How-To Library

Informatica

Prerequisites to create a Microsoft Azure Blob Storage V3 connection

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

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.

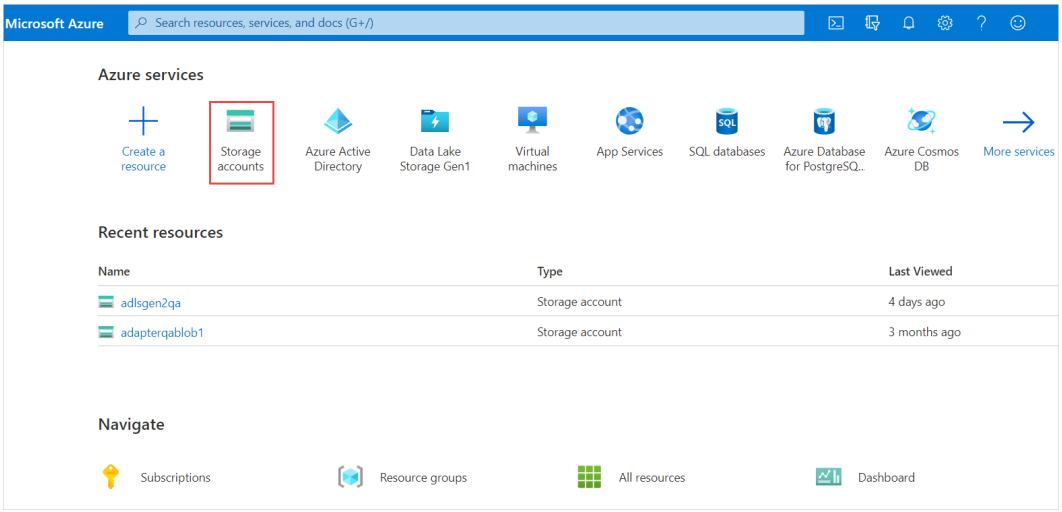
For information about configuring a Microsoft Azure Blob Storage V3 connection, see the Informatica Cloud® Data Integration Microsoft Azure Blob Storage V3 Connector documentation.

Create a storage account to use with Microsoft Azure Blob Storage

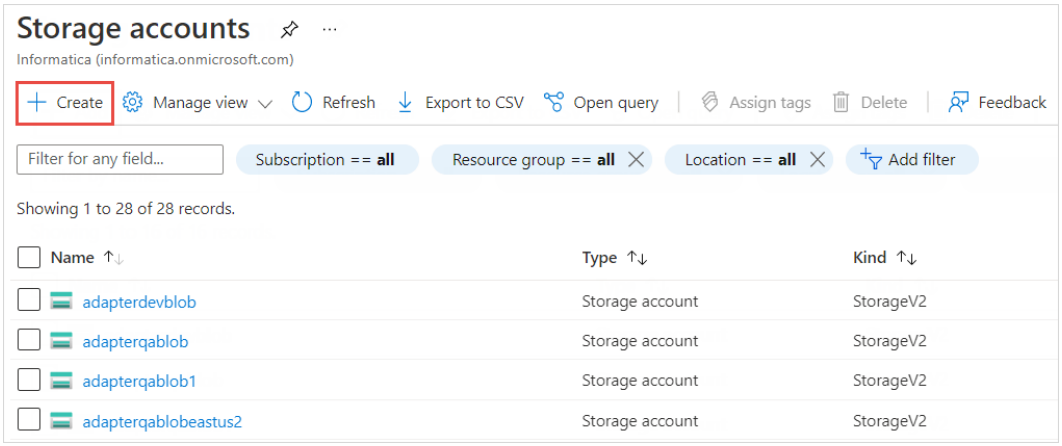
An Azure storage account contains all of your Azure Storage data objects, including blobs, file shares, queues, tables, and disks. Create a storage account and enable access to the storage account using the shared key or shared access signature.

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

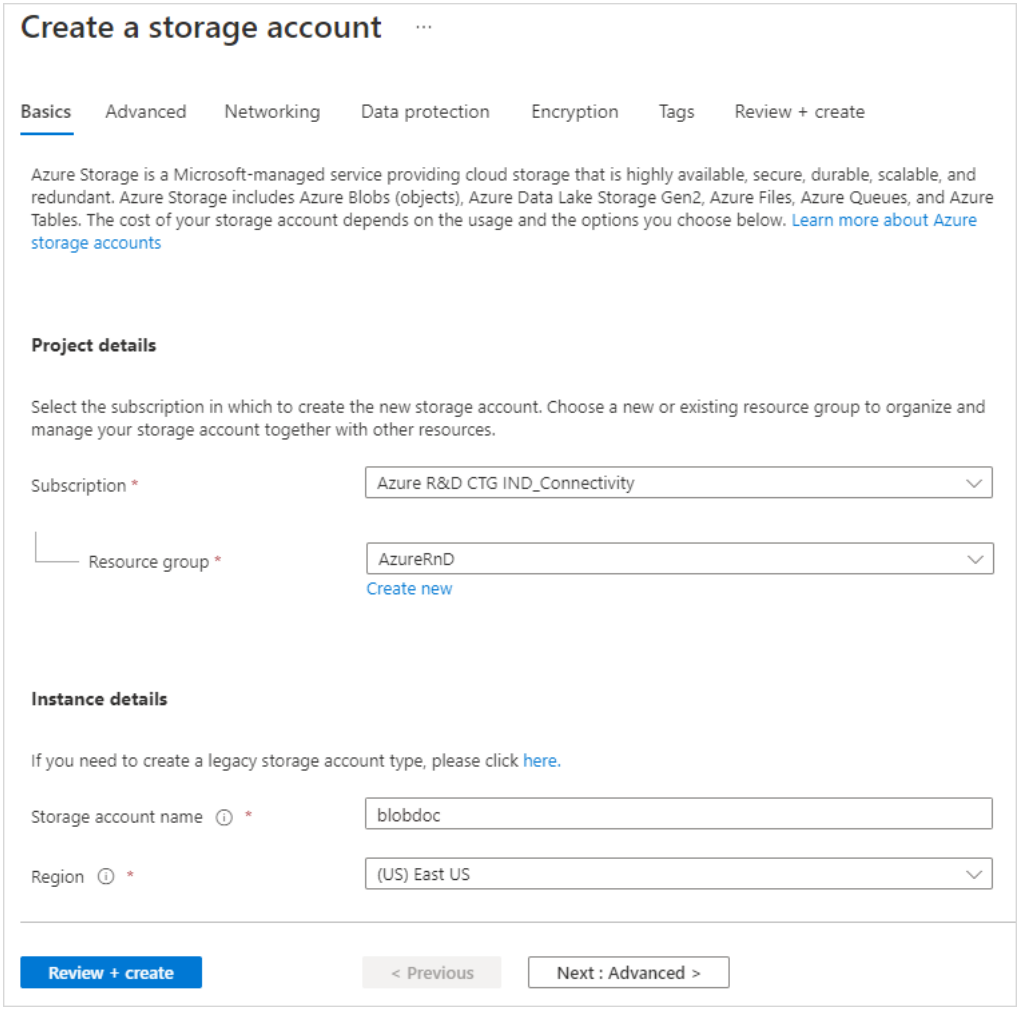
2. Under Azure Services, click **Storage accounts**.



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



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



a. In the **Subscription** field, select the subscription for which you want to create the storage account.

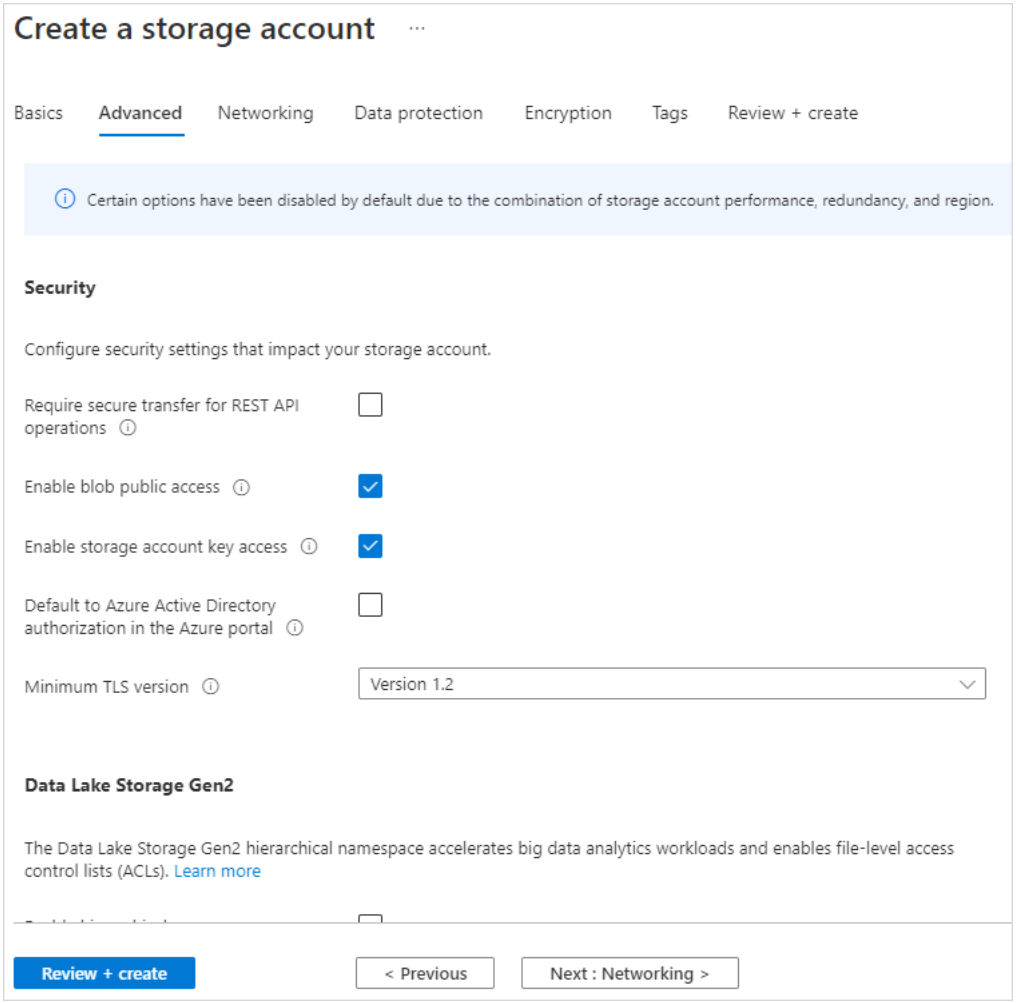
b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

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.

5. On the **Advanced** tab, configure the security settings.



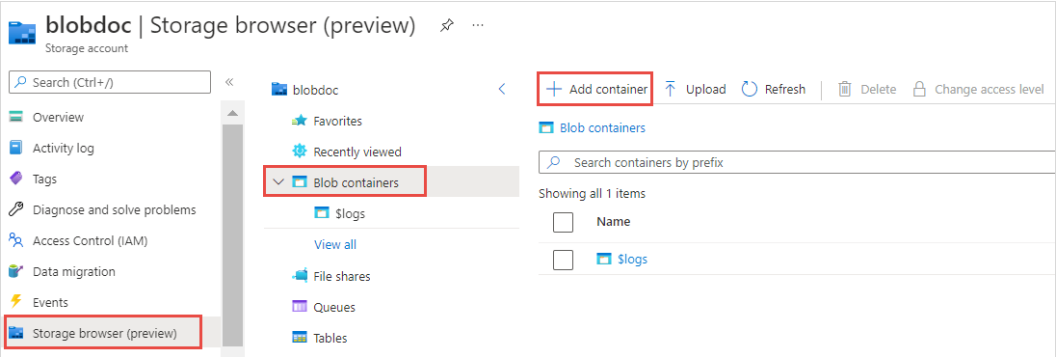
   a. Disable the **Require secure transfer for REST API operations** option.
   b. Select **Enable blob public access** to allow anonymous access to blobs within the storage account.
   c. Select **Enable storage account key access** to allow access to storage account using the shared key or shared access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

Create a blob container in the storage account

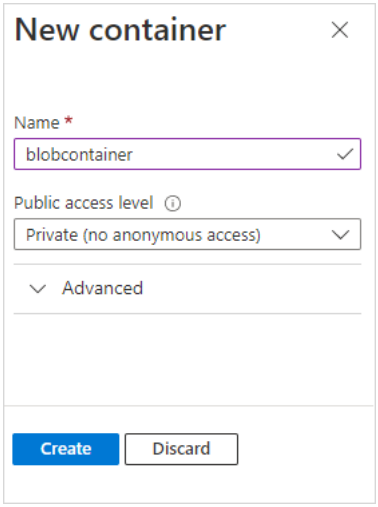
After you create the storage account, create a blob container and a virtual directory within the blob container.

1. Open the storage account that you created.

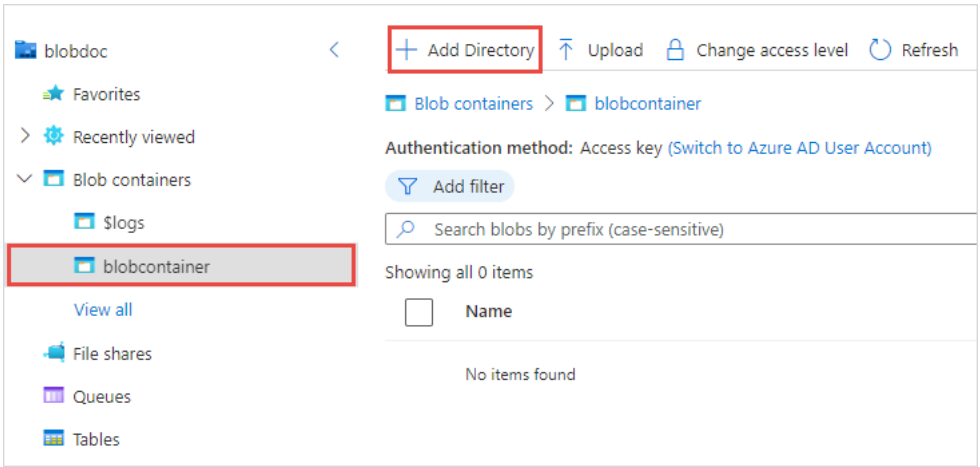
2. Click **Storage browsers** > **Blob containers**.



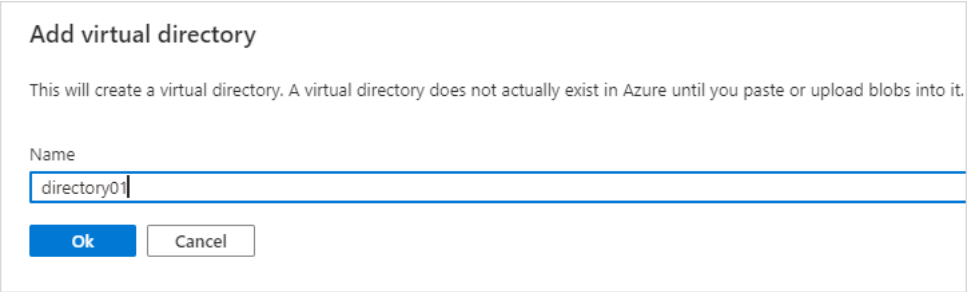
3. Click **Add container**.
4. Enter a name for the new container.



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



8. Enter a name for the directory.

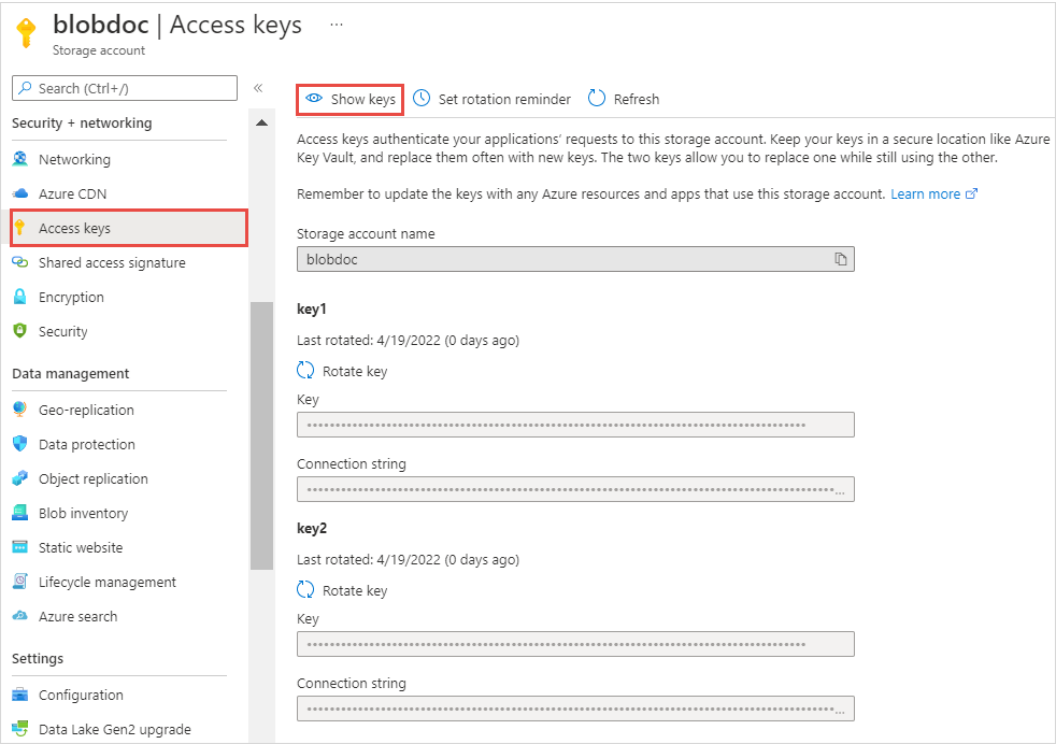


9. Click **Ok**.

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**.



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

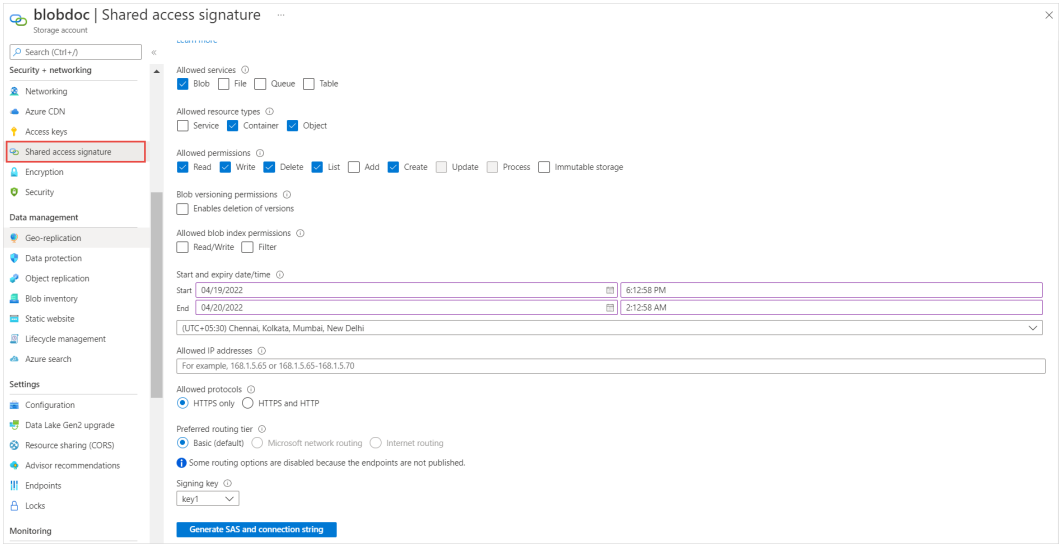
The shared access signature authentication uses the SAS token to connect to Microsoft Azure Blob Storage.

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**.



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.

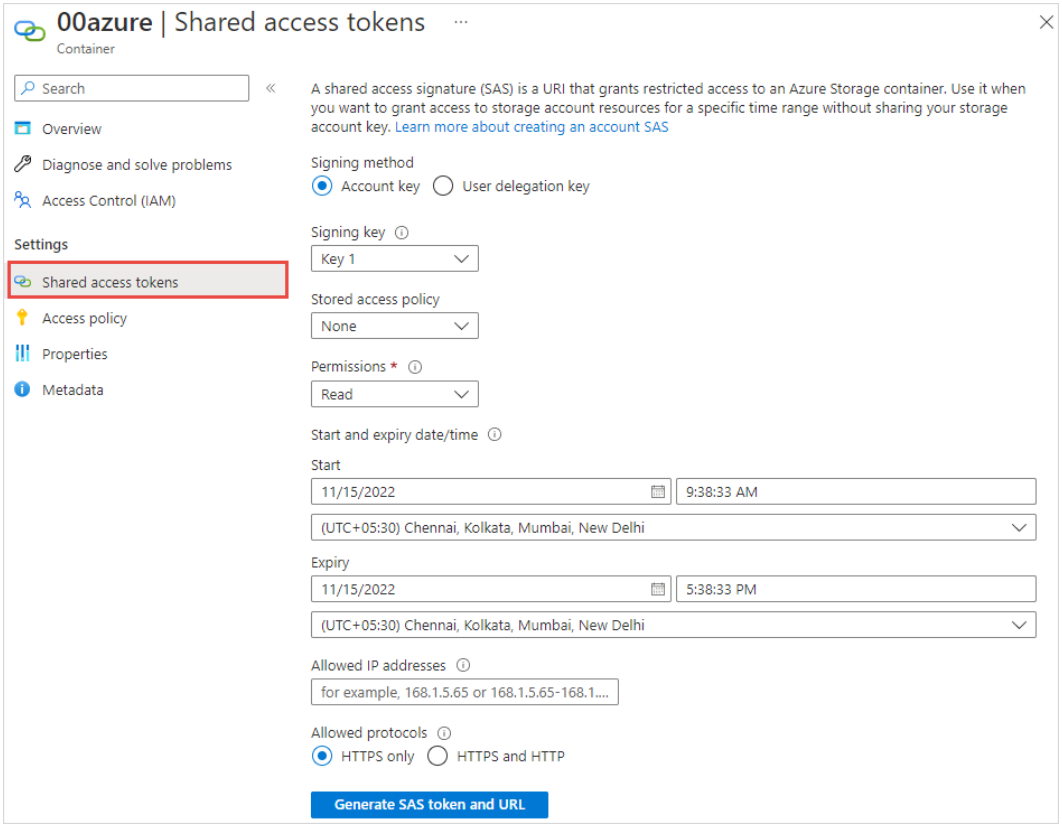
Get SAS token for the container

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**.



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.
7. In the **Allowed IP addresses** field, specify a public IP address or a range of public IP addresses.

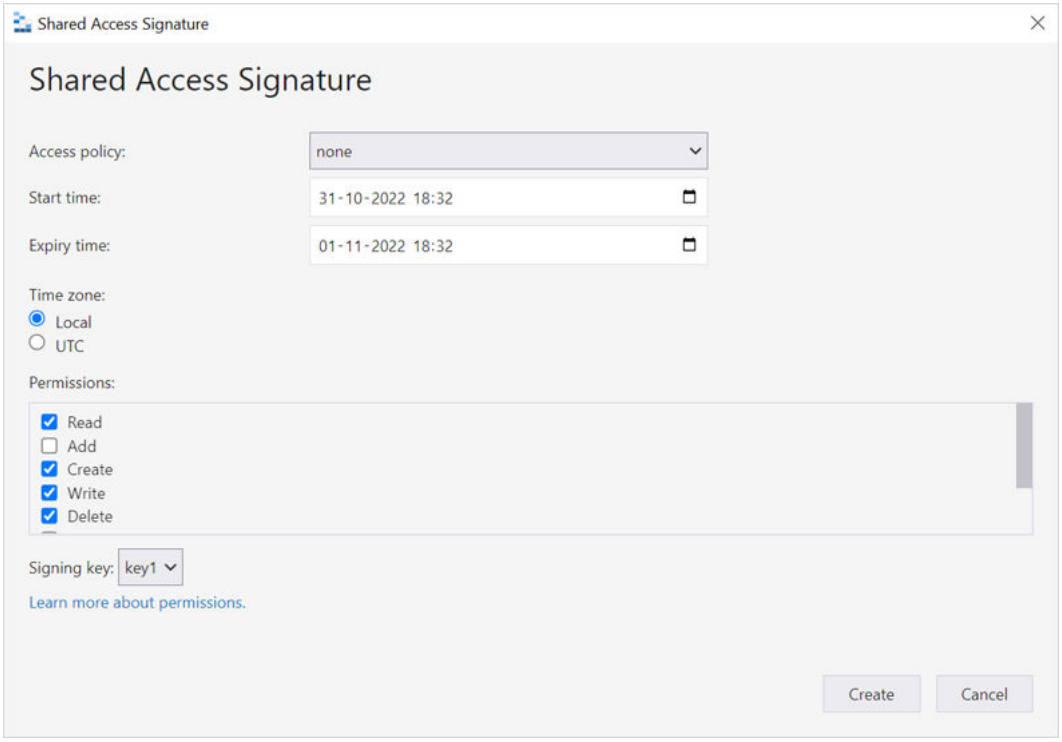
   Note: When you read Avro or Parquet files, do not specify the IP address.

8. 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.



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.