Oracle® Fusion Middleware

Using Oracle GoldenGate Microservices Architecture

12*c* (12.3.0.1)
E84970-06
November 2018

Oracle Fusion Middleware Using Oracle GoldenGate Microservices Architecture, 12*c* (12.3.0.1)

E84970-06

Primary Author: Oracle Corporation

Contents

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

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

Getting Started with Oracle GoldenGate

Oracle GoldenGate supports two architectures, the Classic Architecture and the Microservices Architecture (MA).

Oracle GoldenGate can be configured for the following purposes:

- A static extraction of data records from one database and the loading of those records to another database.
- Continuous extraction and replication of transactional Data Manipulation Language (DML) operations and data definition language (DDL) changes (for supported databases) to keep source and target data consistent.
- Extraction from a database and replication to a file outside the database.

Oracle GoldenGate Architectures Overview

The following table describes the two Oracle GoldenGate architectures and when you should use each of the architectures.

X	Classic Architecture	Microservices Architecture
What is it?	Oracle GoldenGate classic architecture provides the processes and files required to effectively move data across a variety of topologies. These processes and files form the main components of the classic architecture and was the product design until this release.	Oracle GoldenGate Microservices Architecture is a new microservices architecture that provides REST-enabled services as part of the Oracle GoldenGate environment. The REST-enabled services provide remote configuration, administration, and monitoring through HTML5 web pages, command line, and APIs.

X	Classic Architecture	Microservices Architecture
When should I use it?	Oracle GoldenGate can be installed and configured to use the Oracle GoldenGate classic architecture for the following purposes: • A static extraction of data records from one database and the loading of those records to another database. • Continuous extraction and replication of transactional Data Manipulation Language (DML) operations and Data Definition Language (DDL) changes (for supported databases) to keep source and target data consistent. • Extraction from a database and replication to a file outside the database. • Capture from heterogeneous database sources.	Oracle GoldenGate can be installed and configured to use the Oracle GoldenGate Microservices Architecture for the following purposes: • Large scale and cloud deployments with fully-secure HTTPS interfaces and Secure WebSockets for streaming data. • Simpler management of multiple implementations of Oracle GoldenGate environments and control user access for the different aspects of Oracle GoldenGate setup and monitoring. • Support system managed database sharding to deliver fine-grained, multi-master replication where all shards are writable, and each shard can be partially replicated to other shards within a shardgroup. • Support the following features: – Thin and browser-based clients – Network security – User Authorization – Distributed deployments – Remote administration – Performance monitoring and orchestration – Coordination with other systems and services in an Oracle Database environment. – Custom embedding of Oracle GoldenGate into applications or to use secure, remote HTML5 applications.
Which databases are supported?	Classic Architecture supports all supported databases as per the **certification matrix**.	MA only supports the Oracle database.

- Preparing the Database
  Configure the Oracle Database for Oracle GoldenGatereplication.
- Setting Environment Variables
  You can set the MA-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 MA-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
```

For more information about the corresponding directories, see What are the Key Microservices Architecture Directory Directories?.

> **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
Register the Replicat	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:

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 MA 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.

ORACLE_HOME
The directory where you installed your database.

LD_LIBRARY_PATH
The library directories to your `$OGG_HOME`, OUI, database installation, and database network (`TNS_ADMIN`).

TNS_ADMIN
The directory that contains the Oracle Net Services configuration. The default is `$ORACLE_HOME/rdbms/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 enabled sharding or are using Integrated Extract or 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 MA 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. 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 check box "This non-secure deployment will be used to send trail data to a secure deployment." Check this 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. (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 Self-Signed Root Certificate,

      and Creating a Distribution Server User Certificate.
   c. 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.
   d. For your Client, select one of the options, and then provide the required information as you did for your server.
   e. Click **Next**.
9. (If Security is enabled) On the **Advanced Security Settings** page:

   The set of cryptographic algorithms used for secure communication with the Oracle GoldenGate services display. The default cipher suites are:

   - TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_RSA_WITH_AES_128_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA
- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_3DES_EDE_CBC_SHA

> **Note:**
>
> The cipher suites that are grey in color and italicized are *not* supported by your current JRE environment.

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. 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.

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. Click the + sign.
2. Enter a unique user name.
3. Select one of these roles:

   User
   Can view resources hosted by the server. This includes monitoring performance, requesting reports, and viewing resource configuration

   Operator
   Can create, update, destroy, start, pause, and stop server hosted resources in addition to User role rights

   Administrator
   Can manage and administer all services with the exception of security related configurations and profiles in addition to User and Operator role rights.

   Security
   Can administer security related objects and invoke security related service requests. This role has full rights.
4. Enter information that describes the user.
5. Enter the password twice to verify it. Passwords can contain the user name.
6. Click **Submit**.

   The user is registered

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

2.3 Creating a Self-Signed Root Certificate

In a secure mode, communication with Oracle GoldeGate SA including administrative calls and data transport is secured using SSL/TLS certificates, which you purchase or create your own for testing purposes.

You may apply your existing root certificate or use the `orapki` in the `OGG_HOME/bin` directory, see About the orapki Utility in the *Oracle Database Security Guide*.

Here's an example of how you can create a root certificate using `orapki`:

1. Create a directory to store your wallets and certificates. For example, `~/wallet_directory`.

2. Create an automatic login wallet. This example uses `root_ca` for the wallet name.

   ```
   orapki wallet create -wallet ~/wallet_directory/root_ca -auto_login -pwd
   welcome123
   ```

3. Create a new self-signed (root user) certificate and add it to the wallet.

   ```
   orapki wallet add -wallet ~/wallet_directory/root_ca -dn "CN=RootCA" -keysize
   2048 -self_signed -validity 7300 -pwd welcome123
   ```

4. Export the certificate to a `.pem` file.

   ```
   orapki wallet export -wallet ~/wallet_directory/root_ca -dn "CN=RootCA" -cert ~/
   wallet_directory/rootCA_Cert.pem -pwd welcome123
   ```

The wallet creation is complete.

2.4 Creating Server Certificates

You must make sure that your Oracle GoldenGate SA implementation has a clear guideline for security certificates, before you go into production. For testing purposes, however, you can generate server certificates.

You must create a wallet with a server certificate for each server on which you installed Oracle GoldenGate SA. Each server certificate is signed with the root certificate. This provides a common trust point because the server considers any certificate signed by the same root certificate as the server's certificate authentication.

To create the certificate, use the `orapki` in the `OGG_HOME/bin` directory. For more information about `orapki`, see About the orapki Utility in the *Oracle Database Security Guide*.

The following steps are an example of how you can create a sever certificate using a root certificate named `root_ca`. In addition, `servername` must be replaced with the actual name of the server where you installed Oracle GoldenGate:

1. Create a directory to store your wallets and certificates. For example, `~/wallet_directory`.
2. Create an automatic login server wallet.

   ```
   orapki wallet create -wallet /wallet_directory/servername
   ```

   Enter the password for the server when prompted.

3. Add a Certificate Signing Request (CSR) to the server's wallet.

   ```
   orapki wallet add -wallet /wallet_directory/servername -dn "CN=servername" -
   keysize 2048
   ```

4. Export the CSR to a `.pem` file.

   ```
   orapki wallet export -wallet /wallet_directory/servername -dn "CN=servername" -
   request /wallet_directory/servername_req.pem
   ```

5. Using the CSR, create a signed server or client certificate and sign it using the root certificate. Assign a unique serial number to each certificate.

   ```
   orapki cert create -wallet ~/wallet_directory/root_ca -request ~/
   wallet_directory/servername_req.pem -cert ~/wallet_directory/servername_Cert.pem
   -serial_num 20 -validity 375
   ```

6. Add the root certificate into the client's or server's wallet as a trusted certificate.

```
orapki wallet add -wallet ~/wallet_directory/servername -trusted_cert -cert ~/
wallet_directory/rootCA_Cert.pem
```

7. Add the server or client certificate as a user certificate into the client's or server's wallet.

```
orapki wallet add -wallet ~/wallet_directory/servername -user_cert -cert ~/
wallet_directory/servername_Cert.pem
```

The wallet creation is complete.

2.5 Creating a Distribution Server User Certificate

To replicate data to an SSL/TLS secured target Oracle GoldenGate MAdeployment, you must create a wallet with a client certificate for the Distribution Server. This certificate is also signed by the root certificate. It provides a common trust point because the server considers any certificate signed by the same root certificate as the server's certificate authentication.

To create the certificate, use the `orapki` in the `OGG_HOME/bin` directory. For more information about `orapki`, see About the orapki Utility in the *Oracle Database Security Guide*.

The following steps are an example of how you can create a distribution sever user certificate:

1. Create a directory to store your wallets and certificates. For example, `~/wallet_directory`.
2. Create an automatic login client wallet. This example uses `dist_client` for the wallet name.

```
orapki wallet create -wallet ~/wallet_directory/dist_client -auto_login -pwd
welcome123
```

3. Add a CSR to the wallet.

```
orapki wallet add -wallet ~/wallet_directory/dist_client -dn "CN=dist_client" -
keysize 2048 -pwd welcome123
```

4. Export the CSR to a `.pem` file.

```
orapki wallet export -wallet ~/wallet_directory/dist_client -dn "CN=dist_client"
-request ~/wallet_directory/dist_client_req.pem -pwd welcome123
```

5. Using CSR, create a signed server or client certificate and sign it using the root certificate. Assign a unique serial number to each certificate.

```
orapki cert create -wallet ~/wallet_directory/root_ca -request ~/
wallet_directory/dist_client_req.pem -cert ~/wallet_directory/
dist_client_Cert.pem -serial_num 30 -validity 375 -pwd welcome123
```

6. Add the root certificate as a trusted certificate into the client's or server's wallet.

```
orapki wallet add -wallet ~/wallet_directory/dist_client -trusted_cert -cert ~/
wallet_directory/rootCA_Cert.pem -pwd welcome123
```

7. Add the server or client certificate as a user certificate into the client's or server's wallet.

```
orapki wallet add -wallet ~/wallet_directory/dist_client -user_cert -cert ~/
wallet_directory/dist_client_Cert.pem -pwd welcome123
```

The wallet creation is complete.

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 MA installation, you must then create a new deployment using the Configuration Assistant. You can use this wizard to add multiple deployments to one Service Manager. So, you only have to upgrade the one Service Manager with new releases or patches.

Topics:

3.1 How to Connect to a Service Manager

You can select the Service Manager as a daemon service that enables you to control all other services in MA and run as a system service, while creating a deployment.

> **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.

Check that the Service Manager is Running

You must ensure that the Service Manager is running before you connect to it. To start a Service Manager:

1. On a Linux platform, type:

```
cd $OGG_HOME/bin
```

2. Run the command:

```
./ServiceManager
```

Login to Service Manager

To start using Oracle GoldenGateMA, you have to connect to Service Manager:

1. Open a web browser and connect to the Service Manager that you created with the 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 click Sign In.

In the Service Manager, you can see that the other services 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
- Quick Tour of the Service Manager Home Page
  When you complete the Oracle GoldenGate MA installation, the Service Manager Home page 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

3.1.1 How to Start and Stop the Service Manager

You can run scripts to start and stop the Service Manager in Oracle GoldenGate Microservices Architecture. Run the scripts from the following locations:

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

3.1.2 Quick Tour of the Service Manager Home Page

When you complete the Oracle GoldenGate MA installation, the Service Manager Home page 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.

3.2 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 (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 the deployment using the `oggca` program.

By removing a deployment, you get to 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 MA, 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**.

Files to be Removed Manually After Removing Deployment

It's mandatory to delete some files manually only in case there's a Service Manager registered but you have to unregister it and register a new one. To remove files manually, you must have `root` or `sudo` privileges. The files to be deleted include:

Operating System	Files to be Removed Manually to Unregister an Existing Service Manager
Linux 6	• `/etc/init.d/OracleGoldenGate` • `/etc/rc.d/*OracleGoldenGate` • `/etc/rc*.d/*OracleGoldenGate` • `/etc/oggInst.loc`
Linux 7	`/etc/systemd/system/OracleGoldenGate.service`

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
Config Force	Forces the configuration data.
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 Replications

You can perform all data replication tasks from the Administration Server home page. You can, add Extracts and Replicats and start the distribution path, once your deployments are created.

Topics:

- Quick Tour of the Administration Service Home Page
  When you click the Administrator Service link on the Service Manager home page, the login page for the Administration Service is displayed. After logging in, you're taken to the Administration Service Home page. You can use this page to configure Extract and Replicat processes.
- How to Add a Database Credential
  To create and run Extracts, you must first set up and test database credentials.
- How to Add Extracts
  To create and run Extracts, you must first set up database credentials. Once the Extract is running, you can monitor checkpoint table, and the Extract report from the Administration Server.
- How to Add Replicats
  You can add Replicats for the target deployment from 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.
- How to Access the Parameter Files
  The Global parameters, Extract, Replicat parameter files are available in the Parameter Files section of the Administration Server.
- 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 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 in Microservices Architecture
  Oracle GoldenGate MAusers can be created from the Administration Server, once you log in using the credentials created at the time of configuring the deployment.
- Connecting Microservices Architecture to Classic Architecture
  To successfully link Oracle GoldenGate Microservices Architecture and Classic Architecture, ensure that the Distribution Service knows where to place the remote trail file for reading.

4.1 Quick Tour of the Administration Service Home Page

When you click the Administrator Service link on the Service Manager home page, the login page for the Administration Service is displayed. After logging in, you're taken to the Administration Service Home page. You can use this page to configure Extract and Replicat processes.

The Administration Service Home page is used to add Extracts and Replicats and view the current state of them. 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 Service 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
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 Extracts, you must first set up and test database credentials.

1. Launch the Administration Server interface.
2. Log in to the server.
3. Click the **Application Navigation** icon in the upper left of the Administration Server.
4. Select **Configuration** from the exposed left pane.
5. Click the **+** sign next to Credentials, and set up your new credential alias, then click **Submit**.
6. 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 How to Add Extracts

To create and run Extracts, you must first set up database credentials. Once the Extract is running, you can monitor checkpoint table, and the Extract report from the Administration Server.

1. Launch the Administration Server interface.
2. Log in to the server.
3. Click the **Application Navigation** icon in the upper left of the Administration Server.
4. Select **Configuration** from the exposed left pane.
5. Click the **+** sign next to Credentials, and set up your new credential alias, then click **Submit**.
6. 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.
7. Click **+** to add your Extract.
8. 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.
9. 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:

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

Option	Description	Extract Type
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
Log Retention	Set to retain the Extract logs.	Classic

10. Click **Next**.
11. 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.
12. 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. You can select the **Action** list to look at Details of the Extract, such as process information, checkpoint, statistics, parameters, and report.

    See Using Extract Actions.

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

4.3.1 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.

4.4 How to Add Replicats

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. Click **Create and Run** to create and run the Replicat or **Create** to run the created Replicat later.

   You can select **Register Replicat in the background** to speed the Replicat creation.

   You are returned to the Overview page of the Administration Server. You can select the **Action** list to look at Details of the Replicat, such as the report file, statistics, and parameters.

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

4.4.1 Creating a Parallel Replicat

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

A parallel Replicat requires a checkpoint table so both the Administration Server UI and Admin Client issue an error when the parallel Replicat does not include a checkpoint table.

> **Note:**
>
> Parallel Replicat in Integrated Mode does not support `COMMIT_SERIALIZATION`.

Creating a Non-Integrated Parallel Replication 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 http://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

4.4.1.1 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 *.*;
```

4.4.2 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.

4.5 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.

Starting an Administration Service Task

You can set up various automated operations for Administration Service tasks, such as purging, load balancing, and failover support. To set up this operation:

1. Select **Configuration** from the left navigation pane of the Administration Service.
2. Select the **Maintenance** tab.

3. Enter the **Operation Name** for the Administration Service task in the **Create New Auto Start Task** section.
4. Select **Enabled** to keep the task active.
5. Enter the process name associated with the task that you need to perform and click **Submit**.

Restarting an Administration Service Task

Auto Restart allows you to automatically restart a process that has abended. It enables you to configure the number of retries to attempt restart and set the delay parameter as well.

You can configure these options from the Auto Restart page on the Maintenance tab.

1. Select **Auto Restart**.
2. Enter the Administration Service task name in the **Operation Name** field.
3. Keep the Enabled setting ON to ensure that the operation is active.
4. Enter the Oracle GoldenGate process name, such as `START EXTRACT` or `STOP REPLICAT`, associated with the task.
5. Specify the Delay time to attempt restarting the task.
6. Enter the maximum number of retries to attempt restarting the task. You can choose to enable the option to **Disable Task After All Retries**, to disable auto restart attempts after exhausting the number of retries.
7. Click **Submit**.

   The new task is displayed in the Auto Restart task table.
   You can edit or delete a task from the table also, using the Delete and Edit icons for the corresponding task in the table.

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 Maintenance 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.
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 must 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.

Purging Tasks

You can automatically purge processes associated with an Administration Service.

From the Maintenance tab, use the Purge Tasks page.

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.

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. .

4.6 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.

4.7 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.

4.8 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.

4.9 How to Create Users in Microservices Architecture

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

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.

4.10 Connecting Microservices Architecture to Classic Architecture

To successfully link Oracle GoldenGate Microservices Architecture and Classic Architecture, ensure that the Distribution Service knows where to place the remote trail file for reading.

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

> **Note:**
>
> For this procedure to work, an existing Extract must be running in Microservices Architecture.

1. Go to the Distribution Server home page from the Service Manager home page.
2. Add the Distribution Path using steps given in How to Add a New Path.
3. In Classic Architecture, start Manager using the steps provided in Starting Manager.
4. Create and start Replicat using steps given in Creating the Replicat Group.

5
Working with Paths

The path between a source and target deployment can be set using the Distribution 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 .
- 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.

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
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. From the Service Manager, click **Distribution Server**.
2. Click the plus (+) sign next to Path.

   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.
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.
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*

Options	Description
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.
Use Basic Authentication	Select to add a credential to the target URI creating basic MA authentication.
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.
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.

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.
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.

Additional Options	Description
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 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.
- `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.

5.4 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.

5.5 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.
Chunk ID	Edit or delete the database shard settings if sharding is used.

Option	Description
Object Type:	Edit or delete the type of object for the rule.

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 provides steps to perform the tasks required 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.
- Monitoring Paths
  You can monitor the path statistics from the Receiver Server.
- Tuning Network Parameters
  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.

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 Monitoring Paths

You can monitor the path statistics from the Receiver Server.

To monitor path statistics:, visit 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. From Service Manager, click **Receiver Server**.
2. Click **Action**, **Details.**

   The Process Information page is displayed. You can constantly monitor the activity of the path on the Process Information page. 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.

6.3 Tuning Network Parameters

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.

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

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

   The Process Information page is displayed. This page displays Advanced Options.

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.

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 Changestab 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.

3. Scroll through the list of messages or search for a specific message by entering the text in the message. Click **Refresh** to get a synchronized real-time list of messages before you start searching.

   You can 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.

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.

8.1 Oracle GoldenGate With a Sharded Database

Oracle GoldenGate provides a cohesive platform for a sharded Oracle Database.

Sharding is only available with Oracle Database 12.2.0.1 or later, over a secure MA 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).
- Install at least one Oracle GoldenGate MAinstance for the catalog and each of the shards.
- Generate Oracle GoldenGate MAserver 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 MAservers 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 <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 Administrator's 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 MA Servers to accomplish control and configuration tasks in an Oracle GoldenGatedeployment.

Admin Client is used to create, modify, and remove processes, rather than using MA. It's not used by MA services such as the Administration, Distribution and other servers. For example, you can either use Admin Client to execute all the commands necessary to create an Extract or customize a new Extract application, or use the Administration Server available with MA to configure an Extract.

> **Note:**
>
> Ensure that the `OGG_HOME`, `OGG_VAR_HOME`, and `OGG_ETC_HOME` are set up correctly in the environment.

For more information on environment variables, see Setting Up the Environment Variables.

To run Admin Client:

1. Set the environment variables: `OGG_HOME`, `OGG_ETC_HOME`, `OGG_VAR_HOME`.
2. Move to `$OGG_HOME/bin` and run the command:

```
[oracle@bigdatalite bin]$ ./adminclient
Oracle GoldenGate Administration Client for Oracle
Version 18.1.0.0.0 OGGCORE_18.1.0.0.0_PLATFORMS_yymmdd.HHMM_FBO

Copyright (C) 1995, 2018, 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>
```

   You can view the full list of Admin Client commands using the `HELP` command.

3. Connect only to the Service Manager from Admin Client.

   Connect to the `https://localhost:<service_manager_port>` source deployment using the administrator credentials.

> **Important:**
>
> You must use http or https in the connection string or the Admin Client will not connect. In the given example, a non-SSL connection is used.

If you use `DBLOGIN`, you have to use the `USERIDALIAS` because you cannot use the `USERID`.

By default, Admin Client does not allow connecting to a server through HTTPS when the server certificate is invalid. To override this behavior, use the `!` modifier with the `CONNECT` command. For example, when using the Admin Client to connect to the Oracle GoldenGate Microservices Architecture services that are secured with a self-signed SSL certificate, you must use a command with the `!` modifier:

```
CONNECT http://myserver.example.org as oggadmin !
```

If you enter an incorrect deployment name, a list of deployments is displayed. Depending on the option you choose to connect to a deployment with the Admin Client, different outputs are generated, as explained in the following scenarios:

- When you connect without using the deployment name, the default deployment is connected and displayed in the output. .

  For example:

  ```
  OGG (not connected) 1>  connect https://localhost:9000 as admin password
  adminpw
  Using default deployment 'D1'
  ```

  In this example, `D1` is the name of the deployment.

- When the connection occurs with the deployment, the Admin Client connects to the deployment but doesn't provide the deployment name in the output.

  For example:

  ```
  OGG (not connected) 1> connect https://localhost:9000 deployment D1 as admin
  password adminpw
  ```

  The command is successful but without any output.

- When you connect to the deployment with the deployment name and user name but without the password, then Admin Client doesn't display the output but waits for the password.

  For example:

  ```
  OGG (not connected) 1>  connect https://localhost:9000 deployment D1 as admin !
  Password for 'admin' at 'https://localhost:9000':

  OGG (https://localhost:9000D1) 2>
  ```

B

Connecting Microservices Architecture to Classic Architecture

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

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

> **Note:**
>
> For this procedure to work, an existing Extract must be running in Microservices Architecture.

Task 1: Add a Distribution Path

1. From the Service Manager, click **Distribution Server**.
2. Click the plus (+) sign next to Path. The Add Path page is displayed.
3. Enter the details:

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

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*
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.
Use Basic Authentication	Select to add a credential to the target URI creating basic MA authentication.
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.
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.

Options	Description
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.

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

Rule Configuration	Description
	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.
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 Architecture.

Follow these steps for establishing a connection betweenOracle GoldenGate Microservices Architecture 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.