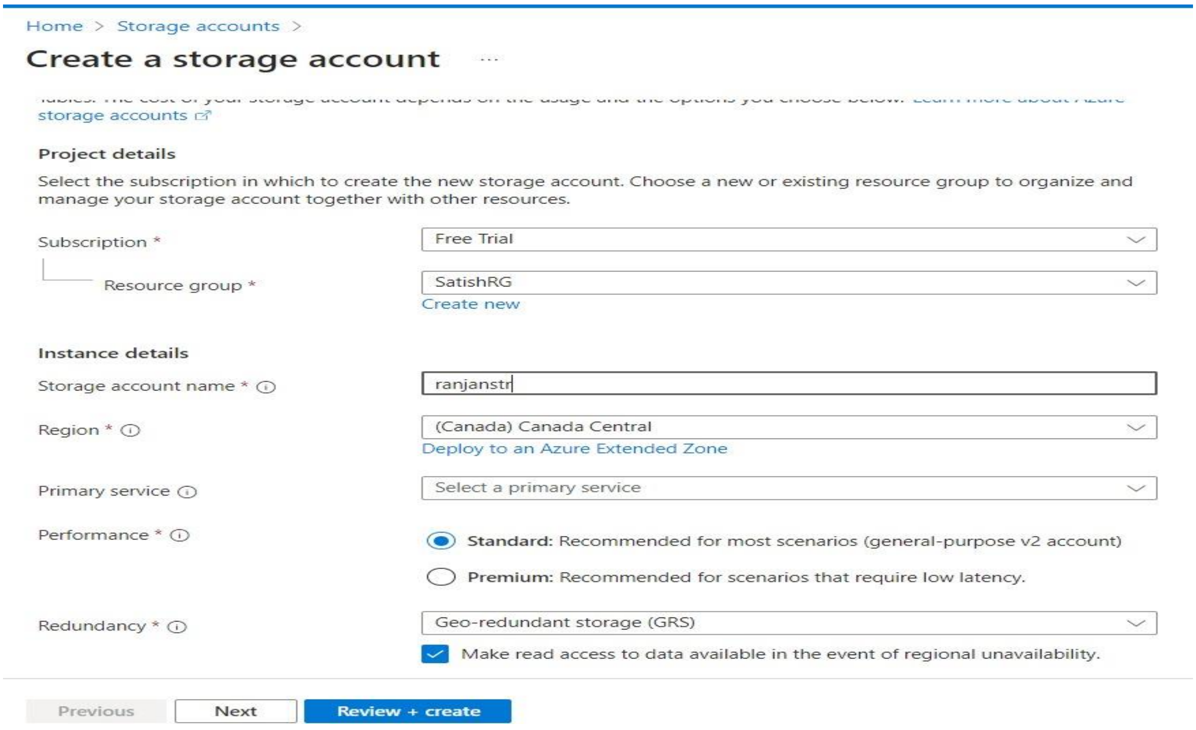
Azure Storage Steps

Steps to create Azure Storage Account with container:

Step1:   Need to create one Storage Account with enable Network access “Enable public access from all networks”



Home > Storage accounts >

Create a storage account ...

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 * : Free Trial

Resource group * : SatishRG

Create new

Instance details

Storage account name * ⓘ : ranjanstr

Region * ⓘ : (Canada) Canada Central

Deploy to an Azure Extended Zone

Primary service ⓘ : Select a primary service

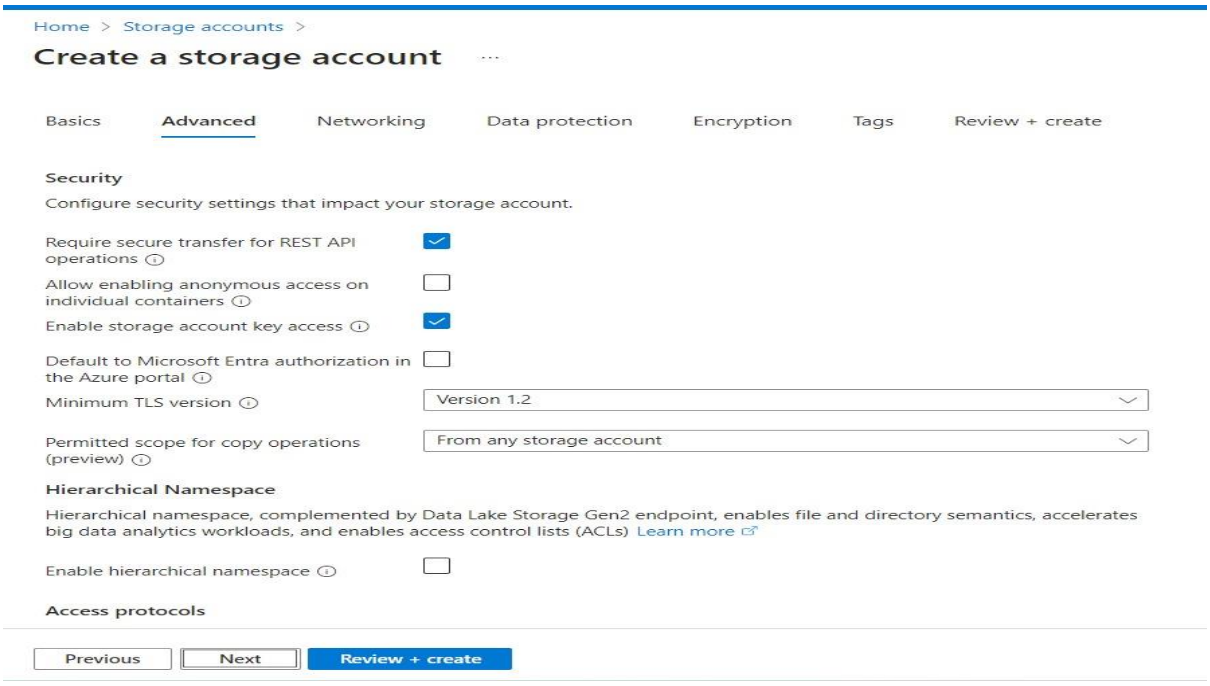
Performance * ⓘ :

● **Standard:** Recommended for most scenarios (general-purpose v2 account)

○ **Premium:** Recommended for scenarios that require low latency.

Redundancy * ⓘ : Geo-redundant storage (GRS)

☑ Make read access to data available in the event of regional unavailability.



Home > Storage accounts >

Create a storage account ...

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 ⓘ : Version 1.2

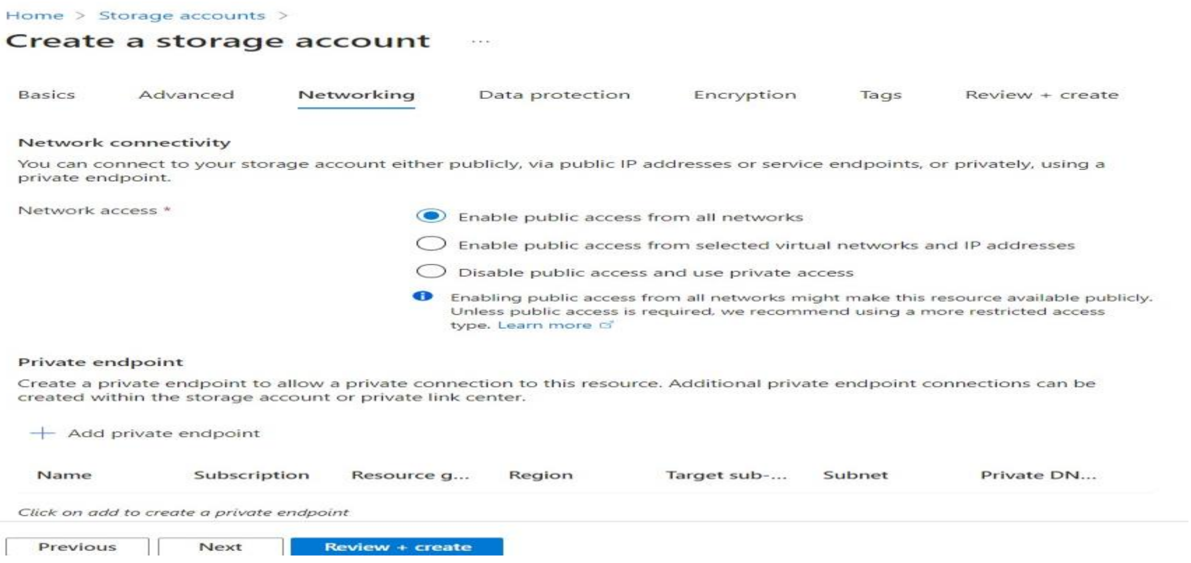
Permitted scope for copy operations (preview) ⓘ : From any storage account

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



Home > Storage accounts >

Create a storage account ···

Basics | Advanced | **Networking** | Data protection | Encryption | 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.

Network access *

● Enable public access from all networks

○ Enable public access from selected virtual networks and IP addresses

○ Disable public access and use private access

Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more

Private endpoint

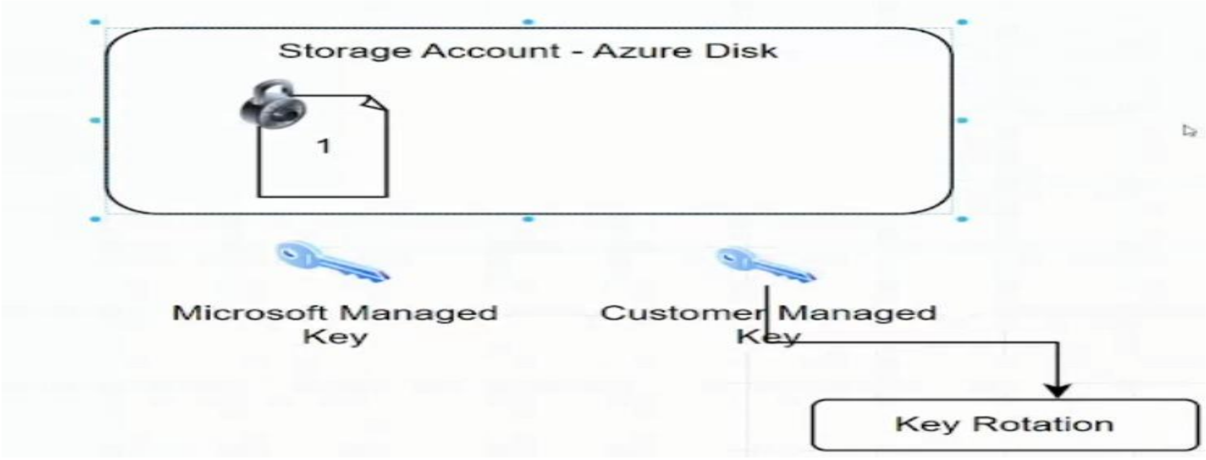
Create a private endpoint to allow a private connection to this resource. Additional private endpoint connections can be created within the storage account or private link center.

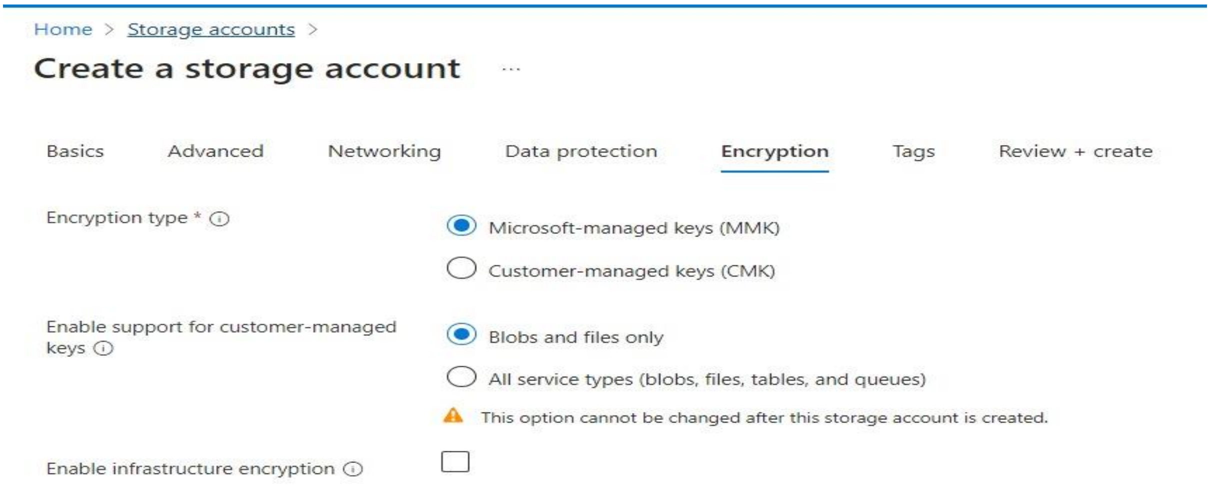
+ Add private endpoint

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

Click on add to create a private endpoint

There are two types of encrpytions keys in azure - One is MMK and CMK. CMK is more secure. For using CMK, A new key is created and stored in key vault and the storage account is given access to the key stored in the key vault using managed identities.





Home > Storage accounts >

Create a storage account ···

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

Encryption type * ⓘ

● Microsoft-managed keys (MMK)

○ Customer-managed keys (CMK)

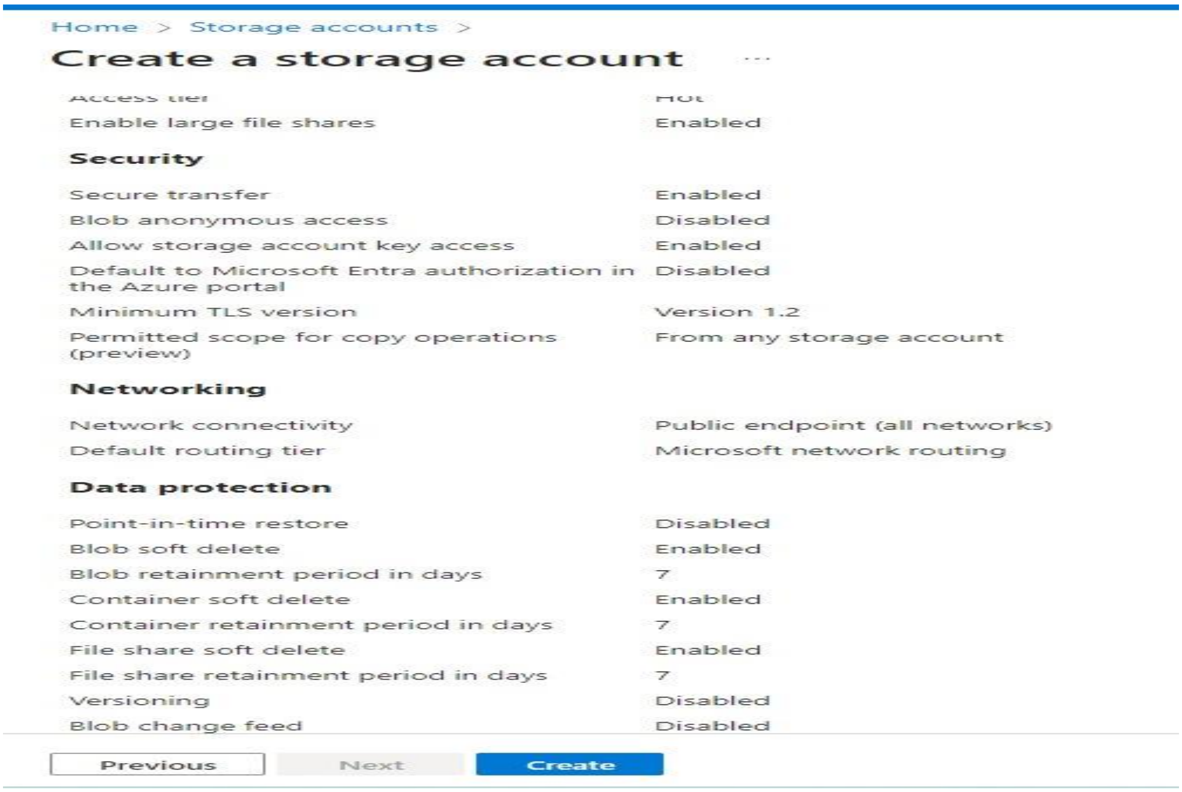
Enable support for customer-managed keys ⓘ

● Blobs and files only

○ All service types (blobs, files, tables, and queues)

⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ⓘ □



Create a storage account

Access tier	Hot
Enable large file shares	Enabled

Security

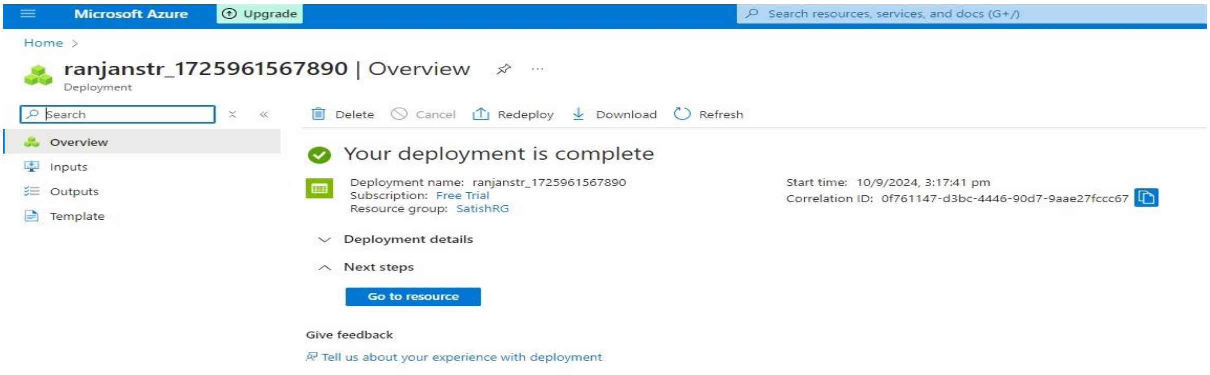
Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in the Azure portal	Disabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account

Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing

Data protection

Point-in-time restore	Disabled
Blob soft delete	Enabled
Blob retainment period in days	7
Container soft delete	Enabled
Container retainment period in days	7
File share soft delete	Enabled
File share retainment period in days	7
Versioning	Disabled
Blob change feed	Disabled



ranjanstr_1725961567890 | Overview

Deployment

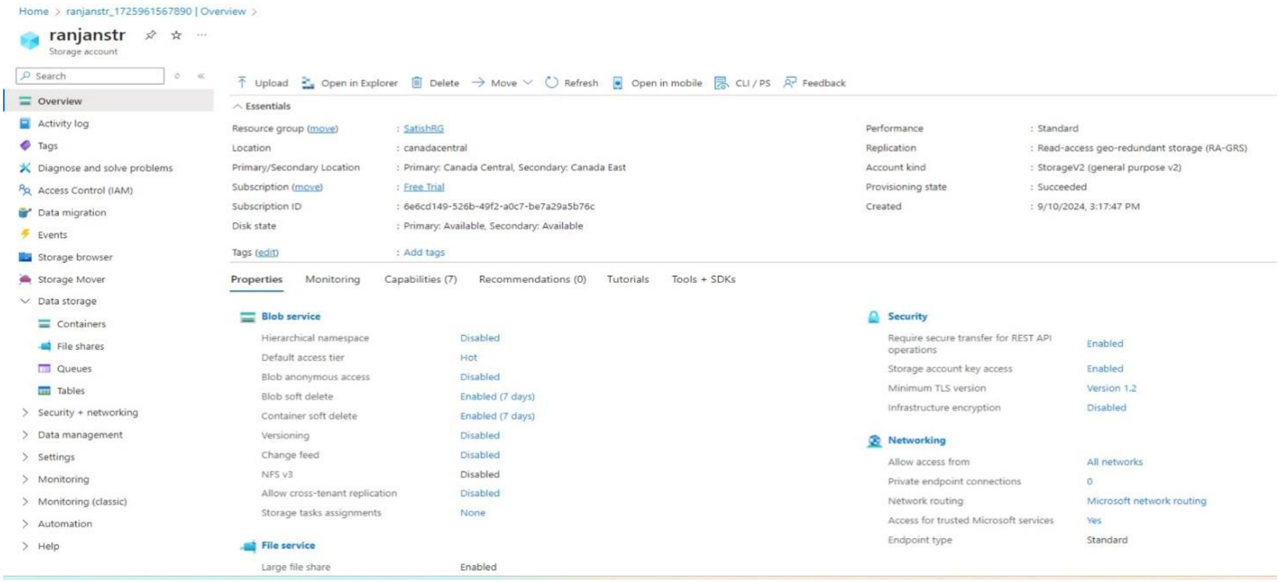
Your deployment is complete

Deployment name: ranjanstr_1725961567890
Subscription: Free Trial
Resource group: SatishRG

Start time: 10/9/2024, 3:17:41 pm
Correlation ID: 0f761147-d3bc-4446-90d7-9aae27fccc67

Give feedback

Tell us about your experience with deployment



ranjanstr

Storage account

Essentials

Resource group (move)	: SatishRG	Performance	: Standard
Location	: canadacentral	Replication	: Read-access geo-redundant storage (RA-GRS)
Primary/Secondary Location	: Primary: Canada Central, Secondary: Canada East	Account kind	: StorageV2 (general purpose v2)
Subscription (move)	: Free Trial	Provisioning state	: Succeeded
Subscription ID	: 6e6cd149-526b-49f2-a0c7-be7a29a5b76c	Created	: 9/10/2024, 3:17:47 PM
Disk state	: Primary: Available, Secondary: Available		
Tags (edit)	: Add tags		

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Disabled
Blob soft delete	Enabled (7 days)
Container soft delete	Enabled (7 days)
Versioning	Disabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled
Storage tasks assignments	None

File service

Large file share	Enabled

Security

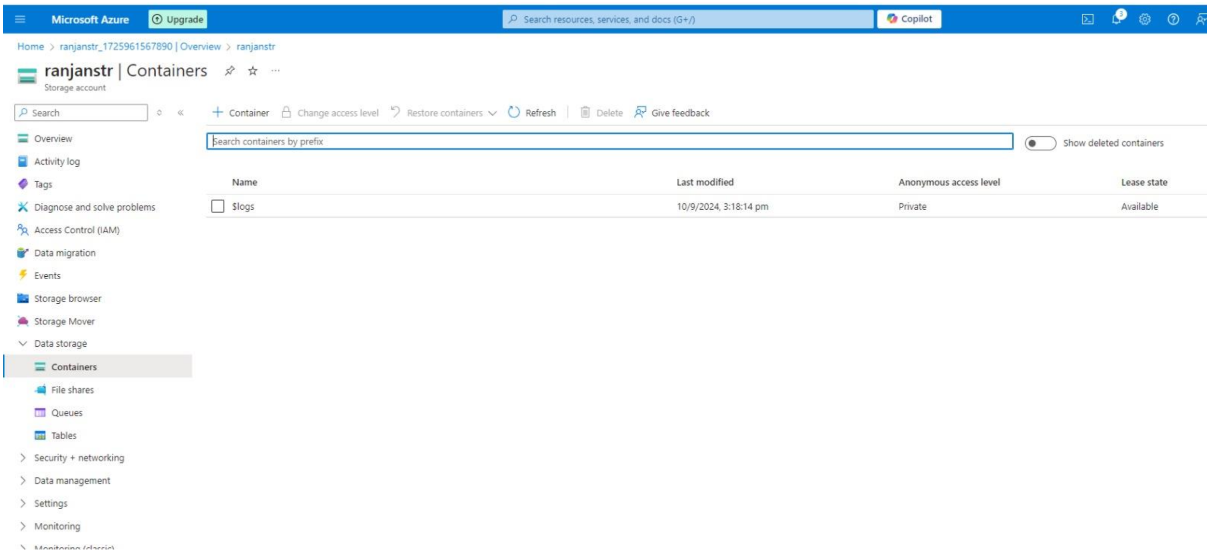
Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

Networking

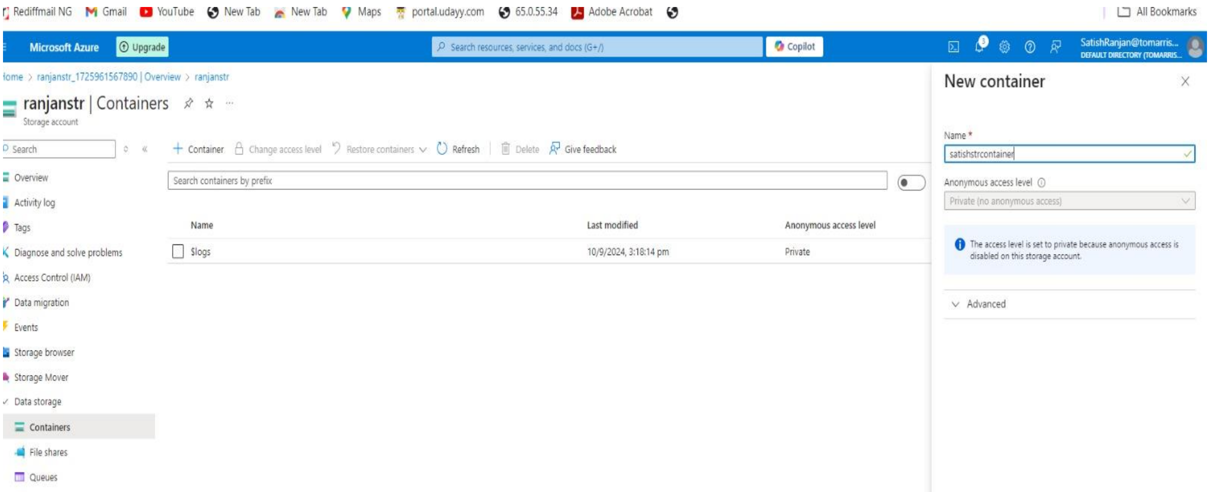
Allow access from	All networks
Private endpoint connections	0
Network routing	Microsoft network routing
Access for trusted Microsoft services	Yes
Endpoint type	Standard

How to Create Container and accessible over internet

Step2: Create one container and upload one image in container



Name	Last modified	Anonymous access level	Lease state
$logs	10/9/2024, 3:18:14 pm	Private	Available

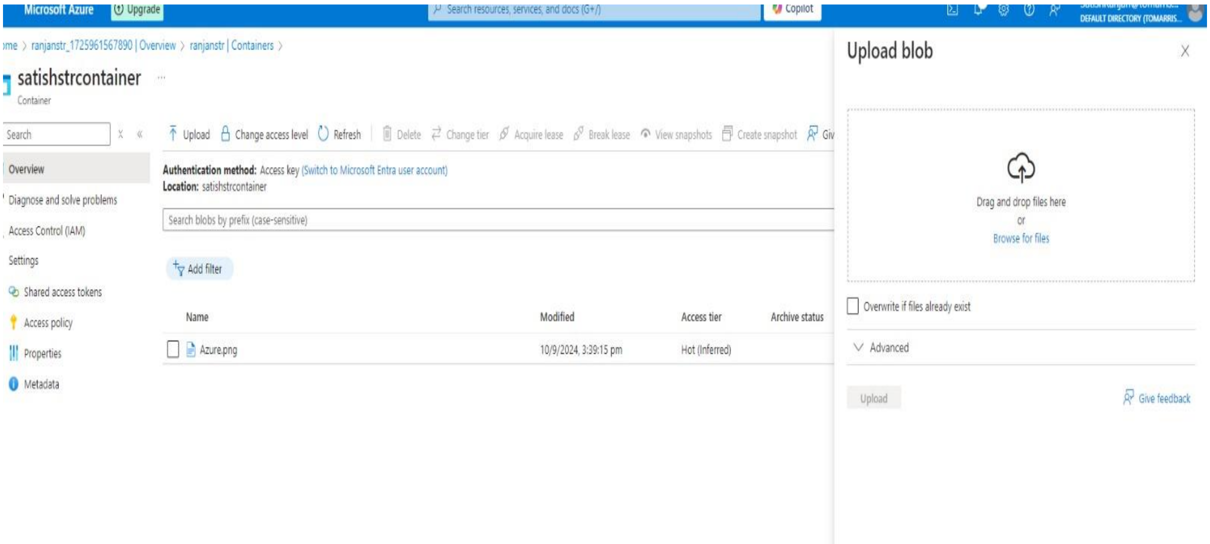


Name	Last modified	Anonymous access level
$logs	10/9/2024, 3:18:14 pm	Private

Name * satishstrcontainer

Anonymous access level: Private (no anonymous access)

The access level is set to private because anonymous access is disabled on this storage account.

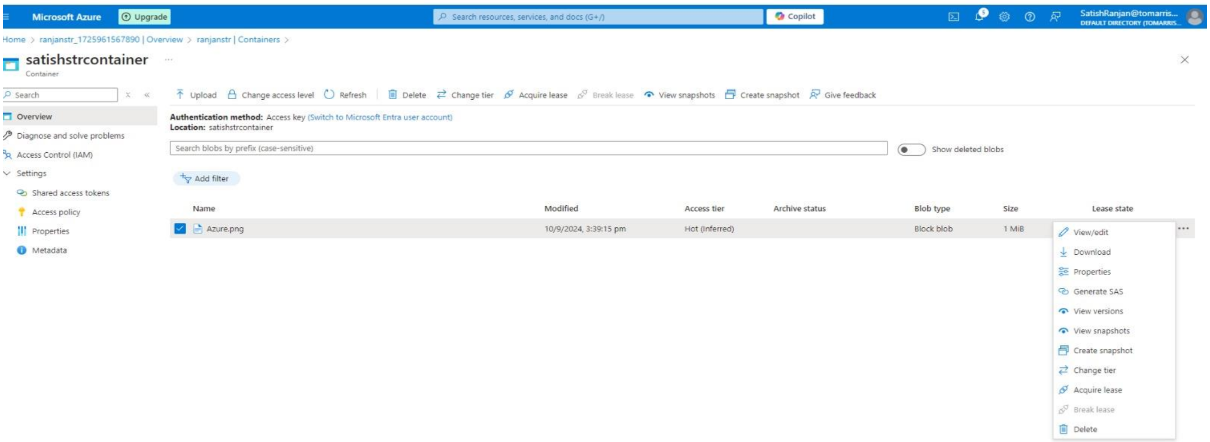


Authentication method: Access key (Switch to Microsoft Entra user account)
Location: satishstrcontainer

Name	Modified	Access tier	Archive status
Azure.png	10/9/2024, 3:39:15 pm	Hot (Inferred)	

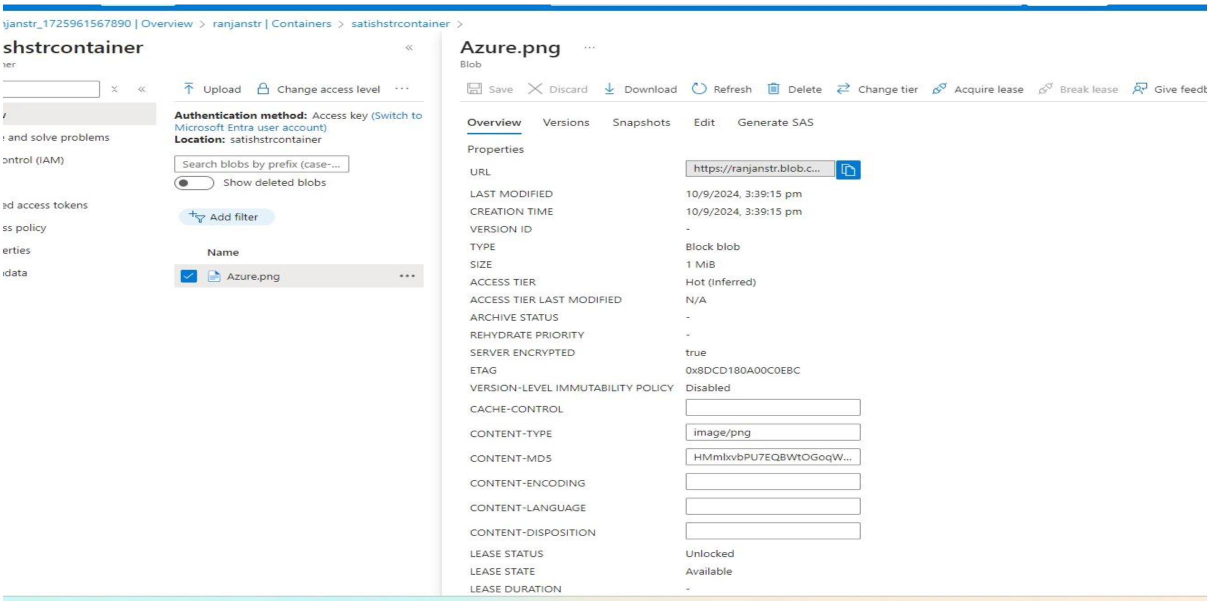
□ Overwrite if files already exist

Step3:   Click on 3 dots in the image and click on generate SAS, and then go to overview and copy URL and paste in browser to check image accessible over internet or not?



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

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
☑ Azure.png	10/9/2024, 3:39:15 pm	Hot (Inferred)		Block blob	1 MiB	

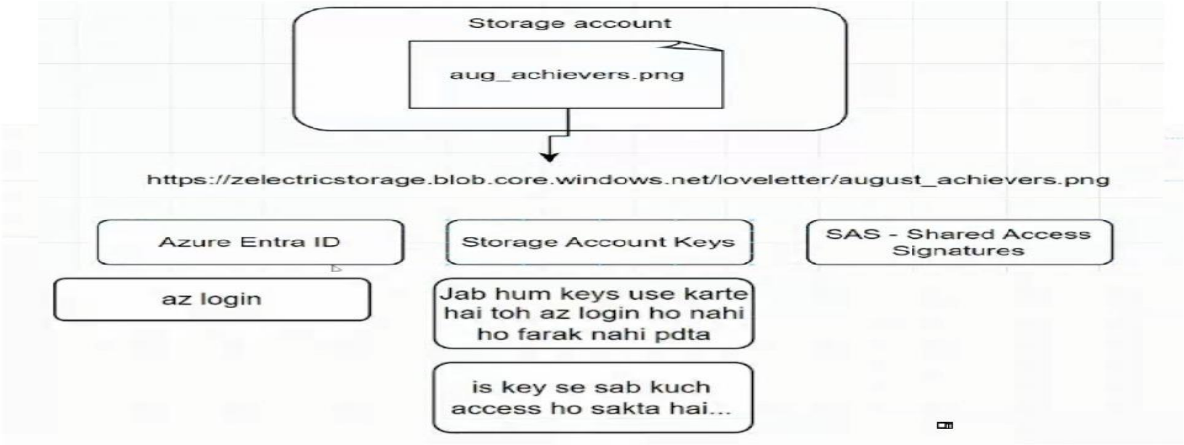


Authentication method: Access key (Switch to Microsoft Entra user account)
Location: satishstrcontainer

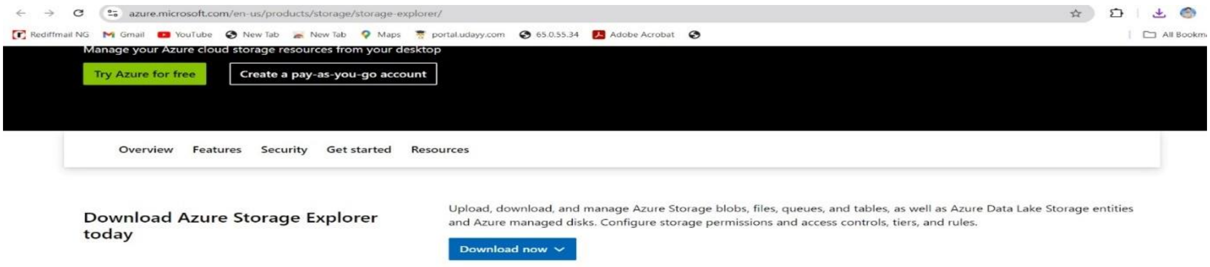
Properties

URL	https://ranjanstr.blob.c...
LAST MODIFIED	10/9/2024, 3:39:15 pm
CREATION TIME	10/9/2024, 3:39:15 pm
VERSION ID	-
TYPE	Block blob
SIZE	1 MiB
ACCESS TIER	Hot (Inferred)
ACCESS TIER LAST MODIFIED	N/A
ARCHIVE STATUS	-
REHYDRATE PRIORITY	-
SERVER ENCRYPTED	true
ETAG	0x8DCD180A00C0EBC
VERSION-LEVEL IMMUTABILITY POLICY	Disabled
CACHE-CONTROL	
CONTENT-TYPE	image/png
CONTENT-MD5	HMmlxvbPU7EQBWtOGoqW...
CONTENT-ENCODING	
CONTENT-LANGUAGE	
CONTENT-DISPOSITION	
LEASE STATUS	Unlocked
LEASE STATE	Available
LEASE DURATION	-

Note : But we cant able to access publicly due to permission issue, so need to authenticate by using below method:


Storage account
aug_achievers.png
https://zelectricstorage.blob.core.windows.net/loveletter/august_achievers.png
Azure Entra ID
Storage Account Keys
SAS - Shared Access Signatures
az login
Jab hum keys use karte hai toh az login ho nahi ho farak nahi pdta
is key se sab kuch access ho sakta hai...

Step4: We can also use Azure Storage Explorer software for Windows, linux and MAC for uploading, downloading purpose of any object.

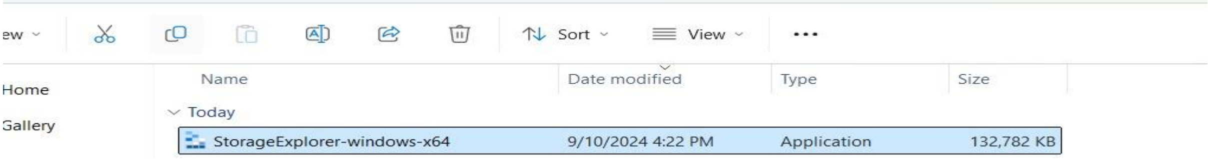


azure.microsoft.com/en-us/products/storage/storage-explorer/

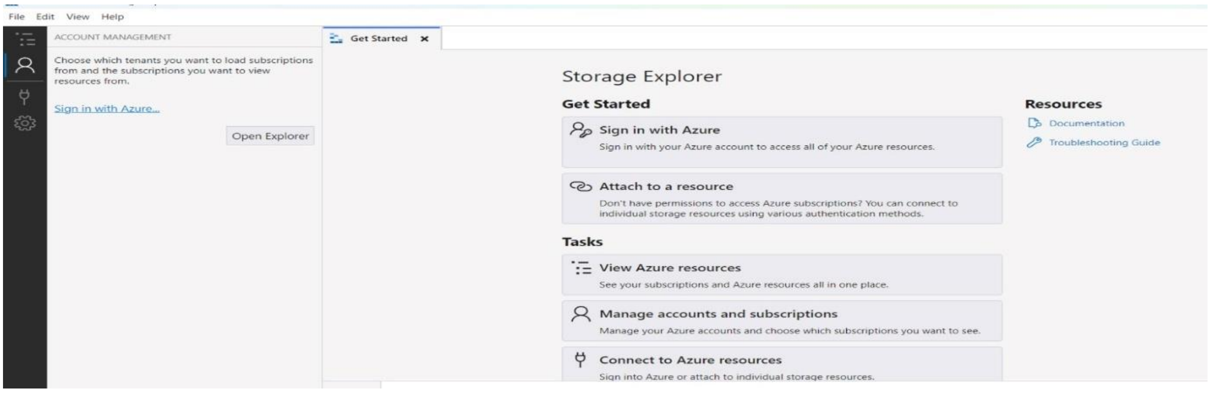
Manage your Azure cloud storage resources from your desktop

Download Azure Storage Explorer today

Upload, download, and manage Azure Storage blobs, files, queues, and tables, as well as Azure Data Lake Storage entities and Azure managed disks. Configure storage permissions and access controls, tiers, and rules.



Name	Date modified	Type	Size
Today			
StorageExplorer-windows-x64	9/10/2024 4:22 PM	Application	132,782 KB



Choose which tenants you want to load subscriptions from and the subscriptions you want to view resources from.

Storage Explorer

Get Started

Sign in with Azure
Sign in with your Azure account to access all of your Azure resources.

Attach to a resource
Don't have permissions to access Azure subscriptions? You can connect to individual storage resources using various authentication methods.

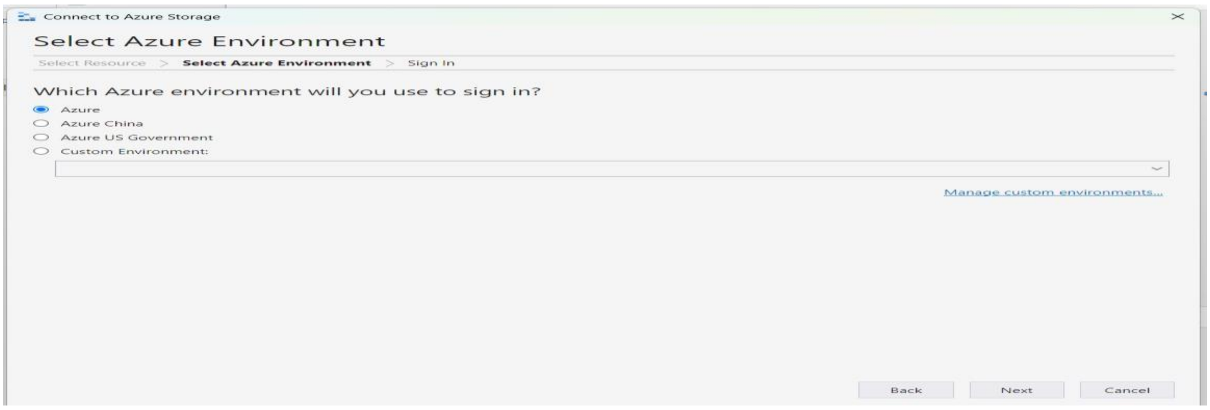
Tasks

View Azure resources
See your subscriptions and Azure resources all in one place.

Manage accounts and subscriptions
Manage your Azure accounts and choose which subscriptions you want to see.

Connect to Azure resources
Sign into Azure or attach to individual storage resources.

Resources
Documentation
Troubleshooting Guide



Connect to Azure Storage

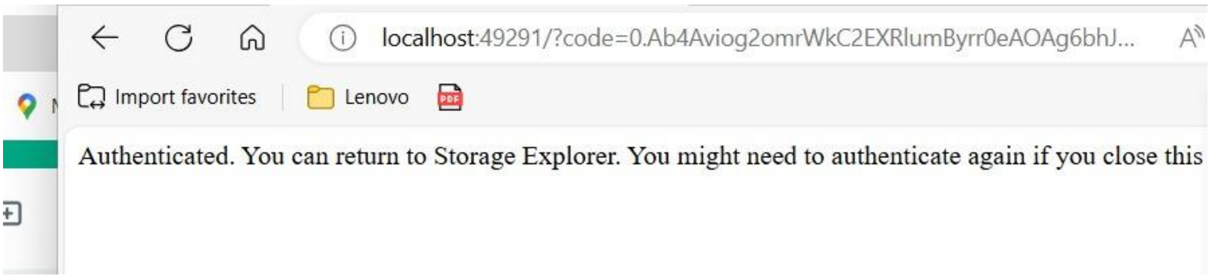
Select Azure Environment

Select Resource > Select Azure Environment > Sign In

Which Azure environment will you use to sign in?

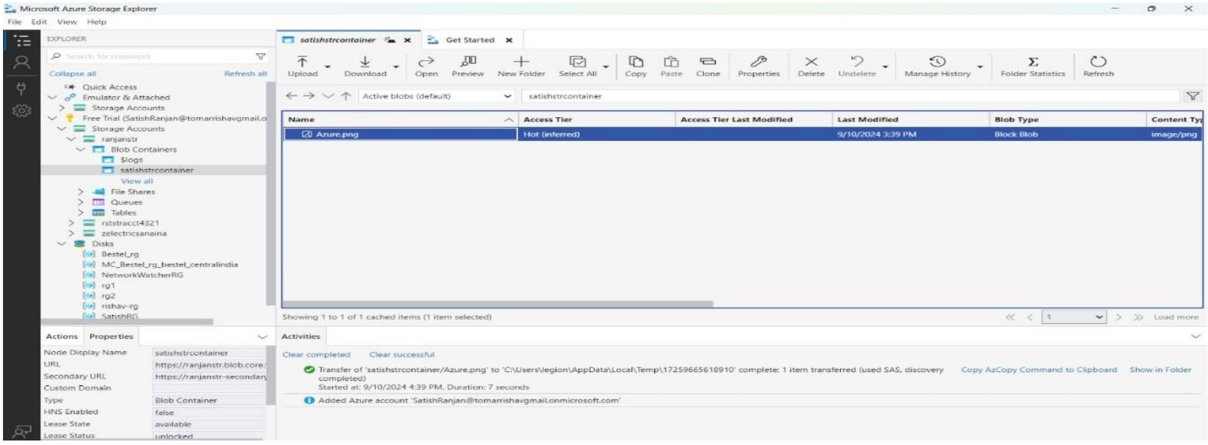
● Azure
○ Azure China
○ Azure US Government
○ Custom Environment:

Manage custom environments...
Back
Next
Cancel



localhost:49291/?code=0.Ab4Aviog2omrWkC2EXRlumByrr0eAOAg6bhJ...

Authenticated. You can return to Storage Explorer. You might need to authenticate again if you close this



Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Ty
Azure.png	Hot (inferred)		9/10/2024 3:39 PM	Block Blob	image/png

Showing 1 to 1 of 1 cached items (1 item selected)

Actions	Properties
Node Display Name	satishstrcontainer
URL	https://ranjanstr.blob.core.
Secondary URL	https://ranjanstr-secondary
Custom Domain	
Type	Blob Container
HNS Enabled	false
Lease State	available
Lease Status	unlocked

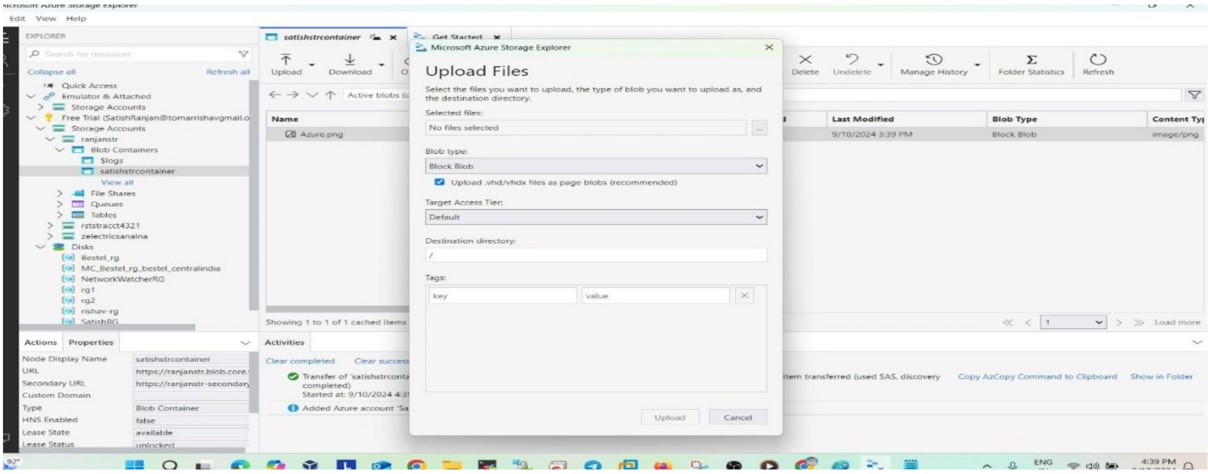
Activities

Clear completed   Clear successful

Transfer of 'satishstrcontainer/Azure.png' to 'C:\Users\legion\AppData\Local\Temp\17259665618910' complete: 1 item transferred (used SAS, discovery completed)
Started at: 9/10/2024 4:39 PM, Duration: 7 seconds

Copy AzCopy Command to Clipboard   Show in Folder

Added Azure account 'SatishRanjan@tomarrishavgmail.onmicrosoft.com'



Microsoft Azure Storage Explorer

Upload Files

Select the files you want to upload, the type of blob you want to upload as, and the destination directory.

Selected files:
No files selected

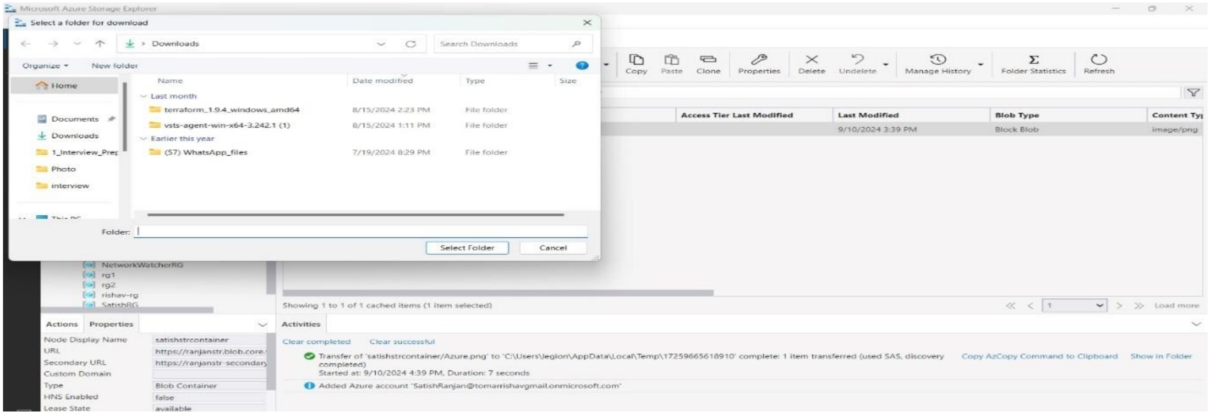
Blob type:
Block Blob

☑ Upload .vhd/vhdx files as page blobs (recommended)

Target Access Tier:
Default

Destination directory:
/

Tags:
key   value



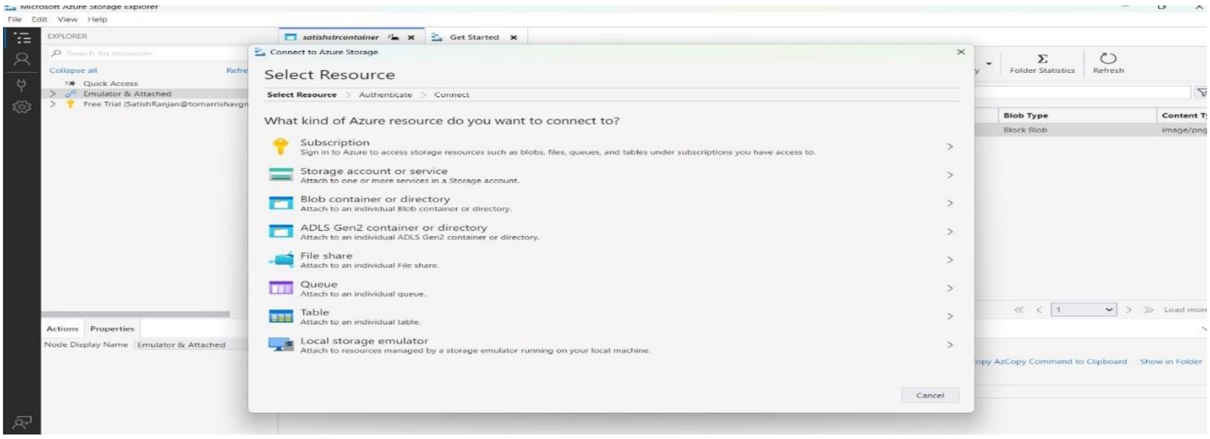
Select a folder for download

Name	Date modified	Type	Size
Last month			
terraform_1.9.4_windows_amd64	8/15/2024 2:23 PM	File folder	
vsts-agent-win-x64-3.242.1 (1)	8/15/2024 1:11 PM	File folder	
Earlier this year			
(57) WhatsApp_files	7/19/2024 8:29 PM	File folder	

Folder:

Transfer of 'satishstrcontainer/Azure.png' to 'C:\Users\legion\AppData\Local\Temp\17259665618910' complete: 1 item transferred (used SAS, discovery completed)
Started at: 9/10/2024 4:39 PM, Duration: 7 seconds

Added Azure account 'SatishRanjan@tomarrishavgmail.onmicrosoft.com'



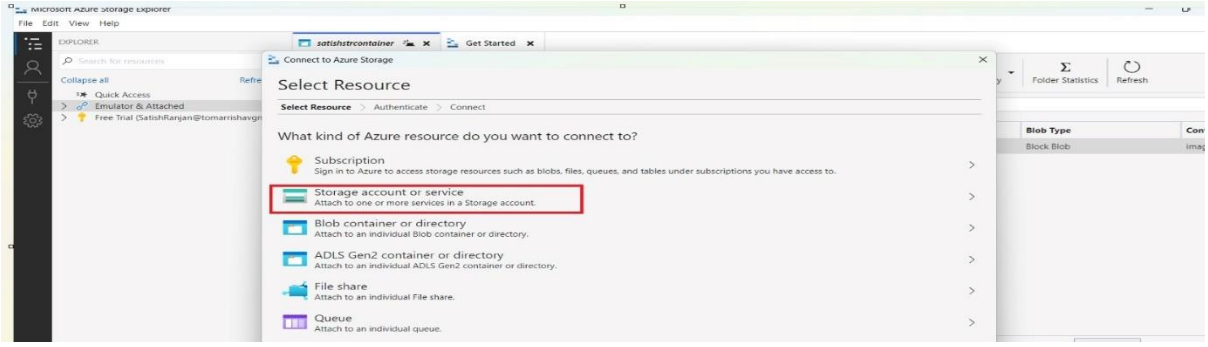
Connect to Azure Storage

Select Resource

Select Resource > Authenticate > Connect

What kind of Azure resource do you want to connect to?

- Subscription
  Sign in to Azure to access storage resources such as blobs, files, queues, and tables under subscriptions you have access to.
- Storage account or service
  Attach to one or more services in a Storage account.
- Blob container or directory
  Attach to an individual Blob container or directory.
- ADLS Gen2 container or directory
  Attach to an individual ADLS Gen2 container or directory.
- File share
  Attach to an individual File share.
- Queue
  Attach to an individual queue.
- Table
  Attach to an individual table.
- Local storage emulator
  Attach to resources managed by a storage emulator running on your local machine.



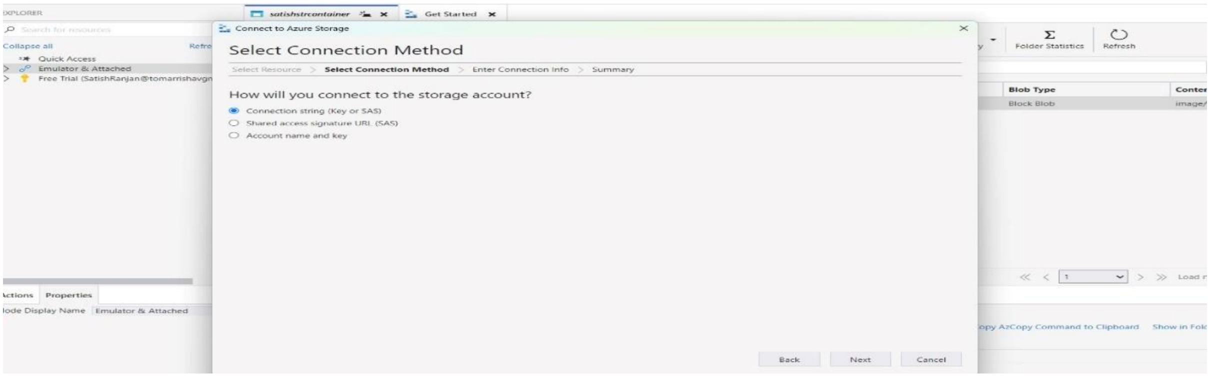
Connect to Azure Storage

Select Resource

Select Resource > Authenticate > Connect

What kind of Azure resource do you want to connect to?

- Subscription
  Sign in to Azure to access storage resources such as blobs, files, queues, and tables under subscriptions you have access to.
- Storage account or service
  Attach to one or more services in a Storage account.
- Blob container or directory
  Attach to an individual Blob container or directory.
- ADLS Gen2 container or directory
  Attach to an individual ADLS Gen2 container or directory.
- File share
  Attach to an individual File share.
- Queue
  Attach to an individual queue.



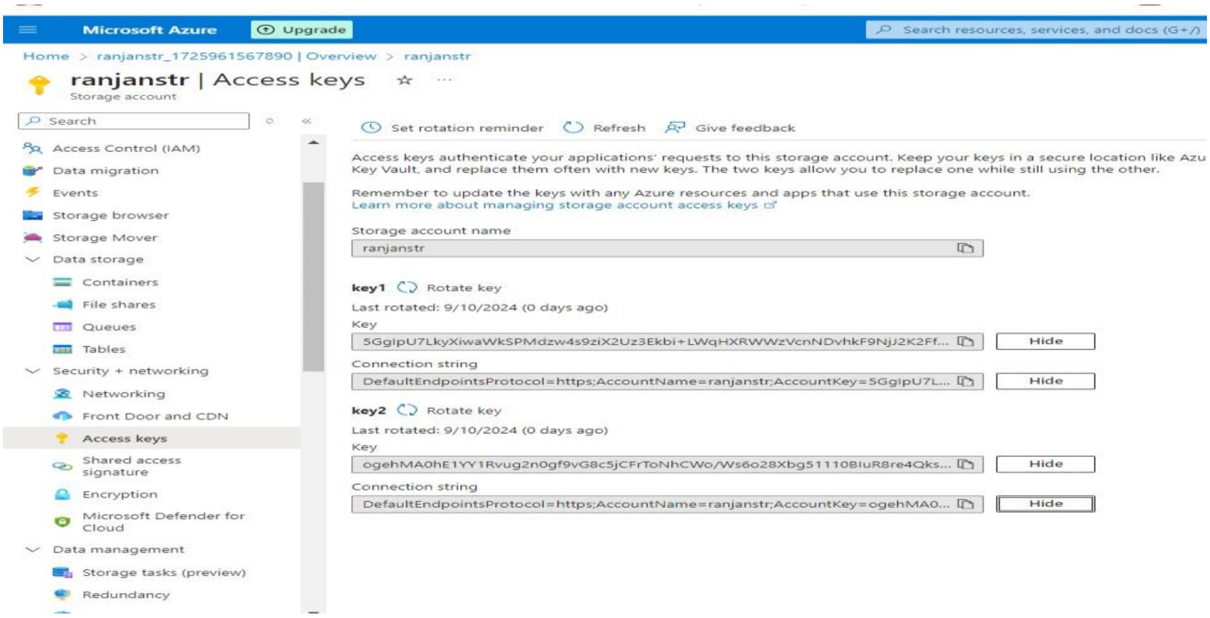
Connect to Azure Storage

Select Connection Method

Select Resource > **Select Connection Method** > Enter Connection Info > Summary

How will you connect to the storage account?

● Connection string (Key or SAS)
○ Shared access signature URL (SAS)
○ Account name and key



ranjanstr | Access keys

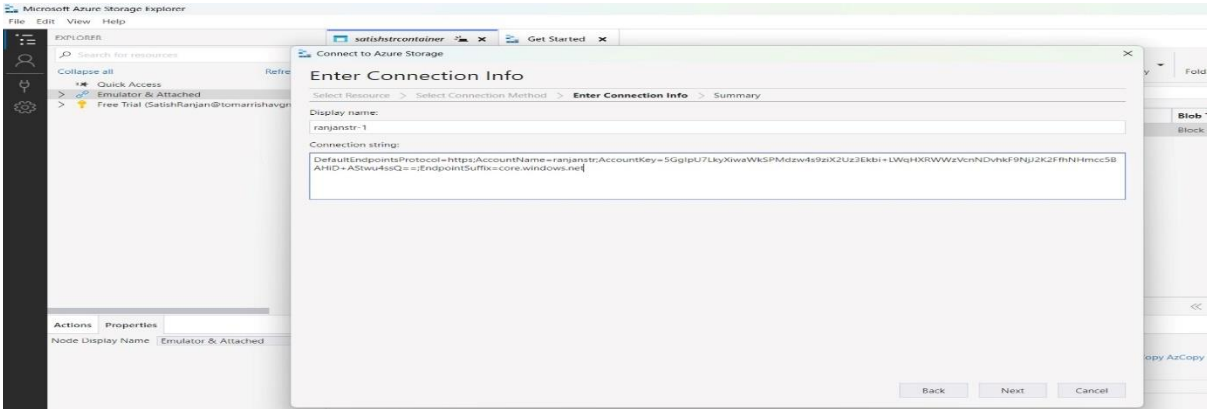
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azu Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

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
ranjanstr

key1 Rotate key
Last rotated: 9/10/2024 (0 days ago)
Key
5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2Ff... Hide
Connection string
DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=5GgIpU7L... Hide

key2 Rotate key
Last rotated: 9/10/2024 (0 days ago)
Key
ogehMA0hE1YY1Rvug2n0gf9vG8c5jCFrToNhCWo/Ws6o28Xbg51110BIuR8re4Qks... Hide
Connection string
DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=ogehMA0... Hide



Connect to Azure Storage

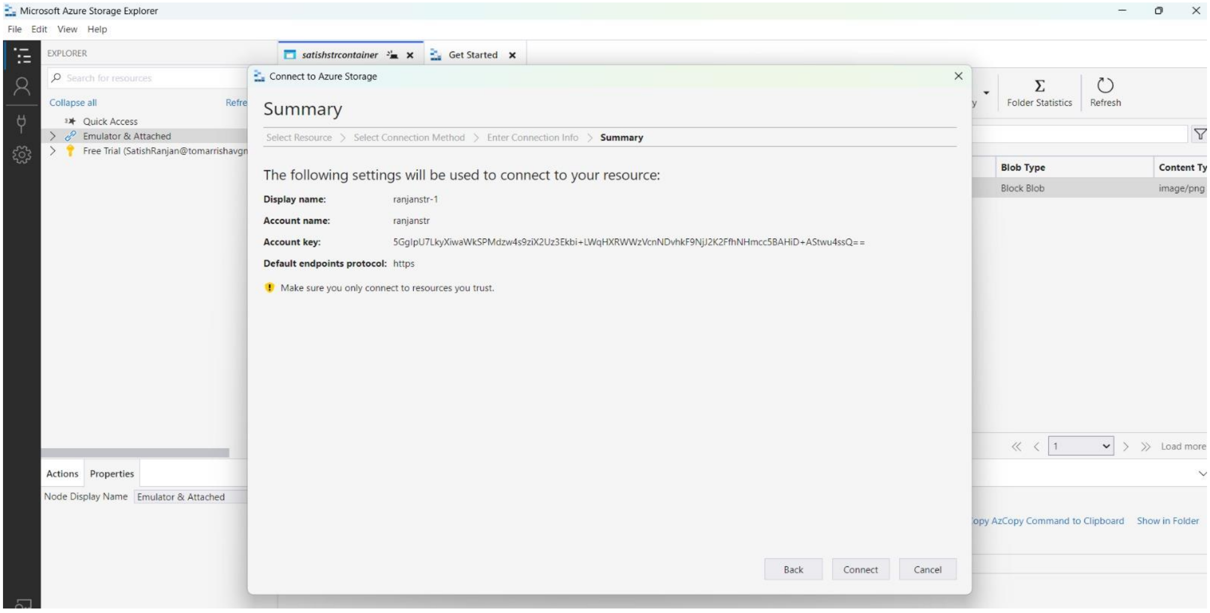
Enter Connection Info

Select Resource > Select Connection Method > **Enter Connection Info** > Summary

Display name:
ranjanstr-1

Connection string:

```
DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2FfhNHmcc5B
AHiD+AStwu4ssQ==;EndpointSuffix=core.windows.net
```



Node Display Name: Emulator & Attached

Connect to Azure Storage

Summary

Select Resource > Select Connection Method > Enter Connection Info > **Summary**

The following settings will be used to connect to your resource:

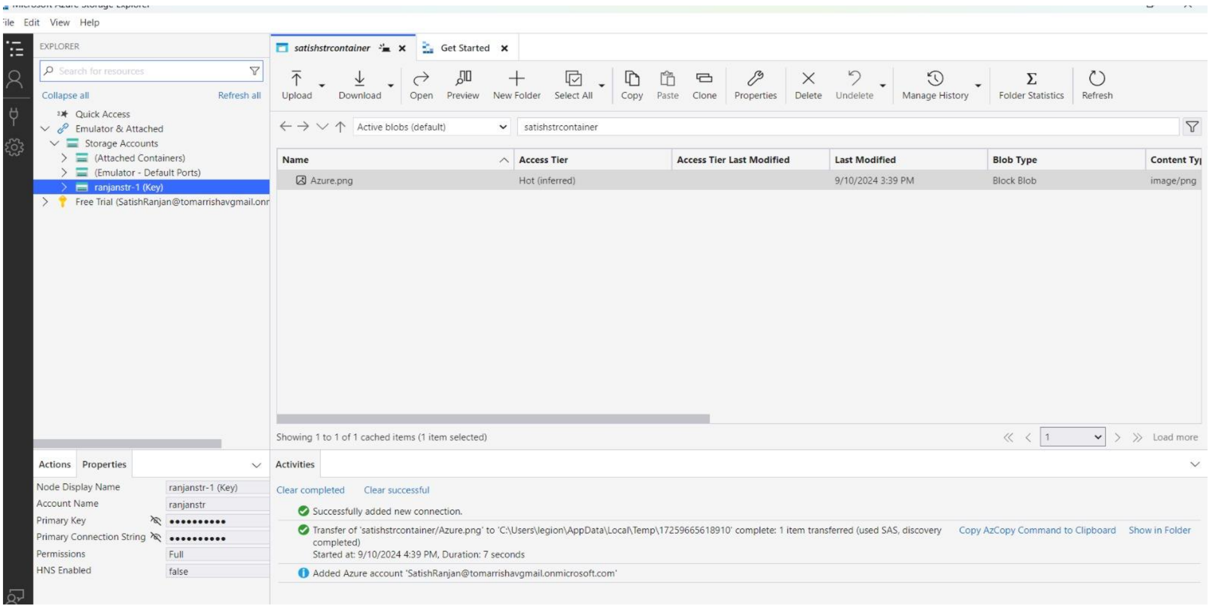
Display name: ranjanstr-1

Account name: ranjanstr

Account key: 5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2FfhNHmcc5BAHiD+AStwu4ssQ==

Default endpoints protocol: https

Make sure you only connect to resources you trust.



Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Ty
Azure.png	Hot (inferred)		9/10/2024 3:39 PM	Block Blob	image/png

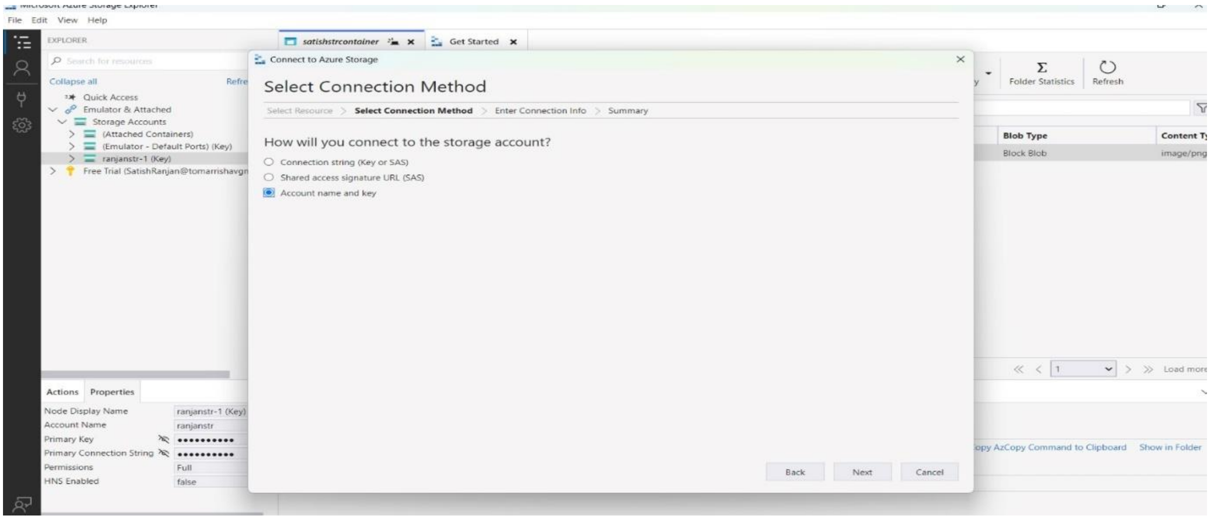
Showing 1 to 1 of 1 cached items (1 item selected)

Actions	Properties
Node Display Name	ranjanstr-1 (Key)
Account Name	ranjanstr
Primary Key	••••••••••
Primary Connection String	••••••••••
Permissions	Full
HNS Enabled	false

Activities

Clear completed Clear successful

- Successfully added new connection.
- Transfer of 'satishstrcontainer/Azure.png' to 'C:\Users\legion\AppData\Local\Temp\17259665618910' complete: 1 item transferred (used SAS, discovery completed)
  Started at: 9/10/2024 4:39 PM, Duration: 7 seconds — Copy AzCopy Command to Clipboard Show in Folder
- Added Azure account 'SatishRanjan@tomarrishavgmail.onmicrosoft.com'



Actions	Properties
Node Display Name	ranjanstr-1 (Key)
Account Name	ranjanstr
Primary Key	••••••••••
Primary Connection String	••••••••••
Permissions	Full
HNS Enabled	false

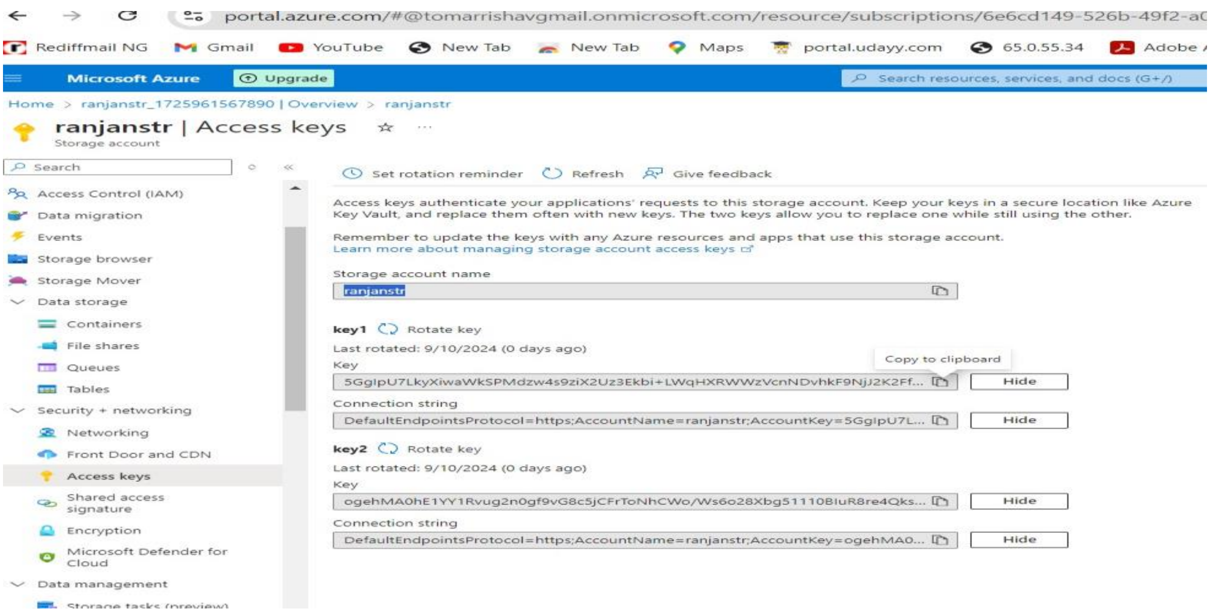
Connect to Azure Storage

Select Connection Method

Select Resource > **Select Connection Method** > Enter Connection Info > Summary

How will you connect to the storage account?

- ○ Connection string (Key or SAS)
- ○ Shared access signature URL (SAS)
- ● Account name and key



ranjanstr | Access keys

Storage account

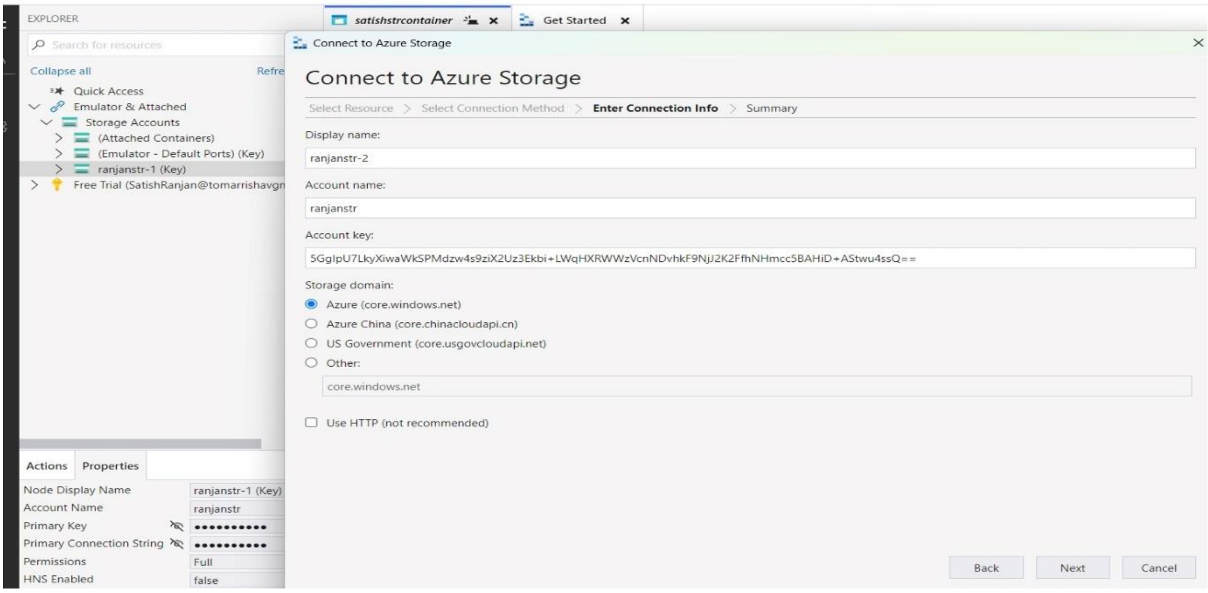
Access keys authenticate your applications' requests to this storage account. Keep your keys in a secure location like Azure Key Vault, and replace them often with new keys. The two keys allow you to replace one while still using the other.

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: ranjanstr

key1 Rotate key
Last rotated: 9/10/2024 (0 days ago)
Key: 5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2Ff...
Connection string: DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=5GgIpU7L...

key2 Rotate key
Last rotated: 9/10/2024 (0 days ago)
Key: ogehMA0hE1YY1Rvug2n0gf9vG8c5jCFrToNhCWo/Ws6o28Xbg51110BIuR8re4Qks...
Connection string: DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=ogehMA0...



Connect to Azure Storage

Connect to Azure Storage

Display name: ranjanstr-2

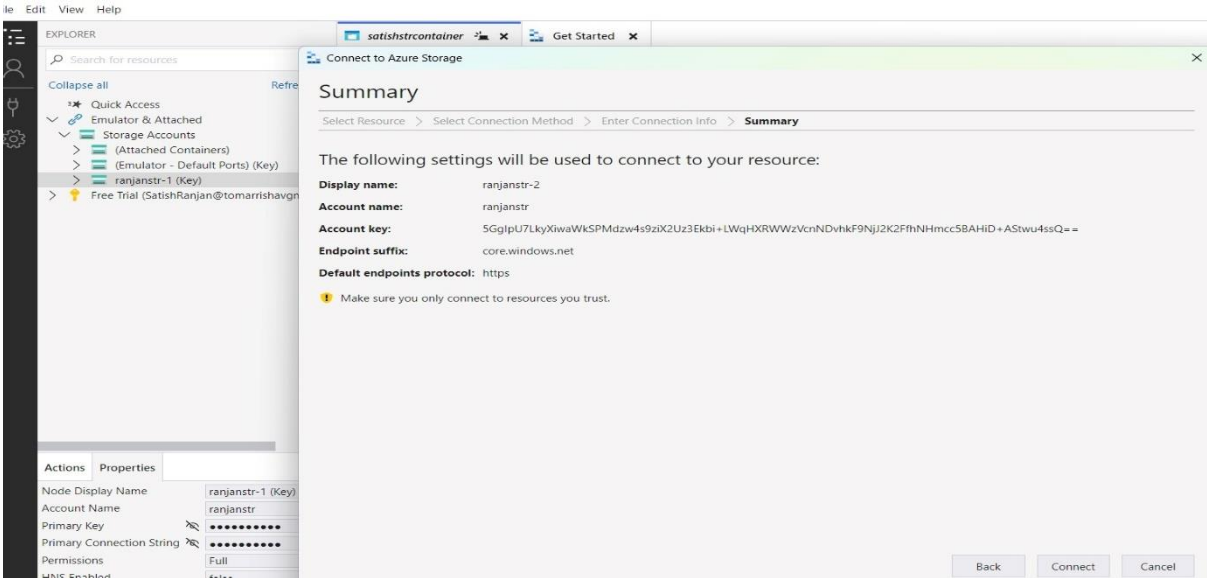
Account name: ranjanstr

Account key: 5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2FfhNHmcc5BAHiD+AStwu4ssQ==

Storage domain:
● Azure (core.windows.net)
○ Azure China (core.chinacloudapi.cn)
○ US Government (core.usgovcloudapi.net)
○ Other:
core.windows.net

□ Use HTTP (not recommended)

Node Display Name	ranjanstr-1 (Key)
Account Name	ranjanstr
Primary Key	••••••••••
Primary Connection String	••••••••••
Permissions	Full
HNS Enabled	false



Connect to Azure Storage

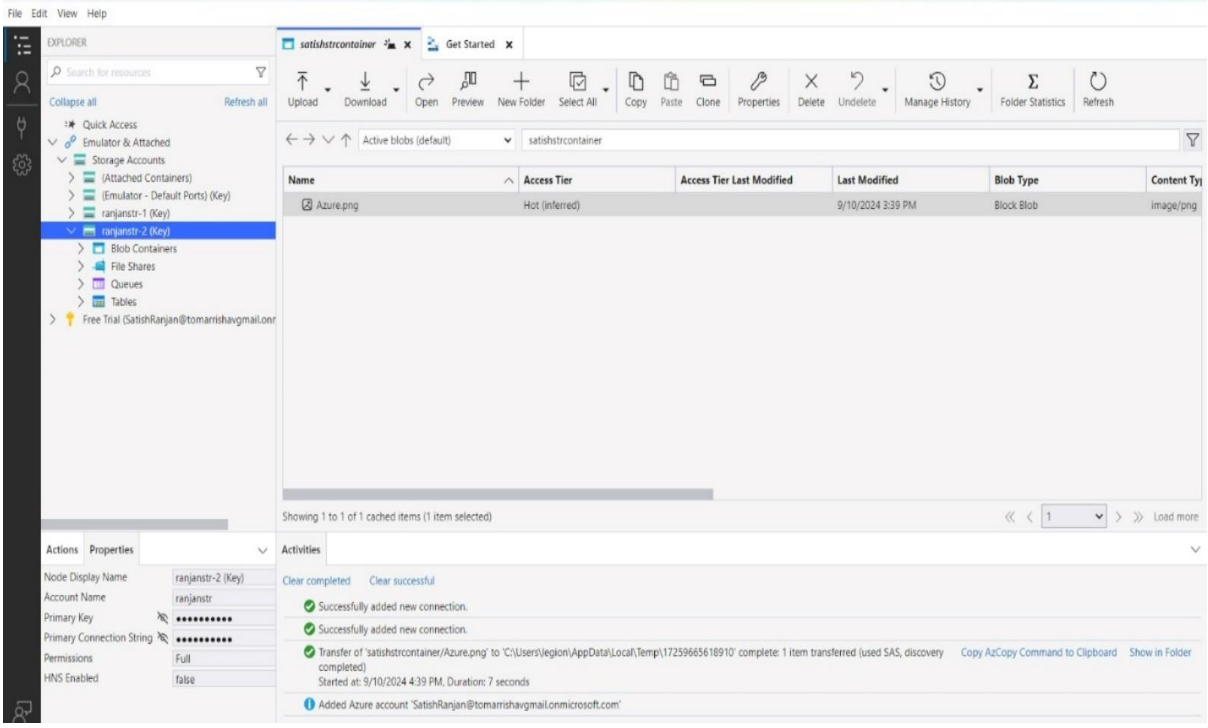
Summary

The following settings will be used to connect to your resource:

Display name: ranjanstr-2
Account name: ranjanstr
Account key: 5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2FfhNHmcc5BAHiD+AStwu4ssQ==
Endpoint suffix: core.windows.net
Default endpoints protocol: https

Make sure you only connect to resources you trust.

Node Display Name	ranjanstr-1 (Key)
Account Name	ranjanstr
Primary Key	••••••••••
Primary Connection String	••••••••••
Permissions	Full
HNS Enabled	false



Name	Access Tier	Access Tier Last Modified	Last Modified	Blob Type	Content Ty
Azure.png	Hot (inferred)		9/10/2024 3:39 PM	Block Blob	image/png

Showing 1 to 1 of 1 cached items (1 item selected)

Node Display Name	ranjanstr-2 (Key)
Account Name	ranjanstr
Primary Key	•••••••••••
Primary Connection String	•••••••••••
Permissions	Full
HNS Enabled	false

✓ Successfully added new connection.

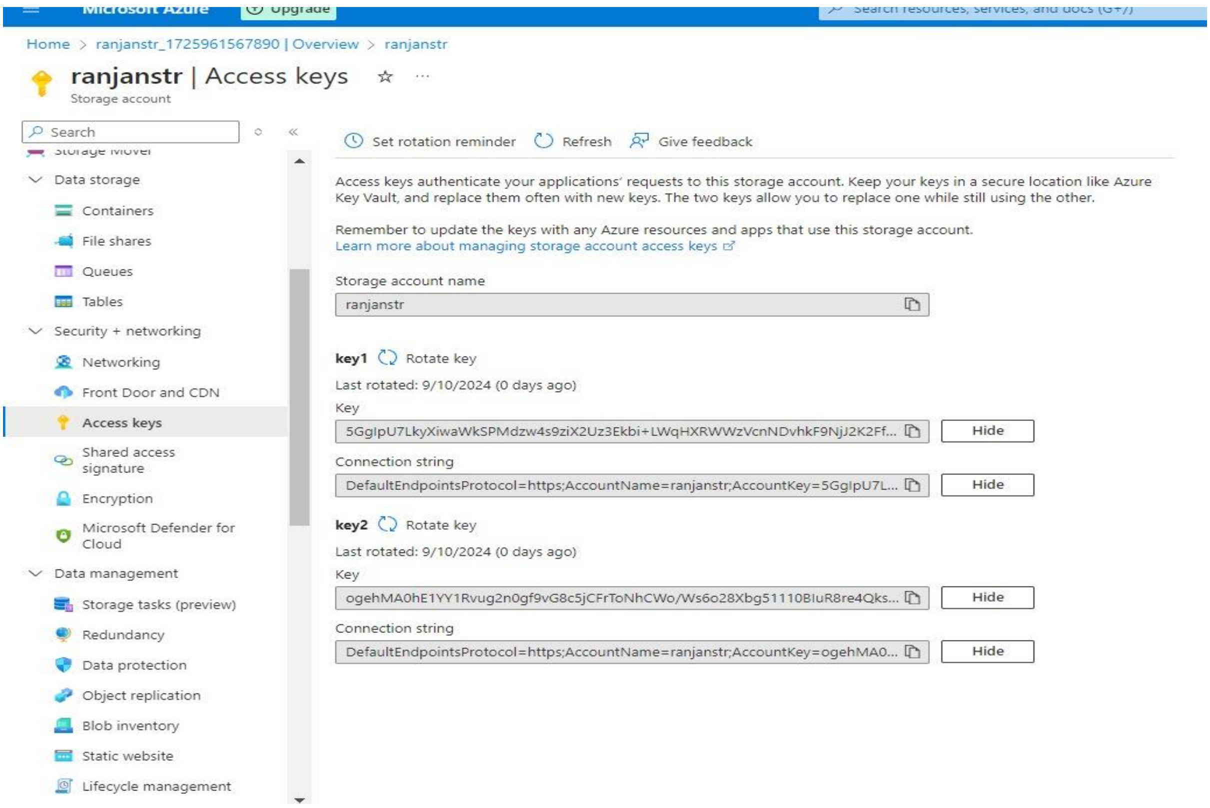
✓ Successfully added new connection.

✓ Transfer of 'satishstrcontainer/Azure.png' to 'C:\Users\legion\AppData\Local\Temp\17259665618910' complete: 1 item transferred (used SAS, discovery completed)
Started at: 9/10/2024 4:39 PM, Duration: 7 seconds

Added Azure account 'SatishRanjan@tomarrishavgmail.onmicrosoft.com'

Step5: For Accessing container image externally need to use Storage Account Keys method and SAS Method:

1. **Storage Account Keys Method**



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.

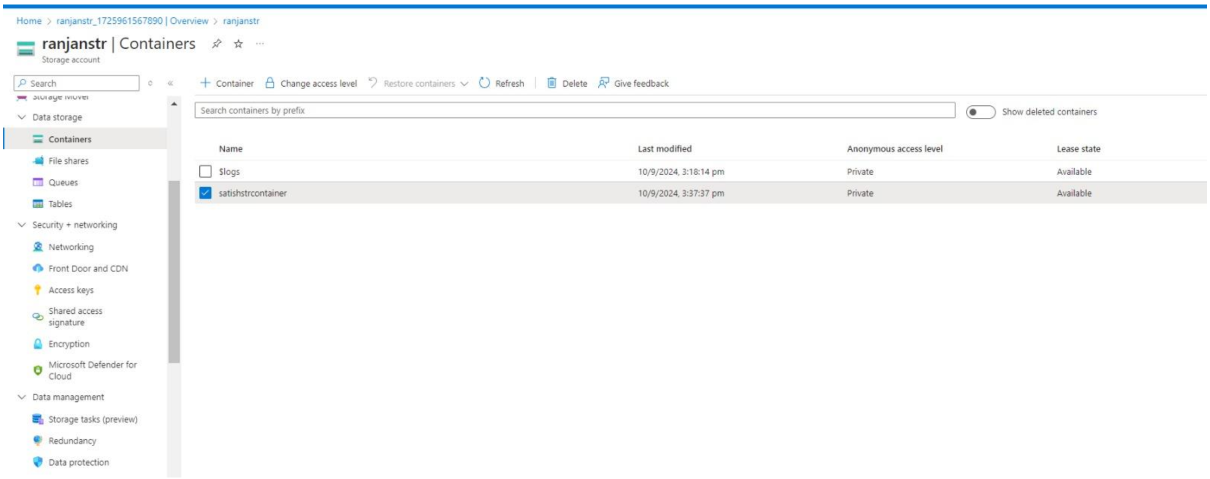
Remember to update the keys with any Azure resources and apps that use this storage account.
Learn more about managing storage account access keys

Storage account name: ranjanstr

key1
Last rotated: 9/10/2024 (0 days ago)
Key: 5GgIpU7LkyXiwaWkSPMdzw4s9ziX2Uz3Ekbi+LWqHXRWWzVcnNDvhkF9NjJ2K2Ff...
Connection string: DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=5GgIpU7L...

key2
Last rotated: 9/10/2024 (0 days ago)
Key: ogehMA0hE1YY1Rvug2n0gf9vG8c5jCFrToNhCWo/Ws6o28Xbg51110BIuR8re4Qks...
Connection string: DefaultEndpointsProtocol=https;AccountName=ranjanstr;AccountKey=ogehMA0...

2. SAS Method:



Home > ranjanstr_1725961567890 | Overview > ranjanstr

ranjanstr | Containers
Storage account

Search | + Container | Change access level | Restore containers | Refresh | Delete | Give feedback

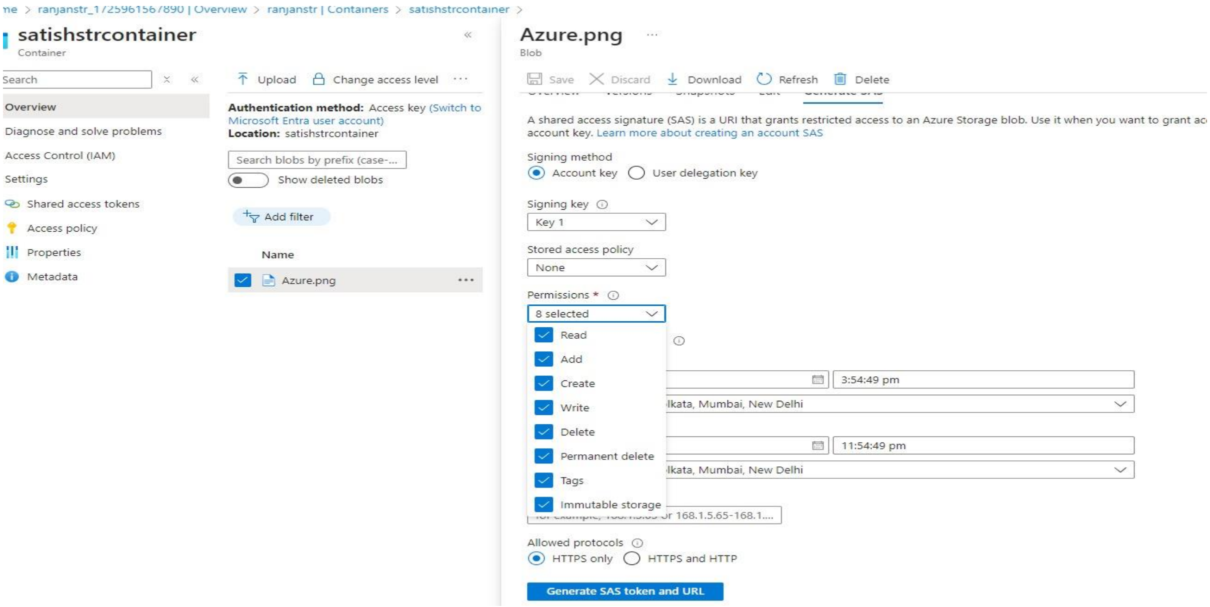
Data storage
- Containers
- File shares
- Queues
- Tables

Security + networking
- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management
- Storage tasks (preview)
- Redundancy
- Data protection

Search containers by prefix | Show deleted containers

	Name	Last modified	Anonymous access level	Lease state
□	$logs	10/9/2024, 3:18:14 pm	Private	Available
☑	satishstrcontainer	10/9/2024, 3:37:37 pm	Private	Available



ne > ranjanstr_1725961567890 | Overview > ranjanstr | Containers > satishstrcontainer >

satishstrcontainer
Container

Search

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

Upload | Change access level

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

Search blobs by prefix (case-...
Show deleted blobs

Add filter

	Name
☑	Azure.png

Azure.png
Blob

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 ac account key. Learn more about creating an account SAS

Signing method
● Account key ○ User delegation key

Signing key: Key 1

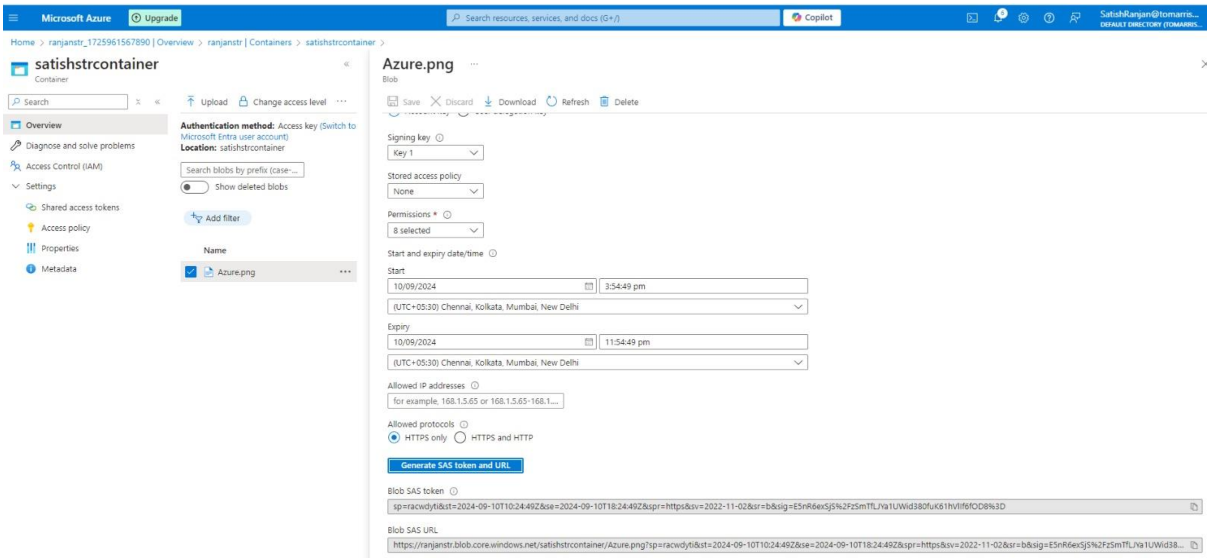
Stored access policy: None

Permissions *: 8 selected
- ☑ Read
- ☑ Add
- ☑ Create
- ☑ Write
- ☑ Delete
- ☑ Permanent delete
- ☑ Tags
- ☑ Immutable storage

3:54:49 pm
lkata, Mumbai, New Delhi
11:54:49 pm
lkata, Mumbai, New Delhi
r 168.1.5.65-168.1....

Allowed protocols
● HTTPS only ○ HTTPS and HTTP

Generate SAS token and URL



Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot | SatishRanjan@tomarris... DEFAULT DIRECTORY (TOMARRIS...

Home > ranjanstr_1725961567890 | Overview > ranjanstr | Containers > satishstrcontainer >

satishstrcontainer
Container

Search

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

Upload | Change access level

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

Search blobs by prefix (case-...
Show deleted blobs

Add filter

	Name
☑	Azure.png

Azure.png
Blob

Save | Discard | Download | Refresh | Delete

Signing key: Key 1

Stored access policy: None

Permissions *: 8 selected

Start and expiry date/time

Start: 10/09/2024 | 3:54:49 pm
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Expiry: 10/09/2024 | 11:54:49 pm
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Allowed IP addresses: for example, 168.1.5.65 or 168.1.5.65-168.1....

Allowed protocols
● HTTPS only ○ HTTPS and HTTP

Generate SAS token and URL

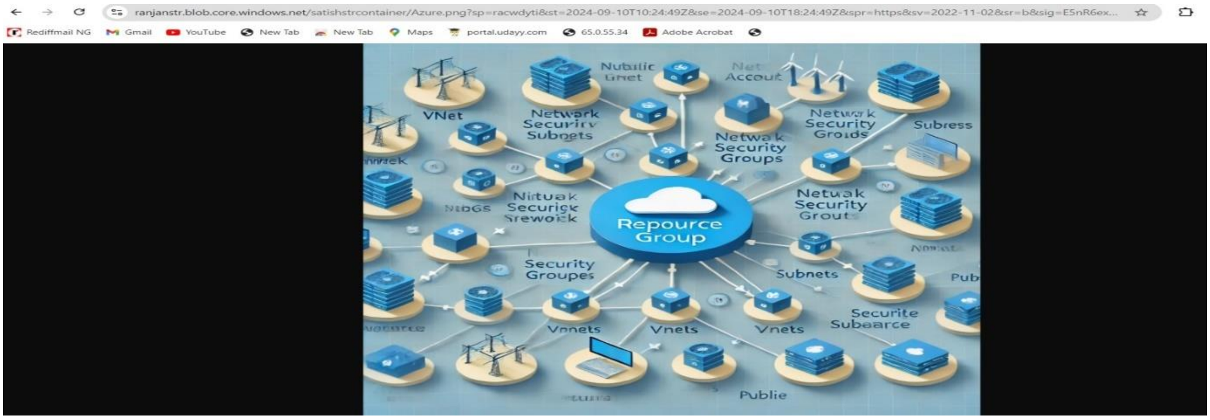
Blob SAS token

```
sp=racwdyti&st=2024-09-10T10:24:49Z&se=2024-09-10T18:24:49Z&spr=https&sv=2022-11-02&sr=b&sig=E5nR6exSjS%2FzSmTfLJYa1UWid380fuK61hVIIf6fOD8%3D
```

Blob SAS URL

```
https://ranjanstr.blob.core.windows.net/satishstrcontainer/Azure.png?sp=racwdyti&st=2024-09-10T10:24:49Z&se=2024-09-10T18:24:49Z&spr=https&sv=2022-11-02&sr=b&sig=E5nR6exSjS%2FzSmTfLJYa1UWid38...
```

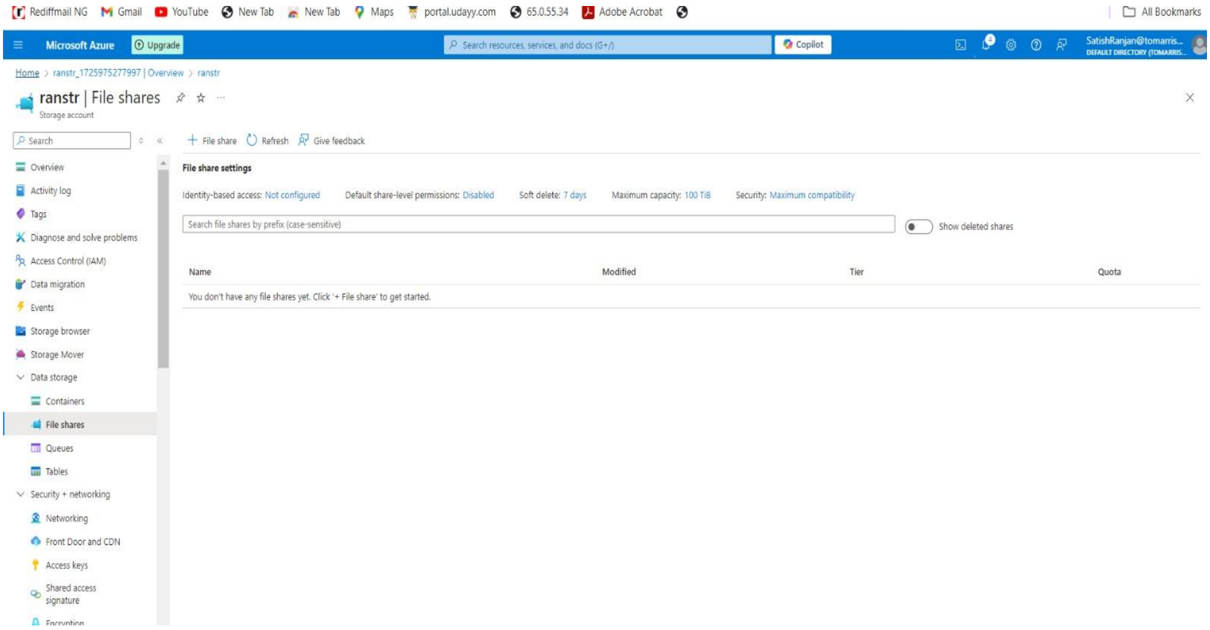
Step6:   Now image accessible publicly



ranjanstr.blob.core.windows.net/satishstrcontainer/Azure.png?sp=racwdyti&st=2024-09-10T10:24:49Z&se=2024-09-10T18:24:49Z&spr=https&sv=2022-11-02&sr=b&sig=E5nR6ex...

How to Create File Share and check

Step7: Go to File share in storage and then create one file share



Home > ranstr_1725975277997 | Overview > ranstr

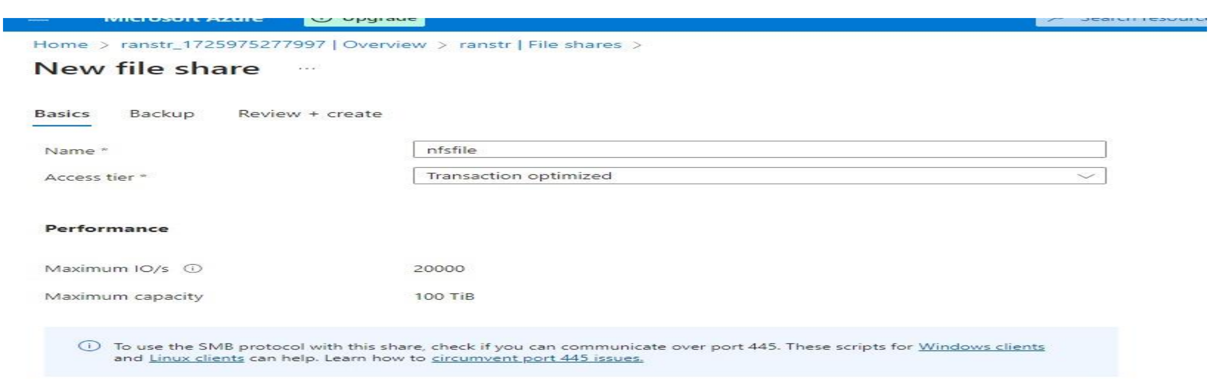
ranstr | File shares

Storage account

File share settings

Identity-based access: Not configured   Default share-level permissions: Disabled   Soft delete: 7 days   Maximum capacity: 100 TiB   Security: Maximum compatibility

Name	Modified	Tier	Quota
You don't have any file shares yet. Click '+ File share' to get started.			



Home > ranstr_1725977277997 | Overview > ranstr | File shares >

New file share

Name * nfsfile

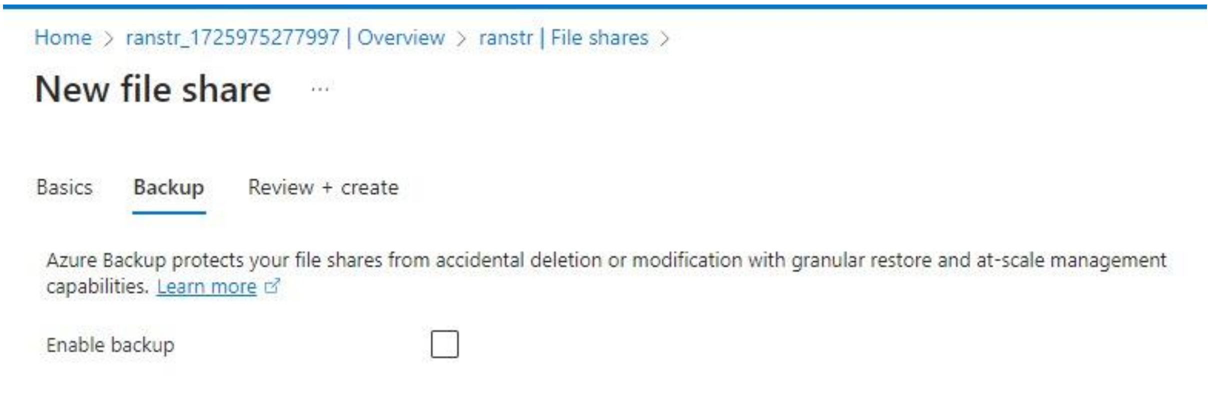
Access tier * Transaction optimized

Performance

Maximum IO/s 20000

Maximum capacity 100 TiB

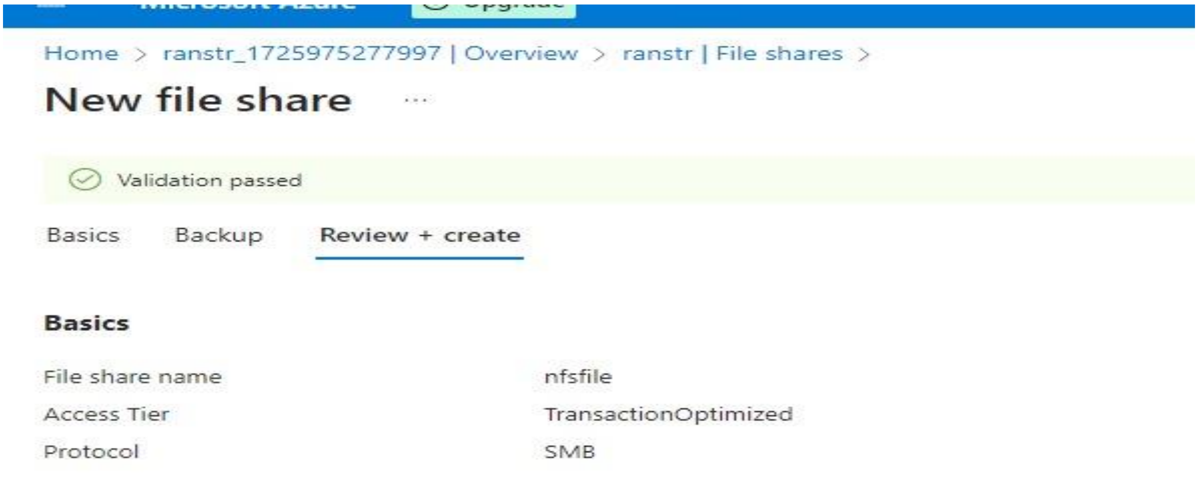
To use the SMB protocol with this share, check if you can communicate over port 445. These scripts for Windows clients and Linux clients can help. Learn how to circumvent port 445 issues.


Home > ranstr_1725975277997 | Overview > ranstr | File shares >
Basics
Backup
Review + create

New file share

Azure Backup protects your file shares from accidental deletion or modification with granular restore and at-scale management capabilities. Learn more

Enable backup □

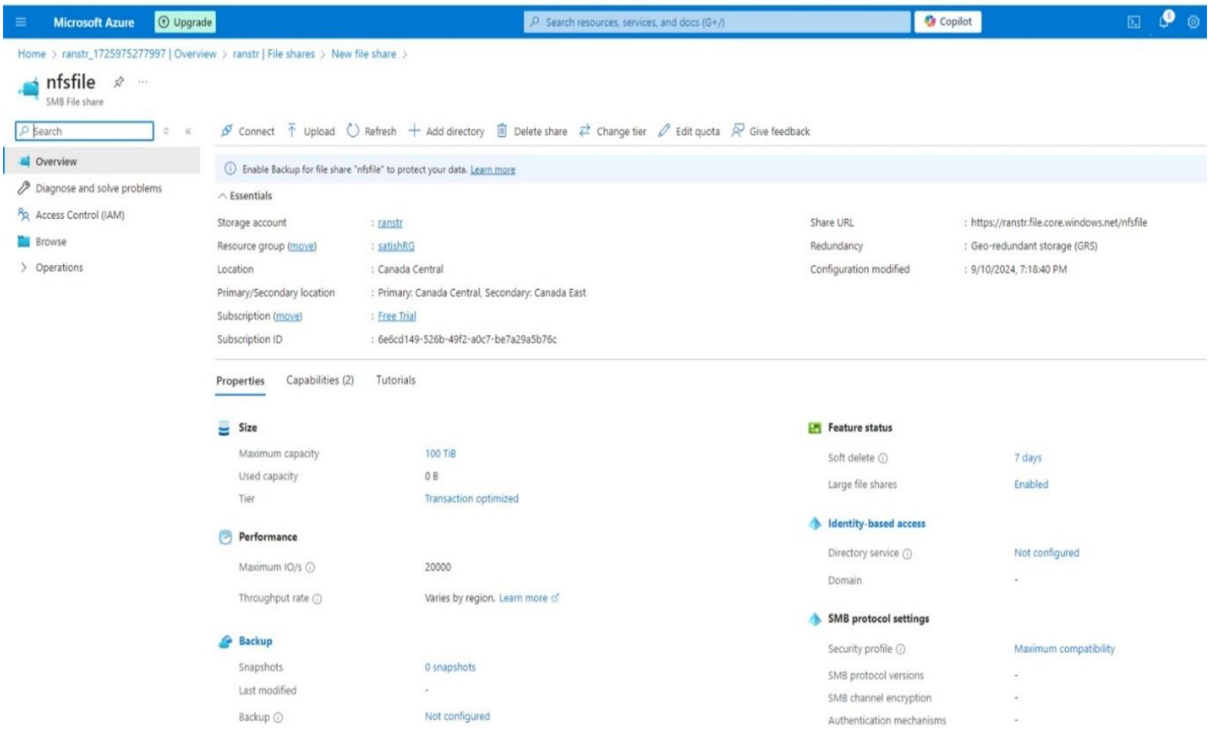

Home > ranstr_1725975277997 | Overview > ranstr | File shares >
Basics
Backup
Review + create

New file share

Validation passed

Basics

File share name	nfsfile
Access Tier	TransactionOptimized
Protocol	SMB



nfsfile

SMB File share

Enable Backup for file share "nfsfile" to protect your data. Learn more

Essentials

Storage account	: ranstr	Share URL	: https://ranstr.file.core.windows.net/nfsfile
Resource group (move)	: satishRG	Redundancy	: Geo-redundant storage (GRS)
Location	: Canada Central	Configuration modified	: 9/10/2024, 7:18:40 PM
Primary/Secondary location	: Primary: Canada Central, Secondary: Canada East		
Subscription (move)	: Free Trial		
Subscription ID	: 6e6cd149-526b-49f2-a0c7-be7a29a5b76c		

Size

Maximum capacity	100 TiB
Used capacity	0 B
Tier	Transaction optimized

Performance

Maximum IO/s	20000
Throughput rate	Varies by region. Learn more

Backup

Snapshots	0 snapshots
Last modified	-
Backup	Not configured

Feature status

Soft delete	7 days
Large file shares	Enabled

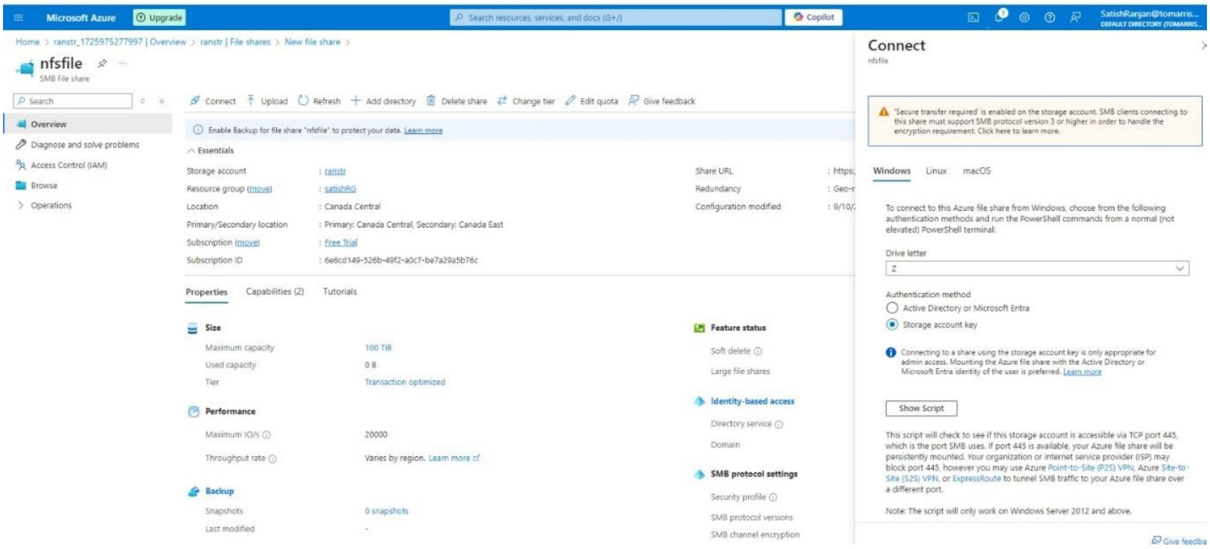
Identity-based access

Directory service	Not configured
Domain	-

SMB protocol settings

Security profile	Maximum compatibility
SMB protocol versions	-
SMB channel encryption	-
Authentication mechanisms	-

Step8: Click to connect and then create any drive for any OS like windows, linux and macos, here we are using for windows.



Home > ranstr_1725975277997 | Overview > ranstr | File shares > New file share >

nfsfile
SMB File share

Essentials

Storage account : ranstr
Resource group (move) : satishRG
Location : Canada Central
Primary/Secondary location : Primary: Canada Central, Secondary: Canada East
Subscription (move) : Free Trial
Subscription ID : 6e6cd149-526b-49f2-a0c7-be7a29a5b76c
Share URL : https:
Redundancy : Geo-r
Configuration modified : 9/10/

Size
Maximum capacity 100 TiB
Used capacity 0 B
Tier Transaction optimized

Performance
Maximum IO/s 20000
Throughput rate Varies by region. Learn more

Backup
Snapshots 0 snapshots
Last modified -

Connect
nfsfile

'Secure transfer required' is enabled on the storage account. SMB clients connecting to this share must support SMB protocol version 3 or higher in order to handle the encryption requirement. Click here to learn more.

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

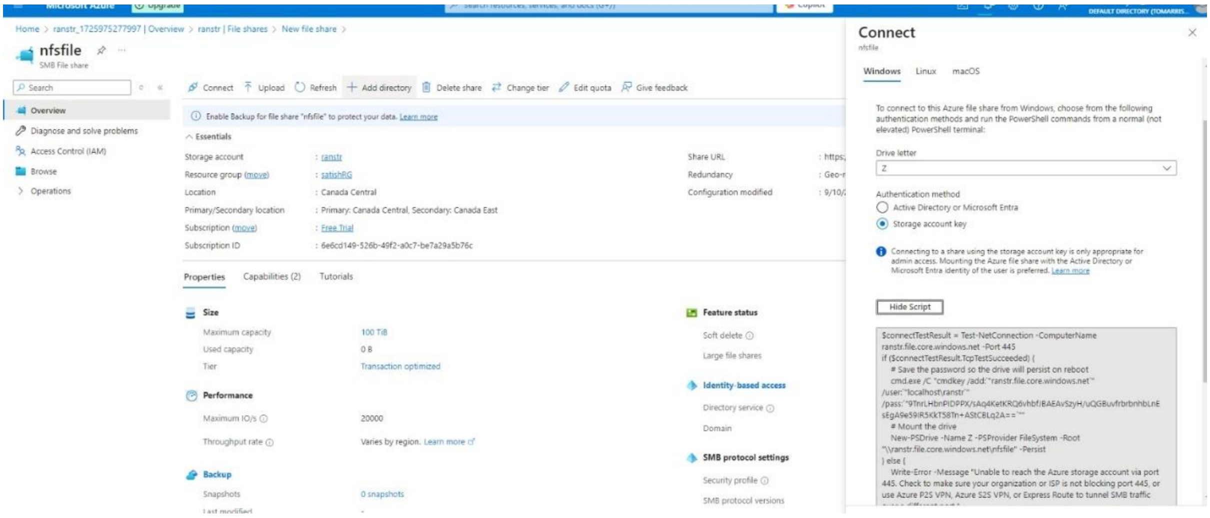
Drive letter: Z

Authentication method
○ Active Directory or Microsoft Entra
● Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory or Microsoft Entra identity of the user is preferred. Learn more

This script will check to see if this storage account is accessible via TCP port 445, which is the port SMB uses. If port 445 is available, your Azure file share will be persistently mounted. Your organization or internet service provider (ISP) may block port 445, however you may use Azure Point-to-Site (P2S) VPN, Azure Site-to-Site (S2S) VPN, or ExpressRoute to tunnel SMB traffic to your Azure file share over a different port.

Note: The script will only work on Windows Server 2012 and above.



Connect
nfsfile

To connect to this Azure file share from Windows, choose from the following authentication methods and run the PowerShell commands from a normal (not elevated) PowerShell terminal:

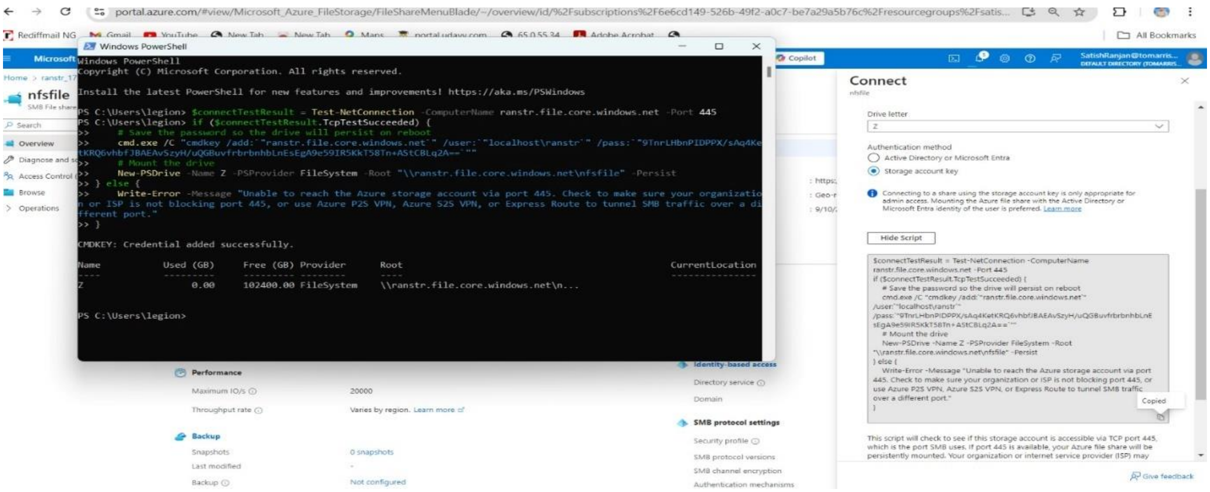
Drive letter: Z

Authentication method
○ Active Directory or Microsoft Entra
● Storage account key

Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory or Microsoft Entra identity of the user is preferred. Learn more

```
$connectTestResult = Test-NetConnection -ComputerName
ranstr.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"ranstr.file.core.windows.net`"
/user:`"localhost\ranstr`"
/pass:`"9TnrLHbnPIDPPX/sAq4KetKRQ6vhbfJBAEAvSzyH/uQGBuvfrbrbnhbLnE
sEgA9e59IR5KkT58Tn+AStCBLq2A==`""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\ranstr.file.core.windows.net\nfsfile" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port
445. Check to make sure your organization or ISP is not blocking port 445, or
use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic
```

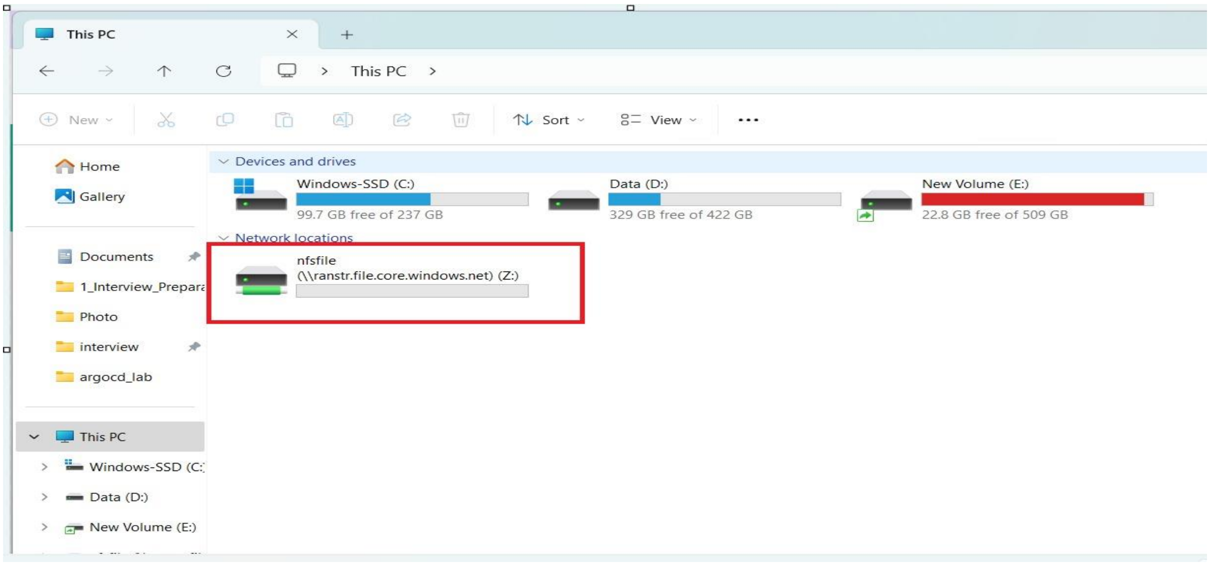
Step9: copy script for windows and run in powershell, we can use a new Azure windows VM or we can use our laptop windows



portal.azure.com/#view/Microsoft_Azure_FileStorage/FileShareMenuBlade/~/overview/id/%2Fsubscriptions%2F6e6cd149-526b-49f2-a0c7-be7a29a5b76c%2Fresourcegroups%2Fsatis...

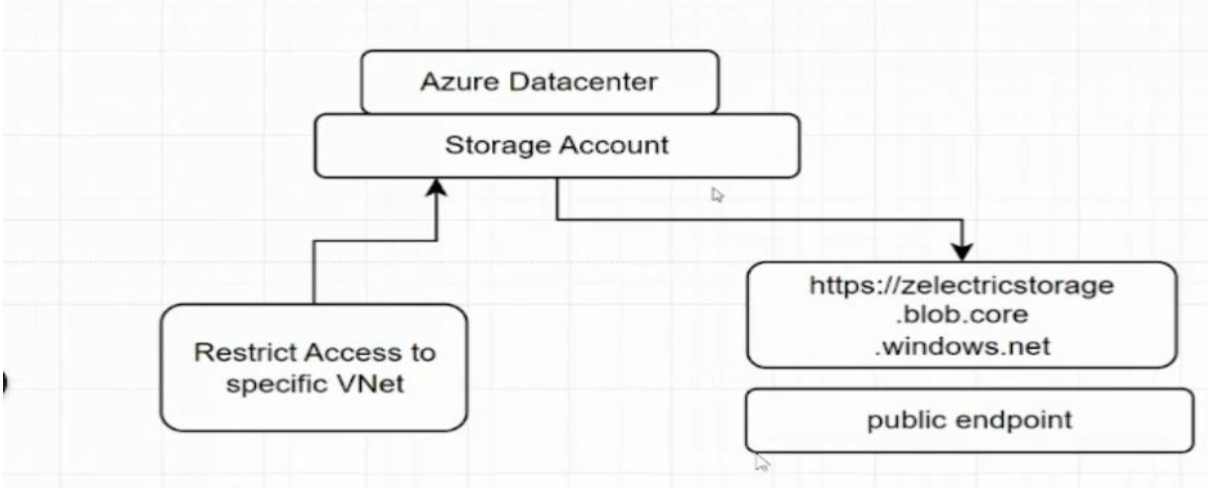
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\legion> $connectTestResult = Test-NetConnection -ComputerName ranstr.file.core.windows.net -Port 445
PS C:\Users\legion> if ($connectTestResult.TcpTestSucceeded) {
>>     # Save the password so the drive will persist on reboot
>>     cmd.exe /C "cmdkey /add:`"ranstr.file.core.windows.net`" /user:`"localhost\ranstr`" /pass:`"9TnrLHbnPIDPPX/sAq4Ke
tKRQ6vhbfJBAEAvSzyH/uQGBuvfrbrbnhbLnEsEgA9e59IR5KkT58Tn+AStCBLq2A==`""
>>     # Mount the drive
>>     New-PSDrive -Name Z -PSProvider FileSystem -Root "\\ranstr.file.core.windows.net\nfsfile" -Persist
>> } else {
>>     Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organizatio
n or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a di
fferent port."
>> }

CMDKEY: Credential added successfully.

Name           Used (GB)     Free (GB) Provider      Root                                               CurrentLocation
----           ---------     --------- --------      ----                                               ---------------
Z                   0.00     102400.00 FileSystem    \\ranstr.file.core.windows.net\n...


PS C:\Users\legion>
```

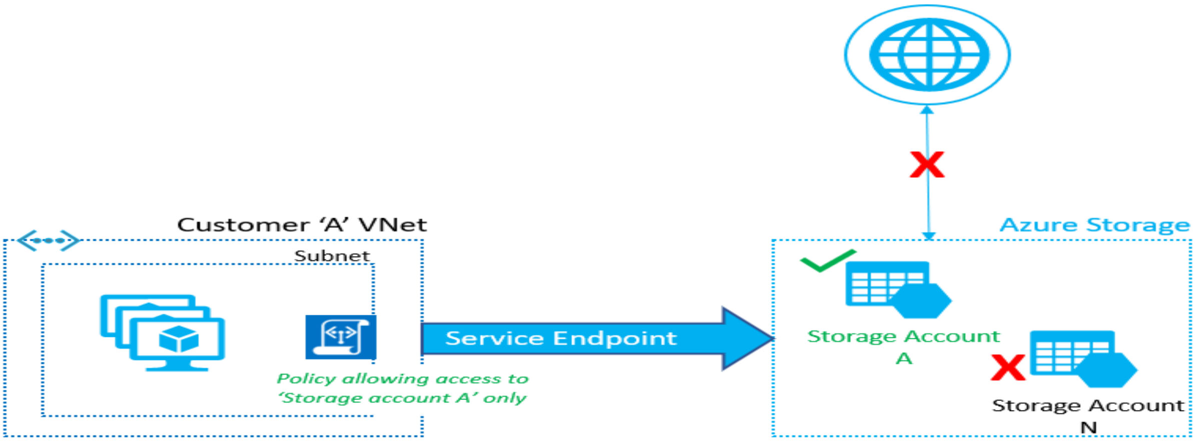
Step10: Now we check in our laptop a new drive showing in devices and drivers in network locations:



Step11: Now our storage container and SMB (Server Message Block) is publicly available

How to Secure our Storage Container and SMB Block by using Service Endpoint


Azure Datacenter
Storage Account
Restrict Access to specific VNet
https://zelectricstorage .blob.core .windows.net
public endpoint



Service Endpoint

1. **Definition**: Service Endpoint ek Azure feature hai jo aapke virtual network (VNet) ko Azure ki specific services se securely connect karta hai.
2. **Kaise Kaam Karta Hai**: Jab aap Service Endpoint enable karte hain, toh aapke VNet ke resources (jaise virtual machines) directly Azure service (jaise Azure Storage, Azure SQL Database) ke saath communicate kar sakte hain. Yeh traffic public internet ke through nahi jata; instead, yeh Azure ki internal backbone network ke through hota hai, jo zyada secure aur reliable hota hai.

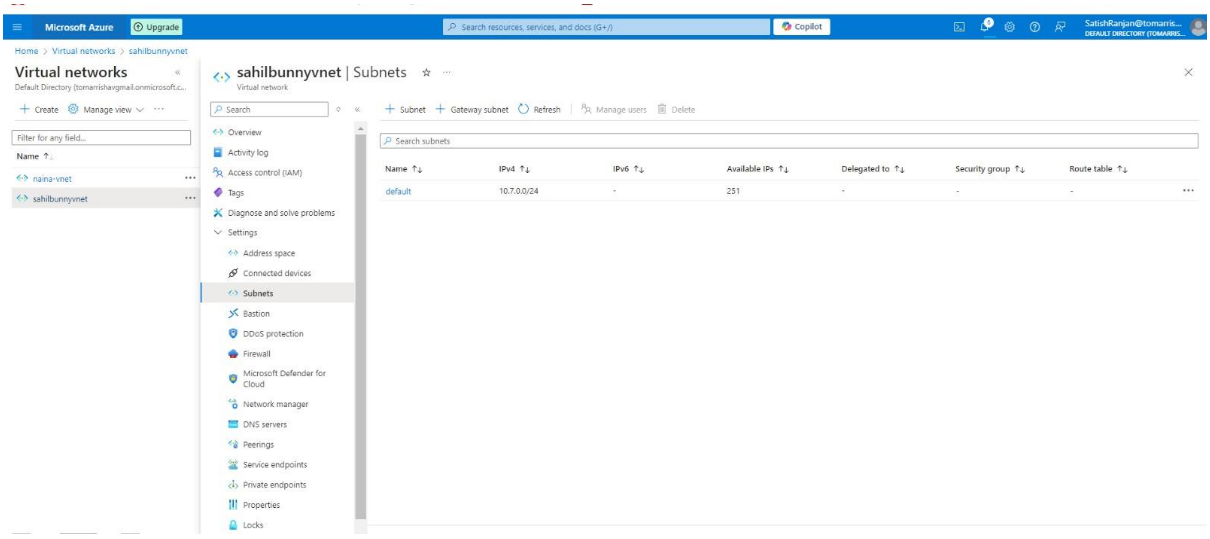
3. **Use Case**: Yeh generally tab use hota hai jab aap chahte hain ki aapke VNet ke resources ek specific Azure service ke saath secure connection banaye bina public internet ka use kiye.

Private Endpoint

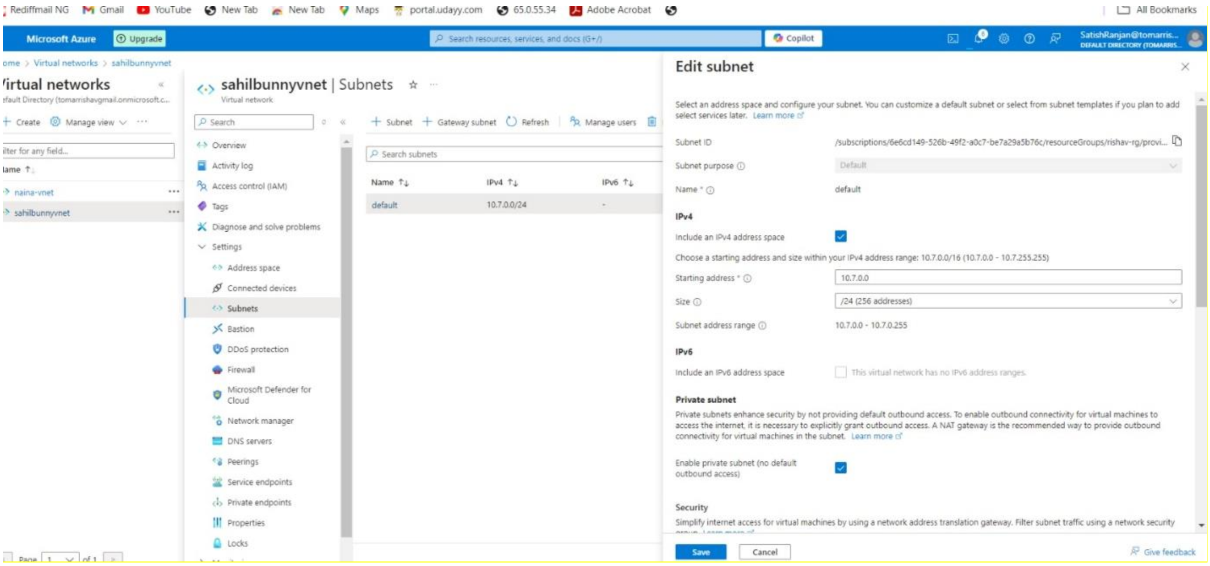
1. **Definition**: Private Endpoint bhi ek Azure feature hai jo aapke VNet ke andar se ek private IP address assign karta hai, jisse aap Azure services ko directly aur securely access kar sakte hain.
2. **Kaise Kaam Karta Hai**: Private Endpoint ke through, Azure service (jaise Azure Storage ya SQL Database) ko aapke VNet ke andar ek private IP address diya jata hai. Iska matlab hai ki aapke VNet ke resources us private IP address ke through service se connect karte hain, jo ki public internet se bilkul bhi interact nahi karta.
3. **Use Case**: Yeh use hota hai jab aap chahte hain ki aapki Azure service ko sirf aapke VNet ke andar se access kiya ja sake aur internet se access nahi ho. Yeh extra security aur data privacy provide karta hai.

Service Endpoint ka use karne ke baad bhi, jo resources hain, wo publicly available hote hain. Yani ki, jab aap Service Endpoint enable karte hain, toh aapke VNet ke resources Azure ki specific service (jaise Azure Storage ya SQL Database) ke saath secure aur direct connection banate hain, lekin woh service abhi bhi public internet se accessible hoti hai.

Step12: First need to create one Subnet inside one VNET



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓
default	10.7.0.0/24	-	251	-	-	-



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓
default	10.7.0.0/24	-

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet ID: /subscriptions/6e6cd149-526b-49f2-a0c7-be7a29a5b76c/resourceGroups/rishav-rg/provi...

Subnet purpose: Default

Name *: default

IPv4

Include an IPv4 address space ☑

Choose a starting address and size within your IPv4 address range: 10.7.0.0/16 (10.7.0.0 - 10.7.255.255)

Starting address *: 10.7.0.0

Size: /24 (256 addresses)

Subnet address range: 10.7.0.0 - 10.7.0.255

IPv6

Include an IPv6 address space □ This virtual network has no IPv6 address ranges.

Private subnet

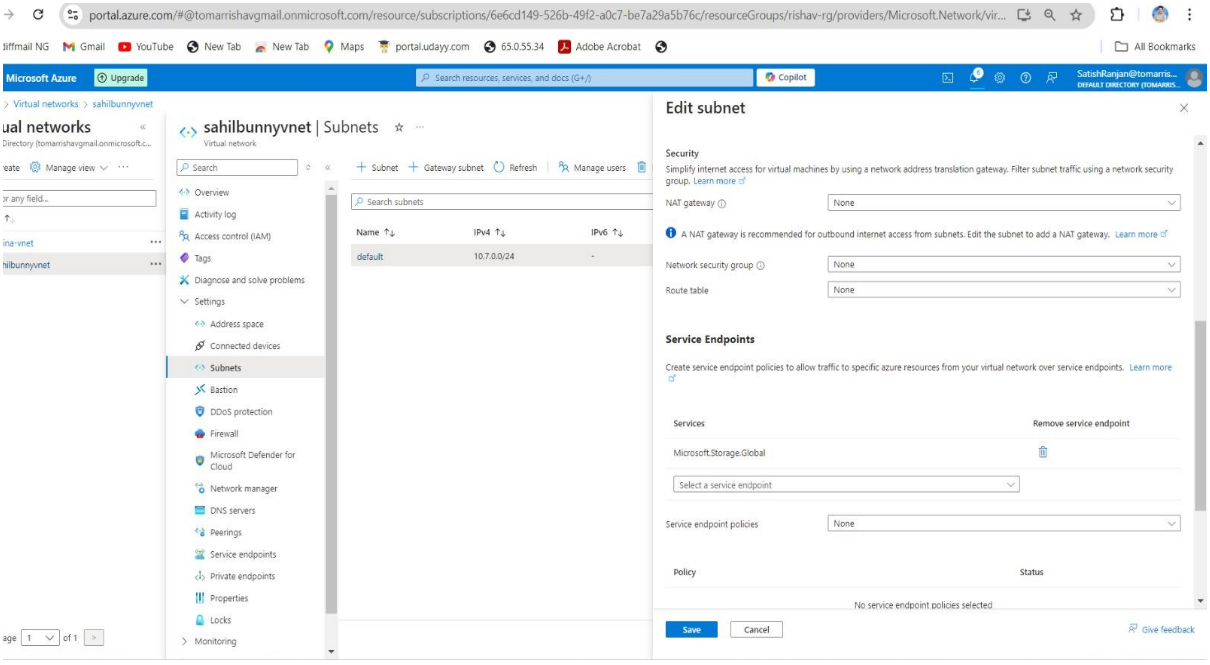
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

Enable private subnet (no default outbound access) ☑

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security

Step13: Need to choose service endpoints for PAAS Services which we want to securely access , here we are choosing Microsoft Storage Global.



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓
default	10.7.0.0/24	-

Edit subnet

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway: None

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more

Network security group: None

Route table: None

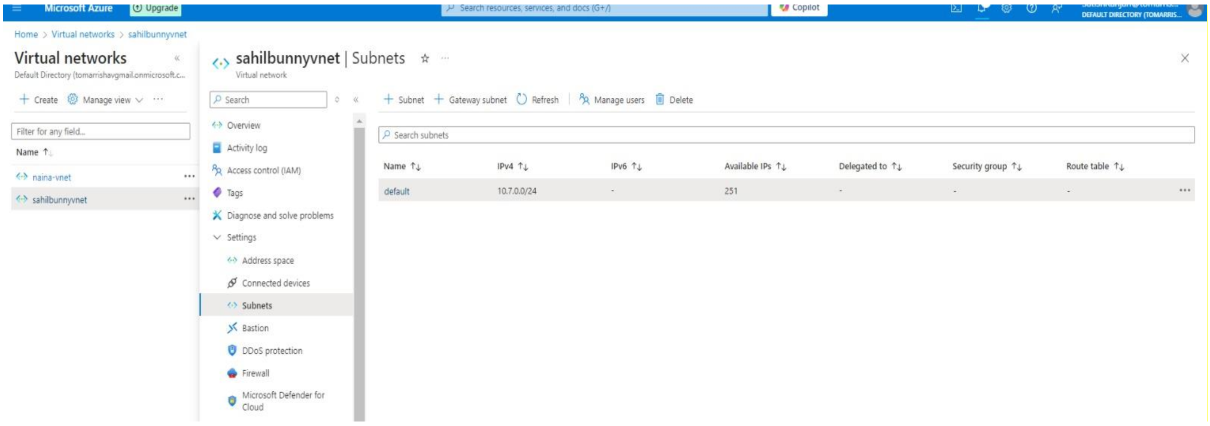
Service Endpoints

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services	Remove service endpoint
Microsoft.Storage.Global	🗑
Select a service endpoint	

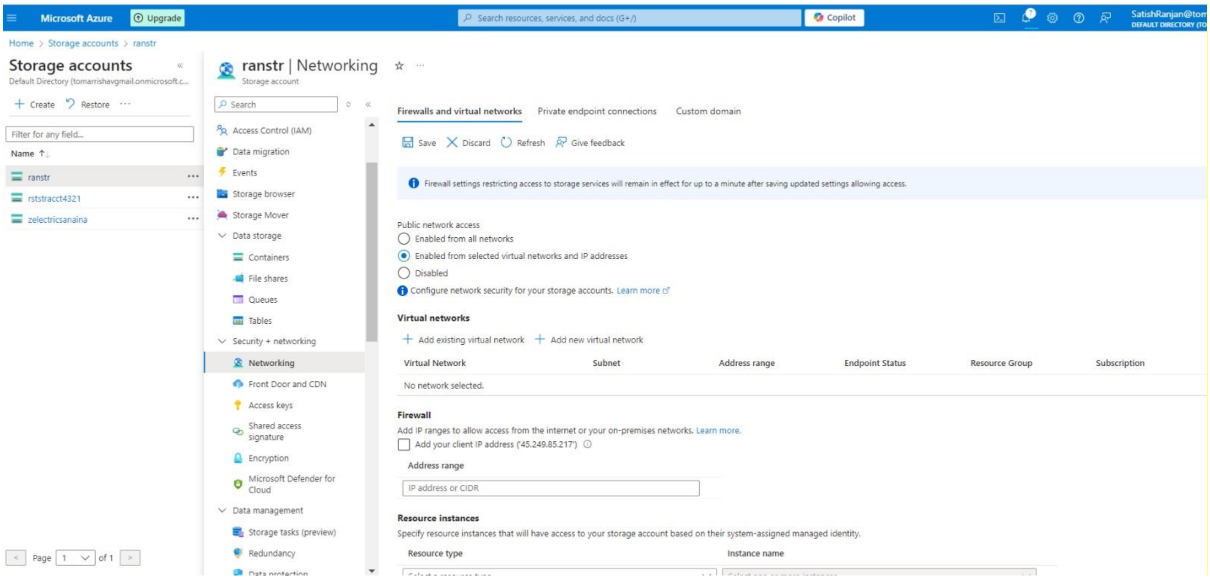
Service endpoint policies: None

Policy	Status
No service endpoint policies selected	



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security group ↑↓	Route table ↑↓
default	10.7.0.0/24	-	251	-	-	-

Step14: Now need to go to Storage account, select our storage account and go to networking , then select vnet and subnet which we created for servicepoint



Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

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
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

□ Add your client IP address ('45.249.85.217')

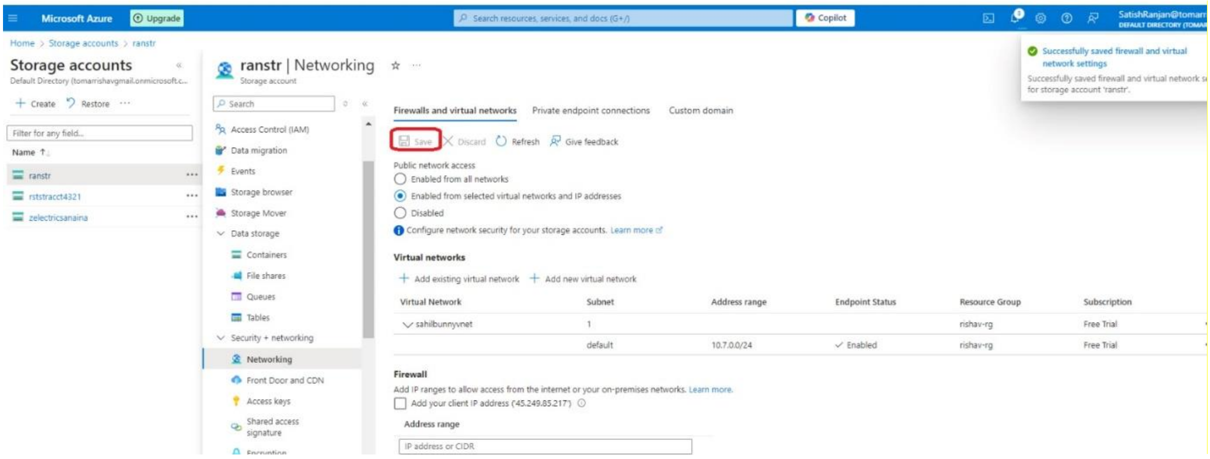
Address range

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



Successfully saved firewall and virtual network settings

Successfully saved firewall and virtual network s for storage account 'ranstr'.

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
sahilbunnyvnet	1			rishav-rg	Free Trial
	default	10.7.0.0/24	✓ Enabled	rishav-rg	Free Trial

Firewall

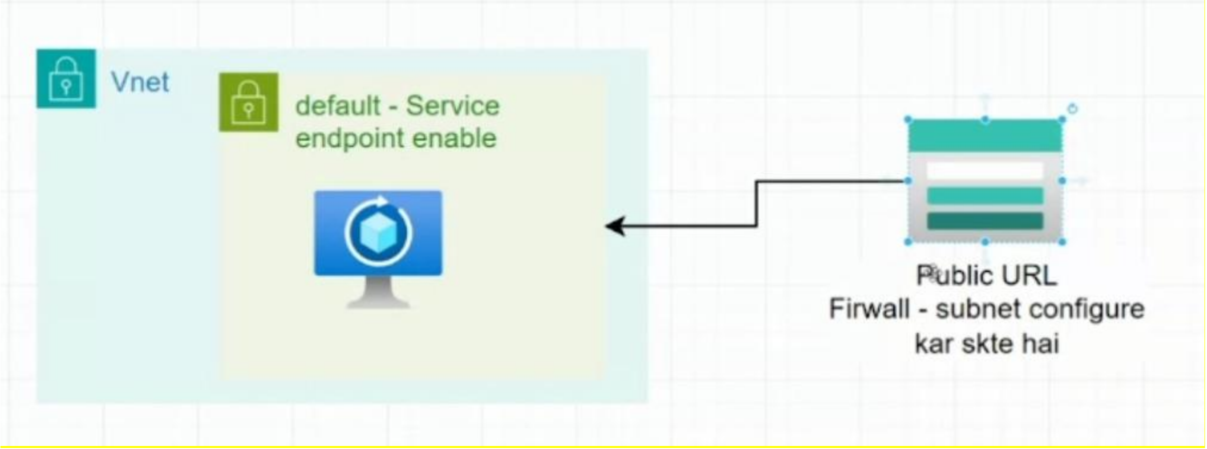
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.

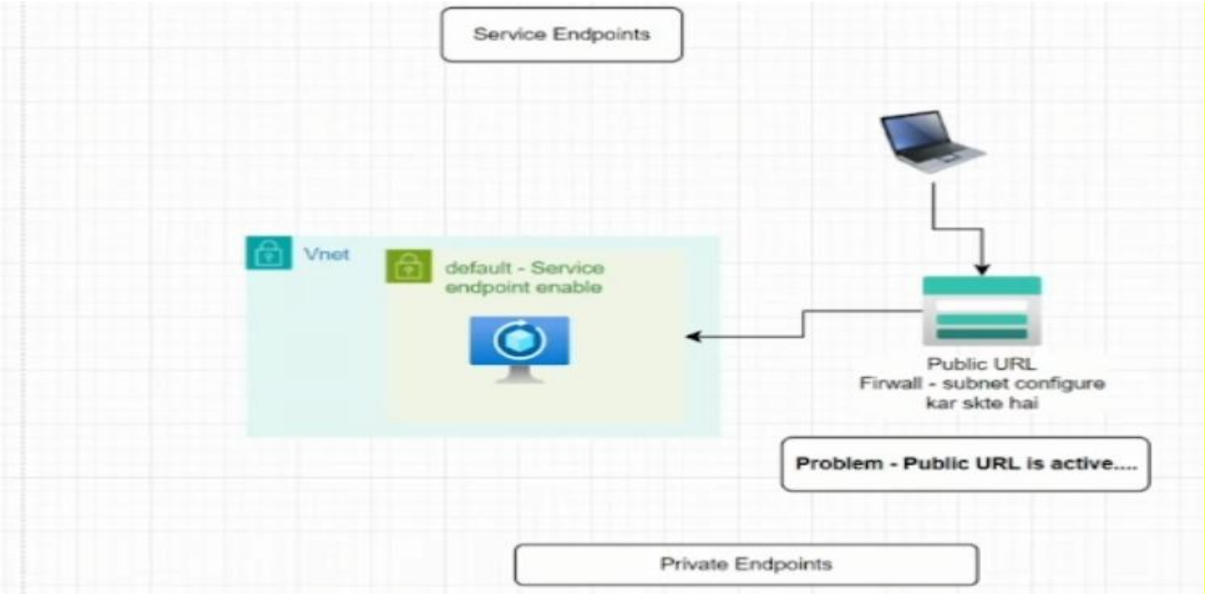
□ Add your client IP address ('45.249.85.217')

Address range

IP address or CIDR

Step15: Now need to create one VM in same subnet which we already created in same subnet.


Vnet
default - Service endpoint enable
Public URL
Firwall - subnet configure kar skte hai


Service Endpoints
Vnet
default - Service endpoint enable
Public URL
Firwall - subnet configure kar skte hai
Problem - Public URL is active....
Private Endpoints

Step16: Now our storage container image is not accessible from internet publicly, it only accessible from VM which present in same subnet where service endpoint exist. For this we need to install Storage service explorer in VM and then try to connect and try to access our container image , it accessible publicly as well as we can connect through apps.