

Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In



(13.5.2.0.0)

F60489-06

April 2024

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

ORACLE®

Oracle Enterprise Manager Oracle GoldenGate System Monitoring Plug-In, (13.5.2.0.0)

F60489-06

Copyright © 2018, 2024, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), 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 embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	viii

1 Overview

1.1 What is Oracle Enterprise Manager Plug-In for Oracle GoldenGate	1-1
1.2 Architecture of Enterprise Manager Plug-in for Oracle GoldenGate	1-1
1.3 Custom Screens	1-3

2 Get Started

2.1 Supported Platforms and Releases	2-1
2.2 Supported Target Types	2-2
2.2.1 Target Types Supported in Classic	2-2
2.2.1.1 Oracle GoldenGate	2-2
2.2.1.2 Extract and Replicat	2-3
2.2.1.3 Manager	2-3
2.2.2 Target Types Supported in Microservices	2-4
2.2.2.1 Administration Service	2-5
2.2.2.2 Extract and Replicat	2-5
2.2.2.3 Service Manager	2-9
2.2.2.4 Deployment	2-10
2.2.2.5 Distribution Service	2-11
2.2.2.6 Receiver Service	2-13
2.3 Before You Begin with Enterprise Plug-In for Oracle GoldenGate	2-16

3 Install

3.1 Deploying the Plug-In	3-1
3.2 Downloading the Plug-In	3-1

3.3	Importing the Plug-in Archive	3-1
3.4	Deploying the Plug-In to the Management Agent	3-2
3.5	Verifying and Validating the Plug-in Deployment	3-3
4	Upgrade	
<hr/>		
4.1	Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Service	4-1
4.2	Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Agent	4-1
5	Discover	
<hr/>		
5.1	Discovering Oracle GoldenGate Targets in the UI	5-1
5.1.1	Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances	5-1
5.1.2	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance	5-3
5.1.3	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance	5-5
5.2	Enterprise Manager CLI Verb-Based Discovery of Oracle GoldenGate Targets	5-6
5.2.1	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance using EM CLI	5-6
5.2.2	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance using EM CLI	5-7
6	Promote	
<hr/>		
6.1	Promoting Oracle GoldenGate Targets	6-1
6.2	Target Metrics Available on OGG Home Page	6-1
7	Configure	
<hr/>		
7.1	Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager	7-1
7.2	Creating the Oracle Wallet	7-1
7.3	Configuring Instance-Level Security	7-2
7.3.1	Authorizing Users with Permissions	7-5
8	Manage	
<hr/>		
8.1	Manage Credentials	8-1
8.1.1	Different Credential Sets for Oracle GoldenGate	8-2
8.1.1.1	Preferred Credentials	8-2
8.1.1.2	Monitoring Credentials	8-2

8.1.2	Setting Credentials for Oracle GoldenGate Targets	8-3
8.1.2.1	Setting Credentials for Oracle GoldenGate Classic Instance	8-3
8.1.2.2	Setting Credentials for Oracle GoldenGate Microservices Instance	8-4
8.2	Manage Events, Alerts, and Incidents	8-5
8.2.1	Events	8-6
8.2.2	Incidents and Alerts	8-6
8.2.2.1	Setting Metric Alerts and Incidents for Extract and Replicat	8-6
8.2.2.2	Setting Metric Alerts and Incidents for Oracle GoldenGate Monitor Agent	8-7
8.2.2.3	Setting Incidents and Alerts for Oracle GoldenGate Target Availability	8-7
8.2.2.4	Setting Metric Alerts and Incidents for Distribution Service Path and Receiver Service Path	8-8
8.2.2.5	Setting Alerts for Events	8-9
8.2.3	Alerts on Home Page	8-9
8.2.3.1	Indication of GoldenGate Monitor Agent and WebService being Down	8-10
8.2.4	Metric Data	8-10
8.2.4.1	Enabling/Disabling Metrics	8-10

9 Monitor

9.5	Events Tab	9-1
9.1	Viewing Target Details	9-2
9.2	Start and Stop a Target	9-2
9.2.1	EMCLI Commands on Oracle GoldenGate Targets	9-3
9.3	Metrics Tab	9-3
9.4	Log Tab	9-4
9.6	Configuration Tab	9-4
9.7	Elements for Monitoring Targets	9-5
9.8	Monitoring the High Availability Features	9-5

10 Audit

10.1	Enabling Audit Logging	10-1
10.2	Viewing the Audit Logs	10-2

11 Troubleshoot

11.7	Troubleshooting High Availability	11-1
11.7.1	Remote EM Agent is not able to Connect to Oracle GoldenGate Agent	11-1
11.1	Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files	11-1
11.2	Troubleshooting Discovery	11-2
11.2.1	Troubleshooting: Oracle GoldenGate Classic Targets	11-2
11.2.1.1	Identifying the Error	11-3

11.2.2	Troubleshooting: Oracle GoldenGate Microservices Targets	11-4
11.2.2.1	Identifying the Error	11-4
11.3	Troubleshooting Credentials	11-6
11.3.1	Troubleshooting: Oracle GoldenGate Classic Credentials	11-6
11.3.1.1	Start and Stop Buttons are Disabled	11-6
11.3.1.2	Preferred credential is not Set or is Incorrectly Set on Host Target	11-6
11.3.1.3	Unable to Check Configurations or Logs of a Process	11-7
11.3.1.4	Decrypt : Failed to decrypt buffer error while testing the preferred credential after upgrade	11-7
11.3.2	Troubleshooting: Oracle GoldenGate Microservices Credentials	11-7
11.3.2.1	Start and Stop Buttons are Disabled	11-7
11.3.2.2	Monitoring Credentials are Either Not Set or Set Incorrectly	11-7
11.3.2.3	Unable to Check Configurations or Logs of a Process	11-8
11.3.2.4	Decrypt : Failed to Decrypt Buffer Error while Testing the Preferred Credential after Upgrade	11-8
11.4	Troubleshooting Metric Collections	11-8
11.4.1	Metrics are not Getting updated for Oracle GoldenGate Targets	11-8
11.5	Troubleshooting GoldenGate Targets Status Issues	11-9
11.5.1	Oracle GoldenGate Target Shows Pending Status	11-9
11.5.2	Oracle GoldenGate Classic Target Status is Shown as Down when all its Processes are Up	11-9
11.5.3	Availability Evaluation Error	11-9
11.5.3.1	Availability Evaluation Error when Monitoring Credentials are Updated in Oracle GoldenGate Core	11-10
11.6	Troubleshooting False Alerts	11-10
11.6.1	False Alerts for Oracle GoldenGate Classic and Microservices (MA) Targets	11-10
11.6.2	False Alerts for Oracle GoldenGate Classic Targets	11-11
11.6.3	False Alerts for Oracle GoldenGate Microservices Targets	11-11

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](#)
- [Documentation Accessibility](#)
- [Related Documents](#)
- [Conventions](#)

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 Administrator'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*.
- [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.
<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

- [What is Oracle Enterprise Manager Plug-In for Oracle GoldenGate](#)
- [Architecture of Enterprise Manager Plug-in for Oracle GoldenGate](#)
- [Custom Screens](#)

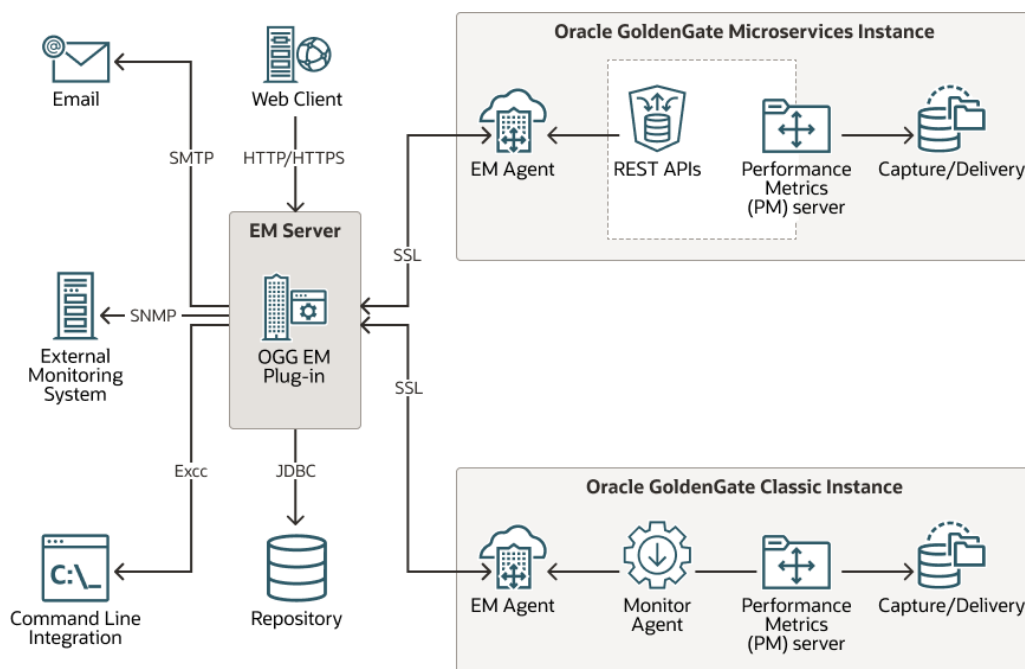
1.1 What is Oracle Enterprise Manager Plug-In for Oracle GoldenGate

The Oracle GoldenGate Enterprise Manager Plug-In extends the Oracle Enterprise Manager (EM) Cloud Control to support monitoring and managing Oracle GoldenGate processes. By deploying it in your Cloud Control environment, you gain the following features:

- Visually monitor current Oracle GoldenGate metrics and historical trends.
- Generate automatic alerts and incidents when thresholds are breached.
- Start, stop, kill, and resume individual processes.
- View and modify existing configuration files.
- View error logs, Oracle GoldenGate error logs, report files, and discard files.
- Audit user access of privileged EM Plug-in features and instance-level security for user creation.

1.2 Architecture of Enterprise Manager Plug-in for Oracle GoldenGate

The Oracle GoldenGate Management Pack extends the common product architecture across both the products, the GoldenGate Enterprise Manager Plug-in and GoldenGate Monitor.

Figure 1-1 Oracle GoldenGate Enterprise Manager Plug-in Architecture

Oracle GoldenGate Enterprise Manager (OEM) Plug-in

The Oracle GoldenGate Enterprise Manager Plug-in coordinates the monitoring of multiple Oracle GoldenGate instances (Classic and Microservices). The Oracle GoldenGate Enterprise Manager Plug-in processes information from the Oracle Enterprise Manager Agent, which in turn gets the information either from Oracle GoldenGate Monitor agents (if Classic instance) or from Oracle GoldenGate REST APIs (in case of Microservices architecture).

You do not have to install the Oracle GoldenGate Monitor Agent, if the GoldenGate Microservices Instance is being monitored. The Oracle GoldenGate Enterprise Manager Plug-in is tightly integrated with the Enterprise Manager to leverage various functionalities, such as incident and alerts, maintenance black-outs, manages users, history, the display of information, and notifications triggered by events. The communication between Oracle GoldenGate Enterprise Manager Plug-in and Enterprise Manager Agent can be secured using SSL communication.

Oracle GoldenGate Monitor Agent

The Performance Metrics Server for each Oracle GoldenGate Classic instance is associated with an Oracle GoldenGate Monitor Agent that supplies information about the Oracle GoldenGate Classic instance to the Oracle GoldenGate Enterprise Manager Plug-in through the Enterprise Manager Agent.

Oracle Enterprise Manager Agent (OEM or EM Agent)

The Oracle Enterprise Manager Agent (EM Agent) is an integral software component that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The EM Agent is a software component that monitors targets running on hosts and communicates that information to the middle-tier Oracle

Management Service (OMS). It works in conjunction with the plug-ins to monitor the targets running on that managed host.

 **Note:**

In the **Oracle GoldenGate Enterprise Manager Plug-in Architecture** diagram shown above, the EM agent runs on the same server as the Oracle GoldenGate instance. However, the OEM Agent can either run locally or remotely.

Performance Metrics Server

In Oracle GoldenGate Microservices Architecture, the Performance Metrics Server (PM Server) provides a dashboard view as well as a detailed view of status changes, and statistical data of the servers' performance. They are represented through statistical charts and real-time data. The Performance Metrics Server uses the metrics service to collect and store instance deployment performance results. All the servers and processes of the Microservices Architecture can be monitored at drill-down levels to allow trend monitoring and statistical analysis of data. The Performance Metrics Server offers these detailed views with graphical representations of statistical data in real-time.

The Performance Metric Server in a Classic architecture does the same work of collecting the metrics of all the Oracle GoldenGate processes and shares them with the Monitor agent. The Classic architecture does not support GUI; therefore, the Performance Metrics Server does not offer graphical representations of statistical data in real-time.

Oracle GoldenGate Enterprise Manager (OEM) Plug-in Repository

The Oracle GoldenGate Enterprise Manager (OEM) Plug-in uses a database as a central repository which can be purged at a user- controlled interval. This repository stores information about users' access privileges to Oracle GoldenGate instances, process statuses, monitoring points, alerts, and additional information.

1.3 Custom Screens

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

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

Get Started

- [Supported Platforms and Releases](#)
- [Supported Target Types](#)
- [Before You Begin with Enterprise Plug-In for Oracle GoldenGate](#)
Oracle Enterprise Manager for Oracle GoldenGate has a number of prerequisites that must be performed before you can get started with deploying and using the product.

2.1 Supported Platforms and Releases

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

Supported Platforms

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

See the Certifications tab on [My Oracle Support](#) for details.

NOT_SUPPORTED:

Oracle has tested and verified the performance of your product on all certified systems and environments; whenever new certifications occur, they are added to the proper certification document right away. New certifications can occur at any time, and for this reason the certification documents are kept outside of the documentation libraries and are available on Oracle Technology Network.

- The Enterprise Manager Plug-In for Oracle GoldenGate supports monitoring of all platforms where both Oracle GoldenGate Classic and Oracle GoldenGate Microservices Releases 18.1 and later, and Oracle Enterprise Manager Cloud Control 13c Agent and later instances can run.
- DB2 z/OS and DB2 for i don't support the installation of the Enterprise Manager and EM Agent. Monitoring of Oracle GoldenGate instances is achieved through remote Enterprise Manager Agent and Oracle GoldenGate Monitor Agent installed on these operating systems (supported with changes in the OEM and Oracle GoldenGate configuration).
- Oracle GoldenGate for HP NonStop is *not* supported.

Supported Releases

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

- Enterprise Manager Cloud Control 13c Release 5 (13.5.x) and later.
- Oracle GoldenGate versions supported include:
 - Oracle GoldenGate Monitor Agent 12.2.1.2.210930 or later

- Oracle GoldenGate 18.1 to 21.7
- Oracle GoldenGate Microservices 18.1 to 21.7

For more information about the supported releases see Oracle GoldenGate Studio Interoperability with Other Fusion Middleware Products in *Understanding Interoperability and Compatibility Guide*.

2.2 Supported Target Types

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

- [Target Types Supported in Classic](#)
- [Target Types Supported in Microservices](#)

2.2.1 Target Types Supported in Classic

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

- [Oracle GoldenGate](#)
Oracle GoldenGate target type represents an Oracle GoldenGate classic instance. It's the parent target of Manager, Extract, and Replicat targets.
- [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, events, and monitor historical trends.
- [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 through start, stop, kill, and resume actions.

2.2.1.1 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.

- [GoldenGate Monitor Agent](#)
The GoldenGate Monitor Agent represents the GoldenGate Monitor agent that is connecting to the Oracle GoldenGate Instance.

2.2.1.1.1 GoldenGate Monitor Agent

The GoldenGate Monitor Agent represents the GoldenGate Monitor agent that is connecting to the Oracle GoldenGate Instance.

Version and details of other metrics are displayed on the **Oracle GoldenGate Target** page.

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

Metric	Description
GoldenGate Monitor Agent Status	UP arrow indicates Golden Gate Agent is up and running. Down arrow indicates Golden Gate agent is down or unreachable. 1 represents UP and 2 represents Down for setting incidents and alerts.
WebService Availability	Indicates whether or not the Webservice of Oracle GoldenGate is up and running. 0 represents down status and 1 represents up status . This metric is available only from Oracle GoldenGate Monitor Agent release 12.2.1.2.210930 onwards.
Host Name	Shows the name of GoldenGate Monitor Agent host.
Agent Port	Shows the port on which the GoldenGate Monitor Agent process is running.
User Name	Shows the user name to connect to the Monitor agent.
Agent Version	Indicates the version of GoldenGate Monitor Agent. This metric is available only from GoldenGate Monitor Agent 12.2.1.2.210930 version onwards
Agent Start Time	Shows the time number of milliseconds from January 1, 1970, 00:00:00 GMT to Oracle GoldenGate Monitor Agent start time. This metric is available only from Oracle GoldenGate Monitor Agent 12.2.1.2.210930 version onwards.
Installation Path	Shows the directory that contains the Oracle GoldenGate Monitor Agent executable file. This is the home directory of the Oracle GoldenGate Monitor Agent installation. This metric is available only from GoldenGate Monitor Agent 12.2.1.2.210930 version onwards.
Config Path	Shows the Oracle GoldenGate Monitor Agent configuration properties location. This metric is available only from Oracle GoldenGate Monitor Agent 12.2.1.2.210930 version onwards.

2.2.1.2 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, events, and monitor historical trends.

For more information, see [Extract and Replicat](#).

2.2.1.3 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 through 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
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

2.2.2 Target Types Supported in Microservices

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

- [Administration Service](#)
You can use the Administration Service to manage Extract and Replicat processes and to monitor their metrics. It is the parent target for Extract and Replicat targets. The Administration Service displays the following Process Summary details: Process Health Overview, Alert Overview, and the metrics details of the Processes.
- [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, events, and monitor historical trends.
- [Service Manager](#)
The **Service Manager** page lists all the Oracle GoldenGate Microservices Architecture deployments. It's the parent target for the Deployment target, which in turn contains Administration Service, Receiver Service, Distribution Service, and Performance Metrics Server targets. If you have multiple deployments, then you can also filter using the **Deployment** drop-down list.
- [Deployment](#)
The Deployment displays the status of target deployment, the location of your deployment configuration files including parameter files, location of deployment artifacts, configuration artifacts, and Oracle GoldenGate events of the deployment.

It's the parent target for Administration Service, Receiver Service, Distribution Service, and Performance Metrics Service.

- [Distribution Service](#)
You can view Path summary and the Path metrics, such as Path Details that include target encryption algorithm, critical, processing lag, auto restart, and Statistics like DDLs, DMLs, and Table Statistics in the Distribution Service detailed page.
- [Receiver Service](#)
You can view Path summary and the Path metrics, such as Path Details that include target encryption algorithm, critical, processing lag, auto restart, and Statistics like DDLs, DMLs, and Table Statistics in the Receiver Service detailed page.

2.2.2.1 Administration Service

You can use the Administration Service to manage Extract and Replicat processes and to monitor their metrics. It is the parent target for Extract and Replicat targets. The Administration Service displays the following Process Summary details: Process Health Overview, Alert Overview, and the metrics details of the Processes.

The following process-related details are displayed in a tabular format:

- **Name:** Name of the process.
- **Status:** Status of the process, indicates whether or not the process is up and running. Status is denoted by up and down arrow icons.
- **Type:** Type of the process/target. For example, Classic Extract or Classic Replicat.
- **Lag:** Displays the delay time between the data fetch by the process and write to trail.
- **Total Discards:** Displays the number of discard operations by the process.
- **Total Ignores:** Displays the number of ignored operations performed by the process.

Using the **Search** option, you can also look up for a process in this view.

For a selected process, the following target metrics are displayed:



- Total Operations
- Total Inserts
- Total Updates
- Total Deletes
- Total Truncates


2.2.2.2 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, events, 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	<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 of DELETE operations that were processed by the selected Oracle GoldenGate process since the last fetched value.</p> <p>Valid values: A positive integer</p>
Delta Discards	<p>Valid for Extract and Replicat</p> <p>Shows the DISCARD operations that were processed by the selected Oracle GoldenGate process since the last fetched value.</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 fetched value.</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 fetched value.</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 fetched value.</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 fetched value.</p> <p>Valid values: A positive integer</p>
Delta Operations	<p>Valid for Extract and Replicat</p> <p>Shows the total number of Data Definition Language (DDL) 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.</p> <p>Valid values: A positive integer</p>

Metric	Description
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 fetched value.</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 fetched value.</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 fetched value.</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 fetched value.</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>
	<div style="border-left: 2px solid #0070C0; padding-left: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>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.</p> </div>
	<div style="border-left: 2px solid #0070C0; padding-left: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>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.</p> </div>
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>

Metric	Description
Last Operation Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log.</p> <p>Valid values: Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example:01/14/2011 09:36:32 AM</p>
Last Processed Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when a valid record was returned to the selected process. For Extract, this time value is assigned when the record is processed after the container transaction commits (not the time when the record is read from the transaction log). For a Data Pump or Replicat, this time value is returned immediately, because all transactions in the trail are known to be committed.</p> <p>Valid values: Date time value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM</p>
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>
<div style="border-left: 2px solid #0070C0; padding-left: 10px; background-color: #E6F2FF;">  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. </div>	
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>

Metric	Description
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>
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>

2.2.2.3 Service Manager

The **Service Manager** page lists all the Oracle GoldenGate Microservices Architecture deployments. It's the parent target for the Deployment target, which in turn contains Administration Service, Receiver Service, Distribution Service, and Performance Metrics

Server targets. If you have multiple deployments, then you can also filter using the **Deployment** drop-down list.

The **Service Manager** page also displays the Goldengate Home for each deployment. This page also lists the following for each deployment:

Details	Description
Service Name	Name of the service, for example: <code>distsrvr:8062</code>
Service Type	Type of the service, such as Administration Service, Distribution Service, Performance Metrics Service or Receiver Service.
Port	Port number
Status	Status of the service type. Valid Values: 1 : Indicates UP status 0 : Indicates DOWN status



Note:

For OCI GoldenGate Service, the Service Manager target does not exist.

2.2.2.4 Deployment

The Deployment displays the status of target deployment, the location of your deployment configuration files including parameter files, location of deployment artifacts, configuration artifacts, and Oracle GoldenGate events of the deployment. It's the parent target for Administration Service, Receiver Service, Distribution Service, and Performance Metrics Service.

In case of OCI GoldenGate Service, Deployment target is the parent target node and therefore only the Status is shown in the OGG Home page. Deployment status is calculated based on it's child targets. If any child is UP, then the deployment status is also UP, else it is marked DOWN.

Details	Description
Status	Shows the run status of the Deployment. The alert for Metric status is set for numeric value. Valid Values: 1 : Indicates UP status 0 : Indicates DOWN status
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: <code>/ogg_install_location</code> .
GoldenGate Etc Home	The location in which your deployment configuration files are stored including parameter files. The default directory path is: <code>/ogg_deployment_location/etc</code> .
GoldenGate Conf Home	The location in which each deployment information and configuration artifacts are stored. The default directory path is: <code>/ogg_deployment_location/etc/conf</code> .
GoldenGate SSL Home	The location in which each deployment security artifacts (certificates, wallets) are stored. The default directory path is: <code>/ogg_deployment_location/etc/ssl</code> .

Details	Description
GoldenGate Var Home	The location in which each deployment logging and reporting processing artifacts are stored. The default directory path is: <code>/ogg_deployment_location/var</code> .
GoldenGate Data Home	The location in which each deployment data artifacts (trail files) are stored. The default directory path is: <code>/ogg_deployment_location/var/lib/data</code> .
Managed by Service Manager	Indicates whether the deployment is managed by the Service Manager. Valid values: true or false .

2.2.2.5 Distribution Service

You can view Path summary and the Path metrics, such as Path Details that include target encryption algorithm, critical, processing lag, auto restart, and Statistics like DDLs, DMLs, and Table Statistics in the Distribution Service detailed page.

The **Distribution Path Summary** summarizes the following:

- Number of paths
- Number of paths that are in Running state.
- Number of paths that are in Failed state.
- Other

You can also search for path details based on the column values of the following columns: Name, Status, Processing Lag, Source, Target, DB Name, and Extract. The search is case insensitive.

Path Information

Path Details	Description
Path Name	Path Name of the Distribution Service.
Description	Description provided for the path name. For example, the name of the Extract and Replicat names.
Status	Status of the Distribution path. The alert for Metric status is set for numeric value. Valid numeric values of the following status are: <ul style="list-style-type: none"> • Uninitialized = 0 • Running = 1 • Unknown = 2 • Paused = 3 • Stopping = 4 • Stopped = 5 • Killed = 6
Processing Lag	Difference between the time when extract wrote a transaction in the trail and the time when Distribution Service processes this transaction.
Source	Complete path name of the Distribution Service.
Target	Complete path name of the Receiver service.
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 Service is connected to.

Source/Target DB Details	Description
Source	<ul style="list-style-type: none"> • Host Name: URL of the source host for example, localhost, if the source is on the same system. • Port: Port number of the Distribution Service. • Protocol Name: Data transfer protocol name. For example, Trail. • Trail Name: Path takes the source trail and sends the data to a target trail, which can be consumed by any Replicats created later. • Generated Source URI: A URI is automatically generated for the trail based on the Extract information. • Source Trail File: Name of the file where the source trail file is generated. • Trail Sequence Length: The length of the trail sequence number. • Trail Size (MB): The maximum size of a file in a trail.
Target	<ul style="list-style-type: none"> • Host Name: URL of the target host for example, localhost, if the source is on the same system. • Port: Port number of the Receiver Server and the trail name of the Replicat. • Protocol Name: Data transfer protocol name. For example, Trail. • Trail Name: Path takes the source trail and sends the data to a target trail, which can be consumed by any Replicats created later. • Generated Target URI: A target URI is automatically generated for the trail based on the target authentication method and target information. • Source Trail File: Name of the file where the source trail file is generated. • Trail Sequence Length: The length of the trail sequence number. • Trail Size (MB): The maximum size of a file in a trail.

- **Target Encryption Algorithm:** The encryption algorithm for the target trail. For example, NONE, AES128, AES192, AES256.
- **Critical:** The default value is `false`. If the value is `true`, this indicates that the Distribution path is critical to the deployment.
- **Processing Lag (Sec):** Difference between the time when extract wrote a transaction in the trail and the time when Distribution Service processes this transaction.
- **Since Lag Reported (Sec):** Time since the last lag reported.
- **Auto restart:** The default value is `false`. If the value is `true`, the Distribution path restarts automatically if it's terminated.

Statistics

The **Statistics** tab shows you detailed information about the Total bytes sent logical change records (LCRs) and DDLs that were read from trails, LCRs and DDLs sent and procedure. It also provides information about the DML types, inserts, updates, upserts, and deletes.

The table information includes the values of Table Name, Inserts, Deletes, Upserts, LCRs read, and sent. You can search for records based on the values of any column of the table. This search is case insensitive.

2.2.2.6 Receiver Service

You can view Path summary and the Path metrics, such as Path Details that include target encryption algorithm, critical, processing lag, auto restart, and Statistics like DDLs, DMLs, and Table Statistics in the Receiver Service detailed page.

The **Receiver Path Summary** summarizes the following:

- Number of paths
- Number of paths that are in Running state.
- Number of paths that are in Failed state.
- Other

You can also search for path details based on the column values of the following columns: Name, Status, Processing Lag, Source, Target, DB Name, and Extract. The search is case insensitive.

Path Information

Path Details	Description
Receiver Service Path Name	Path Name of the Receiver Service
Status	Status of the Receiver path. The alert for Metric status is set for numeric value. Valid numeric values of the following status are: <ul style="list-style-type: none"> • Uninitialized = 0 • Running = 1 • Unknown = 2 • Paused = 3 • Stopping = 4 • Stopped = 5 • Killed = 6
Processing Lag	Difference between the time when Replicat read a transaction in the trail and the time when Receiver Service processes this transaction.
Source	Complete path name of the Distribution service.
Target	Complete path name of the Receiver Service.
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 Service is connected to.

Path Details for a Non-Target Initiated path:

Path Details	Description
Name	Path Name of the Receiver Service
Target Trail File	Name of the target trail of the Replicat you created earlier.
Transfer Protocol	Data transfer protocol. For example, ogg.
Host	Host name of the Receiver path.
Port	Port number of the Receiver path.

Path Details	Description
Database	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 Service is connected to.

Path Details for a Target Initiated path

Path Details	Description
Name	Path Name of the Receiver Service
Description	Description provided for the path name. For example, the name of the Extract and Replicat names.
Status	Status of the Receiver Service path. For example, Stopping, Running, or Stopped.
Database 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 Service is connected to.

Source/Target DB Details	Description
Source	<ul style="list-style-type: none"> • Host Name: URL of the source host for example, localhost, if the source is on the same system. • Port: Port number of the Receiver Service. • Protocol Name: Data transfer protocol name. For example, Trail. • Trail Name: Path takes the source trail and sends the data to a target trail, which can be consumed by any Replicats created later. • Generated Source URI: A URI is automatically generated for the trail based on the Extract information. • Source Trail File: Name of the file where the source trail file is generated. • Trail Sequence Length: The length of the trail sequence number. • Trail Size (MB): The maximum size of a file in a trail.
Target	<ul style="list-style-type: none"> • Host Name: URL of the target host for example, localhost, if the source is on the same system. • Port: Port number of the Receiver Service and the trail name of the Replicat. • Protocol Name: Data transfer protocol name. For example, Trail. • Trail Name: Path takes the source trail and sends the data to a target trail, which can be consumed by any Replicats created later. • Generated Target URI: A target URI is automatically generated for the trail based on the target authentication method and target information. • Source Trail File: Name of the file where the source trail file is generated. • Trail Sequence Length: The length of the trail sequence number. • Trail Size (MB): The maximum size of a file in a trail.

- **Target Encryption Algorithm:** The encryption algorithm for the target trail. For example, NONE, AES128, AES192, AES256.
- **Critical:** The default value is `false`. If the value is `true`, this indicates that the Receiver path is critical to the deployment.

- **Processing Lag (Sec):** Difference between the time when Replicat read a transaction in the trail and the time when Receiver Service processes this transaction.
- **Lag:** Shows the time difference between the Last Operation Timestamp and the Last Processed Timestamp. This attribute represents the true lag between the Oracle GoldenGate process and its data source.
This lag value should match the value that is returned from the GGSCI command `SEND groupGETLAG`.
- **Since Lag Reported (Sec):** Time since the last lag reported.
- **Auto restart:** The default value is `false`. If the value is `true`, the Receiver path restarts automatically if it's terminated.

Statistics

The **Statistics** tab shows you detailed information about the logical change records (LCRs) and DDLs that were read from trails, LCRs and DDLs sent and received, LCRs and DDLs filtered. It also provides information about the DML types, inserts, updates, upserts, and deletes.

The table information includes the values of LCRs read and sent. The search is case insensitive.

For a Target Initiated path, the **Statistics** tab displays the following:

- **Network:** The Network information includes details, such as target trail file name, port number, total messages written out, and so on. You can use this information to go back to the Distribution Server and tune the network parameters, if required.
- **File IO:** The File IO includes total bytes read, total bytes written to file, and total idle time (in seconds).
- **DDL:** The details displayed in the DDL table are LCR Read from Trails, LCR Sent, DDL Read from Trails, DDL Sent, and Procedure.
- **DML:** DML details that are displayed are Type, Inserts, Updates, Upserts, and Deletes.
- **Table:** This table consists of details like Table Name, Inserts, Deletes, Updates, Upserts, LCR Read, and LCR Sent.

For a Non-Target Initiated Path, the **Statistics** tab displays only the **Network** and **File IO** details.

Note:

Target-initiated paths for Microservices enable the Receiver Service to initiate a path to the Distribution Service on the target deployment and pull trail files. For more information, see [About Target-Initiated Paths](#) in the *Step by Step Data Replication Using Oracle GoldenGate Microservices Architecture* guide.

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

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

Software Requirements

- The following must be installed and running:
 - Oracle GoldenGate: to support monitoring by Enterprise Manager Cloud Control.
 - Oracle GoldenGate Monitor Agent for monitoring Oracle GoldenGate classic instances (not required for Oracle GoldenGate Microservices Architecture (MA) instance monitoring); the installation location you chose is referred to as `OGG_AGENT_ORA_HOME` in this document. This location is not necessarily the Oracle GoldenGate installation location.
 - Oracle Enterprise Manager (OEM) Cloud Control
 - (Oracle Management Service (OMS)) and Oracle Management agent) need to be installed in the server where the Oracle GoldenGate server runs.

 **Note:**

On the system, where OMS is installed, ensure to keep the ulimit value (Max. No. of processes) to unlimited.

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

Verify Your Environment Meets Certification Requirements

Make sure that you are installing your product on a supported hardware or software configuration. For more information, see the certification document for your release on the [Oracle Fusion Middleware Supported System Configuration](#) page.

3

Install

- [Deploying the Plug-In](#)
- [Downloading the Plug-In](#)

You can download plug-ins in online or offline mode. *Online* refers to an environment where you have Internet connectivity to the Enterprise Manager Store. *Offline* refers to an environment where you don't have Internet connectivity.
- [Importing the Plug-in Archive](#)

If you manually downloaded the plug-in, then you must manually import the plug-in archive into Oracle Enterprise Manager Cloud Control. This topic tells you how to complete this task.
- [Deploying the Plug-In to the Management Agent](#)

After you've completed the plug-in deployment on the management server, you must deploy the plug-in to the management agent.
- [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.

3.1 Deploying the Plug-In

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

For more information about plug-ins, see *Managing Plug-Ins in Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3.2 Downloading the Plug-In

You can download plug-ins in online or offline mode. *Online* refers to an environment where you have Internet connectivity to the Enterprise Manager Store. *Offline* refers to an environment where you don't have Internet connectivity.

See *Downloading the Plug-in in the Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3.3 Importing the Plug-in Archive

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

To import the plug-in archive:

1. Download the Enterprise Manager Plug-In for Oracle GoldenGate from the [Oracle GoldenGate Downloads](#) page, located in the **Management Pack for Oracle GoldenGate** section.

2. Select **Setup, Command Line Interface** and follow the instructions outlined on the Enterprise Manager Command Line Interface Download page to set up the Enterprise Manager Command Line (EM CLI) utility.
3. Import the plug-in archive:

```
emcli login -username=your user ID-password=password
emcli sync
emcli import_update -file=<../oracle.fmw.gg_xxx.opar -omslocal
emcli get_plugin_deployment_status -plugin_id=oracle.fmw.gg -
omslocal
```

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

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

 **Tip:**

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

- g. Check the status of Enterprise Manager Plug-In for Oracle GoldenGate deployment. After 10 minutes, you can check the status through the `emcli` command: `emcli get_plugin_deployment_status -plugin_id=oracle.fmw.gg -omslocal`.

 **Note:**

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

3.4 Deploying the Plug-In to the Management Agent

After you've completed the plug-in deployment on the management server, you must deploy the plug-in to the management agent.

To deploy the plug-in to the management agent:

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

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

3.5 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.

4

Upgrade

- [Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Service](#)
- [Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Agent](#)

4.1 Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Service

See [Upgrading Plug-Ins Deployed to Oracle Management Service](#) in the [Cloud Control Administrator's Guide](#) for details about how to upgrade the plug-in deployed on Oracle Management Service.

4.2 Upgrading the Enterprise Plug-In for Oracle GoldenGate on Oracle Management Agent

See [Upgrading Plug-Ins Deployed to Oracle Management Agent](#) in the [Oracle Enterprise Manager Cloud Control Administrator's Guide](#) for details about how to upgrade the plug-in deployed on Oracle Management agents.

5

Discover

- [Discovering Oracle GoldenGate Targets in the UI](#)
- [Enterprise Manager CLI Verb-Based Discovery of Oracle GoldenGate Targets](#)

5.1 Discovering Oracle GoldenGate Targets in the UI

- [Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances](#)
- [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.
- [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.

5.1.1 Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances

Ensure to upload the SSL certificate to the Oracle Enterprise Manager Agent which is used to discover and monitor the corresponding Oracle GoldenGate targets. When there are more Oracle Enterprise Manager (OEM) Agents monitoring multiple GoldenGate targets, then ensure that the corresponding SSL certificate of Oracle GoldenGate is imported to the agents.

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

```
./emctl secure add_trust_cert_to_jks -password <password> -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`.

Note:

Occasionally, when you encounter the following error: `Keystore was tampered with, or password was incorrect`, it may indicate the jks truststore is owned by root and marked as read only.

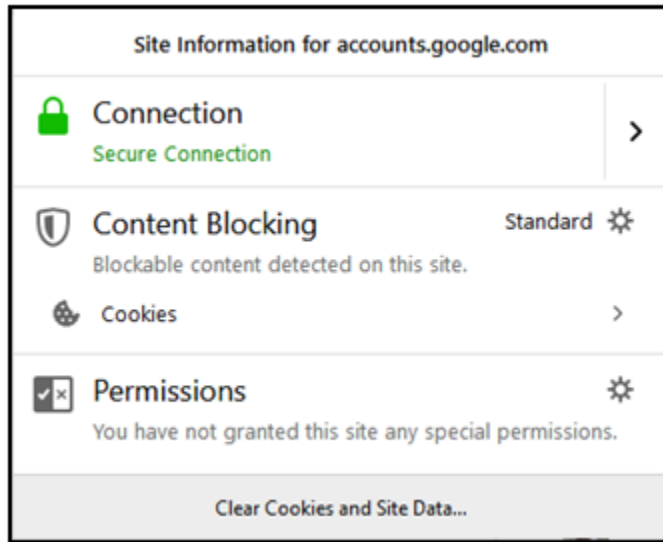
Workaround: Ensure to execute the `root.sh` script after the Enterprise Manager Agent installation.

For all secured GoldenGate instances using HTTPS, you can view and download this certificate from the browser when logged into the Service Manager UI or Administration Service UI.

To download the certificate using Mozilla Firefox:

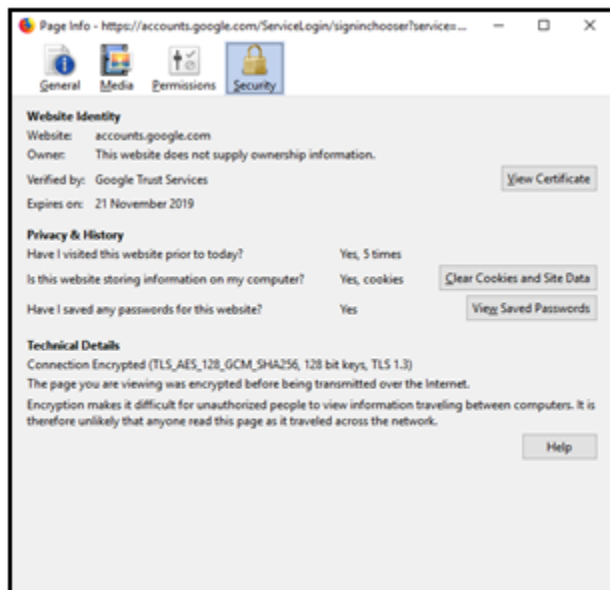
1. Click the **Site Identity** button (a padlock) in an address bar.

Figure 5-1 Site Identity Padlock



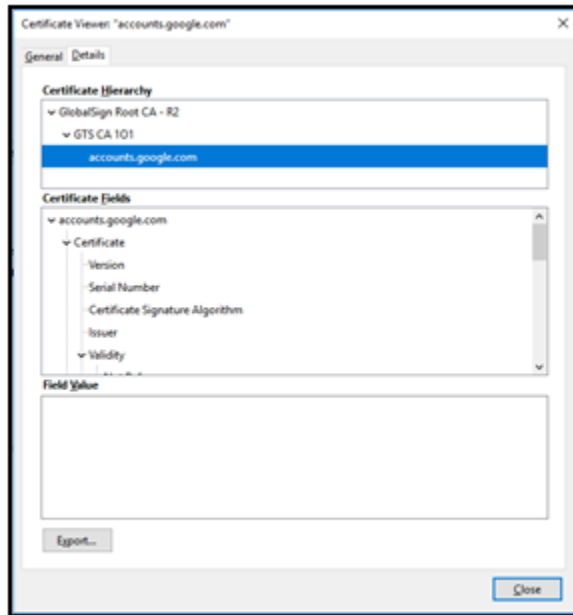
2. Click the **Show connection details** arrow.
3. Click **More Information**.
4. Click **View Certificate**.

Figure 5-2 View Certificate



5. Click **Details** tab, and then click **Export**.
6. Specify the name of the file you want to save the SSL certificate to, keep the x.509 Certificate (PEM) format, and then click the **Save**.

Figure 5-3 Details Tab



5.1.2 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). 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.
 - **Target Name Prefix:** Enter the target name prefix. For example, `test_env_orcl_src`. The target name prefix is appended with colon (":") and this gets prefixed to all target names. For example, `test_env_orcl_src:targetName`. This is an optional field.
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](#).

For more information about troubleshooting Discovery-related issues, see [Troubleshooting Discovery](#).

5.1.3 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 Service Manager information required to connect to Oracle GoldenGate:
 - **Host Name:** Enter the Service Manager hostname or Host name for OCI GoldenGate Service instance. For example: `svrmgr.us.oracle.com`.
 - **User Name:** Enter the User Name to connect to the Service Manager (or User Name of OCI GoldenGate Service instance).
 - **Password:** Enter the Service Manager Password (or Password for OCI GoldenGate Service instance).
 - **Port:** Enter Service Manager Port or port to connect to OCI GoldenGate Service instance, for example, 443.
 - **Target Name Prefix:** Enter the target name prefix. For example, `test_env_orcl_src`. The target name prefix is appended with colon (":") and this gets prefixed to all target names. For example, `test_env_orcl_src:targetName`. This is an optional field.
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 then click **Log from Agent**.

You need to promote these discovered targets now. See [Promoting Oracle GoldenGate Targets](#).

For more information about troubleshooting Discovery-related issues, see [Troubleshooting Discovery](#).

5.2 Enterprise Manager CLI Verb-Based Discovery of Oracle GoldenGate Targets

- [Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance using EM CLI](#)
Oracle Enterprise Manager Command Line Interface (EM CLI) enables you to access Enterprise Manager functionality through a command-line interface or scripts. The `discover_gg` Verb is used to discover Oracle GoldenGate Classic targets. Targets discovered using this emcli verb are auto promoted, except when they are run using the `-check` option.
- [Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance using EM CLI](#)
The `discover_ggma` Verb is used to discover Oracle GoldenGate Microservices targets. Targets discovered using this emcli verb are auto promoted.

5.2.1 Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance using EM CLI

Oracle Enterprise Manager Command Line Interface (EM CLI) enables you to access Enterprise Manager functionality through a command-line interface or scripts. The `discover_gg` Verb is used to discover Oracle GoldenGate Classic targets. Targets discovered using this emcli verb are auto promoted, except when they are run using the `-check` option.

For more information about EM CLI, see EM CLI Overview and Concepts. For more information about discovery, see [Discovering Oracle GoldenGate Targets in the UI](#).

Syntax

```
emcli discover_gg  
[-configFile="configFile"]  
[-debug]  
[-check]
```

Options

-configFile

Path to the discovery input file. Ensure that this file contains the following parameters:

- **host** - Hostname of Oracle GoldenGate Monitor Agent. For example, `host00uaz.us.oracle.com`
- **port** - Port of Oracle GoldenGate Monitor Agent. For example, `5559`.
- **user** - Username to connect to Oracle GoldenGate Monitor Agent. For example, `ogmajmxusr`.
- **password** - Password to connect to Oracle GoldenGate Monitor Agent.
- **agentURL** - Enterprise Manager Agent URL. For example, `https://host00uaz.us.oracle.com:3872/emd/main/`. You can also set multiple secondary agentURLs that are comma separated. The first url in the list that is UP and

running will be considered as the primary agentURL and the rest are all secondary URLs. For example, `https://phoenix93982.dev3sub2phx.databasede3phx.oraclevcn.com:3872/emd/main/,https://london57277.dev1sub11hr.databasede021hr.oraclevcn.com:3872/emd/main,https://phoenix95679.dev3sub2phx.databasede3phx.oraclevcn.com:3872/emd/main/`.

- **targetNamePrefix** - Enter the target name prefix. For example, `test_env_orcl_src`. The target name prefix is appended with colon (":") and this gets prefixed to all target names. For example, `test_env_orcl_src:targetName`. This is an optional field.

-debug

Runs the verb in verbose mode for debugging purposes.

-check

Runs discovery and displays the results. This does not add the targets.

Exit Codes

- 0 - On success
- Non-zero value - Verb processing was not successful.

Example

```
emcli discover_gg
-configFile="/scratch/input.conf"
-debug
-check
```

For more information about troubleshooting Discovery-related issues, see [Troubleshooting Discovery](#).

5.2.2 Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance using EM CLI

The `discover_ggma` Verb is used to discover Oracle GoldenGate Microservices targets. Targets discovered using this `emcli` verb are auto promoted.

For more information about the prerequisites to discover secure Microservices, see [Prerequisites to Discover Secure Oracle GoldenGate Microservices Instances](#).

Syntax

```
emcli discover_ggma
[-configFile="configFile"]
[-debug]
[-check]
```

Options

-configFile

Path to the discovery input file. This file contains the following parameters:

- **host** - Hostname of Oracle GoldenGate Service Manager. For example, `host00smz.us.oracle.com`
- **port** - Port of Oracle GoldenGate Service Manager.

- **user** - Username to connect to Oracle GoldenGate Service Manager. For example, oggmasmsr.
- **password** - Password to connect to Oracle GoldenGate Service Manager.
- **agentURL** - Enterprise Manager Agent URL. For example, `https://host00uaz.us.oracle.com:3872/emd/main/`. You can also set multiple secondary agentURLs that are comma separated. For example, the first url in the list that is UP and running will be considered as the primary agentURL and the rest are all secondary URLs. For example, `https://phoenix93982.dev3sub2phx.databasede3phx.oraclevcn.com:3872/emd/main/,https://london57277.dev1sub11hr.databasede021hr.oraclevcn.com:3872/emd/main,https://phoenix95679.dev3sub2phx.databasede3phx.oraclevcn.com:3872/emd/main/`.
- **targetNamePrefix** - Enter the target name prefix. For example, `test_env_orcl_src`. The target name prefix is appended with colon (":") and this gets prefixed to all target names. For example, `test_env_orcl_src:targetName`. This is an optional field.

-debug

Runs the verb in verbose mode for debugging purposes.

-check

Runs discovery and displays the results. This does not add the targets.

Exit Codes

- 0 - On success
- Non-zero value - Verb processing was not successful.

Example

```
emcli discover_ggma  
[-configFile="/path/gg_discovery_input_file.properties"]  
[-debug]  
[-check]
```

For more information about troubleshooting Discovery-related issues, see [Troubleshooting Discovery](#).

6

Promote

- [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.
- [Target Metrics Available on OGG Home Page](#)

6.1 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 [Target Metrics Available on OGG Home Page](#).

For more details, see [Discovering, Promoting, and Adding Targets](#)

6.2 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 Service, Performance Metrics Service, Distribution Service, Receiver Service, Extract, Replicat (in case of Oracle GoldenGate Microservices instance).

 **Note:**

In case of OCI GoldenGate Service environment, Service Manager is not displayed and Deployment is the root target (parent target).

- 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.

7

Configure

- [Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager](#)
- [Creating the Oracle Wallet](#)
- [Configuring Instance-Level Security](#)
Enterprise Manager provides instance-level security flexibility to provide target-level privileges to administrators.

7.1 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](#).

7.2 Creating the Oracle Wallet

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`

7.3 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**.

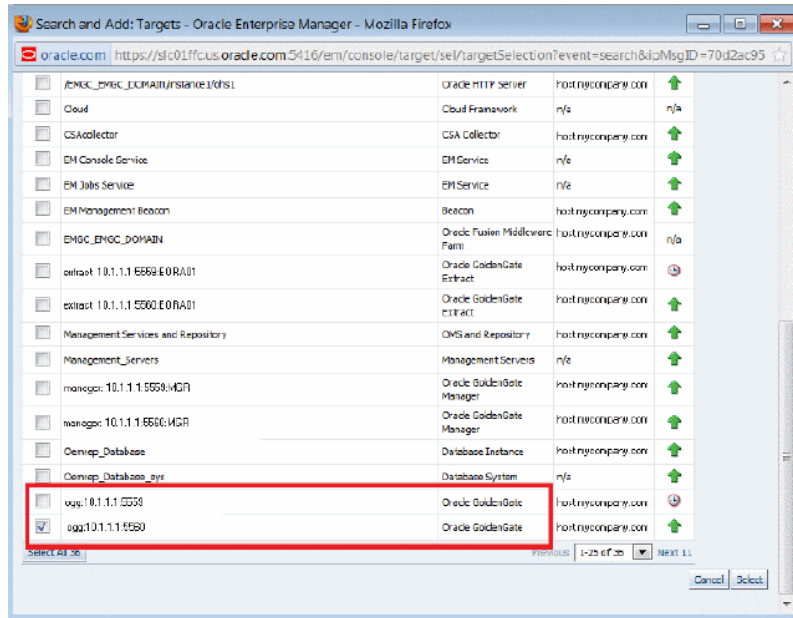
These two roles are required for full functionality and multi-version support.

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 instances.
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.



- 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.

- 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 privileges 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*.

- [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.

7.3.1 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.

8

Manage

- [Manage Credentials](#)
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.
- [Manage Events, Alerts, and Incidents](#)

8.1 Manage Credentials

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 and Monitoring Credentials for Oracle GoldenGate Classic as well as Oracle GoldenGate Microservices (MA) instances. However, Monitoring credentials are auto set after discovery.

Before setting credentials, you can neither view the target Metrics nor can access the log files. You can also notice that the process action buttons (the Start and Stop buttons) are also disabled. These buttons are grayed out.

Figure 8-1 Action Buttons are not active

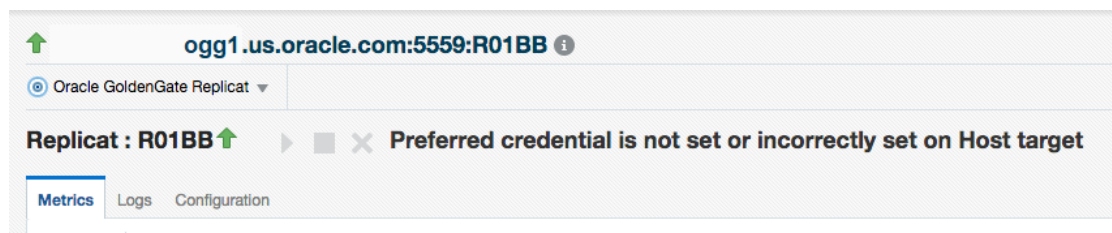
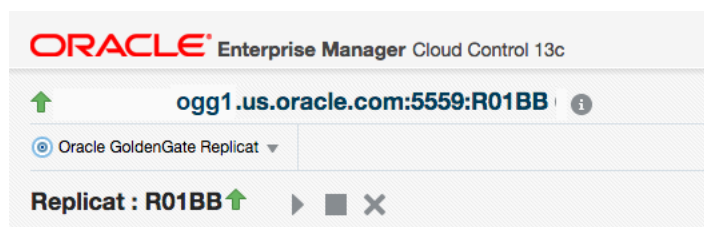


Figure 8-2 Action Buttons are active



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](#).

- [Different Credential Sets for Oracle GoldenGate](#)
- [Setting Credentials for Oracle GoldenGate Targets](#)

8.1.1 Different Credential Sets for Oracle GoldenGate

- [Preferred Credentials](#)
The preferred credentials are hierarchical in nature. 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 as well as Microservices instances.
- [Monitoring Credentials](#)
Monitoring credentials are required to get metrics from GoldenGate targets. These are set by default after discovery.

8.1.1.1 Preferred Credentials

The preferred credentials are hierarchical in nature. 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 as well as Microservices 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. If you don't set this credential, then you can't start or stop the processes.

OGG Admin Credentials

OGG Admin Credentials is the credentials of Oracle GoldenGate Monitoring Agent. In the UI, you set the **Monitor Agent Username** and **Monitor Agent Password**. The **Monitor Agent Username** is defined in the `config.properties` in the Oracle GoldenGate Monitoring Agent installation.

8.1.1.2 Monitoring Credentials

Monitoring credentials are required to get metrics from GoldenGate targets. These are set by default after discovery.

The monitoring credentials are required to be set for Oracle GoldenGate target in case of classic instances and to GoldenGate Service Manager or GoldenGate Deployment and GoldenGate Administration Service target type (optional) in case of MA instances.

8.1.2 Setting Credentials for Oracle GoldenGate Targets

- [Setting Credentials for Oracle GoldenGate Classic Instance](#)
To set Preferred credentials for an Oracle GoldenGate classic instance, you need to set both the Host credentials as well as the OGG Admin credentials. Monitoring credentials is also required for collection of metrics. However, they are set by default after discovery.
- [Setting Credentials for Oracle GoldenGate Microservices Instance](#)
Monitoring credentials are set by default after discovery. Choose to modify them if and when the credentials change. You can set Host and Monitoring credentials for Oracle Administration Service too if the credentials are different than Service Manager, or Oracle GoldenGate Deployment in-case of OCI GoldenGate Service.

8.1.2.1 Setting Credentials for Oracle GoldenGate Classic Instance

To set Preferred credentials for an Oracle GoldenGate classic instance, you need to set both the Host credentials as well as the OGG Admin credentials. Monitoring credentials is also required for collection of metrics. However, they are set by default after discovery.

To set 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 Target Type** 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 **Monitor Agent Username** and **Monitor Agent Password** credentials that were used to discover this GoldenGate instance.

 **Note:**

If there are any changes to the Monitor Agent credentials in Oracle GoldenGate Core, then you need to update the same changes in both the Preferred Credentials as OGG Admin Credentials, as well as Monitoring credential for Oracle GoldenGate target

7. Under **Target Preferred Credentials**, click 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.

8.1.2.2 Setting Credentials for Oracle GoldenGate Microservices Instance

Monitoring credentials are set by default after discovery. Choose to modify them if and when the credentials change. You can set Host and Monitoring credentials for Oracle Administration Service too if the credentials are different than Service Manager, or Oracle GoldenGate Deployment in-case of OCI GoldenGate Service.

Setting Preferred Credentials

These credentials are applicable only to the Service Manager's child targets (Extract and Replicat) or the child targets of Oracle GoldenGate Deployment in case of OCI GoldenGate Service.

To set the Preferred credentials for the Oracle GoldenGate Service Manager (Oracle GoldenGate Deployment in case of OCI GoldenGate Service):

1. Navigate to the **Setup** menu, select **Security**, and then select **Preferred Credentials** to display the **Security > Preferred Credentials** page.
2. Select the **Oracle GoldenGate Service Manager** Target Type. In case of OCI GoldenGate Service, select the **Oracle GoldenGate Deployment Target Type**. Click **Manage Preferred Credentials** to view the **Oracle GoldenGate Service Manager Preferred Credentials** page. Note that in case of OCI GoldenGate Service, you can view the **Oracle GoldenGate Deployment Preferred Credentials** page.
3. Under **Default Preferred Credentials**, select **Host Credentials**, and click **Set** to display the **Select Named Credential** dialog box.
4. Click **New** to enter the **EM Agent UserName**, **Password**, and **Confirm Password**. Use credential that can be used to login to the EM Agent Host machine.
5. Click **Save** to save the new credentials.

The Preferred Credentials are set and an information that the Named credential association has been completed successfully is indicated on the screen.

6. If you want to change the credentials for the Oracle GoldenGate Administration Service, then you can set the credentials under **Oracle GoldenGate Administration Service** Target type. This is an Optional Step.

Setting Monitoring Credentials

These credentials are applicable only to the Service Manager's child targets (Extract and Replicat) or the child targets of Oracle GoldenGate Deployment in case of OCI GoldenGate Service.

To set the Monitoring credentials for the Oracle GoldenGate Service Manager (or Oracle GoldenGate Deployment in case of OCI GoldenGate Service):

1. Navigate to the **Setup** menu, select **Security**, and then select **Monitoring Credentials** to display the **Security > Monitoring Credentials** page.
2. Select **Oracle GoldenGate** and click **Manage Monitoring Credentials** to view the **Oracle GoldenGate Service Manager Monitoring Credentials** page. In case of OCI GoldenGate Service, select **Oracle GoldenGate Deployment** to view the **Oracle GoldenGate Deployment Monitoring Credentials** page.

3. Select the Target under **Target type**.
4. Enter the **Username**, **Password**, and **Confirm Password**, click **Save** and **Close**. You need to provide Service Manager user name and password here in order to administer Oracle GoldenGate Microservices targets.

In case of OCI GoldenGate Service, you need to provide the GGS User Name and Password in order to administer the Oracle GoldenGate Microservices target.

The Monitoring Credentials are set and an information that the credentials are set successfully is shown on the screen.

 **Note:**

If there are any changes to the Service Manager or Deployment credentials for OCI GoldenGate Service in Oracle GoldenGate Core, then you need to include the same as Monitoring credential for the Service Manager (and Deployment target in case of OCI GoldenGate Service).

5. If you want to change the credentials for the Oracle GoldenGate Administration Service, then you can set the credentials under **Oracle GoldenGate Administration Service** Target type. This is an optional step.

 **Note:**

If you have set the Administration Service credentials, then the credentials are applicable only for its child target types.

8.2 Manage Events, Alerts, and Incidents

- **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.
- **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.
- **Alerts on Home Page**
The Oracle GoldenGate Home page displays all the incidents that are generated. An alert is generated when a metric threshold is reached. The most recent alerts are listed first.
- **Metric Data**
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.

8.2.1 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](#).

8.2.2 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.

- [Setting Metric Alerts and Incidents for Extract and Replicat](#)
- [Setting Metric Alerts and Incidents for Oracle GoldenGate Monitor Agent](#)
- [Setting Incidents and Alerts for Oracle GoldenGate Target Availability](#)
You need to set alerts on Target Availability of all the Oracle GoldenGate targets to get notified when there are any issues with these targets.
- [Setting Metric Alerts and Incidents for Distribution Service Path and Receiver Service Path](#)
- [Setting Alerts for Events](#)
You can set alerts for specific patterns on event messages for all targets, except Oracle GoldenGate Service Manager. Select any pattern on messages, severity, and error code for creating alerts and then alerts are triggered when such patterns are generated in event messages. Pattern set is case sensitive.

8.2.2.1 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.

8.2.2.2 Setting Metric Alerts and Incidents for Oracle GoldenGate Monitor Agent

The **OGG Home** page displays a Warning icon and a tool tip, and preserves the previously known status of each of the GoldenGate classic targets in the following conditions:

- If either the Monitor agent or Web Service is down
- If both the Monitor agent and the Web Service are down

If you want to set alerts of metric status values, the following are the status values of Oracle GoldenGate Monitor Agent, which is grouped under the Oracle GoldenGate target.

Metric	Description
GoldenGate Agent Status	Valid Values: 1: Indicates UP status 2: Indicates DOWN status
WebService Availability Status	Valid Values: 1: Indicates Up status 0: Indicates Down status

Note:

Oracle recommends to set alerts for Oracle GoldenGate Monitor agent Status and WebService Availability Status to identify issues with the Oracle GoldenGate Monitor agent target, as these are required to be UP in order to get accurate status or metric updates for other Oracle GoldenGate Classic targets.

8.2.2.3 Setting Incidents and Alerts for Oracle GoldenGate Target Availability

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

This includes occurrences when the Oracle Enterprise Manager is unable to retrieve status of these 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 recipients 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 recipients 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*.

8.2.2.4 Setting Metric Alerts and Incidents for Distribution Service Path and Receiver Service Path

You can set the Status of Distribution Service and Receiver Service paths in the corresponding target of [Distribution Service](#) and [Receiver Service](#). By default, the metric threshold is set to be alerted when path is stopped or killed. You can update these values if required.

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](#).

Distribution Service Path and Receiver Service Path Metric Data

Metric	Description
Status	Status of the Distribution/Receiver paths. The metric values are as follows: <ul style="list-style-type: none"> • Uninitialized = 0 • Running = 1 • Unknown = 2 • Paused = 3 • Stopping = 4 • Stopped = 5 • Killed = 6
Lag	Lag in seconds between the time when extract wrote a transaction in the trail file and the time when the Distribution/Receiver services processes this transaction.

8.2.2.5 Setting Alerts for Events

You can set alerts for specific patterns on event messages for all targets, except Oracle GoldenGate Service Manager. Select any pattern on messages, severity, and error code for creating alerts and then alerts are triggered when such patterns are generated in event messages. Pattern set is case sensitive.

To set alert for events for the entire deployment, you can set alerts for Oracle GoldenGate (in case of classic) or Oracle GoldenGate Deployment (in case of MA).

To set alerts for specific patterns on event messages on a target:

1. Click **Targets** and then select **GoldenGate** to view a list of discovered targets.
2. On the **OGG Home** page, select a target, for example, Oracle GoldenGate or Oracle GoldenGate Deployment.
3. From the corresponding target drop-down, click, **Monitoring**, and then click **Metric and Collection Settings** (click the **Pencil** icon).
4. Expand **Metrics with Tresholds** and select **All Metrics**.
5. Expand **Log Events** and enter values for Code (error code), Message, and Severity. For example:
 - **Code:** OGG-01896
 - **Message:** Alter Extract
 - **Severity:** FATAL
6. Click **OK**.

For more information about viewing the metrics, see [Enabling/Disabling Metrics](#).

8.2.3 Alerts on Home Page

The Oracle GoldenGate Home page displays all the incidents that are generated. An alert is generated when a metric threshold 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*.

- [Indication of GoldenGate Monitor Agent and WebService being Down](#)

8.2.3.1 Indication of GoldenGate Monitor Agent and WebService being Down

The Warning icon if present next to any GoldenGate Classic target status indicates either of the following:

- GoldenGate Monitor Agent is down or unreachable.
- GoldenGate Webservice is down/unreachable to Monitor Agent.

The status of the targets isn't being evaluated due to this and the previous successful status retrieved is being displayed.

8.2.4 Metric Data

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**.

For more information on the metric data specific to targets, see [Supported Target Types](#). 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.

- [Enabling/Disabling Metrics](#)
You can view all the Metrics from the **Metrics and Collection Settings** page. By default, except the Log Event metric, the rest of the collection metrics are enabled.

8.2.4.1 Enabling/Disabling Metrics

You can view all the Metrics from the **Metrics and Collection Settings** page. By default, except the Log Event metric, the rest of the collection metrics are enabled.

For more information about setting alerts for Log Events, see [Setting Alerts for Events](#)

1. Click **Targets**, select Oracle GoldenGate target (for a Classic instance). For Microservices, you need to select **Deployment**.
2. In the **Target** menu, select **Monitoring**, and then select **Metric and Collection Settings**.
3. In the **Other Collected Items** tab, click the **Disabled** link against **Log Event** to view the **Edit Collection Settings: Log Event** page.
4. Under **Collection Settings**, click **Enable**.

5. In the **Metric and Collection Settings** page, click **OK**.

To disable the metric:

1. Click **Every Five Minutes** link.
2. Click **Disabled** in the **Monitor and Collection Settings** page.

9

Monitor

- [Viewing Target Details](#)
- [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.
- [Metrics Tab](#)

The **Metrics** tab on the Targets page enable you to monitor metrics and to alert users about specific metric results.
- [Log Tab](#)

For targets, such as Extract and Replicat, the **Log** tab contains the following: **Report**, **Discards**, and **Events**. The Log tab is valid only for Extract and Replicat and not for the rest of the targets.
- [Events Tab](#)

The **Events** tab shows the **Message Id**, **Timestamp**, **Code**, **Severity**, **Message**, and details of Oracle GoldenGate events pertaining to corresponding deployment (Deployment, Oracle GoldenGate) or respective processes and services. The Oracle GoldenGate events are displayed for all targets, except the Oracle GoldenGate Service Manager.
- [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 for Big Data properties file. There can be multiple such tabs for these files. You can modify the content of the properties and parameter files.
- [Elements for Monitoring Targets](#)
- [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.

9.5 Events Tab

The **Events** tab shows the **Message Id**, **Timestamp**, **Code**, **Severity**, **Message**, and details of Oracle GoldenGate events pertaining to corresponding deployment (Deployment, Oracle GoldenGate) or respective processes and services. The Oracle GoldenGate events are displayed for all targets, except the Oracle GoldenGate Service Manager.

The **Process** column is shown for Oracle GoldenGate target (classic) and Deployment target (MA). These parent targets show cumulative events for the child targets. The Events are in a descending order of event timestamp, ordered by the latest event in the table.

Viewing Event Metrics

By default, this metric is disabled. The Message Id is shown as **No Data Available**, in case the Event Metric is not enabled. Therefore to view the Event Metric in the UI, you need to enable the metrics. See [Enabling/Disabling Metrics](#) to enable and view metric data.

Sort: You can sort the table by clicking on the **Message Id**, **TimeStamp**, **Code**, **Severity**, and **Process** columns. All events are displayed in a descending order of event timestamp by default; latest event is displayed on top. By default, 20 events are displayed on a page.

Search: You can search for any string from the events using the **Search** box. Search is case insensitive and it can be based on any of the following fields: Severity, Error codes, or any message text from the event. For example, if you want to look up for events of Severity `ERROR`, then only `ERROR` events are displayed in UI.

Download: Click **Export** to export all the events. Similarly, in case of Deployment target (MA) and Oracle GoldenGate target (classic), you can view the event messages of all the processes on the **Events** tab. For more information about setting alerts for Events, see [Setting Alerts for Events](#).

Purge: You can view historical data up to a month. Historical data is purged automatically on a monthly basis. You can modify the retention period of the data. To do this, execute the following in the Oracle Enterprise Manager repository:

```
gc_interval_partition_mgr.set_retention('SYSMAN', 'gg_log_events_e', <number of partitions to retain>);
```

Here, the number of partitions can be 1, 2, 3,...N, where N represents number of months. For more information, see [Management Repository Data Retention Policies](#) in *Enterprise Manager Cloud Control Administrator's Guide*.

9.1 Viewing Target Details

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.

9.2 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.
2. Select either the Extract or Replicat Process.
3. Click one of the following: **Start**, **Stop**, or **Kill**.

- [EMCLI Commands on Oracle GoldenGate Targets](#)
The `gg_execute` Verb is used to execute commands on the Oracle GoldenGate Classic as well as Microservices targets.

9.2.1 EMCLI Commands on Oracle GoldenGate Targets

The `gg_execute` Verb is used to execute commands on the Oracle GoldenGate Classic as well as Microservices targets.

Syntax

```
emcli gg_execute -command="<name of the command>"  
-target_type="<type of the target>"  
-target_name="<name of the target>"  
-options=""
```

Explanation of the Command

- **command** : Valid values are `start`, `stop`, or `kill`. Based on the command passed, appropriate action is taken on the process.
- **target_type**: Valid values are either of the following: `oracle_goldengate_extract` or `oracle_goldengate_replicat`.
- **target_name** : Fully qualified name of the process or target as shown in the following example:
- **options** : It is an optional argument. Currently, valid for `START` command. For example, `-options="ATCSN 12456"`

Note:

Before you execute this command, ensure that the preferred credential is already set (either using the UI or the EMCLI, else an error gets displayed when the `gg_execute` command is executed).

Example

```
emcli gg_execute -command="start" -target_type="oracle_goldengate_extract" -  
target_name="extract:hostname:port:EOBEY"
```

9.3 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 displayed on the OGG Home page, see [Target Metrics Available on OGG Home Page](#).

9.4 Log Tab

For targets, such as Extract and Replicat, the **Log** tab contains the following: **Report**, **Discards**, and **Events**. The Log tab is valid only for Extract and Replicat and not for the rest of the targets.

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
```

For more information about the Events tab, see [Events Tab](#).

9.6 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 for Big Data properties file. There can be multiple such tabs for these files. You can modify the content of the properties 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 changes. 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.

9.7 Elements for Monitoring Targets

Table 9-1 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 <i>Enterprise Manager Cloud Control Middleware Management Guide</i> and Monitor .
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*.

9.8 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 in the UI](#).
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.

10 Audit

- [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.
- [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.

10.1 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 <code>ggserr.log</code> 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"
```

10.2 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.

Timestamp	Operation	Status	Administrator	Upstream Component Type	Message	Session
Feb 2, 2016 10:36:22	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	AC2DC338755CA7...
Jan 30, 2016 01:26:50	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	9E90D8CCTD4AE1
Jan 30, 2016 01:04:53	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	71F2248B1A40771C
Jan 29, 2016 10:25:40	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged out suc...	5A3AD814DA709F
Jan 29, 2016 03:39:21	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	9E90D8CCTD4AE1
Jan 29, 2016 12:18:45	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on succ...	5A8AD814DA709F
Jan 29, 2016 10:47:17	Enterprise Man...	Success	SYSMAN	Browser	SYSMAN Logged on suc...	71F77A8A1481771C

Audit Record Details

General | Client Information | OMS Information | Operation Specific 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 06:30:21 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.

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*.

11

Troubleshoot

- [Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files](#)
- [Troubleshooting Discovery](#)
- [Troubleshooting Credentials](#)
- [Troubleshooting Metric Collections](#)
- [Troubleshooting GoldenGate Targets Status Issues](#)
- [Troubleshooting False Alerts](#)
- [Troubleshooting High Availability](#)

11.7 Troubleshooting High Availability

- [Remote EM Agent is not able to Connect to Oracle GoldenGate Agent](#)

11.7.1 Remote EM Agent is not able to Connect to Oracle GoldenGate Agent

In a High Availability environment of the node cluster, Oracle GoldenGate instance can relocate to a different machine in case of a classic instance. In the relocate scenario, the Enterprise Manager Agent of the previous machine continues to serve the Oracle GoldenGate Agent until the source/replica values are changed from Manage Agent UI from the Enterprise Manager console.

If the `mgr port`, `pmsrvr port`, and `jagent.rmi.port` are blocked by the firewall, then the remote Enterprise Manager Agent does not make a connection with the Oracle GoldenGate Agent and monitoring stops.

For a seamless monitoring you need to ensure that the `mgr port`, `pmsrvr port`, and `jagent.rmi.port` were not blocked by a firewall. To verify, execute the following telnet commands:

```
telnet gg-VipName jagent.rmi.port
curl -v telnet://gg-VipName:jagent.rmi.port
nc -zv -w 5 gg-VipName jagent.rmi.port
```

11.1 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.*`, where * can be 0, 1, 2, 3...n

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 Monitoring Agent, the information is logged in this file.

For example:

```
/home/oracle/oem/agent/agent_inst/sysman/emd/ogg_so_logs.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
```

EM Agent REST log file: `gcagent_rest.log.*`

To enable debug logs for REST Fetchlets for Microservices targets, add the following lines to the `$EMSTATE/sysman/config/emd.properties` file:

```
# For REST Fetchlet
ODLLogger.rest.level=DEBUG
ODLLogger.rest.totalSize=5
ODLLogger.rest.segment.count=5
ODLLogger.rest.filename=gcagent_rest.log
ODLLogger.rest.logger=oracle.sysman.gcagent.addon.fetchlet.muws.ws.rs.RESTfulServiceFetchlet
```

This creates the `gcagent_rest.log.*` under `$EMSTATE/sysman/log`, where * can be 0, 1, 2, 3...n

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
```

11.2 Troubleshooting Discovery

Ocasionally, though a Discovery successful message is indicated on the screen, the discovery of targets is not successful. This topic describes various scenarios to troubleshoot the unsuccessful discovery of Oracle GoldenGate targets.

- [Troubleshooting: Oracle GoldenGate Classic Targets](#)
- [Troubleshooting: Oracle GoldenGate Microservices Targets](#)

11.2.1 Troubleshooting: Oracle GoldenGate Classic Targets

- [Identifying the Error](#)

11.2.1.1 Identifying the Error

To identify the error:

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. On the **Targets on Host** tab, select a target and then click **Diagnostic Details** to display the Diagnostic Details page.
3. Select the **Oracle GoldenGate** target that you just discovered.
4. Click **Log from Agent** to display a Confirmation dialog box.
5. Scroll down the Confirmation dialog to view the errors.

Resolution

1. Discover an Oracle GoldenGate instance as described in [Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance](#).
2. While discovering a target, when you come across the **Edit Parameters: Oracle GoldenGate** dialog box, enter the correct **Monitor Agent Password** for the given **Monitor User Name** and click **OK**.
3. Click **Discover Now** and click **Yes** in the **Discover Now** confirmation dialog box.
4. After the discovery is successful, click **Close** in the Confirmation dialog box.
5. 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**.

This topic describes the following discovery-related errors:

- [Authentication Issue: EM-06006: Connection Setup Failed. Security Error or Authentication Issue](#).
- [Connection Issue](#)

11.2.1.1.1 Authentication Issue: EM-06006: Connection Setup Failed. Security Error or Authentication Issue.

Enter the correct Monitor Agent credentials, host, and port names to successfully discover Oracle GoldenGate Classic target.

11.2.1.1.2 Connection Issue

If Discovery is not successful and a Connection Exception has occurred, then you need to check the following:

- In the Oracle GoldenGate Installation location, for example `OGG_HOME`, ensure that the Monitor Agent is running successfully.
- Ensure that there is no firewall blocking connection to the Oracle GoldenGate host from the Enterprise Manager Agent host.
- If the Monitor Agent does not run successfully, then you need to check and update the `config.properties`. For more information about updating the configuration properties, see [Update the Configuration Properties](#) in the *Installing and Configuring Oracle GoldenGate Monitor Agent* guide.

- You may also run the Monitor agent debug tool to check the connection to Oracle GoldenGate Monitor agent with assistance from Oracle Support. See Doc ID 2410209.1 at support.oracle.com

11.2.2 Troubleshooting: Oracle GoldenGate Microservices Targets

- [Identifying the Error](#)

11.2.2.1 Identifying the Error

To identify the error:

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. On the **Targets on Host** tab, select a target and then click **Diagnostic Details** to display the Diagnostic Details page.
3. Select the **Oracle GoldenGate Service Manager** target that you just discovered.
4. Click Log from Agent to display a Confirmation dialog box.
5. Scroll down the Confirmation dialog to view the errors.

Resolution

1. Discover a Microservices instance as described in [Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance](#).
2. While discovering a target, when you come across the Edit Parameters: Oracle GoldenGate dialog box, enter the correct Password for the given User Name and click **OK**.
3. Click **Discover Now** and click **Yes** in the **Discover Now** confirmation dialog box.
4. After the discovery is successful, click **Close** in the Confirmation dialog box.
5. 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**.

Oracle GoldenGate Microservices targets are successfully discovered on entering the appropriate Hostname, Username, Password, Port, and Target Name Prefix in the Edit Parameters dialog box.

This topic describes the following discovery-related errors:

- [Authentication Issue](#)
- [Connection Issue](#)
- [SSL Certificate Issue](#)

11.2.2.1.1 Authentication Issue

Ensure that you are able to login to the Oracle GoldenGate Microservices URL using the correct credentials that you have entered in the Oracle GoldenGate Enterprise Manager Plug-in to successfully discover Oracle GoldenGate Microservices targets.

11.2.2.1.2 Connection Issue

If discovery is not successful and a Connection Exception has occurred, then you need to ensure the following:

- The Oracle GoldenGate Service Manager is up and running in case of Oracle Cloud Infrastructure (OCI) Marketplace instances or on-premises GoldenGate instances.
- Ensure that the Administration Service and Performance Metrics Service are up and running.
- There is no firewall blocking connection to the Oracle GoldenGate host from the Enterprise Manager Agent host.
- Oracle GoldenGate REST APIs ([Performance Metrics Service](#)) are accessible from the Enterprise Manager Agent. For example, use the **cURL** command to test the connectivity to the Oracle GoldenGate REST APIs. For more information about using the command, see [REST API for Oracle GoldenGate](#).
- If Oracle GoldenGate is running with SSL, then you need to import the certificate at the Enterprise Manager Agent TrustStore. Ensure that the certificate is imported in the correct Enterprise Manager agent that monitors the corresponding GoldenGate targets. You can view and download the certificate using the browser by logging into the Oracle GoldenGate Administration Service UI or the Service Manager UI in case of OCI GoldenGate instance.

11.2.2.1.3 SSL Certificate Issue

If discovery is not successful and a valid certification path to requested target is not found, then you need to ensure the following:

- Ensure that the Administration Service and Performance Metrics Service are up and running.
- Ensure that the SSL certificate has been uploaded/installed on the OEM Agent present in GoldenGate Microservices server.

 **Note:**

If you have uploaded SSL certificate in OEM Agent running on the OMS Server and not on OEM Agent running on GoldenGate Microservices Server, then target discovery fails with the following error:

```
SEVERE: Exception during Targets discovery: EM-90000 - Target  
Discovery failed. Internal Error. Please contact System  
Administrator.
```

```
com.oracle.sysman.goldengate.discovery.GoldenGateDiscovery$GGDiscove  
ryException: EM-90000 - Target Discovery failed. Internal Error.  
Please contact System Administrator. Unable to find valid  
certification path to requested target.
```

Performance Metric REST API will directly read with OMS Server.

11.3 Troubleshooting Credentials

Before setting credentials, you can neither view the target Metrics nor can access the log files. You can also notice that the process action buttons (the Start and Stop buttons) are also disabled. These buttons are grayed out.

- [Troubleshooting: Oracle GoldenGate Classic Credentials](#)
- [Troubleshooting: Oracle GoldenGate Microservices Credentials](#)

11.3.1 Troubleshooting: Oracle GoldenGate Classic Credentials

This topic describes how to troubleshoot the Oracle GoldenGate Classic credentials-related issues.

- [Start and Stop Buttons are Disabled](#)
- [Preferred credential is not Set or is Incorrectly Set on Host Target](#)
- [Unable to Check Configurations or Logs of a Process](#)
- [Decrypt : Failed to decrypt buffer error while testing the preferred credential after upgrade](#)

11.3.1.1 Start and Stop Buttons are Disabled

- Ensure that you have all the required entitlements and permissions. Ensure that you have Enterprise Manager Agent machine Host credential and Oracle GoldenGate Monitoring credential permissions set.
- Ensure that you have configured the Preferred Credentials - Host Credentials for the Oracle GoldenGate target. See [Setting Credentials for Oracle GoldenGate Classic Instance](#).
- Ensure that you have configured the Preferred Credentials - OGG Admin Credentials for the Oracle GoldenGate target. See [Setting Credentials for Oracle GoldenGate Classic Instance](#).

11.3.1.2 Preferred credential is not Set or is Incorrectly Set on Host Target

1. Ensure that you have all the required entitlements and permissions. Ensure that you have Enterprise Manager Agent machine Host credential and Oracle GoldenGate Monitoring credential permissions set.
2. Ensure that you have configured the Preferred Credentials - Host Credentials for the Oracle GoldenGate target. See [Setting Credentials for Oracle GoldenGate Classic Instance](#).
3. On the **Target Preferred Credentials** page, click **Test** to test whether the related credentials are correct.
4. After the upgrade, set the Preferred Credentials - Host Credentials and Preferred Credentials - OGG Admin Credentials again. [Setting Credentials for Oracle GoldenGate Classic Instance](#).

11.3.1.3 Unable to Check Configurations or Logs of a Process

1. Ensure that you have all the required entitlements and permissions. Ensure that you have Enterprise Manager Agent machine Host credential and Oracle GoldenGate Monitoring credential permissions set.
2. Ensure that you have configured the Preferred Credentials - Host Credentials for the Oracle GoldenGate target. See [Setting Credentials for Oracle GoldenGate Classic Instance](#).

11.3.1.4 Decrypt : Failed to decrypt buffer error while testing the preferred credential after upgrade

Ensure to execute the `$EMAGENT_HOME/root.sh` command for the upgraded Enterprise Manager agent.

11.3.2 Troubleshooting: Oracle GoldenGate Microservices Credentials

This topic describes how to troubleshoot the Oracle GoldenGate Microservices credentials-related issues.

- [Start and Stop Buttons are Disabled](#)
- [Monitoring Credentials are Either Not Set or Set Incorrectly](#)
- [Unable to Check Configurations or Logs of a Process](#)
- [Decrypt : Failed to Decrypt Buffer Error while Testing the Preferred Credential after Upgrade](#)

11.3.2.1 Start and Stop Buttons are Disabled

- Ensure that you have all the required entitlements and permissions. Ensure that you have Enterprise Manager Agent machine Host credential and Oracle GoldenGate Service Manager credential permissions (or Oracle GoldenGate Deployment credential permissions in case of OCI GoldenGate service) set.
- Ensure that you have configured the Preferred Credentials - Host Credentials for:
 - the Oracle GoldenGate Service Manager**OR**
 - the Oracle GoldenGate Deployment in case of OCI GoldenGate service.See [Setting Credentials for Oracle GoldenGate Microservices Instance](#)
- Ensure that you have set the Monitoring credentials for the Oracle GoldenGate Service Manager. See [Setting Credentials for Oracle GoldenGate Microservices Instance](#).

11.3.2.2 Monitoring Credentials are Either Not Set or Set Incorrectly

Ensure that the Monitoring Credentials are set properly for the Service Manager target (in case of OCI GoldenGate Service, Monitoring Credentials must be set for the Deployment target). See [Setting Credentials for Oracle GoldenGate Microservices Instance](#).

11.3.2.3 Unable to Check Configurations or Logs of a Process

1. Ensure that you have all the required entitlements and permissions. Ensure that you have Enterprise Manager Agent machine Host credential and Oracle GoldenGate Service Manager credential permissions set or Oracle GoldenGate Deployment credential permission in-case of OCI GoldenGate Service.
2. Ensure that you have configured the correct Preferred Credentials - Host Credentials and Monitoring Credentials for:
 - Oracle GoldenGate Service Manager instance.
OR
 - Oracle GoldenGate Deployment instance in-case of OCI GoldenGate Service.See [Setting Credentials for Oracle GoldenGate Microservices Instance](#).

11.3.2.4 Decrypt : Failed to Decrypt Buffer Error while Testing the Preferred Credential after Upgrade

Ensure to execute the `$EMAGENT_HOME/root.sh` command for the upgraded Oracle Enterprise Manager agent.

11.4 Troubleshooting Metric Collections

- [Metrics are not Getting updated for Oracle GoldenGate Targets](#)

11.4.1 Metrics are not Getting updated for Oracle GoldenGate Targets

Metrics are getting updated neither on the Oracle GoldenGate Home page nor within the Target Detail page for Oracle GoldenGate targets.

Verify that Oracle Enterprise Manager Agent evaluates the metric correctly. To check whether the agent can evaluate the metric or not:

Using the `emctl` command:

1. Execute the `emctl` command as follows:

```
emctl config agent listtargets | grep <target_type>
```

2. Check if the target that shows pending status is listed here. If it is listed, then run the command as follows:

```
./emctl getmetric agent <target_name>,<target_type>,<metric_name>
```

- `<target_name>` is the full name you will see on the **OGG Home** page (assuming the name was not changed in the home page or alias not given).
- `<target_type>`: `oracle_goldengate_extract` is the target type for Extract and `oracle_goldengate_replicat` for Replicat.
- `<metric_name>`: `ExtractMetric` is the metric name for **oracle_goldengate_extract** target and `ReplicatMetric` for **oracle_goldengate_replicat** target. List of all metric names can be viewed in the Agent Metric browser.

Using the Metric browser:

1. Open the agent metric browser url: `https://<Agent host>:<Agent Port>/emd/browser/main`. Alternatively, you can find the agent url by using the `emctl status agent` command.
2. Choose the target (that shows pending status). Click **MetricName** and view the results.

Check if the Metric is Suspended:

1. Using the Metric browser: Go to the Metrics browser and click on agent. Lookup for the following metric called **z#Tasks_in_Suspension** and then click the metric.
2. Running the `emctl` command as follows: `./emctl getmetric agent <agentname>,oracle_emd, z#Tasks_in_Suspension`
3. Using the Suspension directory: Check whether the Response metric is listed in the **SUSPENSION** directory as follows: `$Agent_install_location/agent_inst/sysman/emd/state/statemgmt/oracle_emd/agent /SUSPENSION/*.*`

11.5 Troubleshooting GoldenGate Targets Status Issues

This topic lists the Oracle GoldenGate Home Targets Status issues and troubleshooting methods.

- [Oracle GoldenGate Target Shows Pending Status](#)
- [Oracle GoldenGate Classic Target Status is Shown as Down when all its Processes are Up](#)
- [Availability Evaluation Error](#)

11.5.1 Oracle GoldenGate Target Shows Pending Status

If the Oracle GoldenGate target status is shown as pending, then follow the steps here https://support.oracle.com/epmos/faces/DocumentDisplay?_afLoop=9984364293756&parent=EXTERNAL_SEARCH&sourceId=TROUBLESHOOTING&id=1546576.1&_afWindowMode=0&_adf.ctrl-state=1cpdgtojud_4 and make the required changes to the target.

11.5.2 Oracle GoldenGate Classic Target Status is Shown as Down when all its Processes are Up

- The Oracle GoldenGate target shows down when any of the process under this is down. You can check whether or not the process is up using the GoldenGate Software Command Interface (GGSCI).
- Ensure that you have upgraded to the latest Monitoring Agent version 12.2.1.2.210930 that has fixes relating to this issue.

11.5.3 Availability Evaluation Error

For the Oracle GoldenGate targets (Classic as well as Microservices targets), you need to set the credentials correctly for getting the target status and other metrics.

The Preferred credentials are 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 whether the Enterprise Manager agent is up and running. If it 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.
- [Availability Evaluation Error when Monitoring Credentials are Updated in Oracle GoldenGate Core](#)

11.5.3.1 Availability Evaluation Error when Monitoring Credentials are Updated in Oracle GoldenGate Core

When the Monitoring Agent and the Service Manager Credentials are updated in the Oracle GoldenGate Core side, then do the following in the Oracle GoldenGate Enterprise Manager Plug-in UI:

- **For a Classic instance:** Update the OGG Admin credential as Preferred credential and Monitoring credential for the Oracle GoldenGate target.
- **For a Microservices instance:** Update the Service Manager (Deployment credential in case of OCI GoldenGate Service) as Monitoring credentials .

11.6 Troubleshooting False Alerts

Oracle Enterprise Manager sends invalid False/Fake OEM alert for OGG targets - Unexpected HTTP response code [403] received.

- [False Alerts for Oracle GoldenGate Classic and Microservices \(MA\) Targets](#)
- [False Alerts for Oracle GoldenGate Classic Targets](#)
- [False Alerts for Oracle GoldenGate Microservices Targets](#)

11.6.1 False Alerts for Oracle GoldenGate Classic and Microservices (MA) Targets

The Target Availability may go down for a few seconds owing to various reasons, such as network issues. As a workaround, you can change the "Alert occurrence value to 3 or 5" so that you will get alert only when status is down for a longer period of time .

To update the alert occurrence:

1. Click **Targets** and select **GoldenGate**.
2. On the **OGG Home** page, select a target, for example a Replicat target.
3. Click the **Target** drop-down list, click **Monitoring**, and then select **Metric and Collection Settings**.

4. On the **Metric and Collection Settings** page, in the **Metric with Thresholds** table, click **Edit** (pencil icon) in the **Status** row to display the **Edit Advanced Settings: Status** page.
5. Set **Number of Occurrences** to 3.

Figure 11-1 Number of Occurrences

The screenshot shows the 'Edit Advanced Settings: Status' page for a metric. The 'Number of Occurrences' is set to 3. The 'Alert Message' is 'Target is DOWN.' and the 'Alert Message Properties' table is visible.

Name	Description
%metric_name%	Metric name for which the alert has been triggered
%column_name%	Metric column name for which the alert has been triggered
%warning_threshold%	Threshold for which warning violation has been triggered
%critical_threshold%	Threshold for which critical alert has been triggered
%severity%	Severity level of the alert or violation
%operator%	Comparison operation used to trigger the alert
%num_of_occurs%	Number of Occurrences after which alert has been triggered
%actual%	Current metric value on which alert has been triggered
%keyvalue%	Current metric value for a key on which alert has been triggered

11.6.2 False Alerts for Oracle GoldenGate Classic Targets

Ensure the following:

- Upgrade to Oracle GoldenGate Monitor Agent release 12.2.1.2.200131 is complete.
- Oracle GoldenGate Monitor Agent is up and running.
- The **OGG Home** page does not display a Warning icon and a tool tip in either of the conditions:
 - If either the Monitor agent or Web Service is down
 - If both the Monitor agent and the Web Service are down
- If the log suggests that the Oracle GoldenGate web service is going down intermittently, then you can choose to delay notification by completing the following settings: https://support.oracle.com/epmos/faces/DocumentDisplay?_adf.ctrl-state=&_afLoop=89915638796799&parent=DOCUMENT&sourceId=1368036.1&id=1540605.1&_afWindowMode=0&_adf.ctrl-state=xp4ykk3tu_4

11.6.3 False Alerts for Oracle GoldenGate Microservices Targets

Ensure the following:

- The Performance Metric server is up and running to ensure that no false alerts are issued for Administration service, Distribution service, Receiver service, and Extract and Replicat processes.
- Start the Service Manager. If the Service Manager is down and the Enterprise Manager agent is restarted, the status of the Administration, Performance Metric, Distribution, and Receiver services will be DOWN, until the Service Manager is UP.
- The out-of-box rule for metric collection error is disabled.
- A ruleset and rule are created in the Oracle Enterprise Manager as follows:

1. Ensure that the Ruleset applies only to the targets, such as group of GoldenGate targets or specific GoldenGate targets.
2. Create a new rule for event type **Metric Evaluation Error**.
3. Under **Actions**, select the delay equivalent to 30 minutes, and select **Only execute the actions if specified conditions match > Event has been open for specified duration** and enter a value for **Event has been open for**.

Figure 11-2 Create Rules and Rulesets

Add Actions
Add Conditional Actions

Define actions to be taken when an event matches this rule.

▲ **Conditions for actions**
 You can define the actions to apply whenever the rule matches or apply them conditionally.

Always execute the actions

Only execute the actions if specified conditions match

Event matches the following criteria

Event has been open for specified duration

Duration based condition is not supported for corrective action job status updates and causal analysis status update on events.

* **Event has been open for** 24 Hours

Associated incident is not acknowledged

Event is in particular severity for some time (select severity and time)

4. Setup compression as shown in the following screen shot. This will compress all collection error events from a target in an hour; events will be compressed only if they are open for more than 30 minutes (based on the delay setting in the screen shot).

Figure 11-3 Create or Update Incident

▲ **Create Incident or Update Incident**
 If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

Create Incident (if not associated with one) Update Incident

Each event creates a new incident

Compress events into an incident

Enable Global Compression Policy
 . Event compression will be automated based on global compression policies. To revert back to the custom compression logic, disable global compression policies for this rule

▲ **Events are compressed by**

Target