

Tutorial S2: Blob storage container

Creating a storage account in Azure will allow you to create containers of stored data that you can mount onto their machines.

This tutorial covers how to do the following steps through the Azure desktop portal:

1. Create a **storage account****
2. Create a **storage container** within the storage account
3. Look at data within the storage container
4. Read and write data to the storage container using azcopy
5. Get storage account name and key (for NotebookS4)

**The settings you select when creating the storage account are extremely important to make sure it is easily accessible later.

1. Creating a storage account

Create a storage account ...

- Basics
- Advanced
- Networking
- Data protection
- Encryption
- Tags
- Review

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 *

Resource group *

[Create new](#)

Review

< Previous

Next : Advanced >

 Give feedback

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review

Subscription

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).



Storage account name ⓘ * ✖ The value must not be empty.

Region ⓘ * [Deploy to an edge zone](#)

Performance ⓘ *

Review

< Previous

Next : Advanced >

Give feedback

We want to create a legacy storage account type, which makes it easier to access shared file storage. Click here.

Create storage account ...

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 *

Resource group * [Create new](#)

Instance details

Storage account name * ⓘ

Location *

Performance ⓘ Standard Premium

Account kind ⓘ

Replication ⓘ

Name it whatever you like and tie it to your desired resource group.

For Replication, select either “Locally Redundant Storage” or “Zone Redundant Storage”.

Review + create

< Previous

Next : Networking >



Create storage account ...

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

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Connectivity method *

- Public endpoint (all networks)
- Public endpoint (selected networks)
- Private endpoint

Virtual networks

Only the selected network will be able to access this storage account. [Learn more about service endpoints](#)

Virtual network subscription ⓘ

Zoe_Krauss

Virtual network ⓘ

krausszoe_vnet

[Create virtual network](#)
[Manage selected virtual network](#)

Subnets * ⓘ

krausszoe_vnet/default (10.0.0.0/24)

Review + create

< Previous

Next : Data protection >

Under networking, select “Public endpoint (selected networks)”

Select the virtual network you will be working in, with the default subnet.

Default Microsoft network routing is fine.

Create storage account ...

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

Security

Require secure transfer for REST API operations Disabled Enabled ⓘ

Allow storage account key access Disabled Enabled ⓘ

Minimum TLS version ⓘ

Infrastructure encryption Disabled Enabled ⓘ

Blob storage

Allow Blob public access Disabled Enabled ⓘ

Blob access tier (default) Cool Hot ⓘ

NFS v3 Disabled Enabled ⓘ

Data Lake Storage Gen2

Hierarchical namespace Disabled Enabled ⓘ

Azure Files

Large file shares Disabled Enabled ⓘ

Tables and Queues

Customer-managed keys support Disabled Enabled ⓘ

Data Protection selections can be left as default. Navigate to Advanced, and select the options shown to the left.

**Make sure NFS v3 is enabled!
This is how we will be
accessing containers in the
storage account.**

Review & create.

2. Create a storage container

Great! Now we have a storage account set up with the proper permissions and abilities enabled.

Now, we have to create a container within the account in which to actually store data.

Home > Storage accounts > seismiccloud

Storage accounts

UW (cloud.washington.edu)

+ Create ↶ Restore ...

Filter for any field...

Name ↑↓

- seismiccloud
- seismiccloud2

seismiccloud | Containers

Storage account

Search

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)
- Data migration
- Events
- Storage browser
- Data storage**
 - Containers
 - File shares
 - Queues
 - Tables
- Security + networking

+ Container Change access level Restore contain

Search New container prefix

Show deleted containers

Name	Last modified	Pr
<input type="checkbox"/> \$logs	1/20/2023, 3:07:57 PM	Pr
<input type="checkbox"/> seismiccloud	1/20/2023, 3:12:53 PM	Pr

New container

Name * seismiccloud3 ✓

Public access level ⓘ Container (anonymous read access for containers and blobs) ▾

⚠ All container and blob data can be read by anonymous request. Clients can enumerate blobs within the container by anonymous request, but cannot enumerate containers within the storage account. Anonymous access bypasses Access Control List (ACL) settings.

Advanced

Click on your storage account, and then “Containers” on the sidebar. Add a new container.

Name it anything you like, and specify “Container” as the public access level.

3. Look at data in storage
account

Once your container is created, you can navigate to it and see what's inside.

Microsoft Azure

Search resources, services, and docs (G+)

Home > seismiccloud2

seismiccloud2 | Containers Storage account

Search

+ Container Change access level Restore containers Refresh Delete Give feedback

Search containers by prefix Show deleted containers

Name	Last modified	Public access level	Lease state
<input type="checkbox"/> seismiccloud	2/3/2023, 9:37:32 AM	Container	Available

Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Data storage
Containers
File shares
Queues
Tables
Security + networking

zkrauss@uw.edu
UW (CLOUD.WASHINGTON.EDU)

Within the storage account, navigate to "Containers" to see a list of containers you have.

Click on your container of interest to see what's inside!

If you see this screen or a similar error message when you click on your container, you'll need to edit the "Networking" settings of the Storage Account itself. See next slide...

The screenshot shows the Microsoft Azure portal interface. At the top, there is a navigation bar with the Microsoft Azure logo, a search bar, and user information for zkrauss@uw.edu. The main content area displays the 'seismiccloud' container overview page. A large error message is centered on the screen, stating 'This request is not authorized to perform this operation.' Below the error message is a 'Summary' section with a copy icon, containing the following details:

Session ID	79e301041fd547049518df255c6dd94e	Resource ID	/subscriptions/f387c92a-68b5-4d09-8497-e3a4a7199af...
Extension	Microsoft_Azure_Storage	Content	BlobsBlade
Error code	403	Storage Request ID	0103b189-001e-0023-5e75-8a8ee0000000

Below the summary, there is a 'Details' section with the following information:

- This request is not authorized to perform this operation. RequestId:0103b189-001e-0023-5e75-8a8ee0000000 Time:2023-05-19T17:18:29.4585787Z
- This storage account's 'Firewalls and virtual networks' settings may be blocking access to storage services. Trv

On the page for the Storage Account, navigate to “Networking” on the side bar and scroll down to the Firewall section.

Microsoft Azure Search resources, services, and docs (G+)

Home > seismiccloud2

seismiccloud2 | Networking Storage account

Search

Storage browser

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking**
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Redundancy

Firewall
Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Address range	
75.172.164.18	
205.175.106.67	
205.175.106.16	
205.175.106.6	
205.175.106.114	
205.175.106.1148	
205.175.118.225	
205.175.118.224	
205.175.106.100	
<input type="text" value="IP address or CIDR"/>	

Resource instances
Specify resource instances that will have access to your storage account based on their system-assigned managed identity.

Resource type	Instance name
---------------	---------------

Navigate to “Networking”

Here enter your current public IP address.

To check your current public IP, you can use the command:
`>> curl ifconfig.me`

Continued on next slide...

After typing in your Public IP Address, scroll up and hit “Save”.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with 'Microsoft Azure' and a search bar. Below that, the breadcrumb 'Home > seismiccloud2' is visible. The main header reads 'seismiccloud2 | Networking' with a star icon and a close button. A search bar is present on the left. The left sidebar contains various categories: 'Data storage' (Containers, File shares, Queues, Tables), 'Security + networking' (Networking, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and 'Data management' (Redundancy). The main content area is titled 'Firewalls and virtual networks' and 'Private endpoint connections'. Under 'Firewalls and virtual networks', there are three buttons: 'Save' (highlighted with a red circle), 'Discard', and 'Refresh'. A red line points from the 'Save' button to the text 'Here!' on the right. Below this, there are radio buttons for 'Public network access' (Enabled from all networks, Enabled from selected virtual networks and IP addresses, Disabled) and a link to 'Configure network security for your storage accounts'. The 'Virtual networks' section has two '+ Add' buttons. Below that is a table with columns: Virtual Network, Subnet, Address range, Endpoint Status, Resource Group, and Subscription. The table contains one row for 'krausszoe_vnet' with subnet '1', resource group 'krausszoe', and subscription 'Zoe_Krauss'. The 'Firewall' section has a heading and a link to 'Learn more'. Below that is a table with columns: Address range and a trash icon.

Microsoft Azure Search resources, services, and docs (G+)

Home > seismiccloud2

seismiccloud2 | Networking Storage account

Search

Storage browser

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Redundancy

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh

Public network access

- Enabled from all networks
- Enabled from selected virtual networks and IP addresses
- Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

- + Add existing virtual network
- + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
> krausszoe_vnet	1			krausszoe	Zoe_Krauss

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more.](#)

Address range
75.172.164.18

It sometimes takes a few seconds for the new networking settings to take effect, but you should now be able to access your container through “Containers” in the side bar.

Once you successfully have access into the container page, you will see a screen like this. You can click on different folders and navigate through files in the same way you would a laptop!

Microsoft Azure Search resources, services, and docs (G+)

zkrauss@uw.edu UW (CLOUD.WASHINGTON.EDU)

Home > seismiccloud2 | Containers >

seismiccloud

Container

Search

Upload Add Directory Refresh Rename Delete Change tier Acquire lease Break lease Give feedback

Authentication method: Access key ([Switch to Azure AD User Account](#))
Location: seismiccloud

Search blobs by prefix (case-sensitive) Show deleted objects

Name	Modified	Access tier	Archive status	Blob type	Size
<input type="checkbox"/> endeavour					
<input type="checkbox"/> ml_output					
<input type="checkbox"/> mloutput_2016					
<input type="checkbox"/> mloutput_2017					
<input type="checkbox"/> outputs					

Settings

- Shared access tokens
- Manage ACL
- Access policy
- Properties
- Metadata

4. Write and read data to/from the storage container

There are several ways to do this, but the we found that the easiest and most straightforward was using Azure's azcopy Command Line Interface (CLI).

You can interact with the storage container using a CLI called azcopy, which you must install from Azure.

<https://learn.microsoft.com/en-us/azure/storage/common/storage-use-azcopy-files>

To write data *to* the storage container, the command has the form:

```
>> azcopy copy "<local directory to copy>"  
"https://{storage_account_name}.blob.core.windows.net/{storage_container_name}?{sas_token}" -- recursive=True
```

The command to read data *from* the storage container is nearly the same, but with the filepaths switched. To read data from the storage container, the command has the form:

```
>> azcopy copy "https://{storage_account_name}.blob.core.windows.net/{storage_container_name}/path/to/copy/{sas_token}"  
"<local path to copy to>" -- recursive=True
```

The passed argument `--recursive=True` is unnecessary if you are only reading or writing one file.

The storage account name and storage container name you already have. Remember that we made a storage container *inside* the storage account! To get the SAS token for the storage container, check out the next slide...

seismiccloud | Shared access tokens

- Container
- Search
- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Settings
 - Shared access tokens
 - Access policy
 - Properties
 - Metadata

Signing method
 Account key User delegation key

Signing key
 Key 1

Stored access policy
 None

Permissions *
 4 selected

Start and expiry date/time

Start
 01/20/2023 3:16:44 PM
 (UTC-08:00) Pacific Time (US & Canada)

Expiry
 03/15/2023 11:16:44 PM
 (UTC-08:00) Pacific Time (US & Canada)

Allowed IP addresses
 10.19.253.40

1. Click on the storage container you just created.

3. Select the permissions appropriate for what you'll want to do. **Most commonly, read and write.**

4. Specify how long you'll want this token (like a password) to last for you.

5. Input the IP address you plan to access the storage container from. (Note: you can also leave this blank. **But, make sure that the IP address you will use is allowed under /Networking in the Storage account settings.**)

2. Navigate to "Shared access tokens" on the sidebar.

6. Generate the token. This is used in the azcopy command, and you should save and keep in a safe place.

Common problems when trying to write data to the storage container using azcopy...

- Copy and pasting the azcopy command (quotation marks get screwed up).
- Make sure you specified the correct permissions when generating the SAS token: Read AND Write!
- “Description=This request is not authorized to perform this operation.”
 - Permission / authentication errors- in this case you want to check on the storage **account** under “Networking” and make sure the IP address you are trying to read/write from is allowed. Make sure to “save” your changes here!
 - The command “>> curl ifconfig.me” will print your current public IP address.

5. Get storage account
name and key

Navigate to your storage account

Microsoft Azure Search resources, services, and docs (G+)

Home > seismiccloud2

seismiccloud2 | Access keys

Storage account

Search

Events

Storage browser

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking
- Access keys**
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

Set rotation reminder Refresh Give feedback

Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

Remember to update the keys with any Azure resources and apps that use this storage account. [Learn more about managing storage account access keys](#)

Storage account name

seismiccloud2

key1 Rotate key

Last rotated: 2/3/2023 (103 days ago)

Key

..... Show

Connection string

..... Show

key2 Rotate key

Last rotated: 2/3/2023 (103 days ago)

Key

.....

zkrauss@uw.edu UW (CLOUD.WASHINGTON.EDU)

Scroll down to Security & Networking, and click on "Access keys"

Your **storage account name** is here

And your **storage account key** is here. Copy it and save it to a secure place.