Lab Manual- Setup and Manage Azure Storage with Blob

Prepared for:

Date: 18th Nov 2021

Prepared by:

Document Name: Lab Manual

Document Number AZLabn989

Contributor:

Contents

1. Introduction

The storage account is one of the fundamental pieces of cloud technology. It contains all of our Azure Storage data objects: blobs, files, queues, tables, and disks. Microsoft offers several options to store data on the cloud. Storage can be used for two purposes; one is for actually storing files just as we do on a hard disk. So it becomes where we put our backup files, where we put our database files. In addition, we can store our jpeg or videos in a storage account. The other is as the back end to a Virtual Machine. So actually, many services within Azure need a storage account, sometimes for logging and sometimes as a fundamental piece of the technology. By default, Virtual Machine is run on a managed storage account, which is an abstraction on top of a storage account. We cannot use it to create a Virtual Machine on top of an unmanaged account.

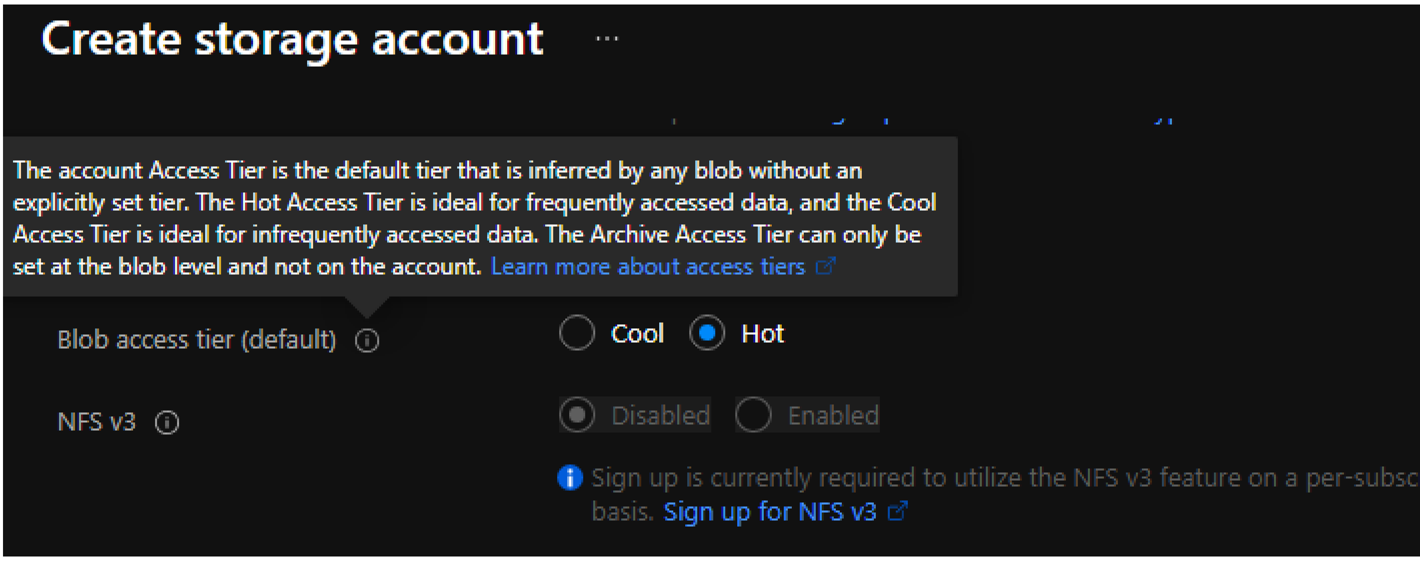
In this article, we will understand how to create an Azure blob storage account and upload a file on the blob.

There are various options available in the Azure Storage Account for storing user data.

2. Blob Storage

The word blob is an acronym, which stands for a binary large object. Blobs typically include large files that are unstructured, such as images, video, music files, backup files, etc.

Blob storage can be divided into two access tiers,



Create storage account ···

The account Access Tier is the default tier that is inferred by any blob without an explicitly set tier. The Hot Access Tier is ideal for frequently accessed data, and the Cool Access Tier is ideal for infrequently accessed data. The Archive Access Tier can only be set at the blob level and not on the account. Learn more about access tiers

Blob access tier (default) ⓘ ○ Cool ● Hot

NFS v3 ⓘ ● Disabled ○ Enabled

ⓘ Sign up is currently required to utilize the NFS v3 feature on a per-subsc basis. Sign up for NFS v3

Hot access tier

Those data, which are accessed frequently, will come under this tier. In addition, the hot storage tier is highly available compared to the cold access tier, like 99.9% as opposed to the 99% of the cold storage tier.

Cold access tier

In this tier, data that is not accessed very often will relay. In addition, the cold access tier is cheaper than the hot access tier and as such, you can store more data at a lower cost.

Note
We can switch between access tiers at any point if we wish to do so.

File Storage

With the help of Azure Files, we can set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol. That means that multiple VMs can share the same files with both read and write access. We can also read the files using the REST interface or the storage client libraries.

There are multiple common scenarios where Azure File storage is very useful,

1. Store configuration files on a file share and access from multiple VMs.

2. We can keep resource logs, metrics, and crash dumps on a file share and later can be processed or used for analysis.

Queue Storage

Queue Storage is somewhat like MSMQ. It allows us to decouple our components and have reliable asynchronous communication. In Azure Queue Storage, the number of queues is only limited by the capacity of the storage account. The Azure Queue service is used to store and retrieve messages. Queues and messages can be created programmatically or using the Storage Explorer tool.

Table Storage

Table storage is used to store semi-structured data in a key-value format in a NoSQL datastore. Azure table storage can store petabytes of data, can scale, and is inexpensive. Table storage can be accessed using REST and some of the OData protocols or using the Storage Explorer tool. Azure Table storage is now part of Azure Cosmos DB.

Disk

An Azure managed disk is a virtual hard disk (VHD). It is like a physical disk in an on-premises server but virtualized. Azure-managed disks are stored as page blobs, which are random IO storage objects in Azure. We call a managed disk 'managed' because it is an abstraction over page blobs, blob containers, and Azure storage accounts.

Azure offers two types of disk storage,

1. ***Managed* -** Managed disk has some advantages over unmanaged disks in the sense that disks will be created and managed for us. This is an IaaS offering.
2. ***Unmanaged*** - With unmanaged disks, we must manage them our self. This means, our virtual hard disks are stored in a storage account as page blobs.

Moreover, Azure offers two types of disks,

1. ***Premium* -** Which means our data will be placed on solid-state disks
2. ***Standard*** - Where data is placed on regular hard disk drives

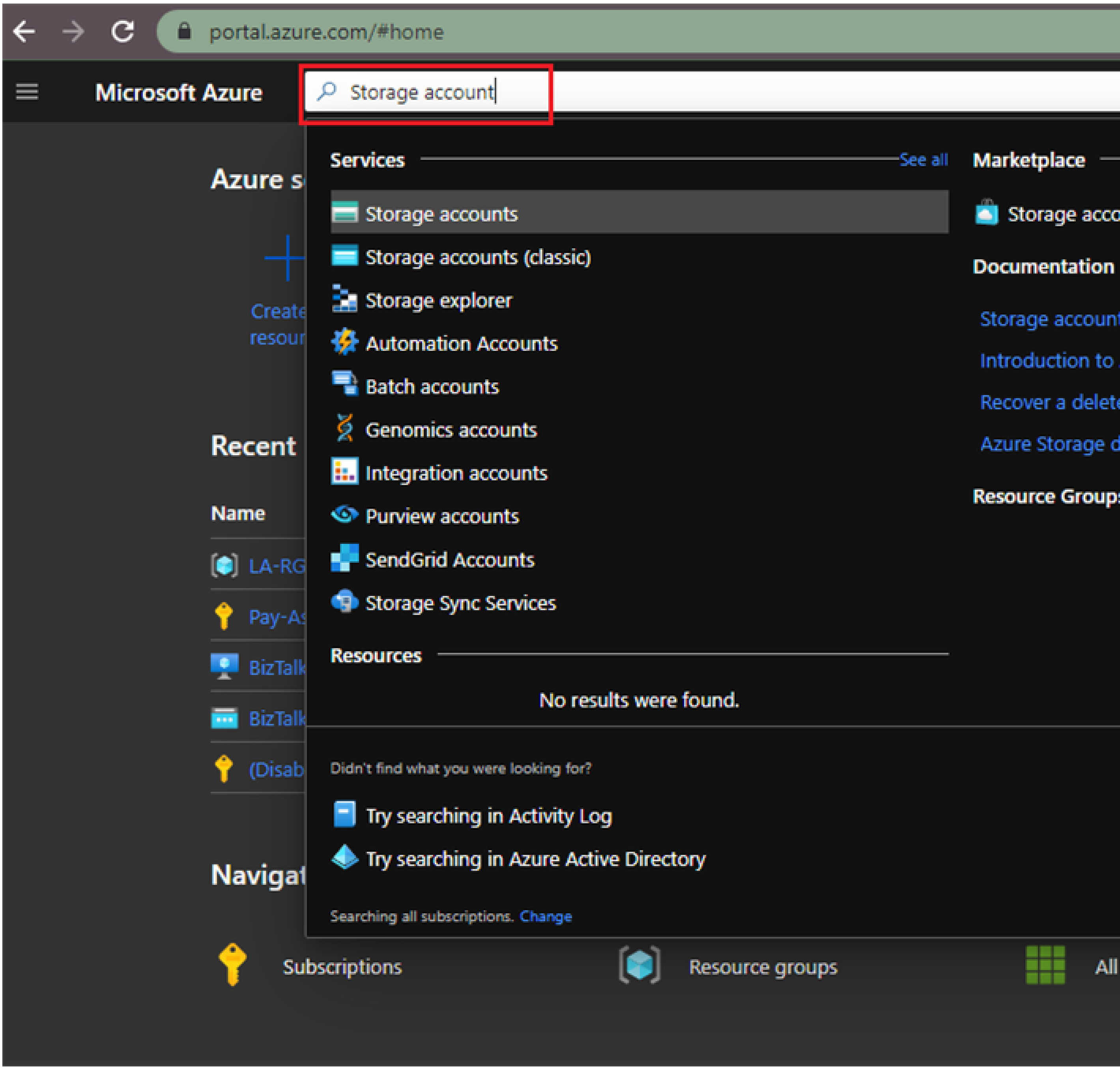
3. Lab: Creating my First Azure Storage Account

There are multiple ways to create a storage account,

1. Azure portal
2. Azure PowerShell
3. Azure CLI
4. Azure Resource Manager (ARM) Template

In this article, we will use the first option i.e. using the Azure portal. For other options, we will understand in different articles.

- Log in to the Azure portal ➜ Search Storage Accounts ➜ then select Storage accounts from the search result



portal.azure.com/#home

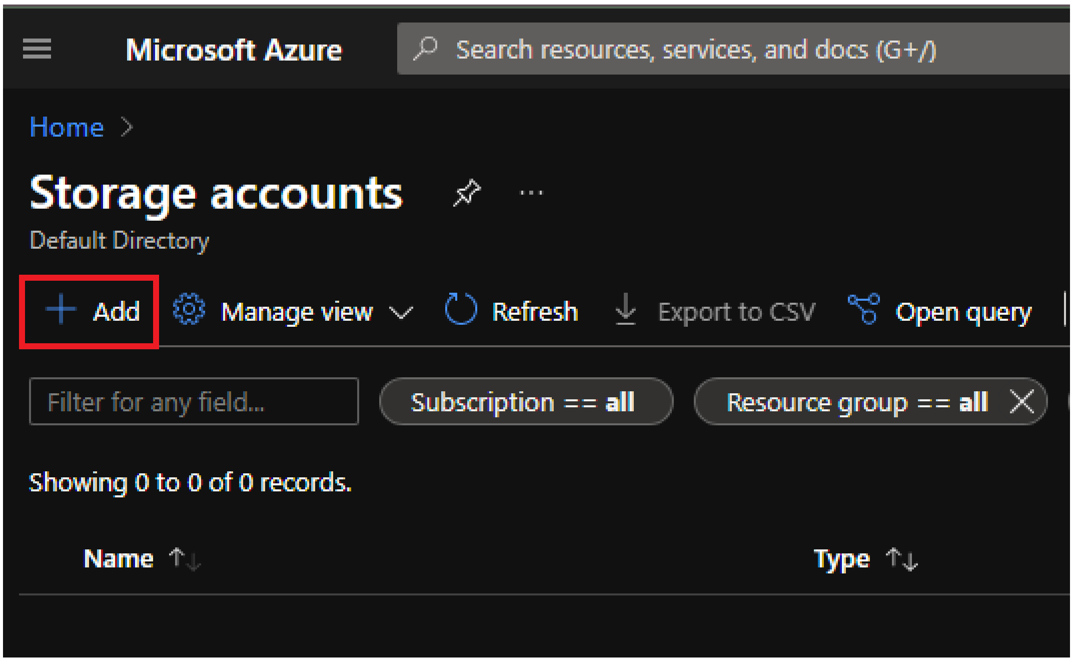
Storage account

No results were found.

Didn't find what you were looking for?

Searching all subscriptions. Change

- It will open a Storage account, now we have to click on Add,

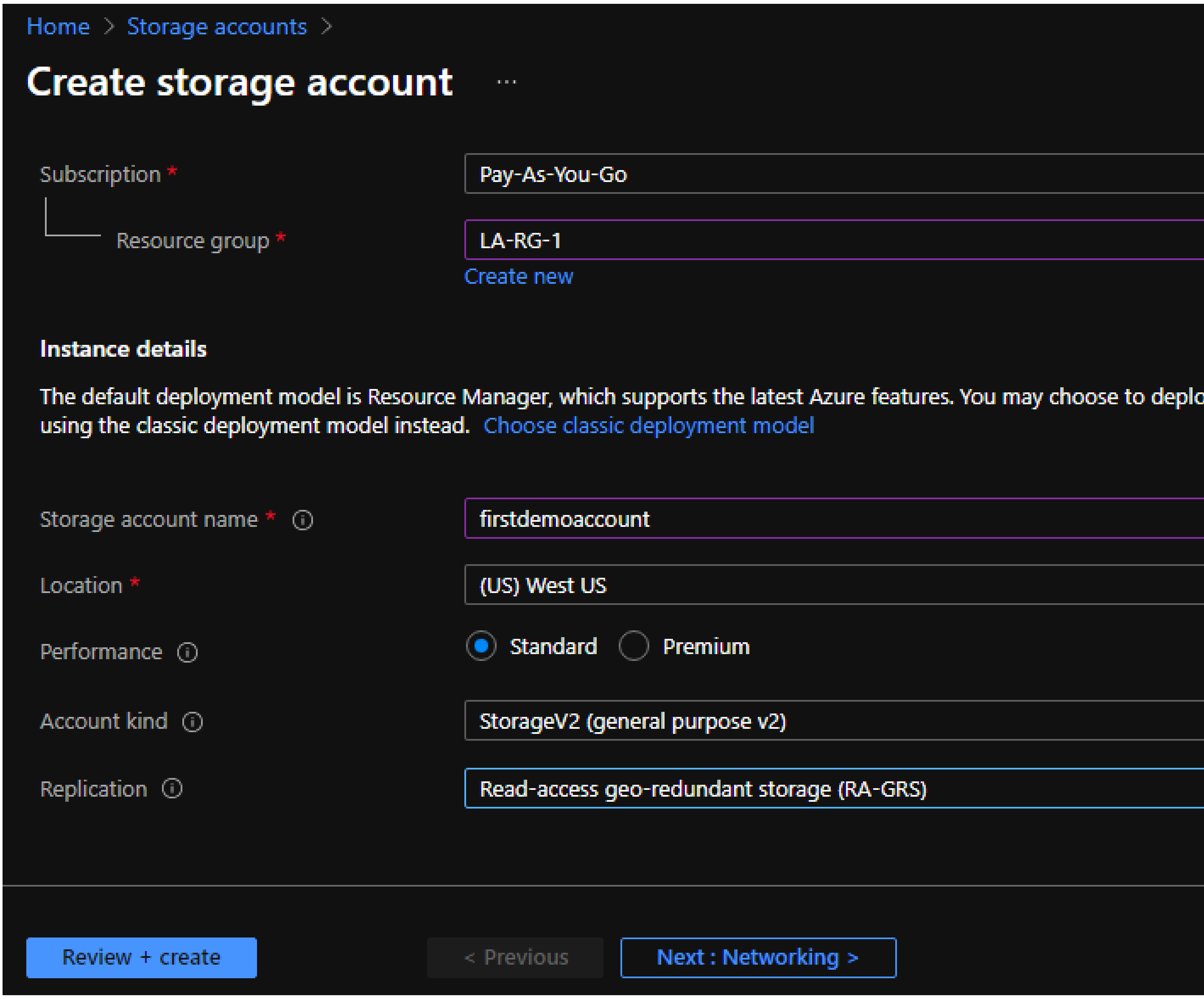


Showing 0 to 0 of 0 records.

Now we have to fill in the mandatory details under the Basic section, like,

1. Select the Subscription from the dropdown.
2. Choose the Resource Group under which this storage account will be created.
3. Provide the Storage account name, it should be unique across Azure and the length must be between 3 and 24 characters. Also, it may include only numbers and lowercase letters.
4. Select the location of the Storage account or use the default location.
5. Select a performance tier. The default tier is Standard.
6. Set the Account kind field to Storage V2 (general-purpose v2).
7. Select replication value, the default replication option is Read-access geo-redundant storage (RA-GRS). It will specify how the storage account will be replicated.

After entering all the values, it will look like below. If you want to keep the default values for the next section then click on '*Review + create*', otherwise click on '*Next: Networking >*'



Create storage account ···

Subscription * Pay-As-You-Go

Resource group * LA-RG-1

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deplo using the classic deployment model instead. Choose classic deployment model

Storage account name * ⓘ firstdemoaccount

Location * (US) West US

Performance ⓘ ● Standard ○ Premium

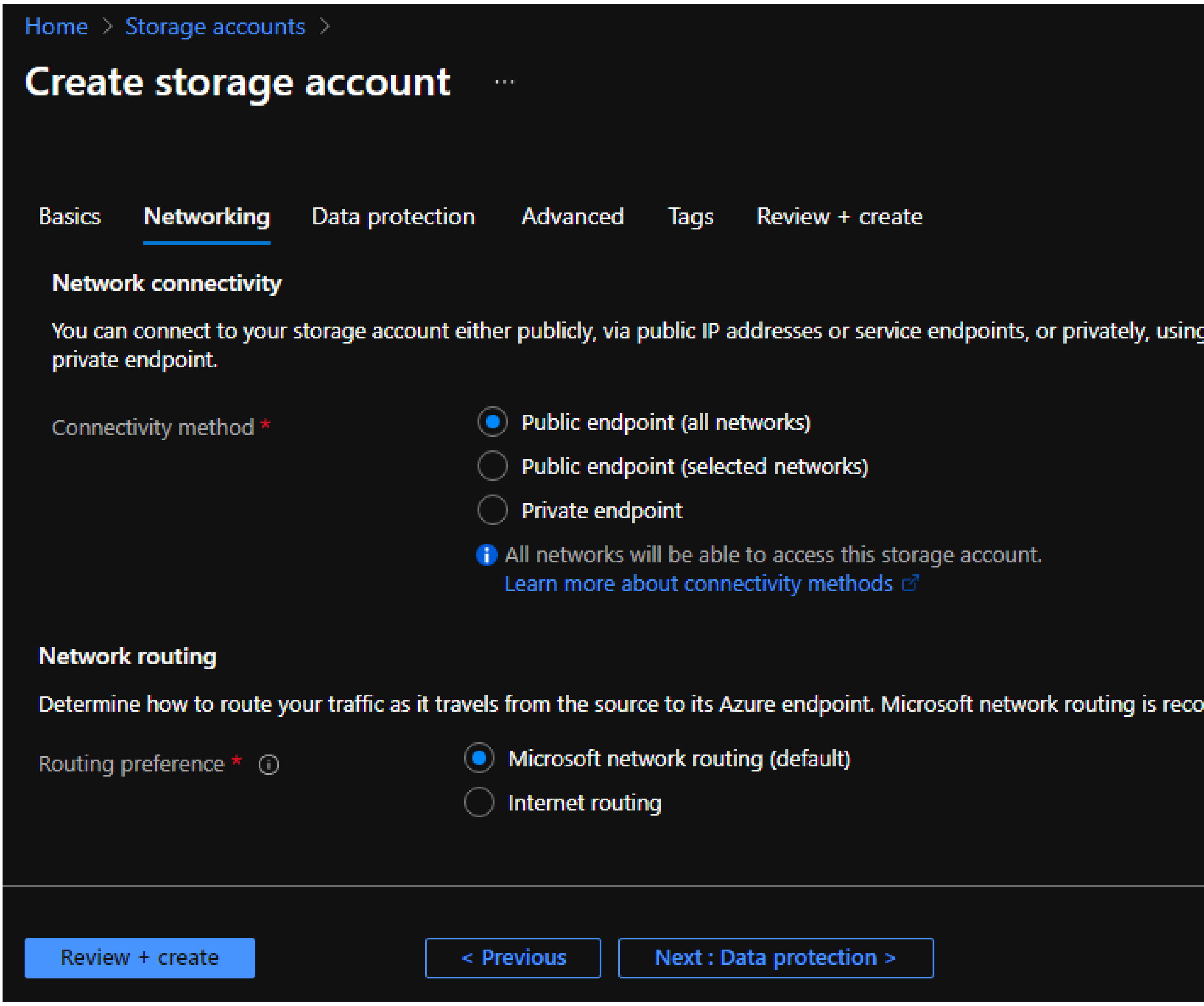
Account kind ⓘ StorageV2 (general purpose v2)

Replication ⓘ Read-access geo-redundant storage (RA-GRS)

- Now we are in the networking section, and here we can change the configuration about Network connectivity and Network routing.

In our case, we will keep the default as it is and not going to change any configuration.

For additional options, we will click on '*Next: Data protection* >'.



Network connectivity

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

Connectivity method *

● Public endpoint (all networks)
○ Public endpoint (selected networks)
○ Private endpoint

All networks will be able to access this storage account.
Learn more about connectivity methods

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is reco

Routing preference *

● Microsoft network routing (default)
○ Internet routing

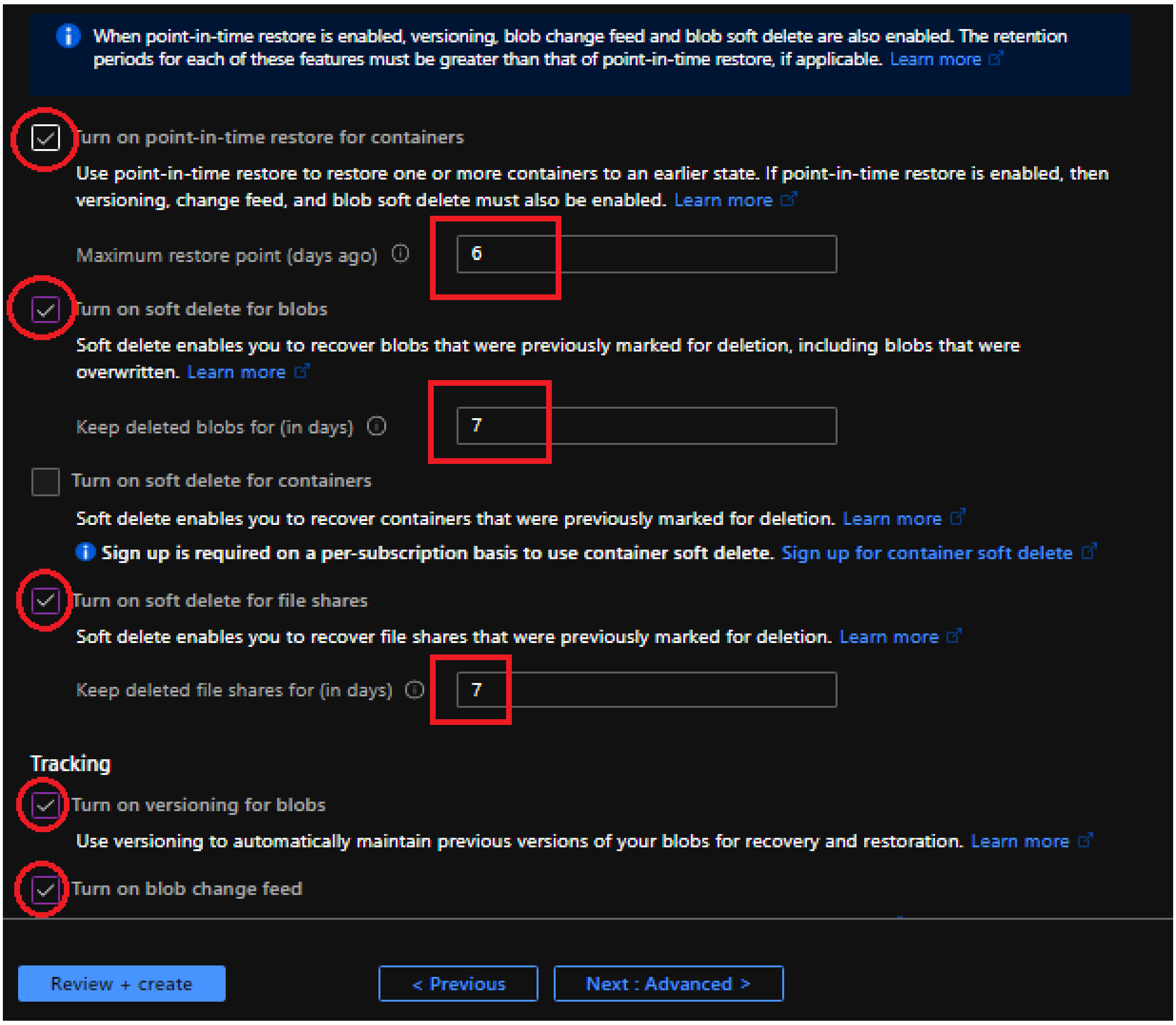
- In the Data protection section, we can define multiple configurations like if want to turn on point-in-time restoration for containers. With help of this configuration, we can restore one or more containers to an earlier state. We have to keep in mind one point here if we are going to enable this '*Point-in-time restore*' configuration, then versioning, change feed and blob soft delete must be enabled. The maximum restore point can be 6 days ago.

Next configuration, *Turn on soft delete for blobs*. With this configuration, we can recover blobs that were previously marked for deletion. Here we can define the number of days to keep deleted blobs.

Similarly, we have other configurations like,

1. Turn on soft delete for containers
2. Turn on soft delete for file shares
3. Turn on versioning for blobs
4. Turn on blob change feed

If you change these setting then it will look like below.



When point-in-time restore is enabled, versioning, blob change feed and blob soft delete are also enabled. The retention periods for each of these features must be greater than that of point-in-time restore, if applicable. Learn more

☑ Turn on 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

Maximum restore point (days ago): 6

☑ Turn on soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

Keep deleted blobs for (in days): 7

□ Turn on soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. Learn more

Sign up is required on a per-subscription basis to use container soft delete. Sign up for container soft delete

☑ Turn on soft delete for file shares

Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Keep deleted file shares for (in days): 7

Tracking

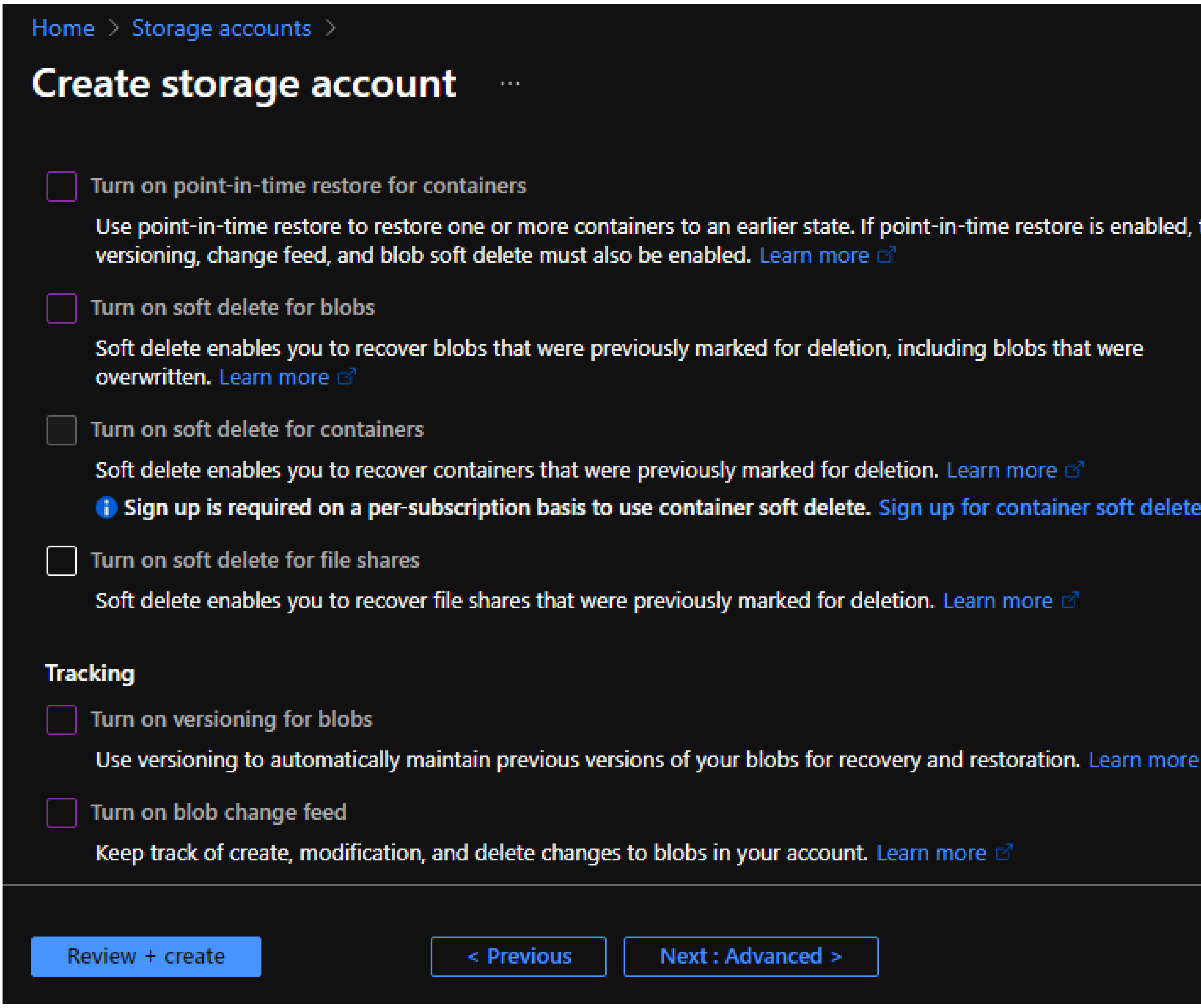
☑ Turn on versioning for blobs

Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. Learn more

☑ Turn on blob change feed

For our scenario, we will keep it as default and not going to change any configuration.

For additional options, we will click on '*Next: Advanced* >'.



Create storage account ...

☐ Turn on 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, versioning, change feed, and blob soft delete must also be enabled. Learn more

☐ Turn on soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more

☐ Turn on soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. Learn more

Sign up is required on a per-subscription basis to use container soft delete. Sign up for container soft delete

☐ Turn on soft delete for file shares

Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Tracking

☐ Turn on versioning for blobs

Use versioning to automatically maintain previous versions of your blobs for recovery and restoration. Learn more

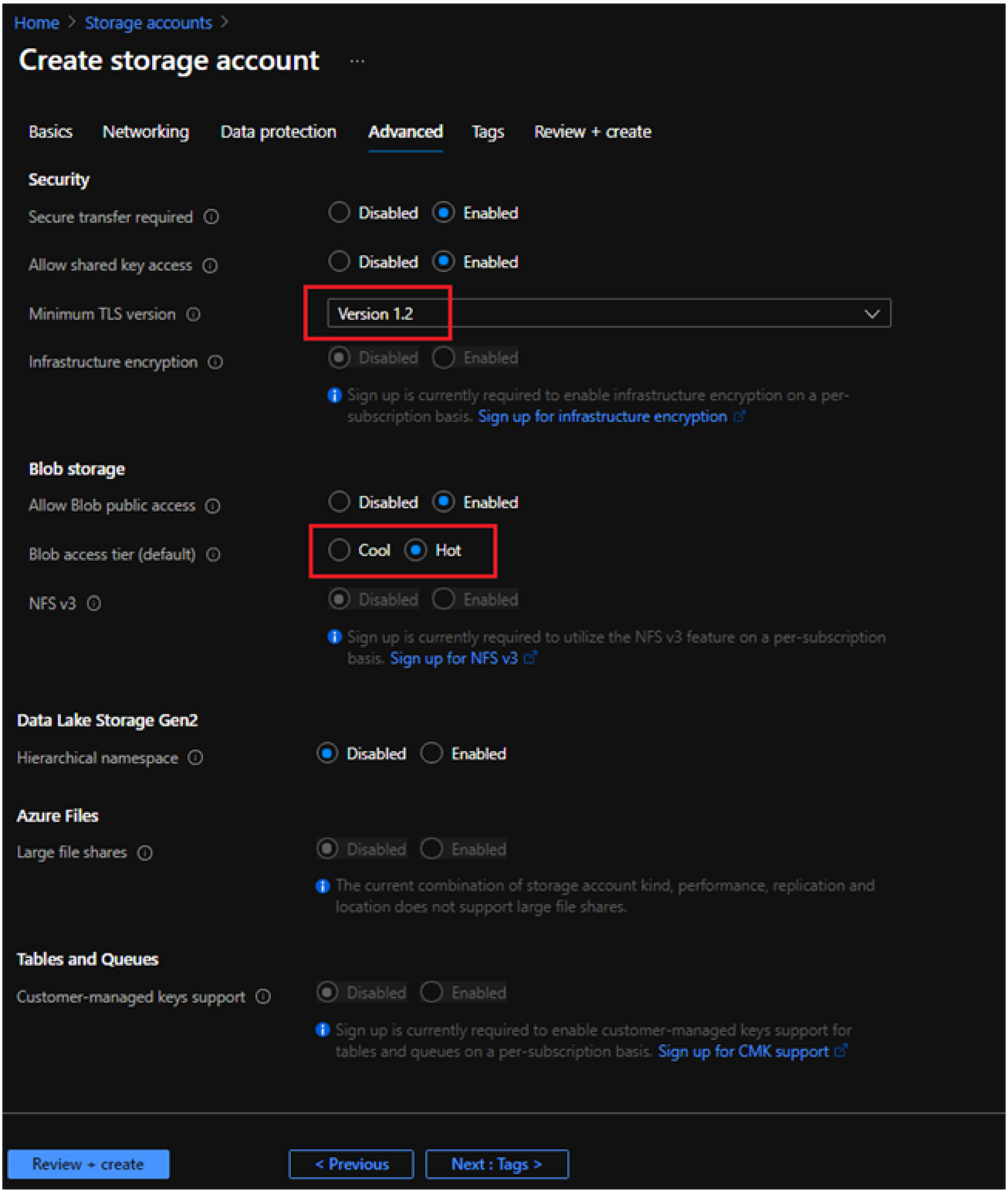
☐ Turn on blob change feed

Keep track of create, modification, and delete changes to blobs in your account. Learn more

- In the Advanced section, we can define the Security, Blob storage, Data Lake Storage Gen2, Azure Files & Table, and Queues configuration.

Please check the configuration in the below image, for our scenario I am keeping the default values.

The next option is Tags; we will bypass this section because here you can just define the tags and their values. Now we will click on '*Review + create*'.



Home > Storage accounts >

Create storage account ...

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

Security

Secure transfer required ⓘ ○ Disabled ● Enabled

Allow shared key access ⓘ ○ Disabled ● Enabled

Minimum TLS version ⓘ Version 1.2

Infrastructure encryption ⓘ ● Disabled ○ Enabled

Sign up is currently required to enable infrastructure encryption on a per-subscription basis. Sign up for infrastructure encryption

Blob storage

Allow Blob public access ⓘ ○ Disabled ● Enabled

Blob access tier (default) ⓘ ○ Cool ● Hot

NFS v3 ⓘ ● Disabled ○ Enabled

Sign up is currently required to utilize the NFS v3 feature on a per-subscription basis. Sign up for NFS v3

Data Lake Storage Gen2

Hierarchical namespace ⓘ ● Disabled ○ Enabled

Azure Files

Large file shares ⓘ ● Disabled ○ Enabled

The current combination of storage account kind, performance, replication and location does not support large file shares.

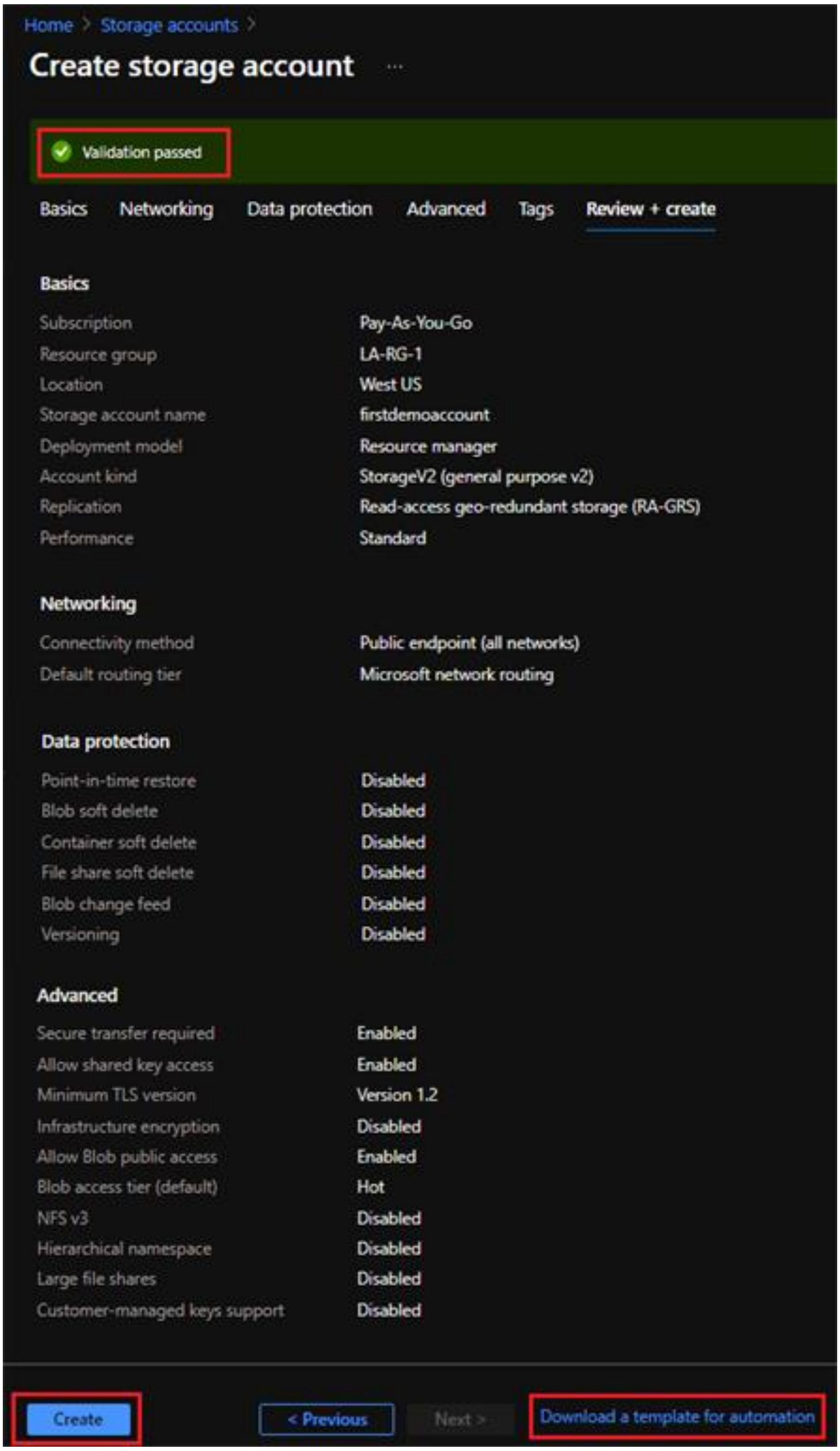
Tables and Queues

Customer-managed keys support ⓘ ● Disabled ○ Enabled

Sign up is currently required to enable customer-managed keys support for tables and queues on a per-subscription basis. Sign up for CMK support

- Once we click on '*Review + Create*', it will review your storage account settings and give the result of the review. In case all configurations are properly defined, we will get the message "Validation Passed". In addition 'Create' button will appear. Clicking on that button will create the Storage account. In case of validation failed then it will give you the reason why and how to fix that issue.

Here, we will get a link to download a template that we can use for automation.



Create storage account

Basics

Subscription	Pay-As-You-Go
Resource group	LA-RG-1
Location	West US
Storage account name	firstdemoaccount
Deployment model	Resource manager
Account kind	StorageV2 (general purpose v2)
Replication	Read-access geo-redundant storage (RA-GRS)
Performance	Standard

Networking

Connectivity method	Public endpoint (all networks)
Default routing tier	Microsoft network routing

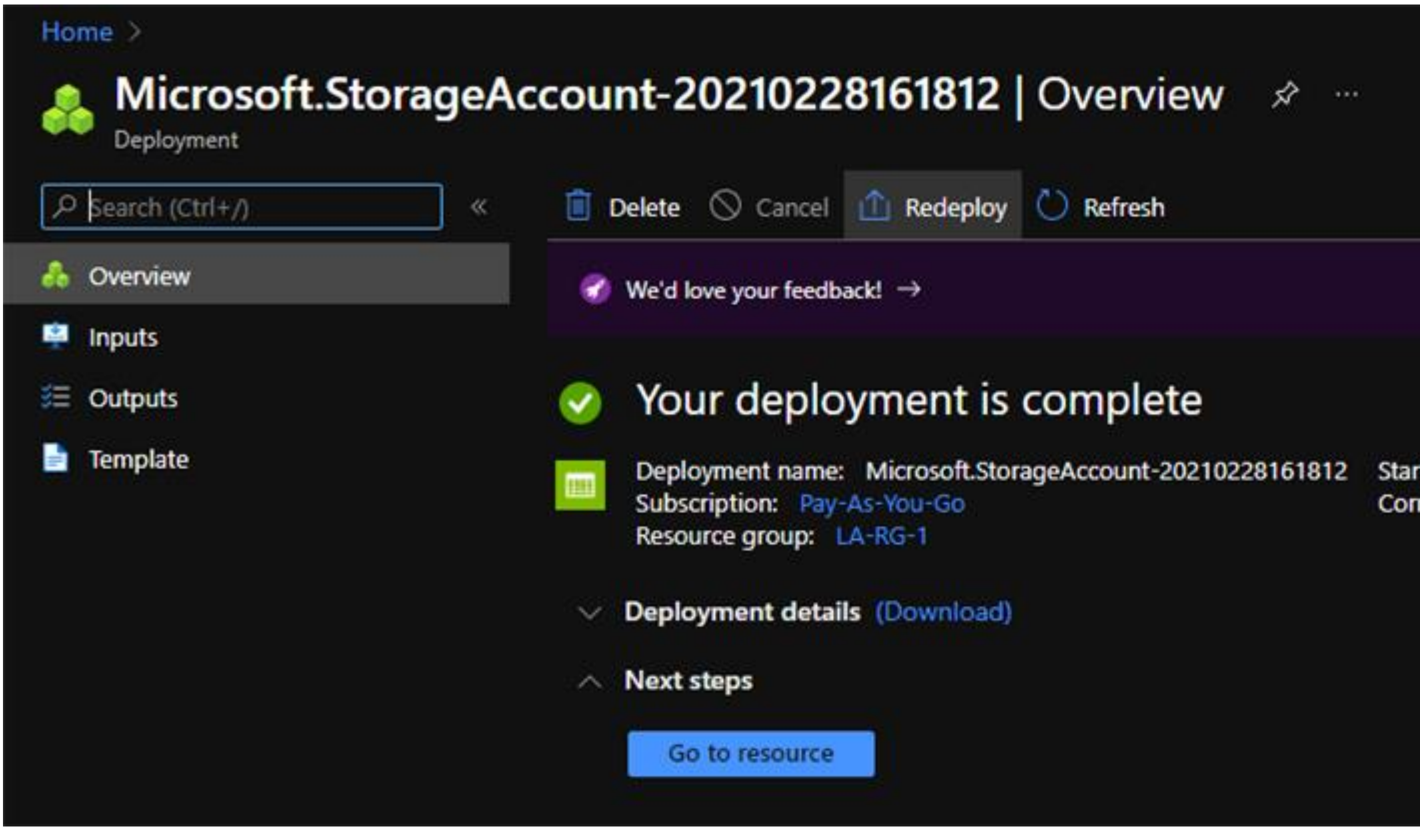
Data protection

Point-in-time restore	Disabled
Blob soft delete	Disabled
Container soft delete	Disabled
File share soft delete	Disabled
Blob change feed	Disabled
Versioning	Disabled

Advanced

Secure transfer required	Enabled
Allow shared key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled
Allow Blob public access	Enabled
Blob access tier (default)	Hot
NFS v3	Disabled
Hierarchical namespace	Disabled
Large file shares	Disabled
Customer-managed keys support	Disabled

- It will take hardly a minute or two to complete the deployment. Once deployment completed below screen will come, then we can click on 'Go to resource'



Microsoft.StorageAccount-20210228161812 | Overview

Deployment

Your deployment is complete

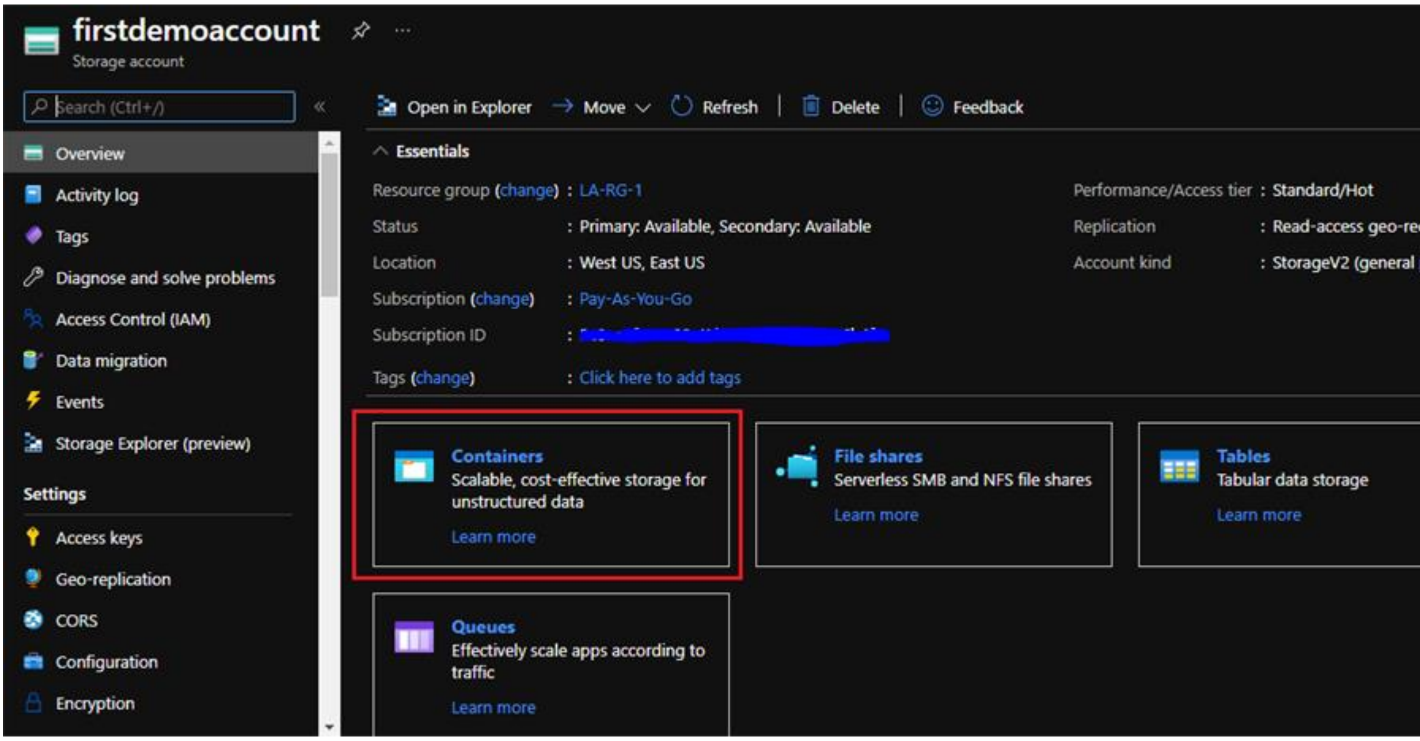
Deployment name: Microsoft.StorageAccount-20210228161812

Subscription: Pay-As-You-Go

Resource group: LA-RG-1

4. Lab: Creating Blob Container

- It will open our newly created Storage account. Once it opens then we have to create a container where we can upload the file. Click on '***Containers***' and it will open to create a new container,



firstdemoaccount

Storage account

Resource group (change) : LA-RG-1

Status : Primary: Available, Secondary: Available

Location : West US, East US

Subscription (change) : Pay-As-You-Go

Subscription ID : [redacted]

Tags (change) : Click here to add tags

Performance/Access tier : Standard/Hot

Replication : Read-access geo-re

Account kind : StorageV2 (general

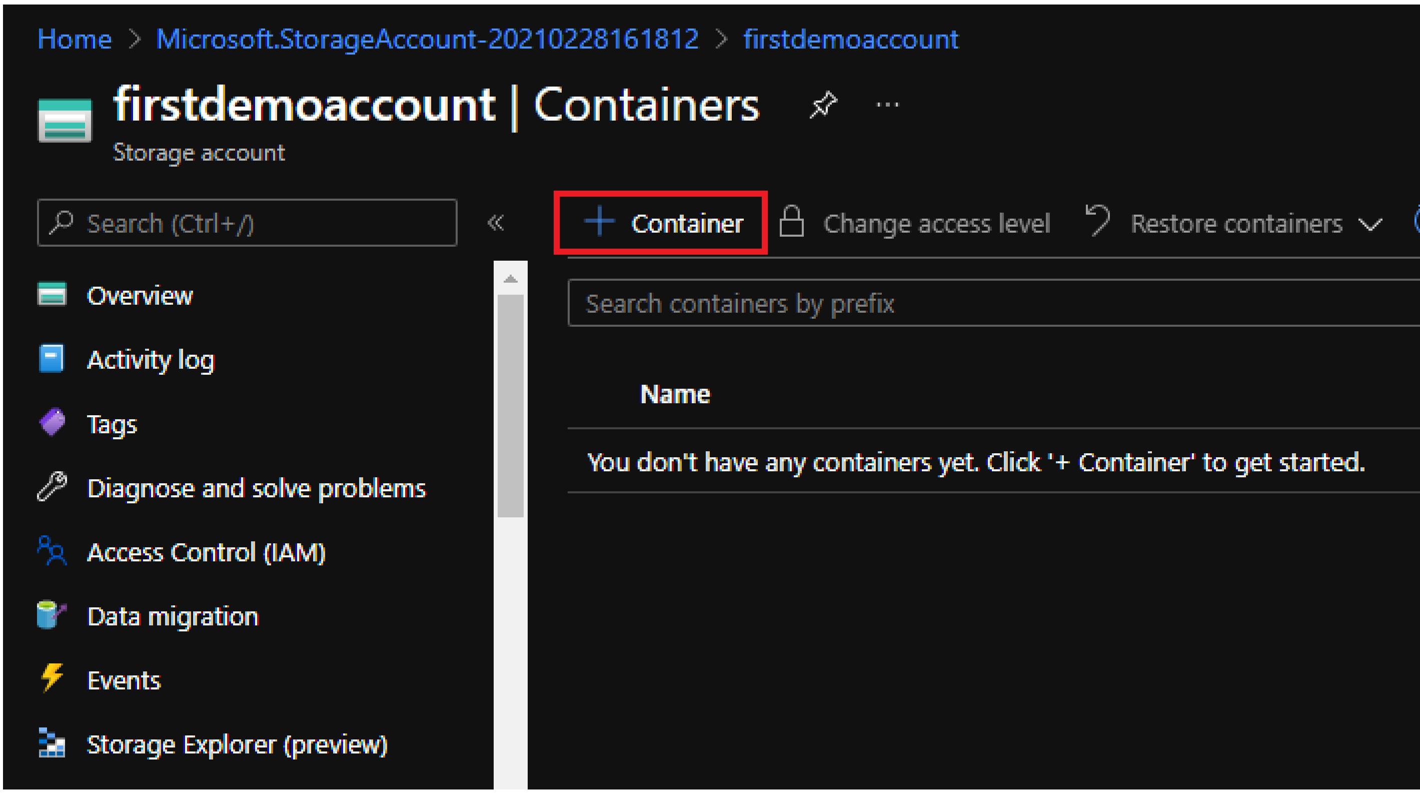
Containers — Scalable, cost-effective storage for unstructured data

File shares — Serverless SMB and NFS file shares

Tables — Tabular data storage

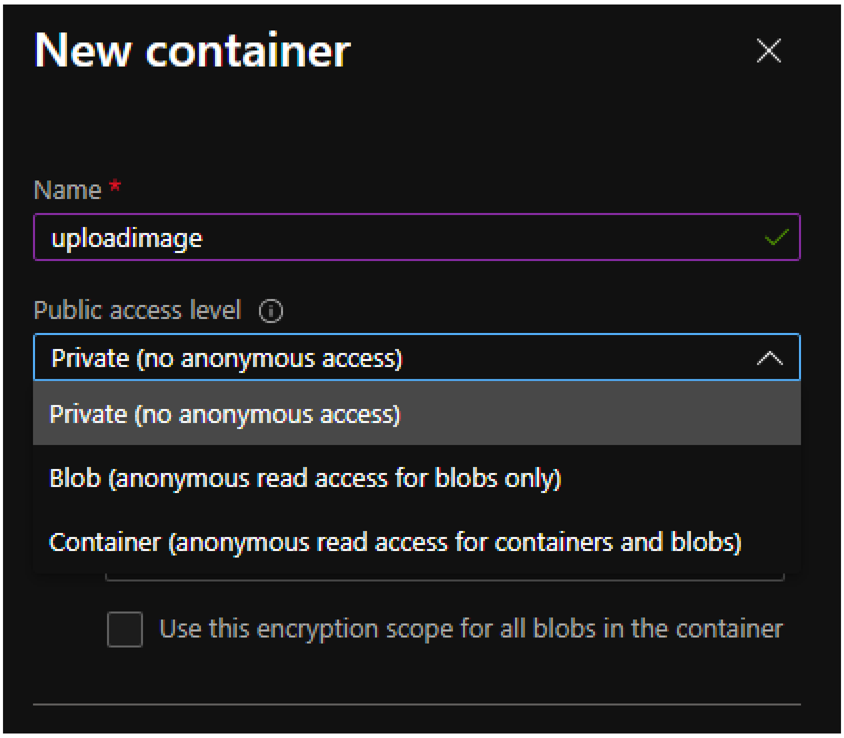
Queues — Effectively scale apps according to traffic

- Click on '+ *Container*' where we will upload the sample file.


Home > Microsoft.StorageAccount-20210228161812 > firstdemoaccount
firstdemoaccount | Containers
Storage account
Search (Ctrl+/)
Overview
Activity log
Tags
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage Explorer (preview)
+ Container
Change access level
Restore containers
Search containers by prefix
Name

You don't have any containers yet. Click '+ Container' to get started.

- Enter the name of the container and select the Public access level based on our need. For our scenario, we will keep this configuration as it is.

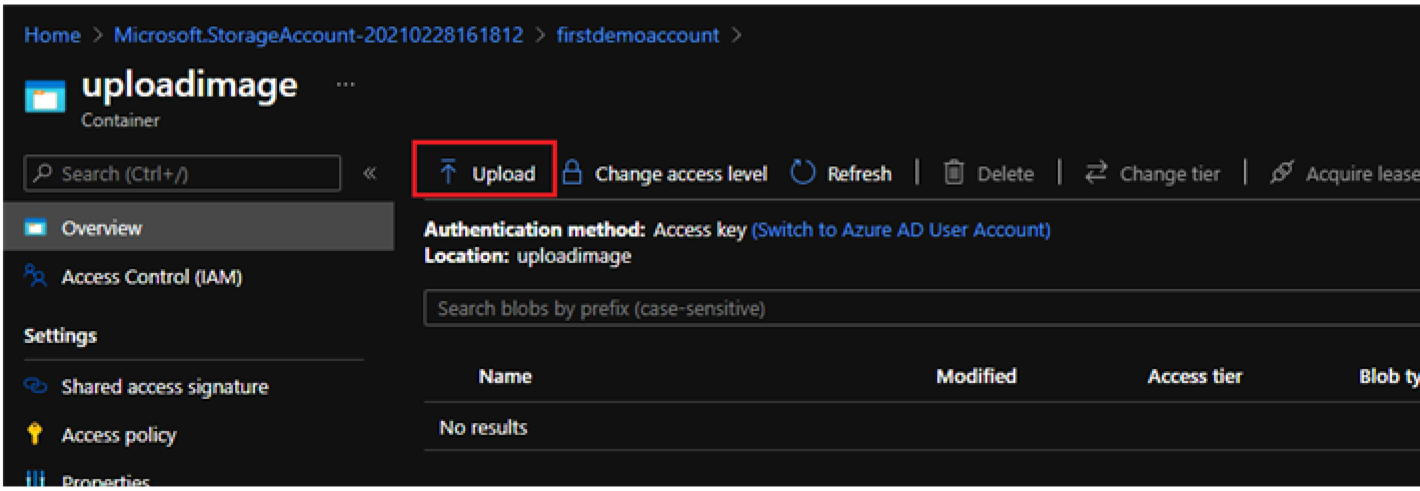

New container
Private (no anonymous access)
Blob (anonymous read access for blobs only)
Container (anonymous read access for containers and blobs)
□ Use this encryption scope for all blobs in the container

Name * uploadimage

Public access level: Private (no anonymous access)

5. Lab: Upload Blob (File)

- Click on **upload** and it will open a new panel where we will see a placeholder to select a file. In addition, we can see a checkbox that will be helpful to overwrite the already existing file.

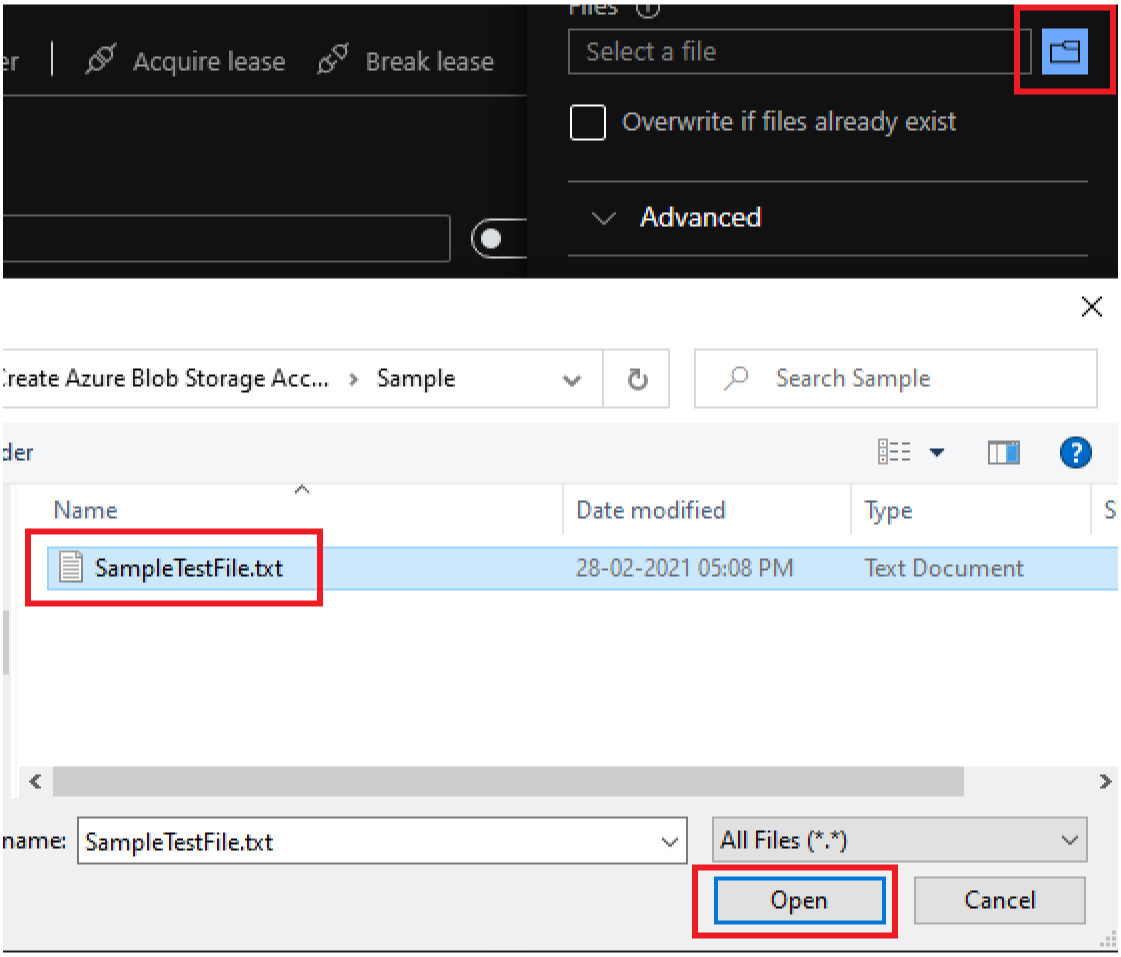


Authentication method: Access key (Switch to Azure AD User Account)
Location: uploadimage

Search blobs by prefix (case-sensitive)

Name	Modified	Access tier	Blob ty
No results			

- Now, click on the folder icon and it will open a pop-up to select the file from the folder. Select the file and click on open. Once it selected then click on 'Upload'.



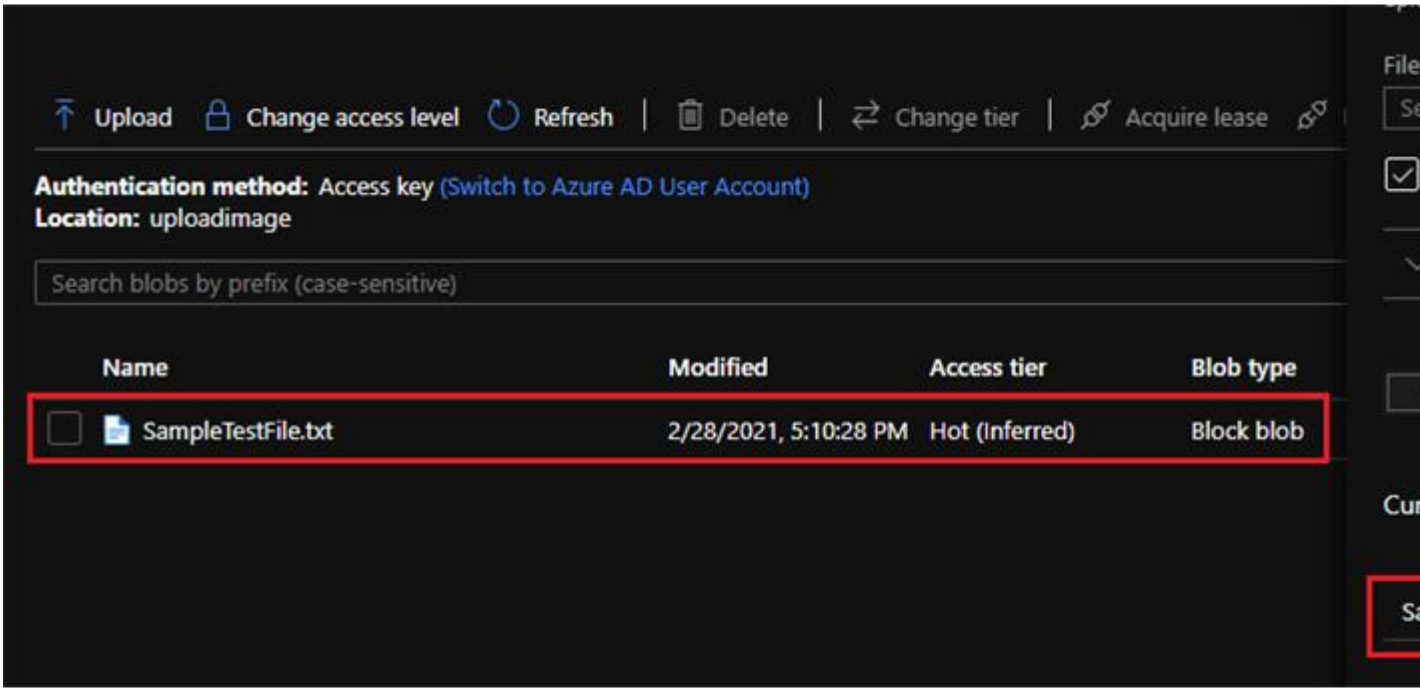
Name	Date modified	Type	S
SampleTestFile.txt	28-02-2021 05:08 PM	Text Document	

name: SampleTestFile.txt

All Files (*.*)

- Once the file uploaded successfully, we can see the file available in the container along with other details.

Please verify the below screen to check the status of the uploaded file on the container.



Authentication method: Access key (Switch to Azure AD User Account)
Location: uploadimage

Name	Modified	Access tier	Blob type
□ SampleTestFile.txt	2/28/2021, 5:10:28 PM	Hot (Inferred)	Block blob

6. Delete a storage account

Deleting a storage account deletes the entire account, including all data in the account, and cannot be undone.

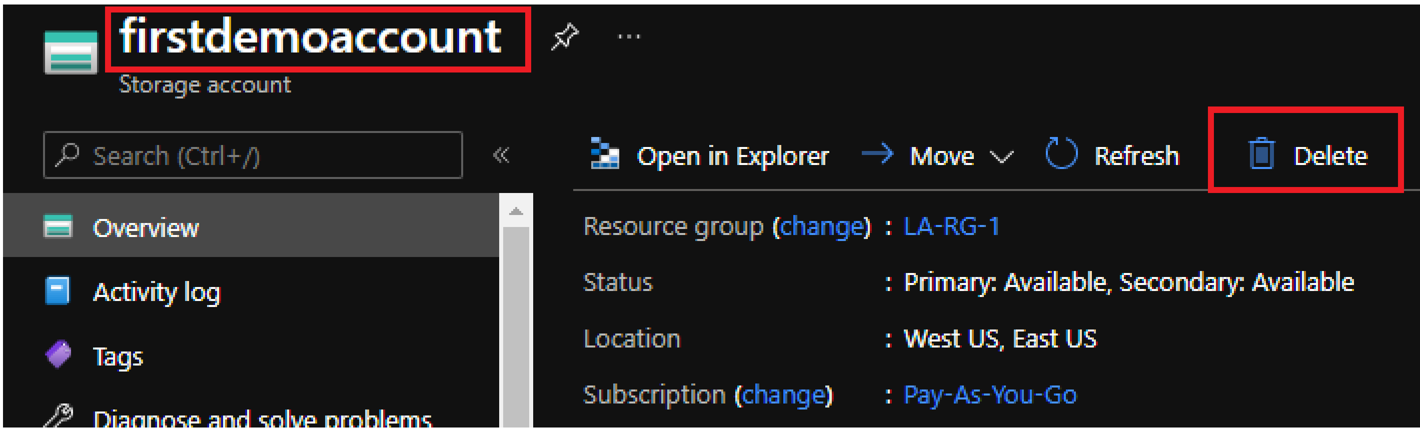
There are again multiple ways to delete the existing storage account

1. Azure portal
2. Azure PowerShell
3. Azure CLI
4. Azure Resource Manager (ARM) Template

In this article, we will use the first option i.e. using the Azure portal. For other options, we will understand in different articles.

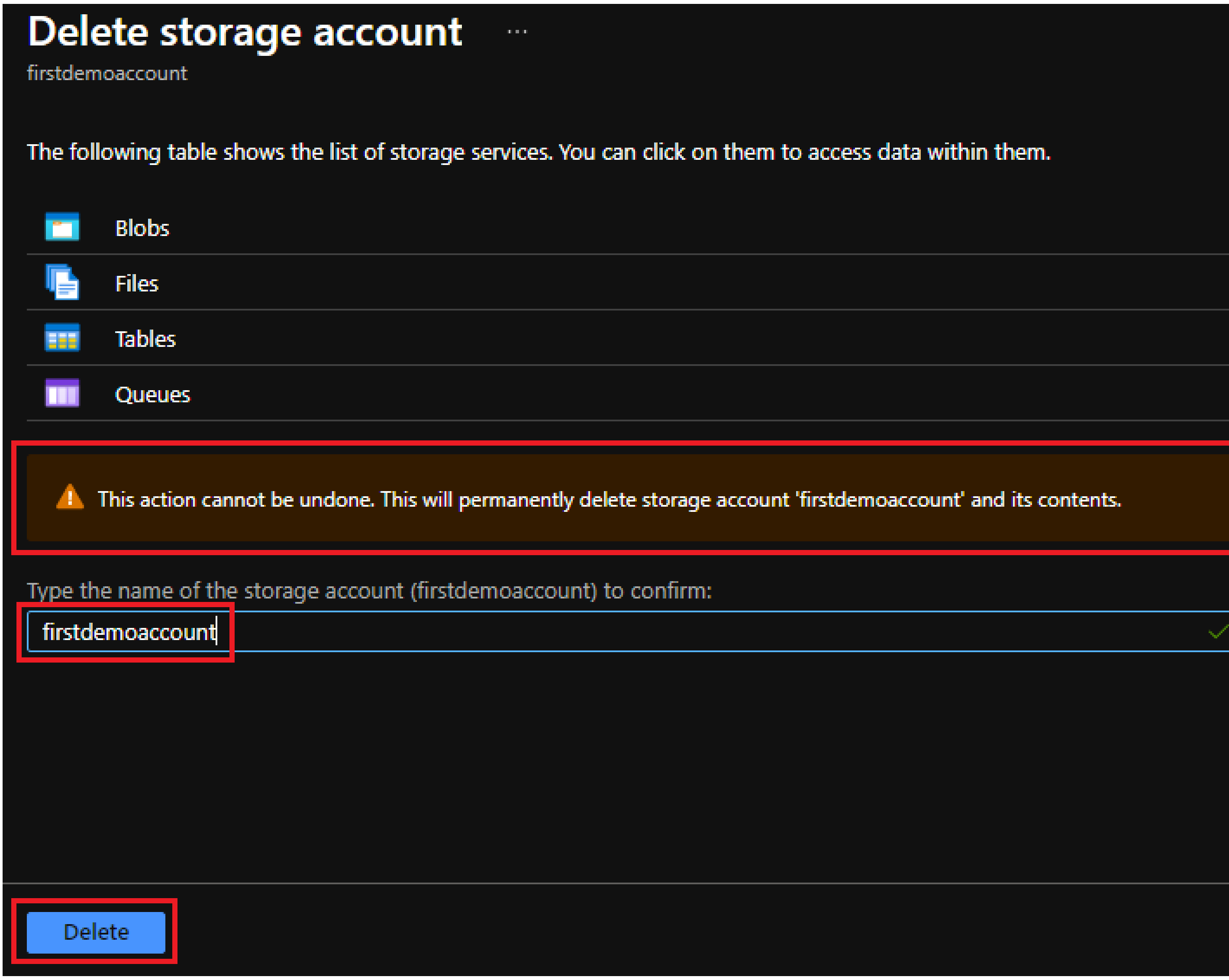
Log in to the Azure portal ➜ Search Storage Accounts ➜ then select Storage accounts, which want to delete

Once we open the storage account, we will have an option to delete it. Click on 'Delete'.



Resource group (change) : LA-RG-1
Status : Primary: Available, Secondary: Available
Location : West US, East US
Subscription (change) : Pay-As-You-Go

It will open the Delete storage account; here we have to type the name of the storage account to confirm. Then click on '*Delete*'.



Delete storage account

firstdemoaccount

The following table shows the list of storage services. You can click on them to access data within them.

This action cannot be undone. This will permanently delete storage account 'firstdemoaccount' and its contents.

Type the name of the storage account (firstdemoaccount) to confirm:

firstdemoaccount

Caution

This action cannot be undone. This will permanently delete the storage account and its contents.

7. Conclusion

There are several advantages to using Azure storage irrespective of type. Azure storage is easily scalable, extremely flexible, and relatively low in cost depending on the options we choose.