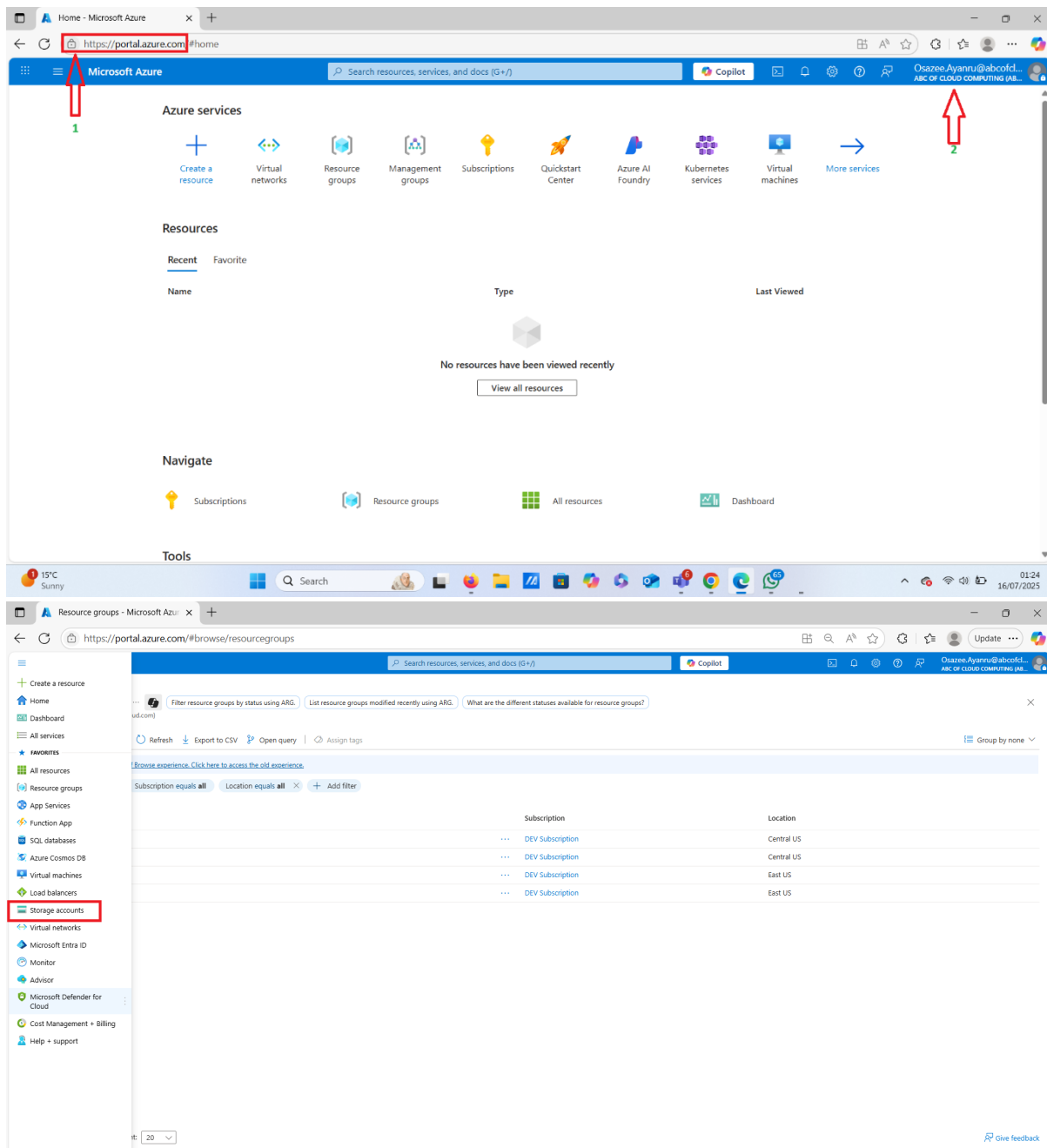


## Step 1 – Create a Storage Account:

- . Log in to the Azure Portal: <https://portal.azure.com>
- . In the search bar, type Storage accounts and select it.
- . Click on Storage Accounts



- . Click Create.
- . Fill in the basics:
  - Subscription: Choose your Azure subscription. E.g., (DEV Subscription).
  - Resource group: Create a new one or select existing. E.g., (SAZYRG).
  - Storage account name: e.g., sazystorage.

Must be unique (only lowercase letters and numbers).

- Region: Choose a location close to your audience. E.g., ((US) East US)
- Performance: Select Standard.
- Redundancy: Choose Locally-redundant storage (LRS) for cost-effectiveness.
- Then Click Next

Storage accounts - Microsoft Azure

https://portal.azure.com/#browse/Microsoft.Storage%2FStorageAccounts

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Update

Home

Storage accounts

ABC OF CLOUD COMPUTING (abcofcloud.com)

Evaluate data resiliency for storage accounts | Check security best practices for these storage accounts | Review disaster recovery posture for storage accounts

+ Create | Restore | Manage view | Refresh | Export to CSV | Open query | Assign tags | Delete

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field... | Subscription equals all | Resource Group equals all | Location equals all | + Add filter

Showing 1 - 0 of 0. Display count: 20

give feedback

No storage accounts to display

Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed.

Create

Learn more

Create a storage account - Microsoft Azure

https://portal.azure.com/#create/Microsoft.StorageAccount

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

Update

Home > Storage accounts >

Create a storage account

Basics | Advanced | Networking | Data protection | Encryption | Tags | Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription \* | DEV Subscription

Resource group \* | SAZYRG

Create new

Instance details

Storage account name \* | sazystorage

Region \* | (US) East US

Deploy to an Azure Extended Zone

Primary service | Azure Blob Storage or Azure Data Lake Storage Gen 2

Performance \* | Standard: Recommended for most scenarios (general purpose v2 account)

Premium: Recommended for scenarios that require low latency.

Redundancy \* | Locally-redundant storage (LRS)

Previous | Next | Review + create

give feedback

- **ADVANCE:** Leave this as Default or make changes if needed, then click next

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal, specifically the 'Advanced' tab. The page is titled 'Create a storage account' and has a breadcrumb trail 'Home > Storage accounts >'. The 'Advanced' tab is selected, with other tabs being 'Basics', 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review + create'. The 'Security' section is expanded, showing options for 'Require secure transfer for REST API operations' (checked), 'Allow enabling anonymous access on individual containers' (unchecked), 'Enable storage account key access' (checked), and 'Default to Microsoft Entra authorization in the Azure portal' (unchecked). There are dropdown menus for 'Minimum TLS version' (set to 'Version 1.2') and 'Permitted scope for copy operations (preview)' (set to 'From any storage account'). The 'Hierarchical Namespace' section is also expanded, showing 'Enable hierarchical namespace' (unchecked). The 'Access protocols' section is expanded, showing 'Enable SFTP' (unchecked) and 'Enable network file system v3' (unchecked). At the bottom, there are three buttons: 'Previous', 'Next' (highlighted with a red box), and 'Review + create'. The Windows taskbar at the bottom shows the date as 15/08/2025 and the time as 08:48.

Create a storage account - Micro: x +

https://portal.azure.com/#create/Microsoft.StorageAccount

Microsoft Azure Search resources, services, and docs (G+V) Copilot Update ...

Home > Storage accounts >

Create a storage account ...

Basics Advanced Networking Data protection Encryption Tags Review + create

**Security**  
Configure security settings that impact your storage account.

Require secure transfer for REST API operations ☒

Allow enabling anonymous access on individual containers ☐

Enable storage account key access ☒

Default to Microsoft Entra authorization in the Azure portal ☐

Minimum TLS version

Permitted scope for copy operations (preview)

**Hierarchical Namespace**  
Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs). [Learn more >](#)

Enable hierarchical namespace ☐

**Access protocols**  
Blob and Data Lake Gen2 endpoints are provisioned by default. [Learn more >](#)

Enable SFTP ☐  
SFTP can only be enabled for hierarchical namespace accounts

Enable network file system v3 ☐  
To enable NFS v3 'hierarchical namespace' must be enabled. [Learn more about NFS >](#)

Previous Next Review + create

25°C Sunny 08:48 15/08/2025

- Network: Leave this as Default or make changes if needed, then click next

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal, specifically the 'Networking' tab. The 'Public access' section is expanded, showing options for 'Public network access'. The 'Enable' option is selected, and the 'Public network access scope' is set to 'Enable from all networks'. A warning message states: 'Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations.' The 'Private endpoint' section is also visible, with a table for adding private endpoints. The 'Network routing' section is at the bottom, with 'Microsoft network routing' selected. The 'Next' button is highlighted with a red box.

Microsoft Azure

Home > Storage accounts >

Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review + create

**Public access**  
Access your resource from anywhere through a public network.  
Note: Allowing access to your resource through a public network increases security risk. [Learn more](#)

Public network access \*

☒ Enable  
Allow inbound and outbound access with the option to restrict select inbound access using resource access configurations for this resource.

☐ Disable  
Restrict inbound access while allowing outbound access.

☐ Secure by perimeter (Most restricted)  
Restrict inbound and outbound access using a network security perimeter. Secure by perimeter offers the greatest level of inbound and outbound restriction to secure your resource.

Public network access scope \*

☒ Enable from all networks

☐ Enable from selected virtual networks and IP addresses

⚠ Enabling public network access will make this resource available publicly. Unless public access is required, consider using the most restricted access configurations.

**Private endpoint**  
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

+ Add private endpoint

Name	Subscription	Resource group	Region	Target sub-	Subnet	Private DN...
------	--------------	----------------	--------	-------------	--------	---------------

Click on add to create a private endpoint

**Network routing**  
Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference \*

☒ Microsoft network routing

☐ Internet routing

Previous **Next** Review + create

- Data Protection: Leave this as Default or make changes if needed, then click next

Microsoft Azure

Home > Storage accounts >

### Create a storage account

Basics Advanced Networking **Data protection** Encryption Tags Review + create

**Recovery**  
Protect your data from accidental or erroneous deletion or modification.

- ☐ Enable point-in-time restore for containers  
Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)
- ☒ Enable soft delete for blobs  
Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)  
Days to retain deleted blobs
- ☒ Enable soft delete for containers  
Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)  
Enabling soft delete for frequently overwritten data may result in increased storage costs. [Learn more](#)  
Days to retain deleted containers
- ☒ Enable soft delete for file shares  
Soft delete enables you to recover file shares that were previously marked for deletion. [Learn more](#)  
Days to retain deleted file shares

**Tracking**  
Manage versions and keep track of changes made to your blob data.

- ☐ Enable versioning for blobs  
Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)  
Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. [Learn more](#)

**Access control**

- ☐ Enable version-level immutability support  
Allows you to set time-based retention policy on the account-level that will apply to all blob versions. Enable this feature to set a default policy at the account level. Without enabling this, you can still set a default policy at the container level or set policies for specific blob versions. Versioning is required for this property to be enabled. [Learn more](#)

- **ENCRYPTION AND TAGS:** Leave this as Default or make changes if needed, then click next.

The image displays two screenshots of the Microsoft Azure portal's 'Create a storage account' wizard, specifically the 'Encryption' and 'Tags' steps.

**Top Screenshot (Encryption Tab):**

- Encryption type:** ☒ Microsoft-managed keys (MMK), ☐ Customer-managed keys (CMK).
- Enable support for customer-managed keys:** ☒ Blobs and files only, ☐ All service types (blobs, files, tables, and queues). A warning states: 'This option cannot be changed after this storage account is created.'
- Enable infrastructure encryption:** ☐
- Navigation:** Previous, **Next** (highlighted), Review + create.

**Bottom Screenshot (Tags Tab):**

Name	Value	Resource
<input type="text"/>	<input type="text"/>	All resources selected

**Navigation:** Previous, **Next** (highlighted), Review + create.

- Click Review + create, then click create and go to resources when Deployment is complete.

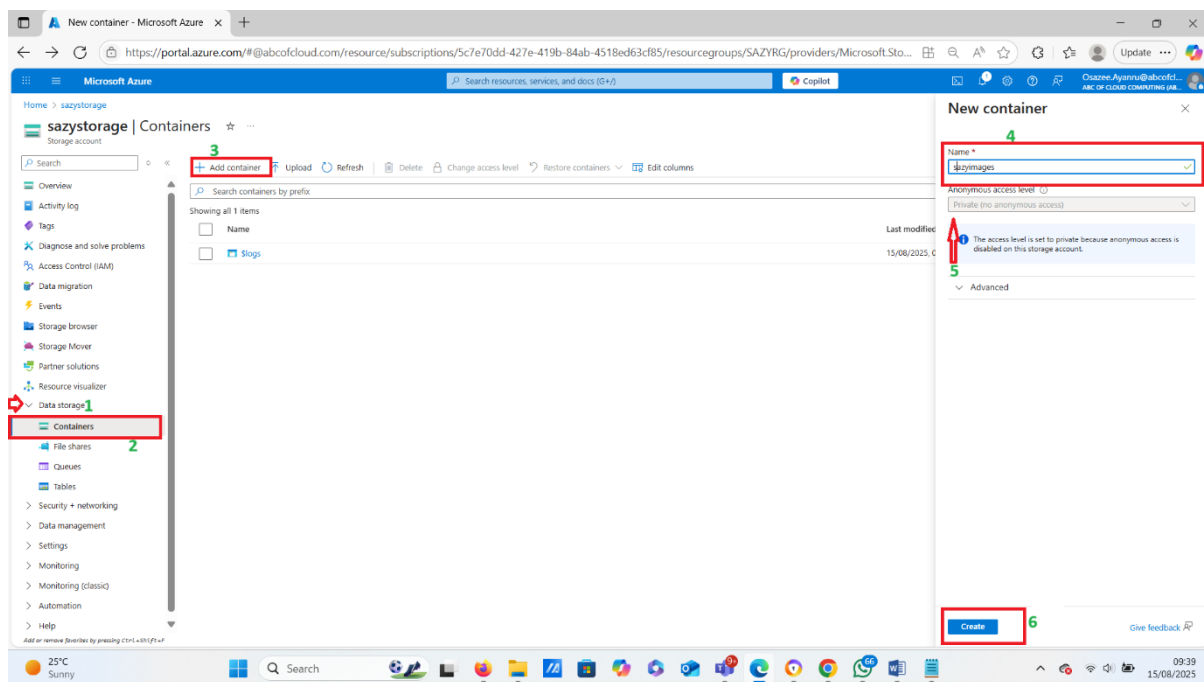
The first screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The 'Review + create' tab is selected and highlighted with a red box. Below the tabs, the 'Basics' section displays configuration details: Subscription (DEV Subscription), Resource group (SAZVRG), Location (East US), Storage account name (sazystorage), Primary service (Azure Blob Storage or Azure Data Lake Storage Gen 2), Performance (Standard), and Replication (Locally-redundant storage (LRS)). The 'Advanced' section shows various settings like 'Enable hierarchical namespace' (Disabled) and 'Access tier' (Hot). The 'Security' section shows 'Secure transfer' (Enabled) and 'Blob anonymous access' (Disabled). At the bottom, the 'Create' button is highlighted with a red box.

The second screenshot shows the 'Overview' page for the storage account 'sazystorage\_1755271286334'. A green checkmark indicates 'Your deployment is complete'. The deployment details show the name 'sazystorage\_1755271286334', subscription 'DEV Subscription', and resource group 'SAZVRG'. The 'Next steps' section includes a 'Go to resource' button, which is highlighted with a red box. The right sidebar contains links for 'Cost Management', 'Microsoft Defender for Cloud', 'Free Microsoft tutorials', and 'Work with an expert'.



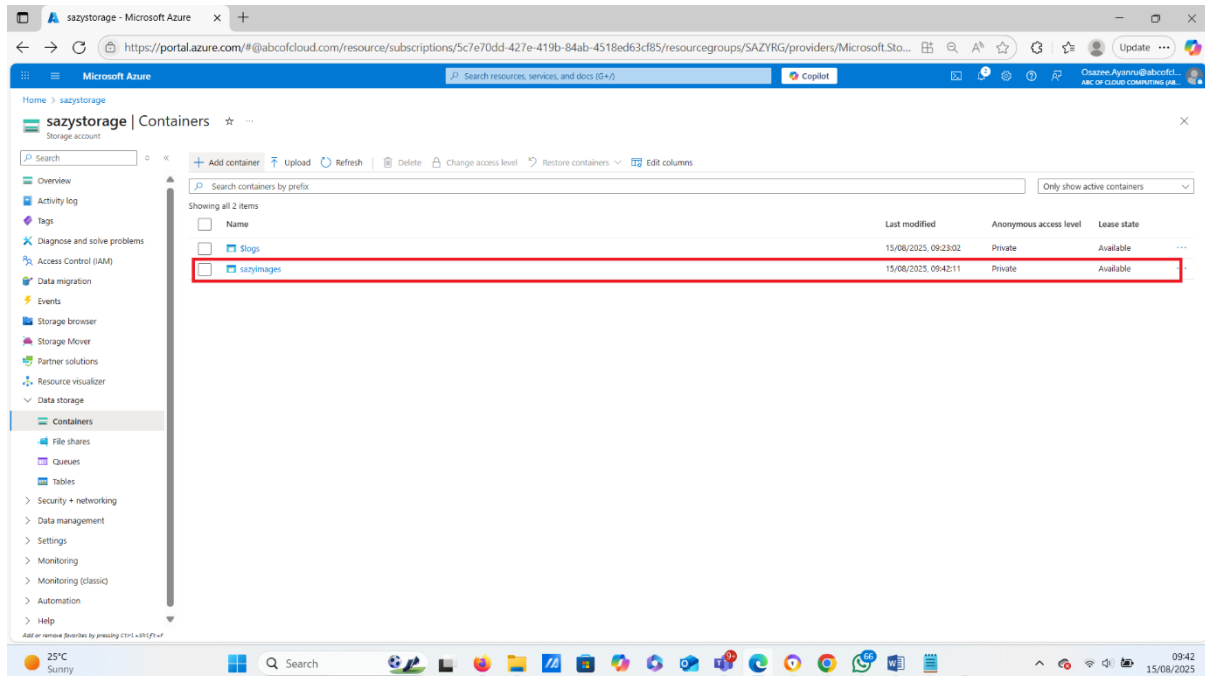
## Step 2 – Create a Blob Container

1. Go to your new Storage Account.
2. In the left menu, under Data storage, select Containers.
3. Click + Container.
4. Name it (e.g., sazyimages).
5. Set Public access level to Private (no anonymous access) — this keeps your data secure until you choose to share via SAS.
6. Click Create.



## Step 3 – Upload an Image

. Open the container you just created.



- . Click Upload.
- . Browse your computer and select the image file and Click Upload.
- . Your file will now appear in the container's blob list.

The first screenshot shows the 'Upload blob' dialog box in the Microsoft Azure portal. The dialog has a title bar 'Upload blob' and a close button. Inside, there is a dashed box for file selection. A red box labeled '2' highlights the text '1 file(s) selected: adid-removebg-preview.png' and 'Drag and drop files here or Browse for files'. Below this, there is a checkbox for 'Overwrite if files already exist' and a section for 'Advanced' options. A red box labeled '3' highlights the 'Upload' button at the bottom left of the dialog.

The second screenshot shows the 'sazyimages' container overview page. The 'Upload' button in the top toolbar is highlighted with a red box. Below the toolbar, the 'Showing all 2 items' section displays a table of blobs. A red box highlights the table content, which lists two blobs: 'adid-removebg-preview.png' and 'back.jpg'. The table has columns for Name, Last modified, Access tier, Blob type, Size, and Lease state.

Name	Last modified	Access tier	Blob type	Size	Lease state
adid-removebg-preview.png	15/08/2025, 09:50:04	Hot (Inferred)	Block blob	8.6 KB	Available
back.jpg	15/08/2025, 09:50:43	Hot (Inferred)	Block blob	6.07 MB	Available

The 'Notifications' panel on the right shows two success messages: 'Successfully uploaded blob(s)' and 'Successfully uploaded 1 blob(s)', each with a green checkmark icon.

## Step 4 – Generate a Shared Access Signature (SAS)

A SAS link gives controlled access without exposing your account keys.

1. In your container, click the image you just uploaded.
2. At the top, select Generate SAS (sometimes shown as Shared access tokens in the menu).
3. In the SAS settings:
  - Permissions: Select Read.
  - Start and Expiry date/time: Set a reasonable expiry window (e.g., a few days or weeks).
  - Allowed protocols: Select HTTPS only for security.
4. Click Generate SAS token and URL.
5. Copy the Blob SAS URL — this is the link you can share.

Microsoft Azure portal interface showing the 'Containers' section. The left sidebar lists various services, with 'Containers' highlighted. The main area displays a table of containers:

Name	Last modified	Anonymous access level	Lease state
slog	15/08/2025, 09:23:02	Private	Available
sazyimages	15/08/2025, 09:42:11	Private	Available

A red arrow points to the 'sazyimages' container.

Microsoft Azure portal interface showing the 'Generate SAS' dialog for the 'adiid-removebg-preview.png' blob. The 'Generate SAS' tab is selected, and the 'Generate SAS token and URL' button is highlighted.

Authentication method: Access key (Switch to Microsoft Entra user account)

Signing method: ☒ Account key ☐ User delegation key

Signing key:

Stored access policy:

Permissions:

Start and expiry date/time:

Start:

Expiry:

Allowed IP addresses:

Allowed protocols: ☒ HTTP only ☐ HTTPS and HTTP

**Generate SAS token and URL**

adid-removebg-preview.png - M x | sazstorage.blob.core.windows.n: x | +

https://portal.azure.com/#view/Microsoft\_Azure\_Storage/ContainerMenuBlade/~/overview/storageAccountId/%2Fsubscriptions%2F5c7e70dd-427e-419b-84ab-4518ed... | Search resources, services, and docs (G+I) | Copilot | Update ...

Microsoft Azure

Home > sazstorage | Containers >

sazyimages Container

Search

+ Add Directory Upload Change access level Refresh De

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

sazyimages

Authentication method: Access key (Switch to Microsoft Entra user account)

Add filter

Search blobs by prefix (case-sensitive)

Showing all 2 items

☐ Name

☒ adid-removebg-preview.png

☐ backG.jpg

adid-removebg-preview.png

Save Discard Download Refresh Delete

A shared access signature (SAS) is a URI that grants restricted access to an Azure Storage blob. 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](#)

Signing method ☒ Account key ☐ User delegation key

Signing key

Stored access policy

Permissions

Start and expiry date/time

Start

(UTC-06:00) Central America

Expiry

(UTC-06:00) Central America

Allowed IP addresses

Allowed protocols ☒ HTTPS only ☐ HTTPS and HTTP

Generate SAS token and URL

Blob SAS token

Blob SAS URL

24°C Sunny

Search

adid-removebg-preview.png - M x | sazstorage.blob.core.windows.n: x | https://sazstorage.blob.core.wi... x | +

https://sazstorage.blob.core.windows.net/sazyimages/adid-removebg-preview.png?sp=r&st=2025-08-15T16:09:02Z&se=2025-08-16T00:24:02Z&spr=https&sv=2024-11-04&sr=b&sig=TMMUJEI642N81oAt6feN1P38IebD7dkm24KApL5hQn63D

adidas

24°C Sunny

Search