

Manage Shared Access Signature Keys

Understand the scenario

You are an Azure® administrator. You need to allow users to access an Azure storage account by using shared access signature (SAS) keys. First, you will create a storage account, and then you will create a container. Next, you will generate a SAS key, and then you will verify that you can access the container by using the SAS key. Finally, you will create an access policy, and then you will revoke the policy.

Understand your environment

You will be using an Azure resource group named corp-datalod26434762 that contains no resources.

# **Create a storage account and a container**

* Sign in to the Azure portal

Select the Copy to clipboard icon to copy the text string to the clipboard.

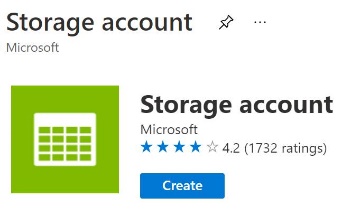
A cloud slice is a subset of an Azure subscription that has been assigned to a user account that was provisioned for you for the duration of this challenge lab. A cloud slice provides temporary access to a subset of resources available in a cloud subscription so that you can learn the concepts in this challenge lab without having to configure your own subscription.

A cloud slice has restrictions on the types of administrative activities that are allowed. Please follow the instructions carefully, especially with regard to names and other configuration details.

* Create an Azure storage account named sa26434762 by using the **corp-datalod26434762** resource group and locally-redundant storage (LRS).

Expand this hint for guidance on creating an Azure storage account.

* + On the Azure portal home page, select **Create a resource** to open the Azure Marketplace.
  + In the Azure Marketplace, search for and select Storage account, and then select **Create**.



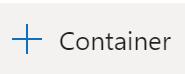
* + On the Create storage account blade, on the Basics page, in Resource group, select **corp-datalod26434762**, in Storage account name, enter sa26434762, and then in Redundancy, select **Locally-redundant storage (LRS)**.
  + Select **Review + create**, review the configuration, and then select **Create**.

An [Azure Storage account](https://docs.microsoft.com/en-us/azure/storage/common/storage-account-overview) supports binary large objects (blobs), file shares, non-relational tables and asynchronous message queues for scalable storage in the cloud.

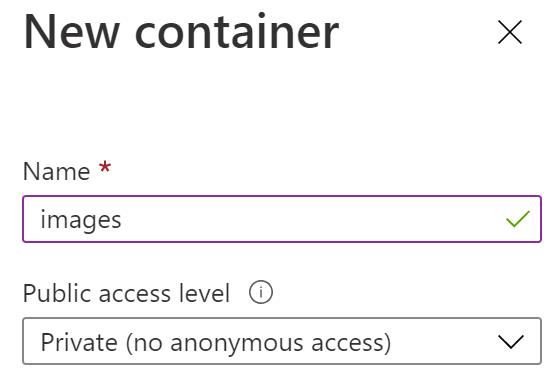
* Create a container named images in the **sa26434762** storage account.

Expand this hint for guidance on creating a blob container.

* + On the Azure portal home page, select **All resources**, and then select the **sa26434762** storage account.
  + On the sa26434762 resource menu, in Data storage, select **Containers**.
  + On the Containers page, on the command bar, select **Container** to add a container.



* + On the New container blade, in Name, enter images, in Public access level, ensure that **Private (no anonymous access)** is selected, and then select **Create**.



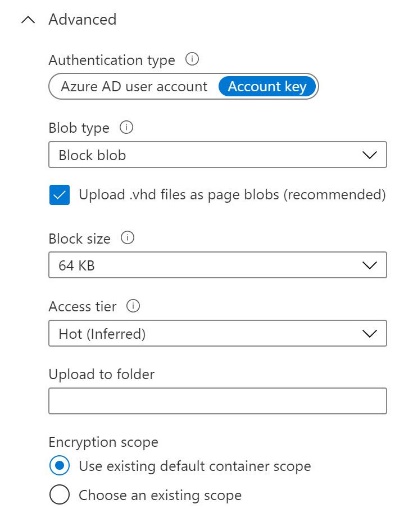
* Upload any image file on your computer to the **images** container as a **64 KB** block blob by using an authentication type of **Account key**.

Expand this hint for guidance on uploading a blob file.

* + On the Containers page, select the **images** container.
  + On the images page, on the command bar, select **Upload**.



* + On the Upload blob blade, in Files, select any image file on your computer (for example, .JPG, .PNG, or .GIF), and then expand **Advanced**.
  + In Advanced, in Authentication type, ensure that **Account key** is selected, in Blob type, ensure that **Block blob** is selected, and then in Block size, select **64 KB**.



* + Select **Upload**, and then if needed, close the Upload blob blade.

## Check your work

* Confirm that you created a storage account named sa26434762.
* Confirm that you created a container named images.
* Confirm that you uploaded a blob file to the images container.

# **Generate a SAS key**

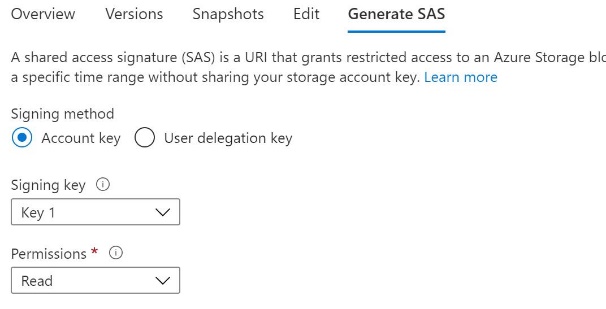
* Generate a SAS key for the blob file that you uploaded by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Signing method | **Account key** |
| Signing key | **Key 1** |
| Permissions | **Read** |
| Allowed protocols | **HTTPS only** |

* Expand this hint for guidance on generating a SAS key for a blob file.
  + If needed, in the **sa26434762** storage account, select the **images** container.
  + On the images page, select the blob file that you uploaded.
  + On the Blob page, select **Generate SAS**.



* + In Signing method, ensure that **Account key** is selected, in Signing key, ensure that **Key 1** is selected, in Permissions, ensure that **Read** is selected, and then in Allowed protocols, ensure that **HTTPS only** is selected.

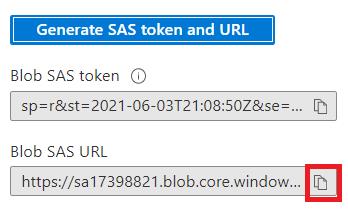


* + Select **Generate SAS token and URL**.
* Copy the **Blob SAS URL**, and then paste it into the following **Blob SAS URL** text box:

**Blob SAS URL**  


Expand this hint for guidance on copying the SAS URL for a blob file.

* + On the Generate SAS page, in Blob SAS URL, select the copy icon, and then paste the value into the **Blob SAS URL** text box.



* + Close the **Blob** page.
* Open a new browser window, and then go to the Blob SAS URL at <Blob\_SAS\_URL> to verify that you can access the blob file.

The blob file should be displayed by using HTTPS and the SAS key.

If you receive an This site has been reported as unsafe error message, select **More information**, and then select **Continue to the unsafe site (not recommended)** as you are only testing access to the blob.

* Close the new browser window.

## Check your work

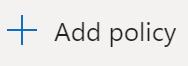
* Confirm that you generated a SAS key for a blob file.
* Confirm that you verified that you can access the blob file by using the SAS URL.

# **Create an access policy**

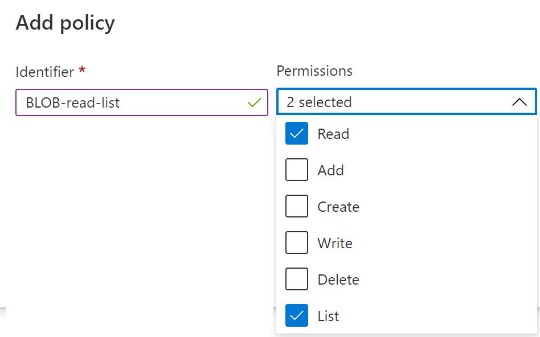
* Create an access policy for the **images** container by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Identifier | BLOB-read-list |
| Permissions | **Read** and **List** |
| Start time | The current date at **12:00 AM** |
| Expiry time | Tomorrow's date at **12:00 AM** |

* Expand this hint for guidance on creating an access policy for a container.
  + On the images resource menu, select **Access policy**.
  + On the Access policy page, in Stored access policies, select **Add policy**.



* + On the Add policy blade, in Identifier, enter BLOB-read-list, and then in Permissions, select **Read** and **List**.



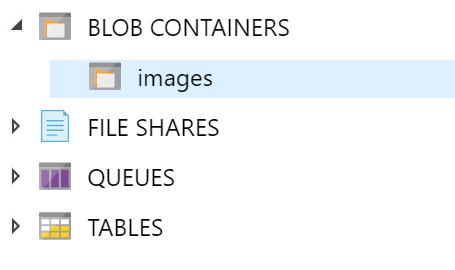
* + In Start time, select the current date, ensure that **12:00 AM** is entered, in Expiry time, select tomorrow’s date, and then ensure that **12:00 AM** is selected.
  + Select **OK**.
  + On the Access policy page, on the command bar, select **Save**, and then close the **Access policy** page.
* Generate a SAS key for the blob file that you uploaded by using the BLOB-read-list access policy.

Expand this hint for guidance on generating a SAS key for a blob file by using an access policy.

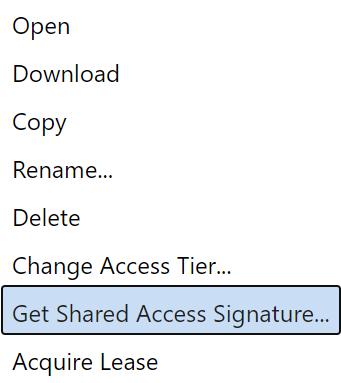
* + On the sa26434762 resource menu, select **Storage browser (preview)**.
  + On the Storage browser (preview) page, on the command bar, select **Switch back to storage explorer**.

Switch to Storage Explorer

* + On the Storage Explorer (preview) page, expand **BLOB CONTAINERS**, and then select **images**.



* + Verify that the image file you uploaded is listed.
  + Right-click the image file, and then select **Get Shared Access Signature**.



* + On the Shared Access Signature blade, in Access policy, select **BLOB-read-list**, and then select **Create**.

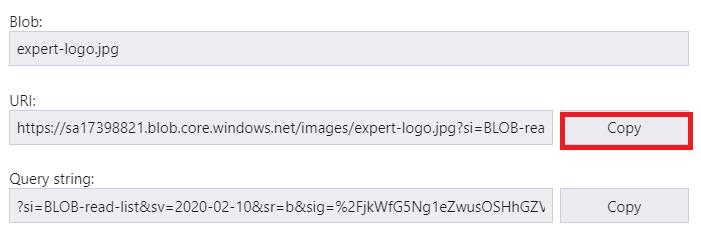
If Storage browser does not appear, select the Overview page on the resource menu, and then select Storage browser again.

* Copy the SAS **URI**, and then paste it into the following **Blob SAS URI** text box:

**Blob SAS URI**  


Expand this hint for guidance on copying a SAS URI for a blob file.

* + On the Shared Access Signature blade, in URI, select **Copy**, and then paste the value into the **Blob SAS URI** text box.



* + Close the **Shared Access Signature** blade.
* Open a new browser window, and then go to the SAS URI at <Blob\_SAS\_URI> to verify that you can access the blob file.

The blob file should be displayed by using the access policy.

* Keep the browser window open for the next task.

## Check your work

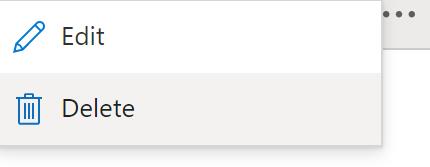
* Confirm that you created an access policy.
* Confirm that you generated a SAS key by using an access policy.
* Confirm that you verified that you can access the blob file by using the SAS URI.

# **Revoke an access policy**

* Delete the **BLOB-read-list** access policy for the **images** container to revoke the access policy.

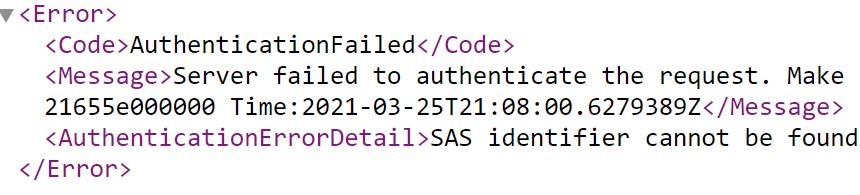
Expand this hint for guidance on revoking an access policy for a container.

* + On the sa26434762 resource menu page, select **Containers**, and then select the **images** container.
  + On the images resource menu, select **Access policy**.
  + On the Access policy page, in Stored access policies, select the ellipsis to the right of the **BLOB-read-list** policy, and then select **Delete**.



* + On the command bar, select **Save**, and then close the **Access policy** page.
* In the browser window, refreshing the SAS URI at <Blob\_SAS\_URI>, and then verify that you are unable to access the page.

You should see an Authentication failed error message because the access policy has been revoked.



## Check your work

* Confirm that you revoked the access policy.

# **Summary**

Congratulations, you have completed the **Manage Shared Access Signature Keys** challenge.

You have accomplished the following:

* Created a storage account and container.
* Generated a SAS key and verified that it grants access to the container.
* Created an access policy.
* Revoked an access policy, and then verified that the policy was revoked.