Informatica

Informatica® Cloud

Spring 2017

Amazon S3 Connector Guide

Informatica Cloud Amazon S3 Connector Guide
Spring 2017
January 2018

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: 2018-10-16

Table of Contents

Preface 5

Informatica Resources. 5

Informatica Documentation. 5

Informatica Cloud Web Site. 5

Informatica Cloud Communities. 5

Informatica Cloud Marketplace. 6

Informatica Cloud Connector Documentation. 6

Informatica Knowledge Base. 6

Informatica Cloud Trust Site. 6

Informatica Global Customer Support. 6

Chapter 1: Introduction to Amazon S3 Connector. 7

Amazon S3 Connector Overview. 7

Amazon S3 Objects. 8

Amazon S3 Object Format. 8

Data Encryption in Amazon S3 Targets. 8

Administration of Amazon S3 Connector. 9

Create an Access Key ID and Secret Access Key. 9

IAM Authentication. 9

Chapter 2: Amazon S3 Connections. 11

Amazon S3 Connections Overview. 11

Amazon S3 Connection Properties. 12

Chapter 3: Amazon S3 Sources and Targets. 14

Amazon S3 Sources. 14

Client-side Encryption for Amazon S3 Sources. 14

Working with Multiple Files. 14

Partitioning. 16

Amazon S3 Targets. 16

Client-side Encryption for Amazon S3 Targets. 16

Distribution Column. 17

Object Tag. 17

Partitioning. 18

Chapter 4: Data Synchronization Tasks with Amazon S3. 20

Amazon S3 Sources in Data Synchronization Tasks. 20

Amazon S3 Targets in Data Synchronization Tasks. 21

Data Synchronization Task Example. 24

Chapter 5: Mappings and Mapping Configuration Tasks with Amazon S3. 25

Amazon S3 Objects in Mappings. 25

Amazon S3 Sources in Mapping. 25

Amazon S3 Targets in Mapping. 27

Amazon S3 Objects in Mapping Configuration Tasks. 29

Amazon S3 Sources in Mapping Configuration Tasks. 30

Amazon S3 Targets in Mapping Configuration Tasks. 31

Amazon S3 Target File Parameterization. 33

Appendix A: Data Type Reference. 35

Data Type Reference Overview. 35

Appendix B: Troubleshooting. 36

Troubleshooting Overview. 36

Troubleshooting for Amazon S3 Connector. 36

Index. 37

Preface

The *Informatica Cloud Amazon S3 Connector Guide* contains information about how to set up and use Amazon S3 Connector. The guide explains how organization administrators and business users can use Amazon S3 Connector to read from and write data to Amazon S3.

Informatica Resources

Informatica Documentation

To get the latest documentation for your product, browse the Informatica Knowledge Base at https://kb.informatica.com/_layouts/ProductDocumentation/Page/ProductDocumentSearch.aspx.

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

Informatica Cloud Web Site

You can access the Informatica Cloud web site at http://www.informatica.com/cloud. This site contains information about Informatica Cloud editions and applications as well as information about other Informatica Cloud integration services.

Informatica Cloud Communities

Use the Informatica Cloud Community to discuss and resolve technical issues in Informatica Cloud. You can also find technical tips, documentation updates, and answers to frequently asked questions.

Access the Informatica Cloud Community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration

To find resources on using Application Integration (the Informatica Cloud Real Time service), access the community at:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-application-integration/content

Developers can learn more and share tips at the Cloud Developer community:

https://network.informatica.com/community/informatica-network/products/cloud-integration/cloud-developers

Informatica Cloud Marketplace

Visit the Informatica Marketplace to try and buy Informatica Cloud Connectors, templates, and mapplets:

https://marketplace.informatica.com/community/collections/cloud_integration

Informatica Cloud Connector Documentation

You can access documentation for Informatica Cloud Connectors at the Informatica Cloud Community: https://network.informatica.com/cloud/index.htm

You can also download individual connector guides: https://network.informatica.com/docs/DOC-15333.

Informatica Knowledge Base

Use the Informatica Knowledge Base to search Informatica Network for product resources such as documentation, how-to articles, best practices, and PAMs.

To access the Knowledge Base, visit https://kb.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 Cloud Trust Site

Subscribe to the Informatica trust site for upgrade, maintenance, and incident notifications.

Status.Informatica.com displays the production status of all the Informatica cloud products. All maintenance updates are posted to this status page, and during an outage, it will have the most current information. To ensure you are notified of updates and outages, you can subscribe to a single component, a single incident, or the site as a whole. Subscribing to the site as a whole is the best way to be certain you never miss an update. To subscribe, go to http://status.informatica.com and click **SUBSCRIBE TO UPDATES**. You can then choose to receive notifications sent as emails, SMS text messages, webhooks, RSS feeds, or any combination of the four.

Informatica Global Customer Support

You can contact a Customer Support Center by telephone or online.

For online support, click **Submit Support Request** in Informatica Cloud. You can also use Online Support to log a case. Online Support requires a login. You can request a login at https://network.informatica.com/welcome.

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 Amazon S3 Connector

This chapter includes the following topics:

- Amazon S3 Connector Overview, 7
- Amazon S3 Objects, 8
- Administration of Amazon S3 Connector, 9

Amazon S3 Connector Overview

You can use Amazon S3 Connector to connect Informatica Cloud and Amazon S3.

Amazon S3 is a cloud-based store that stores many objects in one or more buckets. You can also connect to Amazon S3 buckets available in Virtual Private Cloud (VPC) through VPC endpoints.

You can read from or write to multiple Amazon S3 sources and targets. Use Amazon S3 Connector to read delimited file data from and write delimited file data to Amazon S3. You can upload or download a large object as a set of multiple independent parts.

Create an Amazon S3 connection to specify the location of Amazon S3 sources and targets you want to include in a task. You can use the Amazon S3 connection in Data Synchronization tasks, mappings, and Mapping Configuration tasks. Create a Data Synchronization task to synchronize data between a source and target. Create a Mapping Configuration task to process data based on the data flow logic defined in a mapping or integration template.

Example

You are a medical data analyst in a medical and pharmaceutical organization who maintains patient records. A patient record can contain patient details, doctor details, treatment history, and insurance from multiple data sources.

You use Amazon S3 Connector to collate and organize the patient details from multiple input sources in Amazon S3 buckets.

Amazon S3 Objects

Amazon S3 Connector sources and targets represent delimited file data objects that are read from or written to Amazon S3 buckets as delimited files.

Use Amazon S3 Connector to read delimited files from Amazon S3 and to insert data to delimited files in Amazon S3 buckets.

Amazon S3 Object Format

Amazon S3 objects are delimited files. All fields in a delimited file are of string data type with a data format that you cannot change and with a defined precision of 256. Data in Amazon S3 delimited files is written in String 256 format.

Amazon S3 Connector accepts target data with a precision greater than 256. You do not need to change the precision in the Target transformation.

To read source data with a precision greater than 256, increase the precision in the Source transformation to view the complete data.

To write Amazon S3 source data to any relational target data source, you can specify field expressions in the **Field Mapping** page. The Secure Agent converts the Amazon S3 string data to the target data format.

An Amazon S3 delimited file uses the following data format by default:

- The delimiter is a comma.
- The qualifier is a double-quote.
- The escape character is a backslash.

Use **Formatting Options** to override the default data format values.

When you read data from or write data to an Amazon S3 file, the application might display an exception when you select incorrect **Formatting Options**. You must select valid **Formatting Options** and proceed with the task.

Backslash is the default escape character in the formatting options. Specify a different escape character when you read data from an Amazon S3 file and escape is a part of data.

When you write data to an Amazon S3 file, if there is a single or double quote in the source data, an extra quote is added to the target.

For Amazon S3, you cannot specify space, semi colon, and comma as delimiters in the **Other** option under **Formatting Options**.

Data Encryption in Amazon S3 Targets

To protect data, you can enable server-side encryption or client-side encryption to encrypt data inserted in Amazon S3 buckets. You can encrypt data by using the master symmetric key or customer master key. Do not use the master symmetric key and customer master key together.

Customer master key is a user managed key generated by AWS Key Management Service (AWS KMS) to encrypt data.

Master symmetric key is a 256-bit AES encryption key in the Base64 format that is used to enable client-side encryption. You can generate master symmetric key by using a third-party tool.

Server-side Encryption

Enable server-side encryption if you want to use Amazon S3-managed encryption key or AWS KMS-managed customer master key to encrypt the data while uploading the delimited files to the buckets. To enable server-side encryption, select Server Side Encryption as the encryption type in the advanced target properties on the **Schedule** page.

Client-side Encryption

Enable client-side encryption if you want the Secure Agent to encrypt the data while uploading the delimited files to the buckets. To enable client-side encryption, perform the following tasks:

1. Provide a master symmetric key or customer master key ID when you create an Amazon S3 connection.

   Note: The administrator user of the account can use the default customer master key ID to enable the client-side encryption.
2. Select Client Side Encryption as the encryption type in the advanced target properties on the **Schedule** page.
3. Ensure that an organization administrator updates the security policy .jar files on each Secure Agent machine in the runtime environment.

Administration of Amazon S3 Connector

As a user, you can use Amazon S3 Connector after the organization administrator performs the following tasks:

- Mandatory. Create an Access Key ID and Secret Access Key.
- Optional. Enable client-side encryption.
- Optional. Create minimal Amazon S3 bucket policy for Amazon S3 Connector.

Create an Access Key ID and Secret Access Key

1. Log in to Amazon Web Services and navigate to the Security Credentials page.
2. Expand the **Access Keys** section, and click **Create New Access Key**.
3. Click the **Show Access Key** link.
4. Click **Download Key File** and save the file on the Secure Agent machine.

IAM Authentication

Optional. You can configure IAM authentication when the Secure Agent runs on an Amazon Elastic Compute Cloud (EC2) system. Use IAM authentication for secure and controlled access to Amazon S3 resources when you run a session.

Perform the following steps to configure IAM authentication:

1. Create Minimal Amazon S3 Bucket Policy. For more information, see “Create Minimal Amazon S3 Bucket Policy” on page 10
2. Create the Amazon EC2 role. The Amazon EC2 role is used when you create an EC2 system in the S3 bucket. For more information about creating the Amazon EC2 role, see the AWS documentation.
3. Create an EC2 instance. Assign the Amazon EC2 role that you created in step #2 to the EC2 instance.

4. Install the Secure Agent on the EC2 system.

Create Minimal Amazon S3 Bucket Policy

The minimal Amazon S3 bucket policy restricts user operations and user access to particular Amazon S3 buckets by assigning an AWS Identity and Access Management (IAM) policy to users.

You can configure the IAM policy through the AWS console. Use AWS Identity and Access Management (IAM) authentication to securely control access to Amazon S3 resources. If you have valid AWS credentials and you want to use IAM authentication, you do not have to specify the access key and secret key when you create an Amazon S3 connection.

You can use the following minimum required actions for users to successfully read data from and write data to Amazon S3 bucket:

- PutObject
- GetObject
- DeleteObject
- ListBucket
- GetBucketPolicy

Sample Policy:

```
{

"Version": "2012-10-17", "Statement": [

{ "Effect": "Allow", "Action": [ "s3:PutObject", "s3:GetObject", "s3:DeleteObject",
"s3:ListBucket", "s3:GetBucketPolicy" ], "Resource":
[ "arn:aws:s3:::<specify_bucket_name>/*", "arn:aws:s3:::<specify_bucket_name>" ] }

]

}
```

CHAPTER 2

Amazon S3 Connections

This chapter includes the following topics:

- Amazon S3 Connections Overview, 11
- Amazon S3 Connection Properties, 12

Amazon S3 Connections Overview

Amazon S3 connections enable you to read data from or write data to Amazon S3. You can use Amazon S3 connections to specify sources and targets in Data Synchronization tasks, mappings, and Mapping Configuration tasks.

If you configure the JVM options of the Secure Agent to include proxy server details, the Secure Agent connects to Amazon S3 using a proxy server

You can use AWS Identity and Access Management (IAM) authentication to securely control access to Amazon S3 resources. If you have valid AWS credentials and you want to use IAM authentication, you do not have to specify the access key and secret key when you create an Amazon S3 connection.

Create a connection and associate it with a Data Synchronization task, mapping, or Mapping Configuration task. Define the source and target properties to read data from or write data to Amazon S3.

You create an Amazon S3 connection on the **Connections** page. You can then use the connection in the Mapping Designer when you create a mapping or in the Data Synchronization Task wizard when you create a task.

Amazon S3 Connection Properties

When you set up an Amazon S3 connection, you must configure the connection properties.

The following table describes the Amazon S3 connection properties:

Connection Property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks.
Access Key	The access key ID used to access the Amazon account resources. Required if you do not use AWS Identity and Access Management (IAM) authentication. **Note:** Ensure that you have valid AWS credentials before you create a connection.
Secret Key	The secret access key used to access the Amazon account resources. This value is associated with the access key and uniquely identifies the account. You must specify this value if you specify the access key ID. Required if you do not use AWS Identity and Access Management (IAM) authentication.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, `<bucket name>/<my folder name>`
Master Symmetric Key	Optional. Provide a 256-bit AES encryption key in the Base64 format when you enable client-side encryption. You can generate a key using a third-party tool. If you specify a value, ensure that you specify the encryption type as client side encryption in the advanced target properties in the **Schedule** page.
Customer Master Key ID	Optional. Specify the customer master key ID or alias name generated by AWS Key Management Service (AWS KMS). You must generate the customer master key for the same region where Amazon S3 bucket reside. You can specify any of the following values: - **Customer generated customer master key**: to enable client-side or server-side encryption. - **Default customer master key**: to enable client-side or server-side encryption. Only the administrator user of the account can use the default customer master key ID to enable client-side encryption.

Connection Property	Description
Code Page	The code page compatible with the Amazon S3 source. Select one of the following code pages: - MS Windows Latin 1. Select for ISO 8859-1 Western European data. - UTF-8. Select for Unicode and non-Unicode data. - Shift-JIS. Select for double-byte character data. - ISO 8859-15 Latin 9 (Western European). - ISO 8859-2 Eastern European. - ISO 8859-3 Southeast European. - ISO 8859-5 Cyrillic. - ISO 8859-9 Latin 5 (Turkish). - IBM EBCDIC International Latin-1.
Region Name	Specify the name of the region where the Amazon S3 bucket is available and for which you generated the customer master key ID. Select one of the following regions: - Asia Pacific (Tokyo) - Asia Pacific (Seoul) - Asia Pacific (Singapore) - Asia Pacific (Sydney) - AWS GovCloud - China (Beijing) - EU (Ireland) - EU (Frankfurt) - South America (Sao Paulo) - US East (N. Virginia) - US West (N. California) - US West (Oregon) - US East (Ohio) - Canada (Central) - Asia Pacific (Mumbai) You can only read from or write data to the regions supported by AWS SDK used by the Amazon S3 connector.

CHAPTER 3

Amazon S3 Sources and Targets

This chapter includes the following topics:

- Amazon S3 Sources, 14
- Amazon S3 Targets, 16

Amazon S3 Sources

You can use an Amazon S3 object as a source in a Data Synchronization task, mapping, or Mapping Configuration task.

You can use single Amazon S3 standard object as sources in a Data Synchronization task, mapping, or Mapping Configuration task. When you configure the advanced source properties, you configure properties specific to Amazon S3.

Client-side Encryption for Amazon S3 Sources

Client-side encryption is a technique to encrypt data before transmitting the data to the Amazon S3 server.

When you enable client-side encryption for Amazon S3 sources, Amazon S3 unloads the data in encrypted format, and then pushes the data to the Secure Agent. The Secure Agent writes the data to the target based on the task or mapping logic.

To enable client-side encryption, you must provide a master symmetric key or customer master key in the connection properties. The Secure Agent encrypts the data by using the master symmetric key or customer master key. To enable client-side encryption, perform the following tasks:

1. Provide a master symmetric key or customer master key.
2. Update the security policy `.jar` files on each Secure Agent machine in the runtime environment. Update the `local_policy.jar` and the `US_export_policy.jar` files in the following directory:

   `<Secure Agent installation directory>\jre\lib\security`.

   You can download the `.jar` files supported by the JAVA environment on the Secure Agent machine from the Oracle website.

Working with Multiple Files

You can read from multiple Amazon S3 sources and write to a single target.

To read multiple files, all files must be available in the same Amazon S3 bucket. When you want to read from multiple sources in the Amazon S3 bucket, you must create a `.manifest` file that contains all the source files with the respective absolute path or directory path. You must specify the `.manifest` file name in the following format: `<file_name>.manifest`

For example, the `.manifest` file contains source files in the following format:

```
{
 "fileLocations": [{
 "URIs": [
 "dir1/dir2/file_1.csv",
 "dir1/dir2/dir4/file_2.csv",
 "dirA/dirB/file_3.csv",
 "dirA/dirB/file_4.csv"
 ]
 }, {
 "URIPrefixes": [
 "dir1/dir2/",
 "dir1/dir2/"]
 }
 ],
 "settings": {
 "stopOnFail": "true"
 }
}
```

The **Data Preview** tab displays the data of the first file available in the URI specified in the `.manifest` file. If the URI section is empty, the first file in the folder specified in URIPrefixes is displayed.

You can specify an asterisk (*) wildcard in the file name to fetch files from the Amazon S3 bucket. You can specify the asterisk (*) wildcard to fetch all the files or only the files that match the name pattern. Specify the wildcard character in the following format:

```
abc*.txt
abc.*
```

For example, if you specify `result*.txt`, all the file names starting with the term `result` and ending with the `.txt` file extension are read. If you specify `result.*`, all the file names starting with the term `result` are read regardless of the extension.

Use the wildcard character to specify files from a single folder. For example,

```
{
 "fileLocations": [{
 "URIs": [
 "dir1/dir2/file_1.csv",
 "dir1/dir2/dir4/file_2.csv",
  ]
 }, {
 "URIPrefixes": [
 "dir1/dir2/",
 "dir1/dir2/"]
 }
 ],
{ "WildcardURIs": [ "multiread_wildcard/file_1/*.csv" ] }
 ]
"settings": {
 "stopOnFail": "true"
 }
}
```

You cannot use the wildcard characters to specify folder names. For example,

```
{ "WildcardURIs": [ "multiread_wildcard/dir1*/", "multiread_wildcard/*/" ] }
```

Note: Amazon S3 Connector supports only asterisk (*) wildcard character.

You can configure the `stopOnFail` property to display error messages while reading multiple files. Set the value to true, if you want the Secure Agent to display error messages if the read operation fails for any of the source files. If you set the value to false, the error messages appear only in the session log. The Secure Agent skips the file that generated the error and continues to read other files.

Partitioning

You can configure partitioning to optimize the mapping performance at run time when you read data from Amazon S3 sources.

The partition type controls how the agent distributes data among partitions at partition points. You can define the partition type as passthrough partitioning. With partitioning, the Secure Agent distributes rows of source data based on the number of threads that you define as partition.

You can specify the value of the **Number of Partition** field in the **Partition** tab under the mapping task to configure partitioning for Amazon S3 sources. The Secure Agent configures the partition for Amazon S3 sources based on the value you enter in the **Number of Partition** field. By default, the value of the **Number of Partition** field is one.

The Secure Agent enables the partition according to the size of the Amazon S3 source file. The file name is appended with a number starting from 0 in the following format: `<file name>_<number>`

Note: If you enable partitioning and the precision for the source column is less than the maximum data length in that column, you might receive unexpected results. To avoid unexpected results, the precision for the source column must be equal to or greater than the maximum data length in that column for partitioning to work as expected.

Amazon S3 Targets

You can use an Amazon S3 object as a single target in a Data Synchronization task, mapping, or Mapping Configuration task.

You can also create an Amazon S3 target based on the input source. When you configure the advanced target properties, you configure properties specific to Amazon S3. If a mapping includes a flat file or an Amazon S3 target, you can choose to use an existing target or create a new target at run time.

Client-side Encryption for Amazon S3 Targets

Client-side encryption is a technique to encrypt data before transmitting the data to the Amazon S3 server.

When you enable client-side encryption for Amazon S3 targets, the Secure Agent fetches the data from the source, encrypts the data, and then writes the data to an Amazon S3 bucket.

To enable client-side encryption, you must provide a master symmetric key or customer master key in the connection properties. The Secure Agent encrypts the data by using the master symmetric key or customer master key. To enable client-side encryption, perform the following tasks:

1. Provide a master symmetric key or customer master key.
2. Update the security policy `.jar` files on each Secure Agent machine in the runtime environment.
   Update the `local_policy.jar` and the `US_export_policy.jar` files in the following directory:

   `<Secure Agent installation directory>\jre\lib\security`.

   You can download the `.jar` files supported by the JAVA environment on the Secure Agent machine from the Oracle website.

Distribution Column

You can write multiple files to Amazon S3 target from a single source. Configure the **Distribution Column** option in the advanced target properties.

You can specify one column name in the **Distribution Column** field to create multiple target files during run time. When you specify the column name, the Secure Agent creates multiple target files in the column based on the column values that you specify in **Distribution Column**.

Each target file name is appended with the **Distribution Column** value in the following format:

```
<Target_fileName>+_+<Distribution column value>+<file extension>
```

Each target file contains all the columns of the table including the column that you specify in the **Distribution Column** field.

For example, the name of the target file is `Region.csv` that contains the values North America and South America. The following target files are created based on the values in the **Distribution Column** field:

```
Region_North America.csv
Region_South America.csv
```

You cannot specify two column names in the **Distribution Column** field. If you specify a column name that is not present in target field column, the task fails.

When you specify a column that contains value with special characters in the **Distribution Column** field, the Secure Agent fails to create target file if the corresponding Operating System do not support the special characters.

For example, the Secure Agent fails to create target file if the column contains date value in the following format: YYYY/MM/DD

Object Tag

You can add a tag to the object stored on the Amazon S3 bucket. Each tag contains a key value pair.

Tagging an object helps to categorize the storage. You can add the object tags in the **Object Tags** field under the advanced target properties. Enter the object tag in the `Key=Value` format. You can also enter multiple object tags in the following format:

```
Key1=Value1
Key2=Value2
```

You can either enter the key value pairs or the specify the file path that contains the key value pairs. For example, you can specify the file path in the `C:\object\tags.txt` format. You can specify any file path on which the Secure Agent is installed.

When you upload new objects in the Amazon S3 bucket, you can add tags to the new objects or add tags to the existing objects. If the Secure Agent overrides a file that contains a tag in the Amazon S3 bucket, the tag is not retained. You must add a new tag for the overridden file. If you upload multiple files to the Amazon S3 bucket, each file that you upload must have the same set of tags associated with the multiple objects.

To add tags in the Amazon S3 target object, you must add the `s3:PutObjectTagging` permission in the Amazon S3 policy. Following is the sample policy:

```
{
"Version": "2012-10-17",
"Id": "Policy1500966932533",
"Statement": [
{
"Sid": "Stmt1500966903029",
"Effect": "Allow",
"Principal": "*",
"Action": [
"s3:DeleteObject",
"s3:GetBucketPolicy",
"s3:GetObject",
"s3:ListBucket",
"s3:PutObject",
"s3:PutObjectTagging"
],
"Resource": [
"arn:aws:s3:::<bucket_name>/*",
"arn:aws:s3:::<bucket_name>"
]
}
]
}
```

The following table lists the special characters that Amazon S3 Connector supports during entering the key value pair:

Special Characters	Support
+	Yes
-	Yes
=	No
.	Yes
_	Yes
:	Yes
/	Yes

Rules and Guidelines for Tagging an Object

Use the following rules and guidelines for tagging an object:

- You can add maximum 10 tags for each object.
- When you enter a tag for an object, the tag must contain a unique tag key.
- The tag key can contain maximum 128 Unicode characters in length and tag values can contain maximum 256 Unicode characters in length.
- The key and values are case sensitive.

Partitioning

You can configure partitioning to optimize the mapping performance at run time when you write data to Amazon S3 targets.

The partition type controls how the agent distributes data among partitions at partition points. You can define the partition type as passthrough partitioning. With partitioning, the Secure Agent distributes rows of target data based on the number of threads that you define as partition.

You can configure the **Merge Partition Files** options in the advanced target properties. You can specify whether the Secure Agent must merge the number of partition files as a single file or maintain separate files based on the number of partitions specified to write data to the Amazon S3 targets.

If you do not select the **Merge Partition Files** option, separate files are created based on the number of partitions specified. The file name is appended with a number starting from 0 in the following format: `<file name>_<number>`

For example, the number of threads for the `Region.csv` file is three. If you do not select the **Merge Partition Files** option, the Secure Agent writes three separate files in the Amazon S3 target in the following format:

```
<Region_0>
<Region_1>
<Region_2>
```

If you configure the **Merge Partition Files** option, the Secure Agent merges all the partitioned files as a single file and writes the file to Amazon S3 target.

CHAPTER 4

Data Synchronization Tasks with Amazon S3

This chapter includes the following topics:

- Amazon S3 Sources in Data Synchronization Tasks, 20
- Amazon S3 Targets in Data Synchronization Tasks, 21
- Data Synchronization Task Example, 24

Amazon S3 Sources in Data Synchronization Tasks

When you configure a Data Synchronization task to use an Amazon S3 source, you can configure the source properties.

The source properties appear on the **Source** page of the Data Synchronization Task wizard when you specify an Amazon S3 connection. When you create a task with Amazon S3 as lookup, the lookup condition does not get applied.

The following table describes the Amazon S3 source properties:

Source Property	Description
Connection Type	Name of the source connection.
Source Type	Select **Single** as the source type.
Source Object	Select the source object for the task.
Formatting Options	Amazon S3 format options. Opens the **Formatting Options** dialog box to define the format of the file. Default is delimited. Configure the following format options: - Delimiter: Delimiter character. You can configure other parameters such as comma, tab, colon, semicolon, or others. - Text Qualifier: Character to qualify text. You can configure other parameters such as single quote or double quote. - Escape: Escape character.

The following table describes the Amazon S3 advanced source properties:

Property	Description
Enable Downloading S3 File in Multiple Parts	Downloads large Amazon S3 objects in multiple parts. The Secure Agent downloads the object in multiple parts from Amazon S3. When the file size of an Amazon S3 object is greater than 5 MB, you can choose to download the object in multiple parts in parallel.
Header Line Number	Specify the line number that you want to use as the header when you read data from Amazon S3. Default is 0.
Read Data From Line	Specify the line number from where you want the Secure Agent to read data. Default is 1. **Note:** To read data from the header, the value of the **Header Line Number** and the **Read Data From Line** fields should be the same.
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Part Size	Specifies the part size of an object. Default is 5 MB.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization or verbose data. Default is normal.

Amazon S3 Targets in Data Synchronization Tasks

When you configure a Data Synchronization task to write to an Amazon S3 target, you can configure the target properties.

The target properties appear on the **Target** page of the Data Synchronization Task wizard.

The following table describes the Amazon S3 target properties:

Source Property	Description
Connection	Name of the target connection.
Target Object	Specify the target object for the task.
Formatting Options	Amazon S3 format options. Opens the **Formatting Options** dialog box to define the format of the file. Default is delimited. Configure the following format options: - Delimiter: Delimiter character. You can configure other parameters such as comma, tab, colon, semicolon, or others. - Text Qualifier: Character to qualify text. You can configure other parameters such as single quote or double quote. - Escape: Escape character.
Create Target	Creates a target. Enter a name for the target object and select the source fields that you want to use. Default name is the source object name and by default, all source fields are used. Optionally, enter a file extension for the target object. 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. If you select the advanced source property compression type at run time, the file will be generated with a .gz extension. The .gz file will contain the data.
Child Object	Not applicable.

You can also configure advanced target properties when you schedule the Data Synchronization task. Advanced target properties appear on the **Schedule** page of the Data Synchronization Task wizard.

The following table describes the Amazon S3 advanced target properties:

Advanced Target Property	Description
Encryption Type	Method you want to use to encrypt data. Select one of the following values: - None. The data is not encrypted. - Client Side Encryption. - The Secure Agent encrypts data while uploading the delimited files to Amazon buckets. - You must select client-side encryption in the advanced properties if you specify a master symmetric key or customer master key ID in the Amazon S3 connection properties. - Server Side Encryption. - You must select server-side encryption in the advanced properties if you specify a customer master key ID in the Amazon S3 connection properties. - If you select the server-side encryption in the advanced properties and do not specify the customer master key ID in the connection properties, Amazon S3-managed encryption keys are used to encrypt data.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, `<bucket name>/<my folder name>` The folder path specified at run time overrides the path specified while creating a connection.

Advanced Target Property	**Description**
Part Size	Specifies the part size of an object. Default is 5 MB.
TransferManager Thread Pool Size	Specifies the number of the threads to write data in parallel. Amazon S3 Connector uses the AWS TransferManager API to upload a large object in multiple parts to Amazon S3. When the file size is more than 5 MB, you can configure multipart upload to upload object in multiple parts in parallel. If you set the value of the **TransferManager Thread Pool Size** to greater than 50, the value reverts to 50. Default is 10.
Merge Partition Files	Not applicable.
Distribution Column	Specify the name of the column to create multiple target files during run time.
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Object Tags	You can add single or multiple tags to the objects stored on the Amazon S3 bucket. You can either enter the key value pairs or specify the file path that contains the key value pairs. For more information, see "Object Tag" on page 17.
Success File Directory	Not applicable.
Error File Directory	Not applicable.

Data Synchronization Task Example

You are a data administrator in a product organization. You want to collate legacy sales data from multiple sources and archive it on Amazon S3.

You can read data from multiple sources and use Amazon S3 Connector to upload data to Amazon S3. Configure a Data Synchronization task to consolidate sales data based on product ID and upload data to Amazon S3.

You perform the following Data Synchronization tasks:

Define the Data Synchronization task.

Configure a Data Synchronization task to use the insert operation.

Create the MySQL source objects.

The source for the mapping is a MySQL connection that connects to the sales data. The MySQL object contains multiple source objects in the Data Synchronization task.

The sales_record MySQL object includes the *Row_id*, *Order_id*, *Order_Quantity*, *Order_Date*, *Unit_Price*, *Region*, and *Product_Category* source fields.

The dim_product MySQL object includes the *Product_ID*, *Product_Name*, and *Load_Date* source fields.

Define a relationship the multiple source objects.

Add a join condition between the source field in the sales_record object and the dim_product object to define the following relationship: `sales_record.Product_Category=dim_product.Product_ID`

Create an Amazon S3 target object.

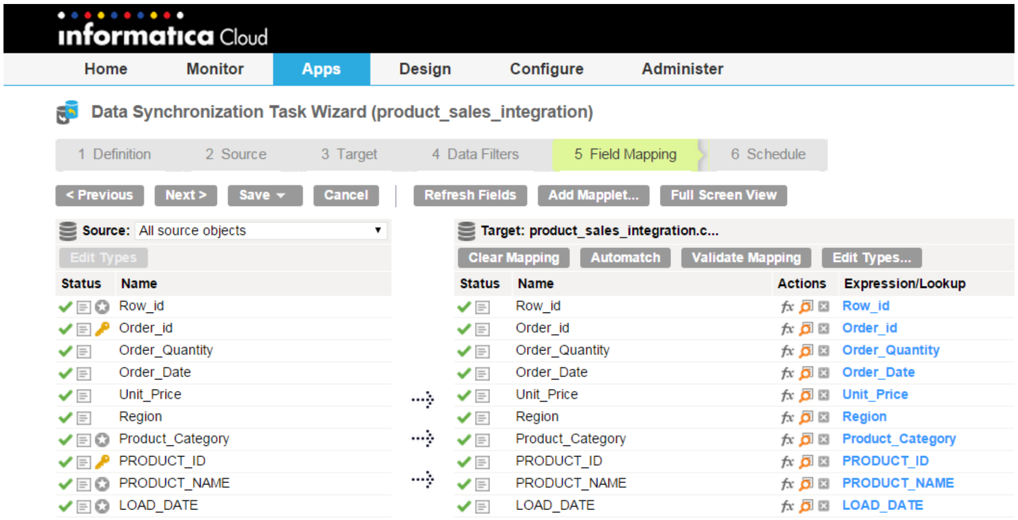
The target for the mapping is an Amazon S3 bucket. Specify the target connection as Amazon S3, the target object as the name of the delimited file into which you want to insert the data. Select the target operation as the insert operation.

Configure a field mapping.

Map the source fields to the target fields.

When you run the task, the Data Synchronization application writes the collated source data to the target delimited file. If you specify the name of an existing file, the Secure Agent replaces all data in the file.

The following image shows a mapping of the MySQL source objects and the Amazon S3 target file:



Data Synchronization Task Wizard (product_sales_integration)

Source: All source objects

Status	Name
✓	Row_id
✓	Order_id
✓	Order_Quantity
✓	Order_Date
✓	Unit_Price
✓	Region
✓	Product_Category
✓	PRODUCT_ID
✓	PRODUCT_NAME
✓	LOAD_DATE

Target: product_sales_integration.c...

Status	Name	Actions	Expression/Lookup
✓	Row_id	fx	Row_id
✓	Order_id	fx	Order_id
✓	Order_Quantity	fx	Order_Quantity
✓	Order_Date	fx	Order_Date
✓	Unit_Price	fx	Unit_Price
✓	Region	fx	Region
✓	Product_Category	fx	Product_Category
✓	PRODUCT_ID	fx	PRODUCT_ID
✓	PRODUCT_NAME	fx	PRODUCT_NAME
✓	LOAD_DATE	fx	LOAD_DATE

CHAPTER 5

Mappings and Mapping Configuration Tasks with Amazon S3

This chapter includes the following topics:

- Amazon S3 Objects in Mappings, 25
- Amazon S3 Objects in Mapping Configuration Tasks, 29
- Amazon S3 Target File Parameterization, 33

Amazon S3 Objects in Mappings

When you create a mapping, you can configure a Source or Target transformation to represent an Amazon S3 object.

Amazon S3 Sources in Mapping

To read data from Amazon S3, configure an Amazon S3 object as the Source transformation in a mapping.

Specify the name and description of the Amazon S3 source. Configure the source and advanced properties for the source object. When you create a task with Amazon S3 as lookup, the lookup condition does not get applied.

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

Property	Description
Connection Name	Name of the source connection.
Source Type	Source type. Select one of the following types: - Single Object. - Parameter. Select **Parameter** to define the source type when you configure the Mapping Configuration task.

Property	Description
Object	Source object for the mapping.
Formatting Options	Amazon S3 format options. Opens the **Formatting Options** dialog box to define the format of the file. Default is delimited. Configure the following format options: - Delimiter: Delimiter character. You can configure other parameters such as comma, tab, colon, semicolon, or others. - Text Qualifier: Character to qualify text. You can configure other parameters such as single quote or double quote.

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

Property	Description
Enable Downloading S3 File in Multiple Parts	Downloads large Amazon S3 objects in multiple parts. The Secure Agent downloads the object in multiple parts from Amazon S3. When the file size of an Amazon S3 object is greater than 5 MB, you can choose to download the object in multiple parts in parallel.
Header Line Number	Specify the line number that you want to use as the header when you read data from Amazon S3. Default is 0.
Read Data From Line	Specify the line number from where you want the Secure Agent to read data. Default is 1. **Note:** To read data from the header, the value of the **Header Line Number** and the **Read Data From Line** fields should be the same.
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Part Size	Specifies the part size of an object. Default is 5 MB.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization or verbose data. Default is normal.

Amazon S3 Targets in Mapping

To insert data to Amazon S3, configure an Amazon S3 object as the target in a mapping.

Specify the name and description of the Amazon S3 target. Configure the target and advanced properties for the target object.

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

Property	Description
Connection	Name of the target connection.
Target Type	Target type. Select one of the following types: - Single Object. - Parameter. Select **Parameter** to define the target type when you configure the task.
Object	Name of the target object. You can select an existing object or create an object at runtime.
Create Target	Creates a target. 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 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. When you specify the name and path for the target object, the object is created in the specified path under the bucket name and folder name specified in the connection properties. For example, if you specify `Finance/Reports` in the Folder name in the connection properties and `East/Sample/Report1` in the Create Target property, the target with name `Report1` will be created under `Finance/Reports/East/Sample`. **Note:** Do not use a single slash (/) in the beginning of the path. Do not use double slash (//) or double dots (..) in the path.
Formatting Options	Amazon S3 format options. Opens the **Formatting Options** dialog box to define the format of the file. Default is delimited. Configure the following format options: - Delimiter: Delimiter character. You can configure other parameters such as comma, tab, colon, semicolon, or others. - Text Qualifier: Character to qualify text. You can configure other parameters such as single quote or double quote. - Escape: Escape character.
Operation	Select the target operation. The Amazon S3 target is a delimited file and you can run the task with only the insert operation. When you run the task, the Secure Agent replaces all data in the file.

You can use parameters defined in a parameter file in the target name for a Mapping Configuration task.

For a mapping, use input and output parameters to parameterize the target file name. Specifying the folder path in create target is applicable only to a mapping.

The following table describes the advanced target properties:

Property	Description
Encryption Type	Method you want to use to encrypt data. Select one of the following values: - None. The data is not encrypted. - Client Side Encryption. - The Secure Agent encrypts data while uploading the delimited files to Amazon buckets. - You must select client-side encryption in the advanced properties if you specify a master symmetric key or customer master key ID in the Amazon S3 connection properties. - Server Side Encryption. - You must select server-side encryption in the advanced properties if you specify a customer master key ID in the Amazon S3 connection properties. - If you select the server-side encryption in the advanced properties and do not specify the customer master key ID in the connection properties, Amazon S3-managed encryption keys are used to encrypt data.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, `<bucket name>/<my folder name>` The folder path specified at run time overrides the path specified while creating a connection.
Compression Type	Compress the data in GZIP format when you write the data to Amazon S3. The target file in Amazon S3 will have `.gz` extension. The Secure Agent compresses the data and then sends the data to Amazon S3 bucket. Default is None.
Part Size	Specifies the part size of an object. Default is 5 MB.
TransferManager Thread Pool Size	Specifies the number of the threads to write data in parallel. Amazon S3 Connector uses the AWS TransferManager API to upload a large object in multiple parts to Amazon S3. When the file size is more than 5 MB, you can configure multipart upload to upload object in multiple parts in parallel. If you set the value of the **TransferManager Thread Pool Size** to greater than 50, the value reverts to 50. Default is 10.
Merge Partition Files	Specifies whether the Secure Agent must merge all the partition files into a single file or maintain separate files based on the number of partitions specified to write data to the Amazon S3 targets. Default is not selected.
Distribution Column	Specify the name of the column that is used to create multiple target files during run time.

Property	Description
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Object Tags	You can add single or multiple tags to the objects stored on the Amazon S3 bucket. You can either enter the key value pairs or specify the file path that contains the key value pairs. For more information, see "Object Tag" on page 17.
Success File Directory	Not applicable.
Error File Directory	Not applicable.
Forward Rejected Rows	Determines whether the transformation passes rejected rows to the next transformation or drops rejected rows. By default, the Mapping Configuration application forwards rejected rows to the next transformation.

Amazon S3 Objects in Mapping Configuration Tasks

When you configure a Mapping Configuration task, you can configure advanced properties for Amazon S3 sources and targets.

Amazon S3 Sources in Mapping Configuration Tasks

For Amazon S3 source connections used in Mapping Configuration tasks, you can configure advanced properties in the **Sources** page of the Mapping Configuration Task wizard.

You can configure the following advanced properties:

Property	Description
Enable Downloading S3 File in Multiple Parts	Downloads large Amazon S3 objects in multiple parts. The Secure Agent downloads the object in multiple parts from Amazon S3. When the file size of an Amazon S3 object is greater than 5 MB, you can choose to download the object in multiple parts in parallel.
Header Line Number	Specify the line number that you want to use as the header when you read data from Amazon S3. Default is 0.
Read Data From Line	Specify the line number from where you want the Secure Agent to read data. Default is 1. **Note:** To read data from the header, the value of the **Header Line Number** and the **Read Data From Line** fields should be the same.
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Part Size	Specifies the part size of an object. Default is 5 MB.
Tracing Level	Sets the amount of detail that appears in the log file. You can choose terse, normal, verbose initialization or verbose data. Default is normal.

Amazon S3 Targets in Mapping Configuration Tasks

For Amazon S3 target connections used in Mapping Configuration tasks, you can configure advanced properties in the **Targets** page of the Mapping Configuration Task wizard.

You can configure the following advanced properties:

Property	Description
Encryption Type	Method you want to use to encrypt data. Select one of the following values: - None. The data is not encrypted. - Client Side Encryption. - The Secure Agent encrypts data while uploading the delimited files to Amazon buckets. - You must select client-side encryption in the advanced properties if you specify a master symmetric key or customer master key ID in the Amazon S3 connection properties. - Server Side Encryption. - You must select server-side encryption in the advanced properties if you specify a customer master key ID in the Amazon S3 connection properties. - If you select the server-side encryption in the advanced properties and do not specify the customer master key ID in the connection properties, Amazon S3-managed encryption keys are used to encrypt data.
Folder Path	The complete path to the Amazon S3 objects and must include the bucket name and any folder name. Ensure that you do not use a forward slash at the end of the folder path. For example, `<bucket name>/<my folder name>` The folder path specified at run time overrides the path specified while creating a connection.
Compression Type	Compress the data in GZIP format when you write the data to Amazon S3. The target file in Amazon S3 will have `.gz` extension. The Secure Agent compresses the data and then sends the data to Amazon S3 bucket. Default is None.
Part Size	Specifies the part size of an object. Default is 5 MB.
TransferManager Thread Pool Size	Specifies the number of the threads to write data in parallel. Amazon S3 Connector uses the AWS TransferManager API to upload a large object in multiple parts to Amazon S3. When the file size is more than 5 MB, you can configure multipart upload to upload object in multiple parts in parallel. If you set the value of the **TransferManager Thread Pool Size** to greater than 50, the value reverts to 50. Default is 10.
Merge Partition Files	Not applicable.
Distribution Column	Specify the name of the column to create multiple target files during run time.

Property	Description
Staging File Location	Amazon S3 staging directory. When you run a task in Secure Agent runtime environment, specify a directory path that is available on the corresponding Secure Agent machine in the runtime environment. When you specify the directory path, the Secure Agent create folders depending on the number of partitions that you specify in the following format: `InfaS3Staging<00/11><timestamp>_<partition number>` where, 00 represents read operation and 11 represents write operation. For example, `InfaS3Staging000703115851268912800_0` **Note:** The temporary files are created within the new directory. When you specify a directory name, if a folder with same name already exists, the Secure Agent deletes the contents of the folder. You must have the write permission for the specified location. If you do not specify a directory path, the Secure Agent uses a temporary directory as the staging file location. When you run a task in Hosted Agent runtime environment, leave the staging directory location blank. The Hosted Agent creates a directory at a temporary location.
Object Tags	You can add single or multiple tags to the objects stored on the Amazon S3 bucket. You can either enter the key value pairs or specify the file path that contains the key value pairs. For more information, see "Object Tag" on page 17.
Success File Directory	Not applicable.
Error File Directory	Not applicable.

Specifying a Target

You can use an existing target or create a target to hold the results of a mapping. If you choose to create the target, the agent creates the target when you run the task.

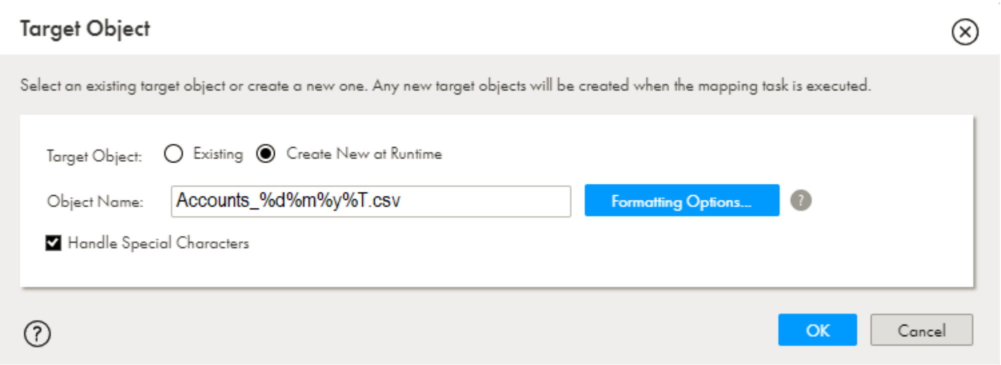
To specify the target properties, follow these steps:

1. Select the Target transformation in the mapping.
2. On the **Incoming Fields** tab, configure field rules to specify the fields to include in the target.
3. To specify the target, click the **Target** tab.
4. Select the target connection.
5. For the target type, choose **Single Object** or **Parameter**.
6. Specify the target object or parameter. You must specify a .csv target file name.
    - To create a target file at run time, enter the name for the target file including the extension, for example, `Accounts.csv`.
    - If you want the file name to include a time stamp, click **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`.

      Note: If you enable **Handle Special Characters**, the input and output parameters in Create Target are ignored.
7. Click **Formatting Options** if you want to configure the formatting options for the file, and click **OK**.

8. Click **Select** and choose a target object. You can select an existing target object or create a new target object at run time and specify the object name.

   The following image shows the Target Object box:



Target Object

Select an existing target object or create a new one. Any new target objects will be created when the mapping task is executed.

Target Object: ○ Existing ● Create New at Runtime

Object Name: Accounts_%d%m%y%T.csv

☑ Handle Special Characters

9. Specify Advanced properties for the target, if needed.

Amazon S3 Target File Parameterization

When you parameterize the file name and target folder location for Amazon S3 target objects, you can pass the file name and folder location at run time. If the folder does not exist, the agent creates the folder structure dynamically. You can also append time stamp information to the file name to show when the file is created.

When you specify the file name for the target file, include special characters based on Apache STRFTIME function formats that the Mapping Configuration task uses to include time stamp information in the file name. You can use the STRFTIME function formats in a mapping.

The following table describes some common STRFTIME function formats that you might use in a mapping or Mapping Configuration task:

Special Character	Description
%d	Day as a two-decimal number, with a range of 01-31.
%m	Month as a two-decimal number, with a range of 01-12.
%y	Year as a two-decimal number without the century, with range of 00-99.
%Y	Year including the century, for example 2015.
%T	Time in 24-hour notation, equivalent to %H:%:M:%S.
%H	Hour in 24-hour clock notation, with a range of 00-24.
%I	Hour in 12-hour clock notation, with a range of 01-12.
%M	Minute as a decimal, with a range of 00-59.

Special Character	Description
%S	Second as a decimal, with a range of 00-60.
%p	Either AM or PM.

APPENDIX A

Data Type Reference

This appendix includes the following topic:

- Data Type Reference Overview, 35

Data Type Reference Overview

Informatica Cloud uses only delimited files in Data Synchronization tasks and Mapping Configuration tasks with Amazon S3.

Informatica Cloud uses the following data types in Data Synchronization tasks, mappings, and Mapping Configuration tasks with Amazon S3:

Amazon S3 native data types

Amazon S3 data types appear in the Fields tab for Source and Target transformations when you choose to edit metadata for the fields.

Transformation data types

Set of data types that appear in the remaining transformations. They are internal data types based on ANSI SQL-92 generic data types, which Informatica Cloud uses to move data across platforms. Transformation data types appear in all remaining transformations in a Data Synchronization task, mapping, or Mapping Configuration task.

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

The following table lists the Amazon S3 data types that Informatica Cloud supports and the corresponding transformation data types:

Amazon S3 Native Data Type	Transformation Data Type	Description
String	String	1 to 104,857,600 characters

APPENDIX B

Troubleshooting

This appendix includes the following topics:

- Troubleshooting Overview, 36
- Troubleshooting for Amazon S3 Connector, 36

Troubleshooting Overview

Use the following sections to troubleshoot errors in Amazon S3 Connector.

Troubleshooting for Amazon S3 Connector

How to enable proxy and non-proxy server settings in the Secure Agent machine to read data from or write data to Amazon S3?

For information about enabling proxy and non-proxy server settings in the Secure Agent machine, see https://kb.informatica.com/howto/6/Pages/20/519423.aspx?myk=519423

How to configure AWS KMS customer master key to encrypt files in Amazon S3?

For information about configuring AWS KMS customer master key, see https://kb.informatica.com/h2l/HowTo%20Library/1/0973-ConfiguringAWSKMSCustomerMasterKeytoEncryptFilestoAmazonS3-H2L.pdf

How to create timestamp parameterized target files using Amazon S3 Connector?

For information about creating timestamp parameterized target files, see https://kb.informatica.com/h2l/HowTo%20Library/1/0983_CreatingTimeStampParameterizedTargetFilesUsingAmazonS3Connector-H2L.pdf

How to configure AWS IAM authentication for Amazon S3 Connector?

For information about configuring AWS IAM authentication, see https://kb.informatica.com/h2l/HowTo%20Library/1/1199-ConfiguringAWSIAMforAmazonS3andAmazonS3V2Connectors-H2L.pdf

How to solve the connection failure issue when you import the Amazon S3 metadata or test an Amazon S3 connection?

For more information about the issue, see https://kb.informatica.com/solution/23/Pages/67/544613.aspx?myk=544613

INDEX

A

administration
  IAM authentication 9
  minimal Amazon S3 bucket policy 10
Amazon S3
  handling multiple files 14
  connection properties 12
  object format 8
  objects 8
  sources 14
  specifying targets 32
  targets 16
Amazon S3 Connector
  administration 9
  overview 7
  troubleshooting 36
Amazon S3 source
  client-side encryption 14
Amazon S3 target
  client-side encryption 16

C

Cloud Application Integration community
  URL 5
Cloud Developer community
  URL 5
connection properties
  Amazon S3 12
  overview 11
create target
  adding time stamps 33
  target file parameterization 33

D

data encryption
  client-side 8
  server-side 8
Data Synchronization
  example 24
Data Synchronization task
  source properties 20
  sources 20
  target 21
  target properties 21
data type reference
  overview 35
distribution column 17

I

Informatica Cloud Community
  URL 5
Informatica Cloud web site
  URL 5
Informatica Global Customer Support
  contact information 6

M

maintenance outages 6
Mapping Configuration task
  source properties 30
  sources 30
  target properties 31
  targets 31
mappings
  Amazon S3 targets 27

O

object tag
  rules and guidelines 18
object tags 17, 18

P

partitioning
  Amazon S3 sources 16
Partitioning
  Amazon S3 targets 18

S

status
  Informatica cloud services 6
system status 6

T

trust site
  description 6

U

upgrades 6