Informatica®

Informatica® Cloud Data Integration

Oracle Cloud Object Storage Connector

Informatica Cloud Data Integration Oracle Cloud Object Storage Connector
July 2024

© Copyright Informatica LLC 2022, 2024

This software and documentation are provided only under a separate license agreement containing restrictions on use and disclosure. No part of this document may be reproduced or transmitted in any form, by any means (electronic, photocopying, recording or otherwise) without prior consent of Informatica LLC.

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation is subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License.

Informatica, the Informatica logo, Informatica Cloud, and PowerCenter are trademarks or registered trademarks of Informatica LLC in the United States and many jurisdictions throughout the world. A current list of Informatica trademarks is available on the web at https://www.informatica.com/trademarks.html. Other company and product names may be trade names or trademarks of their respective owners.

Portions of this software and/or documentation are subject to copyright held by third parties. Required third party notices are included with the product.

See patents at https://www.informatica.com/legal/patents.html.

DISCLAIMER: Informatica LLC provides this documentation "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of noninfringement, merchantability, or use for a particular purpose. Informatica LLC does not warrant that this software or documentation is error free. The information provided in this software or documentation may include technical inaccuracies or typographical errors. The information in this software and documentation is subject to change at any time without notice.

NOTICES

This Informatica product (the "Software") includes certain drivers (the "DataDirect Drivers") from DataDirect Technologies, an operating company of Progress Software Corporation ("DataDirect") which are subject to the following terms and conditions:

1. THE DATADIRECT DRIVERS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.
2. IN NO EVENT WILL DATADIRECT OR ITS THIRD PARTY SUPPLIERS BE LIABLE TO THE END-USER CUSTOMER FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR OTHER DAMAGES ARISING OUT OF THE USE OF THE ODBC DRIVERS, WHETHER OR NOT INFORMED OF THE POSSIBILITIES OF DAMAGES IN ADVANCE. THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION, INCLUDING, WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

The information in this documentation is subject to change without notice. If you find any problems in this documentation, report them to us at infa_documentation@informatica.com.

Informatica products are warranted according to the terms and conditions of the agreements under which they are provided. INFORMATICA PROVIDES THE INFORMATION IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Publication Date: 2024-07-15

Table of Contents

Preface 5

Informatica Resources 5

- Informatica Network 5
- Informatica Knowledge Base 5
- Informatica Documentation 5
- Informatica Product Availability Matrices 6
- Informatica Velocity 6
- Informatica Marketplace 6
- Informatica Global Customer Support 6

Chapter 1: Introduction to Oracle Cloud Object Storage Connector 7

Oracle Cloud Object Storage supported task types and objects types 8

Chapter 2: Oracle Cloud Object Storage connections 9

Prerequisites 9

- Configure Oracle Cloud Infrastructure policies 9
- Prepare for authentication 10

Connect to Oracle Cloud Object Storage 11

- Before you begin 11
- Connection details 11
- Authentication types 11

Proxy server settings 13

Chapter 3: Mappings and tasks for Oracle Cloud Object Storage 14

Sources properties for Oracle Cloud Object Storage 14

Target properties for Oracle Cloud Object Storage 16

- Create a target at runtime 18

File formatting options 19

Data compression for file formats 20

Rules and guidelines for mapping and mapping tasks 20

Chapter 4: Migrating a mapping 21

Use the same object path for the migrated mapping 21

Use a different object path for the migrated mapping 21

- Migration options 22

Rules and guidelines for migrating a mapping 23

Chapter 5: Troubleshooting 24

Troubleshooting for Oracle Cloud Object Storage Connector 24

Appendix A: Data type reference. 25

Avro data types and transformation data types. 25

Flat file data types and transformation data types. 26

ORC data types and transformation data types. 27

Parquet data types and transformation data types. 28

Index. 29

Preface

Use Oracle Cloud Object Storage Connector to learn how to read from or write to Oracle Cloud Object Storage files by using Cloud Data Integration. Learn to create a Oracle Cloud Object Storage connection, run mappings and tasks in Cloud Data Integration.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center through the Informatica Network or by telephone.

To find online support resources on the Informatica Network, click **Contact Support** in the Informatica Intelligent Cloud Services Help menu to go to the **Cloud Support** page. The **Cloud Support** page includes system status information and community discussions. Log in to Informatica Network and click **Need Help** to find additional resources and to contact Informatica Global Customer Support through email.

The telephone numbers for Informatica Global Customer Support are available from the Informatica web site at https://www.informatica.com/services-and-training/support-services/contact-us.html.

CHAPTER 1

Introduction to Oracle Cloud Object Storage Connector

You can use Oracle Cloud Object Storage Connector to read data from or write data to Oracle Cloud Object Storage.

Oracle Cloud Object Storage is agnostic to the data content type and enables a wide variety of use cases. You can send backup and archive data offsite, design big data analytics workloads to generate business insights, or build scale-out web applications. When a read request is made, Oracle Cloud Object Storage serves the most recent copy of the data that was written to the system. The elasticity of the Oracle Cloud Object Storage enables you to start small and scale applications as they evolve, and you always pay for only what you use.

You can store large data sets using Oracle Cloud Object Storage. For example, whether you're storing pharmaceutical or financial data, or multimedia files such as photos and videos, you can use Oracle Cloud Object Storage as your big data object store.

You can use an Oracle Cloud Object Storage connection as a source and as a target in mappings. You can create a mapping task to process data based on the data flow logic defined in a mapping or integration template.

Core components of Oracle Cloud Object Storage

Objects

All data, regardless of content type, is stored as objects in Oracle Cloud Object Storage. For example, log files, video files, and audio files are all stored as objects.

Bucket

A bucket is a logical container that stores objects. Buckets can serve as a grouping mechanism to store related objects together.

Namespace

A namespace is the logical entity that lets you control a personal bucket namespace. Oracle Cloud Object Storage bucket names are not global. Bucket names need to be unique within the context of a namespace, but can be repeated across namespaces. Each tenant is associated with one default namespace (tenant name) that spans all compartments.

Oracle Cloud Object Storage supported task types and objects types

Create assets in Data Integration to integrate data using Oracle Cloud Object Storage Connector.

When you use Oracle Cloud Object Storage Connector, you can include the following Data Integration assets:

- Data transfer task
- Mapping
- Mapping task

For more information about configuring assets and transformations, see *Mappings*, *Transformations*, and *Tasks* in the Data Integration documentation.

CHAPTER 2

Oracle Cloud Object Storage connections

Create a Oracle Cloud Object Storage connection to read data from or write data to Oracle Cloud Object Storage. You can use Oracle Cloud Object Storage connections to specify sources and targets in mappings and mapping tasks.

Prerequisites

Before you create an Oracle Cloud Object Storage connection to read from or write to Oracle Cloud Object Storage, be sure to complete the prerequisites.

Configure Oracle Cloud Infrastructure policies

As a user, you can use Oracle Cloud Object Storage Connector after the organization administrator creates a minimal Oracle Cloud Infrastructure (OCI) Identity and Access Management (IAM) policy for Oracle Cloud Object Storage Connector.

The Oracle Cloud Infrastructure policy defines the resources that users and groups can access in an OCI account and how to access them. You can use policies to manage certain types of resources in a specific compartment in certain ways.

You need to perform the following tasks:

1. Define users, groups, and one or more compartments to hold the cloud resources for your organization.
2. Create the policies.
3. Place users into the appropriate groups depending on the compartments and resources they need to work with.
4. Provide the users with the one-time passwords that they need to access the console and work with the compartments.

For more information about adding users, groups, and policies, see Oracle Cloud Infrastructure documentation.

You can create a policy in the following format:

```
Allow group <group_name> to <verb> <resource-type> in compartment <compartment_name>
```

For example,

```
Allow group ObjectReaders to read buckets in compartment ABC
```

```
Allow group ObjectWriters to manage objects in compartment ABC where any
{request.permission='OBJECT_CREATE', request.permission='OBJECT_INSPECT'}
```

You need to add the following policies to configure the Oracle Cloud Object Storage connection, access objects, and run mappings:

- Policies for Oracle Cloud Object Storage test connection

  ```
  Allow group <group_name> to inspect object-family in compartment <compartment_name>

  Allow group <group_name> to inspect buckets in compartment <compartment_name>
  ```

- Policies for Oracle Cloud Object Storage sources

  ```
  Allow group <group_name> to inspect buckets in compartment <compartment_name>

  Allow group <group_name> to read object-family in compartment <compartment_name>
  ```

- Policies for Oracle Cloud Object Storage targets

  ```
  Allow group <group_name> to manage inspect buckets in compartment <compartment_name>

  Allow group <group_name> to manage object-family in compartment <compartment_name>
  ```

Prepare for authentication

You can configure the following authentication methods for Oracle Cloud Object Storage Connector:

ConfigFile authentication

The ConfigFile authentication uses identity credentials of Oracle Cloud Infrastructure (OCI) account provided through a configuration file for authentication. This authentication method is based on the profile selected in the configuration file.

You can create a configuration file in the following format:

```
[<profile name>]
user=<user ocid>
fingerprint=<fingerprint>
tenancy=<tenancy ocid>
region=<region>
key_file=<private key file location>
```

You require the user OCID, fingerprint, and tenancy OCID information from the OCI account for the configuration file.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the Oracle Cloud Infrastructure documentation.

By default, the OCI configuration file is located at `~/.oci/config` on the Secure Agent machine. The `~/.oci/config` file can contain several profiles. The default profile name is `DEFAULT`. You can change the default profile name to any new profile names based on the profiles that you add to the `~/.oci/config` file. The `~/.oci/config` file cannot contain two profiles with the same name.

Simple authentication

The simple authentication uses API keys for authentication. You can provide the authentication details in the Oracle Cloud Object Storage connection. You need to place the private key file in the Secure Agent machine.

You require the user OCID, fingerprint, and tenancy OCID information from the Oracle Cloud Infrastructure account to create an Oracle Cloud Object Storage connection.

For more information about the steps to extract the identity credentials from the Oracle Cloud Infrastructure Console, see the Oracle Cloud Infrastructure documentation.

Connect to Oracle Cloud Object Storage

Let's configure the Oracle Cloud Object Storage connection properties to connect to Oracle Cloud Object Storage.

Before you begin

Before you get started, configure the Oracle Cloud Infrastructure policies and get the required information from your Oracle Cloud Infrastructure account based on the authentication type that you want to configure.

Check out "Prerequisites" on page 9 to learn more about these tasks.

Connection details

When you create an Oracle Cloud Object Storage connection, configure the connection properties.

The following table describes the basic connection properties:

Property	Description
Connection Name	The name of the connection. Each connection name must be unique within the organization. Connection names can contain alphanumeric characters, spaces, and the following special characters: _ . + -, Maximum length is 255 characters.
Description	The description of the connection. Maximum length is 4000 characters.
Type	Oracle Cloud Object Storage
Runtime Environment	The name of the runtime environment where you want to run tasks. Select a Secure Agent.

Authentication types

You can configure ConfigFile or simple authentication to connect to Oracle Cloud Object Storage. Select the required authentication type and then configure the authentication-specific parameters.
Default is ConfigFile Authentication.

ConfigFile authentication

The following table describes the basic connection properties for ConfigFile authentication:

Property	Description
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.
Bucket Name	The Oracle Cloud Object Storage bucket name that contains the objects.

Advanced settings

The following table describes the advanced connection properties for ConfigFile authentication:

Property	Description
Configuration File Location	The absolute path of the configuration file on the Secure Agent machine. If you do not enter the value, the Secure Agent uses the following configuration file path: `~/.oci/config`
Profile Name	The name of the profile in the configuration file that you want to use. Default is `DEFAULT`.
Folder Path	The folder under the specified Oracle Cloud Object Storage bucket. For example, `bucket/Dir_1/Dir_2/FileName.txt`. Here, `Dir_1/Dir_2` is the folder path.

Simple authentication

The following table describes the basic connection properties for simple authentication:

Property	Description
User OCID	The unique identifier of the user in Oracle Cloud Infrastructure. For example, `ocid1.user.oc1..aaaaaaaaherdgpjknqzrwbdc7n5ksokkot7c5jngtx3pgolr7oqbw7xzksza`
Fingerprint	The fingerprint of the public key.
Tenancy OCID	The unique identifier of the tenancy in Oracle Cloud Infrastructure. The tenancy is the globally unique name of the Oracle Cloud Infrastructure account. For example, `ocid1.tenancy.oc1..aaaaaaaaba3pv6wkcr4jqae5f44n2b2m2yt2j6rx32uzr4h25vqstifsfdsq`
Private Key File Location	The location of the private key file in .PEM format on the Secure Agent machine.
Region	The Oracle Cloud Infrastructure region where the object storage bucket resides. Select the Oracle Cloud Object Storage region from the list.
Bucket Name	The Oracle Cloud Object Storage bucket name that contains the objects.

Advanced settings

The following table describes the advanced connection property for simple authentication:

Property	Description
Folder Path	The folder under the specified Oracle Cloud Object Storage bucket. For example, `bucket/Dir_1/Dir_2/FileName.txt`. Here, `Dir_1/Dir_2` is the folder path.

Proxy server settings

If your organization uses an outgoing proxy server to connect to the Internet, the Secure Agent connects to Informatica Intelligent Cloud Services through the proxy server.

You can configure the Secure Agent to use the proxy server on Windows and Linux. You can use the unauthenticated or authenticated proxy server.

Note: You cannot use a proxy server with managed identity authentication.

You can use one of the following types of proxy servers:

- Unauthenticated proxy - Requires only the host and port address for configuration.
- Authenticated proxy - Requires the host address, port address, user name, and password for configuration.

To configure proxy settings for the Secure Agent, use one of the following methods:

- Configure the Secure Agent through the Secure Agent Manager on Windows or shell command on Linux.

  For instructions, see "Configure the proxy settings on Windows" or "Configure the proxy settings on Linux" in *Getting Started* in the Data Integration help.
- Configure the JVM options for the DTM in the Secure Agent properties. For instructions, see the Proxy server settings Knowledge Base article.

CHAPTER 3

Mappings and tasks for Oracle Cloud Object Storage

You can configure a mapping to read from and write to Oracle Cloud Object Storage files.

Use the Data Integration Mapping Designer to define and configure a mapping or mapping task for Oracle Cloud Object Storage sources and targets.

Sources properties for Oracle Cloud Object Storage

In a mapping, you can configure a Source transformation to represent a Oracle Cloud Object Storage source.

The following table describes the Oracle Cloud Object Storage source properties that you can configure in a Source transformation:

Property	Description
Connection	Name of the source connection. You can select an existing connection, create a new connection, or define parameter values for the source connection property.
Source Type	Type of the source object. Select **Single Object** or **Parameter**.
Parameter	A parameter file where you define values that you want to update without having to edit the task. Select an existing parameter for the source object, or click **New Parameter** to define a new parameter for the source object. The **Parameter** property appears only if you select parameter as the source type. If you want to overwrite the parameter at runtime, select the **Allow parameter to be overridden at run time** option when you create a parameter. When the task runs, the agent uses the parameters from the file that you specify in the advanced session properties.

Property	Description
Object	The source object for the task. Select the source object for a single source.
Format	The file format to read the data. You can select from the following file format types: - Avro - Flat - None - ORC - Parquet Default is None. If you select **None** as the file format type, the connector reads data in binary file format.

The following table describes the advanced properties that you can configure in a Source transformation:

Property	Description
Folder Path	Overrides the folder path value in the Oracle Cloud Object Storage connection.
File Name	Overrides the Oracle Cloud Object Storage source file name.
Staging Directory	Path of the local staging directory. Ensure that the user has write permissions on the directory. In addition, ensure that there is sufficient space to enable staging of the entire file. Default staging directory is the `/temp` directory on the machine that hosts the Secure Agent. The temporary files are created within the new directory.
Encryption Type	Method to decrypt data of the flat and binary file formats. You can select one of the following encryption types: - Informatica Encryption - None Default is None. **Note:** Informatica Encryption uses Informatica crypto libraries to decrypt the data. Ensure that the organization administrator has permission to the Informatica crypto libraries license when you create an Oracle Cloud Object Storage connection.
Multipart Download Threshold	Minimum threshold size to download an Oracle Cloud Object Storage object in multiple parts. To download the object in multiple parts in parallel, ensure that the file size of an Oracle Cloud Object Storage object is greater than the value you specify in this property. **Range**: - Minimum: 4 MB - Maximum: 5 GB Default is 64 MB.
Download Part Size	Downloads the part size of an Oracle Cloud Object Storage object in bytes. **Range**: - Minimum: 4 MB - Maximum: 1GB Default is 32 MB.

Property	Description
Compression Format	Decompresses data when you read data from Oracle Cloud Object Storage. You can choose to decompress data in the following formats: - None - Gzip - Snappy - Deflate - Zlib Default is None. **Note:** You cannot use Deflate, Snappy, and Zlib compression formats even though the options appear in the list. For more information about the supported compression format for each file format, see "Data compression for file formats" on page 20.
Tracing Level	Determines the amount of detail that appears in the log file. You can select Terse, Normal, Verbose Initialization, or Verbose Data. Default is Normal.

Target properties for Oracle Cloud Object Storage

In a mapping, you can configure a Target transformation to represent a Oracle Cloud Object Storage target.

The following table describes the Oracle Cloud Object Storage target properties that you can configure in a Target transformation:

Property	Description
Connection	Name of the target connection. You can select an existing connection, create a new connection, or define parameter values for the target connection property.
Target Type	Type of target object. Select **Single Object** or **Parameter**.
Object	Name of the target object. You can select an existing object or create a new target at run time. When you select **Create New at Runtime**, enter a name and path for the target object and select the source fields that you want to use. By default, all source fields are used. The **Path** attribute is not applicable. The target name can contain alphanumeric characters. You can use only a period (.), an underscore (_), an at the rate sign (@), a dollar sign ($), and a percentage sign (%) special characters in the file name. You can use parameters defined in a parameter file in the target name.
Parameter	A parameter file where you define values that you want to update without having to edit the task. Select an existing parameter for the target object, or click **New Parameter** to define a new parameter for the source object. The **Parameter** property appears only if you select parameter as the source type. If you want to overwrite the parameter at runtime, select the **Allow parameter to be overridden at run time** option when you create a parameter. When the task runs, the agent uses the parameters from the file that you specify in the advanced session properties.

Property	Description
Format	The file format to write the data. You can select from the following file format types: - Avro - Flat - None - ORC - Parquet Default is None. If you select **None** as the file format type, the connector writes data in binary file format.
Operation	The target operation. Select Insert. The other operations are not applicable.

The following table describes the advanced properties that you can configure in a target transformation:

Property	Description
Folder Path	Overrides the folder path value in the Oracle Cloud Object Storage connection. Folder path cannot exceed 255 characters.
File Name	Creates a new file name or overwrites an existing target file name. File name cannot exceed 1024 characters.
Staging Directory	Enter the path of the local staging directory. Ensure that the user has write permissions on the directory. In addition, ensure that there is sufficient space to enable staging of the entire file. Default staging directory is the `/temp` directory on the machine that hosts the Secure Agent. The temporary files are created within the new directory.
Encryption Type	Method to encrypt data of the flat and binary file formats. You can select one of the following encryption types: - Informatica Encryption - None Default is None. **Note:** Informatica Encryption uses Informatica crypto libraries to encrypt the data. Ensure that the organization administrator has permission to the Informatica crypto libraries license when you create an Oracle Cloud Object Storage connection.
Multipart Upload Threshold	Minimum threshold size to upload an Oracle Cloud Object Storage object in multiple parts. To upload the object in multiple parts in parallel, ensure that the file size of an Oracle Cloud Object Storage object is greater than the value you specify in this property. **Range**: - Minimum: 1 MB - Maximum: 50 GB Default is 128 MB.
Upload Part Size	Uploads the part size of an Oracle Cloud Object Storage object in bytes. **Range**: - Minimum: 1 MB - Maximum: 50 GB Default is 128 MB.

Property	Description
Compression Format	Compresses data when you write data to Oracle Cloud Object Storage. You can compress data in the following formats: - Deflate - Gzip - None - Snappy - Zlib Default is None. For more information about the supported compression format for each file format, see "Data compression for file formats" on page 20.
Forward Rejected Rows	Determines whether the transformation passes rejected rows to the next transformation or drops rejected rows. By default, the agent forwards rejected rows to the next transformation.

Create a target at runtime

You can use an existing target or create a target to hold the results of a mapping.

To specify the target properties, perform the following tasks:

1. Select the Target transformation in the mapping.
2. To specify the target, click the **Target** tab.
3. Select the target connection.
4. For the target type, choose **Single Object** or **Parameter**.
5. Specify the target object or parameter.
6. To specify a target object, perform the following tasks:
   a. Click **Select** and choose a target object. You can select an existing target object or create a new target object at runtime.
   b. To create a target object at runtime, select **Create New at Runtime**.
   c. Enter the name for the target file in the **Object Name** field.
   d. If you want the file name to include a time stamp, select **Handle Special Characters** and add special characters to the file name. For example, add the special characters shown here to include all the time stamp information: `Accounts_%d%m%y%T.csv`
   e. Click **Formatting Options** to configure formatting options for the file.
   f. Enter the folder path of the target file in the **Path** field.

      Note: The target file location is relative to the data bucket or data file system name specified in the connection. External target is created if you specify the target file location.
   g. Click **OK**.

Rules and guidelines for creating a target at runtime

When you configure a mapping with the **Create New at Runtime** option, consider the following rules:

- You can create a target file within a folder or in a nested folder. If the specified folder doesn't exist in the bucket, the mapping creates a folder with the given name before creating the target.
- The file name and folder name are case sensitive.
- If you provide an existing target file name, the file is overwritten.

- In a parameterized mapping with object type Binary, the mapping does not consider the folder path and creates the target object in the root folder of the bucket.
- The mapping does not consider the folder path provided in the connection properties and creates the target object in the root folder of the bucket.

File formatting options

You can read and write Avro, Binary, Flat File, ORC, and Parquet formats on Linux. On Windows, you can read and write Binary and Flat File formats.

Certain advanced properties for the Source or Target transformation are applicable to specific file formats.

The following table lists the advanced source properties that you can configure for different file formats:

Advanced source property	File format
Folder Path	Avro, Binary, Flat File, ORC, Parquet
File Name	Avro, Binary, Flat File, ORC, Parquet
Staging Directory	Binary, Flat File
Encryption Type	Binary, Flat File
Multipart Download Threshold	Binary, Flat File
Download Part Size	Binary, Flat File
Tracing Level	Avro, Binary, Flat File, ORC, Parquet

The following table lists the advanced target properties that you can configure for different file formats:

Advanced target property	File format
Folder Path	Avro, Binary, Flat File, ORC, Parquet
File Name	Avro, Binary, Flat File, ORC, Parquet
Compression Format	Avro, ORC, Parquet
Staging Directory	Binary, Flat File
Encryption Type	Binary, Flat File
Multipart Upload Threshold	Binary, Flat File
Upload Part Size	Binary, Flat File
Tracing Level	Avro, Binary, Flat File, ORC, Parquet

Data compression for file formats

You can compress the data when you write data to an Oracle Cloud Object Storage target.

Configure the compression format in the **Compression Format** option under the advanced target properties. The following table lists the supported compression formats in the target for different file formats:

File format	Supported compression format
Avro	Deflate, None, Snappy
Binary	None
Flat File	None
ORC	None, Snappy, Zlib
Parquet	Gzip, None, Snappy

Rules and guidelines for mapping and mapping tasks

Consider the following rules and guidelines when you configure mappings and mapping tasks:

- When the metadata of the source object and override object is different, the mapping fails. If the metadata of the override object matches with the subset of the source object, the mapping runs successfully.
- When you read data from Oracle Cloud Object Storage object, the heap size requirement increases proportionately to the increase in part size.
- When you run a mapping to read a file with a header that contains the at sign (@) special character, the Secure Agent replaces the special character with an underscore (_) in the target.
- When you parameterize the source and target object in a mapping, and you select a file in the task properties, the task displays only the file name instead of the directory along with the file name.
- When you read an ORC file with a size of more than 1 GB, the mapping fails with the following error:
  `Exception in thread "main" java.io.IOException: Problem opening stripe 0 footer in oci://bucket-test@user/test_orc_sf10. Caused by: com.google.protobuf.InvalidProtocolBufferException: Protocol message contained an invalid tag (zero).`

CHAPTER 4

Migrating a mapping

You can configure a connection and mapping in one environment and then migrate and run the mapping in another environment.

After the migration, you can change the connection properties from the Administrator service, but you do not need to modify the mapping. Data Integration uses the configured runtime attributes from the earlier environment to run the mapping successfully in the new environment. The migrated mapping uses the same bucket configured in the connection properties.

Consider a scenario where you develop a mapping in the development organization and you then migrate and run the mapping in the production organization. After you migrate, you might want to use the same or a different connection endpoint in the production organization.

Use the same object path for the migrated mapping

If you want the migrated mapping to use the same object path as in the earlier environment, you must maintain the same folder path and file name in the Oracle Cloud Object Storage account for both the earlier and the new environments.

For example, if you have two different buckets, Bucket1 used for Org 1 and Bucket2 used for Org 2, the object path must be the same in both the buckets. The object path consists of the folder path and the file name.

Bucket1: folder1/filename1

Bucket2: folder1/filename1

You do not need to override the folder path and file name in the advanced properties.

Use a different object path for the migrated mapping

After you migrate the mapping, you can use a different object path to run the mapping from the new environment.

In this scenario, before you migrate the mapping, you can change the object metadata or runtime attributes to reflect the object path in the migrated environment. You do not have to edit or update the mapping in the new environment.

As a rule, when you specify the folder path and file name in the advanced properties or object properties, Data Integration honors the attributes in the following order of precedence:

1. **Runtime advanced attributes**. The advanced properties such as the folder path and file name in the Source, Target, or Lookup transformation in a mapping.
2. **Object metadata**. The object selected in the Source, Target, or Lookup transformation in a mapping.

Migration options

When you migrate, you can choose from one of the following options to update the object path:

Option 1. Update the connection properties to reference the new object

When you import the mapping into Org 2, in the **Review Connections** section, you can change the existing connection to map to the connection that has access to the specified folder path and file name in Org 2.

Option 2. Override the properties from the advanced properties

Before the migration, specify the required folder path and file name for the object from Org 2 in the advanced properties of the Org 1 mapping.

After the migration, when you run the mapping, the Secure Agent uses the configured advanced parameters to override the object specified in the mapping imported from Org 1.

Option 3. Parameterize the properties in the mapping

You can choose to parameterize the advanced attributes, such as the folder path and file name before the migration. You can configure input parameters, in-out parameters, and parameter files in the mapping. After you migrate the mapping, do not edit or update the mapping. If you have used in-out parameters for the advanced attributes such as for the folder path and file name, you can update these from the parameter file.

Parameterizing only the advanced properties, but not the object in the mapping

If you want to parameterize only the advanced properties and use them at runtime, select a placeholder object in the object properties in the mapping and then specify an override to this placeholder object from the advanced properties. Ensure that the placeholder object contains the same metadata as the corresponding table that you specify as an override. When you run the mapping, the value specified in the advanced property overrides the placeholder object.

Parameterizing both the object and the advanced properties

If you want to keep both the Oracle Cloud Object Storage object type and the advanced fields parameterized, you must leave the **Allow parameter to be overridden at runtime** option unselected in the input parameter window while adding the parameters, and then select the required object at the task level. When you run the task, the values specified in the advanced properties take precedence.

Rules and guidelines for migrating a mapping

Consider the following rules and guidelines when you use the same or a different object path for the migrated mapping:

- The following table lists the transformation, object type, and the fields in the advanced properties of a mapping that you can retain when you migrate to the new environment:

Transformations	Object Type	Advanced Fields
Source	Single object	Folder path and file name
Lookup	Single object	
Target	Single object	

- After you migrate the mapping from Org1 to Org2, you must not edit the mapping.
- For an existing target object in Org2, you must specify the folder path and file name in the advanced properties. If the object does not exist in Org2 or the connection does not have access to the object that you used in Org1, the mapping fails.
- Ensure that you specify a valid folder and file name in the advanced properties. Otherwise, the mapping fails.
- You can configure all encryption types, except Informatica encryption, in a mapping that you migrate to the new environment.

CHAPTER 5

Troubleshooting

The topics in this section provide you information on troubleshooting probable issues that you might encounter when you use Oracle Cloud Object Storage Connector.

Troubleshooting for Oracle Cloud Object Storage Connector

"[ERROR] java.lang.OutOfMemoryError: Java heap space" occurs when you select Informatica Encryption as the encryption type and run a mapping to write a file of size 1.4 GB or higher.

To resolve this issue, increase the memory for the Java heap size.

Perform the following tasks to increase the memory using the JVM options in the Secure Agent properties:

1. Select **Administrator** > **Runtime Environments**.
2. On the **Runtime Environments** page, select the Secure Agent for which you want to increase memory from the list of available Secure Agents.
3. In the upper-right corner, click **Edit**.
4. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Server.
5. Edit the **JVMOption1** as **-Xmx8046m**.
6. Restart the Secure Agent manually.

APPENDIX A

Data type reference

Cloud Data Integration uses the following data types in Oracle Cloud Object Storage mappings and mapping tasks:

- Oracle Cloud Object Storage native data types appear in the source and target transformations when you choose to edit metadata for the fields.
- Transformation data types. Set of data types that appear in the transformations. These are internal data types based on ANSI SQL-92 generic data types, which the Secure Agent uses to move data across platforms. They appear in all transformations in a mapping.

When the Secure Agent reads source data, it converts the native data types to the comparable transformation data types before transforming the data. When the Secure Agent writes to a target, it converts the transformation data types to the comparable native data types.

Avro data types and transformation data types

Avro Oracle Cloud Object Storage file data types map to transformation data types that the Secure Agent uses to move data across platforms.

The following table lists the Avro data types that the Secure Agent supports and the corresponding transformation data types:

Avro Oracle Cloud Object Storage File Data Type	Transformation Data Type	Range and Description
Boolean	Integer	TRUE (1) or FALSE (0)
Date	Date/Time	January 1, 0001 to December 31, 9999.
Decimal	Decimal	Precision 18 and 28 digits. Scale 0 to 28. If you specify a precision less than 18 or 28 digits, 18 or 28 is considered as the precision.
Double	Double	Precision 15
Float	Double	Precision 15
Int	Integer	-2,147,483,648 to 2,147,483,647 Precision 10, scale 0

Avro Oracle Cloud Object Storage File Data Type	Transformation Data Type	Range and Description
Long	Bigint	-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 Precision 19, scale 0
Null	Integer	-2,147,483,648 to 2,147,483,647 Precision 10, scale 0
String	String	-1 to 104,857,600 characters
Timestamp - Timestamp_micros - Timestamp_millis - Time_millis - Time_micros	Date/Time	Greater than or equal to 1900-01-01T00:00:00Z

Rules and guidelines for Avro data types

Consider the following rules and guidelines when you use Avro Oracle Cloud Object Storage file data types and transformation data types:

- When you run a mapping to write data to an Oracle Cloud Object Storage target, you cannot use the fixed type of the Avro data type.
- Specify the correct precision and scale in the source file. Otherwise, the decimal point is shifted when you write the source data to a target.
- The source file must have a timestamp value greater than or equal to 1900-01-01T00:00:00Z. Otherwise, the mapping fails with an error.
- When you use the **Create Target** option and modify the precision of an Avro data type in the upstream transformation, the precision is not honored. To resolve the issue, create a target object with the default precision and subsequently edit the precision.

Flat file data types and transformation data types

The following table lists the Flat file data types that the Secure Agent supports and the corresponding transformation data types:

Flat file Oracle Cloud Object Storage Data Type	Transformation Data Type	Range and Description
Number	Decimal	Precision from 1 through 28 digits, scale from 0 through 28 digits
String	String	1 to 104,857,600 characters
Nstring	Text	1 to 104,857,600 characters

Note: The Number and Nstring data types are supported only when you import the flat file by using **Import from Schema File** option.

ORC data types and transformation data types

ORC Oracle Cloud Object Storage file data types map to transformation data types that the Secure Agent uses to move data across platforms.

The following table lists the ORC data types that the Secure Agent supports and the corresponding transformation data types:

ORC Oracle Cloud Object Storage File Data Type	Transformation Data Type	Range and Description
BigInt	BigInt	-9223372036854775808 to 9,223,372,036,854,775,807
Boolean	Integer	TRUE (1) or FALSE (0)
Char	String	1 to 104,857,600 characters
Date	Date/Time	Jan 1, 1753 A.D. to Dec 31, 4712 A.D. (precision to microsecond)
Double	Double	Precision of 15 digits
Float	Double	Precision of 15 digits
Integer	Integer	-2,147,483,648 to 2,147,483,647
SmallInt	Integer	-32,768 to 32,767
String	String	1 to 104,857,600 characters
Timestamp	Date/Time	1 to 19 characters Precision 19 to 26, scale 0 to 6
TinyInt	Integer	-128 to 127
Varchar	String	1 to 104,857,600 characters

Parquet data types and transformation data types

Parquet Oracle Cloud Object Storage file data types map to transformation data types that the Secure Agent uses to move data across platforms.

The following table lists the Parquet data types that the Secure Agent supports and the corresponding transformation data types:

Parquet Oracle Cloud Object Storage File Data Type	Transformation Data Type	Range and Description
Boolean	Integer	TRUE (1) or FALSE (0)
Date	Date/Time	January 1,0001 to December 31,9999
Decimal	Decimal	Precision 18 and 28 digits. Scale 0 to 28. If you specify a precision less than 18 or 28 digits, 18 or 28 is considered as the precision.
Double	Double	Precision 15
Float	Double	Precision 15
Int32	Integer	-2,147,483,648 to +2,147,483,647
Int64	Bigint	-9,223,372,036,854,775,808 to +9,223,372,036,854,775,807 8-byte signed integer
Int96	Binary	12-byte signed integer
String	String	-1 to 104,857,600 characters
Time	Date/Time	Time of the day. Precision to microsecond.
Timestamp - Timestamp_micros - Timestamp_millis - Time_millis - Time_micros - Int96 - Date	Date/Time	January 1,0001 00:00:00 to December 31,9999 23:59:59.997997. Precision to microsecond.

Rules and guidelines for Parquet data types

Consider the following rules and guidelines when you use Parquet Oracle Cloud Object Storage file data types and transformation data types:

- The Secure Agent does not support the following Parquet data types:
  - Timestamp_nanos
  - Time_nanos
  - Timestamp_tz
- The Parquet schema that you specify to read or write a Parquet file must be in lower case. Parquet does not support case-sensitive schema.
- Specify the correct precision and scale in the source file. Otherwise, the decimal point is shifted when you write the source data to a target.

INDEX

C

connection properties
  overview 9

F

File Formatting 19

I

Informatica Global Customer Support
  contact information 6

M

mapping
  Oracle Cloud Object Storage sources 14

O

Oracle Cloud Object Storage connections
  properties 11
Oracle Cloud Object Storage Connector
  overview 7
Oracle Cloud Object Storage Connector *(continued)*
  supported task and object types 8
Oracle Cloud Object Storage data types
  Avro 25
  Flat file 26
  mapping to transformation data types 25–28
  ORC 27
  overview 25
  Parquet 28
Oracle Cloud Object Storage target
  mappings 16

P

Properties 19

S

Source 19
Source Properties 14

T

Target 19
Target Properties 16