Oracle® Fusion Middleware

Using Oracle GoldenGate Microservices Architecture

19c (19.1.0)
E98070-02
December 2019

Oracle Fusion Middleware Using Oracle GoldenGate Microservices Architecture, 19c (19.1.0)

E98070-02

Primary Author: Oracle Corporation

Contents

Preface

Audience vi
Documentation Accessibility vi
Related Information vi
Conventions vii

1 Preparing for Oracle GoldenGate Microservices

1.1 Preparing the Database 1-1
Prerequisites for Database Sharding 1-2
1.2 Setting Environment Variables 1-3
1.3 Data Replication Task Roadmap 1-4

2 Setting Up Secure or Non-Secure Deployments

2.1 How to Add Secure or Non-Secure Deployments 2-1
2.2 How to Add Users 2-7

3 Working with Deployments

3.1 How to Connect to a Service Manager 3-1
3.1.1 How to Start and Stop the Service Manager 3-3
3.1.2 Quick Tour of the Service Manager 3-3
3.1.3 How to Interpret the Log Information 3-4
3.1.4 How to Enable and Use Debug Logging 3-4
3.2 How to Start and Stop Deployments and Servers 3-5
3.3 How to Remove a Deployment 3-6
3.3.1 How to Remove a Deployment: GUI 3-6
3.3.2 How to Remove a Deployment: Silent Mode 3-7
3.4 View and Edit Services Configuration 3-7

4 Working with Data Replication

4.1 Quick Tour of the Administration Server Home Page 4-2
4.2 How to Add a Database Credential 4-3
4.3 Before Creating an Extract 4-3
4.4 How to Add Extracts 4-4
4.4.1 Using Extract Actions 4-6
4.5 Before Creating Replicat 4-7
4.6 How to Add a Replicat 4-7
4.6.1 Creating a Parallel Replicat 4-8
4.6.1.1 Basic Parameters for Parallel Replicat 4-10
4.6.2 Using Replicat Actions 4-11
4.7 How to Use the Master Keys and Encryption Keys 4-12
4.8 How to Access the Parameter Files 4-12
4.9 Setting Up Automated Tasks 4-13
4.10 Review Critical Events 4-14
4.11 How to Configure Managed Processes 4-15
4.12 How to Access Extract and Replicat Log Information 4-16
4.13 How to Create Users from the Administration Server 4-17

5 Working with Paths

5.1 Quick Tour of the Distribution Server Home Page 5-1
5.2 How to Add a Distribution Path 5-2
5.3 How to Add a Target-Initiated Distribution Path 5-6
5.4 Using the Path Actions 5-11
5.5 Repositioning a Path 5-12
5.6 Changing Path Filtering 5-12
5.7 Reviewing the Distribution Server Path Information 5-14

6 Working with Trails

6.1 Quick Tour of the Receiver Server Home Page 6-1
6.2 Tuning Network Parameters 6-1
6.3 Reviewing the Receiver Server Path Information 6-2
6.4 Monitoring Paths 6-2

7 Monitoring Performance

7.1 Quick Tour of the Performance Metrics Server Home Page 7-1
7.2 Monitoring Server Performance 7-2
7.3 Reviewing Messages 7-3

7.4 Review Status Changes 7-3
7.5 How to Purge the Datastore 7-4

8 Working with Oracle GoldenGate Sharding

8.1 Oracle GoldenGate With a Sharded Database 8-1
8.2 How to Configure Sharding in Oracle GoldenGate 8-2

A How to Use the Admin Client

B Connecting Microservices Architecture to Classic Architecture

C Connecting Oracle GoldenGate Classic Architecture to Microservices Architecture

Preface

The *Using the Oracle GoldenGate Microservices Architecture* guide describes how to use the web interface and REST commands available with Microservices Architecture (MA) to perform data replications tasks.

- Audience
- Documentation Accessibility
- Related Information
- Conventions

Audience

This guide is intended for administrators and users who are familiar with Oracle GoldenGate concepts and architecture and who are interested in learning to use the microservices and REST commands for performing various Oracle GoldenGate data replication tasks.

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 Information

The Oracle GoldenGate Product Documentation Libraries are found at

https://docs.oracle.com/en/middleware/goldengate/index.html

Additional Oracle GoldenGate information, including best practices, articles, and solutions, is found at:

Oracle GoldenGate A-Team Chronicles

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, such as "From the File menu, select **Save**." Boldface also is used for terms defined in text or in the glossary.
italic *`italic`*	Italic type indicates placeholder variables for which you supply particular values, such as in the parameter statement: `TABLE` *`table_name`*. Italic type also is used for book titles and emphasis.
`monospace` `MONOSPACE`	Monospace type indicates code components such as user exits and scripts; the names of files and database objects; URL paths; and input and output text that appears on the screen. Uppercase monospace type is generally used to represent the names of Oracle GoldenGate parameters, commands, and user-configurable functions, as well as SQL commands and keywords.
UPPERCASE	Uppercase in the regular text font indicates the name of a utility unless the name is intended to be a specific case.
{ }	Braces within syntax enclose a set of options that are separated by pipe symbols, one of which must be selected, for example: {*`option1`* | *`option2`* | *`option3`*}.
[ ]	Brackets within syntax indicate an optional element. For example in this syntax, the `SAVE` clause is optional: `CLEANUP REPLICAT` *`group_name`* `[, SAVE` *`count`*`]`. Multiple options within an optional element are separated by a pipe symbol, for example: `[`*`option1`* `|` *`option2`*`]`.

1

Preparing for Oracle GoldenGate Microservices

Learn about the preliminary tasks to perform for setting and using Oracle GoldenGate Microservices.

Topics:

- Preparing the Database
  Configure the Oracle Database for Oracle GoldenGatereplication.
- Setting Environment Variables
  You can set the Microservices-specific environment variables while performing the deployment tasks:
- Data Replication Task Roadmap
  There are a number of tasks you must perform to set up data replication.

1.1 Preparing the Database

Configure the Oracle Database for Oracle GoldenGatereplication.

Before starting any Oracle GoldenGate services or processes, ensure that the Oracle Database is configured correctly and started. To start the database, perform the following tasks:

1. On the Linux platform, enter:

```
sqlplus / as sysdba

SQL*Plus: Release 12.2.0.1.0 Production on Thu Jan 5 16:38:53 2018

Copyright (c) 1982, 2018, Oracle.  All rights reserved.

Connected to an idle instance.

SQL> startup
ORACLE instance started.

Total System Global Area 1560281088 bytes
Fixed Size             2924784 bytes
Variable Size           503320336 bytes
Database Buffers     1040187392 bytes
Redo Buffers           13848576 bytes
Database mounted.
Database opened.
SQL> ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;

Database altered.
```

```
SQL> ALTER DATABASE FORCE LOGGING;

Database altered.

SQL> shutdown immediate
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup mount
ORACLE instance started.

Total System Global Area 1560281088 bytes
Fixed Size            2924784 bytes
Variable Size          503320336 bytes
Database Buffers     1040187392 bytes
Redo Buffers           13848576 bytes
Database mounted.
SQL> alter database archivelog;

Database altered.

SQL> alter database open;

Database altered.

SQL> alter system set enable_goldengate_replication=true;

System altered.
```

> **Note:**
>
> If you use the Integrated Extract and/or Integrated Replicat features, it is advised to set the `streams_pool_size` parameter.

2. Exit the SQL prompt once you create the users.

Prerequisites for Database Sharding

If you want to use database sharding with Oracle GoldenGate, you must follow these steps:

1. Set the `STREAMS_POOL_SIZE` to at least 1200 MB.
2. Load Oracle GoldenGate sharding PL/SQL packages prior to deploying, which in turn adds the `ggadmin` schema.
3. Install a client wallet for database to communicate through the PL/SQL `utl_http` routines with Oracle GoldenGate service endponits.

1.2 Setting Environment Variables

You can set the Microservices-specific environment variables while performing the deployment tasks:

- Oracle GoldenGate Configuration Assistant (OGGCA)
- SSL/TLS Security (Optional)

The following environment variables are set for the Oracle GoldenGate Configuration Assistant, `oggca.sh`:

`ORACLE_HOME`

```
export ORACLE_HOME=database_install_location
```

`OGG_HOME`

```
export OGG_HOME=ogg_install_location
```

`LD_LIBRARY_PATH`

```
export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH
```

`TNS_ADMIN`

```
export TNS_ADMIN=$ORACLE_HOME/network/admin
```

`PATH`

```
export PATH=$OGG_HOME/bin:$PATH
```

`Oracle_SID`
Oracle Database SID

An additional environment variable is required to set up a secure deployment:

`JAVA_HOME`

```
export JAVA_HOME=$OGG_HOME/jdk
```

See Components of Oracle GoldenGate Microservices Architecture.

For different platforms the library path variable is different. Following list provides the variable name for different platforms:

- Linux: `LD_LIBRARY_PATH`
- IBM i and AIX: `LIBPATH`
- Solaris: `SHLIB_PATH`
- Windows: `PATH`

Note:

For using any command line utility, you must set up the `OGG_HOME`, `OGG_VAR_HOME`, and `OGG_ETC_HOME` variables correctly in the environment.

1.3 Data Replication Task Roadmap

There are a number of tasks you must perform to set up data replication.

The phases to build the distribution path are listed in the following table.

Task	Description
Run the Oracle GoldenGate Configuration Assistant (oggca) to create and configure secure and non-secure deployments	See Setting Up Secure and Non-Secure Deployment
Login to Service Manager	When you log in to Service Manager, you can see the status of other servers (Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server). See How to Connect to Service Manager
Add Credential Store	Set up the user id and password to connect to the database before you create an Extract. See How to Add Database Credentials. You can also set up your domain alias while setting up the Credentials configuration.
Add Extracts	How to Add Extracts
Register the Extract	You need to register an Extract when creating an Integrated Extract. See How to Add Extracts.
Add Distribution Path	See How to Add a Distribution Path
Add Replicats	See How to Add Replicats
Start the Extract	See How to Add an Extract
Start the Distribution Path	See How to Add a Distribution Path
Start the Replicat	See How to Add a Replicat
Check the Receiver Server for path details	See Monitoring Paths
Monitor Extracts and Replicats	See Monitoring Paths and Tuning Network Parameters and Monitoring Server Performance
Monitor the Performance Metrics	See Monitoring Performance

2 Setting Up Secure or Non-Secure Deployments

You can choose to set up a secure or non-secure deployment. A secure deployment involves making RESTful API calls and conveying trail data between the Distribution Server and Receiver Server, over SSL/TLS. You can use your existing wallets and certificates, or you can create new ones.

When first creating the SSL/TLS security certificates, you must ensure that the SSL/TLS security environment variables are set as described in Setting Environment Variables.

For a non-secure deployment, the RESTful API calls occur over plain-text HTTP and conveyance between Distribution Server and Receiver Server is performed using the UDT, ogg://, and ws:// protocols.

This section describes the steps to configure a non-secure deployment and prerequisites and tasks to configure a secure deployment.

Topics:

- How to Add Secure or Non-Secure Deployments
  Adding deployments is the first task in the process of setting up a data extraction and replication platform. Deployments are managed from the Service Manager.
- How to Add Users
  Each deployment has its own list of users, and when you add users, you add them to that deployment.

2.1 How to Add Secure or Non-Secure Deployments

Adding deployments is the first task in the process of setting up a data extraction and replication platform. Deployments are managed from the Service Manager.

After completing the Oracle GoldenGate Microservices installation, you can add an initial and subsequent deployments using the Configuration Assistant (OGGCA) wizard.

> **Note:**
>
> Oracle recommends that you have a single Service Manager per host, to avoid redundant upgrade and maintenance tasks with Oracle GoldenGate releases.

You can use the Configuration Assistant wizard to add multiple deployments to a Service Manager, which enables you to upgrade the same Service Manager with new releases or patches. The source and target deployments serve as endpoints for setting up the distribution path for data replication. A target deployment is added the same way as the source deployment but for a different database user or a different database.

1. From the `OGG_HOME` directory, run the `$OGG_HOME/bin/oggca.sh` program on UNIX or Linux.

   The Oracle GoldenGate Configuration Assistant (oggca) is started. Run this program, each time you want to add a deployment.

2. In the **Select Service Manager Options** step:

   a. Select whether you want to use an existing Service Manager or a new one. Only one Service Manager per host is supported.

   b. Enter or browse to the directory that you want to use for your deployment. Oracle recommends that you do *not* use your Oracle GoldenGate installation directory.

   c. Enter the hostname or IP Address of the server.

   d. Enter a unique port number that you want to contact your Service Manager on or use the default, which is used in the URL to connect to it. Ensure that the port is unreserved and unrestricted. Each service must use a different port number.

   e. (Optional) You can register the Service Manager to run as a service so as to avoid manually starting and stopping it.

      You can choose to run *one* Service Manager as a service (daemon). If there is an existing Service Manager registered as a service and you select a new Service Manager to register as a service, an alert is displayed indicating that you cannot register the new one as a service. All other Service Managers are started and stopped using scripts installed in the `bin` directory of the deployment. You cannot register an existing Service Manager as a service.

   f. (Optional) You can choose to integrate your deployment with an Oracle Grid Infrastructure for Oracle Database by selecting the option “Integrate with XAG”. This option cannot be used when running your Service Manager as a service.

3. In the **Configuration Options** step, you can add or remove deployments.

   Select the appropriate option.

4. In the **Deployment Details** step:

   a. Enter the deployment name using these conventions:

      - Must begin with a letter.
      - Can be a standard ASCII alphanumeric string not exceeding 32 characters.
      - Cannot include extended ASCII characters.
      - Special characters that are allowed include underscore (‘_’), hyphen (‘/’), dash (‘-’), period (‘.’).
      - Cannot be “ServiceManager”.

   b. Select **Enable Sharding** to use the database sharding feature in your deployment. The schema must be `ggadmin`.

   c. Enter or select the Oracle GoldenGate installation (home) directory. If you have set the `$OGG_HOME` environment variable, the directory is automatically populated. Otherwise, the parent directory of the `oggca.sh` script is used.
   d. Click **Next**.

5. On the **Select Deployment Directories** page:
   a. Enter or select a deployment directory where you want to store the deployment registry and configuration files. When you enter the deployment directory name, it is created if it doesn’t exist. Oracle recommends that you do *not* locate your deployment directory inside your `$OGG_HOME` and that you a separate directory for easier upgrades. The additional fields are automatically populated based on the specified deployment directory.
   b. You can customize the deployment directories so that they are named and located differently from the default.
   c. Enter or select different directories for the various deployment elements.
   d. Click **Next**.

6. On the **Environment Variables** page:

   Enter the requested values for the environment variables. Double-click in the field to edit it. You can copy and paste values in the environment variable fields. Make sure that you tab or click outside of the field after entering each value, otherwise it’s not saved. If you have set any of these environment variables, the directory is automatically populated.

   OGG_HOME
   The directory where you installed Oracle GoldenGate.

   ORACLE_HOME
   The directory where your Oracle database or Oracle client software is installed.

   LD_LIBRARY_PATH
   The library directories in your `$OGG_HOME`, OUI, database installation, and database network. The default is `$OGG_HOME/lib`.

   TNS_ADMIN
   The directory that contains the Oracle Net Services configuration. The default is `$ORACLE_HOME/network/admin`.

   ORACLE_SID
   The Oracle system identifier (SID) is a unique identifier that is used to distinguish this instance from other Oracle Database instances that you may create later and run concurrently on your system.

   STREAMS_POOL_SIZE
   This appears only if you enable sharding, are using Integrated Extract or Integrated Replicat. Use the default or set your pool size value that is at least 1200MB.

   You can add additional environment variables to customize your deployment or remove variables. For instance, you can enter the following variable to default to another international charset: `ENV_LC_ALL=zh_CN.UTF-8`

   Click **Next**.

7. On the **Administrator Account** page:

   a. Enter a user name and password that you want to use to sign in to the Oracle GoldenGate Microservices Service Manager and the other servers. This user is the security user for this deployment. For details on the different types of users, see How to Add Users. If you are using an existing Service Manager, you must enter the same log in credentials that were used when adding the first deployment.

   b. Select the check box that allows you to enable a strong password policy for your new deployment. If you select this option, then the password must adhere to restrictions, otherwise an error occurs, which requires you to specify a stronger password.

   c. Click **Next**.

8. On the **Security Options** page:

   a. You can choose whether or not you want to secure your deployment. Oracle recommends that you enable SSL/TLS security. If you do not want to use security for your deployment, deselect the check box. This operation exposes the option **This non-secure deployment will be used to send trail data to a secure deployment**. Select this check box if the non-secure target deployment is meant to communicate with a secure source deployment.

      However, you must enable security if configuring for Oracle GoldenGate sharding support.

   b. The option **This deployment will be used for target-initiated distribution paths** allows the Receiver Server to create a target initiated path for environments such as DMZ or Cloud to on-premise, where the Distribution Server in the source Oracle GoldenGate deployment cannot open network connections in the target environment to the Receiver Server due to network security policies.

      To know conceptual details, see: Overview of Target-Initiated Paths.

   c. (Optional) You can specify a client wallet location so that you can send trail data to a secure deployment. This option is useful when Distribution Server from the source deployment is unsecured whereas the Receiver Server on the target deployment is secured. In this case, the sender may be configured for public access whereas the Receiver Server requires authentication and authorization, which is established using PKI before the incoming data is applied. For more information, see Creating a Self-Signed Root Certificate

      and Creating a Distribution Server User Certificate in the *Securing the Oracle GoldenGate Environment*.

   d. For your Server, select one of the options, and then provide the required file locations. When using an existing wallet, it must have the appropriate certificates already imported into it. If you choose to use a certificate, enter the corresponding pass phrase. When using a self-signed certificate, a new Oracle Wallet is created in the new deployment and these certificates are imported into it. For certificates, enter the location of the private key file and the pass phrase.

   e. For your Client, select one of the options, and then provide the required information as you did for your server.

   f. Click **Next**.

9. (If Security is enabled) On the **Advanced Security Settings** page, the TLS 1.1 and TLS 1.2 options are available. TLS 1.2 is selected by default.

   When you open the Advanced Security Settings for the first time with TLS 1.2, the following cipher suites are listed:

   ```
   TLS_RSA_WITH_AES_128_CBC_SHA256
   TLS_RSA_WITH_AES_128_GCM_SHA256
   TLS_RSA_WITH_AES_256_CBC_SHA256
   TLS_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
   TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
   TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
   TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
   TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
   TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
   TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
   TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
   TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
   TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
   TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
   TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
   TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
   TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
   TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
   ```

   a. Use the arrows to add or remove cipher suites.

   b. Use **Up** and **Down** to reorder how the cipher suites are applied

   c. Click **Next**.

   > **Note:**
   >
   > For more information on TCP/IP encryption options with `RMTHOST`, see `RMTHOST` in *Reference for Oracle GoldenGate*

10. (If Sharding is enabled) On the **Sharding Options** page:

    a. Locate and import your Oracle GoldenGate Sharding Certificate. Enter the distinguished name from the certificate that will be used by the database sharding code to identify itself when making REST API calls to the Oracle GoldenGate MA services.

    b. Enter a unique name for the certificate.

    c. Click **Next**.

11. On the **Port Settings** page:

a. Enter the Administration Server port number, and then when you leave the field the other port numbers are populated in ascending numbers. Optionally, you can enter unique ports for each of the servers.

b. Select **Enable Monitoring** to use the Performance Metrics Server.

c. Click inside the Performance Metrics Server port fields to populate or enter the ports you want to use.

> **Note:**
>
> Ensure that you choose available ports for TCP and UDP for performance monitoring. After the deployment is done, you can change the TCP port from the Service Manager console. For more information on `PMSRVR`, see `ENABLEMONITORING`

d. Select the type of datastore that you want the Performance Metrics Server to use, the default Berkeley Database (BDB) data store or Open LDAP Lightning Memory-Mapped Database (LMDB). You can also designate the Performance Monitor as a Critical Service.

   For BDB informtion, see Oracle Berkeley DB 12*c* Release 1 For LMDB information, see http://www.lmdb.tech/doc/.

e. Select the location of your datastore. BDB and LMDB are in-memory and disk-resident databases. The Performance Metrics server uses the datastore to store all performance metrics information.

f. Click **Next**.

> **Note:**
>
> The `oggca` utility does not validate whether or not the port you entered is currently in use or not, so you must manually ensure that the ports are free and will not be reassigned to other processes.

12. In the **Replication Settings** step:

    a. Enter the Oracle GoldenGate default schema you want to use to perform the replication settings. For example, ggadmin.

    b. Click **Next**.

13. On the **Summary** page:

    a. Review the detailed configuration settings of the deployment before you continue.

    b. (Optional) You can save the configuration information to a response file. You can run the installer from the command line using this file as an input to duplicate the results of a successful configuration on other systems. You can edit this file or a new one from the provided template.

> **Note:**
>
> When saving to a response file, the administrator password is not saved for security reasons. You must edit the response file and enter the password if you want to reuse the response file for use on other systems.

c. Click **Finish** to the deployment.

d. Click **Next**.

14. On the **Configure Deployment** page:

    Displays the progress of the deployment creation and configuration.

    a. If the Service Manager is being registered as a service, a pop-up appears that directs you how to run the script to register the service. The Configuration Assistant verifies that these scripts have been run. If you did not run them, you are queried if you want to continue. When you click **Yes**, the configuration completes successfully. When you click **No**, a temporary failed status is set and you click **Retry** to run the scripts.

       Click **Ok** after you run the script to continue.

    b. Click **Next**.

15. On the **Finish** page:

    Click **Close** to close the Configuration Assistant.

2.2 How to Add Users

Each deployment has its own list of users, and when you add users, you add them to that deployment.

You can create users from the Service Manager or the Administration Server. See How to Create Users from the Administration Server for steps to create users from the Administration Server.

The only user that can manage the services in Service Manager is the user that was originally added as the security user when you initially add the deployment to the Service Manager. The other users are specific to the MA deployment and the security user needs to create users to every MA deployment individually.

You can create users for that deployment by performing the following steps:

1. Log in to either the Service Manager or the Administration Server.
2. From the left navigation pane, select Administrator.
3. Click Users (+). The maximum length of the characters for users created from the Microservices web interface and the REST API is 512 characters. In RESTAPI, there are no pattern restrictions for the user name for both Basic and Certificate type users. However, when you use the Microservices web interface, certain restrictions apply for creating a Basic type user:

   - The user name must start with an alphabetic character and contain only alphanumeric characters.

- Symbols that can be used are: at sign (@), period (.) , dash(-), comma(,), underscore(_), number sign(#), dollar sign($), plus sign (+), backslash (\), slash (/), equal sign (=), less than sign (<), or greater than sign(>)

4. Enter a unique user name.
5. Select one of these roles:

Role ID	Privilege Level
User	Allows information-only service requests, which do not alter or effect the operation of either the Microservices. Examples of Query/Read-Only information include performance metric information and resource status and monitoring information.
Operator	Allows users to perform only operational actions, such as creating, starting and stopping resources. Operators cannot alter the operational parameters or profiles of the Microservices server.
Administrator	Grants full access to the user, including the ability to alter general, non-security related operational parameters and profiles of the server.
Security	Grants administration of security related objects and invoke security related service requests. This role has full privileges.

6. Enter information that describes the user.
7. Select the type of user as Basic or Certificate from the Type list box.
8. Enter the password twice to verify it. There is a default password verifier that requires a minimum length and pattern for the password.
9. Click **Submit**.

   The user is registered

Users cannot be changed. You must delete a user, and then add it again.

3 Working with Deployments

Once you log into your Service Manager instance, you can create deployments or edit existing ones. You can work with multiple deployments from a single Service Manager instance.

After you have completed the Oracle GoldenGate Microservices installation, you need to create a deployment (secure or non-secure) using the Oracle GoldenGate Configuration Assistant (OGGCA). You can use this wizard to add multiple deployments to one Service Manager.

Oracle recommends the usage of a secure configuration within Oracle GoldenGate Microservices. There are two options for setting up a secure Microservices deployment:

- Run Microservices on loopback address and front it with an HTTPS reverse proxy (nginx). See Reverse Proxy Support.
  - Interoperability between Oracle GoldenGate Classic andOracle GoldenGate Microservices is configured through the `ogg` protocol using data pump Extract from Oracle GoldenGate Classic with `SOCKSPROXY`.
- Run Oracle GoldenGate Microservices with TLS version 1.2 enabled on all services.

Topics:

- How to Connect to a Service Manager
  The Service Manager is the primary watchdog service within Oracle GoldenGate Microservices that enables controlling the deployments and associated services running on the host machine.
- How to Start and Stop Deployments and Servers
  The Service Manager is the central hub from where you can start and stop deployments, Administration Server, Distribution Server, Performance Metrics Server, Receiver Server.
- How to Remove a Deployment
  You can remove a deployment using OGGCA or in silent mode.
- View and Edit Services Configuration
  The services configuration and restart options for Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server can be viewed and edited from the Services Manager.

3.1 How to Connect to a Service Manager

The Service Manager is the primary watchdog service within Oracle GoldenGate Microservices that enables controlling the deployments and associated services running on the host machine.

The ServiceManager can be configured in three different modes:

- Manually

- As a Daemon
- Integrated with XAG agent

> **Note:**
>
> If the Service Manager is registered as a system daemon, then the Service Manager, Administration Server (AS), Distribution Server (DS), Receiver Server (RS), and the Performance Metrics Server are automatically started when the host is (re)started.

Login to Service Manager

To start using your Oracle GoldenGate Microservices deployment, you have to connect to the Service Manager:

> **Note:**
>
> When you log into the Service Manager for the first time, it is recommended to change the password.

1. Open a web browser and connect to the Service Manager that you created with Oracle GoldenGate Configuration Assistant. The URL is similar to `http://localhost:9001`, where 9001 is the port where you have deployed your Service Manager instance. For a secure deployment, the URL is similar to `https://localhost:9001`.
2. Enter the user name and password you created during deployment and sign in.

In the Service Manager, you can check if the Service Manager and all the other servers are all up and running. Use the links to connect you to their specific interfaces, review details, and administer your deployments.
For more information on setting up the Service Manager as a daemon service, see How to Create Secure and Non-Secure Deployments.

- How to Start and Stop the Service Manager
  The start and stop process of the Service Manager within Oracle GoldenGate Microservices is different based on how the Service Manager is configured within your environment.
- Quick Tour of the Service Manager
  When you complete the Oracle GoldenGate Microservices installation, the Service Manager opens up at the specified URL. This page acts as an access point for performing deployment, configuring the Administration Server, Distribution Server, Receiver Server, Performance Metrics Server, and the Admin Client.
- How to Interpret the Log Information
- How to Enable and Use Debug Logging

3.1.1 How to Start and Stop the Service Manager

The start and stop process of the Service Manager within Oracle GoldenGate Microservices is different based on how the Service Manager is configured within your environment.

The following provide context on how the start and stop processes can be done for the Service Manager:

- If the Service Manager is configured in manual mode then there are scripts in the `$DEPLOYMENT_BASE/ServiceManager/bin` directory that can be run to start or stop the Service Manager.

  Run the scripts to start or stop the Service Manager from the following locations:

  - To start the Service Manager: `OGG_Deployment_Home/bin/startSM.sh`
  - To stop the Service Manager: `OGG_Deployment_Home/bin/stopSM.sh`

- If the Service Manager is configured as a daemon, the scripts required to start or stop for manual interaction are not created. The operating system is responsible for starting or stopping the Service Manager.

  For OEL 6:

  ```
  stop/start/status for Service Manager
  ```

  ```
  /etc/init.d/OracleGoldenGate start
  ```

  ```
  /etc/init.d/OracleGoldenGate stop
  ```

  ```
  /etc/init.d/OracleGoldenGate status
  ```

  For OEL 7:

  ```
  systemctl start OracleGoldenGate
  ```

  ```
  systemctl status OracleGoldenGate
  ```

  ```
  systemctl stop OracleGoldenGate
  ```

- If the Service Manager is configured to run with the XAG agent in an Oracle Cluster Ready Service (CRS); then the start and stop process is handled by the CRS stack.

3.1.2 Quick Tour of the Service Manager

When you complete the Oracle GoldenGate Microservices installation, the Service Manager opens up at the specified URL. This page acts as an access point for performing deployment, configuring the Administration Server, Distribution Server, Receiver Server, Performance Metrics Server, and the Admin Client.

The Service Manager home page is a dashboard where you can see the services that have been deployed and access inventory and configuration information pertaining to your deployments. You can also view the status of your deployments, and start and stop services.

Now, that you have an overview of the Service Manager, let’s go through some of the actions you can perform using the Service Manager home page.

Action	Task
View the service status	Review Status Changes
Start and stop deployments	Starting and Stopping Deployments and Services
Access various servers	You can click the respective links to access the following: • Administration Server to add, modify, and delete Extracts and Replicats. • Distribution Server to add, modify, and delete Paths • Performance Metrics Server to Review Messages and Review Status Changes • Receiver Server to view details of the path, including path network statistics and file I/O statistics.
Access details for Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server	Click **Details** for the server for which you need to see the details. See View and Edit Services Configuration.
Application Navigation pane	Click the icon to expand and access the Service Manager or the Diagnosis home pages.

3.1.3 How to Interpret the Log Information

You can review all of the messages logged for your Service Manager with this page.

Using the Table

An updated log of Extract and Replicat server messages is displayed. You can sort the list by date or severity by clicking on the adjacent arrow. Also, you can refresh this log and choose how many pages you want to view.

To search, you select Date, Severity, or Message, and then select the appropriate options to construct your search.

Notice the **Notifications** tab at the bottom of the page. It displays server messages, which are not updated in the log due to transaction errors. For example, failure to log in to the database using the database credentials.

3.1.4 How to Enable and Use Debug Logging

You can enable debug logging and download debug log files from this page.

Enabling Debug Logging:

To enable debug logging:

1. Click the Debug Log option from the Navigation Pane of the Service Manager page.
2. Click the Enable Debug Log option to start logging debug information.

Using the Debug Log

You can use the access and use the debug log file from this page:

1. Click the **Download Log File** option to save a local copy of the debug log
2. Click the **Load Debug Log File** option to view the debug log on this page.
3. Search for specific entries in the debug log using the **Search By** box, if required. You can click **Refresh** to get the latest log information, if it doesn't get refreshed automatically.

.

3.2 How to Start and Stop Deployments and Servers

The Service Manager is the central hub from where you can start and stop deployments, Administration Server, Distribution Server, Performance Metrics Server, Receiver Server.

To start and stop servers you need security admin privileges. In some cases, you may choose to only have incoming trail sources and thereby choose to stop or disable the Distribution Server. In a DMZ setup, you may choose to disable Administation Server.

To start or stop a deployment:

> **Note:**
>
> If Oracle GoldenGate Service Manager is registered as a system daemon, then the Service Manager along with the other servers, are automatically started when the host is (re)started.

1. Connect to Service Manager using the URL specified during installation. For example, let’s assume the Service Manager URL in this case is `http://localhost:9001`
2. Log in with your user name and password.
3. In the Deployments section of the Service Manager home page, locate the deployment that you need to start or stop.
4. In the Actions column, click **start**.
5. Check to see if all the services associated with the deployment have started, once your Deployment starts. The Action column automatically shows the **stop** option, which you can use to stop the deployment. By default, all server instances are in Running state when they are deployed.
6. To start or stop a service, such as the Administration Server or the Distribution server, associated with your Deployment, go to the Services section.
7. Identify the server (or service) that you need to start (or stop) and click start in the Actions column, the same way you did for Deployments.

3.3 How to Remove a Deployment

You can remove a deployment using OGGCA or in silent mode.

Topics:

- How to Remove a Deployment: GUI
  You can remove a deployment or Service Manager using the `oggca` program.
- How to Remove a Deployment: Silent Mode
  You can remove a deployment silently using the Oracle GoldenGate Configuration Assistant (oggca) from the Oracle GoldenGate Home bin directory.

3.3.1 How to Remove a Deployment: GUI

You can remove a deployment or Service Manager using the `oggca` program.

By removing a deployment, you can delete various components of the deployment, including, Extracts, Replicats, paths, and configuration files. However, the Service Manager is not deleted.

To remove a deployment:

1. Run the `oggca` program from the following location: `$OGG_HOME/bin`
2. Select **Existing Service Manager** from the **Select Service Manager Options** screen. Click **Next**
3. Select **Remove Existing Oracle GoldenGate Deployment** from the Configuration Options screen.
4. Select the deployment you need to remove from the **Deployment Name** list box. Also select the **Delete Deployment Files from Disk** check box if you want to remove all the deployment files (including configuration files) from the host.

   > **Note:**
   >
   > When you remove a deployment or uninstall Oracle GoldenGate Microservices, the system does not automatically stop processes. As a result, you may have to stop processes associated with the deployment and you must clean files manually. For details, see “*Files to be Removed Manually After Removing Deployment*”.

5. Enter the Administration account user name and password and click **Next**.
6. See the list of settings that are deleted with the deployment and click **Finish**.

To remove a Service Manager:

1. Run the `oggca` program from the following location: `$OGG_HOME/bin`
2. Select **Existing Service Manager** from the **Select Service Manager Options** screen. Click **Next**.
3. If there are no other deployments to remove, then the option to remove the Service Manager is available in the drop down. Select **Remove Service Manager Deployment** from the Configuration Options screen.

4. Click **Finish**.

   The following commands are executed: to stop the Service Manager:

   `systemctl stop OracleGoldenGate systemctl disable OracleGoldenGate *`

   The following files are deleted:

   `/etc/oggInst.loc /etc/systemd/system/OracleGoldenGate.service`

3.3.2 How to Remove a Deployment: Silent Mode

You can remove a deployment silently using the Oracle GoldenGate Configuration Assistant (oggca) from the Oracle GoldenGate Home bin directory.

By removing a deployment, you can delete various components of the deployment, including, Extracts, Replicats, paths, and configuration files. However, the Service Manager is not deleted.

To remove a deployment silently:

1. Ensure that you have a deployment response file. To get the deployment response file, run the OGGCA and the save the response file.
2. Update the following lines within the deployment response file:

   ```
   CONFIGURATION_OPTION=REMOVE
   ADMINISTRATOR_PASSWORD=********
   CREATE_NEW_SERVICEMANAGER=false
   ```

3. Run the OGGCA program from the following location using the `-silent` and `-responseFile` options. Providing the exact path to the deployment response is needed.

   ```
   $OGG_HOME/bin/oggca.sh -silent -responseFile
   path_to_response_file/response_file.rsp
   ```

   Example:

   ```
   $OGG_HOME/bin/oggca.sh -silent -responseFile
           /home/oracle/software/ogg_deployment.rsp
   ```

3.4 View and Edit Services Configuration

The services configuration and restart options for Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server can be viewed and edited from the Services Manager.

You can access the services configuration for each of the servers, from the Service Manager home page. Click the Details button for the server that you need to check the service configuration for. The Service Configuration page is displayed. This page allows you to view and edit the service configuration and the restart options for the corresponding server. The configuration and restart options for all the servers are the same.

The following table explains the Service Configuration and Restart Options on the Services Configuration page.

Service Configuration Options	**Description**
Port	Port Number for the corresponding server
Enable Legacy Protocol	Enables legacy communication for services that are compatible.
Enabled Async Operation	Enables asynchronous RESTful API method execution
Default Sync Wait	The default time a service will wait before responding with an asynchronous REST API response
Enabled Task Manager	Enable task management for services that provide it.
U-Mask	File mode creation mask
Quiet	Starts the service in quiet mode.
Enabled	Indicates that the service is managed by Service Manager.
Status	Indicates that the service is running.
Restart Options	**Description**
Enabled	If set to true, then it restart a task if it gets terminated.
On Success	If set to false, then the task is only restarted if it fails.
Delay	The time (in minutes) to pause between discovering that a process is terminated abruptly and restarting it.
Retries	The maximum number of trials to restart the service, before aborting the retry effort.
Window	The time interval in which the retries are counted. The default is 120 minutes.
Disable on Failure	If set to true, the task is disabled after it fails all execution attempts in an execution window.

4 Working with Data Replication

You can perform all data replication tasks from the Administration Server home page. You can add Extracts and Replicats after creating your deployments.

Before you begin creating Extract processes, you need to:

- Add trandata or schematrandata
- Enable supplemental logging for SQL Server CDC capture
- Create and enable heartbeat tables.

Before creating Replicats, you need to:

- Create the checkpoint table

You'll also create a user with the admin role from the Administration Server. The initial user created during deployment is a security admin role. The security admin user should not do other tasks. So, you need to create users with the admin role and this user is used to create Extract and Replicat processes.

Users in Service Manager deployment are different from Administration Sever deployment. Service Manager deployment. users are created from the Service Manager web interface, and normal deployment users are created from the Administration Server web interface. Users in Service Manager deployment have control of Service Manager functions like stopping, starting, enabling, and disabling services. Users created from the Administration Server can create Extract, Replicat, and other processes.

Topics:

- Quick Tour of the Administration Server Home Page
  When you click the Administrator Server link on the Service Manager home page, the login page for the Administration Server is displayed. After logging in, you can configure Extract and Replicat processes from this Web UI.
- How to Add a Database Credential
  To create and run Extract and Replicat processes, you need to set up database credentials.
- Before Creating an Extract
  As a prerequisite to create the primary Extract, you must perform the actions described in this topic.
- How to Add Extracts
- Before Creating Replicat
  Before you start creating Replicat, create the checkpoint table.
- How to Add a Replicat
  You can add Replicats for the target deployment from the Administration Server.
- How to Use the Master Keys and Encryption Keys
  You can set the master keys and encryption keys using the **Key Management** tab in the **Configuration** page of the Administration Server.

- How to Access the Parameter Files
  The Global parameters, Extract, Replicat parameter files are available in the Parameter Files section of the Administration Server.
- Setting Up Automated Tasks
  The Administration Server performs the commands that were executed by the GGSCI utility in previous releases. However, the Administration Service provides enhanced capabilities to perform these tasks, while still being compatible with GGSCI.
- Review Critical Events
  You can review and search for critical events from the Administration Server home page, once you set up the distribution path.
- How to Configure Managed Processes
  Oracle GoldenGate Administration Server provides options to set up profiles for managed Extract and Replicat (ER) processes. These processes are assigned auto-start and auto-restart properties to control their life cycles.
- How to Access Extract and Replicat Log Information
  The diagnosis of Extract and Replicat transactions provides information about the severity of a transaction along with the timestamp. This information is helpful in case you need to determine if and when a particular issue occurred including the cause of the issue.
- How to Create Users from the Administration Server
  Oracle GoldenGate Microservicesusers can be created from the Administration Server, once you log in using the credentials created at the time of configuring the deployment.

4.1 Quick Tour of the Administration Server Home Page

When you click the Administrator Server link on the Service Manager home page, the login page for the Administration Server is displayed. After logging in, you can configure Extract and Replicat processes from this Web UI.

The Administration Server home page is used to add Extracts and Replicats. The table on the home page displays the severity of critical events. You can also use the left-navigation pane to access various configuration details, a list of severity issues with their diagnosis, and a list of administrators.

Now, that you have an overview of the Administration Server home page, let’s understand some of the key actions that you can perform from this page.

Action	Description
View the home page in tabular format	Use the Table Layout swivel to turn the tabular format on and off.
View Extracts and Replicats	The statistical representation the home page displays current state of Extracts and Replicats (Starting, Running, Stopped, Abended, Killed)
Add an Extract	See How to Add an Extract for a Deployment
Create a Replicat	See How to Add a Replicat
Stop and start Extracts	Using Extract Actions
Stop and start Replicats	See Using Replicat Actions

Action	Description
View and search critical events	Monitor severity of events using the Critical Events table and also search for specific events, if required.

4.2 How to Add a Database Credential

To create and run Extract and Replicat processes, you need to set up database credentials.

1. Launch the Administration Server interface and log in.
2. Click **Configuration** from the **Application Navigation** pane.
3. Click the **+** sign next to Credentials, and set up your new credential alias, then click **Submit**.
4. Click the Login icon to verify that the new alias can correctly log in to the database.

   If an error occurs, click the **Alter Credential** icon to correct the credential information, and then test the log in.

You can edit existing credentials to change the user name and password. Delete a credential by clicking the trash icon.

When you successfully log into your database, you can add and manage checkpoint tables, transaction information, and heartbeat tables. All of the tables can be searched using the various search fields. As you type, the table is filtered and you can use the search button with the search text.

4.3 Before Creating an Extract

As a prerequisite to create the primary Extract, you must perform the actions described in this topic.

ADD TRANDATA or ADD SCHEMATRANDATA

To enable supplemental logging at the table level, use the `ADD TRANDATA` command and for schema level, use `ADD SCHEMATRANDATA`. For details, see `ADD TRANDATA` and `ADD SCHEMATRANDATA` You can skip `ADD TRANDATA` in case of initial load without CDC.

Enable Supplemental Logging for SQL Server CDC

To capture tables in case of CDC capture, you need to enable supplemental logging for the tables. See Enabling Supplemental Logging old (CDC Extract).

Create Heartbeat Table for SQL Server CDC

You need to create the heartbeat table for SQL Server CDC. To create the heartbeat table:

1. From the Administration Server, select **Configuration** from the navigation pane.
2. Select the + sign next to the Heartbeat section of the Database tab. You'll need to enter the values for the heartbeat frequency, retention time, and purge frequency.

You can create the heartbeat table using the `ADD HEARTBEATTABLE` command from the Admin Client or GGSCI. See ADD HEARTBEATTABLE.

4.4 How to Add Extracts

Set up database credentials to create and run Extracts using the steps in How to Add a Database Credential.

1. From the home page of the Administration Server, click the + sign next to Extract..
2. Choose the type of Extract to create and click **Next**. The types of Extract are:
   - Integrated Extract
   - Classic Extract
   - Initial Load Extract

   > **Note:**
   >
   > An Initial Load Extract cannot be started from a secure deployment. You can only start it in a non-secure deployment.

3. Enter and select the required information, which is designated with an asterisk (*). For all Extracts the Process Name, Credential Domain, and Credential Alias are required. A description is optional. The **Create new credential** option is common to all Extracts. You can configure the following additional required and optional details based on the type of Extract you selected to create:

   You must enter the options for Managed Processes while creating all types of Extract processes. The following table provides these options:

Option	Description	Extract Type
Intent	What you want the Extract to be used for, such as High Availability or the Unidirectional default.	Classic, Integrated, and Initial Load
Begin	How you want the Extract to start. At a custom time that you select, a database CSN, or the Now default.	Classic and Integrated
Trail Name	A two character trail name.	Classic and Integrated
Trail Subdirectory, Size, Sequence, and Offset	You can further configure the trail details.	Classic and Integrated
Remote	Set if the trail is not on the same server.	Classic and Integrated
Thread Number	Set to a specific redo log number. The default is 1.	Classic
Encryption Profile	Provide the name of the encryption profile for the Extract. If no encryption profile is created, then the default encryption profile is selected, by default	Classic, Integrated, and Initial Load.

Option	Description	Extract Type
Encryption Profile Type	Provide the type of Key Management Service being used. Oracle Key Vault is selected by default.	Classic, Integrated, and Initial Load.
Managed Options	X	X
Profile Name	Provides the name of the autostart and autorestart profile. You can select the default or custom options.	Classic, Integrated, and Initial Load.
Critical to deployment health	Enable this option if the profile is critical for the deployment health.	Classic, Integrated, and Initial Load.
Auto Start	Enables autostart for the process.	Enables autostart for the process.
Max Retries	Specify the maximum number of retries to try to start the process	Classic, Integrated, and Initial Load.
Retry Delay	Delay time in trying to start the process	Classic, Integrated, and Initial Load.
Retries Window	The duration interval to try to start the process	Classic, Integrated, and Initial Load.
Restart on Failure only	If true the task is only restarted if it failes	Classic, Integrated, and Initial Load.
Disable Task After Retries Exhausted	If true then the task is disabled after exhausting all attempts to restart the process.	Classic, Integrated, and Initial Load.

4. Click **Next**.
5. You can edit the parameter file in the text area to list the table details that you are interested in capturing. For example, `table source.table1;`

   You can select **Register Extract in the background** to register the Extract in the background asynchronously.

   You can select **Register Extract in the background** to register the Extract in the background asynchronously.
6. You can select Register Extract in the background to register the Extract in the background asynchronously.
7. Click **Create and Run** to create and start the Extract. If you select **Create**, the Extract is created but you need to start it using the Extract drop-down on the Overview page.

   You are returned to the Overview page of the Administration Server. Select the Action list if you want to look at the Extract details such as process information, checkpoint, statistics, parameters, and report.

- Using Extract Actions
  Once you create an Extract, you can monitor various details associated with the Extract from the Administration Server home page.

4.4.1 Using Extract Actions

Once you create an Extract, you can monitor various details associated with the Extract from the Administration Server home page.

You can change the status of the Extract process using the Action button to:

Action	Result
Details	Displays the following tabs: • **Process Information**: The status of the selected process including the type, credentials, and trail. • **Checkpoint**: The checkpoint log name, path, timestamp, sequence, and offset value. You can monitor the input details, such as when starting, at recovery, and the current state. The checkpoint output values display the current checkpoint details. • **Statistics**: The active replication maps along with replication statistics based on the process type. You sort the lost to view the entire statistical data, daily, or hourly basis. • **Parameters**: The parameters configured when the process was added. You can edit the parameters by clicking the pencil icon. Make sure that you apply your changes. • **Report**: A detailed report of the process including parameter settings and a log of the transactions. You could copy the report text and save it to a file so that you can share or archive it.
Start/Stop	The Extract starts or stops immediately.
Start/Stop (in the background)	The Extract is started or stopped using a background process.
Start with Options	Allows you to change the Extract CSN options, then starts the Extract.
Alter	This option is available only when the Extract is stopped. Allows you to change when the Extract begins, the description, and the intent. It does not start the Extract.
Delete	This option displays only when the Extract is stopped. Deletes the Extract if you confirm the deletion.

When you change the status, the list options change accordingly. As status are changing, the icons change to indicate the current and final status. The events are added to the Critical Events table. Additionally, progress pop-up notifications appear at the bottom of the page.

4.5 Before Creating Replicat

Before you start creating Replicat, create the checkpoint table.

Once you connect to the database, you can create the checkpoint table. To create the checkpoint table:

1. From the Administration Server, go the Configuration page using the navigation pane.
2. Click the + sign next to the Checkpoint section on the Database tab.
3. Enter the checkpoint table name in the Checkpoint Table box. The table name must be a two-part or three-part value. For example, GGADMIN.CHKP1.

You can add the checkpoint table using the `ADD CHECKPOINTTABLE` command from the Admin Client or GGSCI. See ADD CHECKPOINTTABLE

4.6 How to Add a Replicat

You can add Replicats for the target deployment from the Administration Server.

Make sure that you have configured your deployments correctly, checked your database credentials, and created an Extract before you set up your Replicat. For details see Working with Deployments and Services. Once you've set up your source and target deployment, you can create and run the Replicat by following these steps:

1. Click the + sign next to Replicats on the Administration Server home page.

   The Add Replicat page is displayed.

2. Select a Replicat type and click **Next**.

   The types of Replicat are:

   - Integrated Replicat
   - Nonintegrated Replicat
   - Coordinated Replicat
   - Parallel Replicat: If you select this option, then select an integrated or nonintegrated parallel Replicat.

3. Enter the required Replicat options on the Replicat Options page and click **Next**. To know more about the Replicat options, see the online help.
4. For managed processes, the options to enter are:

Option	Description	Extract Type
Intent	What you want the Extract to be used for, such as High Availability or the Unidirectional default.	Classic, Integrated, and Initial Load
Begin	How you want the Extract to start. At a custom time that you select, a database CSN, or the Now default.	Classic and Integrated
Trail Name	A two character trail name.	Classic and Integrated

Option	Description	Extract Type
Trail Subdirectory, Size, Sequence, and Offset	You can further configure the trail details.	Classic and Integrated
Remote	Set if the trail is not on the same server.	Classic and Integrated
Thread Number	Set to a specific redo log number. The default is 1.	Classic
Encryption Profile	Provide the name of the encryption profile for the Extract. If no encryption profile is created, then the default encryption profile is selected, by default	Classic, Integrated, and Initial Load.
Encryption Profile Type	Provide the type of Key Management Service being used. Oracle Key Vault is selected by default.	Classic, Integrated, and Initial Load.
Managed Options	X	X
Profile Name	Provides the name of the autostart and autorestart profile. You can select the default or custom options.	Classic, Integrated, and Initial Load.
Critical to deployment health	Enable this option if the profile is critical for the deployment health.	Classic, Integrated, and Initial Load.
Auto Start	Enables autostart for the process.	Enables autostart for the process.
Max Retries	Specify the maximum number of retries to try to start the process	Classic, Integrated, and Initial Load.
Retry Delay	Delay time in trying to start the process	Classic, Integrated, and Initial Load.
Retries Window	The duration interval to try to start the process	Classic, Integrated, and Initial Load.
Restart on Failure only	If true the task is only restarted if it failes	Classic, Integrated, and Initial Load.
Disable Task After Retries Exhausted	If true then the task is disabled after exhausting all attempts to restart the process.	Classic, Integrated, and Initial Load.

5. Click **Create and Run** to create and run the Replicat.

- Creating a Parallel Replicat
- Using Replicat Actions
  Various Replicat actions can be performed from the Administration Server Overview page.

4.6.1 Creating a Parallel Replicat

You can create a parallel Replicat from the user interface or the command line interface.

Before you start creating the parallel Replicat, make sure that you've select the checkpoint table.

Creating a Non-Integrated Parallel Replicat with the Administration Server

1. Log into the Administration Server.
2. Click Application Navigation on the top-left corner.
3. Select **Configuration**. Make sure that the database credentials are correct and the database user is connected. See How to Add a Database User

   for details.
4. Click the **+** sign to add a checkpoint table.
5. Enter the `*schema.name*` of the checkpoint table that you would like to create, and then click **Submit**.
6. Validate that the table was created correctly by logging out of the Credential Alias using the log out database icon, and then log back in.

   Once the log in is complete, your new checkpoint table is listed.
7. Click **Overview** to return to the main Administration Server page.
8. Click the **+** sign next to **Replicats**.
9. Select **Nonintegrated Replicat** then click **Next**.
10. Enter the required information making sure that you complete the Credential Domain and Credential Alias fields before completing the Checkpoint Table field, and then select your newly created Checkpoint Table from the list.
11. Click **Next**, and then click **Create and Run** to complete the Replicat creation.

Creating a Non-Integrated Parallel Replicat with the Admin Client

1. Go the `bin` directory of your Oracle GoldenGatehome directory.

   ```
   cd $OGG_HOME/bin
   ```
2. Start the Admin Client.

   ```
   adminclient
   ```

   The Admin Client command prompt is displayed.

   ```
   OGG (not connected) 12>
   ```
3. Connect to the Service Manager deployment source:

   ```
   connect https://localhost:9500 deployment Target1 as oggadmin password welcome1
   ```

   You must use http or https in the connection string; this example is a non-SSL connection.
4. Add the Parallel Replicat, which may take a few minutes to complete:

   ```
   add replicat R1, parallel, exttrail bb checkpointtable ggadmin.ggcheckpoint
   ```

   You could use just the two character trail name as part of the `ADD REPLICAT` or you can use the full path, such as `/u01/oggdeployments/target1/var/lib/data/bb`.
5. Verify that the Replicat is running:

   ```
   info replicat R1
   ```

Messages similar to the following are displayed:

```
REPLICAT   R1        Initialized   2016-12-20 13:56   Status RUNNING
NONINTEGRATED
Parallel
Checkpoint Lag       00:00:00 (updated 00:00:22 ago)
Process ID           30007
Log Read
Checkpoint  File ./ra000000000First Record  RBA 0
```

- Basic Parameters for Parallel Replicat

4.6.1.1 Basic Parameters for Parallel Replicat

The following table lists the basic parallel Replicat parameters and their description.

Parameter	Description
MAP_PARALLELISM	Configures number of mappers. This controls the number of threads used to read the trail file. The minimum value is 1, maximum value is 100 and the default value is 2.
APPLY_PARALLELISM	Configures number of appliers. This controls the number of connections in the target database used to apply the changes. The default value is 4.
MIN_APPLY_PARALLELISM MAX_APPLY_PARALLELISM	The Apply parallelism is auto-tuned. You can set a minimum and maximum value to define the ranges in which the Replicat automatically adjusts its parallelism. There are no defaults. Do *not* use with APPLY_PARALLELISM at the same time.
SPLIT_TRANS_REC	Specifies that large transactions should be broken into pieces of specified size and applied in parallel. Dependencies between pieces are still honored. Disabled by default.
COMMIT_SERIALIZATION	Enables commit FULL serialization mode, which forces transactions to be committed in trail order.
Advanced Parameters	
LOOK_AHEAD_TRANSACTIONS	Controls how far ahead the Scheduler looks when batching transactions. The default value is 10000.
CHUNK_SIZE	Controls how large a transaction must be for parallel Replicat to consider it as large. When parallel Replicat encounters a transaction larger than this size, it will serialize it, resulting in decreased performance. However, increasing this value will also increase the amount of memory consumed by parallel Replicat.

Example Parameter File

```
replicat repA
userid ggadmin, password ***
MAP_PARALLELISM 3
MIN_APPLY_PARALLELISM 2
MAX_APPLY_PARALLELISM 10
SPLIT_TRANS_RECS 1000
map *.*, target *.*;
```

4.6.2 Using Replicat Actions

Various Replicat actions can be performed from the Administration Server Overview page.

You can change the status of the Replicat process using the Actions button to:

Action	Result
Details	Displays the Process Information page that has the following details: • **Statistics**: Displays the active replication maps along with replication statistics based on the type of Replicat. • **Parameters**: Displays the parameters configured when the Replicat was added. You can change these parameters to adjust your Replicat. • **Report**: Displays the details about the Replicat including the parameters with which the replicat is running, and run time messages. • **Checkpoint**: Displays the checkpoint log name, path, timestamp, sequence, and offset value. You can click the Checkpoint Detail icon to view elaborate information about the checkpoint.
Start/Stop	The Replicat starts or stops immediately.
Start/Stop (in the background)	The Replicat is started or stopped using a background process.
Start with Options	Allows you to change the Replicat start point, CSN, filter duplicates, and threads options, then starts the Replicat.
Force Stop	The Replicat is immediately, forcibly stopped.
Alter	Allows you to change when the Replicat begins, the description, and the intent. It does not start the Replicat.
Delete	Deletes the Replicat if you confirm the deletion.

When you change the status, the list options change accordingly. As status are changing, the icons change to indicate the current and final status. The events are added to the Critical Events table. Additionally, progress pop-up messages appear in the bottom of your browser.

4.7 How to Use the Master Keys and Encryption Keys

You can set the master keys and encryption keys using the **Key Management** tab in the **Configuration** page of the Administration Server.

Using Master Keys

If you want to encrypt your data, then create a Master Key by clicking the + sign in the Master Key section. The master key is generated automatically.

You can change the status of the key to Available or Unavailable, by clicking the edit icon in the Master Key table. You can also delete the Master Key from the table by clicking the delete icon.

For details on the Master Key concept, see Encrypting Data with the Master Key and Wallet Method. .

Using the Encryption Keys

To use this method of data encryption, you configure Oracle GoldenGate to generate an encryption key and store the key in a local `ENCKEYS` file. The `ENCKEYS` file must be secured through the normal method of assigning file permissions in the operating system. This procedure generates an AES encryption key and provides instructions for storing it in the `ENCKEYS` file.

To generate the ENCKEYS files, click the + sign in the Encryption Keys section. The Encryption Keys is generated.

For details on the Encryption Keys concept, see the Encrypting the Data with the ENCKEYS Method.

4.8 How to Access the Parameter Files

The Global parameters, Extract, Replicat parameter files are available in the Parameter Files section of the Administration Server.

You use the Administration Server Configuration page and Parameter Files tab to work with your various parameter files.

You use the different parameter file options:

1. Select the **Configuration** option from the Administration Server left-navigation pane.
2. Select the **Parameter Files** tab.

   A list of existing parameter files is displayed along with the GLOBALS parameter file.
3. If you select any of the parameter files, you are presented with the option to edit or delete the selected file. If you want to change the GLOBALS parameter file, you need to stop and restart all of the services.
4. Click + add parameter files.

5. Enter the file name and the required parameters. Make sure to enter the file name with the `.prm` extension.
6. Click **Submit**. The new parameter file is displayed in the list of parameter files.

The actual location of the parameter files on the disk can be determined using the following step:

1. Identify the GoldenGate Deployment ETC Home:
   a. Go to Service Manager Overview page.
   b. Click the deployment from the Deployments section for which you need to find the parameters file.
   c. Under the Deployment Detail window, navigate to the Oracle GoldenGate deployment `/etc` home directory.
   d. Go into the `/config/ogg` directory where the parameter file is located.

The following example shows how to navigate to your parameter file location:

```
[oracle ~]$ cd /opt/app/oracle/gg_deployments/Atlanta/etc
[oracle etc]$ cd conf/ogg[oracle ogg]$ lsEXT_DEMO.prm GLOBALS REP_DEMO.prm
```

4.9 Setting Up Automated Tasks

The Administration Server performs the commands that were executed by the GGSCI utility in previous releases. However, the Administration Service provides enhanced capabilities to perform these tasks, while still being compatible with GGSCI.

Purging Trails

The Purge Trail page works the same way as the Manager `PURGEOLDEXTRACTS` parameter in the Classic Architecture. It allows you to purge trail files when Oracle GoldenGate has finished processing them. Automating this task ensures that the trail files are periodically deleted to avoid excessive consumption of disk space.

From the Tasks tab, when you select the Purge Trail page, it allows you to configure the Administration Service purge trail process.

1. Add a Purge Trail task by clicking the + sign .
2. Enter the **Operation Name** of the Administration Service task. The operation name is case sensitive. For example, you can create an operation with the name **TASK1** and another operation named **task1**.
3. Enter the trail path or trail name in the **Trail** field.
4. Click the **+** sign to add the trail to the **Selected Trails** list.
5. If you don’t need to use Checkpoints, disable the option **Use Checkpoints**.
6. Set the **Keep Rule** value to specify the maximum number of hours, days, or number of files for which the Purge Trails task needs to be active.
7. Specify the number of hours or days when the purge trails task has to run, in the Purge Frequency field and click Submit.
8. Use the Purge Trails task table to edit or delete the task, as required.

   Also see PURGE EXTTRAIL.

Purging Tasks

You can automatically purge processes associated with an Administration Service.

From the Tasks tab, click Purge Tasks.

1. Enter the **Operation Name** that you need to set up for automatic purging.
2. Select the Extract or Replicat task (initial load process) **Process Name** for the operation. The list contains all processes so ensure that you select the correct task.
3. Select the Extract or Replicat task (initial load) **Process Type** for the operation.
4. If you enable **Use Stop Status**, the status of the task is used to perform the purge task.
5. Enter the hours or days after which you need to purge the process and click **Submit**.
6. Edit or delete the purge process task using the relevant icon from the Purge Tasks table.

Reporting Lag

You can manage lag reports from the Lag Report tab. To do so:

1. From the Tasks tab, click Lag Report.
2. The Action column contains all the options to delete, alter, refresh, and view the lag report task details.
3. Select the required option.
4. If you select the Alter Task option, you are presented with options to edit the lag report. The options are:
   - Enabled: To keep processing the lag report task.
   - Check Every (in minutes): To set a time interval to check the lag report.
   - Report: To log report for the task.
   - If Exceeds: To specify a threshold after which a warning would be initiated.
   - Warning: To allow a warning to be generated incase the lag threshold exceeds the specified limit.
   - When Exceeds: The lag threshold after which the warning is triggered.
5. Click Submit.

4.10 Review Critical Events

You can review and search for critical events from the Administration Server home page, once you set up the distribution path.

Once you set up the Extracts and Replicats along with the Distribution path, you are able to see the critical events associated with them.

Search for Critical Events from the Review Critical Events Table

The Review Critical Events table displays the severity, error code, and error messages for critical events. You can view 20 error messages on a single page and you can also search for specific events.

Additionally, you can examine events in depth from the Performance Metrics Server. For details see Quick Tour of the Performance Metric Server home page.

4.11 How to Configure Managed Processes

Oracle GoldenGate Administration Server provides options to set up profiles for managed Extract and Replicat (ER) processes. These processes are assigned auto-start and auto-restart properties to control their life cycles.

You can create profiles for managed processes using the Administration Server or the Admin Client. To create a profile in the Administration Server, perform the following tasks:

1. Click Profile from the Administration Server navigation pane.
2. In the Managed Process Settings tab, you can click + sign to start creating a profile. There's also a default profile preset on this page.
3. Enter the details for the profile options including the Profile Name, Description, Auto Start and Auto Restart options. See the following table for Auto Start and Auto Restart options

Option	Description	Extract Type
Intent	What you want the Extract to be used for, such as High Availability or the Unidirectional default.	Classic, Integrated, and Initial Load
Begin	How you want the Extract to start. At a custom time that you select, a database CSN, or the Now default.	Classic and Integrated
Trail Name	A two character trail name.	Classic and Integrated
Trail Subdirectory, Size, Sequence, and Offset	You can further configure the trail details.	Classic and Integrated
Remote	Set if the trail is not on the same server.	Classic and Integrated
Thread Number	Set to a specific redo log number. The default is 1.	Classic
Encryption Profile	Provide the name of the encryption profile for the Extract. If no encryption profile is created, then the default encryption profile is selected, by default	Classic, Integrated, and Initial Load.
Encryption Profile Type	Provide the type of Key Management Service being used. Oracle Key Vault is selected by default.	Classic, Integrated, and Initial Load.

Option	Description	Extract Type
Managed Options	X	X
Profile Name	Provides the name of the autostart and autorestart profile. You can select the default or custom options.	Classic, Integrated, and Initial Load.
Critical to deployment health	Enable this option if the profile is critical for the deployment health.	Classic, Integrated, and Initial Load.
Auto Start	Enables autostart for the process.	Enables autostart for the process.
Max Retries	Specify the maximum number of retries to try to start the process	Classic, Integrated, and Initial Load.
Retry Delay	Delay time in trying to start the process	Classic, Integrated, and Initial Load.
Retries Window	The duration interval to try to start the process	Classic, Integrated, and Initial Load.
Restart on Failure only	If true the task is only restarted if it failes	Classic, Integrated, and Initial Load.
Disable Task After Retries Exhausted	If true then the task is disabled after exhausting all attempts to restart the process.	Classic, Integrated, and Initial Load.

4.12 How to Access Extract and Replicat Log Information

The diagnosis of Extract and Replicat transactions provides information about the severity of a transaction along with the timestamp. This information is helpful in case you need to determine if and when a particular issue occurred including the cause of the issue.

The Extract and Replicat log information is available on the Diagnosis page of Administration Server. To access the Diagnosis page, click the **left navigation page** of the Administration Server and select **Diagnosis**.

Using the Table

An updated log of Extract and Replicat server messages is displayed. You can sort the list by date or severity by clicking on the adjacent arrow. Also, you can refresh this log and choose how many pages you want to view.

To search, you select Date, Severity, or Message, and then select the appropriate options to construct your search.

Notice the **Notifications** tab at the bottom of the page. It displays server messages, which are not updated in the log due to transaction errors. For example, failure to log in to the database using the database credentials.

4.13 How to Create Users from the Administration Server

Oracle GoldenGate Microservicesusers can be created from the Administration Server, once you log in using the credentials created at the time of configuring the deployment.

This is an optional step with which you can easily identify if replication (setup) is working or not. To create a user, perform the following tasks:

1. Click **Administrator** from the left navigation pane of the Administration Server.
2. Click **+** to add a user.
3. Enter the required credentials in the fields.
4. Make sure that you select a role from the **Role** drop-down list. The available roles are: Administrator, Security, User, and Operator.
5. Click **Submit**.

   The new user is listed in the Users table including the role and information that you supplied.

5 Working with Paths

The path between a source and target deployment can be set using the Distribution Server. You can also create target-initiated distribution paths from the Receiver Server.

This section discusses the steps to create a path once the Extracts and Replicats are configured in the Administration Server.

Topics:

- Quick Tour of the Distribution Server Home Page
  The Distribution Server is accessible from the Service Manager home page.
- How to Add a Distribution Path
  A path is created to send the transaction of data from the Extract to the Replicat. You can create a new path from the Distribution Server .
- How to Add a Target-Initiated Distribution Path
  A target-initiated distribution path is created from the Receiver Server.
- Using the Path Actions
  Once a new path is added, you can perform actions such as stop or pause a path, view reports and statistics, reposition the path, change its filtering, and delete a path, if required.
- Repositioning a Path
  You can reposition a path whenever it’s necessary.
- Changing Path Filtering
  If you want to change the filter settings for an existing path, the steps are mostly the same as those for creating the filtering for a new path.
- Reviewing the Distribution Server Path Information

5.1 Quick Tour of the Distribution Server Home Page

The Distribution Server is accessible from the Service Manager home page.

From the Service Manager home page, click the Distribution Server. The Distribution Server Overview page is displayed where you can view the path that connects the extract and replicat.

You can add paths from the Distribution Server home page. It also offers a dashboard view of the paths, where you can perform various actions.

Action	Task
Add paths	See Adding New Paths
View path details	See Using the Path Actions
Start or Stop the path	See Using the Path Actions
Reposition the path	See Using the Path Actions

Action	Task
Enable sharding using filters	See Using the Path Actions and also Adding New Paths
Set or customize the DML filtering	See Using the Path Actions and also Adding New Paths
Set the DDL filtering	See Using the Path Actions and also Adding New Paths
Set or customize Procedure filtering	See Using the Path Actions and also Adding New Paths
Customize Tag filtering	See Adding New Paths
Delete a Path	See Using Path Actions

5.2 How to Add a Distribution Path

A path is created to send the transaction of data from the Extract to the Replicat. You can create a new path from the Distribution Server .

To add a path to set the trail for the source deployment:

1. Log in to the **Distribution Server**.
2. Click the plus (+) sign next to Path on the Distribution Server home page.

   The Add Path page is displayed.
3. Enter the details as follows:

Options	Description
Path Name	Select a name for the path.
Description	Provide a description. For example, the name of the Extract and Replicat names.
Reverse proxy enabled?	Select to use reverse proxy. To know more about configuring you reverser proxy servers, see Reverse Proxy Support in *Securing the Oracle GoldenGate Environment*
Use Basic Authentication	Select to add a credential to the target URI creating basic MA authentication.
Use Digest Authorization	Select this option to set the Distribution Server to use Digest authorization to communicate with the Receiver Server. **Note:** Both the Distribution Server and Receiver Server must have Digest Authorization for the path, otherwise the path is killed.

Options	Description
Source: *Trail Name*	Select the Extract name from the drop-down list, which populates the trail name automatically. If it doesn't, enter the trail name that you provided while adding the Extract.
Generated Source URI:	A URI is automatically generated for the trail based on the Extract information you provided. You can edit this URI by clicking the pencil, then modifying the source. Typically, you will need to edit the URI if you want to use reverse proxy.
Target	Enter the target endpoint of the path. From the drop-down list, select your data transfer protocol. The default option is `wss`. You also need to enter the URL of the target host, for example, localhost, if the target is on the same system. You may enter the port number of the Receiver Server and the trail name of the Replicat you created earlier. However, it's not mandatory. The port is the Manager port number for Classic Architecture. Path takes the source trail and sends the date to a target trail given here, which can be consumed by any Replicats created later.
Generated Target URI	A source URI is automatically generated for the trail based on the Extract information you provided. You can edit this URI by clicking the pencil, then modifying the source.
Sequence Length	The length of the trail sequence number.
Trail Size (MB)	The maximum size of a file in a trail.
Encryption Profile	Name of the encryption profile associated with the path.
Configure Trail Format	You can optionally toggle this switch to select one of these types `Plain Text`, `XML`, or `SQL`.
Begin	Select the point from where you need to log data. You can select the following options from the drop-down list: • Now • Custom Time • Position is Log (default)
Source Sequence Number	Select the sequence number of the trail from source deployment Extract.
Source RBA Offset	This setting provides the RBA of the record for the source deployment.
Critical	The default value is false. If set to true, this indicates that the distribution path is critical to the deployment.

Options	Description
Auto Restart	The default value is false. If set to true, the distribution path is restarted automatically when killed.
Retries	The number of times to try an restart the task (path process).
Delay	The duration interval to wait between retries.

Rule Configuration	Description
Enable filtering	If you enable filtering by selecting it from the toggle button and click the `Add Rule` button, you’ll see the Rule Definition dialog box. • `Rule Name` • `Rule Action`: Select either Exclude or Include • `Filter Type`: Select from the following list of options: – `Object Type`: Select from three object types: `DML`, `DDL`, and `Procedure` – `Object Names:` Select this option to provide an existing object name. A 3–part naming convention depends on whether you are using CDB. With CDB, you need to use a 3–part naming convention, otherwise a 2–part convention is mandatory. 3–part convention includes container, *`schema`*, *`object`*. 2–part convention includes *`schema`*, *`object name`*. – `Procedure Feature Name`: Select this option to filter, based on existing procedure feature name. – `Column Based`: If you select this option, you are presented with the option to enter the table and column name to which the rule applies. You can filter out using column value with `LT`, `GT`, `EQ`, `LE`, `GE`, `NE` conditions. You can also specify if you want to have before image or after image in filtered data. – `Tag:` Select this option to set the filter based on tags. – `Chunk ID`: Displays the configuration details of database shards, however, the details can’t be edited. • `Negate`: Select this check box if you need to negate any existing rule. You can also see the JSON script for the rule by clicking the JSON tab.

Additional Options	Description
Eof Delay (cent sec)	You can specify the Eof Delay in centiseconds. On Linux platforms, the default settings can be retained. However, on non-Linux platforms, you may need to adjust this setting for high bandwidth, high latency networks, or for networks that have Quality of Service (QoS) settings (DSCP and Time of Service (ToS)).
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.
DSCP	Select the Differentiated Services Code Point (DSCP) value from the drop-down list, or search for it from the list.
TOS	Select the Type of service (TOS) value from the drop-down list.
Nodelay	Enable this option to prevent delay when using the Nagle's option.
Quick ack	Enable this option to send quick acknowledgment after receiving data.
Cork	Enable this option to allow using the Nagle's algorithm cork option.
System Send Buffer Size	You can set the value for the send buffer size for flow control.
System Receiver Buffer Size	You can set the value for the receive buffer size for flow control.

4. Click **Create Path** or **Create and Run**, as required. Select **Cancel** if you need to get out of the Add Path page without adding a path.

Once the path is created, you'll be able to see the new path in the Overview page of the Distribution Server.

5.3 How to Add a Target-Initiated Distribution Path

A target-initiated distribution path is created from the Receiver Server.

To know more about target-initiated distribution paths, see Using Target-Initiated Distribution Paths in MA.

To create a target-initiated distribution path, perform the following steps:

1. Log in to the Receiver Server.
2. Click the + sign on the home page to start adding a path.
3. The following table lists the options to set up the path:

Options	Description
Path Name	Select a name for the path.
Description	Provide a description. For example, the name of the Extract and Replicat names.

Options	Description
Reverse proxy enabled?	Select to use reverse proxy. To know more about configuring you reverser proxy servers, see Reverse Proxy Support in *Securing the Oracle GoldenGate Environment*
Use Basic Authentication	Select to add a credential to the target URI creating basic MA authentication.
Use Digest Authorization	Select this option to set the Distribution Server to use Digest authorization to communicate with the Receiver Server. **Note:** Both the Distribution Server and Receiver Server must have Digest Authorization for the path, otherwise the path is killed.
Source: *Trail Name*	Select the Extract name from the drop-down list, which populates the trail name automatically. If it doesn't, enter the trail name that you provided while adding the Extract.
Generated Source URI:	A URI is automatically generated for the trail based on the Extract information you provided. You can edit this URI by clicking the pencil, then modifying the source. Typically, you will need to edit the URI if you want to use reverse proxy.
Target	Enter the target endpoint of the path. From the drop-down list, select your data transfer protocol. The default option is `wss`. You also need to enter the URL of the target host, for example, localhost, if the target is on the same system. You may enter the port number of the Receiver Server and the trail name of the Replicat you created earlier. However, it's not mandatory. The port is the Manager port number for Classic Architecture. Path takes the source trail and sends the date to a target trail given here, which can be consumed by any Replicats created later.
Generated Target URI	A source URI is automatically generated for the trail based on the Extract information you provided. You can edit this URI by clicking the pencil, then modifying the source.
Sequence Length	The length of the trail sequence number.

Options	Description
Trail Size (MB)	The maximum size of a file in a trail.
Encryption Profile	Name of the encryption profile associated with the path.
Configure Trail Format	You can optionally toggle this switch to select one of these types `Plain Text`, `XML`, or `SQL`.
Begin	Select the point from where you need to log data. You can select the following options from the drop-down list: • Now • Custom Time • Position is Log (default)
Source Sequence Number	Select the sequence number of the trail from source deployment Extract.
Source RBA Offset	This setting provides the RBA of the record for the source deployment.
Critical	The default value is false. If set to true, this indicates that the distribution path is critical to the deployment.
Auto Restart	The default value is false. If set to true, the distribution path is restarted automatically when killed.
Retries	The number of times to try an restart the task (path process).
Delay	The duration interval to wait between retries.

Rule Configuration	Description
Enable filtering	If you enable filtering by selecting it from the toggle button and click the `Add Rule` button, you'll see the Rule Definition dialog box. • `Rule Name` • `Rule Action`: Select either Exclude or Include • `Filter Type`: Select from the following list of options: – `Object Type`: Select from three object types: `DML`, `DDL`, and `Procedure` – `Object Names:` Select this option to provide an existing object name. A 3–part naming convention depends on whether you are using CDB. With CDB, you need to use a 3–part naming convention, otherwise a 2–part convention is mandatory. 3–part convention includes container, *`schema`*, *`object`*. 2–part convention includes *`schema`*, *`object name`*. – `Procedure Feature Name`: Select this option to filter, based on existing procedure feature name. – `Column Based`: If you select this option, you are presented with the option to enter the table and column name to which the rule applies. You can filter out using column value with `LT`, `GT`, `EQ`, `LE`, `GE`, `NE` conditions. You can also specify if you want to have before image or after image in filtered data. – `Tag:` Select this option to set the filter based on tags. – `Chunk ID`: Displays the configuration details of database shards, however, the details can't be edited. • `Negate`: Select this check box if you need to negate any existing rule. You can also see the JSON script for the rule by clicking the JSON tab.

Additional Options	Description
Eof Delay (cent sec)	You can specify the Eof Delay in centiseconds. On Linux platforms, the default settings can be retained. However, on non-Linux platforms, you may need to adjust this setting for high bandwidth, high latency networks, or for networks that have Quality of Service (QoS) settings (DSCP and Time of Service (ToS)).
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.
DSCP	Select the Differentiated Services Code Point (DSCP) value from the drop-down list, or search for it from the list.
TOS	Select the Type of service (TOS) value from the drop-down list.
Nodelay	Enable this option to prevent delay when using the Nagle’s option.
Quick ack	Enable this option to send quick acknowledgment after receiving data.
Cork	Enable this option to allow using the Nagle’s algorithm cork option.
System Send Buffer Size	You can set the value for the send buffer size for flow control.
System Receiver Buffer Size	You can set the value for the receive buffer size for flow control.

Note:

The the protocol options in Use Basic Authentication are wss and ws only for target-initiated distribution paths, unlike regular distribution paths, which provide `ogg` and `udt` options.

For target-initiated distribution paths, the use case for the ws and wss protocols is explained in the following table:

X	Target Deployment (Non-Secure)	Target Deployment (Secure)
Source Deployment (Non-secure)	`ws`	`ws`
Source Deployment (Secure)	`wss`	`wss`

The `wss` protocol must be specified whenever the source deployment (Distribution Server host) has been configured with security enabled. The secured communication channel can be created using an SSL certificate in a client Wallet, even if the target deployment (Receiver Server host) has disabled security.

Limitations

Here are the limitations when working with target-initiated paths:

- There is no support for interaction between legacy and secure deployments using this mode of operation.
- No support for `ogg` nor `udt` protocols. Only `ws` and `wss` protocols are supported.
- It is possible to only get information and stop a target-initiated distribution path on Distribution Server and after the path stops, it is not be visible on the Distribution Server.

You can also set up target-initiated distribution paths using the Admin Client. For command options, see the Admin Client commands `ADD RECVPATH`, `ALTER RECVPATH`, `INFO RECVPATH`, `DELETE RECVPATH`, `START RECVPATH` in Admin Client Command Line Interface Commands.

5.4 Using the Path Actions

Once a new path is added, you can perform actions such as stop or pause a path, view reports and statistics, reposition the path, change its filtering, and delete a path, if required.

On the Overview page of the Distribution Server, click the **Action** button adjacent to the path. From the drop-down list, use the following path actions:

- **Details**: Use this option to view details of the path. You can view the path information including the source and target. You can also edit the description of the path. Statistical data is also displayed including LCR Read from Trails, LCR Sent, LCR Filtered, DDL, Procedure, DML inserts, updates, and deletes, and so on. You can also update the App Options and TCP Options.
- **Stop**: Use this option to stop a path. If the path isn’t started, the Start option is displayed rather than the Stop option. You can stop a target-initiated distribution path only from the Distribution Server. Once you stop the path, it'll not be avaiable on the Distrbution Server.
- **Stop (in the background)**: This option stops the path in the background, without engaging the interface. For this option also, the Start (in background) option is displayed incase the path isn’t started.
- **Delete**: Use this option to delete a path. Click Yes on the confirmation screen to complete path deletion.
- **Reposition**: Use this option to change the Source Sequence Number and Source RBA Offset
- **Change Filtering**: Use this option to enter sharding, DML filtering, DDL filtering, Procedure filtering, and Tag filtering options.

Depending on the action you select, you can see the change in status at the bottom of the Overview page.

5.5 Repositioning a Path

You can reposition a path whenever it’s necessary.

On the Overview page of the Distribution Server, click `Action` adjacent to the path of interest. From the drop-down list, click `Reposition`.

Change one or both of the source database options to reposition the path, then apply the changes.

5.6 Changing Path Filtering

If you want to change the filter settings for an existing path, the steps are mostly the same as those for creating the filtering for a new path.

On the Overview page of the Distribution Server, click `Action` adjacent to the path of interest. From the drop-down list, click `Change Filtering`.

Rule Configuration	Description
Enable filtering	If you enable filtering by selecting it from the toggle button and click the `Add Rule` button, you'll see the Rule Definition dialog box. • `Rule Name` • `Rule Action`: Select either Exclude or Include • `Filter Type`: Select from the following list of options: – `Object Type`: Select from three object types: `DML`, `DDL`, and `Procedure` – `Object Names:` Select this option to provide an existing object name. A 3–part naming convention depends on whether you are using CDB. With CDB, you need to use a 3–part naming convention, otherwise a 2–part convention is mandatory. 3–part convention includes container, *schema*, *object*. 2–part convention includes *schema*, *object name*. – `Procedure Feature Name`: Select this option to filter, based on existing procedure feature name. – `Column Based`: If you select this option, you are presented with the option to enter the table and column name to which the rule applies. You can filter out using column value with `LT`, `GT`, `EQ`, `LE`, `GE`, `NE` conditions. You can also specify if you want to have before image or after image in filtered data. – `Tag:` Select this option to set the filter based on tags. – `Chunk ID`: Displays the configuration details of database shards, however, the details can't be edited. • `Negate`: Select this check box if you need to negate any existing rule. You can also see the JSON script for the rule by clicking the JSON tab.

After you add a rule, it is listed in Inclusion Rules. You can delete rules or edit them. When you edit a rule, you have the same options as adding a rule with the following added filters:

Option	Description
OR AND	Select one logical operator.

Option	Description
Chunk ID	Edit or delete the database shard settings if sharding is used.
Object Type:	Edit or delete the type of object for the rule.

5.7 Reviewing the Distribution Server Path Information

You can constantly monitor the activity of the path on the Distribution Server Process Information page.

- The path details that you configured. You can change the Description and change the trail format type. When changing the trail format, be sure to apply your changes.
- The advanced options are the delay, flush, and TCP that you configured. You can change any or all of these options, then apply to the path.

The Statistics tab shows you detailed information about the path, such as the different path types and tables. You can use the arrows to sort the tables and the search to quickly locate a specific table. The search is case insensitive and starts searching as you type to update the table.

6

Working with Trails

A trail is a series of files on disk where Oracle GoldenGate stores the captured changes temporarily to support the continuous extraction and replication of database changes You can use trails to monitor path, tune networks, and data input and output.

This section describes the tasks to set up trails:

Topics:

- Quick Tour of the Receiver Server Home Page
  The Receiver Server is the central control service that handles all incoming trail files.
- Tuning Network Parameters
  The network settings in Receiver Server are for Receiver Server initiated paths and must mirror the ones in Distribution Server. Network parameters include TCP flush byte options, DSCP, ToS, buffer size settings and so on.
- Reviewing the Receiver Server Path Information
- Monitoring Paths
  You can monitor the path network statistics from the Receiver Server.

6.1 Quick Tour of the Receiver Server Home Page

The Receiver Server is the central control service that handles all incoming trail files.

The Receiver Server works with the Distribution Server to provide compatibility with the classic remote architecture. The Receiver Server home page shows the condition of the distribution path with one end depicting the Extract and the other end, the Replicat.

You can use the Receiver Server home page to view the path details. Simply click **Action**, **Details** to see the path details. To know more, see Monitoring Paths.

6.2 Tuning Network Parameters

The network settings in Receiver Server are for Receiver Server initiated paths and must mirror the ones in Distribution Server. Network parameters include TCP flush byte options, DSCP, ToS, buffer size settings and so on.

You can monitor and fine-tune these parameters depending on your requirements using the Performance Metrics and Distribution Server. However, this applies to Distribution Server if the path is initiated from the Distrbution Server and to Receiver Server when the path is initiated from the Receiver Server.

You can view the network parameters from the Performance Monitor Server Overview page for paths that are initiated from the Distribution Server. If you need to tweak them, go to the Distribution Server and do the following:

1. Click the path **Action**, **Details**.

The Path Information page is displayed.

2. Expand the Advanced Options.

   You'll see App Options, which contain the TCP Flush Bytes and TCP Flush Seconds values. By default, this value is set to OS Default.

   The TCP Options, include the following parameters:

   - DSCP
   - TOS
   - Nodelay
   - Quick ack
   - Cork
   - System Send Buffer Size
   - System Receiver Buffer Size

3. Click the **Edit** icon next to **Advanced Options**, to change any of the these values,.
4. Click **Apply** to save the changes to the network parameters.

Once you edit the network parameters, do monitor their status changes and messages from the server. You can do so using the Performance Monitor Server. See Monitoring Performance for details.
For paths initiated from the Receiver Server, the network statistics can be tweaked from the Receiver Server by performing the following steps:

1. Click the target-initiated path **Action** button and select **Details**.
2. From the Path Information tab, expand the Advanced Options, which has the setting for EoF Delay (centiseconds). You may typically need to edit this setting for non-Linux platfoms.

6.3 Reviewing the Receiver Server Path Information

You can constantly monitor the activity of the path on the Receiver Server Statistics page.

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

The table information includes the values of LCRs read and sent. You can use the arrows to sort the tables and the search to quickly locate a specific table. The search is case insensitive and starts searching as you type to update the table.

6.4 Monitoring Paths

You can monitor the path network statistics from the Receiver Server.

In the Receiver Server, you'll see the path depicted in a graphical representation and you can perform the following steps to monitor the selected path:

1. Log in to the **Receiver Server** home page.
2. Click **Action**, **Details** for a running path.

3. Click the Network tab.

   You can review the path statistics from this tab. This page displays the following details:

   - Network Statistics: The network statistics information includes details such as target trail file name, port number, total messages written out, and so on. You can use this information to go back to the Distribution Server and tune the network parameters, if required.
   - File IO Statistics: The file IO statistics include total bytes read, total idle time and so on.

7
Monitoring Performance

The Performance Metrics Server provides a dashboard view as well as a detailed view of status changes, statistical data of the servers' performance. They are represented through statistical charts and real-time data.

Topics:

- Quick Tour of the Performance Metrics Server Home Page
  The Performance Metrics Server uses the metrics service to collect and store instance deployment performance results. The Performance Metrics Server home page allows you to perform these tasks.
- Monitoring Server Performance
  All the servers and processes of the Microservices Architecture can be monitored at drill-down levels to allow trend monitoring and statistical analysis of data. The Performance Metrics Server offers these detailed views with graphical representations of statistical data in real-time.
- Reviewing Messages
  Messages from the servers are displayed in Performance Metrics server home page.
- Review Status Changes
  Real-time status changes to servers can be monitored from the Performance Metrics Server Status Changes Overview tab.
- How to Purge the Datastore
  You can change the datastore retention and purge it from the Performance Metrics Server Monitoring Commands tab.

7.1 Quick Tour of the Performance Metrics Server Home Page

The Performance Metrics Server uses the metrics service to collect and store instance deployment performance results. The Performance Metrics Server home page allows you to perform these tasks.

When you arrive at the Performance Metrics Server home page, you see all the Oracle Golden Gate processes in their current state. You can click a process to view its performance metrics. You can also access server messages and status change details from this page.

Here's a general overview of the tasks that you can perform from this page.

Task	Description
Review Messages	Reviewing Messages from the Messages Overview tab.
Review Status Changes	Click the Review Status Changes tab to review changes in status of a server.

7.2 Monitoring Server Performance

All the servers and processes of the Microservices Architecture can be monitored at drill-down levels to allow trend monitoring and statistical analysis of data. The Performance Metrics Server offers these detailed views with graphical representations of statistical data in real-time.

The Performance Metrics Server home page presents a dashboard view of all the servers, along with their statuses. If you want to drill down to any of the servers performance, simply click the server to open the reports page for that particular server.

Each server provides an elaborate view of the processes, threads, trail files, database configuration, and so on, depending on the server that you are viewing. The page also provides the option to **Pause** or **Clear** the data displayed on the page. To get a snapshot of the trends captured for each of the servers, see the following table:

Metrics Report Tab	Available with Server
Process Performance	• Administration Server • Distribution Server • Performance Metrics Server • Receiver Server • Extracts • Replicats
Thread Performance	• Administration Server • Distribution Server • Performance Metrics Server • Receiver Server • Extracts • Replicats
Status and Configuration	• Administration Server • Distribution Server • Performance Metrics Server • Receiver Server • Extracts • Replicats
Server Statistics	• Distribution Server • Performance Metrics Server

Trail Files	• Extracts • Replicats
Database Statistics	• Extracts • Replicats
Procedure Statistics	• Extracts • Replicats
Cache Statistics	Extracts
Queue Statistics	Extracts

7.3 Reviewing Messages

Messages from the servers are displayed in Performance Metrics server home page.

To review the messages sent or received, do the following:

1. From the Service Manager, click **Performance Metrics Server**.

   The Performance Metrics Server Overview page is displayed.

2. Click the **Messages Overview** tab (if it’s not already selected) to see a drill down into all the server messages.

   Scroll through the list of messages or search for a specific message by entering the text in the message.

3. Click **Refresh** to get a synchronized real-time list of messages before you start searching. You can also change the page size to view more or fewer messages.

7.4 Review Status Changes

Real-time status changes to servers can be monitored from the Performance Metrics Server Status Changes Overview tab.

Status change messages show the date, process name, and its status, which could be running, starting, stopped, or killed.

To view status changes, click **Performance Metrics Server** from the Service Manager home page, and then click the **Status Changes Overview** tab. A list of status change messages from the server appears.

If you are searching for specific messages, you can use the search but make sure you click **Refresh** before you search to ensure that you get the updated status for servers.

Note that the search messages appear in different colors to differentiate critical and informational messages.

7.5 How to Purge the Datastore

You can change the datastore retention and purge it from the Performance Metrics Server Monitoring Commands tab.

To view status changes, click **Performance Metrics Server** from the Service Manager home page, and then click the **Monitoring Commands** tab.

The current process retention in days displays.

You can enter the number of retention days or use the sliding icon to set the new period from 1 to 365 days, then **Execute** to activate the purge. The details of the purge displays.

8 Working with Oracle GoldenGate Sharding

Oracle GoldenGate provides a cohesive platform for a sharded Oracle Database, allowing data replication across various sharded database topologies.

All the functionality of a sharded database, in addition to providing pre-configured Oracle GoldenGate replication as part of the `GDSCTL DEPLOY` command, is included.

- Oracle GoldenGate With a Sharded Database
  Sharding is only available with Oracle Database 12.2.0.1 or later, over a secure Microservices deployment.
- How to Configure Sharding in Oracle GoldenGate
  If you enable sharding, you must set up a secure deployment.

8.1 Oracle GoldenGate With a Sharded Database

Sharding is only available with Oracle Database 12.2.0.1 or later, over a secure Microservices deployment.

You need to make sure that you setup your SSL certificate before you setup sharding. To configure a sharded Oracle Database with Oracle GoldenGate, see Configuring Sharding for Oracle GoldenGate.

Advantages of Oracle GoldenGate Sharding

Oracle GoldenGate provides a complete data replication platform for sharded databases.

This is a powerful capability with the following advantages:

- Horizontally partitions data and workload across numerous discrete Oracle databases that do not share hardware or software
- Enables automatic partitioning and replication, elastic scaling, rebalancing, data-dependent routing for single-shard and cross-shard queries
- Provides an enterprise-class database platform for new generation developers who:
  - Explicitly design applications to scale linearly with fault tolerance
  - Assume schema flexibility with JSON
  - See benefits in the power of relational SQL and ACID
- Active replication within and across shardgroups
- Flexible Deployment, which could have single shardgroup for high availability, multiple shardgroups with varying replication factors
- Different shardgroups can have different replication factors, different number of shards, different hardware platforms and OS versions, or different database versions and patch sets.

8.2 How to Configure Sharding in Oracle GoldenGate

If you enable sharding, you must set up a secure deployment.

Prerequisites

Before you begin with the sharding setup, you must adhere to the following prerequisites:

- Complete Oracle Database install for the catalog and each shard database.
- Create `ggshd_wallet` directory for storing Oracle GoldenGate client certificate under `$ORACLE_BASE/admin` (if `$ORACLE_BASE` is defined) or `$ORACLE_HOME/admin` (when `$ORACLE_HOME` is defined).
- Add one microservices deployment per host where shard catalog or shards is set up.
- Generate Oracle GoldenGate Microservices server and client wallets and certificates.
- Authorize a sharding client user identified by SSL certificate.

  (Recommended) Assign only one Oracle GoldenGate deployment for each shard for High Availability and simplified patching of shards.

For more information on generating security certificates, see Setting Up a Secure Deployment.

Sharding Configuration in Oracle GoldenGate

As a best practice, a deployment should be dedicated to each shard. This ensures high availability. For more information on the advantages of using Oracle GoldenGate sharding, see How Does Oracle GoldenGate Work for a Sharded Database.

The following steps are required to configure sharding in cases where you add a shard from a `shardcatalog` or create a shard:

1. Add a deployment using Oracle GoldenGate Configuration Assistant (OGGCA) in secure mode. See How to Create Deployments.
2. Import the client certificate to `ggshd_wallet`. Ensure Oracle GoldenGate Microservicesservers are up and running on Shards.
3. Prepare to set up a sharded database by connecting to the Oracle Sharding Coordinator (catalog database).
4. Load the Oracle GoldenGate sharding bootstrap scripts located in the `$OGG_HOME/lib/sql/sharding` directory. This is a one-time task.
5. Run the following command from the Oracle Sharding Coordinator:

   `shardcatalog load (as SYS):`

   `$OGGHOME/lib/sql/sharding/ggsys_setup.sql`
6. Before adding shards, load the following command (`as SYS`):

   ```
   $OGGHOME/lib/sql/sharding/orashard_setup.sql
   A <serviceManagerURI>/<OGGDeployName>
   <ggadmin_password> <shardconnect_string>
   ```

> **Note:**
>
> This command is not required when you create a shard.

There are two ways to configure shards for Oracle GoldenGate:

- **Add shards**: It converts an existing single instance database into a shard. However, the instance must *not* contain any user data and should be an empty database.
- **Create shard**: It sets up a new database at runtime. These commands are issued from the GDSCTL shell interface. See Sharded Database Deployment in *Oracle Database Using Oracle Sharding Guide*.

```
create shardcatalog -database bpodb12s:1521/sdbcat1 -user gsmcatuser/
gsmcatuser -repl OGG -sharding SYSTEM -chunks 36

add gsm -gsm gsm1 -listener 1540 -catalog bpodb12s:1521/sdbcat1 -pwd
gsmcatuser

add shardgroup -shardgroup shgrp1 -repfactor 3
add shardgroup -shardgroup shgrp2 -repfactor 2
…
create shard -shardgroup shgrp1 -destination host01 -CREDENTIAL gds_oracle
-netparam none
-gg_service host01:9000/deploy1
-gg_password ggadmin pw
create shard -shardgroup shgrp1 -destination host02 -CREDENTIAL gds_oracle
-netparam none
-gg_service host02:9000/deploy2 -gg_password ggadmin status
configure
add service ...
start service ..
```

A

How to Use the Admin Client

Admin Client is a command line utility (similar to the classic GGSCI utility). It uses the REST API published by the Microservices Servers to accomplish control and configuration tasks in an Oracle GoldenGate deployment.

Admin Client is used to create, modify, and remove processes, instead of using the Microservices web user interface.

If you need to automate the Admin Client connection with the deployment, you can use an Oracle Wallet to store the user credentials. The credentials stored must have the following characteristics:

- Single user name (account) and password
- Local to the environment where the Admin Client runs
- Available only to the currently logged user
- Managed by the Admin Client
- Referenced using a credential name
- Available for Oracle GoldenGate deployments and proxy connections.

> **Note:**
>
> To use the Admin Client for administration tasks, you need the user credentials that work with both the Service Manager and Administration Server.

To use the Admin Client, perform the following steps:

1. Set the environment variables: `OGG_HOME`, `OGG_VAR_HOME`.

   Move to `$OGG_HOME/bin` and run the command:

   ```
   [oracle@bigdatalite bin]$ ./adminclient
   Oracle GoldenGate Administration Client for Oracle
   Version 19.1.0.0.0 OGGCORE_19.1.0.0.0_PLATFORMS_yymmdd.HHMM_FBO

   Copyright (C) 1995, 2019, Oracle and/or its affiliates. All rights
   reserved.

   Linux, x64, 64bit (optimized) on Dec 31 2016 23:58:36
   Operating system character set identified as UTF-8.

   OGG (not connected) 1>
   ```

2. Log into the deployment using the security user credentials. This is the user you created while adding the deployment for your Oracle GoldenGate instance.

   ```
   connect http(s)://localhost:port deployment deployment name as security
   role user
   ```

3. To add users, other than the security role user, for the deployment, use the `ADD CREDENTIALS` command. To know how this command works, see `ADD CREDENTIALS` in *Command Line Interface Reference for Oracle GoldenGate*. Other commands for user credentials are `INFO CREDENTIALS` and `DELETE CREDENTIALS`.

4. You can connect to a deployment or to a proxy server from the Admin Client.

   > **Note:**
   >
   > If your password to connect to a secure or non-secure deployment from the Admin Client has an exclamation mark (!) at the end, then you must enter the password in double quotes when using the `CONNECT` command in a single line. Otherwise, the password is not accepted and the connection fails. This is required for all deployments with a strong password policy.

   Syntax:

   ```
   CONNECT - Connect to an Oracle GoldenGate Service Manager
           |CONNECT server-url [ DEPLOYMENT deployment-name]
           |[ ( AS deployment-credentials-name|
           | USER  deployment-user-name )
           |[PASSWORD deployment-password] ]
           |[PROXY proxy-uri|
           |[(AS proxy-credentials-name
           |USER proxy-user-name)
           |[ PASSWORD proxy-password] ] ] [ ! ]
   ```

   > **Note:**
   >
   > The deployment credentials cannot be stored as a `USERIDALIAS` in the credential store because the Oracle wallet used for storing database credentials is managed by the Administration Server. Instead, a separate Oracle wallet is created for the Admin Client. The Oracle wallet is stored in the users home directory.

   The following example shows the connection to a deployment and to a proxy server:

   ```
   OGG (not connected) 1> ADD CREDENTIALS admin USER oggadmin PASSWORD
   oggadmin-A1
   2019-02-14T00:35:38Z  INFO OGG-15114  Credential store altered.
   OGG (not connected) 2> ADD CREDENTIALS proxy USER oggadmin PASSWORD
   oggadmin-A2
   ```

```
2019-02-14T00:35:48Z  INFO OGG-15114  Credential store altered.
OGG (not connected) 3> CONNECT http://abc.oracle.com:12000 AS admin
PROXY http:111.1.1.1:3128 as proxy
Using default deployment 'Local'
OGG (http://abc.oracle.com:12000 Local) 4>
```

If the credentials are invalid for a proxy connection, then an error similar to the following error occurs:

```
OGG (not connected) 2> ADD CREDENTIALS proxy USER proxyadmin PASSWORD
invalid
2019-02-14T00:48:12Z  INFO OGG-15114  Credential store altered.
OGG (not connected) 3> CONNECT http://abc.oracle.com:12000 AS admin
PROXY http://111.1.1.1:3128 as proxy
ERROR: Proxy server user name 'proxyadmin' or password is incorrect.
```

5. You can view the full list of Admin Client commands using the `HELP` command. Use the `HELP SHOWSYNTAX` command to view the syntax for specific commands.

B

Connecting Microservices Architecture to Classic Architecture

For establishing a connection to Classic Architecture, the Distribution Server in Oracle GoldenGate Microservices must know where to place the remote trail file for reading.

To connect Oracle GoldenGate Microservices and Classic Architecture follow these steps:

> **Note:**
>
> For this procedure to work only the `ogg` protocol is supported and an existing Extract must be running in Microservices.

Task 1: Add a Distribution Path

1. Launch the **Distribution Server** web interface.
2. Click the plus (+) sign next to Path. The Add Path page is displayed.
3. Enter the details:

Rule Configuration	Description
Enable filtering	If you enable filtering by selecting it from the toggle button and click the `Add Rule` button, you'll see the Rule Definition dialog box. • `Rule Name` • `Rule Action`: Select either Exclude or Include • `Filter Type`: Select from the following list of options: – `Object Type`: Select from three object types: `DML`, `DDL`, and `Procedure` – `Object Names:` Select this option to provide an existing object name. A 3–part naming convention depends on whether you are using CDB. With CDB, you need to use a 3–part naming convention, otherwise a 2–part convention is mandatory. 3–part convention includes container, *`schema`*, *`object`*. 2–part convention includes *`schema`*, *`object name`*. – `Procedure Feature Name`: Select this option to filter, based on existing procedure feature name. – `Column Based`: If you select this option, you are presented with the option to enter the table and column name to which the rule applies. You can filter out using column value with `LT`, `GT`, `EQ`, `LE`, `GE`, `NE` conditions. You can also specify if you want to have before image or after image in filtered data. – `Tag:` Select this option to set the filter based on tags.

Rule Configuration	Description
	– `Chunk ID`: Displays the configuration details of database shards, however, the details can't be edited. • `Negate`: Select this check box if you need to negate any existing rule. You can also see the JSON script for the rule by clicking the JSON tab.

Additional Options	Description
Eof Delay (cent sec)	You can specify the Eof Delay in centiseconds. On Linux platforms, the default settings can be retained. However, on non-Linux platforms, you may need to adjust this setting for high bandwidth, high latency networks, or for networks that have Quality of Service (QoS) settings (DSCP and Time of Service (ToS)).
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.
DSCP	Select the Differentiated Services Code Point (DSCP) value from the drop-down list, or search for it from the list.
TOS	Select the Type of service (TOS) value from the drop-down list.
Nodelay	Enable this option to prevent delay when using the Nagle's option.
Quick ack	Enable this option to send quick acknowledgment after receiving data.
Cork	Enable this option to allow using the Nagle's algorithm cork option.
System Send Buffer Size	You can set the value for the send buffer size for flow control.
System Receiver Buffer Size	You can set the value for the receive buffer size for flow control.

4. Click `Create Path` or `Create and Run`, as required. Select `Cancel` if you need to get out of the Add Path page without adding a path.

Once the path is created, you'll be able to see the new path in the Overview page of the Distribution Server.

Task 2: Start Manager in Classic Architecture

1. Log in to GGSCI.
2. Use the command:

   ```
   START MANAGER
   ```

   For more information, see `START MANAGER` in *Reference for Oracle GoldenGate*.

Task 3: Create and start Replicat in Classic Architecture

If you are already logged into GGSCI, use the command:

```
ADD REPLICAT group_name
```

`group_name` is the name of the Replicat group. For more information, see Creating an Online Replicat Group in *Administering Oracle GoldenGate* and GGSCI Command Interface Help. in *Reference for Oracle GoldenGate*.

C

Connecting Oracle GoldenGate Classic Architecture to Microservices Architecture

Oracle GoldenGate Classic Architecture uses the data pump Extract in GGSCI to connect to Microservices.

Follow these steps for establishing a connection between a non-secure Microservices deployment and Classic Architecture:

Create a data pump Extract

> **Note:**
>
> To perform this task, an existing data pump Extract must be running in Classic Architecture.

1. Log in to GGSCI.
2. Add a data pump Extract using the command:

   ```
   ADD EXTRACT dp_name, EXTTRAILSOURCE ./dirdat/aa
   ```

   This example uses, `dp_name` as the name of the data pump Extract.
3. Add the remote trail to the data pump Extract using the command:

   ```
   ADD RMTTRAIL ab, EXTRACT dp_name, MEGABYTES 500
   ```

4. Edit the parameter file for the data pump Extract using the command:

   ```
   EDIT PARAMS dp_name
   ```

   Here’s an example of the data pump Extract parameter file:

   ```
   EXTRACT dp_name
   RMTHOST hostname/IP address, PORT receiver service port
   RMTTRAIL ab
   PASSTHRU
   TABLE pdb.schema.table;
   ```

Start the data pump Extract
Use the following command to start the data pump Extract `dp_name`:

```
START EXTRACT dp_name
```

Once the data pump Extract has started, the Receiver Server establishes a path and begins reading the remote trail file. The remote trail file appears in the `$OGG_VAR_HOME/lib/data` of the associated deployment running the Receiver Server.