Oracle® Database

Step by Step Data Replication Using Oracle GoldenGate Microservices Architecture

21c (21.1.0)
F25739-02
May 2021

Oracle Database Step by Step Data Replication Using Oracle GoldenGate Microservices Architecture, 21c (21.1.0)

F25739-02

Primary Author: Oracle Corporation

Contents

Preface

Audience vi
Documentation Accessibility vi
Related Information vi
Conventions vii

1 Preparing for Oracle GoldenGate Microservices

1.1 Preparing the Database 1-1
1.2 Setting Environment Variables 1-1

2 Setting Up Secure or Non-Secure Deployments

2.1 How to Add Secure or Non-Secure Deployments 2-1
2.1.1 How to Create Different Types of Certificates for a Secure Deployment 2-8
2.1.1.1 Creating a Self-Signed Root Certificate 2-8
2.1.1.2 Creating Server Certificates 2-9
2.1.1.3 Creating a Client Certificate 2-9
2.1.1.4 Setting Up Trusted Certificates 2-10
2.2 How to Remove a Deployment 2-11
2.2.1 How to Remove a Deployment: GUI 2-12
2.2.2 How to Remove a Deployment: Silent Mode 2-13

3 Working with Service Manager

3.1 How to Use the Service Manager 3-1
3.1.1 Quick Tour of the Service Manager 3-2
3.1.2 How to Start and Stop Service Manager and Deployments 3-3
3.1.3 View and Edit the Configuration for MA Servers 3-4
3.1.4 How to Change Deployment Details and Configuration 3-5
3.1.5 How to Enable and Use Debug Logging 3-6
3.1.6 How to Interpret the Log Information 3-6
3.1.7 How to Add and Manage Certificates for the Deployment 3-6

3.1.8 How to Add Users 3-7

4 Working with Data Replication

4.1 Quick Tour of the Administration Server Home Page 4-2
4.2 How to Add a Database Credential 4-3
4.2.1 Using Kerberos Authentication with MA 4-3
4.2.1.1 Example: Using USERIDALIAS in Parameter File for Kerberos Account 4-4
4.2.2 Configuring Kerberos Authentication 4-5
4.3 How to Create Users from the Administration Server 4-6
4.4 Before Creating an Extract 4-6
4.5 How to Add Extracts 4-7
4.5.1 How to Add an Initial Load Extract 4-11
4.5.2 Using Extract Actions 4-11
4.6 Before Creating Replicat 4-13
4.7 How to Add a Replicat 4-13
4.7.1 Creating a Parallel Replicat 4-14
4.7.1.1 Basic Parameters for Parallel Replicat 4-15
4.7.2 Using Replicat Actions 4-16
4.8 How to Use the Master Keys and Encryption Keys 4-18
4.9 How to Access the Parameter Files 4-18
4.10 Setting Up Automated Tasks 4-19
4.11 Review Critical Events 4-21
4.12 How to Configure Encryption Profile 4-21
4.13 How to Configure Managed Processes 4-22
4.14 How to Access Extract and Replicat Log Information 4-23

5 Working with Paths

5.1 Quick Tour of the Distribution Server Home Page 5-1
5.2 How to Add a Distribution Path 5-2
5.3 How to Add a Target-Initiated Distribution Path 5-7
5.4 Using the Path Actions 5-13
5.5 Repositioning a Path 5-14
5.6 Changing Path Filtering 5-14
5.7 Reviewing the Distribution Server Path Information 5-16

6 Working with Trails

6.1 Quick Tour of the Receiver Server Home Page 6-1
6.2 Tuning Network Parameters 6-1

6.3 Reviewing the Receiver Server Path Information 6-2
6.4 Monitoring Paths 6-2

7 Monitoring Performance

7.1 Quick Tour of the Performance Metrics Server Home Page 7-1
7.2 Monitoring Server Performance 7-2
7.3 Reviewing Messages 7-3
7.4 Review Status Changes 7-3
7.5 How to Purge the Datastore 7-4

A About Target-Initiated Paths

B Integration with Reverse Proxy

Preface

The *Step by Step Data Replication Using Oracle GoldenGate Microservices Architecture* is a walk through the entire Oracle GoldenGate data replication cycle using Microservices.

- Audience
- Documentation Accessibility
- Related Information
- Conventions

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Accessible Access to Oracle Support

Oracle customers who have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Information

The Oracle GoldenGate Product Documentation Libraries are found at:

https://docs.us.oracle.com/en/middleware/goldengate/core/21.1/

The Oracle GoldenGate related product documentation libraries are found at:

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

For additional information on Oracle GoldenGate, refer to:

https://www.oracle.com/middleware/technologies/goldengate.html

https://www.oracle.com/database/technologies/high-availability/oracle-database-maa-best-practices.html

For licensing information, refer to Licensing Information in the *Oracle GoldenGate Licensing Information* guide.

Conventions

The following text conventions are used in this document:

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

1 Preparing for Oracle GoldenGate Microservices

Learn about the tasks to perform for setting up and using Oracle GoldenGate microservices.

This guide assumes that you have already completed installation Oracle GoldenGate Microservices Architecture.

Topics:

- Preparing the Database
  Configure the database for Oracle GoldenGate replication.
- Setting Environment Variables
  You can set the Microservices-specific environment variables while performing the deployment tasks:

1.1 Preparing the Database

Configure the database for Oracle GoldenGate replication.

To prepare your database for Oracle GoldenGate, ensure that your database meets the requirements as outlined in *Installing Oracle GoldenGate* , *Using Oracle GoldenGate for Oracle Database* and *Using Oracle GoldenGate for Heterogeneous Databases* guides.

1.2 Setting Environment Variables

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

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

From Oracle GoldenGate 21c onwards, the options to set up the environment variables have changed:

> **Note:**
>
> `ORACLE_HOME` and `LD_LIBRARY_PATH` do not point to any database directories. With the unified build feature, these environment variables now point to the `OGG_HOME` (sub)directories as the Oracle Database Client Software is embedded in Oracle GoldenGate.

ORACLE_HOME
You don't need to set this variable as it is set to a fixed location.

OGG_HOME

```
export OGG_HOME=ogg_install_location
```

LD_LIBRARY_PATH
The variable will be set to a fixed location although you can change it if required. Before running Oracle GoldenGate on Linux, Solaris, and HP-UX, `LD_LIBRARY_PATH` must include the directories of the Oracle GoldenGate shared libraries and Oracle Instant Client shared libraries.
For Microservices Architecture, `LD_LIBRARY_PATH` must include the Oracle GoldenGate `lib` directory and its `instantclient` subdirectory, as shown in the following example:

> **Note:**
>
> The `instantclient` subdirectory is only applicable for Oracle database.

```
LD_LIBRARY_PATH = $OGG_HOME/lib:$OGG_HOME/lib/instantclient
```

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

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

TNS_ADMIN
(Valid for Oracle only) This variable points to the directory where the SQL*Net configuration files (like `sqlnet. ora` and `tnsnames. ora`) are located.

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

It is recommended (but not required) to set the environment variable `$TNS_ADMIN`. If this environment variable is not set, Oracle GoldenGate looks for `$HOME/.tnsnames.ora` or `/etc/tnsnames.ora`. In addition to this, the environment variable must be set before starting the Admin Client or GGSCI prompt, otherwise, this variable is not caught.

PATH

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

OGG_ETC_HOME
Specifies the location of the `/etc` directory for the Service Manager deployment. This variable is required when you don't register the Service Manager as a system daemon.

OGG_VAR_HOME
Specifies the location /var directory for the Service Manager deployment. This variable is required when you don't register the Service Manager as a system daemon.

> **Note:**
>
> The `OGG_ETC_HOME` and `OGG_VAR_HOME` environment variables are required to start and stop the Service Manager manually as the `startSM.sh` and `stopSM.sh` scripts are located in these directories.

JAVA_HOME
This is an additional environment variable, which is required during installation and patching:

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

See Components of Oracle GoldenGate Microservices Architecture.

IBM CLI DRIVER
See Setting up for DB2 in the Using Oracle GoldenGate on Oracle Cloud Marketplace for details. You need to set this variable to ensure that the Administration Server is up and running after you set up your deployment on Oracle Cloud Marketplace. Also see, Setting up Environment Variables for Db2 z/OS.

TZ
Valid for MySQL.
This variable is used to set the time zone of the Oracle GoldenGate deployment to that of the source MySQL database and is required when capturing columns that contain `TIMESTAMP` data and the database server and Oracle GoldenGate server are in different time zones.

2
Setting Up Secure or Non-Secure Deployments

You can choose to set up a secure or non-secure deployment but whatever type you choose, all subsequent deployments of the same Service Manager must be of the same security type and cannot be changed afterwards.

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 own existing business cerificate from your Certificate Authority (CA) or you might create your own certificates.

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 wss, ogg, and ws protocols.

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

Topics:

- How to Add Secure or Non-Secure Deployments
  Adding deployments is the first task in the process of setting up a data replication platform. Deployments are managed from the Service Manager.
- How to Remove a Deployment
  You can remove a deployment using OGGCA or in silent mode.

2.1 How to Add Secure or Non-Secure Deployments

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

After completing the Oracle GoldenGate Microservices installation, you can add 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.

Use OGGCA to add multiple deployments to a Service Manager. This allows 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.

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 create a new one. In most configurations, you only have one Service Manager that is responsible for multiple deployments.

   b. For a new Service Manager, enter or browse to the directory that you want to use for your deployment. Oracle recommends that you create a `ServiceManager` directory within the deployment sub-directory structure to store the Service Manager files.

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

   d. Enter a unique port number that the Service Manager will listen on, or choose the port already in use if selecting an existing Service Manager.

   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. This is available for Oracle database only.) 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.

   You can only add or remove one deployment for one Service Manager at a time.

   > **Note:**
   >
   > Ensure that your Service Manager is up and running prior to launching OGGCA.

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 (‘.’). The name before the / symbol should be "slash" or "forward slash".
- Cannot be “ServiceManager”.

b. (Oracle Database only) 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 directory. If you have set the `$OGG_HOME` environment variable, the directory is automatically populated. Otherwise, the parent directory of the `oggca.sh` (Linux) or `oggca.bat` (Windows) 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 create a separate directory for easier upgrades. The additional fields are automatically populated based on the specified deployment directory.

> **Note:**
>
> The deployment directory name (user deployment directory) needs to be different than the directory name chosen in the first screen (Service Manager deployment directory).

b. You can customize the deployment directories so that they are named and located differently from the default.

c. Enter or select different directories for the various deployment elements.

d. Click **Next**.

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

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

OGG_HOME

The directory where you installed Oracle GoldenGate. This variable is fixed and cannot be changed.

> **Note:**
>
> On a Windows platform, ensure that there's no space in the `OGG_HOME` directory path otherwise OGGCA will not run.

IBMCLIDRIVER
DB2 zOS only. Specifies the location where the IBM Data Server Driver for ODBC and CLI (IBMCLIDRIVER) software is installed.

LD_LIBRARY_PATH
This variable is used to specify the path to search for libraries on UNIX and Linux. It may have a different name on some operating systems, such as `LIBPATH` on IBM AIX on POWER Systems (64-Bit), and `SHLIB_PATH` on HP-UX. This path points to the Oracle GoldenGate installation directory and the underlying instant client directory by default. It might be extended if `USER EXITS` are in use.

TNS_ADMIN
This variable points to the directory location containing `tnsnames.ora`, which has the database connection details. This variable is optional.

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

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

Click **Next**.

7. On the **Administrator Account** page:
   a. Enter a user name and password that you want to use to sign in to the Oracle GoldenGate Microservices Service Manager and the other servers. This user is the security user for this deployment. Select the **Enable strong password policy in the new deployment** checkbox to ensure setting a highly secure password for your user account. The strong password policy has the following requirements:
      - At least one lowercase character [a...z]
      - At least one upposercase character [A...Z]
      - At least one digit [0...9]
      - At least one special character [- ! @ % & * . #]
      - The length should be between 8 and 30 characters.

      For details on the different types of users, see How to Add Users. If you are using an existing Service Manager, you must enter the same log in credentials that were used when adding the first deployment.
   b. Select the check box that allows you to enable a strong password policy for your new deployment. If you select this option, then the password must adhere to restrictions, otherwise an error occurs, which requires you to specify a stronger password.
   c. Click **Next**.
8. On the **Security Options** page:
   a. You can choose whether or not you want to secure your deployment. Oracle recommends that you enable SSL/TLS security.

      If you do not want to use security for your deployment, deselect the check box.

When you deselect the SSL/TLS check box, the option **This non-secure deployment will be used to send trail data to a secure deployment** appears. Select this check box if the non-secure target deployment is meant to communicate with a secure source deployment.

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

b. Also see: About Target-Initiated Paths.

c. (Optional) You can specify a client wallet location so that you can send trail data to a secure deployment. This option is useful when Distribution Server from the source deployment is unsecured whereas the Receiver Server on the target deployment is secured. So, the sender may be configured for public access while the Receiver Server requires authentication and authorization, which is established using PKI before the incoming data is applied.

For more information, see How to Create Different Types of Certificates for a Secure Deployment.

d. For your Server, select one of the options, and then provide the required file locations. When using an existing wallet, it must have the appropriate certificates already imported into it. If you choose to use a certificate, enter the corresponding pass phrase.

When using a self-signed certificate, a new Oracle Wallet is created in the new deployment and these certificates are imported into it. For certificates, enter the location of the private key file and the pass phrase. The private key files must be in the `PKCS#8` format.

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

f. Click **Next**.

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

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

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

```
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
```

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

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

c. Click **Next**.

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

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

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

    b. Enter a unique name for the certificate.

    c. Click **Next**.

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

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

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

    c. Click inside the Performance Metrics Server port fields to populate or enter the ports you want to use. Ensure that you choose available ports for TCP.

    Select the UDP port for performance monitoring. The option to select the UDP port is displayed only with deployments on Windows and other operating systems that don't support UDS communication with Performance Metric Server. See Supported Operating Systems for UDS.

    You can change the TCP port from the Service Manager console after the deployment is done. For more information on `PMSRVR`, see `ENABLEMONITORING`.

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

    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 validates whether or not the port you entered is currently in use or not.

12. In the **Replication Settings** step:
    a. Enter the Oracle GoldenGate default schema that you want to use to perform the replication settings. For example, `ggadmin`.

    > **Note:**
    >
    > OGGCA does not connect to the database, so it cannot validate the schema. The schema specified in OGGCA is written to the GLOBALS file as a default schema. When creating an Extract, if you do not specify a replication schema, Extract will use that default schema.

    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. Oracle recommends that you save the 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 exit the Configuration Assistant.

- How to Create Different Types of Certificates for a Secure Deployment
  Here's how you can create client and server certificates to set up a secure Oracle GoldenGate Microservices Architecture deployment:

2.1.1 How to Create Different Types of Certificates for a Secure Deployment

Here's how you can create client and server certificates to set up a secure Oracle GoldenGate Microservices Architecture deployment:

Topics:

- Creating a Self-Signed Root Certificate
- Creating Server Certificates
- Creating a Client Certificate
- Setting Up Trusted Certificates
  There are two types of TLS connections. To use TLS, there are certain requirement for the certificate trust chain.

2.1.1.1 Creating a Self-Signed Root Certificate

You may apply your existing root certificate or use the `orapki` in the `OGG_HOME/bin` directory.

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. In the `orapki` command to create self-signed (root user) certificate, specify the `-sign_alg sha256` option.
4. In `orapki` wallet:

   ```
   add -wallet ~/wallet_directory/root_ca -dn "CN=RootCA" -keysize
   2048 -self_signed -validity 7300 -pwd welcome123 -sign_alg sha256
   ```

5. 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.

2.1.1.2 Creating Server Certificates

The following steps are an example of how you can create a sever certificate using a root certificate named `root_ca`.

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/$(hostname) -
   auto_login -pwd welcome123*
   ```

   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/$(hostname) -dn "CN=$
   (hostname)" -keysize 2048 -pwd welcome123
   ```

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

   ```
   orapki wallet export -wallet ~/wallet_directory/$(hostname) -dn
   "CN=$(hostname)" -request ~/wallet_directory/servername_req.pem -
   pwd welcome123
   ```

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  -sign_alg sha256
   ```

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

   ```
   orapki wallet add -wallet ~/wallet_directory/$(hostname)
   -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/$(hostname) -user_cert
   -cert ~/wallet_directory/servername_Cert.pem  -pwd welcome123
   ```

The wallet creation is complete.

2.1.1.3 Creating a Client Certificate

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.

2.1.1.4 Setting Up Trusted Certificates

There are two types of TLS connections. To use TLS, there are certain requirement for the certificate trust chain.

The `wss` communication protocol is used in the Distribution Server for the Distribution Path to meet the needs of secure communication using TLS in Oracle GoldenGate Microservices Architecture.

Distribution Server and Receiver Server

Both the Distribution Server and Receiver Server need certificates. The Distribution Server uses the certificate in the client wallet location under outbound section. The

location of that wallet can be found in the `deploymentConfiguration.dat` file under *`deployment_home`*`/etc/conf`.

The certificates in both wallets need to be trusted by each other, so either both need to have commercial certificates issued by Classic Architecture, or they have to trust each other for self-signed certificates.

For self-signed certificates, you can choose from one of the following:

- Have both certificates signed by the same root certificate. (`rootCA`)
- The other side's certificate is added to the local wallet as a trusted certificate

For the Receiver Server, the certificate is in the wallet for the local wallet location, which is also in the `deploymentConfiguration.dat` file.

On the Distribution Server, if the hostname used in the Receiver Server's certificate can't be routed correctly, `/etc/hosts` file should be updated with the correct IP address for that host. The Distribution Server will use this IP address to communicate with the Receiver Server once it accepts the certificate from the Receiver Server.

Using the Reverse Proxy (Nginx) with the Distribution Server and Receiver Server

You only need to add the Nginx certificate to the Distribution server's client wallet as a trusted certificate. Usually the certificate used by Nginx is self-signed. If it is issued by Classic Architecture, then there is no need to perform this step.

The host name in the Nginx certificate should also be routable. If not, on the Distribution Server, `/etc/hosts` file needs to be updated to reflect the correct IP address for that host name.The Distribution Server will use the host name in the certificate to communicate to the target. If the Nginx certificate doesn't have a valid host name in it, but has a Subject Alternative Name record, then the host name is the DNS name there.

2.2 How to Remove a Deployment

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

Topics:

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

2.2.1 How to Remove a Deployment: GUI

You can remove a deployment using the Oracle GoldenGate Configuration Assistnat wizard.

To remove a deployment:

> **Note:**
>
> When you remove a deployment or uninstall Oracle GoldenGate Microservices, the system does not automatically stop processes. As a result, you may have to stop processes associated with the deployment and you must clean files manually.

1. Run the Oracle GoldenGate Configuration Assistant wizard:

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

To remove a Service Manager:

1. Run Oracle GoldenGate Configuration Assistant wizard:

   ```
   $OGG_HOME/bin
   ```

2. Select **Existing Service Manager** from the **Select Service Manager Options** screen. Click **Next**.
3. If there are no other deployments to remove, then the option to remove the Service Manager is available in the drop down. Select **Remove Service Manager Deployment** from the Configuration Options screen.
4. Click **Finish**.

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`

The following commands are executed to stop the Service Manager:

```
systemctl stop OracleGoldenGate
systemctl disable OracleGoldenGate *
```

> **Note:**
>
> If the Service Manager is not registered as a service (with or without the integration with XAG), OGGCA stops the Service Manager deployment, otherwise, a script called `unregisterServiceManager` is created, and when executed by the user, it runs the `systemctl` commands and deletes the mentioned files.

2.2.2 How to Remove a Deployment: Silent Mode

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

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

To remove a deployment silently:

> **Note:**
>
> If the Service Manager is registered as a system service, removing a deployment silently will not unregister the service.

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

```
CONFIGURATION_OPTION=REMOVE
ADMINISTRATOR_PASSWORD=********
CREATE_NEW_SERVICEMANAGER=false
DEPLOYMENT_NAME=deployment_name
REMOVE_DEPLOYMENT_FROM_DISK=true
```

In case of multiple deployments, you must specify the deployment name using the `DEPLOYMENT_NAME` field. You can use the `REMOVE_DEPLOYMENT_FROM_DISK` option to remove physical files and folders associated with deployment.

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

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

Example:

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

3
Working with Service Manager

After you access your Service Manager instance, you can add deployments or edit existing ones.

Oracle recommends using a secure configuration within Oracle GoldenGate Microservices.

For a secure configuration, you need to run Microservices on loopback address and front it with an HTTPS reverse proxy (nginx). See Reverse Proxy Support.

When sending trail files from Oracle GoldenGate Classic to Microservices environment that is configured with a reverse proxy, use a pump Extract from Oracle GoldenGate Classic with `SOCKSPROXY` option. When sending trail files from Oracle GoldenGate Microservices to Classic Architecture use the `ogg` protocol in the Distribution Server configuration.

Topics:

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

3.1 How to Use the Service Manager

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

The Service Manager can be configured in three different modes:

- Manually
- As a Daemon
- Integrated with XAG agent

See How to Start and Stop the Service Manager to know more.

Logging in to Service Manager

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

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

1. Open a web browser and connect to the Service Manager that you created with Oracle GoldenGate Configuration Assistant. The URL is similar to `http://host:port`, where *host* is the name of the server or IP of the server that is running the Service Manager and *port* is the port number of the Service Manager. For a secure deployment, the URL is similar to `https://localhost:9001`.
2. Enter the user name and password you created during deployment and sign in.

In the Service Manager, you can check if the Service Manager and other deployment services are up and running. Use the links to connect you to their specific interfaces, review details, and administer your deployments.
See How to Use the Admin Client to learn about connecting to the Service Manager from the Admin Client.

For more information on setting up the Service Manager as a daemon service, see How to Create Secure and Non-Secure Deployments.

- Quick Tour of the Service Manager
  This page acts as an access point for accessing the Administration Server, Distribution Server, Receiver Server, Performance Metrics Server, setting up user accounts, and manage certificates.
- How to Start and Stop Service Manager and Deployments
- View and Edit the Configuration for MA Servers
  Use the Service Manager Overview (Home) page to view and edit the configuration and restart options for Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server.
- How to Change Deployment Details and Configuration
- How to Enable and Use Debug Logging
- How to Interpret the Log Information
- How to Add and Manage Certificates for the Deployment
- How to Add Users
  Each deployment has its own list of users, and when you add users, you add them to that deployment.

3.1.1 Quick Tour of the Service Manager

This page acts as an access point for accessing the Administration Server, Distribution Server, Receiver Server, Performance Metrics Server, setting up user accounts, and manage certificates.

After configuring the Oracle GoldenGate Microservices deployment, to access the Service Manager web interface, open up the Service Manager URL and login with the user credentials you provided while setting up the deployment in OGGCA.

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.

3.1.2 How to Start and Stop Service Manager and Deployments

Starting and Stopping the Service Manager

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

- If the Service Manager is configured in manual mode then there are scripts in the `$DEPLOYMENT_HOME/servicemanager/bin` directory that you can run to start or stop the Service Manager. The `$DEPLOYMENT_HOME` is the directory where Oracle GoldenGate is installed.
  - To start the Service Manager: `$DEPLOYMENT_HOME/servicemanager/bin/startSM.sh`
  - To stop the Service Manager: `$DEPLOYMENT_HOME/servicemanager/bin/stopSM.sh`

  > **Note:**
  >
  > If you want to start or stop the Service Manager, you also have to set the `$OGG_ETC_HOME` and `$OGG_VAR_HOME` to the Service Manager sub-directories.

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

For OEL 7 and OEL 8:

```
systemctl start OracleGoldenGate

systemctl status OracleGoldenGate

systemctl stop OracleGoldenGate
```

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

Stopping and Starting Deployments and Other Microservices

> **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. Log in to your Service Manager instance as the system adminstrator.
2. In the **Deployments** section of the Service Manager home page, locate the deployment that you need to start or stop.
3. In the **Actions** column, click **Start**.
4. Verify if all the services associated with the deployment have started. An indication that the services have started is that the **Action** column automatically shows the **Stop** option. By default, all server instances are in **Running** state after the deployment process is complete.
5. To start or stop a service, such as the Administration Server or the Distribution Server, go to the Services section.
6. Identify the server (or service) that you need to start (or stop) and click start in the **Action** column, the same way you did for Deployments.

3.1.3 View and Edit the Configuration for MA Servers

Use the Service Manager Overview (Home) page to view and edit the configuration and restart options for Administration Server, Distribution Server, Performance Metrics Server, and Receiver Server.

You can access the services configuration for each of the servers, from the Service Manager home page. Click the **Details** settings icon for the server that needs to be checked for the service configuration. 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

U-Mask	File mode creation mask
Config Force	Forces using the configuration data
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.

3.1.4 How to Change Deployment Details and Configuration

You can review and change the selected service (server) configuration.

Details Tab

Use to review the selected deployment configuration. All the deployment directories that you configured with the Configuration Assistant are displayed. For Oracle database, the only directory that you can edit is the Oracle GoldenGate home (`OGG_HOME`). This allows you to use a different installation than the one you originally configured.

For SQL Server and DB2 z/OS, you need to follow the steps given in the Setting up Environment Variables for Db2 z/OS , Setting up for DB2 and Setting up for SQL Server in the *Using Oracle GoldenGate on Oracle Cloud Marketplace* guide.

> **Note:**
>
> It's important to do the settings for SQL Server and DB2 z/OS to make sure that the Administration Server starts when using either of these databases.

Configuration Tab

Use to review and change the selected deployment environment variables. The environment variables that you configured for your deployment are displayed. You van add new variables, modify existing variables, and delete selected variables.

Certificates

Use this tab to manage certificates for client and CA certificates. See How to Add and Manage Certificates for the Deployment for details.

3.1.5 How to Enable and Use Debug Logging

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

Enabling Debug Logging:

To enable debug logging:

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

Using the Debug Log

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

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

.

3.1.6 How to Interpret the Log Information

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

Using the Table

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

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

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

3.1.7 How to Add and Manage Certificates for the Deployment

Access the Certificate Management tab from the left navigation pane of the Service Manager.

Select the deployment from the drop down list to view information about the server, client certificates and its trusted certificates. The time period of validity with the used signing algorithms from the issuer are displayed.

Click the **Detail** icon from the **Action** column of the certificate store table to view details about the certificate including the issuer, issuee, and signature algorithm.

Click the **Replace** (pencil) icon to replace server certificates.

> **Note:**
>
> You cannot modify or edit an existing certificate. You can only replace it with a new certificate.

Click the **Delete** icon in the Action column to delete the certificate.

Add Client Certificate

To add a client certificate:

1. Click the plus (+) sign next to the Client Certificates section. Add Client Certificate dialog box appears.
2. Enter the following details for the client certificate:
   - Unique Name: Name of the certificate.
   - Certificate PEM: Enter a certificate .pem file or upload a .pem file.
   - Private-Key PEM: Enter or upload the private key for the .pem file.
   - CA Certificates: Enter or upload the CA certificate.
3. Click **Add**.

Add CA Certificate

To add a CA certificate:

1. Click the plus (+) sign next to CA Certificates. Add CA Certificate dialog box appears.
2. Enter the following details for the CA certificate:
   - Unique Name for the CA certificate.
   - Certificate PEM value can be entered in the box or uploaded.
   - Certificate Location can be shared. CA Certificates are always shared and cannot be local. When adding or replacing CA certificates, the **Shared** option is always force-checked.
3. Click **Add**.

Also see Certificate Management in the *Oracle GoldenGate Security Guide*.

3.1.8 How to Add Users

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

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

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

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

1. Log in to either the Service Manager or the Administration Server.
2. From the left navigation pane, select Administrator.
3. Click Users (+) to add users.
4. Enter a unique user name.
5. Select one of these roles from the Role list box:

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

6. Select the user type from the Type list box as **Basic** (digest authentication) or **Certificate**.
7. Enter information that describes the user.
8. If you select the user type as Basic, then the authentication is done based on the username and password. So, the **Password** option comes up, if you select the **Basic** security type and not with the **Certificate** option. Enter the password twice to verify it.

   If you select the user type as Certificate, then the user will authernticate themselves by presenting a client certificate. After you select the Certificate option, you need to enter the common name (in the certificate that will be presented such **CN="certuser"**.

> **Note:**
>
> The certificate is with the user and not saved by the Oracle GoldenGate server. When presented for autherntication, the Oracle GoldenGate server first authenticates that the certificate presented can be trusted and then checks to see that the common name in the certificate has been registered as a valid user. If yes, it will assign the appropriate user role.

9. Click **Submit**.

   The user is registered

Users cannot be changed. You must delete a user, and then add it again. However, you can modify or edit a user's attributes, by clicking the **Edit User** (pencil) in the Action column of the **Users** table.

You can switch the User Type from Basic to Certificate or the other way around.

You can also change the password for the user, if required.

Click **Submit** to confirm the modifications to the user attributes.

4
Working with Data Replication

You can perform all Extract, Replicat, and database credential setup tasks from the Administration Server home page, including adding table and schema level transaction logging (`TRANDATA/SCHEMATRANDATA`), and checkpoint and heartbeat tables.

You can also create additional role-based users that are authorized to do more granular tasks than that of the security user that was created when you added the deployment. Unlike users that are created in the Service Manager deployment, Administration Server users can create Extracts, Replicats, Paths, Credentials, and adjust deployment related settings, while Server Manager users can enable, disable, start and stop deployments and individual services.

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

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

Topics:

- Quick Tour of the Administration Server Home Page
  When you click the Administrator Server link on the Service Manager home page, the login page for the Administration Server is displayed. After logging in, you can configure Extract and Replicat processes from this Web UI.
- How to Add a Database Credential
  To create and run Extract and Replicat processes, you need to set up database credentials.
- How to Create Users from the Administration Server
  Oracle GoldenGate Microservices users can be created from the Administration Server, once you log in using the credentials created at the time of configuring the deployment.
- Before Creating an Extract
  Here are the prerequisites to creating a primary Extract.
- How to Add Extracts
- Before Creating Replicat
  Before you start creating Replicat, create the checkpoint table.
- How to Add a Replicat
  You can add Replicats for the target deployment from the Administration Server.
- How to Use the Master Keys and Encryption Keys
  You can set the master keys and encryption keys using the **Key Management** tab in the **Configuration** page of the Administration Server.

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

4.1 Quick Tour of the Administration Server Home Page

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

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

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

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

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

4.2 How to Add a Database Credential

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

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

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

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

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

- Using Kerberos Authentication with MA
- Configuring Kerberos Authentication

4.2.1 Using Kerberos Authentication with MA

For Microservices Architecture, you need to first create an alias before you use `DBLOGIN`:

```
OGG (not connected) 1> connect http://localhost:9005 as admin password
We1come_$
```

Using default deployment `demo`:

```
OGG (http://localhost:9005 demo) 2> alter credentialstore add user
/@cdb1_pdb1 nopassword alias ora1

2020-06-22T21:08:33Z  INFO OGG-15102  Credential store created.
2020-06-22T21:08:33Z  INFO OGG-15114  Credential store altered.

OGG (http://localhost:9005 demo) 3> info credentialstore

Default domain: OracleGoldenGate
  Alias: ora1
  Userid: /@cdb1_pdb1
```

```
OGG (http://localhost:9005 demo) 4> dblogin useridalias ora1

Successfully logged into database CDB1_PDB1.
```

When using the MA web UI to create the credential, if the **User ID** field begins with a **/** character, then the password is not required. So, in the **User ID** field, enter */ connect_string* where *connect_string* is your connection string.

Here, the `NET SERVICE` is the simple name for the database service. Alternatively, a complete connect string (descriptor) can be used instead of the Oracle net service name.

Here's an example of a predefined net service name and connect descriptor mapping:

```
cdb1_pdb1 = (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=db1))
(CONNECT_DATA=(SERVICE_NAME=cdb1_pdb1.regress.rdbms.test.us.oracle.com))
)
```

- Example: Using USERIDALIAS in Parameter File for Kerberos Account

4.2.1.1 Example: Using USERIDALIAS in Parameter File for Kerberos Account

The following example shows how to set the `USERIDALIAS` values in the parameter file after creating the credential store with Kerberos authentication:

```
OGG (http://localhost:9005 demo) 2> alter credentialstore add user /
@extract_user nopassword alias ext_user 2020-12-17T21:08:33
INFO    OGG-15102  Credential store created.2020-12-17T21:08:33
INFO    OGG-15114  Credential store altered.

OGG (http://localhost:9005 demo) 2> alter credentialstore add user /
@miningdb_user nopassword alias mine_db_user 2020-12-17T21:09:45
INFO    OGG-15102  Credential store created.2020-12-17T21:09:45
INFO    OGG-15114  Credential store altered.

OGG (http://localhost:9005 demo) 3> info credentialstore

Default domain: OracleGoldenGate
Alias: ext_user
Userid: /@extract_user

Default domain: OracleGoldenGate
Alias: mine_db_user
Userid: /@miningdb_user
```

After altering the credentialstore, you can specify `USERIDALIAS` options in the parameter file:

```
USERIDALIAS ext_user DOMAIN OracleGoldenGate
TRANLOGOPTIONS MININUSERIDLIAS mine_db_user DOMAIN OracleGoldenGate
```

4.2.2 Configuring Kerberos Authentication

For Classic Architecture, Kerberos authentication is configured using the DBLOGIN command:

```
GGSCI> DBLOGIN USERID /@NET_SERVICE_NAME
```

A valid DBLOGIN command without USERID and password can then be specified as:

```
GGSCI> DBLOGIN USERID /@cdb1_pdb1
```

On the Oracle GoldenGate side, if you want to issue the DBLOGIN command with different externally authenticated users, the usage of a default Kerberos cache location is specified in the SQLNET.ORA file. This is then assumed to be the externally authenticated user for the database login.

For example, observe a Kerberos Cache location specified in the client side SQLNET.ORA file:

```
SQLNET.KERBEROS5_CONF = /ade/b/3910426782/oracle/work/krb/krb.conf
SQLNET.KERBEROS5_KEYTAB = /ade/b/3910426782/oracle/work/krb/v5srvtab
SQLNET.KERBEROS5_CC_NAME = /ade/b/3910426782/oracle/work/krb/krb.cc
```

In this example, the krb.cc is the Kerberos Cache used in this Oracle GoldenGate deployment. If you open the krb.cc cache file with the oklist utility, you can see that the default principal is used as the externally authenticated user oratst@US.ORACLE.COM.

```
ade:[ demo_vw2 ] [demo@test02swv krb]$ oklist krb.cc

Kerberos Utilities for Linux: Version 21.1.0.0.0 - Production on 27-
JUN-2020 23:59:13

Copyright (c) 1996, 2021 Oracle.  All rights reserved.

Configuration file : /ade/b/3910426782/oracle/work/krb/krb.conf.
Ticket cache: FILE:krb.cc
Default principal: oratst@US.ORACLE.COM

Valid starting     Expires            Service principal
06/27/20 12:12:34  06/28/20 12:12:34  krbtst/US.ORACLE.COM@US.ORACLE.COM
06/27/20 12:12:34  06/28/20 12:12:34  oratst/
demo2swv.us.oracle.com@US.ORACLE.COM
```

To know more, see the ALTER CREDENTIALSTORE, DBLOGIN, and MININGDBLOGIN commands. Also see, USERID | NOUSERID, USERIDALIAS parameters.

4.3 How to Create Users from the Administration Server

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

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

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

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

4.4 Before Creating an Extract

Here are the prerequisites to creating a primary Extract.

Before performing the tasks in this topic, make sure you are connected to the database. See How to Add a Database Credential for steps to create credentials for for the database. After you have connected to the database, the Configuration page will show the Checkpoint and Heartbeat configuration sections.

Enable TRANDATA or SCHEMATRANDATA Information

Valid for Oracle, DB2, and SQL Server.

Enabling supplemental logging is required for some databases, and depending on the database, this can be done at the table, schema, or procedure level.

To enable supplemental logging at the table and schema level, on Configuration page:

1. Select the **Table** or **Schema** option as required and click plus sign to add.
2. Enter the name of the table for which you need to set up supplemental logging. Make sure to enter the full table name with schema name, such as, `schema.table1`. You can also use wildcard instead of specific table name.
3. Select the **Add TRANDATA Information in the background?** option as required.
4. Click **Submit**.

You can also use the commands `ADD TRANDATA` and `ADD SCHEMATRANDATA` for setting up trandata and schema level trandata. For details, see `ADD TRANDATA` and `ADD SCHEMATRANDATA`. You can skip `ADD TRANDATA` in case of initial load without CDC.

Create Heartbeat Table

To create the heartbeat table:

> **Note:**
>
> Creating the heartbeat table is optional.

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

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

Create the Oracle GoldenGate CDC Cleanup Task

For SQL Server users, there is a requirement to create Oracle GoldenGate CDC Cleanup tasks before adding an Extract. You can do so by performing the steps in Details of the Oracle GoldenGate CDC Cleanup Process

in the *Using Oracle GoldenGate for Heterogeneous Databases* guide.

Add Checkpoint Table

You can view a list of existing checkpoint tables from the checkpoint section. In case you want to add a checkpoint table:

1. Click the plus sign to enable adding a checkpoint table.
2. Add the checkpoint table name in the format *`table.checkpoint_table_name`*.
3. Click **Submit**. After the checkpoint is created, you'll be able to see in the list of checkpoint tables.

To perform this task from the command line, see `ADD CHECKPOINTTABLE` in the *Command Line Interface Reference for Oracle GoldenGate*.

4.5 How to Add Extracts

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

Now, you're ready to add an Extract for your deployment.

1. From the Overview page of the Administration Server, click the + sign next to Extracts.
2. Choose the type of Extract to create and click **Next**.

> **Note:**
>
> To learn about creating Initial Load Extract, see How to Add an Initial Load Extract and also see Loading Data from File to Replicat in MA in *Administering Oracle GoldenGate*.

You can also create a Change Data Capture Extract for MySQL and SQL Server databases.

3. Provide the required information designated with an asterisk (*). Here's a description of the options in the different sections for the Add Extract screen:

Option	Description	Database
Basic Information Section		
Process Name	Name of the Extract process	All
Description	Description of the Extract process being created.	All
Intent	Describes the purpose of creating the Extract. The default option is Unidirectional. Other options are High Availability, Disaster Recovery, N-Way, which are informational only.	All databases
Begin	Used to set the beginning location in the redo or transaction log from which the Extract will start to capture data. Available options are Now, Custom Time, CSN or Position in Log, and EOF depending on the supported database.	All databases
Trail Name	A two character trail name.	All databases
Trail Subdirectory, Size, Sequence, and Offset	You can further configure the trail details.	All databases
Remote	Enable this option if the Extract trail is remote. For Oracle databases, enable this option if the Extract trail is to be written directly to a remote Oracle GoldenGate Classic installation. For MySQL, setting this option enables the `TRANLOGOPTIONS ALTLOGDEST REMOTE` parameter to support a remote Extract, and is not related to trails.	Oracle, MySQL
Registration Information Section		
CSN	Commit Sequence Number (CSN) value	Oracle, PostgreSQL

Option	Description	Database
Share	Choose the method to share the LogMiner data dictionary. Options are: • Automatic: This option allows the system to choose the method for sharing the dictionary . • None: Choosing this option, will not allow the dictionary to be shared. • Extract: Choose this option to allow sharing the logminer dictionary for specific Extract.	Oracle, PostgreSQL
Optimized	Enable this option to optimize the Extract registration.	Oracle, PostgreSQL
Downstream Capture	Enable this option to set up a downstream Extract for log mining.	Oracle, PostgreSQL
Source Database Credential		
Create new credential	If you haven't set up your database login credentials, you can create and save the database login credentials from here.	All
Credential Domain	Create a domain for the database.	All
Credential Alias	Specifiy a credential for the database login.	All
User ID	Specify a user name for logging into the database.	All
Password, Verify Password	Enter the password used to login to the database and reenter the password to verify.	All
Credential Domain	Saves the credential user under the specified domain name. Enables the same alias to be used by multiple Oracle GoldenGate installations that use the same credential store. The default domain is Oracle GoldenGate.	All databases

Option	Description	Database
Credential Alias	Specifies an alias for the user name. Use this option if you do not want the user name to be in a parameter file or command. If `ALIAS` is not used, the alias defaults to the user name, which then must be used in parameter files and commands where a login is required. You can create multiple entries for a user, each with a different alias, by using the `ADD USER` option with `ALIAS`.	All databases
Downstream Mining		
Mining Credential Domain	Domain name of the downstream mining database.	Oracle
Mining Credential Alias	Alias for the mining downstream database.	Oracle
No UserID	Enable this option if there is no source database connection. Selecting this option enables the ADG fetch options.	Oracle
ADG Fetch Credential Domain	Domain name for the ADG fetch database.	Oracle
ADG Fetch Credential Alias	Domain alias for the ADG fetch database.	Oracle

4. Enter the encryption profile details. If you have not created an encryption profile, then the Local Wallet profile would be selected by default. :
   a. Select the profile name from the list box. You can select the Local Wallet or a custom profile.
   b. Select the encryption profile type from the list box.
   c. Specify the masterkey for the encryption profile. This option doesn't exist with SQL Server.
5. This is an optional step. Enter the Managed Options while creating all types of Extract processes. The following table provides these options:
6. Click **Next**.
7. 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;`
8. You can select **Register Extract in the background** to register the Extract in the background asynchronously. This option is required for Oracle and PostgreSQL databases.
9. Click **Create and Run** to create and start the Extract. If you select **Create**, the Extract is created but you need to start it using the Extract drop-down on the Overview page.

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

- How to Add an Initial Load Extract
- Using Extract Actions
  Extract action include tasks like monitoring details for the Extract such as profile management, checkpoint details, statistical data, cache manager statistics, and more.

4.5.1 How to Add an Initial Load Extract

An initial load Extract pulls data from tables and writes the records to an external file (`EXTFILE`) rather than to a trail (`EXTTRAIL`). Common uses for an initial load Extract are to instantiate the data to a heterogeneous target, such as from Oracle to SQL Server or from MySQL to DB2.

Here are the steps to set up an initial load Extract in MA:

1. In the Administration Server, click the plus sign in the Extract section to open the Add Extract wizard.
2. Choose the initial load Extract and click Next.
3. In the Extract Options section, enter the details for the Extract such as process name, intent, credential details, the name of the trail file and subdirectory which needs to be loaded and click Next.
4. Check the option for the Extract in the Parameter file and click Create and Run to complete setting up the Extract.

4.5.2 Using Extract Actions

Extract action include tasks like monitoring details for the Extract such as profile management, checkpoint details, statistical data, cache manager statistics, and more.

Use the Action button to start or stop the Extract or view and manage its details. When you select the Action, Details option for an Extract, you can perform the following tasks for it.

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. • **Cache Manager Statistics**: Access the global statistics and object pool statistics information for the Extract process from this page. • **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.

4.6 Before Creating Replicat

Before you start creating Replicat, create the checkpoint table.

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

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

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

4.7 How to Add a Replicat

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

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

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

   The Add Replicat page is displayed.
2. Select a Replicat type and click **Next**.

   > **Note:**
   >
   > Some Replicat types are only available for certain databases. All Replicat types may not be applicable to your database.

   The types of Replicat are:

   - Integrated Replicat
   - Nonintegrated Replicat: This option is displayed with heterogeneous or non-Oracle databases.
   - Classic Replicat: This option is displayed with Oracle database.
   - Coordinated Replicat
   - Parallel Replicat: If you select this option, then select an integrated or nonintegrated parallel Replicat.
3. Enter the required Replicat options on the Replicat Options page and click **Next**. To know more about the Replicat options, see the online help.
4. For managed processes, the options to enter are:
5. Click **Create and Run** to create and run the Replicat.

- Creating a Parallel Replicat
- Using Replicat Actions
  You can manage a Replicat process using the **Action**, **Details** option of the Replicat from the Administration Server Overview page.

4.7.1 Creating a Parallel Replicat

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

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

Creating a Non-Integrated Parallel Replicat with the Administration Server

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

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

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

Creating a Non-Integrated Parallel Replicat with the Admin Client

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

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

   ```
   adminclient
   ```

   The Admin Client command prompt is displayed.

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

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

You must use http or https in the connection string; this example is a non-SSL connection.

4. Add the Parallel Replicat, which may take a few minutes to complete:

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

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

5. Verify that the Replicat is running:

```
info replicat R1
```

Messages similar to the following are displayed:

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

- Basic Parameters for Parallel Replicat

4.7.1.1 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	

Parameter	Description
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 2
MIN_APPLY_PARALLELISM 2
MAX_APPLY_PARALLELISM 10
SPLIT_TRANS_RECS 10.000
map *.*, target *.*;
```

4.7.2 Using Replicat Actions

You can manage a Replicat process using the **Action**, **Details** option of the Replicat from the Administration Server Overview page.

You can change the status of the Replicat process using the **Action** button to start or stop a Replicat or manage the Replicat process from the Details option:

Action	Result
Details	Displays the Process Information page that has the following details: • **Process Information** • **Checkpoint** • **Statistics** • **Cache Manager Statistics**: • **Parameters** • **Report** • **Heartbeat**
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.

Action	Result
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.

Using Replicat Action Options

Process Information
Displays Replicat process details such as status of Replicat as running or stopped. You can also edit the encryption profile and managed options for auto start and auto restart from here.

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.

Statistics
Displays the active replication maps along with replication statistics based on the type of Replicat.

Cache Manager Statistics
Access the global statistics and object pool statistics information for the Extract process from this page.

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.

Heartbeat
You can access heartbeat information from the Heartbeat tab of the Replicat Process Information page. Oracle GoldenGate provides endpoints for automatic heartbeat tables that allow creating and modifying a heartbeat table using a database connection and retrieving heartbeat information.
This tab displays the current heartbeat or lag records for specific Replicat database connection.
Heartbeat Information
You can view the heartbeat information for a Replicat in this section. It includes the frequency, retention time, and purge frequency.
Latest Heartbeats
Latest heartbeat is based on the GG_LAG view, which is accessible using the specific database connection for the heartbeat endpoint.

Information in this section includes the source and target database names, distribution path, heartbeat lag value, timestamp of the latest heartbeat. The **Actions** column provides the **See History** option.
Click the **See History** option to view the heartbeat history table.
Heartbeat History
This section appears when you select the **See History** option from the Latest Heartbeats section. You can perform the following tasks in this section:

- Search the heartbeat history based on the latest heartbeat by clicking the **Latest Heartbeat** option or the timestamp interval by selecting the **Received Timestamp** option.
- If you select the Received Timestamp option, you need to specify a heartbeat period between 0 and 4095.
- View the heartbeat history in **Chart View** or **Table View** by selecting the required option.

4.8 How to Use the Master Keys and Encryption Keys

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

Using Master Keys

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

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

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

Using the Encryption Keys

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

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

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

4.9 How to Access the Parameter Files

The Global parameters and 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 restart the Administration Server and any Extracts and Replicats..
4. Click + add parameter files.
5. Enter the file name and the required parameters. Make sure to enter the file name with the `.prm` extension.
6. Click **Submit**. The new parameter file is displayed in the list of parameter files.

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

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

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

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

4.10 Setting Up Automated Tasks

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

Purging Trails

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

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

1. Add a Purge Trail task by clicking the + sign .
2. Enter the **Operation Name** of the Administration Service task. The operation name is case sensitive. For example, you can create an operation with the name **TASK1** and another operation named **task1**.

3. Enter the trail path or trail name in the **Trail** field.
4. Click the **+** sign to add the trail to the **Selected Trails** list.
5. If you don't need to use checkpoints, disable the option **Use Checkpoints**. However, Oracle recommends using checkpoints. If you don't use checkpoints. the trail will be purged whether or not it has been consumed if the keep rule is met.
6. Set the **Keep Rule** value to specify the maximum number of hours, days, or number of files for which the Purge Trails task needs to be active.
7. Specify the number of hours or days when the purge trails task has to run, in the Purge Frequency field and click Submit.
8. Use the Purge Trails task table to edit or delete the task, as required.

   Also see PURGE EXTTRAIL.

Purging Tasks

You can automatically purge processes associated with an Administration Service.

From the Tasks tab, click Purge Tasks.

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

Reporting Lag

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

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

5. Click Submit.

4.11 Review Critical Events

You can review and search for critical events from the Review Critical Events section of the Administration Server home page.

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.

4.12 How to Configure Encryption Profile

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

To set up the encryption profile, click Profile from the navigation pane and then select the Key Management System (KMS) tab.

1. By default, the Local Wallet profile is created. If you select the Local Wallet encryption profile, you'll see its options, which you can edit using the pen icon.

Options	Description
Description	A description of the local wallet.
Default Profile	This option is enabled by default. You can select to disable it.
Encryption Profile Type	This option cannot be changed for the local wallet.
Masterkey Name	This is the default master key for the local wallet. You cannot edit this value.
Masterkey Version	This is the master key version number. The value is set to **LATEST** and cannot be changed.

2. Click the + sign next to Profile to create an encryption profile by specifying the following details:

Option	Description
Profile Name	Name of the encryption profile
Description	Describe the encryption profile.
Default Profile	If you want to make this profile the default, then enable this option.

Option	Description
Encryption Profile Type	Available options are Oracle Key Vault (OKV) and Oracle Cloud Infrastructure (OCI).
OKV Configuration Options	Options that appear when you select the Oracle Key Vault (OKV) option encryption profile type.
KMS Library Path	Specify the directory location where Oracle Key Vault is installed.
Oracle Key Vault Version	The supported Oracle Key Vault version is 18.1.
Masterkey Name	Specify the name of the master key
Time to Live	Time to live (TTL) for the key retrieved by Extract from KMS. When encrypting the next trail, Extract checks if TTL has expired. If so, it retrieves the latest version of the master key. The default is 24 hours.
OCI KMS Configuration Options	Options to set up an OCI KMS.
Crypto Endpoint URL	You can access this from the OCI KMS Vault wizard. See OCI Command Line Reference and Managing Keys in *OCI Documentation* to know more.
Tenancy OCID	When you sign up for Oracle Cloud Infrastructure, Oracle creates a *tenancy* for your company, which is a secure and isolated partition within Oracle Cloud Infrastructure where you can create, organize, and administer your cloud resources. See Key Concepts in *OCI Documentation* to learn more.
Key OCID	See the OCI Documetnation for details.
User OCID	See the OCI Documetnation for details.
API Key	A credential for securing requests to the Oracle Cloud Infrastructure REST API.
API Key Fingerprint	See Required Keys and OCIDs in the OCI documentation for details.

4.13 How to Configure Managed Processes

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

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

1. Click Profile from the Administration Server navigation pane.
2. In the Managed Process Settings tab, you can click + sign to start creating a profile. There's also a default profile preset on this page.

3. Enter the details for the profile options including the Profile Name, Description, Auto Start and Auto Restart options. See the following table for Auto Start and Auto Restart options.

Option	Description
Profile Name	Provides the name of the autostart and autorestart profile. You can select the default or custom options. If you have already created a profile, then you can select that profile also. If you select the Custom option, then you can set up a new profile from this section itself.
Critical to deployment health	(Oracle only) Enable this option if the profile is critical for the deployment health. **Note:** This option only appears while creating the Extract or Replicat and not when you set up the managed processes in the Profiles page.
Auto Start	Enables autostart for the process.
Startup Delay	Time to wait in seconds before starting the process
Auto Restart	Configures how to restart the process if it terminates
Max Retries	Specify the maximum number of retries to try to start the process
Retry Delay	Delay time in trying to start the process
Retries Window	The duration interval to try to start the process
Restart on Failure only	If true the task is only restarted if it failes
Disable Task After Retries Exhausted	If true then the task is disabled after exhausting all attempts to restart the process.

4.14 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.

5
Working with Paths

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

This section discusses the steps to create a distribution and receiver paths.

Topics:

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

5.1 Quick Tour of the Distribution Server Home Page

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

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

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

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

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

5.2 How to Add a Distribution Path

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

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

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

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

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

Options	Description
Source: *Trail Name*	Select the Extract name from the drop-down list, which populates the trail name automatically. If it doesn't, enter the trail name that you provided while adding the Extract.
Generated Source URI:	A URI is automatically generated for the trail based on the Extract information you provided. You can edit this URI by clicking the pencil, then modifying the source. Typically, you will need to edit the URI if you want to use reverse proxy.
Target Authentication Method	Select the authentication method for the target URI. Authentication options are Certificate, UserID Alias.
Target	Enter the target endpoint of the path. From the drop-down list, select your data transfer protocol. The default option is **wss** (secure web socket). Specify the following details when you select this option: • Target Host: Enter the URL of the target host, for example, localhost, if the target is on the same system. • Port Number: 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. • Trail Name: Path takes the source trail and sends the date to a target trail given here, which can be consumed by any Replicats created later. • Domain: Name of the target domain. • Alias: User alias of the target domain. You can also choose **ogg** or **ws** (web socket) protocol. For the **ogg** protocol, you need to specify only the target host, port number, and trail file name. For the **ws** protocol, the options are the same as the wss protocol.
Generated Target URI	A target URI is automatically generated for the trail based on the target authentication method and target you provided. You can edit this URI by clicking the pencil, then modifying the target.
Target Encryption Algorithm	Select the encryption algorithm for the target trail. Options include NONE, AES128, AES192, AES256.

Options	Description
Target Encryption Keyname	Specify a logical name for the encryption key based on the specified type of target encryption algorithm.
Enable Network Compression	Set the compression threshold value if you enable this option.
Compression Threshold	Option appears when you enable the network compression. Specify the compresion threshold value.
Sequence Length	The length of the trail sequence number.
Trail Size (MB)	The maximum size of a file in a trail.
Encryption Profile	Name of the encryption profile associated with the path.
Configure Trail Format	Toggle this switch to enable and configure the trail file format.
Type	Select one of these types of trail file formats: • Plain Text • XML • SQL
Compatible With	Select the utility that is compatible with the trail file. Options are: • BCP • SQLLOADER • COMCAST
Timestamp Precision	Specify the timestamp precision value for the trail file.
Extra Columns	Includes placeholders for additional columns at the end of each record. Use this option when a target table has more columns than the source table. Specify a value between 1 and 9.
Include SYSKEY	Select this option incase your Replicat configuration includes tables with SYSKEY.
Quote Style	Select the quote style depending on the database requirements.
Include Column Name?	Enable this option to include column names in the trail file.
Null Is Space?	Select this option to indicate that any null values in the trail file is a space.
Include Place Holder?	Outputs a placeholder for missing columns.
Include Header Fields?	Select to include header fields in the trail file.
Delimiter	An alternative delimiter character.
Use Qualified Name?	Select to use the fully qualified name of the parameter file.

Options	Description
Include Transaction Info?	Enable to to include transaction information.
Encryption Profile	Section
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 Relative Byte Address (RBA) offset value which is the point in the trail file (in bytes) from where you want the process to start.
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 restarts automatically if it's terminated.
Auto Restart Options	Section
Retries	The number of times to try an restart the task (path process).
Delay	The duration interval to wait between retries.

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

Additional Options	Description
Eof Delay (cent sec)	You can specify the Eof Delay in centiseconds. On Linux platforms, the default settings can be retained. However, on non-Linux platforms, you may need to adjust this setting for high bandwidth, high latency networks, or for networks that have Quality of Service (QoS) settings (DSCP and Time of Service (ToS)).
Checkpoint Frequency	Frequency of the path that is taking the checkpoint (in seconds).
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.
TCP Options	Section
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.
TCP_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.
TCP_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 Receive Buffer Size	You can set the value for the receive buffer size for flow control.
Keep Alive	Timeout for keep-alive.

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

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

5.3 How to Add a Target-Initiated Distribution Path

A target-initiated distribution path is created from the Receiver Server. These paths can be used when communication must be initiated from the target.

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

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

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

Table 5-1 Adding Target Initiated Distribution Path

Options	Description
Path Name	Name of the target-initiated distribution path
Description	Provide a description of the path.
Reverse Proxy Enabled	Select to use reverse proxy. To know more about configuring you reverser proxy servers, see Reverse Proxy Support in *Oracle GoldenGate Security Guide*
Source Authentication Method	Select the authentication method for the source URI. Various authentication options are OAuth 2.0, Certificate, UserID Alias.
Source	From the drop-down list, select your data transfer protocol. The default option is **wss**. You also need to enter the following details: • Source Host: URL of the source host for example, **localhost**, if the source is on the same system. • Port Number: Enter the port number of the Distribution Server. • Trail Name: Enter the trail name you want to read on your source. **NOTE:** The Distribution Server doesn't not create any trail on source. It can only read the provided trail name. • Domain: Enter the domain for the host. • Alias: Provide an alias for this host. Path takes the source trail and sends the data to a target trail given here, which can be consumed by any Replicats created later.
Generated Source URI	A URI is automatically generated for the trail based on the source information you provided.
Target	Name of the target trail of the Replicat you created earlier.
Generated Target URI	A Target URI is automatically generated for the trail based on target trail information you provided.
Target Encryption Algorithm	Select the encryption algorithm for the target trail. Options include AES128, AES192, AES256.
Enable Network Compression	Set the compression threshold value if you decide enable this option.
Sequence Length	The length of the trail sequence number.
Trail Size	The maximum size of a file in a trail.
Configure Trail Format	Toggle this switch to enable and configure the trail file format.

Table 5-1 (Cont.) Adding Target Initiated Distribution Path

Options	Description
Type	Select one of these types of trail file formats: • Plain Text • XML • SQL
Compatible With	Select the utility that is compatible with the trail file. Options are: • BCP • SQLLOADER • COMCAST
Timestamp Precision	Specify the timestamp precision value for the trail file.
Extra Columns	Includes placeholders for additional columns at the end of each record. Use this option when a target table has more columns than the source table. Specify a value between 1 and 9.
Include SYSKEY	Select this option incase your Replicat configuration includes tables with SYSKEY.
Quote Style	Select the quote style depending on the database requirements.
Include Column Name?	Enable this option to include column names in the trail file.
Null Is Space?	Select this option to indicate that any null values in the trail file is a space.
Include Place Holder?	Outputs a placeholder for missing columns.
Include Header Fields?	Select to include header fields in the trail file.
Delimiter	An alternative delimiter character.
Use Qualified Name?	Select to use the fully qualified name of the parameter file.
Include Transaction Info?	Enable to to include transaction information.
Encryption Profile	Section
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 Relative Byte Address (RBA) offset value which is the point in the trail file (in bytes) from where you want the process to start.

Table 5-1 (Cont.) Adding Target Initiated Distribution Path

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.
Auto Restart Options	X
Retries	The number of times to try an restart the task (path process).
Delay	The duration interval to wait between retries.

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

Additional Options	Description
Eof Delay (cent sec)	You can specify the Eof Delay in centiseconds. On Linux platforms, the default settings can be retained. However, on non-Linux platforms, you may need to adjust this setting for high bandwidth, high latency networks, or for networks that have Quality of Service (QoS) settings (DSCP and Time of Service (ToS)).
Checkpoint Frequency	Frequency of the path that is taking the checkpoint (in seconds).
TCP Flush Bytes	Enter the TCP flush size in bytes.
TCP Flush Seconds	Enter the TCP flush interval in seconds.
TCP Options	Section
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.
TCP_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.
TCP_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 Receive Buffer Size	You can set the value for the receive buffer size for flow control.
Keep Alive	Timeout for keep-alive.

Note:

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

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

X	Target Deployment (Non-Secure)	Target Deployment (Secure)
Source Deployment (Non-secure)	`WS`	`WS`
Source Deployment (Secure)	`WSS`	`WSS`

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

Limitations

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

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

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

5.4 Using the Path Actions

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

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

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

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

5.5 Repositioning a Path

You can reposition a path whenever it's necessary.

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

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

5.6 Changing Path Filtering

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

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

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

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

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

5.7 Reviewing the Distribution Server Path Information

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

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

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

6
Working with Trails

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

This section describes the tasks to set up trails:

Topics:

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

6.1 Quick Tour of the Receiver Server Home Page

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

The Receiver Server works with the Distribution Server to receive incoming trail file information. 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 by clicking the **Action**, **Details** option.

Also see Monitoring Paths.

6.2 Tuning Network Parameters

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

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

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

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

The Path Information page is displayed.

2. Expand the Advanced Options.

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

   The TCP Options, include the following parameters:

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

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

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

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

6.3 Reviewing the Receiver Server Path Information

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

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

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

6.4 Monitoring Paths

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

Use the information provided on this page to troubleshoot performance issues with the distribution server. If it's not able to keep up, they can come here and see the reasons why, and then use that information to tune the TCP window size, or enable compression, or even split the trails into multiple threads (multiple distribution service paths, each moving a subset of tables)

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

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

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

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

7
Monitoring Performance

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

Topics:

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

7.1 Quick Tour of the Performance Metrics Server Home Page

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

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

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

Task	Description
Review Messages	Reviewing Messages from the Messages Overview tab.

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

7.2 Monitoring Server Performance

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

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

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

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

Server Statistics	• Distribution Server • Performance Metrics Server
Trail Files	• Extracts • Replicats
Database Statistics	• Extracts • Replicats
Procedure Statistics	• Extracts • Replicats
Cache Statistics	Extracts
Queue Statistics	Extracts

7.3 Reviewing Messages

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

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

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

   The Performance Metrics Server Overview page is displayed.

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

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

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

7.4 Review Status Changes

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

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

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

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

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

7.5 How to Purge the Datastore

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

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

The current process retention in days displays.

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

A
About Target-Initiated Paths

Target-initiated paths for microservices enable the Receiver Server to initiate a path to the Distribution Service on the target deployment and pull trail files. This feature allows the Receiver Server to create a target initiated path for environments such as Demilitarized Zone Paths (DMZ) or Cloud to on-premise, where the Distribution Server in the source Oracle GoldenGate deployment cannot open network connections in the target environment to the Receiver Server due to network security policies.

If the Distribution Server cannot initiate connections to the Receiver Server, but Receiver Server can initiate a connection to the machine running the Distribution Server, then the Receiver Server establishes a secure or non-secure target initiated path to the Distribution Server through a firewall or Demilitarized (DMZ) zone using Oracle GoldenGate and pull the requested trail files.

The Receiver Server endpoints display that the retrieval of the trail files was initiated by the Receiver Server, see Quick Tour of the Receiver Server Home Page.

You can enable this option from the Configuration Assistant wizard Security options, see How to Create Deployments. For steps to create a target-initiated distribution path, see How to Add a Target-Initiated Distrbution Path in the *Step by Step Data Replication Using Oracle GoldenGate Microservices* guide.

B
Integration with Reverse Proxy

Learn how to configure your reverse proxy servers.

Reverse Proxy allows the connect using one single port for the different microservices in a deployment. You can configure a proxy server depending on your environment setup and network requirements.

> **Note:**
>
> Reverse proxy is optional, however, Oracle recommends that you ensure easy access to microservices and provide enhanced security.

Reverse Proxy Support

You can configure Oracle GoldenGate Microservices to use a reverse proxy. Oracle GoldenGate Microservices includes a script called `ReverseProxySettings` that generates configuration file for only the NGINX reverse proxy server.

For example, the Administration Server is available on `HTTPS://goldengate.example.com:9001` and the Distribution Server is on `HTTPS://goldengate.example.com:9002`. With reverse proxy, each of the microservices can simply be accessed from the single address. For example, `https://goldengate.example.com/distsrvr` for the Distribution Server. The URL is different for each service and is by name instead of by port.

You can use these options with the `ReverseProxySettings`:

`-o` or `--output`
The output file name. The default file name is `ogg.conf`.

`-P` or `--password`
A password for a Service Manager account.

`-l` or `--log`
Log file name and initiates logging. The default is no logging.

`--trailOnly`
Configure only for inbound trail data.

`-t` or `--type`
The proxy server type. The default is Nginx.

`-s` or `--no-ssl`
Configure without SSL.

`-h` or `--host`
The virtual host name for reverse proxy.

`-p` or `--port`
The reverse proxy port number. The defaults are 80 or 443.

`-?` or `--help`
Display usage information.

`-u` or `--user`
Name of the Service Manager account to use.

`-v` or `--version`
Displays the version.

These values are used when connecting to the Service Manager and are required when authentication is enabled.

You can use any reverse proxy service with Microservices. The following example provides a process that you can follow to configure other reverse proxy services in conjunction with the documentation for your proxy server.

Prerequisites

The following prerequisites provide details on the minimum requirements to configure an NGINX Reverse Proxy. Similar requirements may be required for your environment and reverse proxy if not using NGINX. Consult the documentation for your reverse proxy.

1. Install NGINX, see Installing NGINX Reverse Proxy. For Oracle Linux, the command to install NGINX is:

   ```
   yum –y install NGINX
   ```

2. Check the JRE version to be JRE 8 or higher.
3. Install Oracle GoldenGate Microservices.
4. Create one or more active Microservices deployments.
5. Ensure that the Oracle user has `sudo` permissions.

Configuring NGINX Reverse Proxy

An Oracle GoldenGate Microservices installation includes the `ReverseProxySettings` utility. The `ReverseProxySettings` utility is located in the *`$OGG_HOME`*`/lib/utl/reverseproxy` directory. To identify additional commands that can be used with the `ReverseProxySettings` utility, run the utility with the `--help` option:

```
$OGG_HOME/lib/utl/reverseproxy/ReverseProxySettings --help
```

To add the NGINX certificate to the Distribution server's client wallet as a trusted certificate, see Setting Up Trusted Certificates.

1. To generate a configuration file for NGINX Reverse Proxy, run a similar command using the `ReverseProxySettings` utility. If you are configuring NGINX to use a secure configuration, you have to omit the `-s` option and ensure you are using HTTPS instead of HTTP.

   ```
   $OGG_HOME/lib/utl/reverseproxy/ReverseProxySettings -u adminuser -P
   adminpwd -o ogg.conf HTTPS://localhost:9100
   ```

2. Replace the existing NGINX configuration with the configuration that was generated using the `ReverseProxySetting` utility for your Microservices deployment:

   ```
   sudo mv ogg.conf /etc/nginx/conf.d/nginx.conf
   ```

   However, this NGINX configuration isn't complete without the `events` section, and enclosing the `map` and `server` sections in `http`.

   Optionally, you can use the default `nginx.conf` file and add the generated `ogg.conf` by adding an `include` statement similar to this:

   ```
   include /etc/nginx/conf.d/ogg.conf;
   ```

   In this case, you must comment out the other `servers` section.

3. Generate a Self-Signed certificate for NGINX:

   ```
   sudo sh /etc/ssl/certs/make-dummy-cert /etc/NGINX/ogg.pem
   ```

   For distribution paths to go through the reverse proxy, you need to use a valid certificate. It's better to specify the same certificate that the deployment is using to process incoming requests, otherwise, starting the path will fail with the next error in Distribution Server:

   ```
   2019-03-26T11:26:00.324-0700 ERROR| ERROR   OGG-10351  Oracle
   GoldenGate Distribution
           Server for Oracle:  Generic error -1 noticed. Error
   description - Certificate validation
           error: Unacceptable certificate from test00abc: application
   verification failure.
         (A4)
   ```

4. Validate the NGINX configuration:

   ```
   sudo NGINX -t

   NGINX: the configuration file /etc/NGINX/NGINX.conf syntax is ok
   NGINX: configuration file /etc/NGINX/NGINX.conf test is successful
   ```

5. Reload NGINX with the new configuration:

   ```
   sudo NGINX -s reload
   ```

   If the changes for the configuration file are not loaded, stop and restart the proxy.

6. Use cURL to verify that reverse proxy is working:

   ```
   curl -sv HTTPS://localhost/services/v2
   {"$schema":"api:version","catalog":{"links":[
   {"href":"HTTPS://localhost/service s/v2/metadata-
   catalog","rel":"canonical"}]},"isLatest":true,"lifecycle":"active","
   links":[
   {"href":"HTTPS://localhost/services/v2","mediaType":"application/js
   on","rel":"canonical"},
   ```

```
{"href":"HTTPS://localhost/services/v2","mediaType":"app lication/
json","rel":"self"}],"version":"v2"}
```

> **Note:**
>
> If the deployments associated with the target Service Manager change, the NGINX configuration file must be re-generated and reloaded.

SSL Termination

When there is an unsecure connection between the Reverse Proxy, which uses a TLS-based connection, and the origin server, it is referred to as Reverse Proxy SSL-termination.

Note that in SSL-Termination the connections between the Reverse Proxy and the origin servers are unsecure.

However, SSL-bridging is also supported where the connections between the client and Reverse Proxy is secured and the connection between the Reverse Proxy and the origin server is also secured.