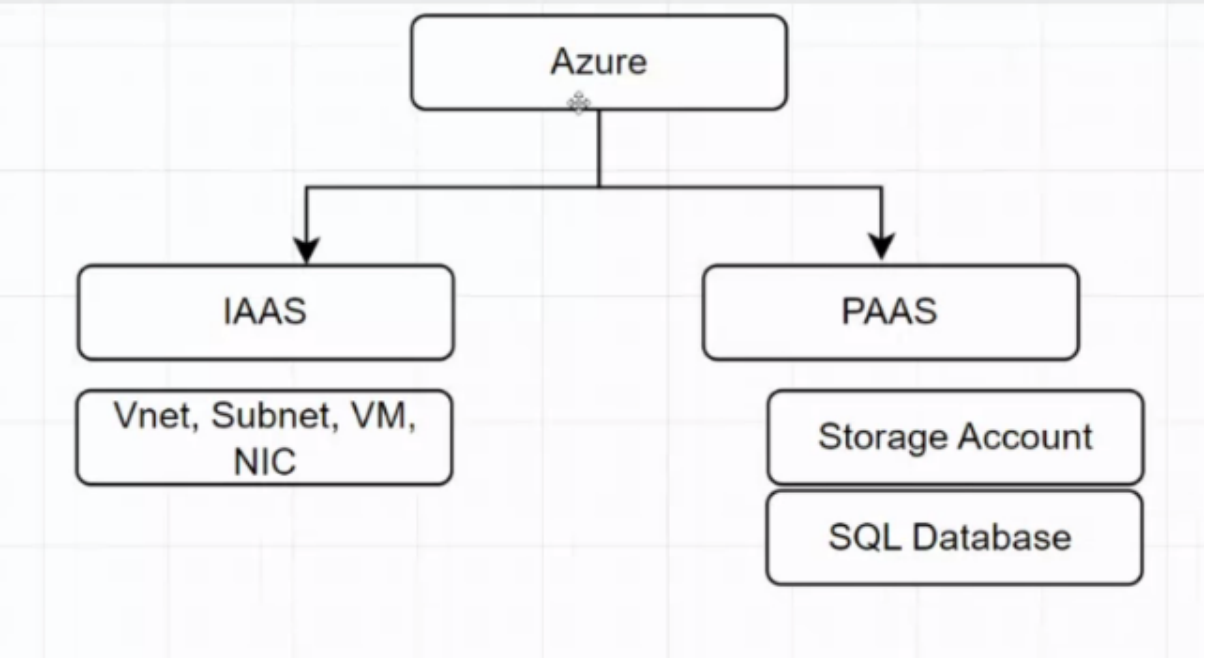
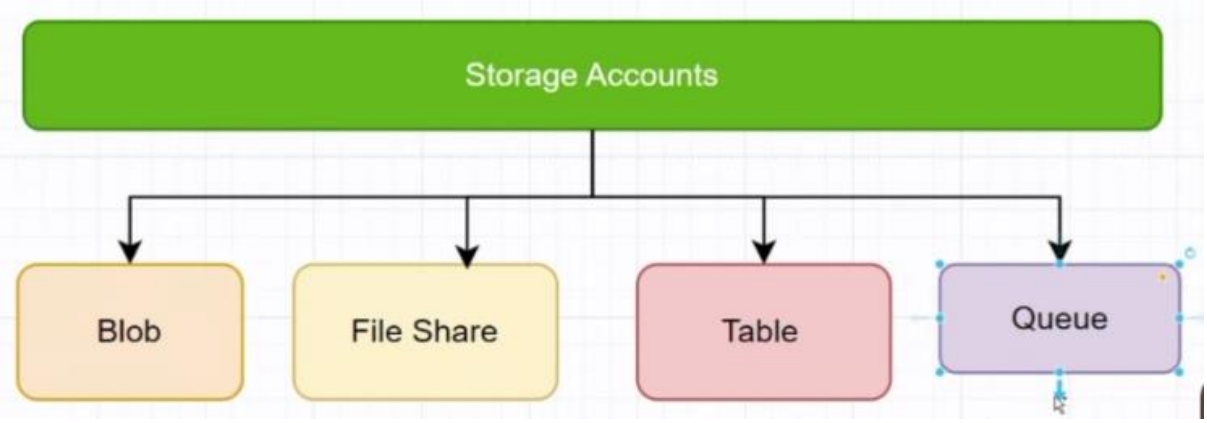
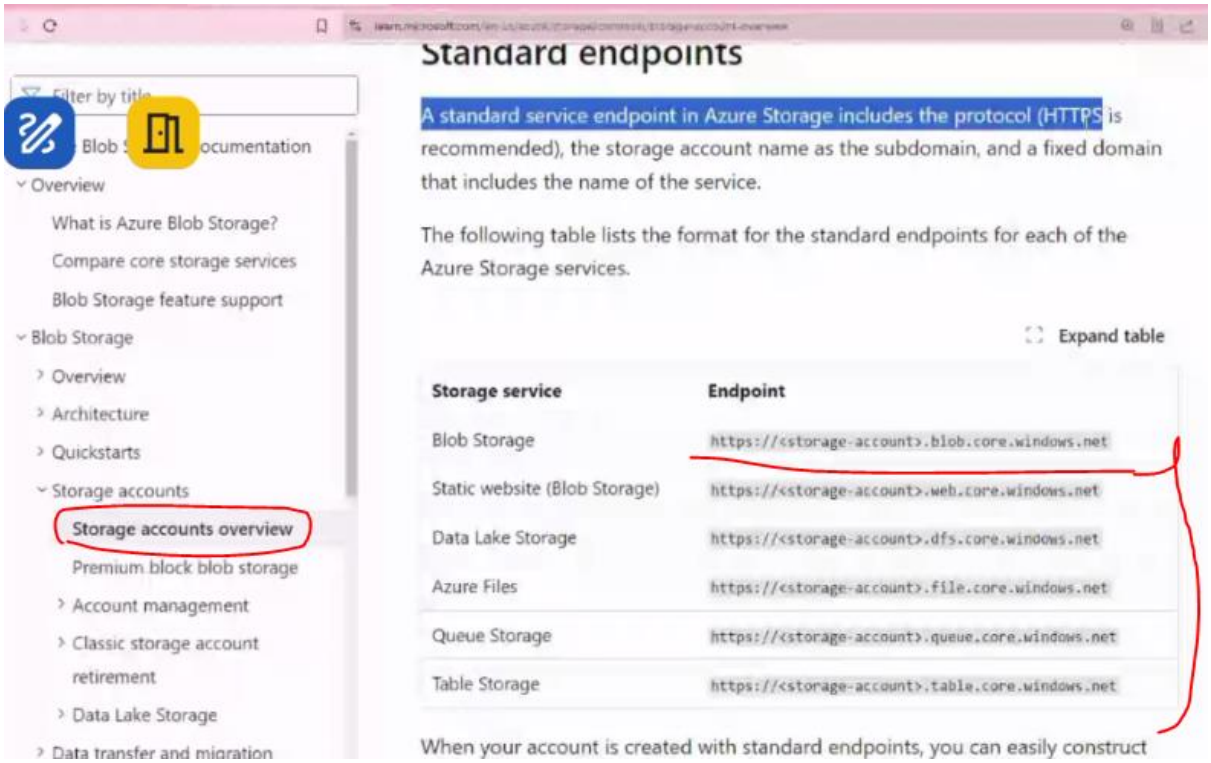
8 sept

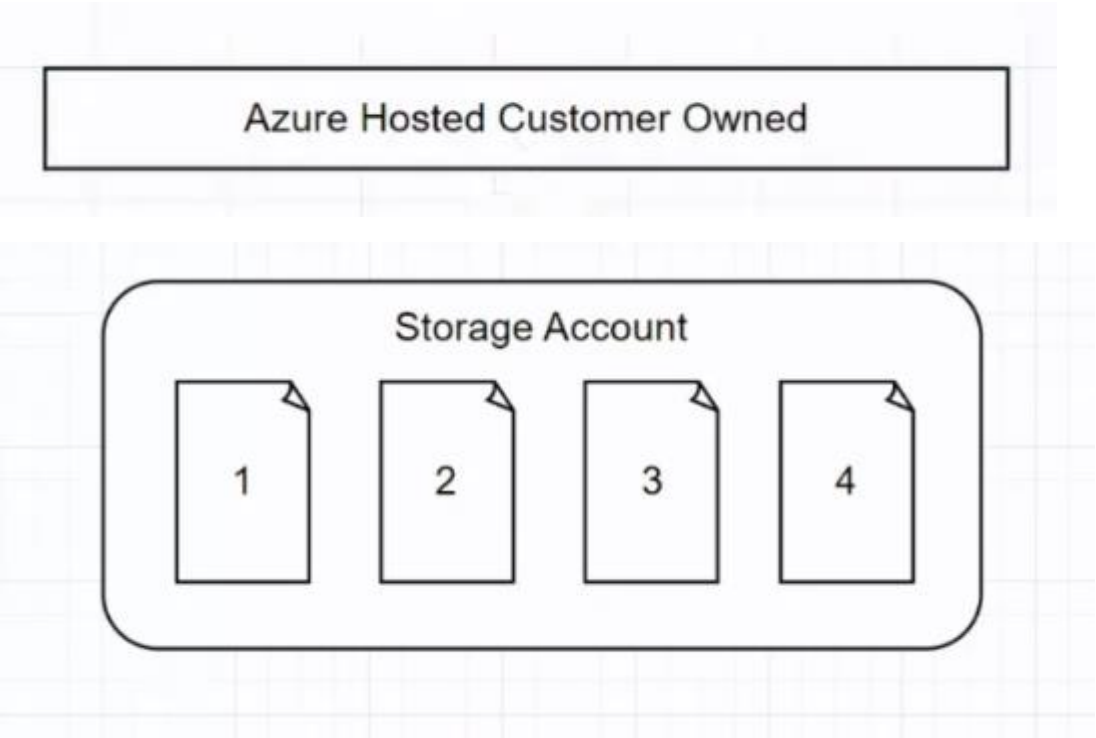


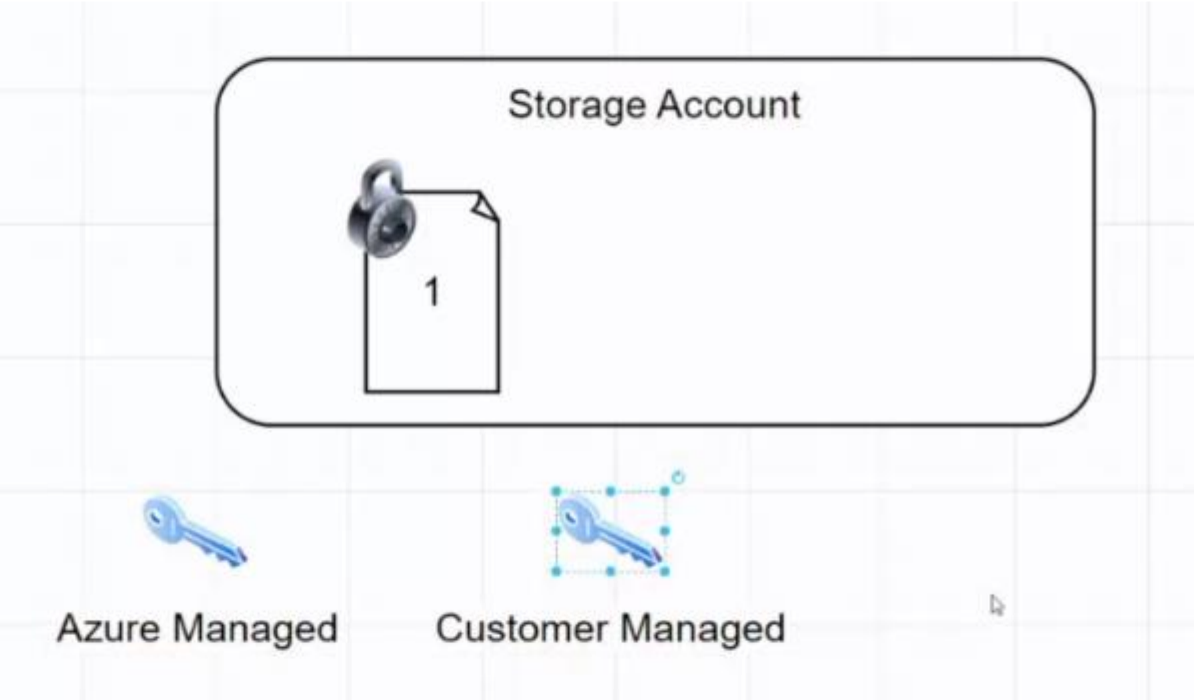


3) Urls for different storages


Standard endpoints
Filter by title
Blob S ocumentation
Overview
What is Azure Blob Storage?
Compare core storage services
Blob Storage feature support
Blob Storage
Overview
Architecture
Quickstarts
Storage accounts
Storage accounts overview
Premium block blob storage
Account management
Classic storage account retirement
Data Lake Storage
Data transfer and migration
A standard service endpoint in Azure Storage includes the protocol (HTTPS is recommended), the storage account name as the subdomain, and a fixed domain that includes the name of the service.
The following table lists the format for the standard endpoints for each of the Azure Storage services.
Expand table
Storage service
Endpoint
Blob Storage
https://<storage-account>.blob.core.windows.net
Static website (Blob Storage)
https://<storage-account>.web.core.windows.net
Data Lake Storage
https://<storage-account>.dfs.core.windows.net
Azure Files
https://<storage-account>.file.core.windows.net
Queue Storage
https://<storage-account>.queue.core.windows.net
Table Storage
https://<storage-account>.table.core.windows.net
When your account is created with standard endpoints, you can easily construct

4)

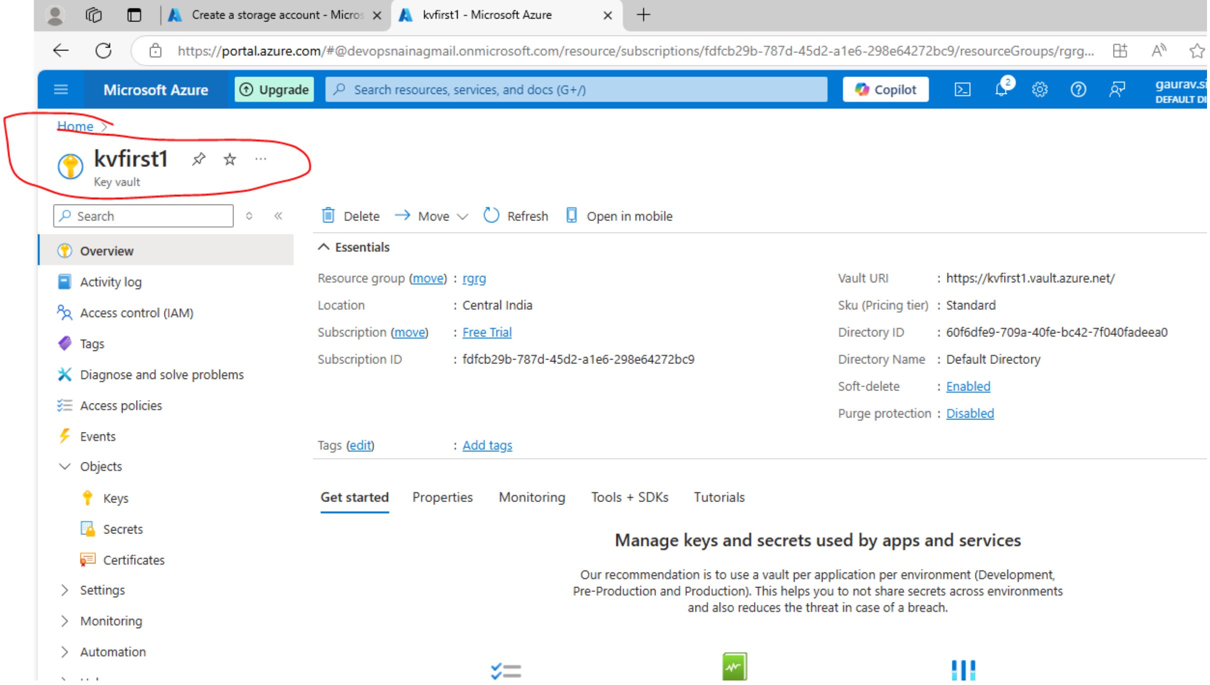

Azure Hosted Customer Owned
Storage Account
1
2
3
4



+++

AGENDA – Creating keyvault

1)



Resource group (move) : rgrg
Location : Central India
Subscription (move) : Free Trial
Subscription ID : fdfcb29b-787d-45d2-a1e6-298e64272bc9
Vault URI : https://kvfirst1.vault.azure.net/
Sku (Pricing tier) : Standard
Directory ID : 60f6dfe9-709a-40fe-bc42-7f040fadeea0
Directory Name : Default Directory
Soft-delete : Enabled
Purge protection : Disabled
Tags (edit) : Add tags

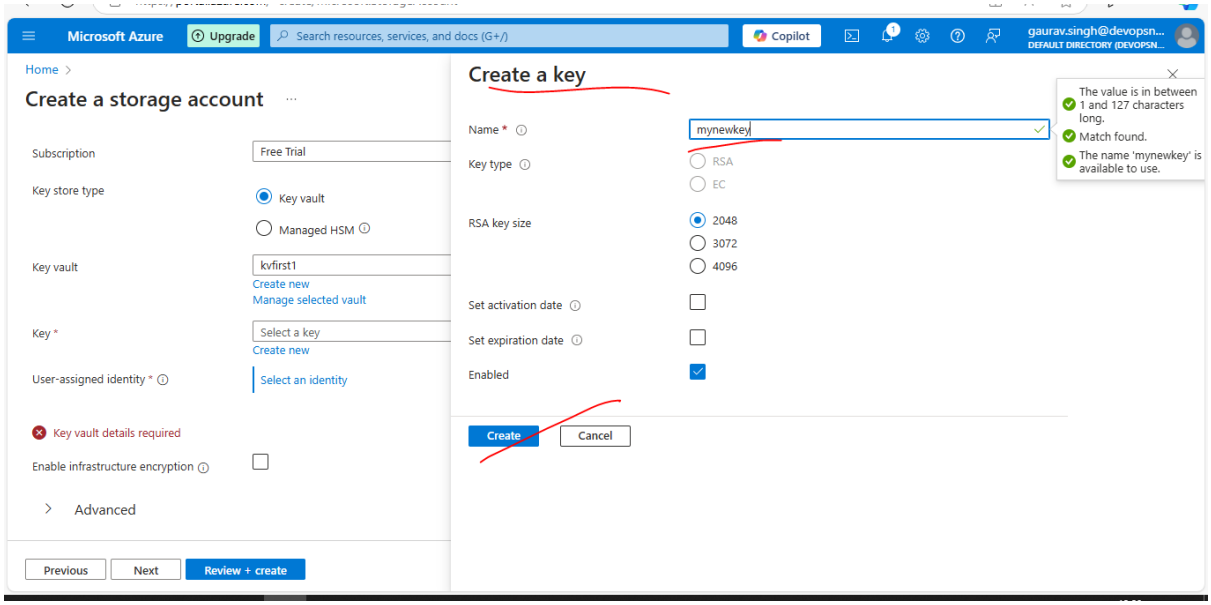
Manage keys and secrets used by apps and services

Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.

+++

AGENDA – Creating Storage account

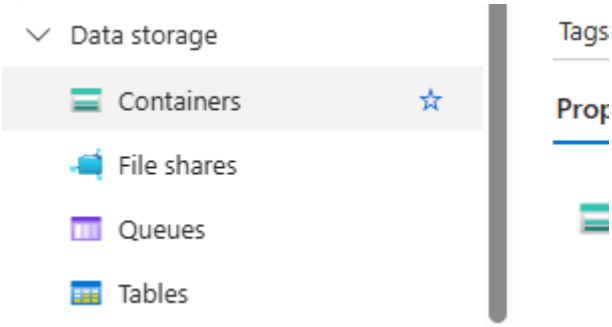
1)



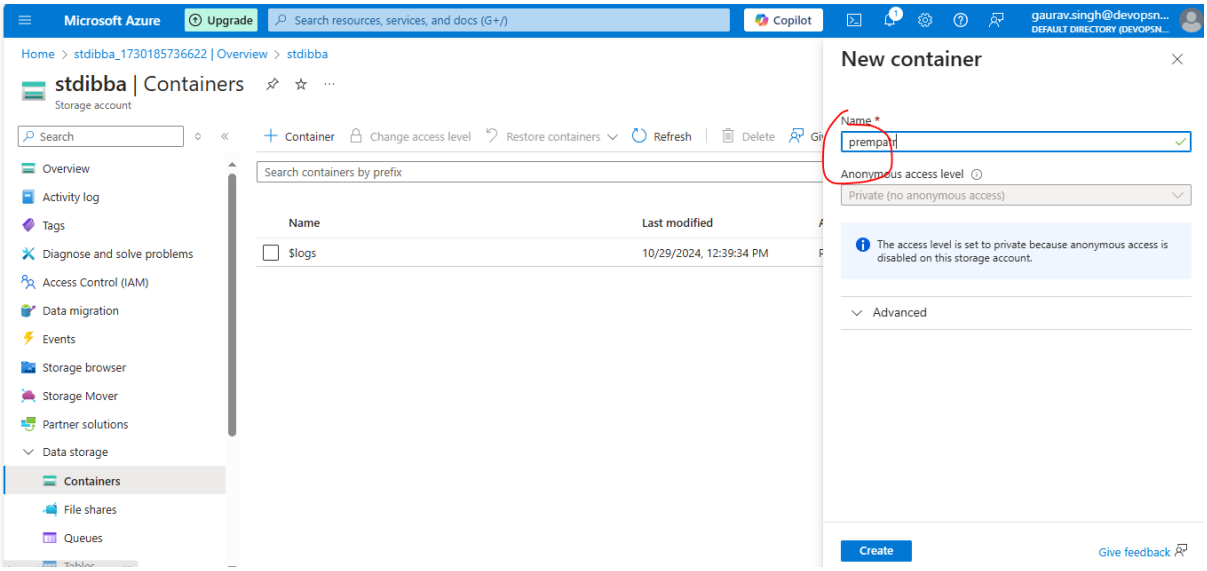
There are two types of encrpytions keys in azure - One is MMK and CMK. CMK is more secure. For using CMK, A new key is created and stored in key vault and the storage account is given access to the key stored in the key vault using managed identities.

Using CMK we can do disk encryption also.

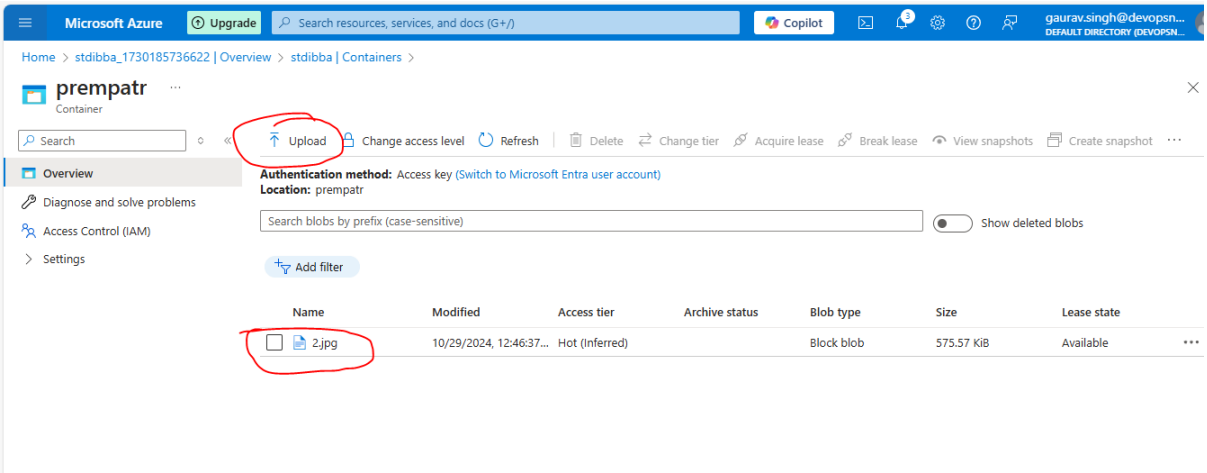
2) So now we can see all four services



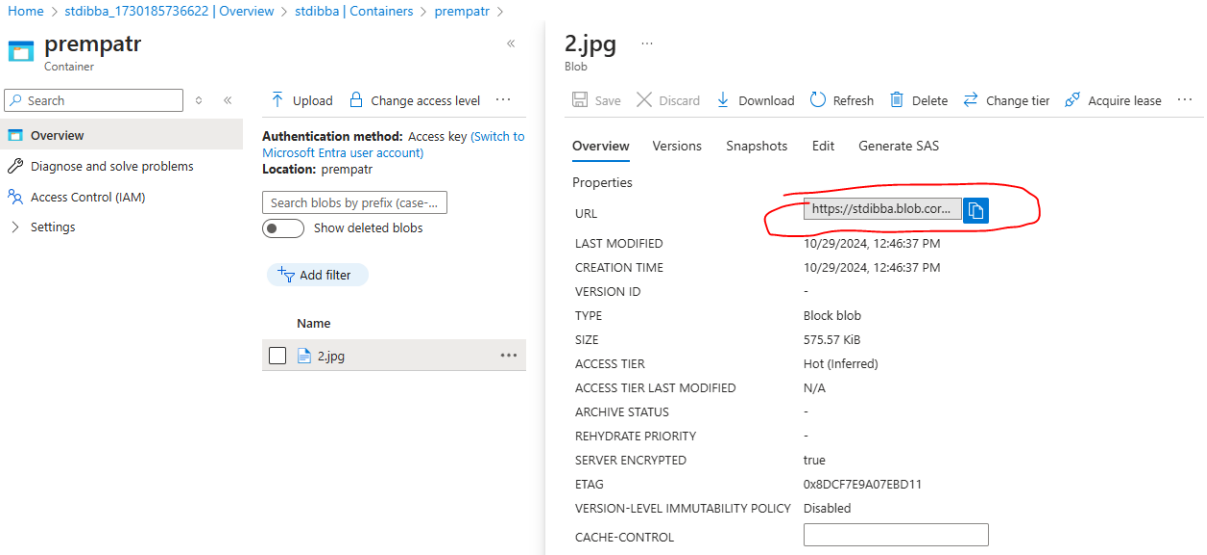
3) Now create a container



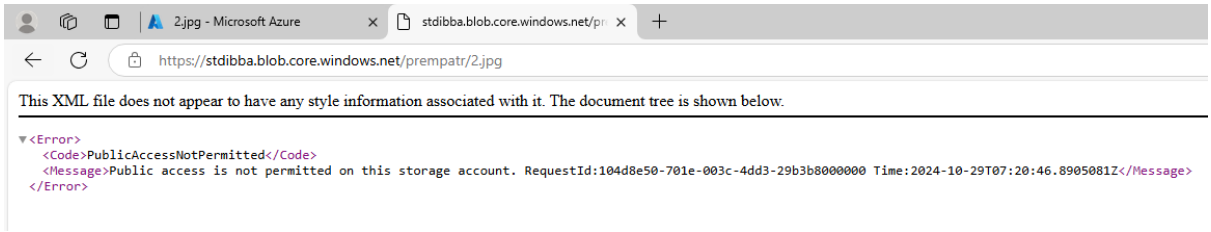
4) Now uploading a file in container from local



5) Now if we click on it then we will get url same it was told in general in document



https://stdibba.blob.core.windows.net/prempatr/2.jpg

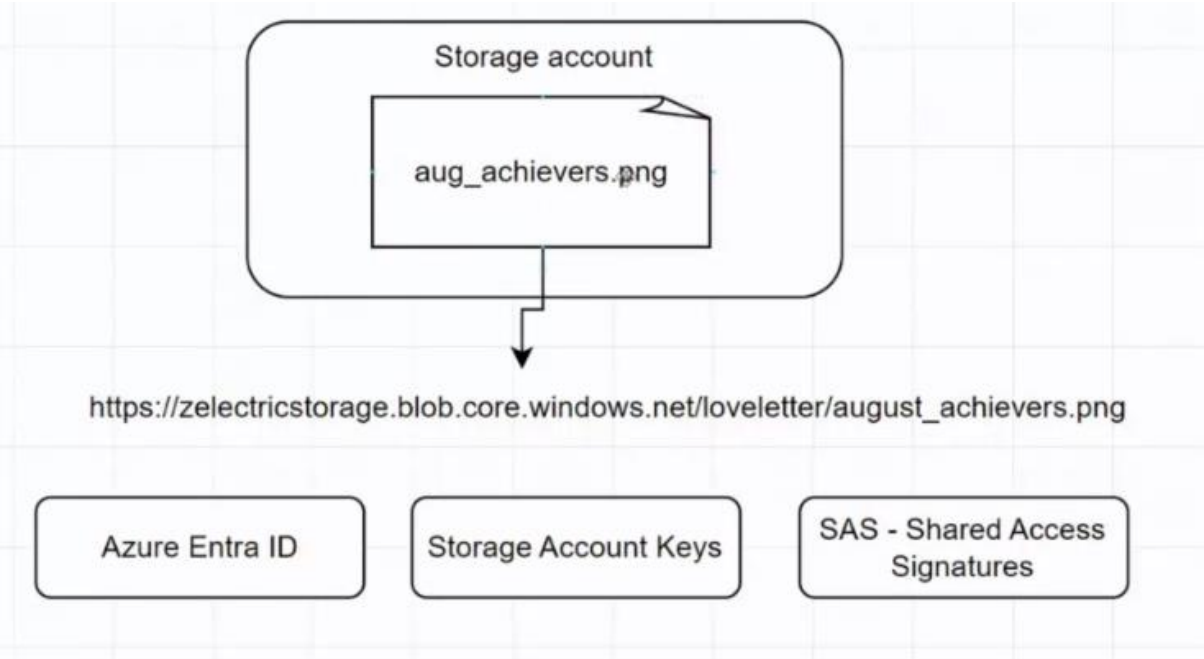


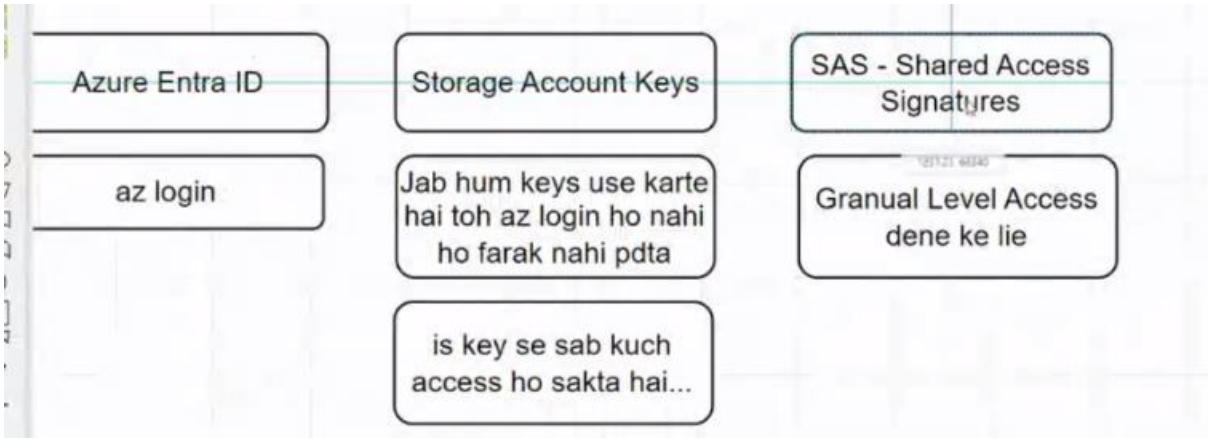
6) So we are unable to access that image using url because we don't have the permission to access it publicly. We can use below methods to access

i) Azure Entra ID

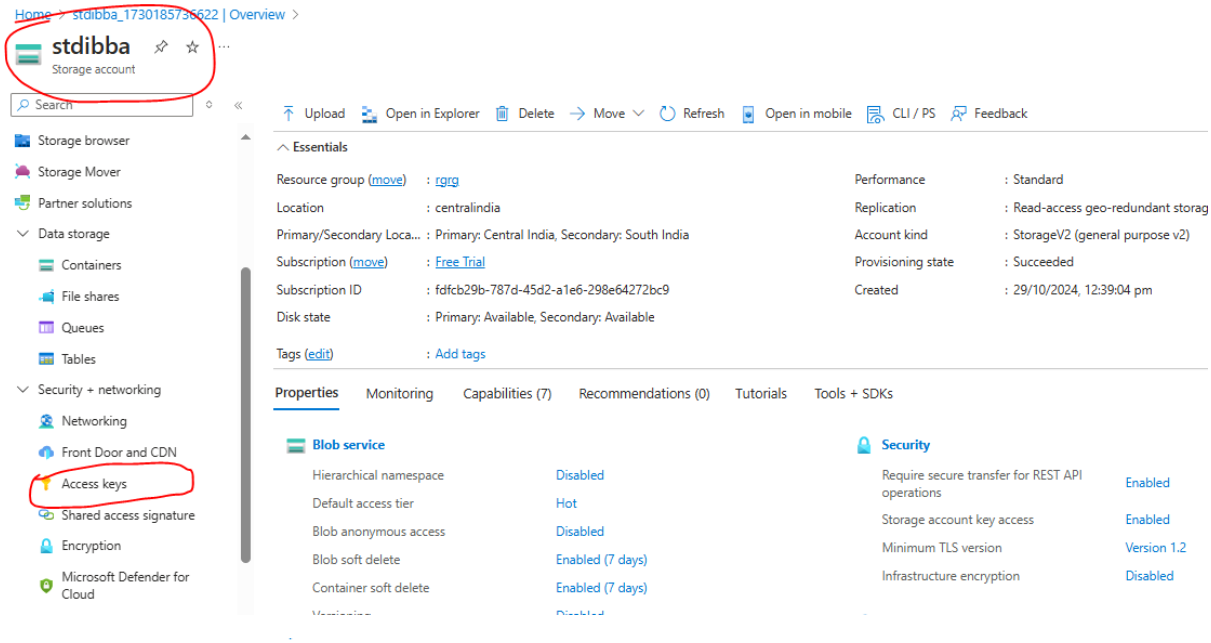
ii) Storage account keys

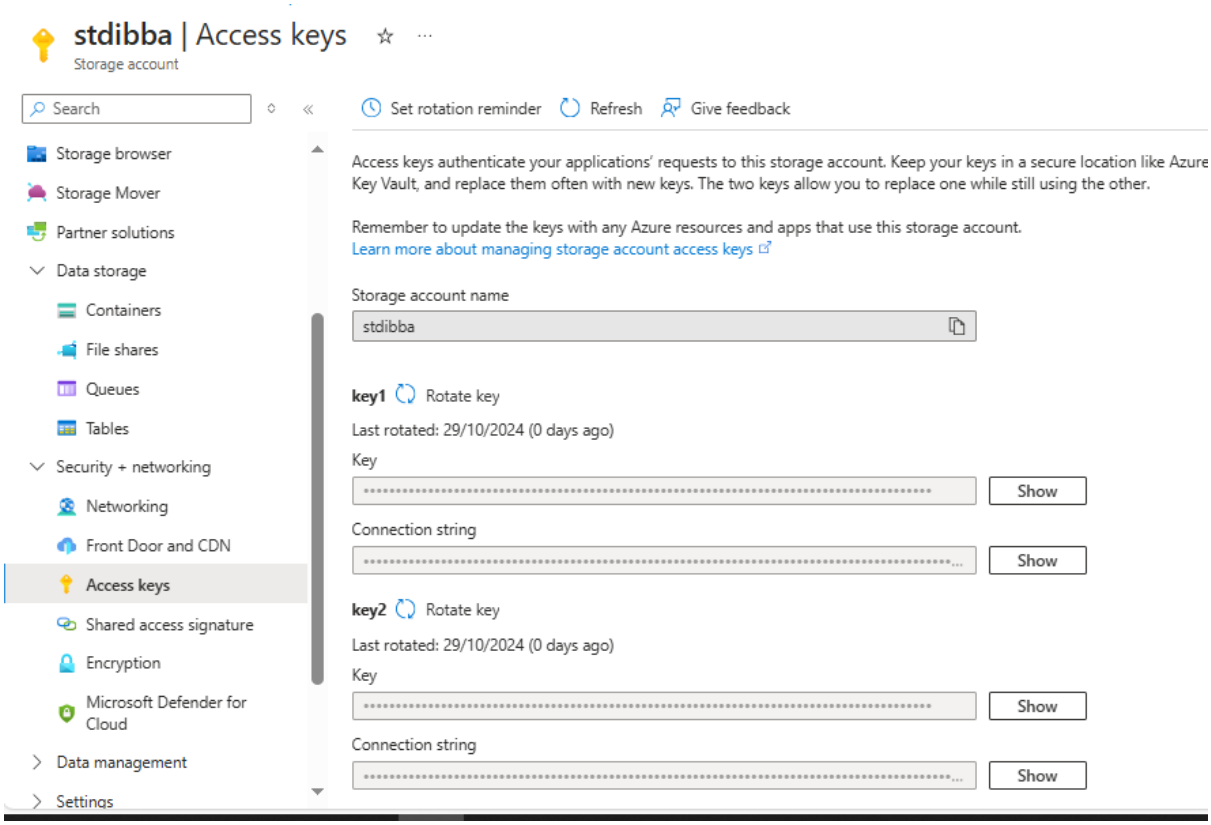
iii) SAS – Shared access signatures





7) So we have access keys in storage account to access its data





8) Inside container we can “Generate SAS” to give access at granular level

Microsoft Azure | Upgrade | Search resources, services, and docs (G+/) | Copilot

Home > stdibba_1730185736622 | Overview > stdibba | Containers > prempatr >

prempatr
Container

Search

- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Settings

Upload | Change access level

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

Search blobs by prefix (case-...

Show deleted blobs

Add filter

Name
2.jpg

2.jpg
Blob

Save | Discard | Download | Refresh | Delete | Change tier | Acquire lease

Overview | Versions | Snapshots | Edit | Generate SAS

Properties

URL	https://stdibba.blob.cor...
LAST MODIFIED	10/29/2024, 12:46:37 PM
CREATION TIME	10/29/2024, 12:46:37 PM
VERSION ID	-
TYPE	Block blob
SIZE	575.57 KiB
ACCESS TIER	Hot (Inferred)
ACCESS TIER LAST MODIFIED	N/A
ARCHIVE STATUS	-
REHYDRATE PRIORITY	-
SERVER ENCRYPTED	true
ETAG	0x8DCF7E9A07EBD11
VERSION-LEVEL IMMUTABILITY POLICY	Disabled
CACHE-CONTROL	
CONTENT-TYPE	image/jpeg
CONTENT-MD5	mqnN8ZwqDbEnTOes1YnGG

Home > stdibba_1730185736622 | Overview > stdibba | Containers > prempatr >

prempatr
Container

Search

- Overview
- Diagnose and solve problems
- Access Control (IAM)
- Settings

Upload | Change access level

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

Search blobs by prefix (case...

Show deleted blobs

Add filter

Name
2.jpg

2.jpg
Blob

Save | Discard | Download | Refresh | Delete

Overview | Versions | Snapshots | Edit | Generate SAS

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 stor
about creating an account SAS

Signing method
(•) Account key ( ) User delegation key

Signing key
Key 1

Stored access policy
None

Permissions
8 selected

Start and expiry date/time

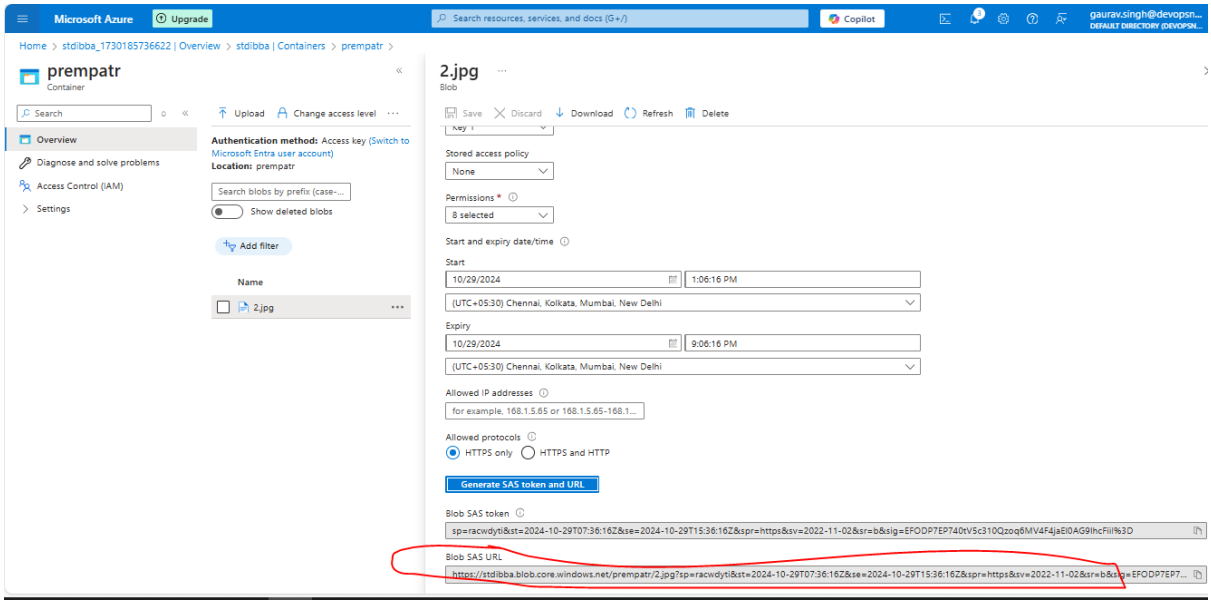
Start
10/29/2024 | 1:06:16 PM
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Expiry
10/29/2024 | 9:06:16 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



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

Stored access policy: None

Permissions *: 8 selected

Start and expiry date/time

Start: 10/29/2024 1:06:16 PM (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Expiry: 10/29/2024 9:06:16 PM (UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

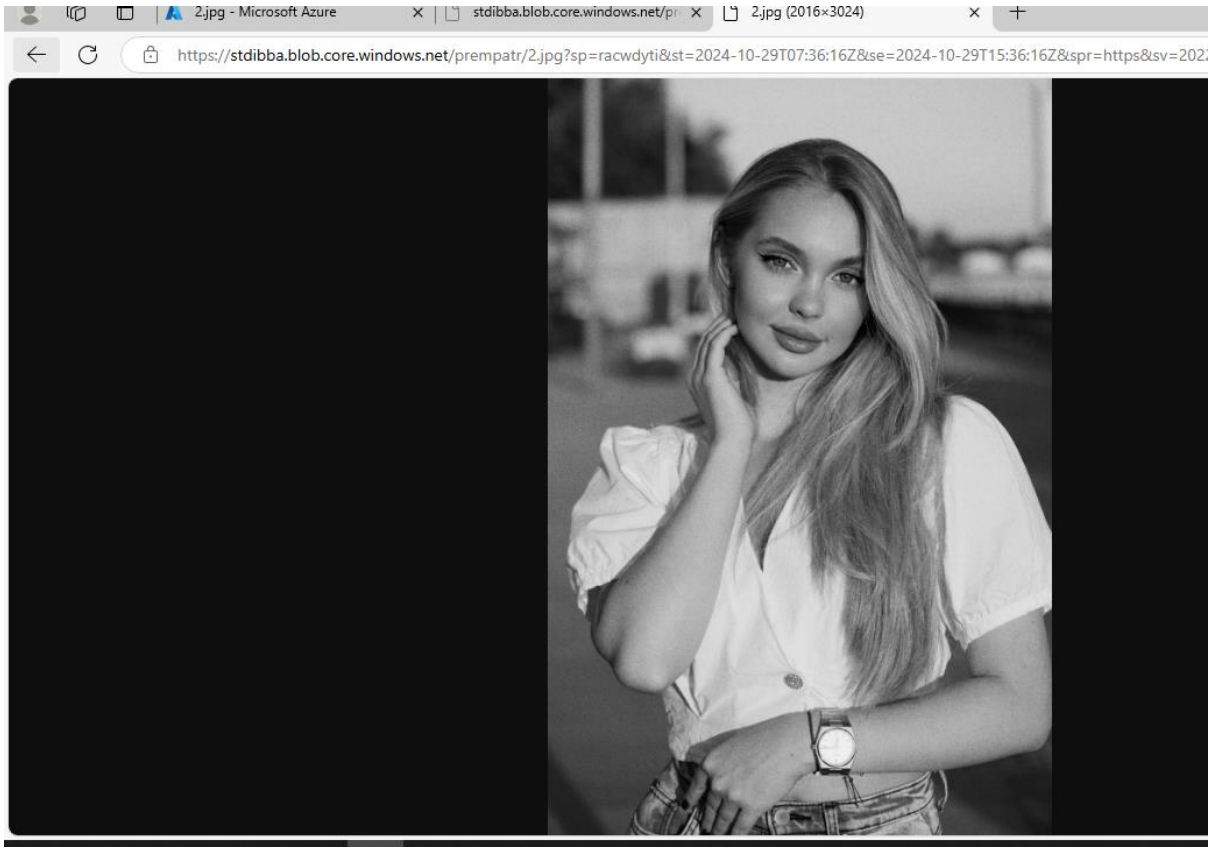
Allowed IP addresses: for example, 168.1.5.65 or 168.1.5.65-168.1...

Allowed protocols: ● HTTPS only ○ HTTPS and HTTP

Blob SAS token: sp=racwdyti&st=2024-10-29T07:36:16Z&se=2024-10-29T15:36:16Z&spr=https&sv=2022-11-02&sr=b&sig=EFODP7EP740tV5c310Qzoq6MV4F4jaEI0AG9lhcFiil%3D

Blob SAS URL: https://stdibba.blob.core.windows.net/prempatr/2.jpg?sp=racwdyti&st=2024-10-29T07:36:16Z&se=2024-10-29T15:36:16Z&spr=https&sv=2022-11-02&sr=b&sig=EFODP7EP7...

9) Using above url we can access now the data in container



https://stdibba.blob.core.windows.net/prempatr/2.jpg?sp=racwdyti&st=2024-10-29T07:36:16Z&se=2024-10-29T15:36:16Z&spr=https&sv=202

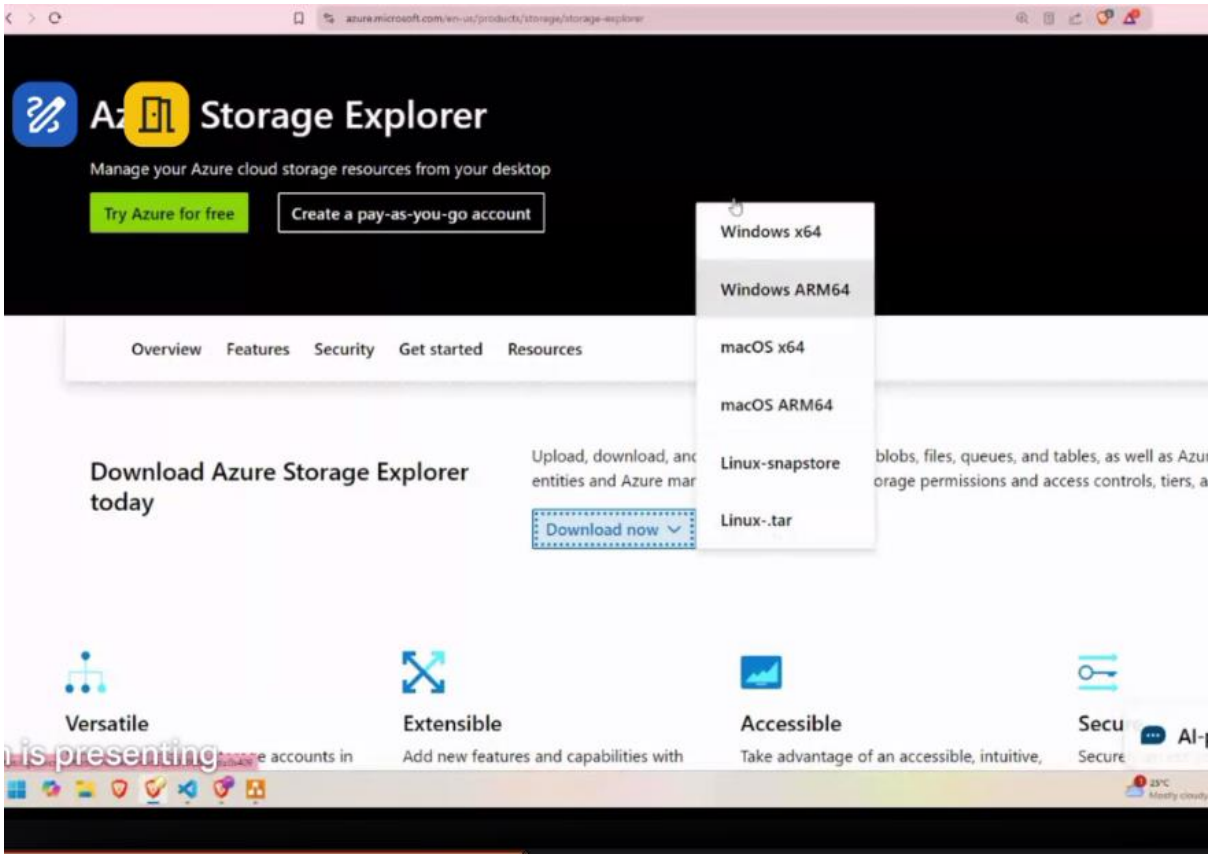
10) So as per interview if we have to provide access to any user for 2 hours then we can use Generate SAS method in container.

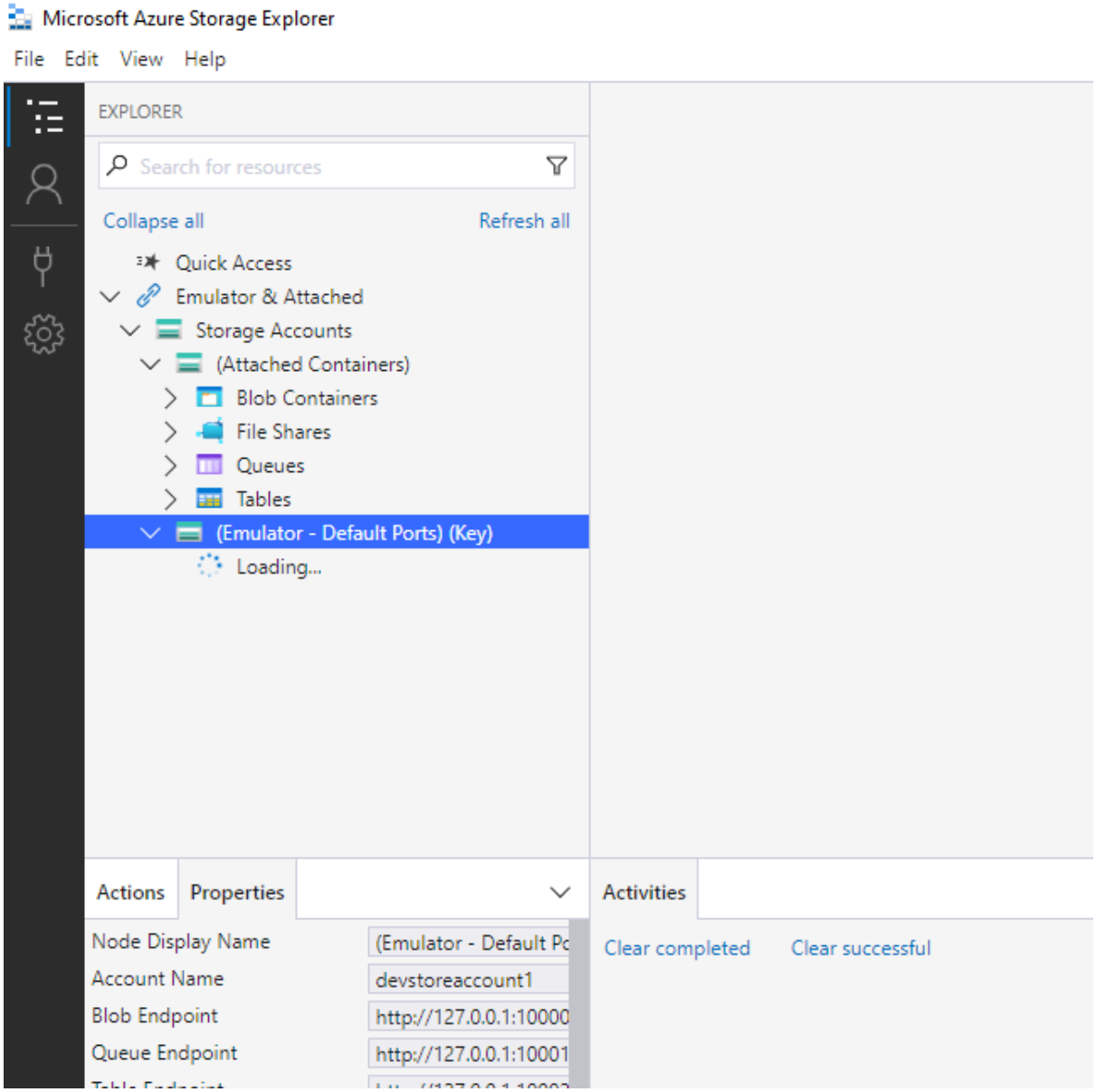
++

AGENDA – STORAGE EXPLORER – a more better method

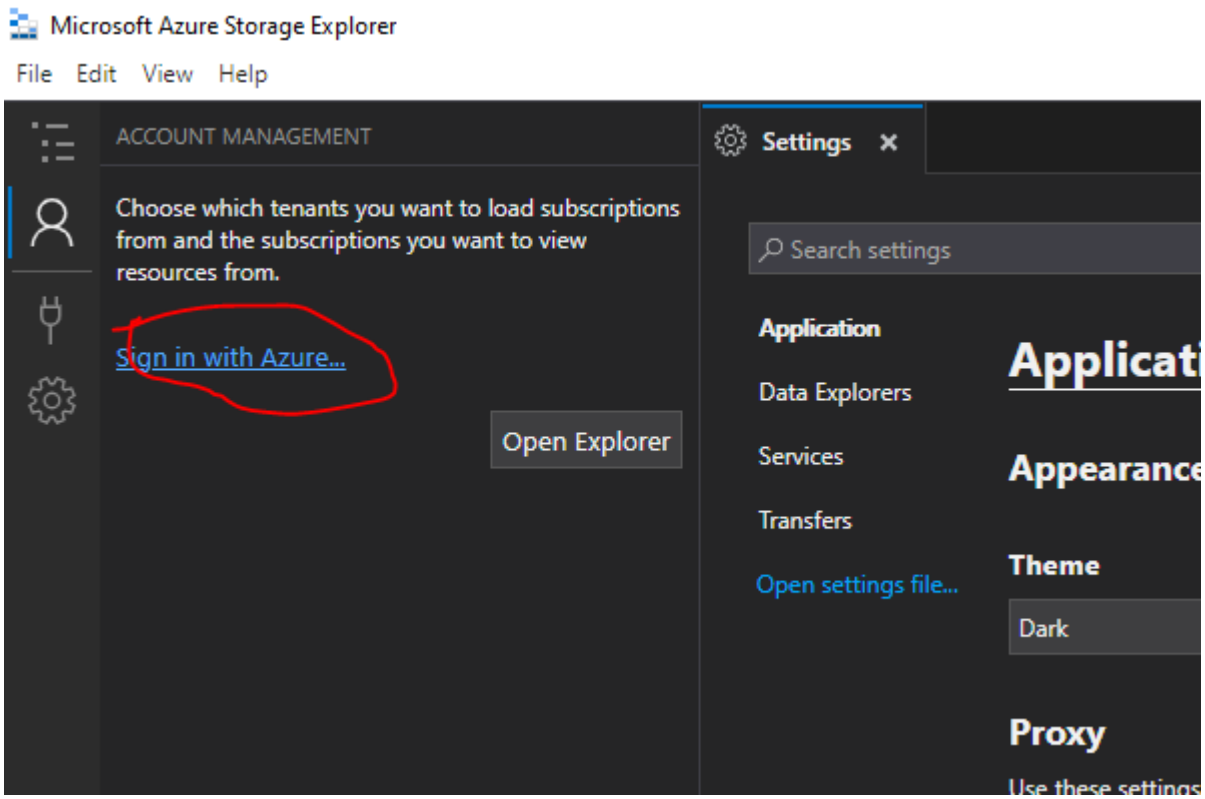
1)

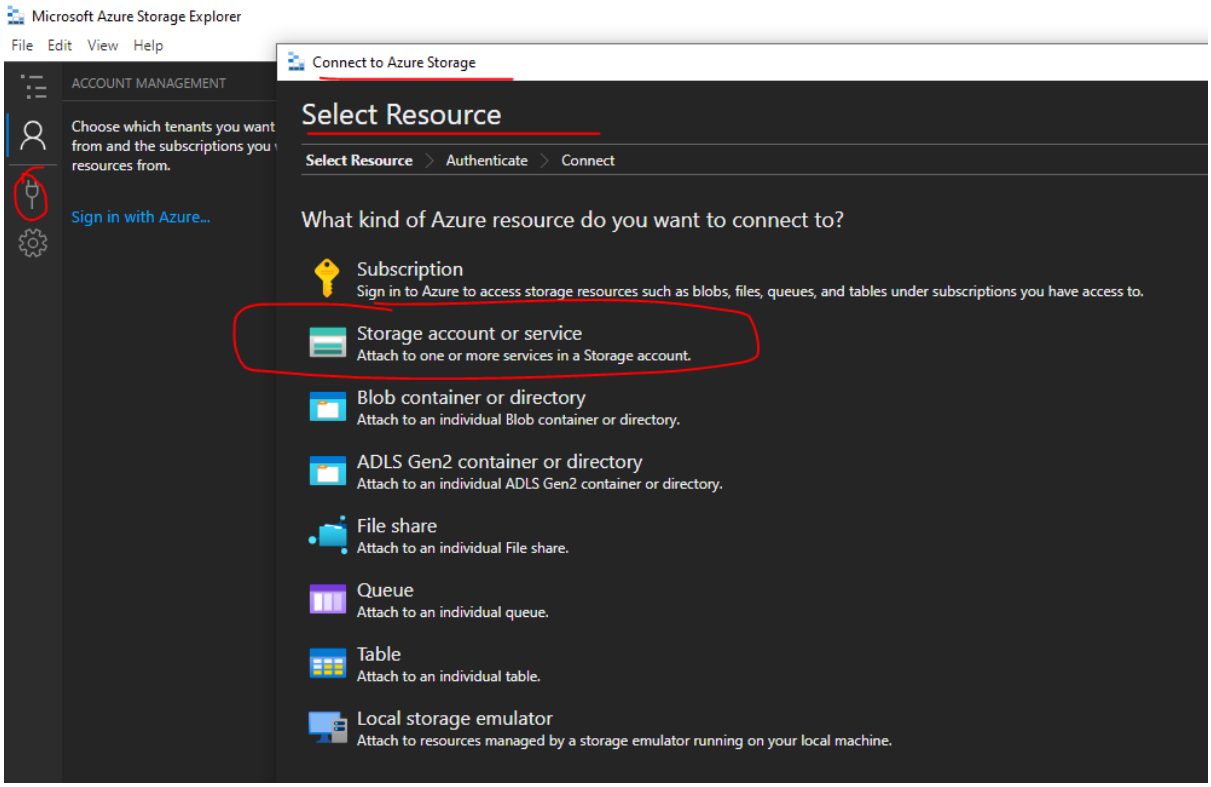
2) SEARCH – AZURE STORAGE EXLORER DOWNLOAD

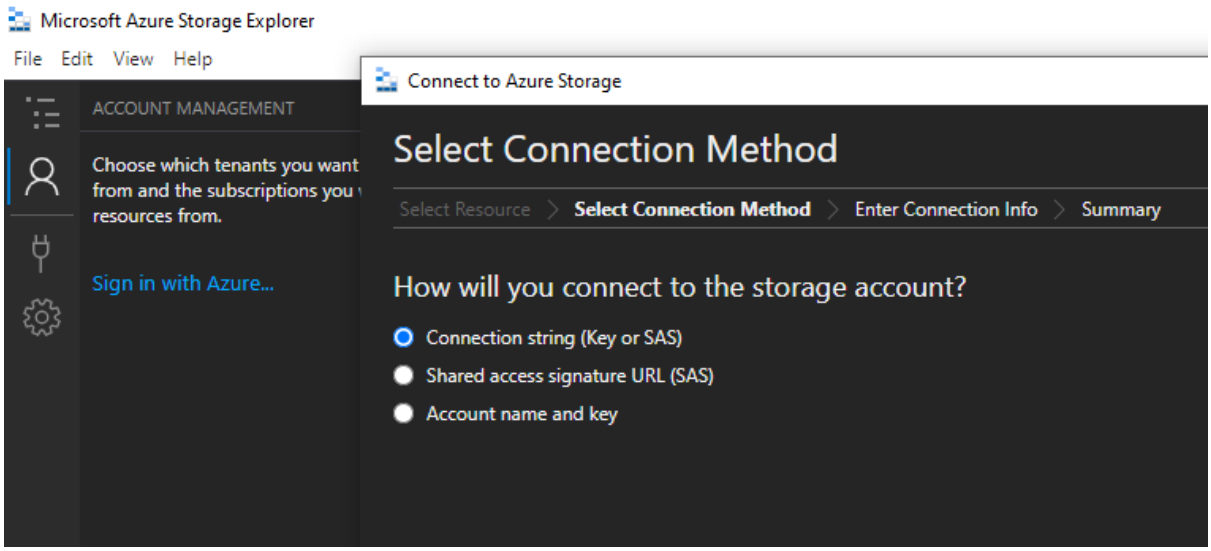




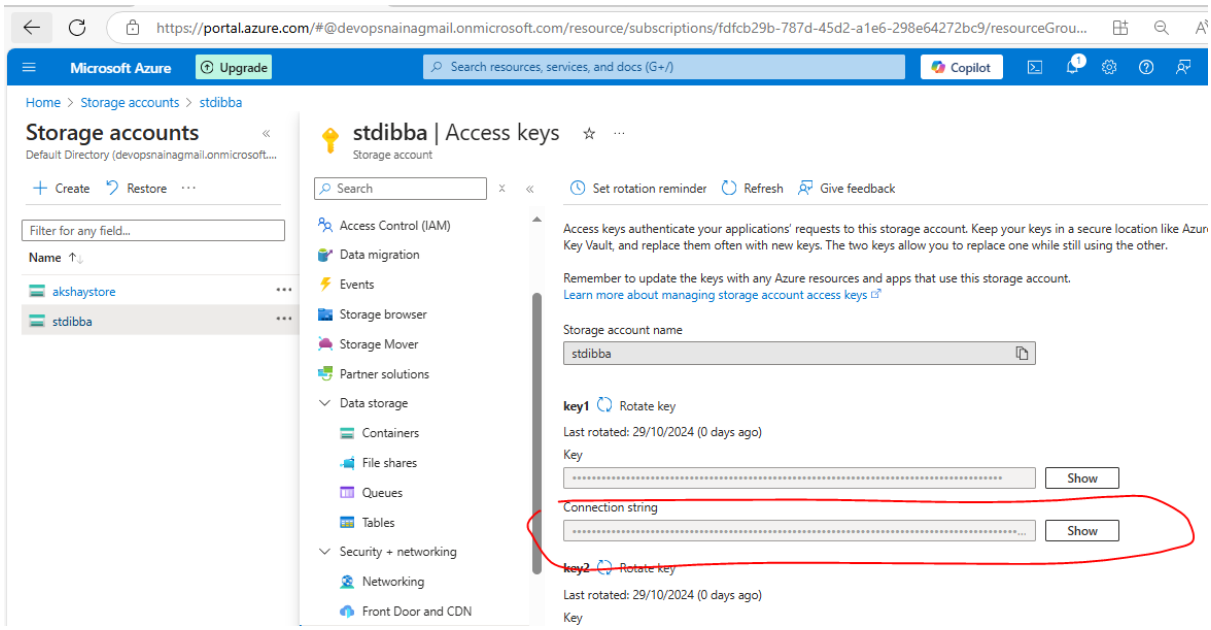
3) We can use different methods using explorer software to connect to storage account

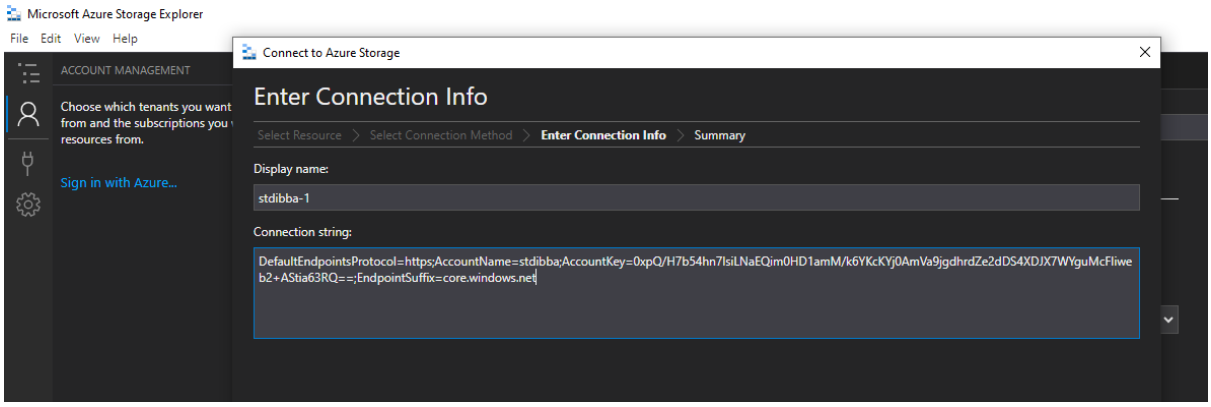

Microsoft Azure Storage Explorer
File Edit View Help
ACCOUNT MANAGEMENT
Choose which tenants you want to load subscriptions from and the subscriptions you want to view resources from.
Sign in with Azure...
Open Explorer
Settings
Search settings
Application
Data Explorers
Services
Transfers
Open settings file...
Applicati
Appearance
Theme
Dark
Proxy

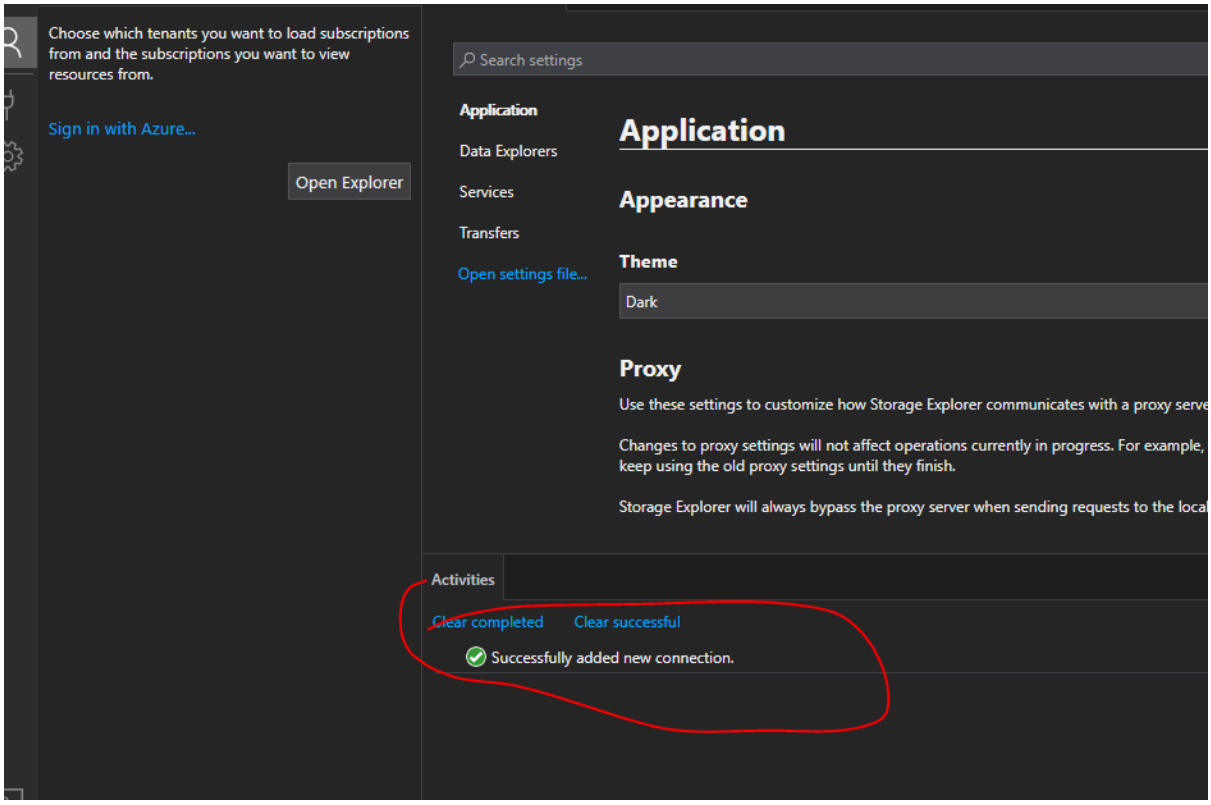

Microsoft Azure Storage Explorer
File Edit View Help
ACCOUNT MANAGEMENT
Choose which tenants you want from and the subscriptions you resources from.
Sign in with Azure...
Connect to Azure Storage
Select Resource
Select Resource > Authenticate > Connect
What kind of Azure resource do you want to connect 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.

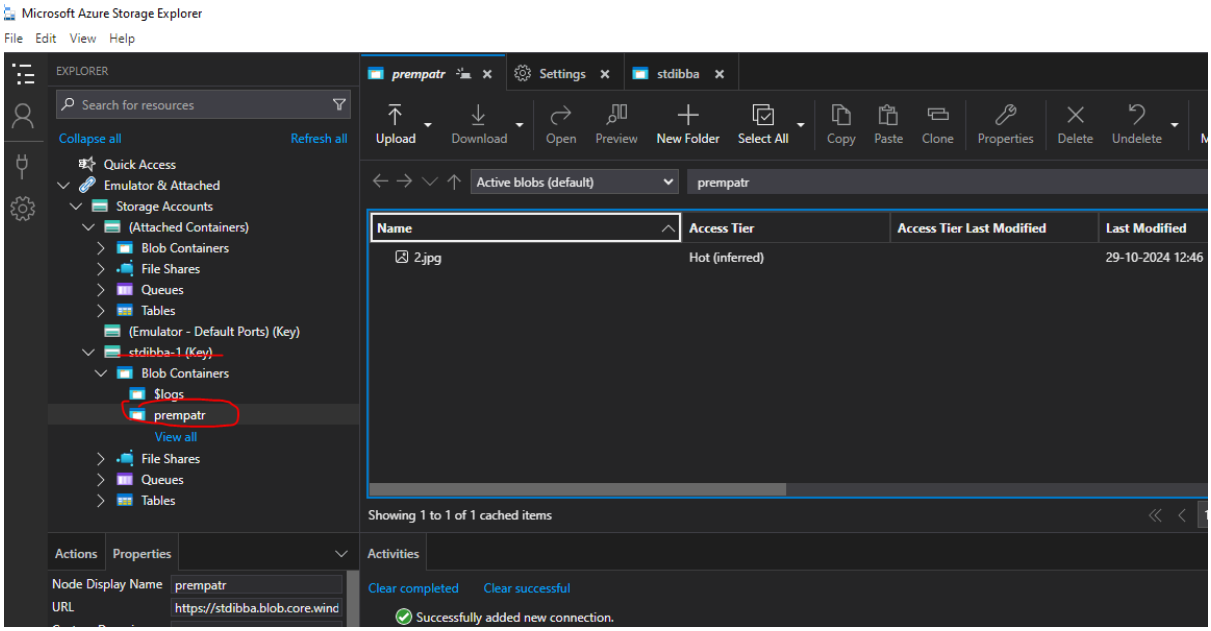


4) So in storage account, access keys we will get connection string









AGENDA – FILE SHARE

1)

https://portal.azure.com/#view/Microsoft_Azure_FileStorage/CreateFileShare.ReactView/_provisi

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

Home > Storage accounts > stdibba | File shares >

New file share

Basics | Backup | Review + create

Name * fileshare1

Performance

Maximum IO/s	1000
Maximum capacity	5 TiB
Large file shares	Disabled

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.

Review + create | < Previous | Next : Backup >

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

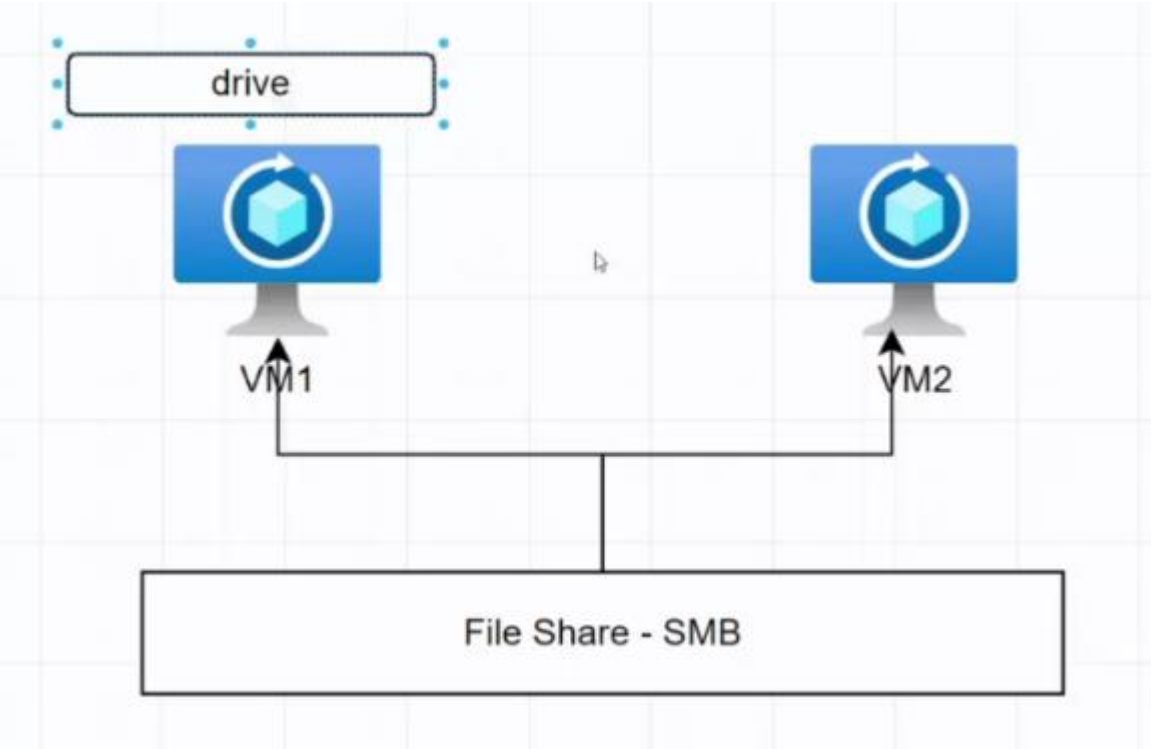
Home > Storage accounts > stdibba | File shares >

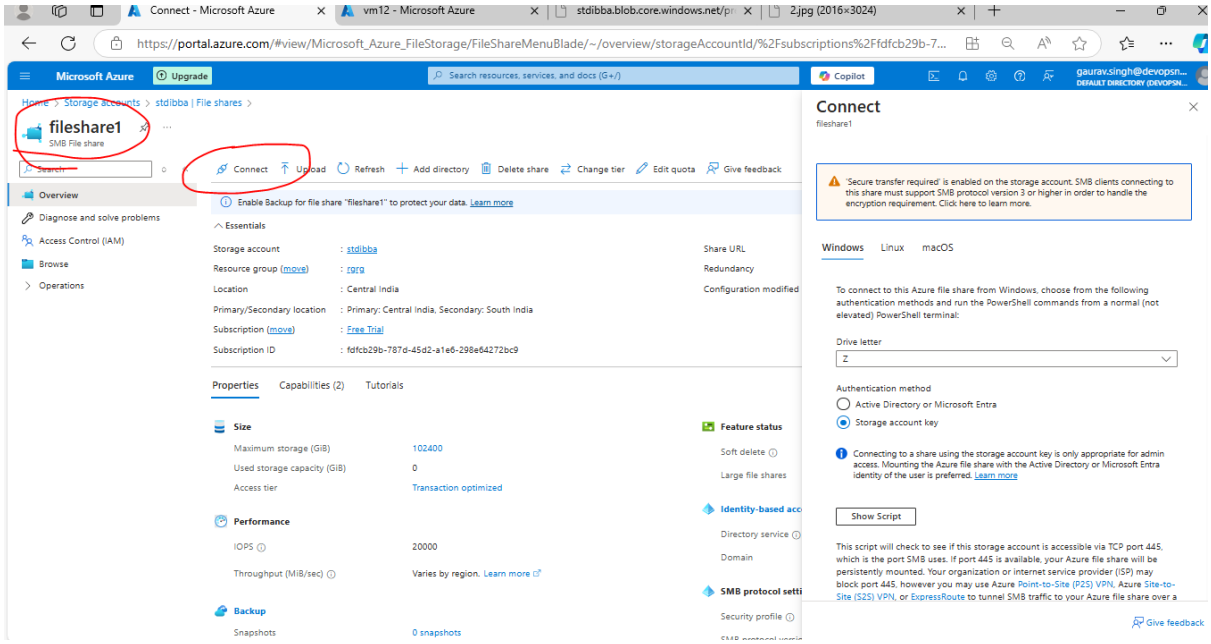
New file share

Basics | Backup | Review + create

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

Enable backup ☐


drive
VM1
VM2
File Share - SMB


Connect - Microsoft Azure
vm12 - Microsoft Azure
stdibba.blob.core.windows.net/pr
2.jpg (2016×3024)
https://portal.azure.com/#view/Microsoft_Azure_FileStorage/FileShareMenuBlade/~/overview/storageAccountId/%2Fsubscriptions%2Ffdfcb29b-7...
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
gaurav.singh@devopsn...
DEFAULT DIRECTORY (DEVOPSN...
Home > Storage accounts > stdibba | File shares >
fileshare1
SMB File share
Search
Overview
Diagnose and solve problems
Access Control (IAM)
Browse
Operations
Connect
Upload
Refresh
Add directory
Delete share
Change tier
Edit quota
Give feedback
Enable Backup for file share "fileshare1" to protect your data. Learn more
Essentials
Storage account : stdibba
Resource group (move) : rgrg
Location : Central India
Primary/Secondary location : Primary: Central India, Secondary: South India
Subscription (move) : Free Trial
Subscription ID : fdfcb29b-787d-45d2-a1e6-298e64272bc9
Share URL
Redundancy
Configuration modified
Properties
Capabilities (2)
Tutorials
Size
Maximum storage (GiB) 102400
Used storage capacity (GiB) 0
Access tier Transaction optimized
Performance
IOPS 20000
Throughput (MiB/sec) Varies by region. Learn more
Backup
Snapshots 0 snapshots
Feature status
Soft delete
Large file shares
Identity-based acc
Directory service
Domain
SMB protocol setti
Security profile
Connect
fileshare1
'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.
Windows
Linux
macOS
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
Show Script
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
Give feedback

fileshare1

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

Hide Script

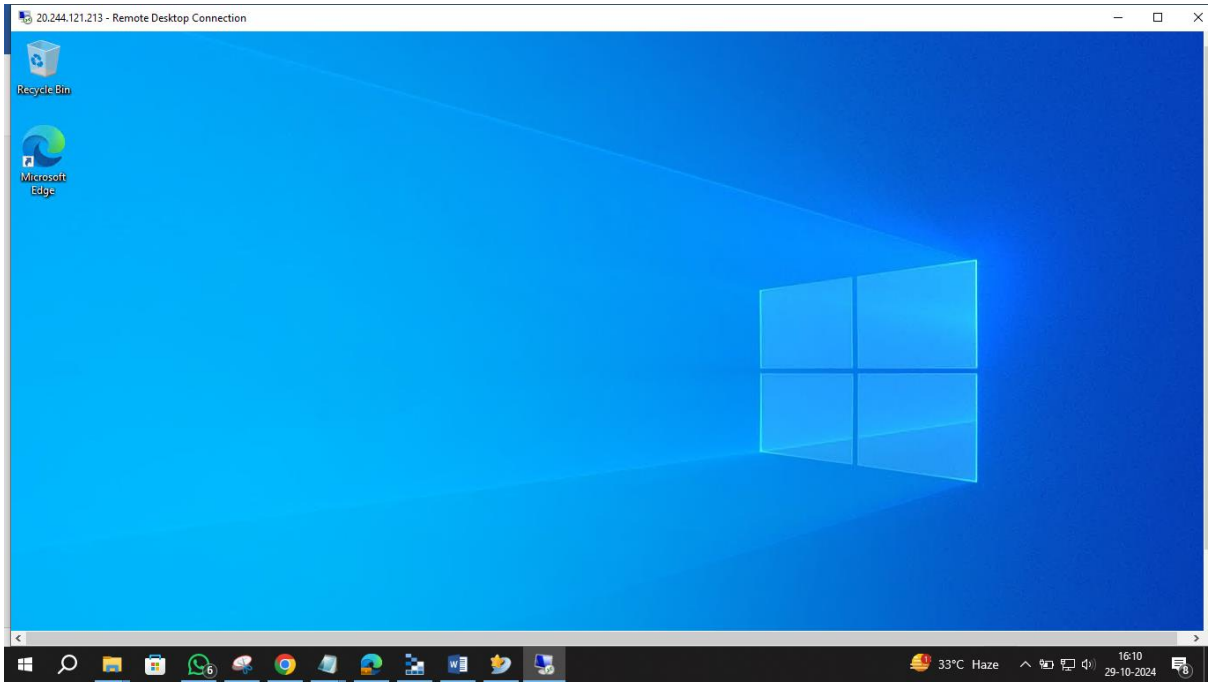
```
$connectTestResult = Test-NetConnection -ComputerName
stdibba.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
   # Save the password so the drive will persist on reboot
   cmd.exe /C "cmdkey /add:`"stdibba.file.core.windows.net`"
/user:`"localhost\stdibba`"
/pass:`"0xpQ/H7b54hn7lsiLNaEQim0HD1amM/k6YKcKYj0AmVa9jgdhrdZe2dD
S4XDJX7WYguMcFIiweb2+AStia63RQ==`""
   # Mount the drive
   New-PSDrive -Name Z -PSProvider FileSystem -Root
"\\stdibba.file.core.windows.net\fileshare1" -Persist
} else {
```

Give feedba

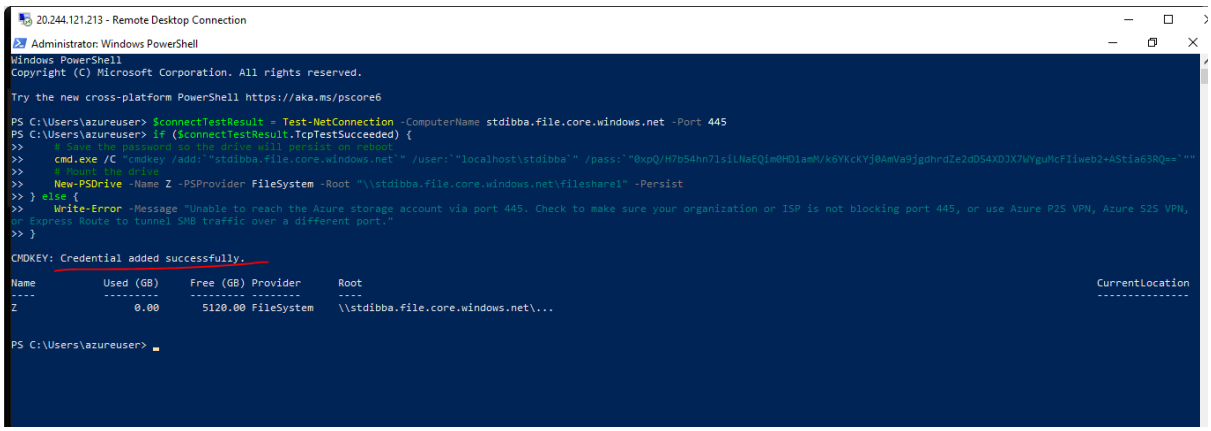
2) Now run above script in powershell

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

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\HP> $connectTestResult = Test-NetConnection -ComputerName stdibba.file.core.windows.net -Port 445
 TCP connect to (20.209.56.206 : 445) failed
WARNING: Ping to 20.209.56.206 failed with status: DestinationHostUnreachable
PS C:\Users\HP> if ($connectTestResult.TcpTestSucceeded) {
>>     # Save the password so the drive will persist on reboot
>>     cmd.exe /C "cmdkey /add:`"stdibba.file.core.windows.net`" /user:`"localhost\stdibba`" /pass:`"0xpQ/H7b54hn7lsiLNaEQim0HD1amM/k6YKcKYj0AmVa9jgdhrdZe2dDS4XDJX7WYguMcFIiweb2+AStia63RQ==`""
>>     # Mount the drive
>>     New-PSDrive -Name Z -PSProvider FileSystem -Root "\\stdibba.file.core.windows.net\fileshare1" -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 over a different port."
>> }
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmd.exe /C "cmdkey /add:`"stdibba.file.core.windows.net`" /user:`"localhost\stdibba`" /pass:`"0xpQ/H7b54hn7lsiLNaEQim0HD1amM/k6YKcKYj0AmVa9jgdhrdZe2dDS4XDJX7WYguMcFIiweb2+AStia63RQ==`""
    # Mount the drive
    New-PSDrive -Name Z -PSProvider FileSystem -Root "\\stdibba.file.core.windows.net\fileshare1" -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 over a different port."
} : 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 over a different port.
    + CategoryInfo          : NotSpecified: (:) [Write-Error], WriteErrorException
    + FullyQualifiedErrorId : Microsoft.PowerShell.Commands.WriteErrorException

PS C:\Users\HP>
```

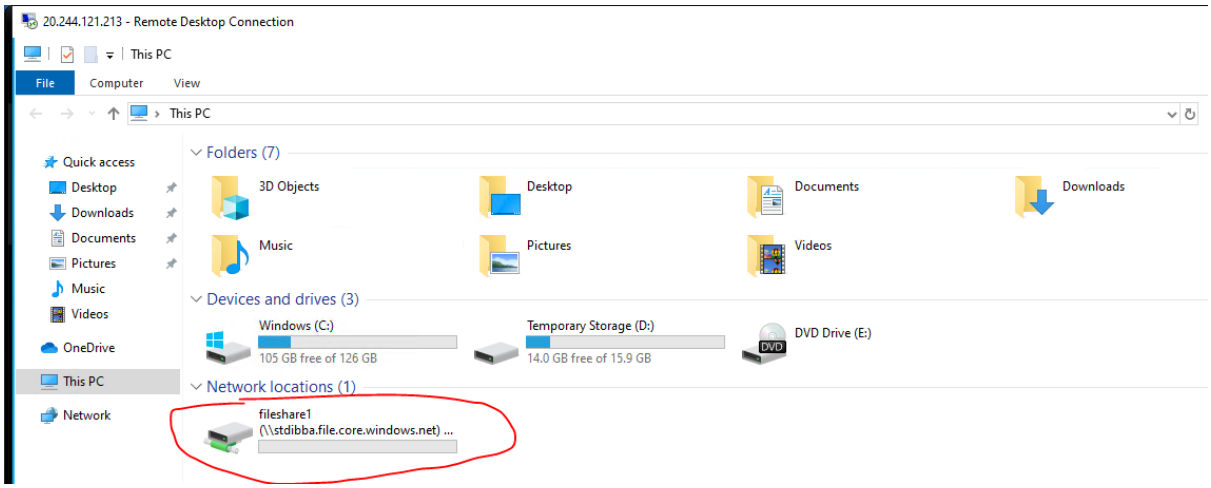
3) Now create a new vm of windows vm and do into it. Do rdp



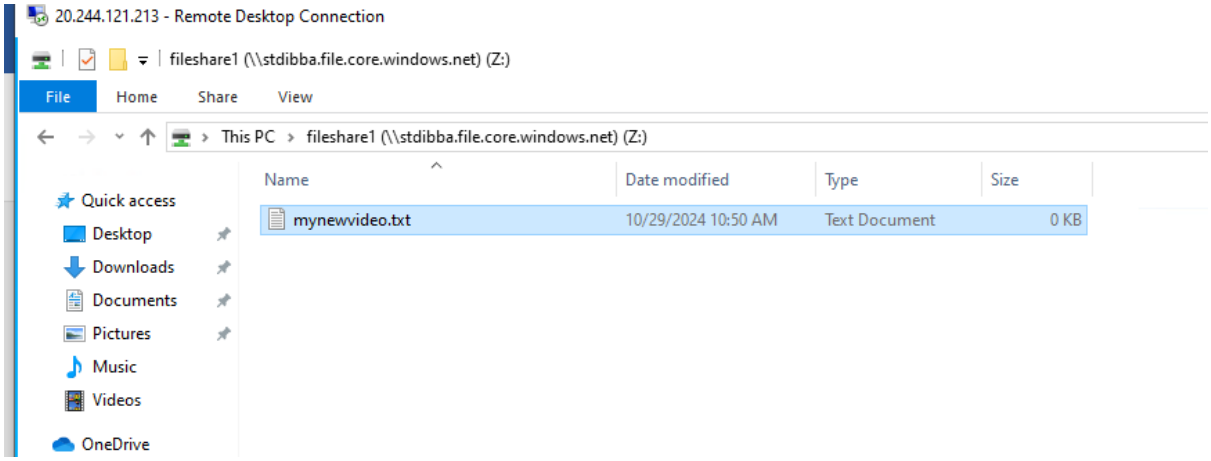
4) Copy and paste the file share script in powershell of vm by which credentials will be added successfully.



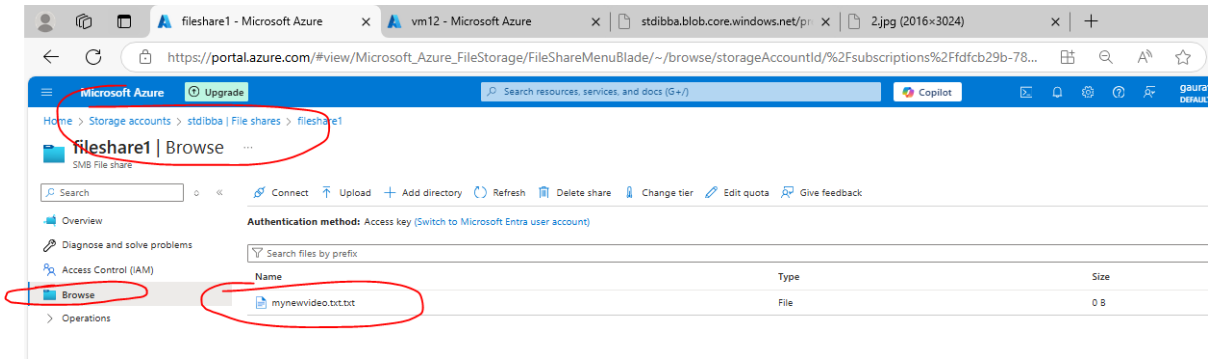
5) Now now a new file share disk is created



6) Go inside it and make a new file “mynewvideo.txt”



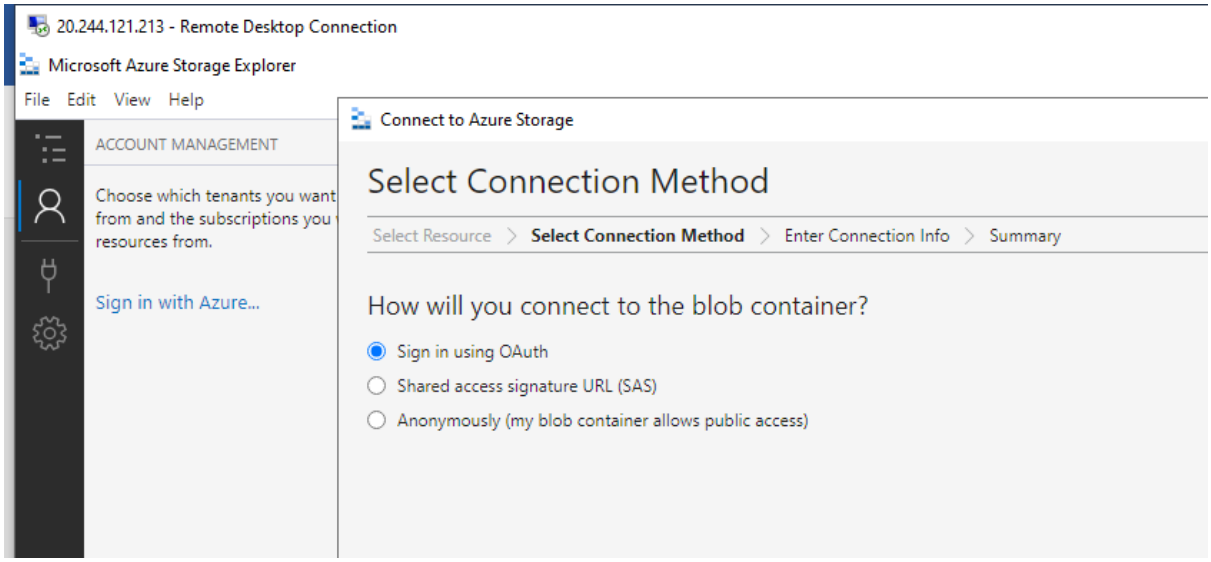
7) Now we can see on portal in “browse” of file share



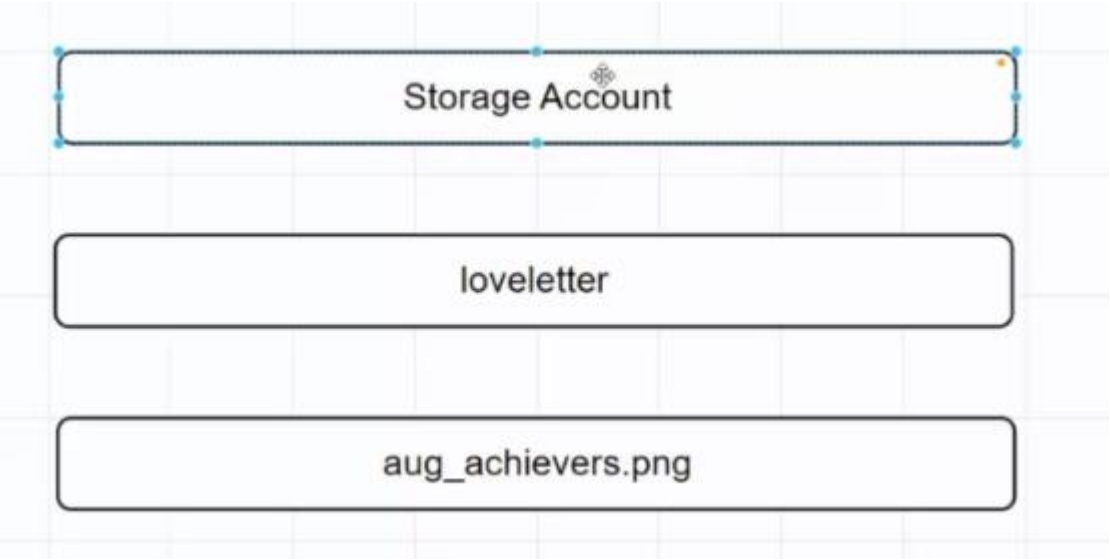
8) Now we can connect multiple computers using connect button so that many users can use a common place or location

9) In vm install azure storage explorer

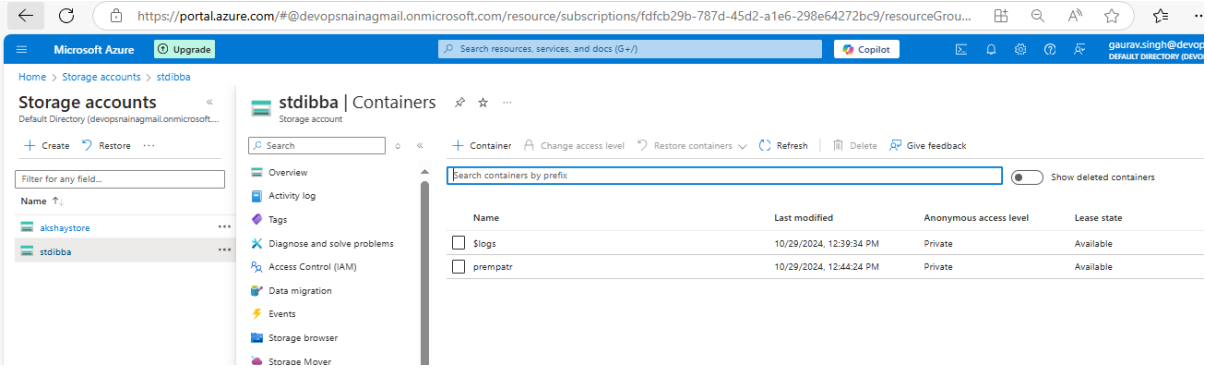
10) open and now connecting blob storage

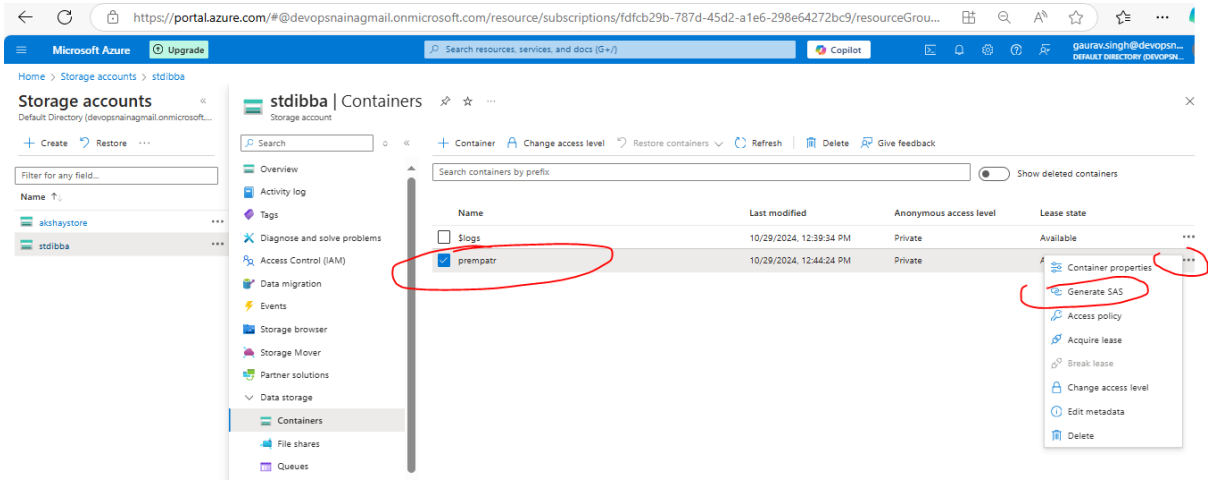


11) We get SAS access at 3 levels



12) So now we are making sas for blob level





Search resources, services, and docs (G+/)

Copilot

gaurav.singh@de
DEFAULT DIRECTORY (D

S

Container | Change access level | Restore containers | Refresh

Search containers by prefix

Name	Last modifi
$logs	10/29/2024,
prempatr	10/29/2024,

Generate SAS

time range without sharing your storage account key. Learn more about creating a
account SAS

Signing method
Account key | User delegation key

Signing key
Key 1

Stored access policy
None

Permissions *
7 selected

Start and expiry date/time

Start
10/29/2024 | 4:41:32 PM
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Expiry
10/30/2024 | 12:41:32 AM
(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

portal.azure.com/#@devopsnainagmail.onmicrosoft.com/resource/subscriptions/fdfcb29b-78d-45d2-a1e6-298e6427bc9/resourceGrou...

pgrade

Search resources, services, and docs (G+/)

Copilot

gaurav.singh@devopsn...
DEFAULT DIRECTORY (DEVOPSN...

ba

stdibba | Containers
Storage account

Search

Storage Mover
Partner solutions
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
Settings
Monitoring
Monitoring (classic)
Automation

Container | Change access level | Restore containers | Refresh

Search containers by prefix

Name	Last modifi
$logs	10/29/2024,
prempatr	10/29/2024,

Generate SAS

Signing key
Key 1

Stored access policy
None

Permissions *
7 selected

Start and expiry date/time

Start
10/29/2024 | 4:41:32 PM
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

Expiry
10/30/2024 | 12:41:32 AM
(UTC+05:30) Chennai, Kolkata, Mumbai, New Delhi

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

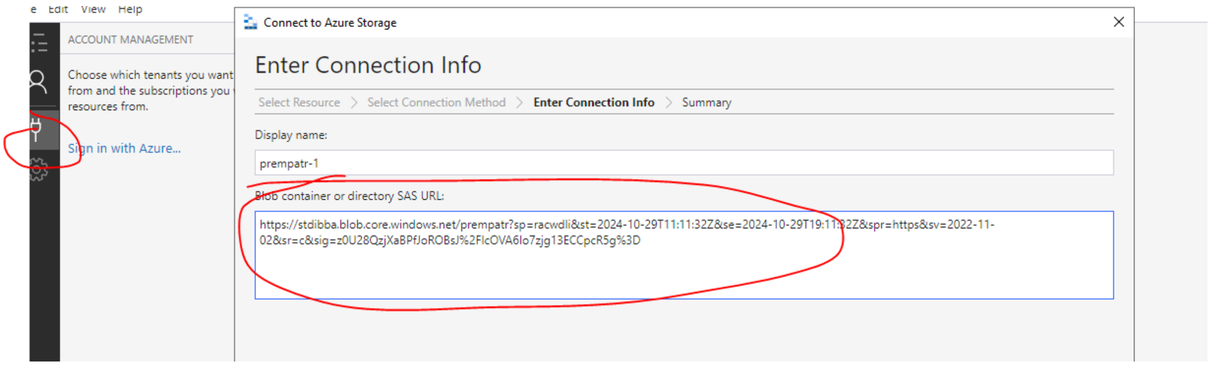
Allowed protocols
HTTPS only | HTTPS and HTTP

Generate SAS token and URL

Blob SAS token
sp=racwdli&st=2024-10-29T11:11:32Z&se=2024-10-29T19:11:32Z&spr=https&sv=...

Blob SAS URL
https://stdibba.blob.core.windows.net/prempatr?sp=racwdli&st=2024-10-29T11:11:...

Copy to clipboard



Choose which tenants you want
from and the subscriptions you
resources from.

Connect to Azure Storage

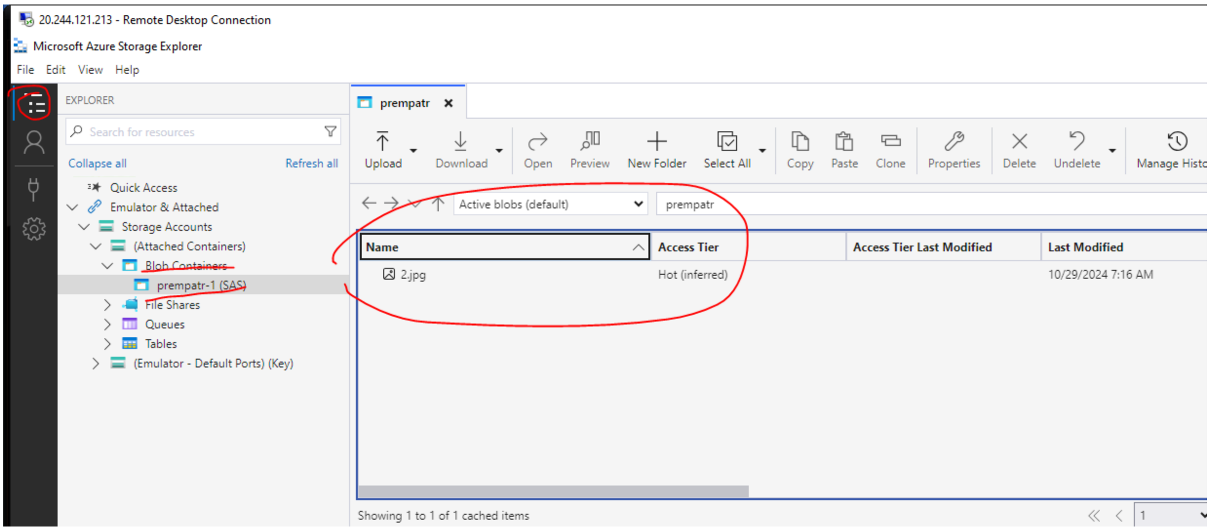
Enter Connection Info

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

Display name: prempatr-1

Blob container or directory SAS URL:

```
https://stdibba.blob.core.windows.net/prempatr?sp=racwdli&st=2024-10-29T11:11:32Z&se=2024-10-29T19:11:32Z&spr=https&sv=2022-11-
02&sr=c&sig=z0U28QzjXaBPfJoROBsJ%2FlcOVA6lo7zjg13ECCpcR5g%3D
```



20.244.121.213 - Remote Desktop Connection

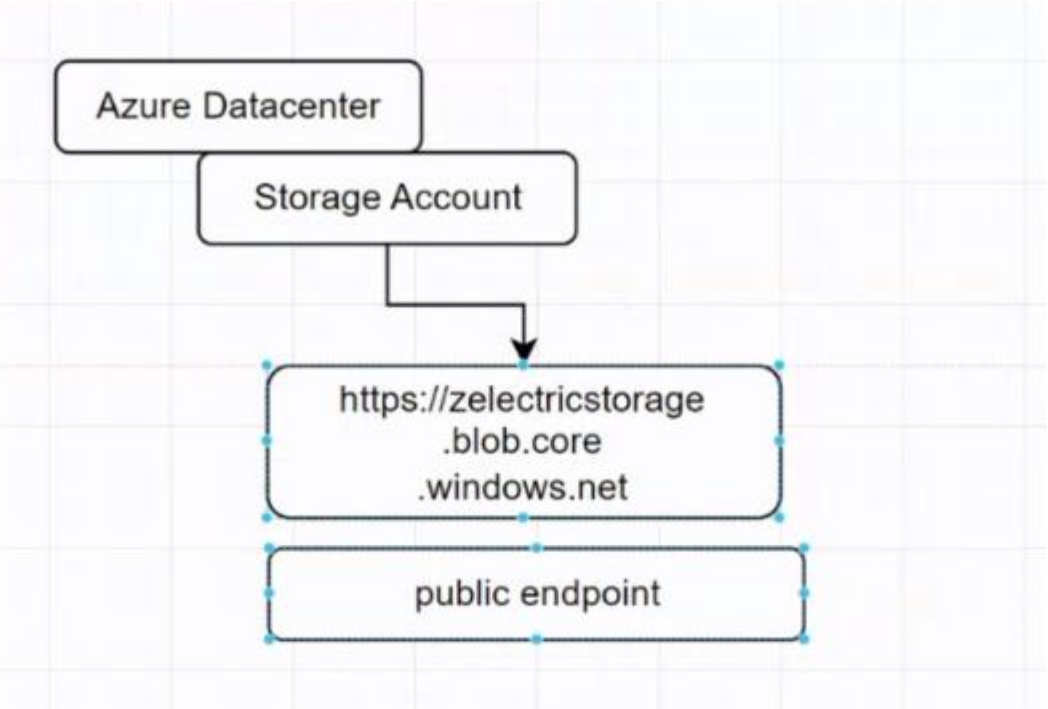
Microsoft Azure Storage Explorer

Name	Access Tier	Access Tier Last Modified	Last Modified
2.jpg	Hot (inferred)		10/29/2024 7:16 AM

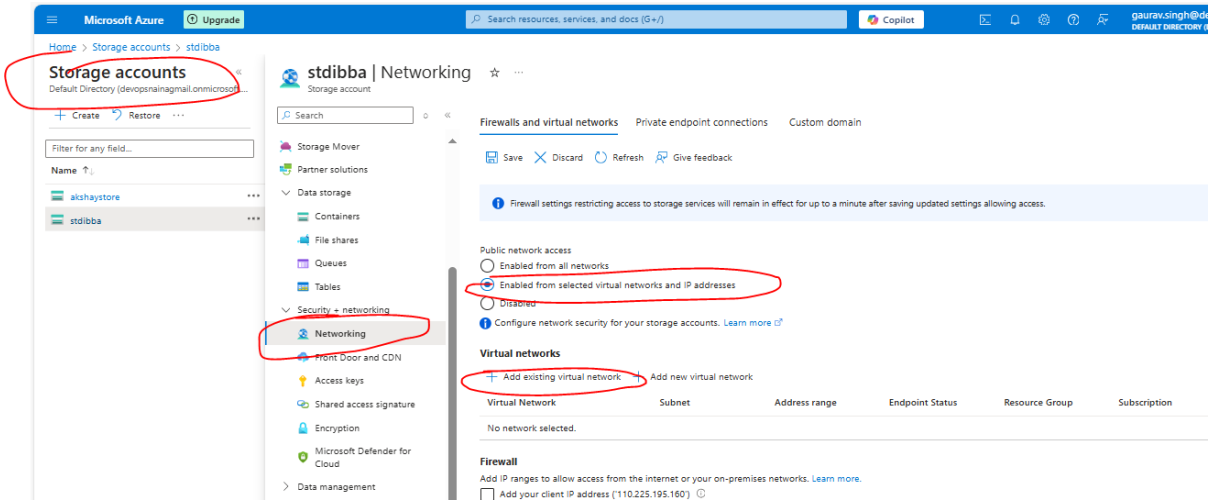
Showing 1 to 1 of 1 cached items

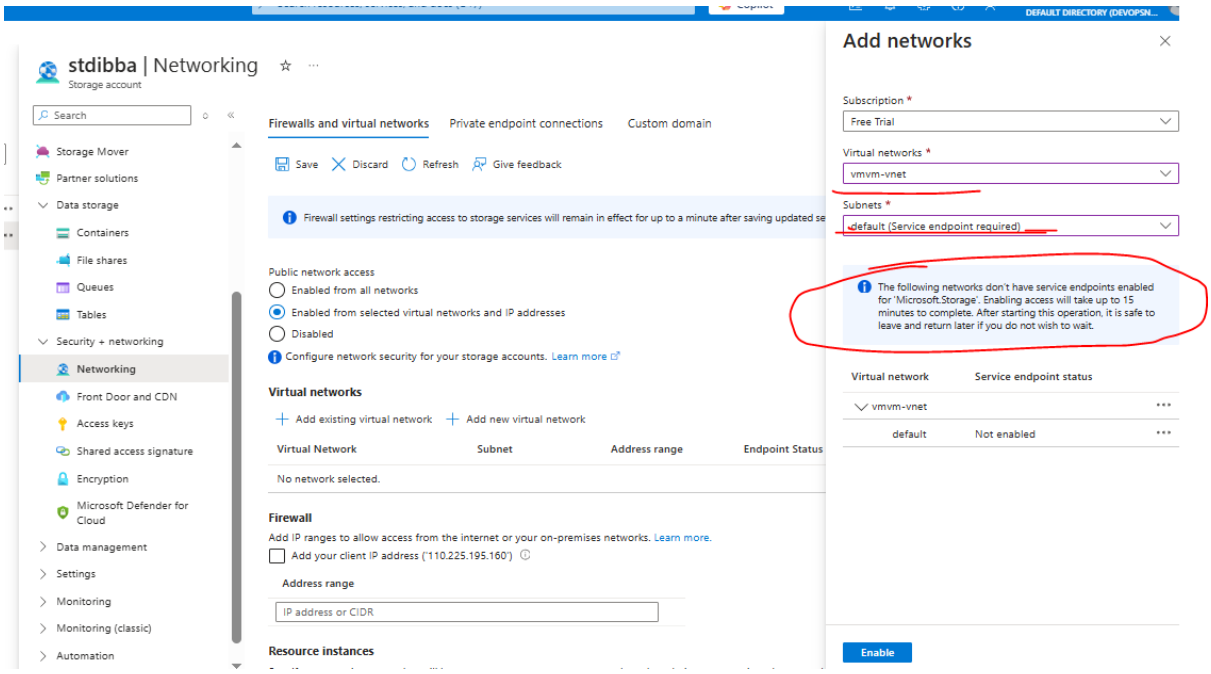
++

PAIN – Data can get loss as it uses public end point so use private end point

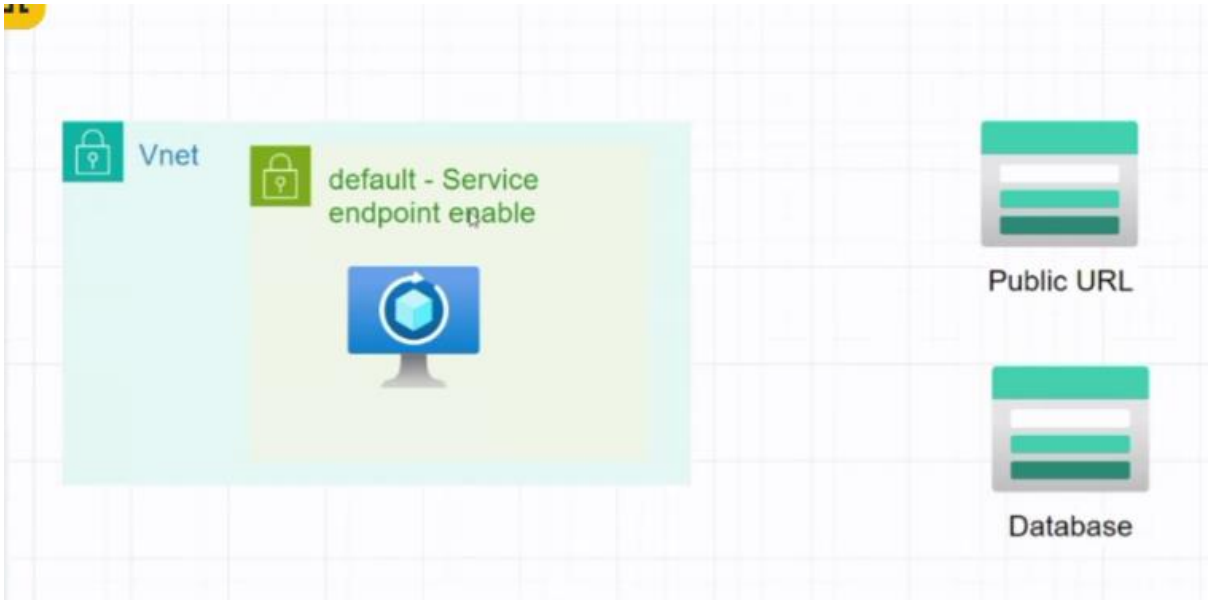


1) So now go to networking section and enable firewall so that only selected users can access





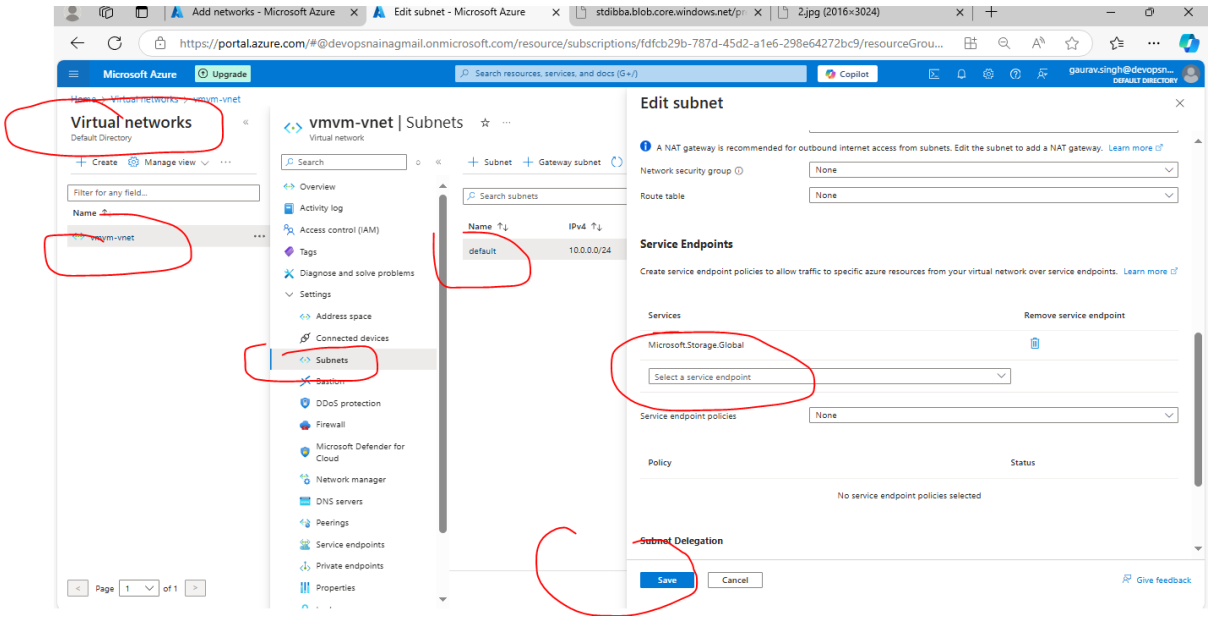
2) So as per above error doing service endpoint enabled. Go to vnet, subnet, default and add service end point



3) Do as below and for

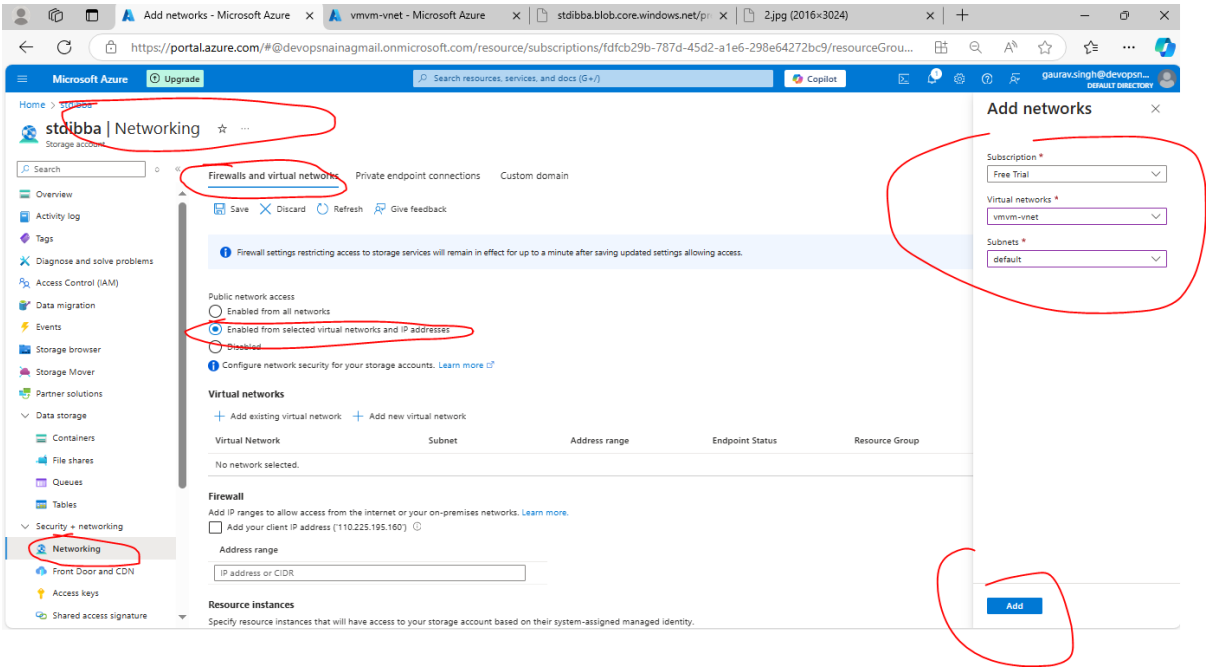
i) same same region – take normal one service end point

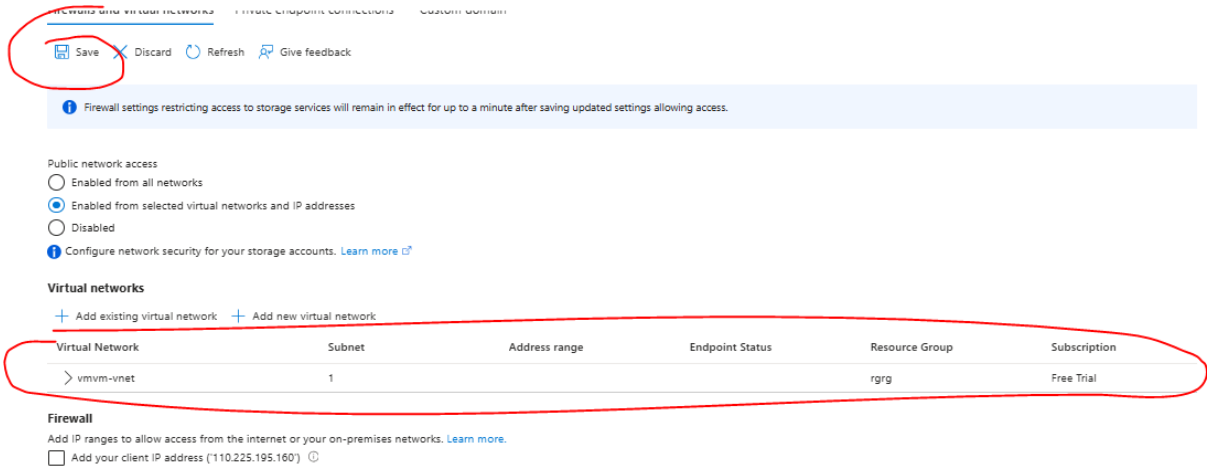
ii) for different regions – take Microsoft one service end point



3) Now basically we have enabled a service end point inside our subnet

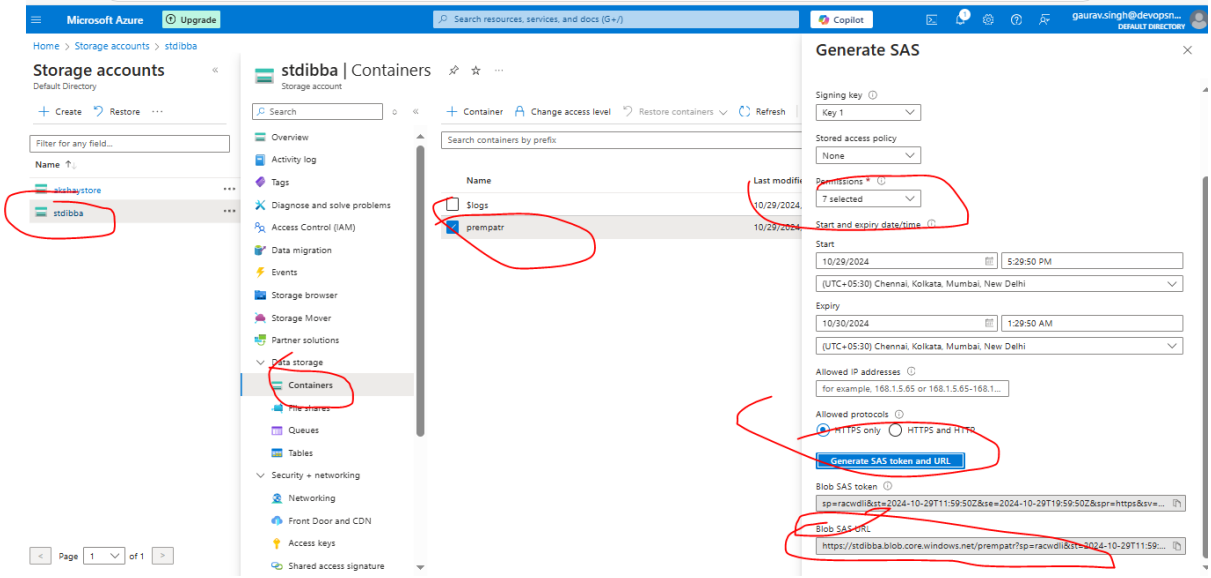
4) Now go to storage account



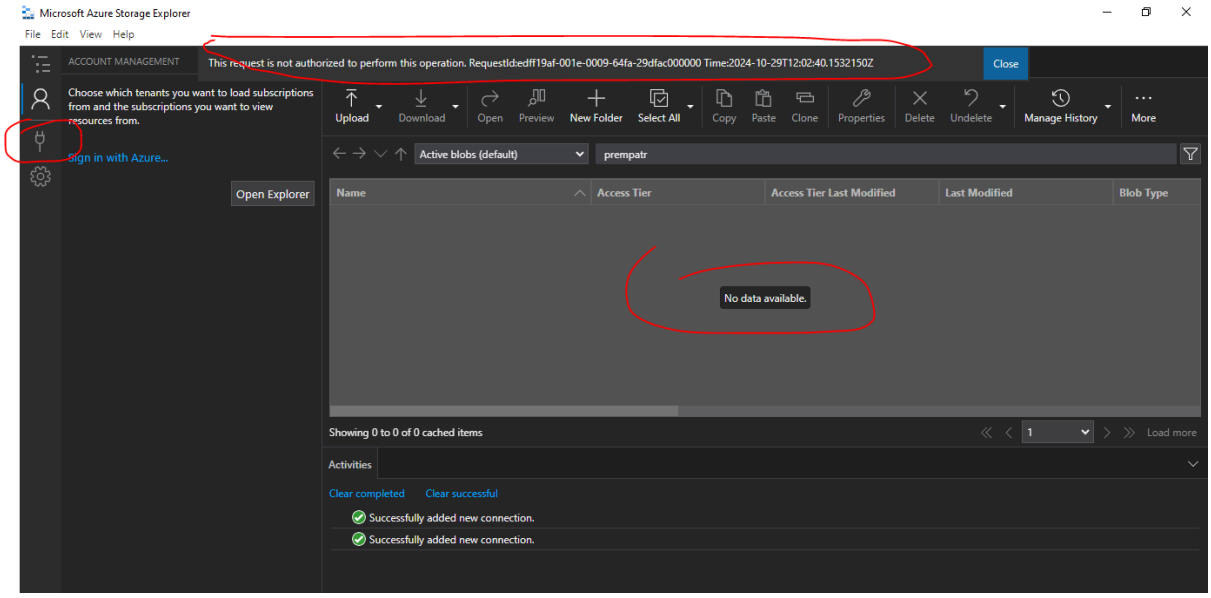


5) So now we have made our storage account little bit safe as now we will be able to access storage account through a specific subnet only

6) So now lets try to connect blob storage from our local computer

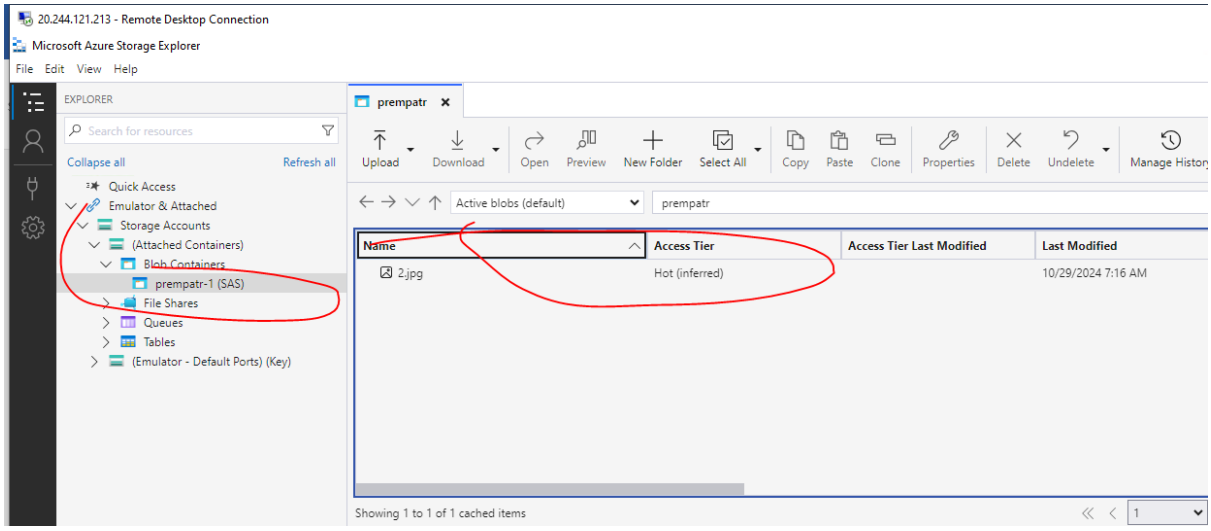


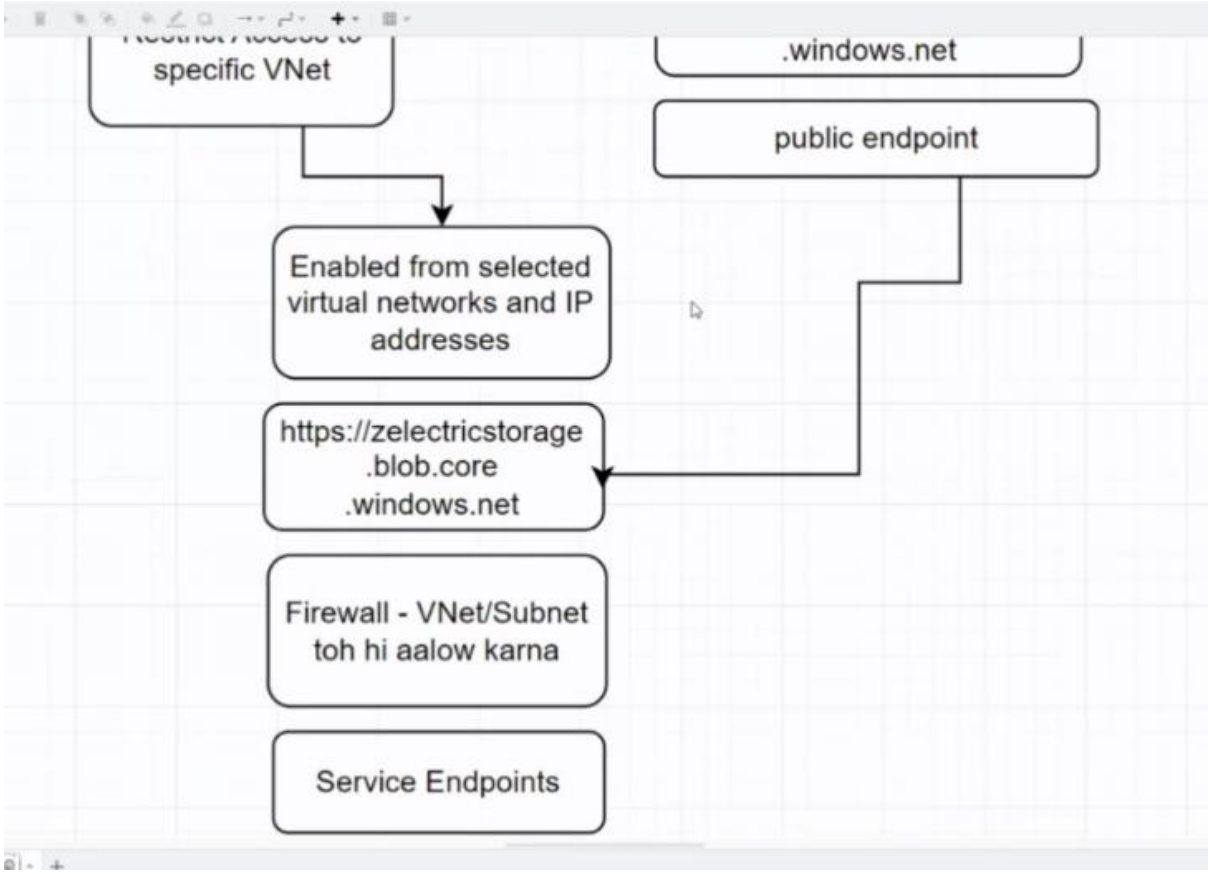
Select blob storage option



So it not showing anything

7) Now go to vm rdp and try to connect into it so we got that it is able to connect & access





8) But still problem is

Assignment for the Week

1. Azure Storage Account Encryption Methods
2. Azure Storage Account Authentication Methods
3. Azure Storage Account File Share Connect to VM
4. Try to restrict connection to Storage Account using Service Endpoints