



Informatica® Data Integration - Free & PayGo

Microsoft Azure Blob Storage V3 Connector

© Copyright Informatica LLC 2019, 2023

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: 2023-04-04

Table of Contents

Preface	4
Informatica Resources.	4
Informatica Documentation.	4
Informatica Intelligent Cloud Services web site.	4
Informatica Intelligent Cloud Services Communities.	4
Informatica Intelligent Cloud Services Marketplace.	4
Simple Data Integration connector documentation.	5
Informatica Knowledge Base.	5
Informatica Intelligent Cloud Services Trust Center.	5
Informatica Global Customer Support.	5
 Chapter 1: Introduction to Microsoft Azure Blob Storage V3 Connector.....	6
Microsoft Azure Blob Storage V3 Connector assets.	6
Administration of Microsoft Azure Blob Storage V3 Connector.	6
 Chapter 2: Connections for Microsoft Azure Blob Storage V3.....	8
Microsoft Azure Blob Storage V3 connection properties.	8
Configuring the proxy server.	9
Configuring proxy server settings on Windows.	9
Configuring proxy server settings on Linux.	10
 Chapter 3: Mappings for Microsoft Azure Blob Storage V3.....	11
Data compression in Microsoft Azure Blob Storage V3 sources	11
Directory source in Microsoft Azure Blob Storage sources.	12
Microsoft Azure Blob Storage V3 sources in mappings.	13
File formatting options.	14
Rules and guidelines for mappings and mapping tasks.	16
 Chapter 4: Data type reference.....	17
Microsoft Azure Blob Storage V3 and transformation data types.	17
Avro data types and transformation data types.	18
JSON data types and transformation data types.	18
Parquet data types and transformation data types.	19
 Chapter 5: Troubleshooting.....	20
Troubleshooting a connection.	20
Troubleshooting a mapping or mapping task.	20
 Index.....	22

Preface

Use *Microsoft Azure Blob Storage V3 Connector* to learn how to read from Microsoft Azure Blob Storage. Learn to create a connection, develop and run mappings, mapping tasks, and data transfer tasks in 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 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 Intelligent Cloud Services web site

You can access the Informatica Intelligent Cloud Services web site at <http://www.informatica.com/cloud>. This site contains information about Informatica Cloud integration services.

Informatica Intelligent Cloud Services Communities

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

Access the Informatica Intelligent Cloud Services Community at:

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

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 Intelligent Cloud Services Marketplace

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

<https://marketplace.informatica.com/>

Simple Data Integration connector documentation

You can access documentation for Simple Data Integration Connectors at the Documentation Portal. To explore the Documentation Portal, visit <https://docs.informatica.com>.

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 Intelligent Cloud Services Trust Center

The Informatica Intelligent Cloud Services Trust Center provides information about Informatica security policies and real-time system availability.

You can access the trust center at <https://www.informatica.com/trust-center.html>.

Subscribe to the Informatica Intelligent Cloud Services Trust Center to receive upgrade, maintenance, and incident notifications. The [Informatica Intelligent Cloud Services Status](#) page displays the production status of all the Informatica cloud products. All maintenance updates are posted to this 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 receive updates for a single component or all Informatica Intelligent Cloud Services components. Subscribing to all components is the best way to be certain you never miss an update.

To subscribe, go to <https://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 Intelligent Cloud Services. 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 Microsoft Azure Blob Storage V3 Connector

You can use Microsoft Azure Blob Storage V3 Connector to securely read from Microsoft Azure Blob Storage.

Use Microsoft Azure Blob Storage V3 Connector to read delimited files and complex files such as Avro, JSON, and Parquet.

Blobs are files of any type and size, and are organized into containers in Microsoft Azure Storage. You can use a Microsoft Azure Blob Storage V3 connection to access delimited, Avro, and Parquet files that are block blobs or append blobs.

You cannot read nested and multi-line indented JSON files.

You can use Microsoft Azure Blob Storage V3 objects as sources in mappings and mapping tasks.

Microsoft Azure Blob Storage V3 Connector assets

Create assets in Data Integration to integrate data using Microsoft Azure Blob Storage V3 Connector.

When you use Microsoft Azure Blob Storage V3 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.

Administration of Microsoft Azure Blob Storage V3 Connector

Before you use Microsoft Azure Blob Storage V3 objects in tasks, an administrator must perform the following tasks:

- To use shared key authentication, get the storage account name and account key.

- Ensure that you have a container in Microsoft Azure Blob Storage.
- Configure the minimum permissions for shared access signature authentication and generate the SAS token in the Azure portal.

You can generate the SAS token for the storage account or for the container.

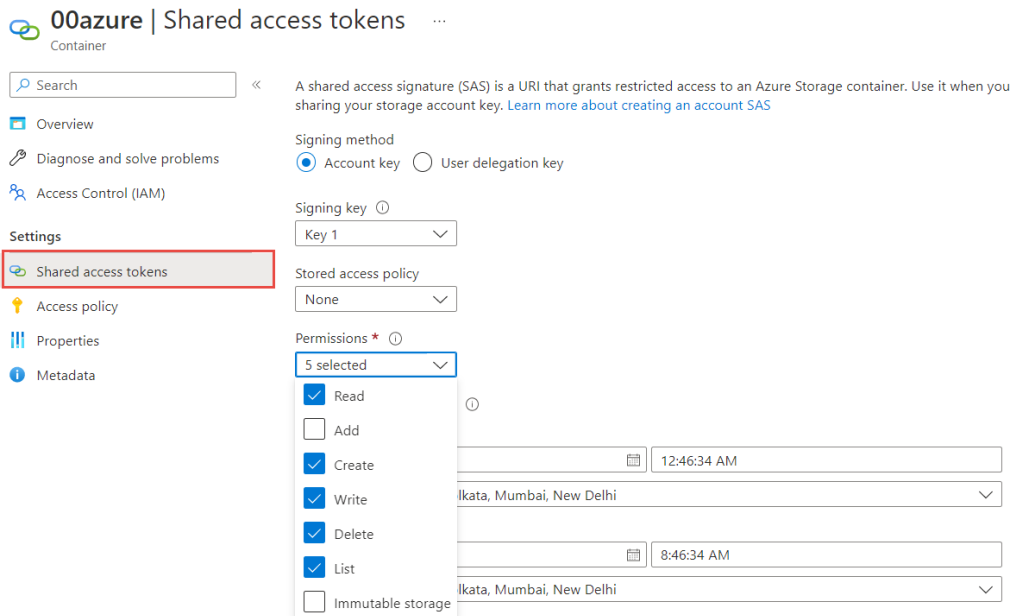
- To generate the SAS token for the storage account, go to **Security + Networking**, and click **Shared access signature**.

The following image shows the minimum permissions required for shared access signature authentication:



- To generate the SAS token for the Blob container, go to **Settings** of the container, and click **Shared access tokens**.

The following image shows the minimum permissions required for shared access signature authentication:



Note: If you use the User delegation key signing method, ensure that you have the **Storage Blob Data Owner** role for the container or the storage account.

- Get the license for the SDKPatch package for your Data Integration organization.

For more information about configuring a Microsoft Azure Blob Storage V3 connection, see the Informatica How-To Library article, [Prerequisites to create a Microsoft Azure Blob Storage V3 connection](#).

CHAPTER 2

Connections for Microsoft Azure Blob Storage V3

Create a Microsoft Azure Blob Storage V3 connection to securely read data from Microsoft Azure Blob Storage. You can use a Microsoft Azure Blob Storage V3 connection to specify sources in mappings and mapping tasks.

Microsoft Azure Blob Storage V3 connection properties

When you set up a Microsoft Azure Blob Storage V3 connection, configure the connection properties.

The following table describes the Microsoft Azure Blob Storage V3 connection properties:

Property	Description
Connection Name	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	Description of the connection. Maximum length is 4000 characters.
Type	The Microsoft Azure Blob Storage V3 connection type.
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent or a Hosted Agent.
Account Name	Microsoft Azure Blob Storage account name.
Authentication Type	Authentication type to access the Microsoft Azure Blob Storage account. Select one of the following options: <ul style="list-style-type: none">- Shared Key Authentication. Uses the account key to connect to Microsoft Azure Blob Storage.- Shared Access Signature. Uses the SAS token to connect to Microsoft Azure Blob Storage. Use the SAS token to grant access to the resources in the storage account or container for a specific time range without sharing the account key.

Property	Description
Account Key	Applies to shared key authentication. The account key for the Microsoft Azure Blob Storage account.
SAS Token	Applies to shared access signature. The shared access signature token generated in the Azure portal.
Container Name	Microsoft Azure Blob Storage container name.
Endpoint Suffix	Type of Microsoft Azure endpoints. Select one of the following options: <ul style="list-style-type: none"> - core.windows.net. Connects to Azure endpoints. - core.usgovcloudapi.net. Connects to Azure Government endpoints. - core.chinacloudapi.cn. Not applicable. Default is core.windows.net.

Configuring the proxy server

If your organization uses an outgoing proxy server to connect to the internet, the 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.

Contact your network administrator for the correct proxy settings.

Configuring proxy server settings on Windows

To configure the proxy server settings for the Secure Agent on a Windows machine, you can configure the proxy server settings through the Secure Agent or the JVM options of the Secure Agent.

Configuring proxy server settings through the Secure Agent Manager

To configure the proxy server settings through the Secure Agent Manager, perform the following steps:

1. In the Secure Agent Manager, click **Proxy**.
2. To enter proxy server settings, click **Use a proxy server**.
3. Configure the following fields:

Field	Description
Proxy Host	Required. Host name of the outgoing proxy server that the Secure Agent uses.
Proxy Port	Required. Port number of the outgoing proxy server.

4. Click **OK**.
The Secure Agent Manager restarts the Secure Agent to apply the settings.

Configuring proxy server settings through the JVMOptions

1. Log in to Informatica Intelligent Cloud Services.
2. Open Administrator and select **Runtime Environments**.
3. Select the Secure Agent for which you want to configure the proxy server.
4. On the upper-right corner of the page, click **Edit**.
5. In the **System Configuration Details** section, select the **Type** as **DTM** for the Data Integration Service.
6. Add the following parameters in any **JVMOption** field and specify appropriate values for each parameter:

Parameter	Description
-DproxyEnabled=	Required. Set the value to true to enable proxy server.
-Dhttp.proxyHost=	Required. Host name of the outgoing HTTP proxy server.
-Dhttp.proxyPort=	Required. Port number of the outgoing HTTP proxy server.

Example for HTTP:

```
JVMOption1=-DproxyEnabled=true
```

```
JVMOption2=-Dhttp.proxyHost=<proxy_server_hostname>
```

```
JVMOption3=-Dhttp.proxyPort=8081
```

7. Click **Save**.

The Secure Agent restarts to apply the settings.

Configuring proxy server settings on Linux

The Secure Agent installer configures the proxy server settings for the Secure Agent based on settings configured in the browser. You can update the proxy server settings defined for the Secure Agent from the command line.

To configure the proxy server settings for the Secure Agent on a Linux machine, use a shell command that updates the `proxy.ini` file. Contact the network administrator to determine the proxy settings.

1. Navigate to the following directory:

```
<Secure Agent installation directory>/apps/agentcore
```
2. Update the unauthenticated proxy details directly in the `proxy.ini` file, or run the following command to update the proxy details in the `proxy.ini` file:

```
consoleAgentManager.sh configureProxy <proxy host> <proxy port>
```
3. Restart the Secure Agent.

CHAPTER 3

Mappings for Microsoft Azure Blob Storage V3

When you configure a mapping, you describe the flow of data from the source to the target.

When you create a mapping, you define the Source transformation to represent a Microsoft Azure Blob Storage V3 object. Use the Mapping Designer in Data Integration to add the Source or Target transformations in the mapping canvas and configure the Microsoft Azure Blob Storage V3 source properties.

You can use Monitor to monitor the jobs.

Data compression in Microsoft Azure Blob Storage V3 sources

You can decompress data when you read data from Microsoft Azure Blob Storage.

Configure the compression format in the **Compression Format** option under the advanced source properties.

For the Flat resource type, select only the Gzip compression format. The following table lists the compression formats for Avro and Parquet resource types:

Compression format	Avro File	Flat File	JSON File	Parquet File
None	Yes	Yes	Yes	Yes
Deflate*	Yes	N/A	No	No
Gzip	No	Yes	No	Yes
Bzip2	N/A	N/A	No	N/A
Lzo	N/A	N/A	No	N/A
Snappy*	Yes	N/A	No	Yes
*Select None to decompress the Deflate and Snappy file formats.				

To read a compressed file from Microsoft Azure Blob Storage, the compressed file must have specific extensions. If the extensions used to read the compressed file are not valid, the Secure Agent does not

process the file. The following table describes the extensions that are appended based on the compression format that you use:

Compression format	File Name Extension
Deflate	.deflate
Gzip	.GZ
Bzip2	.BZ2
Lzo	.LZO
Snappy	.snappy

Directory source in Microsoft Azure Blob Storage sources

You can select the type of source from which you want to read data.

You can select the following type of sources from the **Source Type** option under the advanced source properties:

- File
- Directory

Use the following rules and guidelines to select **Directory** as the source type:

- All the source files in the directory must contain the same metadata.
- All the files must have data in the same format. For example, delimiters, header fields, and escape characters must be same.
- All the files under a specified directory are parsed. The files under subdirectories are not parsed.
- The connector does not perform any validation if there are multiple blob formats in the directory you select and might result into errors.

Microsoft Azure Blob Storage V3 sources in mappings

In a mapping, you can configure a Source transformation to represent a Microsoft Azure Blob Storage V3 object.

The following table describes the Microsoft Azure Blob Storage V3 source properties that you can configure in a Source transformation:

Property	Description
Connection	Name of the source connection. Select a source connection or click New Parameter to define a new parameter for the source connection.
Source Type	Source type. Select one of the following types: <ul style="list-style-type: none">- Single Object- Parameter: Select Parameter to define the source type when you configure the mapping task.
Object	Name of the source object. You can drill-down and select an object from a sub-folder to fetch metadata from a particular object. When you run a task, the Secure Agent reads data from the container you specified either in connection properties or in the advance properties.
Parameter	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.
Format	Specifies the file format that the Microsoft Azure Blob Storage V3 Connector uses to read data from Microsoft Azure Blob Storage. You can select the following file format types: <ul style="list-style-type: none">- Flat- Avro- Parquet- JSON Default is None . You must select the Format Type as None to read binary files. For more information, see "File formatting options" on page 14 .

The following table describes the Microsoft Azure Blob Storage V3 advanced source properties that you can configure in a Source transformation:

Property	Description
Number of concurrent connections to Blob Store	The number of concurrent connections to Blob Store to upload files. Default is 4.
Source Type	Select the type of source from which you want to read data. You can select the following source types: <ul style="list-style-type: none">- File- Directory Default is File.

Property	Description
Blob Name Override	Overrides the default file name.
Blob Container Override	<p>Overrides the default container name.</p> <p>When you read data from a directory and override the Blob container, ensure that files in the Blob container that you override with are not empty.</p> <p>When you generate the SAS token at the container-level, the default container name and the container name that you specify for the container override must be the same.</p>
Compression Format	<p>Decompresses data when you read data from Microsoft Azure Blob Storage. You can decompress the data in the following formats:</p> <ul style="list-style-type: none"> - None. Select None to decompress deflate and snappy file formats. - Gzip - Bzip2 - Lzo <p>Default is None.</p>
Tracing Level	<p>Sets the amount of detail that appears in the log file.</p> <p>You can choose terse, normal, verbose initialization, or verbose data.</p> <p>Default is normal.</p>

File formatting options

When you select the format of a Microsoft Azure Blob Storage file, you can configure the formatting options.

The following table describes the formatting options for Avro, Parquet, JSON, and delimited flat files:

Property	Description
Schema Source	<p>The schema of the source file.</p> <p>Select one of the following options to specify a schema:</p> <ul style="list-style-type: none"> - Read from data file. Imports the schema from the file in Microsoft Azure Blob Storage. - Import from schema file. Imports schema from a schema definition file in your local machine.
Schema File	The schema definition file in the agent machine from where you want to upload the schema.

The following table describes the formatting options for flat files:

Property	Description
Flat File Type	The type of flat file. Select one of the following options: - Delimited. Reads a flat file that contains column delimiters. - Fixed Width. Not applicable.
Delimiter	Character used to separate columns of data. You can set values as comma, tab, colon, semicolon, or others. You can't set a tab as a delimiter directly in the Delimiter field. To set a tab as a delimiter, you must type the tab character in any text editor. Then, copy the character to the Delimiter field.
EscapeChar	Character immediately preceding a column delimiter character embedded in an unquoted string, or immediately preceding the quote character in a quoted string.
Qualifier	Quote character that defines the boundaries of text strings. You can configure parameters such as single quote or double quote. You can use the output text qualifier when a delimiter value is present in the data.
Qualifier Mode	Not applicable.
Code Page	Select the code page that the Secure Agent must use to read data from a delimited flat file. Select UTF-8 for mappings.
Header Line Number	Specify the line number that you want to use as the header when you read data from Microsoft Azure Blob Storage. You can also read a data from a file that does not have a header. To read data from a file with no header, specify the value of the Header Line Number field as 0.
First Data Row	Specify the line number from where you want to start reading the data. Enter a value greater than or equal to one. To read data from the header, the value of the Header Line Number and the First Data Row fields should be the same. Default is 1.
Target Header	Not applicable.
Distribution Column	Not applicable.
Is Escape Character Data Retained	Not applicable.
Max Rows To Preview	Not applicable.
Row Delimiter	Not applicable.

The following table describes the formatting options for JSON files:

Property	Description
Data elements to sample	Not applicable.
Memory available to process data	Not applicable.

Rules and guidelines for mappings and mapping tasks

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

- When you edit the metadata, all native data types change to Bigint and you cannot change the scale and precision of data types except for the string data type.
- The data preview and mapping fail if you read an Avro file that contains binary fields.
- Ensure that the field names in the source object do not contain special characters or unicode characters.
- You cannot preview data when you read a compressed file.
- You cannot select append blob as blob type when you read JSON file.

CHAPTER 4

Data type reference

Data Integration uses the following data types in Microsoft Azure Blob Storage V3 mappings and mapping tasks:

- Microsoft Azure Blob Storage V3 native data types appear in the source 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.

Microsoft Azure Blob Storage V3 and transformation data types

The following table lists the Microsoft Azure Blob Storage V3 data types that the Secure Agent supports and the corresponding transformation data types:

Microsoft Azure Blob Storage V3 Native Data Type	Transformation Data Type	Range and Description
String	String	1 to 104,857,600 characters

Avro data types and transformation data types

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

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

Avro Data Type	Transformation Data Type	Range and Description
Boolean	Integer	TRUE (1) or FALSE (0)
Bytes	Binary	Precision 4000
Double	Double	Precision 15
Float	Double	Precision 15
Int	Integer	-2,147,483,648 to 2,147,483,647 Precision 10, scale 0
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

JSON data types and transformation data types

JSON complex file data types map to transformation data types that the Secure Agent uses to move data across platforms.

The following table lists the JSON complex file data types that the Data Integration supports and the corresponding transformation data types:

JSON Data Type	Transformation Data Type	Range and Description
boolean	integer	The default transformation type for boolean is integer. You can specify string data type with values of True and False. True is equivalent to the integer 1 and False is equivalent to the integer 0.
Number (double)	double	-1.79769313486231570E+308 to +1.79769313486231570E+308. Precision 15.

JSON Data Type	Transformation Data Type	Range and Description
Number (float)	double	-1.79769313486231570E+308 to +1.79769313486231570E+308. Precision 15.
Number (int)	integer	-2,147,483,648 to 2,147,483,647 Precision 10, scale 0
Number (long)	bigint	-9,223,372,036,854,775,808 to 9,223,372,036,854,775,807 Precision 19, scale 0.
string	string	1 to 104,857,600 characters.

Parquet data types and transformation data types

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

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

Parquet Data Type	Transformation Data Type	Range and Description
Boolean	Integer	TRUE (1) or FALSE (0)
Byte_Array	Binary	Arbitrarily long byte array
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

The Parquet schema that you specify to read a Parquet file must be in smaller case. Parquet does not support case-sensitive schema.

CHAPTER 5

Troubleshooting

Use the following sections to troubleshoot errors in mappings.

Troubleshooting a connection

The session log does not log the proxy server details

When you configure a proxy server through the Informatica Cloud Secure Agent user interface, the session log does not log the proxy server details.

Configure the proxy server by setting the JVM Options for your Secure Agent in the Administrator service.

Troubleshooting a mapping or mapping task

[ERROR] Exception: java.io.IOException: Too many open files

When you run a mapping on a Linux machine to read a large file, the mapping might fail with the following error:

```
[ERROR] Exception: java.io.IOException: Too many open files
```

To resolve this issue, perform the following steps:

1. Increase the value of file-max that is the maximum File Descriptors enforced on a kernel level. To change the file descriptor setting, edit the kernel parameter file `/etc/sysctl.conf` and add `fs.file-max=[new value]` to it.

For example:

```
# vi /etc/sysctl.conf  
fs.file-max = 400000
```

2. Set the ulimit. The ulimit must be less than file-max.

To change the ulimit setting, edit the file `/etc/security/limits.conf` and set the hard and soft limits in it.

For example:

```
# vi /etc/security/limits.conf
* soft nfile 40000
* hard nfile 40000
```

The same error message is displayed for every failed mapping.

You can verify the error message in the session log.

INDEX

A

administration [6](#)

C

Cloud Application Integration community
URL [4](#)
Cloud Developer community
URL [4](#)
complex file format
JSON [18](#)
connections
Microsoft Azure Blob Storage V3 [8](#)

D

data compression
sources and targets [11](#)
Data Integration community
URL [4](#)
data type reference
overview [17](#)
data types
avro [18](#)
parquet [19](#)
directory source
Microsoft Azure Blob Storage sources [12](#)

I

Informatica Global Customer Support
contact information [5](#)
Informatica Intelligent Cloud Services
web site [4](#)

L

Linux
configuring proxy server settings [10](#)

M

maintenance outages [5](#)

mappings
source properties [13](#)
Microsoft Azure Blob Storage connection
overview [8](#)
Microsoft Azure Blob Storage V3
connection properties [8](#)
Microsoft Azure Blob Storage V3 Connector
overview [6](#)

P

proxy server settings
configuring on Linux [10](#)
proxy settings
configuring on Windows [9](#)
JVMOptions [10](#)

S

Source transformation
Microsoft Azure Blob Storage properties [13](#)
sources in mappings [13](#)
status
Informatica Intelligent Cloud Services [5](#)
system status [5](#)

T

tracing level [13](#)
trust site
description [5](#)

U

upgrade notifications [5](#)

W

web site [4](#)
Windows
configuring proxy settings [9](#)