



Prerequisites to create a Microsoft Azure Blob Storage V3 connection

[©] Copyright Informatica LLC 2022, 2024. Informatica, Informatica Cloud, and the Informatica logo 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.

Abstract

You can use Microsoft Azure Blob Storage V3 Connector to connect to Microsoft Azure Blob Storage from Cloud Data Integration. This article explains the prerequisite tasks that you must complete before you create a Microsoft Azure Blob Storage V3 connection.

Supported Versions

• Informatica Cloud[®] Data Integration Microsoft Azure Blob Storage V3 Connector

Table of Contents

| Overview | 2 |
|---|---|
| Create a storage account to use with Microsoft Azure Blob Storage | 2 |
| Create a blob container in the storage account | 5 |
| Get credentials for shared key authentication | 7 |
| Get credentials for shared access signature authentication | 7 |
| Get SAS token for the storage account | 8 |
| Get SAS token for the container | 8 |

Overview

You can use Microsoft Azure Blob Storage V3 Connector to connect to Microsoft Azure Blob Storage using shared key authentication or shared access signature authentication.

Before you create a Microsoft Azure Blob Storage V3 connection, complete the following prerequisite tasks:

- 1. Create a storage account to use with Microsoft Azure Blob Storage.
- 2. Create a blob container in the storage account.
- 3. Get credentials for shared key authentication.
- 4. Get credentials for shared access signature authentication.

For information about configuring a Microsoft Azure Blob Storage V3 connection, see the Informatica Cloud[®] Data Integration Microsoft Azure Blob Storage V3 Connector documentation.

Create a storage account to use with Microsoft Azure Blob Storage

An Azure storage account contains all of your Azure Storage data objects, including blobs, file shares, queues, tables, and disks. Create a storage account and enable access to the storage account using the shared key or shared access signature.

1. Log in to the following Azure portal: <u>https://portal.azure.com/</u>

2. Under Azure Services, click Storage accounts.

| Microsoft Azure | | ources, services | , and docs (G+/) | | | | | | ₽ Q @ | ? 🙂 |
|-----------------|-------------------|---------------------|---------------------------|---------------------------|---------------------|--------------|---------------|---------------------------------|--------------------|---------------|
| Az | zure services | | | | | | | | | |
| | Create a resource | Storage accounts | Azure Active Directory | Data Lake Storage Gen1 | Virtual machines | Rpp Services | SQL databases | Azure Database for PostgreSQ | Azure Cosmos DB | More services |
| Re | ecent resource | es | | | | | | | | |
| Nar | me | | | | Туре | | | | Last Viewed | |
| = | adlsgen2qa | | | | Storage | account | | | 4 days ago | |
| = | adapterqablob1 | | | | Storage | account | | | 3 months ago | |
| Na | avigate | | | | | | | | | |
| • | Subscriptions | | [9] F | lesource groups | | All resourc | es | <mark>≃lı</mark> Da | shboard | |

3. On the Storage accounts page, click Create to create a new storage account.

| Storage accounts 🖈 … Informatica (informatica.onmicrosoft.com) | | |
|---|------------------------------|---------------------------|
| + Create 🕲 Manage view \lor 🕐 Refresh \downarrow Export to CSV 😵 | Open query 🔗 Assign tags 👔 | Delete 🛛 🔗 Feedback |
| Filter for any field Subscription == all Resource group | == all X Location == all X | + _▼ Add filter |
| Showing 1 to 28 of 28 records. | | |
| □ Name ↑↓ | Туре ↑↓ | Kind ↑↓ |
| adapterdevblob | Storage account | StorageV2 |
| adaptergablob | Storage account | StorageV2 |
| adapterqablob1 | Storage account | StorageV2 |
| adapterqablobeastus2 | Storage account | StorageV2 |

4. On the **Basics** tab, enter the project and instance details.

| Creat | te a stor | age accou | nt … | | | |
|---|--|---|--|--|--|---|
| Basics | Advanced | Networking | Data protection | Encryption | Tags | Review + create |
| Azure Si redunda Tables. 1 storage | torage is a Micr ant. Azure Stora The cost of your accounts | osoft-managed ser ge includes Azure E · storage account d | vice providing cloud s Bobs (objects), Azure epends on the usage | storage that is hig Data Lake Storag and the options | ghly availa Je Gen2, A you choos | ble, secure, durable, scalable, and zure Files, Azure Queues, and Azure e below. Learn more about Azure |
| Project | details | | | | | |
| Select tł manage | he subscription 9 your storage a | in which to create t ccount together wi | he new storage accou th other resources. | unt. Choose a ne | w or existin | ng resource group to organize and |
| Subscrip | otion * | | Azure R&D CTG IN | ID_Connectivity | | \checkmark |
| | | | | | | |
| | Resource group | * | AzureRnD | | | \checkmark |
| Instanc | e details | | | | | |
| lf you n | eed to create a | legacy storage acco | ount type, please click | here. | | |
| Storage | account name | (i) * | blobdoc | | | |
| Region | i) * | | (US) East US | | | ~ |
| Revie | w + create | | < Previous | Next : Adva | anced > |] |

- a. In the **Subscription** field, select the subscription for which you want to create the storage account.
- b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.
- c. In the **Storage account name** field, enter a name for your storage account.

Note: The name must be unique across Azure, between 3 and 24 characters in length, and can include only numbers and lowercase letters.

d. In the **Region** field, select a location for your storage account, or use the default location.

- Create a storage account Basics Advanced Networking Data protection Encryption Tags Review + create () Certain options have been disabled by default due to the combination of storage account performance, redundancy, and region. Security Configure security settings that impact your storage account. \square Require secure transfer for REST API operations (i) Enable blob public access (i) \checkmark Enable storage account key access (i) \checkmark Default to Azure Active Directory \square authorization in the Azure portal ① Version 1.2 \sim Minimum TLS version 🛈 Data Lake Storage Gen2 The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). Learn more Review + create < Previous Next : Networking >
- 5. On the **Advanced** tab, configure the security settings.

- a. Disable the Require secure transfer for REST API operations option.
- b. Select Enable blob public access to allow anonymous access to blobs within the storage account.
- c. Select **Enable storage account key access** to allow access to storage account using the shared key or shared access signature.
- 6. Click Review + Create > Create.

Create a blob container in the storage account

After you create the storage account, create a blob container and a virtual directory within the blob container.

1. Open the storage account that you created.

2. Click Storage browsers > Blob containers.

| Blobdoc Storag | ge b | rowser (preview) | \$? ··· | |
|-----------------------------|------|-------------------|---------|---|
| Search (Ctrl+/) | « | ilobdoc | < | + Add container 👎 Upload 🖒 Refresh 🔟 Delete 🔒 Change access level |
| Overview | | 🔺 Favorites | | Blob containers |
| Activity log | | 🍄 Recently viewed | | Search containers by prefix |
| 🗳 Tags | | ✓ | | Showing all 1 itams |
| Diagnose and solve problems | | 🔳 \$logs | | Name |
| Access Control (IAM) | | View all | | |
| 💕 Data migration | | 🛋 File shares | | Slogs |
| 🗲 Events | | 0 Queues | | |
| 🚞 Storage browser (preview) | | I Tables | | |

- 3. Click Add container.
- 4. Enter a name for the new container.

| New container | \times |
|-------------------------------|----------|
| | |
| Name * | |
| blobcontainer | ~ |
| Public access level (i) | |
| Private (no anonymous access) | \sim |
| ✓ Advanced | |
| Create Discard | |

- 5. Click Create.
- 6. Click the container that you created.
- 7. Click Add Directory to create a new directory within the container.

| 🔤 blobdoc < | + Add Directory 🔨 Upload 🔒 Change access level 🖒 Refresh |
|---------------------|---|
| 📫 Favorites | Blob containers > blobcontainer |
| > 🔅 Recently viewed | Authentication method: Access key (Switch to Azure AD User Account) |
| ✓ ■ Blob containers | √ Add filter |
| 🗖 \$logs | ✓ Search blobs by prefix (case-sensitive) |
| blobcontainer | Showing all 0 items |
| View all | Name |
| 🛋 File shares | No items found |
| 🔟 Queues | NO REINS FOUND |
| 🎫 Tables | |

8. Enter a name for the directory.

| Add virtual directory |
|---|
| This will create a virtual directory. A virtual directory does not actually exist in Azure until you paste or upload blobs into it. |
| Name |
| directory01 |
| Ok Cancel |

9. Click Ok.

Get credentials for shared key authentication

You can use the shared key authentication to connect to Microsoft Azure Blob Storage using the account name and account key. Obtain the account name and account key.

- 1. Open the storage account.
- 2. Under Security + Networking, click Access keys.
- 3. Click Show keys.

| + blobdoc Access ke | ys … |
|--------------------------|--|
| | Show keys Set rotation reminder Refresh |
| Security + networking | Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure |
| Retworking | Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other. |
| Azure CDN | Remember to update the keys with any Azure resources and apps that use this storage account. Learn more 🗗 |
| 📍 Access keys | Storage account name |
| Shared access signature | blobdoc 🗅 |
| Encryption | kev1 |
| Security | Last rotated: 4/19/2022 (0 days ago) |
| Data management | 🗘 Rotate key |
| Geo-replication | Key |
| 💎 Data protection | |
| 🤣 Object replication | Connection string |
| Blob inventory | ····· |
| 📼 Static website | Key2 |
| Lifecycle management | C) Rotate key |
| 🙆 Azure search | Key |
| Settings | |
| Configuration | Connection string |
| 5 Data Lake Gen2 upgrade | ····· |

4. Make a note of the storage account name and account key. You can use key1 or key2.

Get credentials for shared access signature authentication

The shared access signature authentication uses the SAS token to connect to Microsoft Azure Blob Storage.

Get 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.

Get SAS token for the storage account

You can get the SAS taken for the storage account from the Azure portal.

- 1. Navigate to the storage account.
- 2. Under Security + Networking, click Shared access signature.

| blobdoc Shared ad Storage account | ccess signature | × |
|---|---|------------|
| Search (Ctrl+/) « | | |
| Security + networking | Allowed services ① | |
| 2 Networking | Blob File Queue Table | |
| Azure CDN | Allowed resource types ① | |
| 📍 Access keys | Service 🗹 Container 🧹 Object | |
| Shared access signature | Allowed permissions () | |
| Encryption | Read Vite Vite Vite Vist Add Viceate Update Process Immutable stora | ge |
| Security | Blob versioning permissions | |
| Data management | Enables deletion of versions | |
| Geo-replication | Allowed blob index permissions ① | |
| 💎 Data protection | Nead/Write Hiter | |
| Object replication | Start and expiry date/time ① | |
| Blob inventory | Start 04/19/2022 | 6:12:58 PM |
| Static website | End U4/20/2022 | 2:12:58 AM |
| Lifecycle management | (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi | × |
| 📣 Azure search | Allowed IP addresses ① | |
| Setting | For example, 166.1.5.65 or 168.1.5.65-168.1.5.70 | |
| Casformation | Allowed protocols () | |
| Conliguration | | |
| Data cake deliz upgrade | Preferred routing tier | |
| Resource sharing (CORS) | Some routing options are disabled because the endpoints are not published | |
| Advisor recommendations | | |
| Endpoints | signing key O | |
| 🗄 Locks | | |
| Monitoring | Generate SAS and connection string | |

- 3. In the Allowed services field, select Blob.
- 4. In the Allowed resource types field, select Container and Object.
- 5. In the Allowed permissions field, select Read, Write, Delete, List, and Create.
- 6. Set the start and expiry date during which the SAS token is valid.
- 7. In the **Allowed IP addresses** field, specify a public IP address or a range of public IP addresses. **Note:** When you read Avro or Parquet files, do not specify the IP address.
- 8. In the **Preferred routing tier** field, select **Basic**.
- 9. Select the Signing key.
- 10. Click Generate SAS and connection string and make a note of the SAS token.

Get SAS token for the container

You can get the SAS token for the container from the Azure Portal or Microsoft Azure Storage Explorer.

Get SAS token from the Azure Portal

Perform the following steps to get the SAS token for the container from the Azure portal:

- 1. Navigate to the blob container.
- 2. Under Settings, click Shared access tokens.

| O0azure Shared acc Container | ess tokens | \times |
|---|--|----------|
| Search «Overview | A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage container. Use it when you want to grant access to storage account resources for a specific time range without sharing your storage account key. Learn more about creating an account SAS | |
| Diagnose and solve problems Access Control (IAM) | Signing method • Account key User delegation key | |
| Settings Shared access tokens | Signing key ① Key 1 | |
| Access policy Properties | Stored access policy None V | |
| Metadata | Permissions * ① Read V | |
| | Start and expiry date/time ① Start | _ |
| | 11/15/2022 |] |
| | (UC+US:SU) Chennal, kolkata, Mumbal, New Deini V | J |
| | 11/15/2022 🗐 5:38:33 PM |] |
| | (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi 🗸 🗸 |] |
| | Allowed IP addresses ① for example, 168.1.5.65 or 168.1.5.65-168.1 | |
| | Allowed protocols ① HTTPS only HTTPS and HTTP | |
| | Generate SAS token and URL | |

3. In the Signing method field, select Account key or User delegation key.

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.

- 4. If you select the Account key signing method, select the Signing key.
- 5. In the **Permissions** field, select **Read**, **Write**, **Delete**, **List**, and **Create**.
- 6. Set the start and expiry date during which the SAS token is valid.
- In the Allowed IP addresses field, specify a public IP address or a range of public IP addresses.
 Note: When you read Avro or Parquet files, do not specify the IP address.
- 8. Click Generate SAS token and URL and make a note of the SAS token.

Get SAS token from Microsoft Azure Storage Explorer

Perform the following steps to get the SAS token for the container from Microsoft Azure Storage Explorer:

- 1. Log in to your Microsoft Azure Storage Explorer account.
- 2. On the Explorer, right-click on the container name and select **Get Shared Access Signature**. The Shared Access Signature window appears.

| Access policy: | none | ~ | |
|--|------------------|---|--|
| Start time: | 31-10-2022 18:32 | | |
| Expiry time: | 01-11-2022 18:32 | | |
| Time zone: Local UTC Permissions: | | | |
| Read Add Create Write Delete | | | |
| | | | |

- 3. In the Access policy field, select**none**.
- 4. Set the start and expiry date during which the SAS token is valid.
- 5. Select the time zone.
- 6. In the Permissions field, select Read, Create, Write, Delete, and List.
- 7. Select the Signing key.
- 8. Click **Create** to generate the SAS token and make a note of the SAS token.

Author

Adrija Pandya

Acknowledgements

The author would like to acknowledge K.R. Kiran for his technical assistance with this article.