

Oracle® Enterprise Manager

Oracle GoldenGate System Monitoring Plug-In



(13.4.2.0.0)

F38486-06

May 2022

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, (13.4.2.0.0)

F38486-06

Copyright © 2018, 2022, 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 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" or "commercial computer software documentation" 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, and MySQL 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	vi
Documentation Accessibility	vi
Related Documents	vi
Conventions	vii

1 Overview

1.1 What is Oracle Enterprise Manager Plug-In for Oracle GoldenGate	1-1
1.2 Custom Screens	1-1

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 Server	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 Server	2-10
2.2.2.6 Receiver Server	2-11
2.3 Before You Begin with Enterprise Plug-In for Oracle GoldenGate	2-11

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	5-1
5.1.3	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance	5-3
5.2	Enterprise Manager CLI Verb-Based Discovery of Oracle GoldenGate Targets	5-3
5.2.1	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Classic Instance using EM CLI	5-4
5.2.2	Discovering an Oracle GoldenGate Enterprise Manager Plug-in Microservices Instance using EM CLI	5-5
6	Promote	
<hr/>		
6.2	Target Metrics Available on OGG Home Page	6-1
6.1	Promoting Oracle GoldenGate Targets	6-1
7	Configure	
<hr/>		
7.3	Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service	7-1
7.3.1	About Hybrid Cloud Monitoring	7-1
7.3.2	Installing the Monitor Agent on Cloud Device to Configure the Oracle GoldenGate Monitoring Agent	7-2
7.3.3	Creating an Inventory Location for Non Oracle Users	7-2
7.3.4	Configuring Oracle GoldenGate Monitoring Agent in the Provisioning Environment	7-3
7.3.5	Installing the Hybrid Cloud Gateway Agent	7-3
7.3.6	Configuring the EM Hybrid Cloud	7-4
7.3.7	Configuring the SOCKS Proxy Setup	7-4
7.1	Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager	7-5

7.2	Creating the Oracle Wallet	7-5
-----	----------------------------	-----

8 Manage

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	8-3
8.2	Manage Events, Alerts, and Incidents	8-5
8.2.1	Events	8-5
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
8.2.3	Alerts on Home Page	8-8
8.2.3.1	Indication of GoldenGate Monitor Agent and WebService being Down	8-8
8.2.4	Metric Data and Alerts	8-9

9 Monitor

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

10 Audit

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

11 Troubleshoot

11.1	Correcting ADFC Error on Windows 64-Bit Machines	11-1
11.2	Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files	11-1
11.3	Availability Error	11-2

Preface

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

- [Audience](#)
- [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*.
- Deploying the Enterprise Manager Plug-in in *Oracle GoldenGate System Monitoring Plug-In Installation and Upgrade Guide*.

- [Oracle Fusion Middleware 12c \(12.2.1.4.0\) Interoperability and Compatibility in Understanding Interoperability and Compatibility Guide.](#)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<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](#)
- [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 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 12.3 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 4 (13.4.x) and later.
- Oracle GoldenGate versions supported include:
 - Oracle GoldenGate Monitor Agent 12.2.1.2.190530 or later

- Oracle GoldenGate 12.3.x - 19.1.x
- Oracle GoldenGate Microservices 12.3.x – 19.1

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](#)
You can view detailed metrics of Extract, logs, and configuration of extract on an Extract page; and view detailed metrics of Replicat, logs, and configuration of Replicat on a Replicat page.
- [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

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

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

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 Server](#)
You can use the Administration Server page to manage Extract and Replicat processes and to monitor the metrics of these 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, and monitor historical trends.
- [Service Manager](#)
The **Service Manager** page lists all the Oracle GoldenGate Microservices Architecture deployments. From the Service Manager page, you can access Administration Server, Receiver Server, and Distribution Server targets. If you have multiple deployments, then you can also filter using the **Deployment** drop-down list.
- [Deployment](#)
Following are the details that you can view for each deployment.
- [Distribution Server](#)
The Distribution Server displays the distribution path, and the details of each path, such as status, time taken for data movement, source and target path details, and the database name.

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

2.2.2.1 Administration Server

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



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, 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>

Metric	Description
Delta Ignores	Valid for Extract Shows the number of data manipulation language (DML) operations that through an error were configured to be ignored since the last fetched value. Valid values: Positive integer
Delta Inserts	Valid for Extract and Replicat Shows the number of data manipulation language (DML) INSERT operations that were processed by the selected Oracle GoldenGate process since the last fetched value. Valid values: A positive integer
Delta Operation Per Second	Valid for Extract and Replicat Shows the number of operations (per second) that were processed by the selected Oracle GoldenGate process since the last fetched value. Valid values: A positive integer
Delta Operations	Valid for Extract and Replicat Shows the total number of Data Definition Language (DDL) and Data Manipulation Language (DML) INSERT, UPDATE, DELETE, AND TRUNCATE operations that were processed by the selected Oracle GoldenGate process since the last fetched value. Valid values: A positive integer
Delta Row Fetch Attempts	Valid for Extract Shows the number of row fetch attempts that were processed by the selected Oracle GoldenGate process since the last fetched value. Valid values: Positive integer
Delta Row Fetch Failures	Valid for Extract Shows the number of row fetch failures that were processed by the selected Oracle GoldenGate process since the last fetched value. Valid values: Positive integer
Delta Truncates	Valid for Extract and Replicat Shows the number of TRUNCATE operations that were processed by the selected Oracle GoldenGate process in its current run session since the last fetched value. Valid values: A positive integer
Delta Updates	Valid for Extract and Replicat Shows the number of UPDATE (including primary key updates) operations that were processed by the selected Oracle GoldenGate process in its current run session since the last fetched value. Valid values: A positive integer

Metric	Description
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>
	<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>
	<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>
Lag (sec)	<p>Valid for Extract and Replicat</p> <p>Shows the time difference between the Last Operation Timestamp and the Last Processed Timestamp. This attribute represents the true lag between the Oracle GoldenGate process and its data source. This lag value should match the value that is returned from the GGSCI command <code>SEND groupGETLAG</code>.</p> <p>Valid values: The lag time, in seconds</p>
Last Checkpoint Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when the last checkpoint was written by the process.</p> <p>Valid values: Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM.</p>
Last Operation Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when an operation (INSERT, UPDATE, DELETE) was committed in the data source, as recorded in the transaction log.</p> <p>Valid values: Datetime value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM</p>
Last Processed Timestamp	<p>Valid for Extract and Replicat</p> <p>Shows the time when a valid record was returned to the selected process. For Extract, this time value is assigned when the record is processed after the container transaction commits (not the time when the record is read from the transaction log). For a Data Pump or Replicat, this time value is returned immediately, because all transactions in the trail are known to be committed.</p> <p>Valid values: Date time value in the format of MM/DD/YYYY HH:MM:SS {AM PM}, for example: 01/14/2011 09:36:32 AM</p>

Metric	Description
Message	<p>Valid for Extract and Replicat</p> <p>The message includes the following information:</p> <ul style="list-style-type: none"> Message code number of an event message from the Oracle GoldenGate error log. Valid values: The numerical code of an Oracle GoldenGate event message in the event log, for example, OGG-00651. Message Date: Timestamp of an event message from the Oracle GoldenGate log. Valid values: A datetime value in the form of YYYY-MM-DD HH:MM:SS (in 24-hour clock format) Message Text: Text of an event message from the Oracle GoldenGate error log. Valid values: A text string from the message.
Name	<p>Valid for Extract and Replicat</p> <p>Name of the selected object. 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. 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. 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. 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. 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. From the Service Manager page, you can access Administration Server,

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

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

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

2.2.2.4 Deployment

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

Details	Description
Status	Status of target deployment. For example, running .
GoldenGate Home	The Oracle GoldenGate home that is created on a host computer is the directory that you choose to install the product. This read-only directory contains binary, executable, and library files for the product. The default directory path is: <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> .
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 Server

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

Path Details	Description
Distribution Server Path Name	Path Name of the Distribution Server
Status	Status of the Distribution Server. Valid values are: <ul style="list-style-type: none"> • Running • Stopped
Processing Lag	Time (number of seconds) taken to move the data from source to target.
Source	Complete path name of the Distribution server.
Target	Complete path name of the Receiver server.

Path Details	Description
DB Name	Name of the database from which the Extract target is fetching the data from.
Extract	Name of the Extract target (to which the data is fetched into) the Distribution server is connected to.

2.2.2.6 Receiver Server

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

Path Details	Description
Receiver Server Path Name	Path Name of the Receiver Server
Status	Status of the Receiver Server. Valid values are: <ul style="list-style-type: none"> Running Stopped
Processing Lag	Time (number of seconds) taken to move the data from source to target.
Source	Complete path name of the Distribution server.
Target	Complete path name of the Receiver server.
DB Name	Name of the database from which the Extract target is fetching the data from.
Extract	Name of the Extract target (to which the data is fetched into) the Receiver server is connected to.

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 Core 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).

 **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:

- 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`.

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). For example, `<agenthost>.us.oracle.com`. The Monitor agent is a secure tunnel way, and therefore, these agent details are required to connect the Enterprise Manager and Oracle GoldenGate.

 **Note:**

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

 **Note:**

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

- **Monitor Agent User Name:** Enter the Monitor agent user name. Enter the user credential that you have used while configuring the Monitor agent.
 - **Monitor Agent Password:** Enter the Monitor agent password.
 - **Monitor Agent Port:** Enter the port number of the agent host. For example, `5559`.
6. Click **OK** when finished in the **Edit Parameters** page.
 7. Click **OK** to go back to the **Setup Discovery** page.
 8. Select the target host, click **Discovered Targets**, and then click **Discover Now** to discover targets, and click **Yes** in the **Discover Now** confirmation dialog box.
 9. After the discovery is successful, click **Close** in the **Confirmation** dialog box.
 10. To view the discovery logs in case of an error occurrence, select the target, click **Diagnostic Details**, select **Oracle GoldenGate Classic**, and then click **Log from Agent**.

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

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 information required to connect to the Oracle GoldenGate agent:
 - **Service Manager Host Name:** Enter the host name of the machine on which the Service Manager Service is installed. For example: *adsvmgr.us.oracle.com*.
 - **Service Manager User Name:** Enter the User Name which you have entered while installing the service manager.
 - **Service Manager Password:** Enter the Service Manager Password.
 - **Service Manager Port:** Enter the port number of the host. For example, 8050.
6. Click **OK** when finished in the **Edit Parameters** page.
7. Click **OK** to go back to the **Setup Discovery** page.
8. Select the target host and then click **Discover Now** to discover targets, and click **Yes** in the **Discover Now** confirmation dialog box.
9. After the discovery is successful, click **Close** in the **Confirmation** dialog box.
10. To view the discovery logs in case of an error occurrence, select the target, click **Diagnostic Details**, select **Oracle GoldenGate Microservices**, and the click **Log from Agent**.

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

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](#)
The `discover_gg` Verb is used to discover Oracle GoldenGate Classic targets.

- [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.

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

The `discover_gg` Verb is used to discover Oracle GoldenGate Classic targets.

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, `oggmajmxusr`.
- **password** - Password to connect to Oracle GoldenGate Monitor Agent.
- **agentURL** - Enterprise Manager Agent URL. For example, `https://host00uaz.us.oracle.com:3872/emd/main/`.

-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
```

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.

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, `oggmasmusr`.
- **password** - Password to connect to Oracle GoldenGate Service Manager.
- **agentURL** - Enterprise Manager Agent URL. For example, `https://host00uaz.us.oracle.com:3872/emd/main/`.

-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]
```

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](#)

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

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](#)

7

Configure

- [Configuring Oracle GoldenGate Instances for Enabling Monitoring in the Oracle Enterprise Manager](#)
- [Creating the Oracle Wallet](#)
- [Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service](#)
This section discusses using the Enterprise manager Cloud Control console to administer both your Oracle cloud and on-premises deployments.

7.3 Enabling Hybrid Cloud Monitoring on Oracle GoldenGate Cloud Service

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

- [About Hybrid Cloud Monitoring](#)
You can use the Enterprise Manager Cloud Control console to administer both your on-premises and Oracle Cloud deployments.
- [Installing the Monitor Agent on Cloud Device to Configure the Oracle GoldenGate Monitoring Agent](#)
- [Creating an Inventory Location for Non Oracle Users](#)
You must create a new inventory location for non Oracle users as they do not have direct access to Oracle GoldenGate Cloud Service POD machines through Oracle user. Without this access they're unable to push the Hybrid cloud agent from the Enterprise Cloud interface.
- [Configuring Oracle GoldenGate Monitoring Agent in the Provisioning Environment](#)
You must configure the Oracle GoldenGate Monitoring Agent to work in the provisioning environment.
- [Installing the Hybrid Cloud Gateway Agent](#)
- [Configuring the EM Hybrid Cloud](#)
- [Configuring the SOCKS Proxy Setup](#)

7.3.1 About Hybrid Cloud Monitoring

You can use the Enterprise Manager Cloud Control console to administer both your on-premises and Oracle Cloud deployments.

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

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

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

1. Provide the latest release file, which is `fmw_12.2.1.4.0_ogg_generic.jar`.
2. Copy the file into the cloud device.
3. Select **Monitor agent only** and provide the location for installation.

 **Note:**

You must have permission to install in the mentioned location.

4. Once the installation is complete, go to `MON_AGENT_INST_LOC/oggmon/ogg_agent` directory.
5. Run the `createMonitorAgentInstance.sh`. Provide the Oracle GoldenGate core location, for example `/u01/app/oracle/gghome` when asked.
Provide a new location `/u02/data/Agent_Inst` to create an agent instance for the monitor.
6. Go to the `AGENT_INST_LOC/bin` directory.
7. Run `pw_agent_util.sh -jagentonly`.
 - Create a password for Java Agent:
 - Confirm password for Java Agent:
8. Go to the `AGENT_INST_LOC/cfg` directory.
9. Modify the `Config.properties` file and change **agent.type = OEM** and save the file.

7.3.3 Creating an Inventory Location for Non Oracle Users

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

To create a new inventory location for the `opc` user:

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

Example: `/u02/data/opcuser/oraInventory` directory.

4. Run the create inventory script `./createCentralInventory1479193434142.sh inventory_location group_name`.

Example: `./createCentralInventory1479193434142.sh /u02/data/opcuser/oraInventory opc.`

5. Change the permission of inventory folder from root to opc using the `chown` command.

Example: `chown opc /u02/data/opcuser/oraInventory.`

6. Use `Ctrl+D` to come out from root user and change to opc user.
7. Create an `emagent` folder as opc user to push the Hybrid cloud agent.
8. Push the Hybrid cloud agent from Enterprise Manager interface.

The location of `createCentralInventory.sh` will be provided separately.

7.3.4 Configuring Oracle GoldenGate Monitoring Agent in the Provisioning Environment

You must configure the Oracle GoldenGate Monitoring Agent to work in the provisioning environment.

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

Note:

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

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

7.3.5 Installing the Hybrid Cloud Gateway Agent

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

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

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

7.3.6 Configuring the EM Hybrid Cloud

You must configure the Hybrid Cloud agent.

1. In the Enterprise Manager Plug-in for Oracle GoldenGate UI, select **Setup, Add Target, Add Target Manually, Install Agent on Host**.
2. Add the `Host Target`. Enter the host name and platform. Click **Next**.
3. Add the `Installation base directory`. It is the same location as in host provided in step 2.
It's the same location as you provided in the previous step for the host .
4. Add the `Named Credential` to the host as provided in step 2.
You must have privilege to the location provided in the previous step.
5. Don't provide the `port` value. The system allocates a free port. Click **Next**.
6. Click **Deploy Agent**.
7. Provide the details about the known error, which appears.

7.3.7 Configuring the SOCKS Proxy Setup

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

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

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

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

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

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

7.1 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`

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

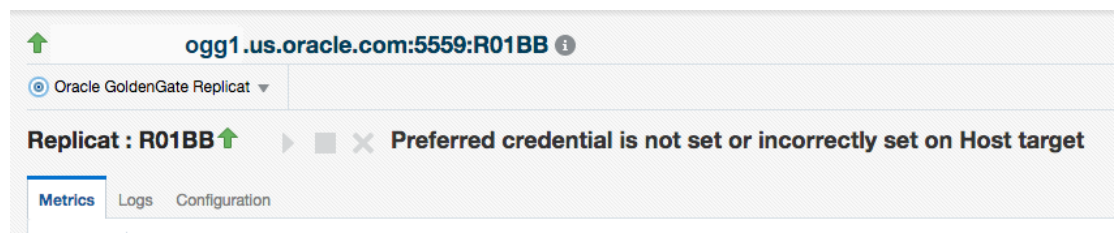
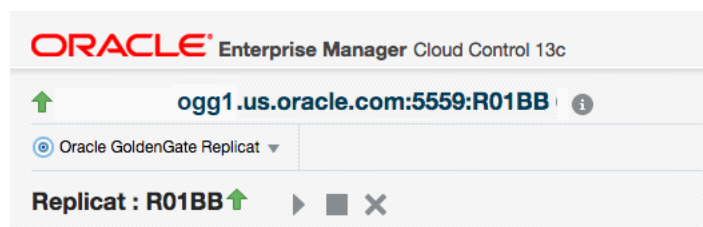


Figure 8-2 Action Buttons are active



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](#)
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](#)
The monitoring credentials are hierarchical in nature. For example, if credentials are provided for Oracle GoldenGate Service Manager target type, then by default, they are applicable to its child target types as well, such as Oracle GoldenGate Administration/Distribution/Receiver Server.

8.1.1.1 Preferred Credentials

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

The monitoring credentials are hierarchical in nature. For example, if credentials are provided for Oracle GoldenGate Service Manager target type, then by default, they are applicable to its child target types as well, such as Oracle GoldenGate Administration/Distribution/Receiver Server.

For monitoring credential, use the same credential that can access Service Manager on Oracle GoldenGate microservices instances.

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.
- [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.

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

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.

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

- [Setting Metric Alerts and Incidents for Extract and Replicat](#)
- [Setting Incidents and Alerts for Oracle GoldenGate Target Availability](#)
- [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 Oracle GoldenGate targets to get notified when there are any issues with these targets.

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 Oracle GoldenGate targets to get notified when there are any issues with these targets.

This includes occurrences when the Enterprise Manager is unable to retrieve status of Oracle GoldenGate targets, or is unable to communicate with the Oracle GoldenGate Monitor Agent in case of Oracle GoldenGate classic targets.

To set incidents and alerts for target availability:

1. On the Home page, click **Setup**, select **Incidents**, and then click **Incident Rule** to display the **Incident Rules - All Enterprise Rules** page.
2. Click **Create Rule Set...**
3. Enter a **Name**, for example **Incident management rule set for Target Availability** and click **Save**.
4. In the **Target** area, select **All Targets of types**, and select the target type from the adjacent drop-down.
5. In the **Rules** area, click **Create...** to display the **Select Type of Rule to Create** dialog box.
6. Select **Incoming events and updates to events** and click **Continue** to display the **Create New Rule: Select Events** page.

7. Select **Target Availability** from the **Type** drop-down list and click **Next** to display the **Create New Rule: Add Actions** page.
8. Click **Add** to display the **Add Conditional Actions** page, select **Always execute the actions**.
9. Under **Send Notifications**, expand **Basic Notifications**, and enter email IDs in **E-mail To** and **E-mail Cc** to assign 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*.

8.2.3 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 and Alerts

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

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

- Checkpoint Position
- Name
- Status
- Start Time
- End of File
- Lag (Sec)
- Total Inserts
- Delta Inserts
- Total Deletes
- Delta Deletes
- Total Truncates
- Delta Truncates
- Total Operations
- Delta Operations
- Delta Operation Per seconds
- Total Executed DDLs
- Delta Executed DDLs
- Total Discards
- Delta Discards
- Total Ignores
- Delta Ignores
- Last OGG Checkpoint Timestamp
- Last Processed Timestamp
- Delta Row Fetch Attempts
- Delta Row Fetch Failures
- Total Row Fetch Failures

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

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 **GG Error Log**.
- [Configuration Tab](#)

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

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.
(Optional) Enter the result of the step here.
2. Select either the Extract or Replicat Process.

3. Click one of the following: **Start**, **Stop**, or **Kill**.
- [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 **GG Error Log**.

- **Report:** The **Report** tab contains a list of reports generated for the selected target type. The files have an extension of `.rpt`. These report files contain details of the targets, such as target directories, database versions, parameters they run on, and recovery parameters.
- **Discards:** If there are any discard files specified in the parameter files and the file exists in Oracle GoldenGate Core, then these files are also displayed in the **Discards** tab as a list of Discard Files. You can specify the names of the folder, files, or file extensions of your choice. The default discard files are read from the `dirrpt` folder, for example, `dirrpt/processName*.dsc`. Note that the file name is an absolute path of the discard file or path related to the `OGGCORE` location and file extension can be any of the following: `.txt`, `.discard`, or `.dsc`. You can specify multiple discard files as follows:

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

- **GG S Error Log:** The **GG SERR log** tab shows the file contents of the `ggserr.log` file.

9.5 Configuration Tab

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

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

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

Note:

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

3. Click **Save** after you have made the 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.

9.6 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*.

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 10:26:22	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...	71F72A814481771C

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

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

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

11.1 Correcting ADFC Error on Windows 64-Bit Machines

Selecting a target from the Oracle GoldenGate Enterprise Manager Plug-In home page may cause an ADFC exception on Windows 64-bit machines. To correct this issue, execute following command:

```
emctl load policies -plugin_id "oracle.fmw.gg" -policies_file  
"middleware_home/plugins/goldengate_plugin_home  
/metadata/security/jaznpolicy/jazn-data.xml"
```



Note:

`middleware_home` is where you installed Oracle Fusion Middleware products.

11.2 Locating Oracle GoldenGate Enterprise Manager Plug-in Log Files

Following are the Oracle GoldenGate Enterprise Manager Plug-in log files (assuming that `ORACLE_HOME` is set to `/home/oracle/`) that can help you with troubleshooting the Oracle GoldenGate Enterprise Manager Plug-In.

Discovery related error details log file: `ogg_so_logs.log.0`

This file is in the `$AGENT_STATE_DIR/sysman/emd/` directory.

The `ogg_so_log` file contains discovery related errors, details about execute commands, and report/discard/config file operations. If there are any errors while the Oracle GoldenGate Enterprise Manager Plug-in Agent connects with iAgent, the information is logged in this file. For example:

```
/home/oracle/oem/agent/agent_inst/sysman/emd/ogg_so_1 ogs.log.0
```

EM Agent error details log file: `emagent.log`

This file is in the `$AGENT_STATE_DIR/sysman/log/` directory. For example:

```
/home/oracle/oem/agent/agent_inst/sysman/log/gcagent.log
```

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

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

Oracle Management Services log file: EMGC_OMS1.out

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

11.3 Availability Error

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

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

- whether the Enterprise Manager agent is up and running.
- If the agent is running, then you need to reset the credentials. To change the credentials:
 1. Change the username.
 2. Save the new username details.
 3. Use the same username and password.