How do I Configure Instance-Level Security](#)
- [Monitoring the High Availability Features](#)

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](#) 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 (jAgent) is used by classic instance.

To create the Oracle Wallet:

1. Navigate to the `OGG_AGENT_ORA_HOME` directory.

 **Note:**

Oracle GoldenGate 12c (12.1.2.0.0) introduced the storing of passwords for extract and replicats in Oracle Wallets. However, both the Oracle GoldenGate core replication and Oracle GoldenGate 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 `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`

2.2 Discovering Oracle GoldenGate Targets

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.

To discover Oracle GoldenGate targets:

1. In the **OGG Home** page, select **Setup**, click **Add Target**, and then select **Configure Auto Discovery** to display the **Setup Discovery** page.
2. In **Setup Discovery** page, click **Advanced: Discovery Modules** to go to modules page. In the **Discovery Module** page, you can find **GoldenGate Discovery module**.
3. Click **GoldenGate Discovery Module** to display the **Configure Target Discovery for Target Types** page, select the agent host name and click **Edit Parameters** to display the **Edit Parameters: GoldenGate Discovery** dialog box.
4. Enter the following information required to connect to the Oracle GoldenGate agent:
 - **JAgent/Service Manager Username:** Enter the Service Manager User Name in case of the MA instance. In case of a classic instance, enter the jAgent username.
 - **JAgent/Service Manager Password:** Enter the Service Manager Password in case of the MA instance. In case of a classic instance, enter the jAgent password.
 - **JAgent RMI Port/Service Manager Port:** Enter the Service Manager port for the connection in case of the MA instance. In case of a classic instance, enter the jAgent RMI Port.
 - **JAgent/Service Manager Host Name:** Enter the hostname of the Oracle GoldenGate instance or Cluster Virtual IP (VIP) of high availability cluster environment (HA/RAC).

 **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 VIP. 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 monitoring the Oracle GoldenGate instance irrespective of where the Oracle GoldenGate instance is actually running.

- **GoldenGate (Classic or Microservices):** Enter **microservices** if you want to discover Oracle GoldenGate microservices instance or else enter **classic**.
5. Click **OK** when finished to display the **Discovery Module: GoldenGate Discovery module** page.
 6. In the **Discovery Module: GoldenGate Discovery module** page, click **OK** to display the **Setup Discovery** page.

Target discovery has been configured on this host.

7. In the **Setup Discovery** page, click the **Targets on Host** tab.
8. Search for a target host name, and click **Search**.
9. Select the target host and then click **Discover Now** to discover targets, and click **Yes** in the **Discover Now** confirmation dialog box.
10. After the discovery is successful, click **Close** in the **Confirmation** dialog box.

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 successfully 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 [Home Page Metrics](#).

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](#).

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.

2.5 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. Select the User for whom you need to modify the access.
4. Click **Edit** to modify access for an existing user.
5. Click **Create/Create Like** to create a new user and to assign the appropriate user roles to display the **Properties** tab.
6. 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.

7. 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*.

8. Click **Next** to open the Target Privileges page.
9. 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**.

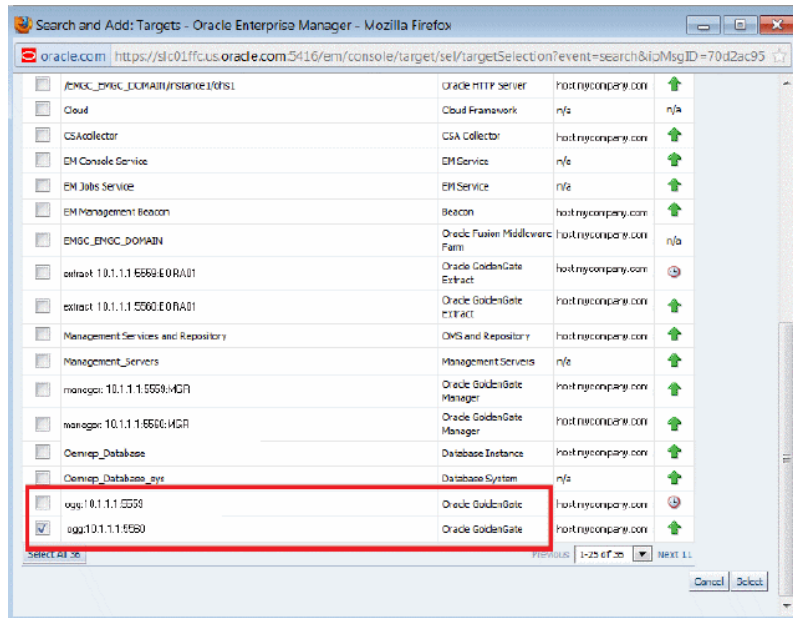
These two roles are required for full functionality and multi-version support.

10. 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.
11. 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.



12. 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.

13. 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 (<i>Start</i> , <i>Stop</i> , <i>Kill</i> , and <i>Resume</i>) 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*.

14. Click **Continue**.
15. 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.

16. 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](#) 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`).
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 Oracle GoldenGate Targets](#).
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](#)
- **Credential Sets for Oracle GoldenGate**
- [Setting the Preferred Credentials for Oracle GoldenGate Classic Instances](#)
- [Monitoring Credentials for Oracle GoldenGate Microservices](#)

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.

3.1.1 Oracle GoldenGate Preferred Credentials

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

3.2 Credential Sets for Oracle GoldenGate

Oracle GoldenGate provides the Preferred credentials in an Oracle GoldenGate classic instance.

Preferred Credentials

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 EM host machine. It is used by the Enterprise Management agent to communicate with the Oracle GoldenGate Enterprise Manager Plug-In .

OGG Admin Credentials

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

3.3 Setting Preferred Credentials for Oracle GoldenGate Classic Instance

To create Preferred credentials:

1. Navigate to the **Setup** menu, select **Security**, then select **Preferred Credentials**, and then click **Manage Preferred Credentials** to display the **Agent Preferred Credentials page > My Preferences** tab. 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**.

2. Under **Default Preferred Credentials**, select a Credential set, and click **Set** to display the **Select Preferred Credential** dialog box.
3. Select **New**, and enter values in the **UserName**, **Password**, and **Confirm Password** fields.
4. In the **Save As** text box, enter a name for the credential and click **Save** the credentials.

3.4 Monitoring Credentials for Oracle GoldenGate Microservices

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

1. Navigate to the **Setup** menu, select **Security**, then select **Monitoring Credentials** to display the **Security > Monitoring Credentials** page.
2. Select the Oracle GoldenGate Service Manager **Target Type**.
3. Click **Manage Monitoring Credentials** to display the **Oracle GoldenGate Monitoring Credentials** page.
4. Select the Target Name and click **Set Credentials** to display the **Enter monitor credentials** dialog box.

5. Enter the service manager **Username**, **Password**, and **Confirm Password**, and click **Save**.

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

4

Using the Enterprise Manager Plug-In for Oracle GoldenGate

The Target page displays the following tabs: **Metrics**, **Logs**, and **Configurations**, which enable you to monitor metrics and to alert users about specific metric results, search and interpret audit logs, and to configure parameter files respectively.

Topics

- [Enabling Audit Logging](#)
- [Viewing the Audit Logs](#)
- [Home Page Metrics](#)
- [Monitoring Oracle GoldenGate Targets](#)
- [Monitoring Current Oracle GoldenGate Metrics and Historical Trends](#)
- [Generating Automatic Alerts and Incidents When Thresholds are Breached](#)
- [Creating an Incident Rule](#)
- [Sending Email Alerts](#)

4.1 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

Operation	Value
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_REPOR
T;OGG_VIEW_DISCARD;OGG_VIEW_GGSERRLOG;OGG_EDIT_PARAM"
```

4.2 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.

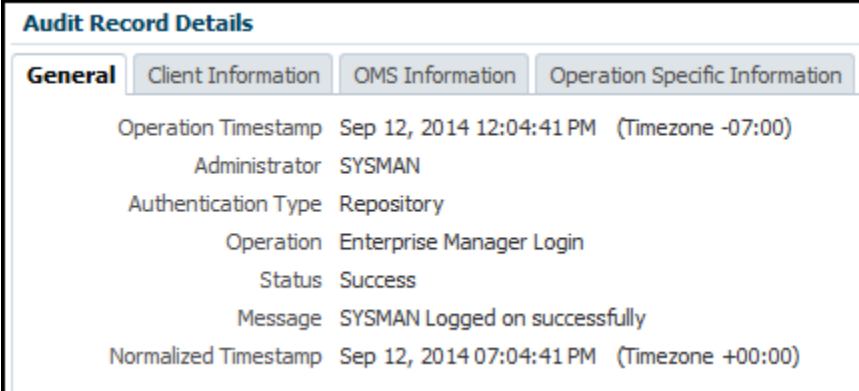
To view a specific audit log:

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

The screenshot shows the Oracle Enterprise Manager Cloud Control interface. The top navigation bar includes 'Security' and 'Audit Data'. The search panel on the left has the following settings: Date Range from Jan 1, 2016 10:38:08 AM to Feb 2, 2016 11:59:59 PM; Operation set to 'OGG-Start Target'; Administrator set to 'All'. The main table lists several audit records, with the first one selected. The 'Audit Record Details' section below the table shows the following information: Operation Timestamp: Feb 2, 2016 10:36:22 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 05:36:21 PM (Timezone +09:00).

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.



The screenshot shows a window titled "Audit Record Details" with four tabs: "General", "Client Information", "OMS Information", and "Operation Specific Information". The "General" tab is selected and displays the following 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 Auditing Framework](#) in the *Enterprise Manager Cloud Control Getting Started Guide* and [Configuring the Audit Data Export Service](#) in the *Enterprise Manager Cloud Control Security Guide*.

4.3 Home Page Metrics

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).
- Process status
- The lag in seconds
- 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.

Click a target on the **OGG Home** page to view detailed metrics for each of the 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 Attempts
- Delta Row Fetch Failures
- Total Row Fetch Failures

4.4 Monitoring Oracle GoldenGate Targets

Click the target name on the **OGG Home** page to view the status and metrics of each of the target types.

This topic describes the following target types:

- [Service Manager](#)
- [Administration Server](#)
- [Extract and Replicat](#)
- [Manager](#)

4.4.1 Service Manager

The **Service Manager** page lists all the Oracle GoldenGate Microservices 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.

4.4.2 Administration Server

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

4.4.3 Extract and Replicat

User 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.

This topic discusses the metrics used to monitor the Extract and Replicat processes.

- *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.

User can view detailed metrics of Extract, logs, and configuration of extract in the Extract page.

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

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

Metric	Description
Checkpoint Position	<p>Valid for Extract and Replicat</p> <p>Shows a composite representation of the checkpoints that were persisted to disk most recently by Extract or Replicat. The value is captured by the monitoring agent when the attribute is published, right after the checkpoint gets persisted.</p> <p>Extract creates read and write checkpoints, and Replicat creates only read checkpoints. Each individual checkpoint within the composite Checkpoint Position consists of the RBA (relative byte address) of a record in the transaction log or trail (depending on the process and whether it is a read or write checkpoint) and the sequence number of the log or trail file that contains the record. There can be a series of read checkpoints in multiple data source log files (such as Extract from Oracle Real Application Cluster), and/or multiple write checkpoints such as in Extract configurations with multiple trail files.</p> <p>Valid values: Different databases use different representations of the position of a record in the log. Therefore, instead of numeric values, Checkpoint Position is published as a string of text characters encoded in UTF8. For each individual checkpoint within Checkpoint Position, the following are shown the way that they are returned by the GGSCI SEND <i>group-name</i> STATUS command:</p> <ul style="list-style-type: none"> • The values of the RBA (relative byte address) • The file sequence number • The time stamp
Delta Deletes	<p>Valid for Extract and Replicat</p> <p>Shows the number, since the metric was last reported, of DELETE operations that were processed by the selected Oracle GoldenGate process in its current run session.</p> <p>Valid values: A positive integer</p>
Delta Discards	<p>Valid for Extract and Replicat</p> <p>Shows the number, since the metric was last reported, of DISCARD operations that were processed by the selected Oracle GoldenGate process in its current run session. The records are written to the discard file that is associated with the process.</p> <p>Valid values: Positive integer.</p>
Delta Executed DDLs	<p>Valid for Extract and Replicat</p> <p>Shows the count of executed Data Definition Language (DDL) operations that were processed by the selected Oracle GoldenGate process since the last sample time.</p> <p>Valid values: Positive integer</p>
Delta Ignores	<p>Valid for Extract</p> <p>Shows the number of data manipulation language (DML) operations that through an error were configured to be ignored since the last sample time.</p> <p>Valid values: Positive integer</p>
Delta Inserts	<p>Valid for Extract and Replicat</p> <p>Shows the number of data manipulation language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process since the last sample.</p> <p>Valid values: A positive integer</p>
Delta Operation Per Second	<p>Valid for Extract and Replicat</p> <p>Shows the number of operations (per second) that were processed by the selected Oracle GoldenGate process since the last sample.</p> <p>Valid values: A positive integer</p>

Metric	Description
Delta Operations	<p>Valid for Extract and Replicat</p> <p>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 sample.</p> <p>Valid values: A positive integer</p>
Delta Row Fetch Attempts	<p>Valid for Extract</p> <p>Shows the number of row fetch attempts that were processed by the selected Oracle GoldenGate process since the last sample. A fetch must be done occasionally to obtain row values when the information is incomplete or absent in the transaction log.</p> <p>Valid values: Positive integer</p>
Delta Row Fetch Failures	<p>Valid for Extract</p> <p>Shows the number of row fetch failures that were processed by the selected Oracle GoldenGate process since the last sample. A fetch must be done occasionally to obtain row values when the information is incomplete or absent in the transaction log</p> <p>Valid values: Positive integer</p>
Delta Truncates	<p>Valid for Extract and Replicat</p> <p>Shows the number of TRUNCATE operations that were processed by the selected Oracle GoldenGate process in its current run session since the last sample.</p> <p>Valid values: A positive integer</p>
Delta Updates	<p>Valid for Extract and Replicat</p> <p>Shows the number of UPDATE (including primary key updates) operations that were processed by the selected Oracle GoldenGate process in its current run session since the last sample.</p> <p>Valid values: A positive integer</p>
End of File	<p>Valid for Extract and Replicat</p> <p>Shows whether or not the selected process has reached the end of the input from its data source (transaction log or trail file).</p> <p>Valid values: TRUE (at end of file) or FALSE.</p>

 **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.

Metric	Description
Lag (sec)	<p>Valid for Extract and Replicat</p> <p>Shows the time difference between the Last Operation Timestamp and the Last Processed Timestamp. This attribute represents the true lag between the Oracle GoldenGate process and its data source. This lag value should match the value that is returned from the GGSCI command <code>SEND groupGETLAG</code>.</p> <p>Valid values: The lag time, in seconds</p>
Last Checkpoint Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when the last checkpoint was written by the process.</p> <p>Valid values: Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM.</p>
Last Operation Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log.</p> <p>Valid values: Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM</p>
Last Processed Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when a valid record was returned to the selected process. For Extract, this time value is assigned when the record is processed after the container transaction commits (not the time when the record is read from the transaction log). For a Data Pump or Replicat, this time value is returned immediately, because all transactions in the trail are known to be committed.</p> <p>Valid values: Date time value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM</p>
Message	<p>Valid for Extract and Replicat</p> <p>The message includes the following information:</p> <ul style="list-style-type: none"> • Message code number of an event message from the Oracle GoldenGate error log. Valid values: The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651. • Message Date: Timestamp of an event message from the Oracle GoldenGate log. Valid values: A datetime value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format) • Message Text: Text of an event message from the Oracle GoldenGate error log. Valid values: A text string from the message.
Name	<p>Valid for Extract and Replicat</p> <p>Name of the selected object.</p> <p>Valid values: Name of the object as displayed in the Oracle GoldenGate Monitor interface.</p>
Seconds Since Last OGG Checkpoint	<p>Valid for Extract and Replicat</p> <p>Time (in seconds) since the last OGG checkpoint.</p>
Start Time	<p>Valid for Extract and Replicat</p> <p>Shows the time that an Oracle GoldenGate component received its startup information after it has been created.</p> <p>Valid values: 64-bit Julian GMT time stamp in microseconds</p>
Status	<p>Valid for Extract and Replicat</p> <p>Shows the run status of the selected process.</p> <p>Valid values: Starting, Running, Stopped, Abended, or Aborted.</p>

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

Metric	Description
Total Updates	<p>Valid for Extract and Replicat</p> <p>Shows the total number of UPDATE (including primary key updates) operations that were processed by the selected Oracle GoldenGate process in its current run session. The statistic reflects the total operations performed on all of the tables that are specified in the parameter file for that process. Note: If any tables are mapped to targets in the Extract configuration, the statistics will reflect the total operations for all of the targets.</p> <p>Valid values: A positive integer</p>

On the **Oracle GoldenGate Home** page, the status is displayed in String, and internally, the values are in numeric. Numeric values are shown in the **Metric History** page and alerts are created based on these numeric values.

The following table provides list of Metric status values of the Extract and Replicat processes that are stored in the Enterprise Manager Plugin repository:

ProcessStatus Mapped Value	Integer Values for Status
ProcessStatus.REGISTERED_STATE	2
ProcessStatus.INITIALIZING_STATE	3
ProcessStatus.RUNNING_STATE	7
ProcessStatus.STOPPING_STATE	8
ProcessStatus.FORCESTOPPING_STATE	9
ProcessStatus.STOPPED_STATE	10
ProcessStatus.FORCESTOP_STATE	11
ProcessStatus.ABEND_STATE	12
ProcessStatus.KILLED_STATE	13
ProcessStatus.UNRESPONSIVE_STATE	16
ProcessStatus.UNKNOWN_STATE	0

4.4.3.1 Starting, Stopping, or Killing Extract and Replicat Processes

You can use the start, stop, or kill the Extract and Replicat processes from the **Metrics** page itself or the **OGG Home** page.

To start, stop, or kill Extract and Replicat processes:

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 icons: **Start**, **Stop**, or **Kill**.

4.4.3.2 Displaying Discard Files

The Discard files are displayed in the **Discards** sub tab under the **Logs** tab.

To display Discard files:

1. In the Oracle GoldenGate Home Page, click **Oracle GoldenGate Replicat** or **Oracle GoldenGate Extract** to display the **Detail Metrics**, **Logs**, and **Configuration** tabs.
2. Click the **Logs** tab and then the **Discards** tab to display the discard file contents.

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
```

 **Note:**

- If you want to view a discard file listed in a respective parameter file, then restart the corresponding Extract or Replicat process, select either of the following **Oracle GoldenGate Replicat** or **Oracle GoldenGate Extract**. Then click the **Logs** tab and then the **Discards** tab.
- If you want to view all the discard files in a respective parameter file, then set the discard file location more than once, then restart the corresponding Extract or Replicat process, select either of the following **Oracle GoldenGate Replicat** or **Oracle GoldenGate Extract**. Then click the **Logs** tab and then the **Discards** tab.

 **Note:**

The Logs tab contains the following 3 sub tabs: **GGSErr log**, **Discards**, and **Reports**. The **GGSErr log** tab shows the file contents of the `ggserr.log` file, the **Report** tab show report file contents and the **Discard** tab show discard file contents.

4.4.3.3 Editing Files on the 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**. If you haven't modified any content, then no action is taken. If you modified the content was modified and then clicked **Save** , then the new content is saved.

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.

4.4.4 Manager

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

The Manager process 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. For target types Replicat, Extract, and Manager, you can control the process though start, stop, kill, and resume actions. For target types Extract and Replicat, you can view and edit the associated configuration files, view all the associated report and discard the files as well.

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

Metric	Description
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 Monitoring Current Oracle GoldenGate Metrics and Historical Trends

If you are interested in viewing the data pattern of the targets and analyzing the historical trends, then you can view the details under Metric Data. You can also modify the thresholds to generate alerts.

To monitor the Oracle GoldenGate metrics and historical trends:

1. Click the **OGG Home** tab in the Oracle GoldenGate Home page.
2. Click a target in the **Target Name** column to display the corresponding process page (either a REPLICAT or an EXTRACT page).
3. Click a metric from the **Metrics** tab to display the **All Metrics** page and select a Metric, such as **Total Deletes** to display the details, such as Statistics, Thresholds, Metric Value History chart, and Metric Alert History table.

You can also view the Metric Value History in a tabular format, apart from the chart that is displayed by default.

4. Click **Table View** to display the **Metric Value History** table.
5. Click **Modify Thresholds...** to display the **Modify Thresholds** page.
6. Set the following values:

Warning Threshold

1. If the lead value is 1, then a warning alert is generated.

Critical Threshold

4. If the total lead value is greater than or equal to 4, then an alert is generated.

The generated alert is displayed in the **Metric Alert History** table.

7. Click the **Alerts** icon in the top-right corner of the **All Metrics** page to display the **Metric Events** details.

All the metrics of the corresponding process along with the alerts are displayed in the **Metric Events** page.

8. In the **Metric Alert History** table, click the **Details** icon to display the Event Details and Metric Details.

4.6 Generating Automatic Alerts and Incidents When Thresholds are Breached

The notification system allows you to notify Enterprise Manager administrators when specific incidents, events, or problems arise. In addition to notifying administrators, the notification system can perform actions such as executing operating system commands (including scripts) and PL/SQL procedures when an alert is triggered. This capability allows you to implement automatically specific IT practices under particular alert conditions.

To generate automatic alerts and incidents:

1. Click the **OGG Home** tab in the Oracle GoldenGate Home page.
2. Click a target in the **Target Name** column to display the corresponding process page (either a REPLICAT or an EXTRACT page).
3. Select the process drop-down list and click **Monitoring** and then click **Metric and Collection String** to display the **Metrics and Collection Settings** page.

There are two tabs on this page: Metrics and Other Collected Items. The **Metrics** tab displays all the configured metrics for the selected process. From the View drop-down list on this page, you can select the following to view the corresponding details: All metrics, Metrics with Thresholds, Metrics with Adaptive Thresholds, and Metrics with Time based Static thresholds.

4. Select **All metrics** and specify the **Warning Threshold** and **Critical Threshold** in the **Metric** table, and then click **OK** to save the changes.

A threshold gets created for the respective metrics.

Once you have created a threshold, you need to set the incident rule.

4.7 Creating an Incident Rule

If you want to create incidents to be reported for a particular threshold, you need to create an incident rule. An incident rule instructs Enterprise Manager to take specific actions when incidents, events, or problems occur, such as performing notifications. An incident rule set is a collection of rules that apply to a common set of objects such as targets (hosts, databases, groups), jobs, metric extensions, or self updates, and take appropriate actions when there are events and incidents. An event is a significant occurrence of interest on a target that has been detected by Enterprise Manager. An incident is a set of significant events or combination of related events that pertain to the same issue. Create your incident rule sets and subscribe to them so that you are notified every time there is an event or incident.

To create an incident Rule:

1. In the Home page, click **Enterprise**, select **Monitoring**, and then click **Incident Manager** to display the **Incident Manager** page. All the open incidents are listed in this page.

Alternatively, from the Home page, click **Targets**, and in the respective process page, click any **Incident** link in the **Incident** table to display the **Incident Manager** page that lists all the incidents for the selected target.

2. To create an Incident Rule, in the Home page, click **Setup**, select **Incidents**, and then click **Incident Rule**.
3. In the **Incident Rule** page, click **Create Rule Set...** to display the **Create Rule Set** page.
4. Enter the following details to create a Rule Set:
 - **Name**: Enter a name for the Rule set.
 - **Applies To**: Select an option, such as **Targets** from the **Applies To** drop-down list.
 - In the **Targets** area, select a **Targets**, such as **Oracle GoldenGate Extract** from the **All targets of types** drop-down list to create incident rule sets for all Oracle GoldenGate Extract targets.
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**.
7. In the **Create New Rule: Select Events** page, select **Metric Alert** from the **Type** drop-down list to define incident rule for a metric alert.
8. Click **Add** to display the **Select Specific Metric Alert** page.
9. Select a target type, such as **Oracle GoldenGate Extract** from the **Target Type** drop-down list, and then click **Search** to display the search results in a table.
10. Select a metric, such as **Total Insert** from the table
11. From the **Select Severity and Corrective Action Status** area, select a value, such as **All** from the **Severity** drop-down list, and then click **OK**.

When a threshold is reached for the **Total Inserts** metrics, an alert is displayed.
12. In the **Create New Rule: Add Actions** page, click **Next** to display the **Create New Rule: Add Actions** page to add an action for the incident rule.
13. Click **Add** to display **Add Conditional Actions** page to add any action, such as sending an email notification.
14. In the **Send Notifications** area, enter an email address in the **E-mail To** field, and then click **Continue**.
15. In the **Create New Rule: Add Actions** page, click **Next** to specify a name and description for the incident rule in the **Create New Rule: Specify Name and Description** page, and then click **Next** to display the **Create New Rule: Review** page.
16. Click **Continue** to go back to the **Incident Rules** page.

You can view the new rule in the Incident Rules table.
17. In the Home page, click **Target**, select **Golden Gate** to display the **OGG Home** and **Manage Agents** tabs.
18. In the **OGG Home** tab, click the respective **Target Name** to display the corresponding process page, with the **Metrics**, **Logs**, and **Configuration** tabs.
19. Click the respective metrics, such as **Total Inserts**, in the **Metrics** tab to view the notification that is set. An email is also sent to the recipient's email address. Ensure that you configure the notifications as described in the next steps:
20. In the Home page, click **Setup**, and select **Notifications**, and then click **Mail Servers** to display the **Mail Servers** page.

21. In the **Outgoing Mail (SMTP) Servers** page, click **Edit** to display the **Outgoing Mail (SMTP) Server** dialog box.
22. Enter the Host, Port, User Name, and Password.
23. Select SSL/TLS as a **Use Secure Connection** option.
24. Click **OK** to display the **Mail Servers** page.
25. In the **Outgoing Mail (SMTP) Servers** page, click **Test Mail Servers** to display an Information in the top of the **Mail Servers** page.
An Information is displayed in the

4.8 Sending 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

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 JAgent](#)
- [Creating an Inventory Location for Non Oracle Users](#)
- [Configuring JAgent in the Provisioning Environment](#)
- [Installing the Hybrid Cloud Gateway Agent](#)
- [Configuring the EM Hybrid Cloud](#)
- [Configuring the SOCKS Proxy Setup](#)

5.1 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*.

5.2 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.

5.3 Creating an Inventory Location for Non Oracle Users

You must create a new inventory location for non Oracle 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.

5.4 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.

5.5 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.

5.6 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.

5.7 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

6

Troubleshooting

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

Topics

- [Correcting ADFC Error on Windows 64-Bit Machines](#)
- [Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files](#)
- [Availability Error](#)

6.1 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.

6.2 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_1 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`

6.3 Availability Error

For the Oracle GoldenGate Microservices targets, you need to set the monitoring credential correctly for getting the target status and others metric, unlike the classic targets. In case of the classic targets, there was no requirement for preferred credentials to display the metrics. The preferred credentials were only required to get logs and the Configuration Tab.

Users who did not set the monitoring credentials may expect to view the metrics and as a result come across the **AVAILABILITY EVALUATION ERROR**. In such cases, you need to check the following:

- Whether the Enterprise Manager agent is up and running.
- Whether the monitoring credential is set and if set, you need to reset to ensure that the credentials are set correctly.