DEVOPS with MULTI-CLOUD
Practice Tasks

Institute Name : V Cube software solutions
Course **:** DevOps with Multi-Cloud
Batch **:** 30
Trainer **:** Krishna reddy sir

Prepared by **:** G.Bhavish
(MCD-AZ30-024)

TASK-16 :- Service & Private Endpoints. (Storage Account).

Date : 09/02/26

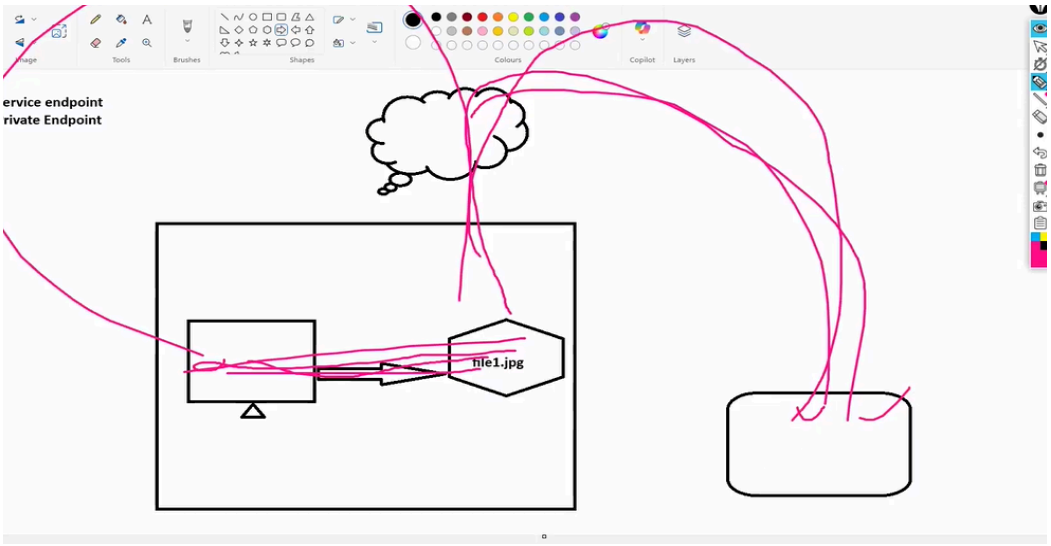
Objective :-
To securely connect Azure services to a Virtual Network by restricting access over the Azure backbone network using Service Endpoints and enabling private access through a private IP address using Private Endpoints, thereby preventing exposure to the public internet.

Service Endpoint :-
A Service Endpoint extends a Virtual Network to Azure services, allowing secure communication over the Azure backbone network without using the public internet.

Private Endpoint :-
A Private Endpoint provides a private IP address from your Virtual Network to an Azure service, enabling secure access without exposing the service publicly.

→ When we create a Storage Account, it is created by a default public endpoint. If we access storage account with a public endpoint, we are connected over the internet.

→ if we connect over the internet, we will be exposed and our data will not be safe.
→ so for the internal connection we need to enable "Service end point",
→ whenever we enable the service end point, it uses the backbone network i.e internal network for connecting to the storage account.



→ connecting to a storage account by a

Internal vm - Intranet.
Outsiders - Internet.

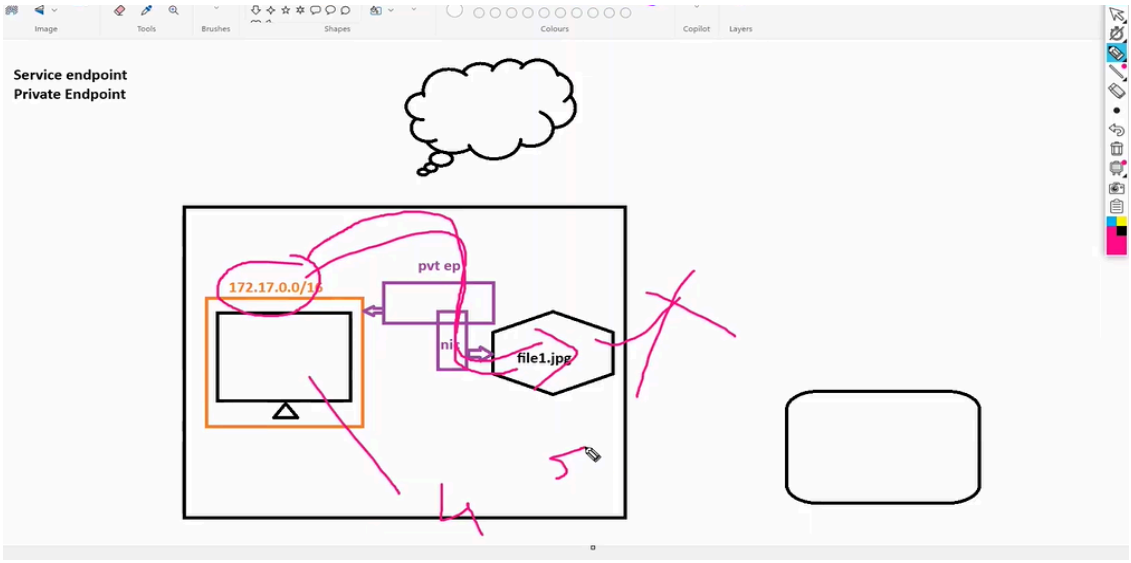
→ we can internally transfer the data to a storage account by using service endpoint. And outsiders can also access the data over the internet.

⦿ Note :-

- We can configure service & private endpoint to any PaaS model
- We canFind our ipv4&v6 in whatismyipaddress.com .

→ Unlike the service endpoint, for completely blocking the outside internet access to storage account we use the “Private Endpoint”.

→ when we configure a private end point ,one private ip is attached to our storage account so that we can access it internally.



→ Once we create a private endpoint

- Get one nic card which is attached to storage account
- The pub ip will get deleted.
- Picks one ip address from subnet range.
- In the backend one private dns is created.

→ And the dns maps the name with the pvt-ip.

→ with this private ip we can connect to a storage account internally & also blocks other connections.

“Service endpoint - for internal & outsider connection”.

“Private endpoint - for internal & more secure connection”.

→ create a vm and storage account, also create a container and add an image.

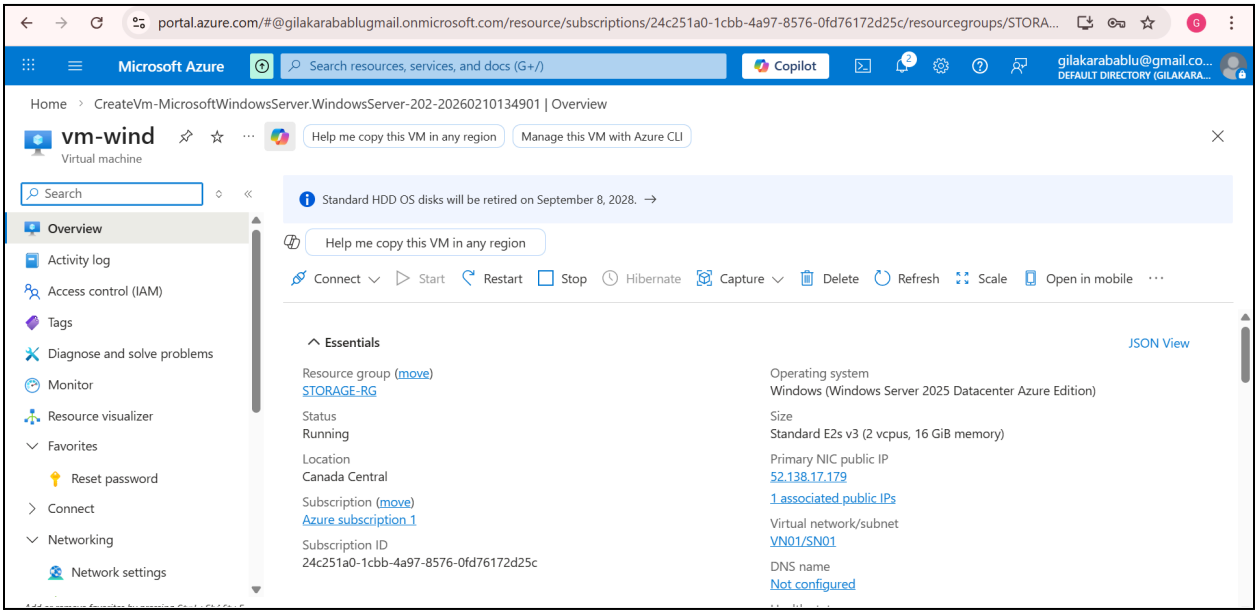


Fig (1) created a windows machine.

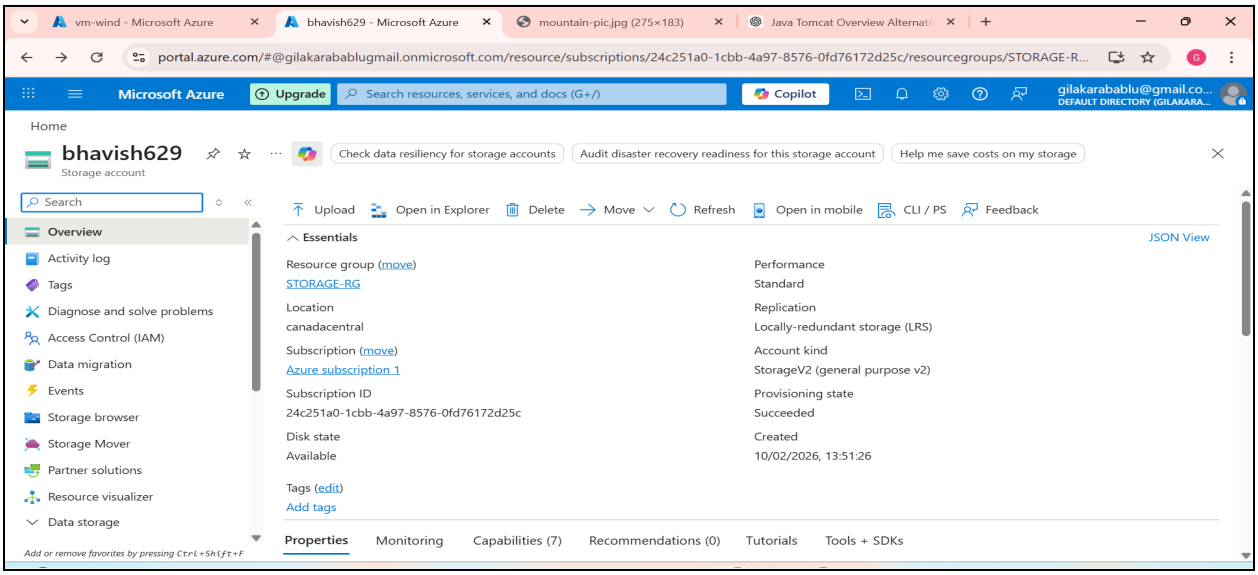
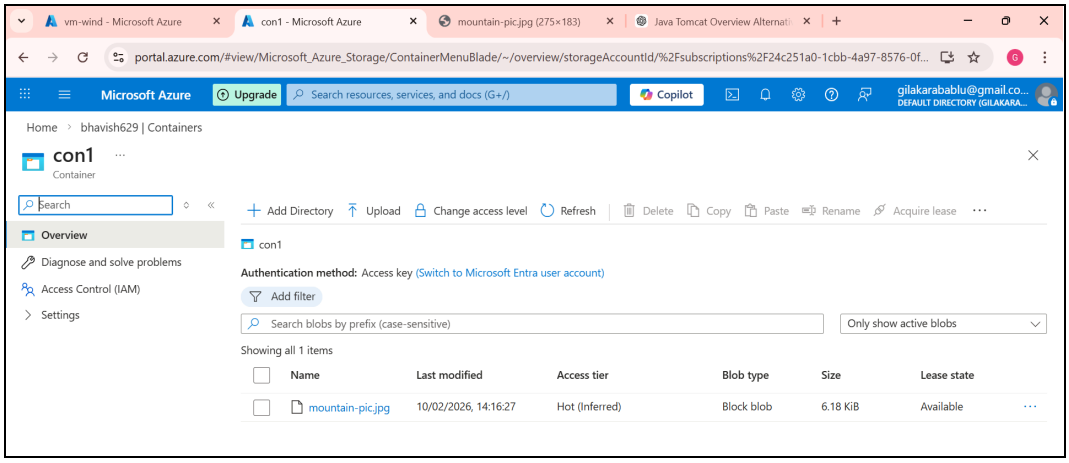


Fig (2) created a storage account.

→ create a container and add an image, try to access the image by browsing.



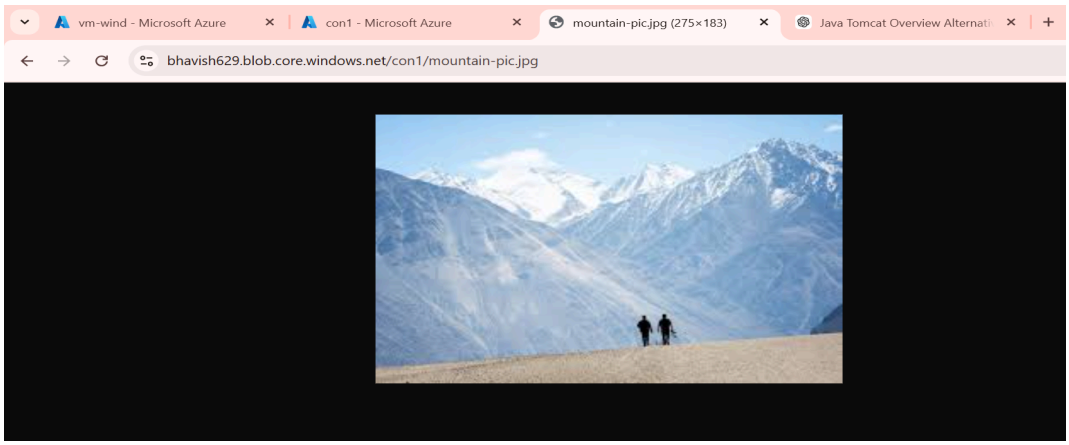


Fig (3&4) created a container and added an image.

→ Now let's configure the service endpoint.

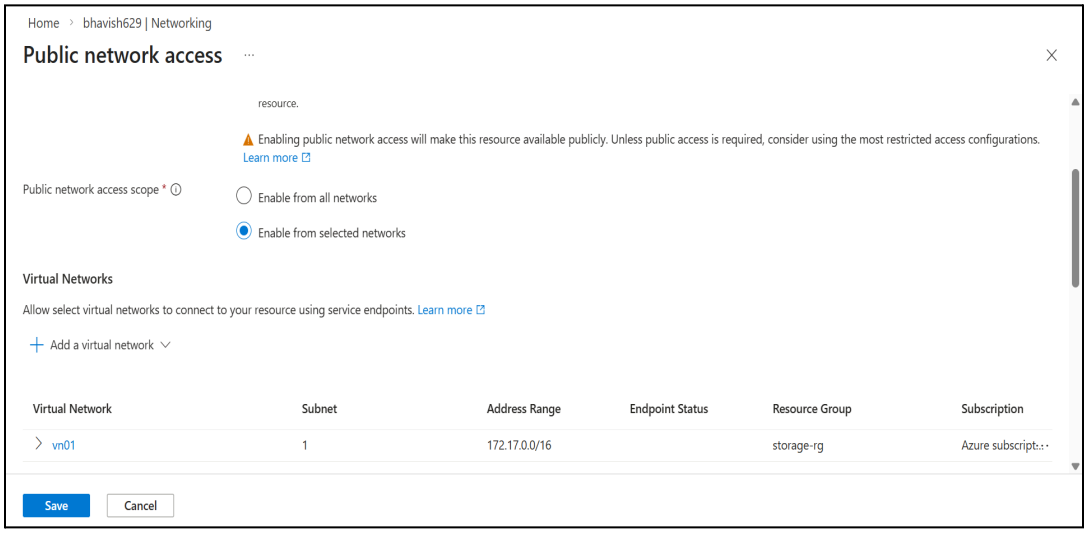
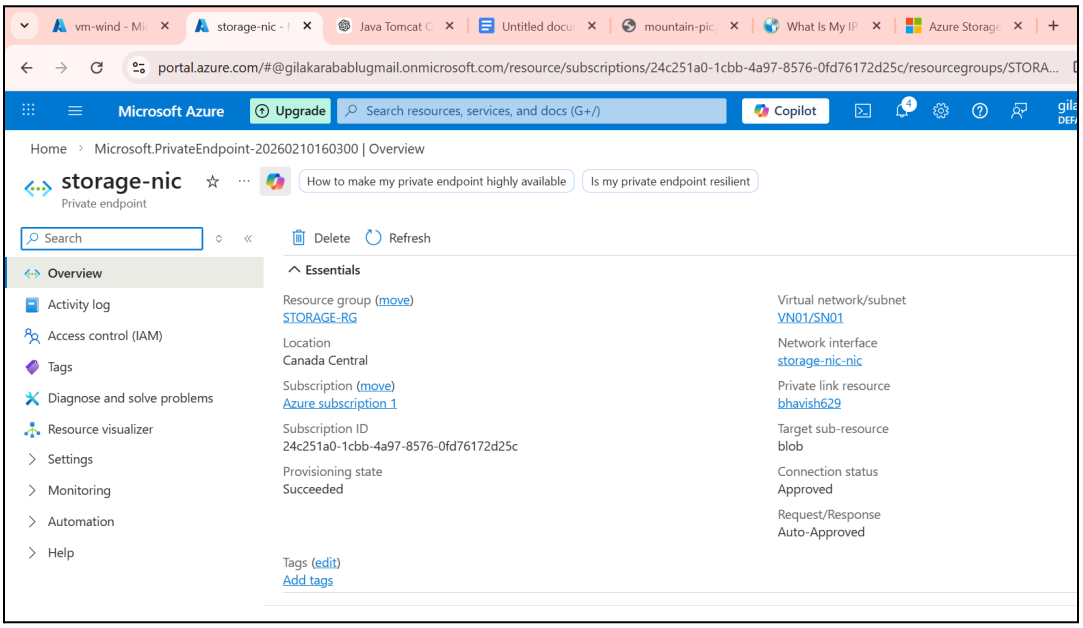


Fig (5) enabling service endpoint by selected networks.

→ the service endpoint is enabled at subnet level. Here we enabled selected networks and added machines vnet. Now only the machine can access the file.
→ we can also add our laptop ip address , so that we can also access the file.(add laptop ip in client ip.)

→ Now let's create a Private Endpoint.

- Search private endpoint and create,we can give the details in the basics, resources and vn.



fig(6) created a private endpoint.

→ Now only the vm can access the file in the storage account.

→ There are four ways to connect to the storage account.

- Portal Access - connecting by azure portal.
- Access keys

- SAS Keys
- RBAC Rules.

→ Access Keys :-

- Using access keys we can connect to the storage account, we can add and download data.
- The issue is it gives all the admin rights on the storage account.

→ SAS Keys :-

- Shared Access Signature, used to restrict the access like which data storage can be accessed.
- Eg:- only blob, only file and permissions like read,write,which ip address and how much time also.

→ RBAC Rules :-

- Roll Based Access Control, used to restrict even more than sas keys.
- Can give access to a particular user to a particular role with permissions & restrictions.
- Eg:- Sr.engg : Admin/Owner
  Jr.engg : Can be accessed only till his work or job role.

<u>NOTE</u> :-

1. SAS Keys can restrict and give permissions to all the users.
2. RBAC Rules can restrict & give permission to a particular person and to only his work.

→ the above three ways(access keys,sas keys and rbac rules) used to connect to the storage account via the “Storage Explorer”.

Note :- before using these keys and rules enable to all networks from selected networks.

→ Now download the Storage Explorer in the vm, and connect to storage account via keys and rules.

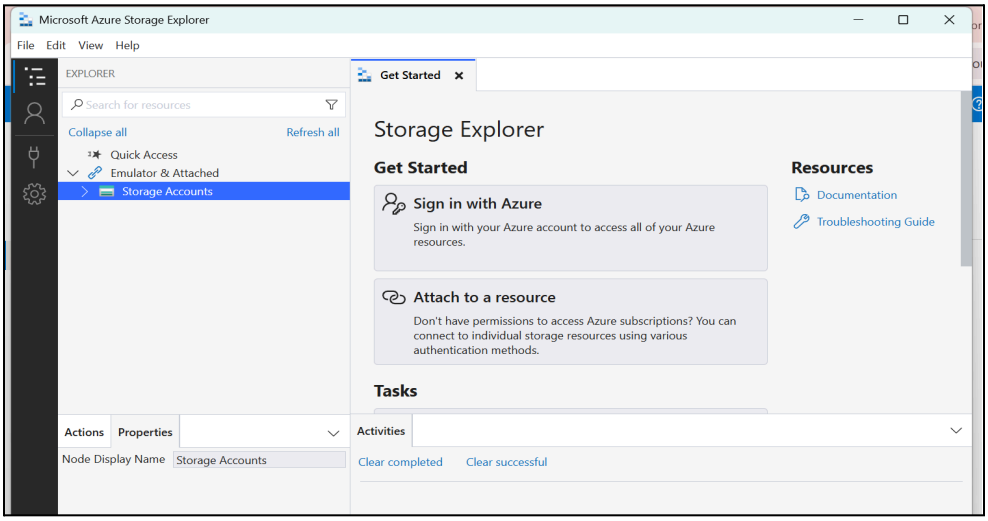


Fig (7) downloaded storage explorer.

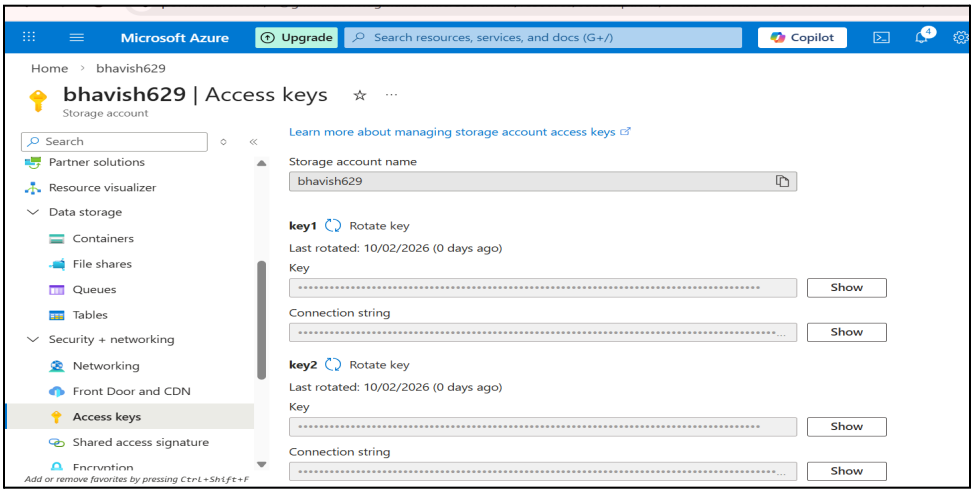


Fig (8) Access keys and connecting string.

→ use the access keys and connecting string and account name to connect the storage account.

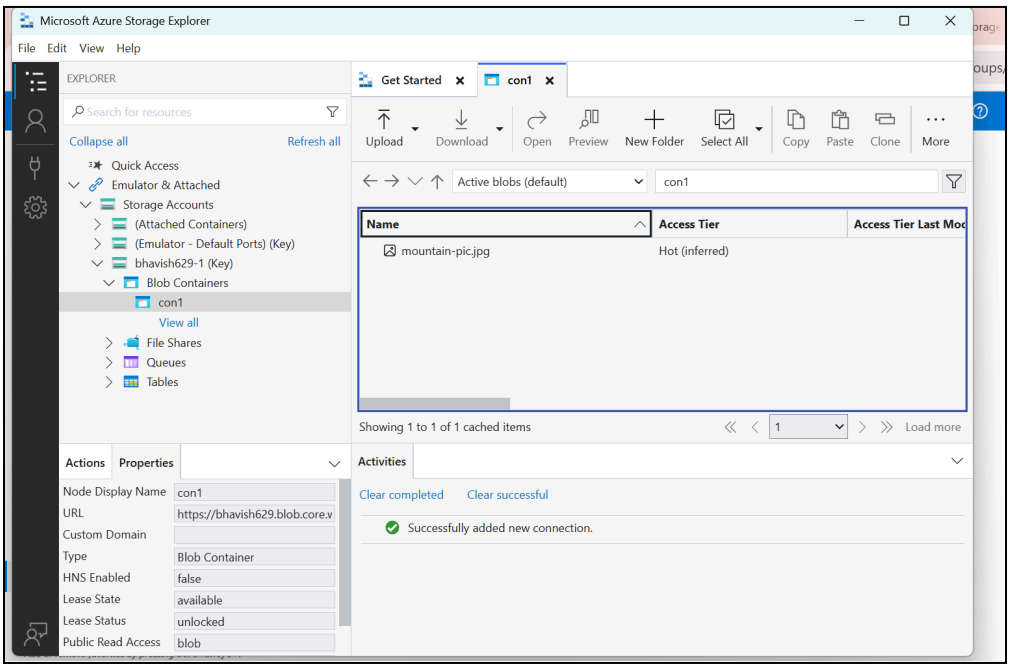


Fig (9) connected to the storage account using access keys.

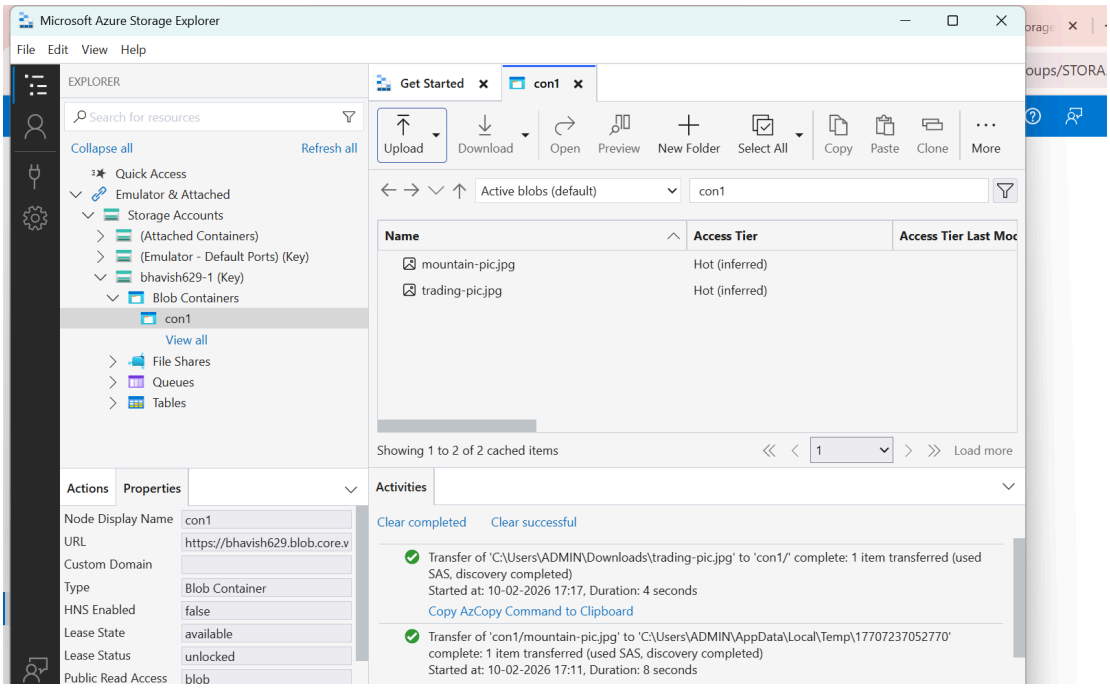
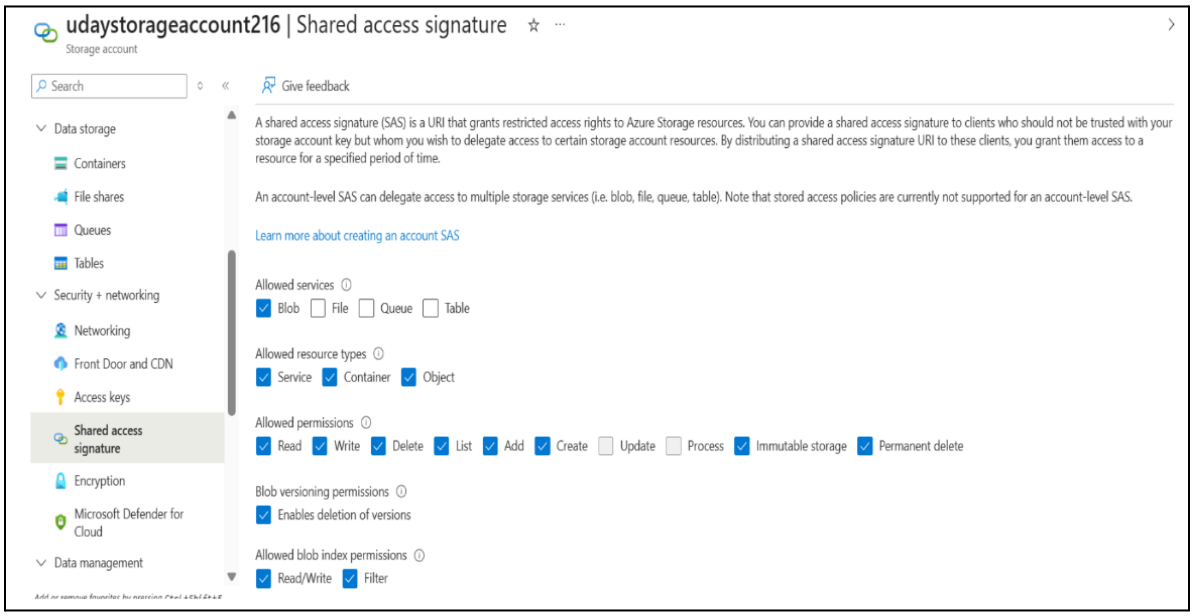


Fig (10) uploaded an image in the storage account using storage explorer.

→ now let's access with sas keys



fig(11) permissions in shared access signature.

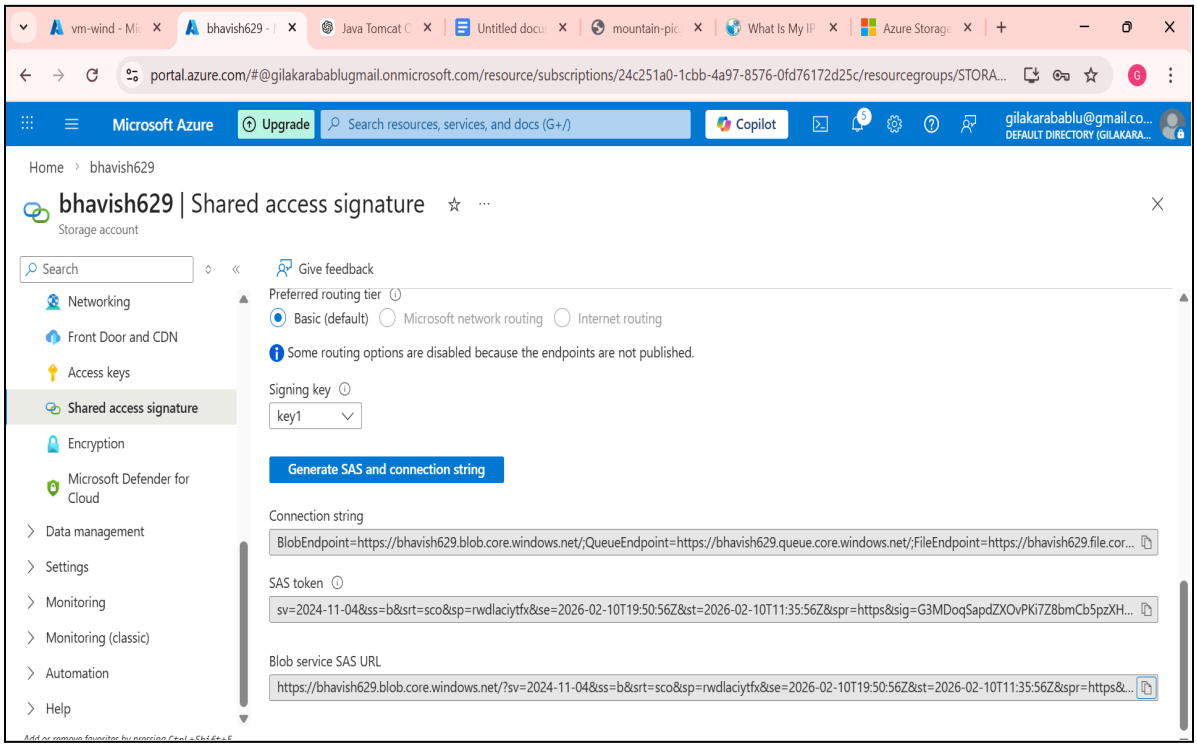


Fig (12) sas keys and connecting string.

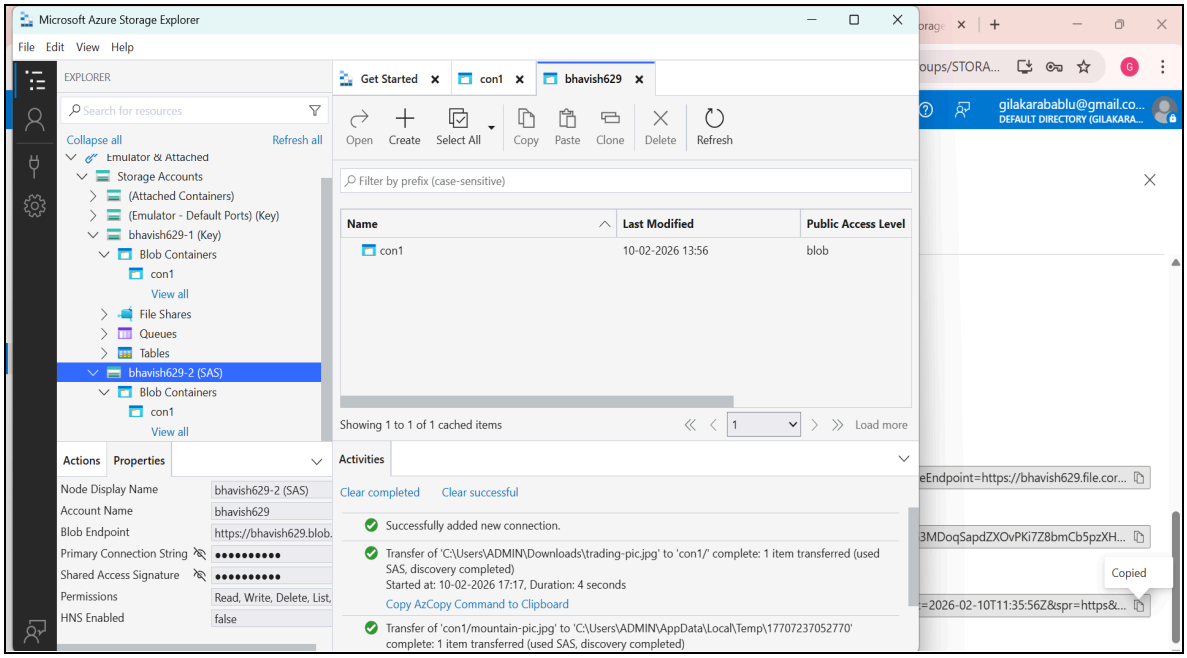
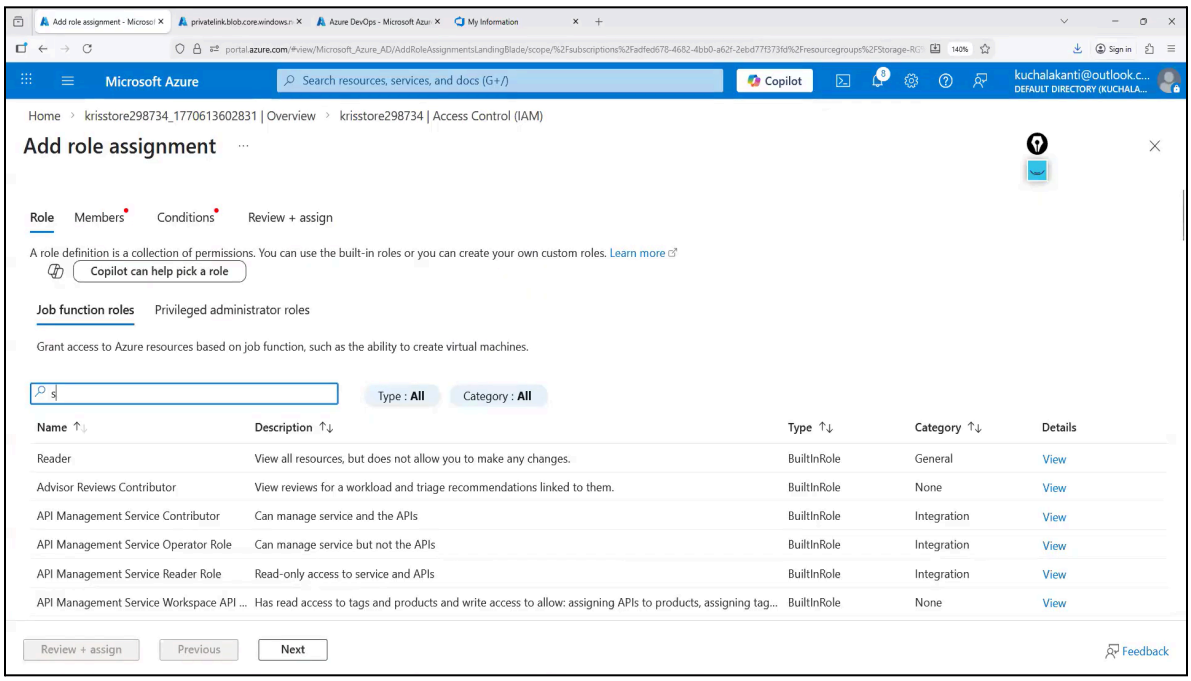


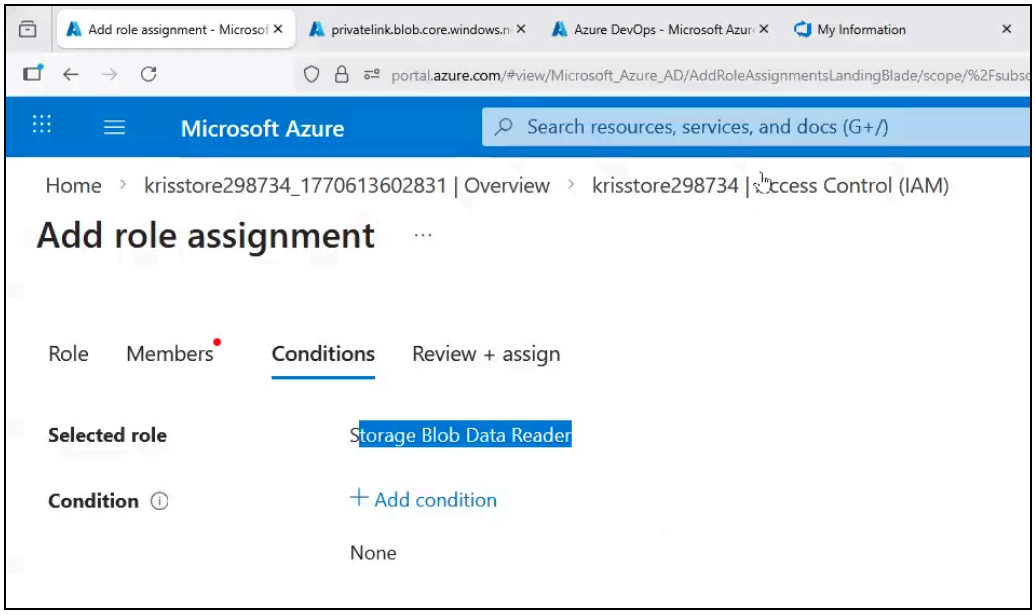
Fig (13) connected to the storage account using sas keys.

→ Roll Based Access Control.



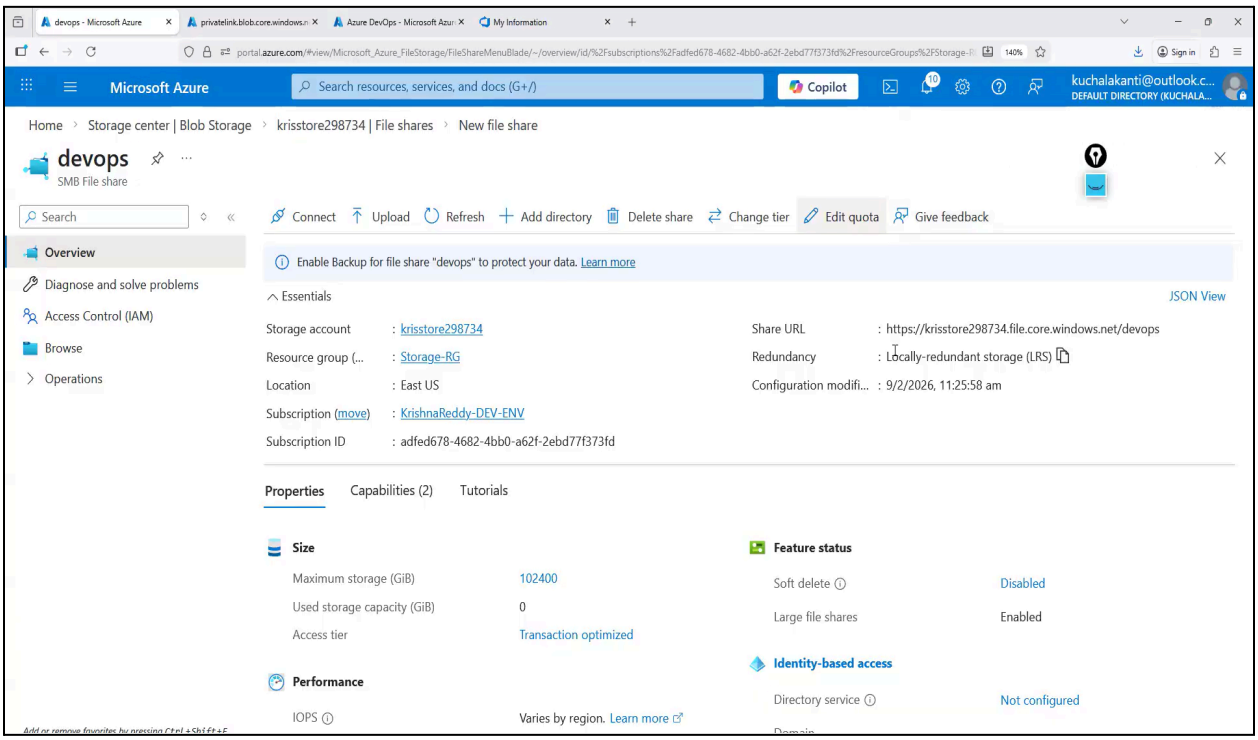
fig(14) adding a role assignment.

→ to add a role goto IAM access control.



fig(15) assigning a storage blob data reader.

→ create a file share.



fig(16) file share is created.

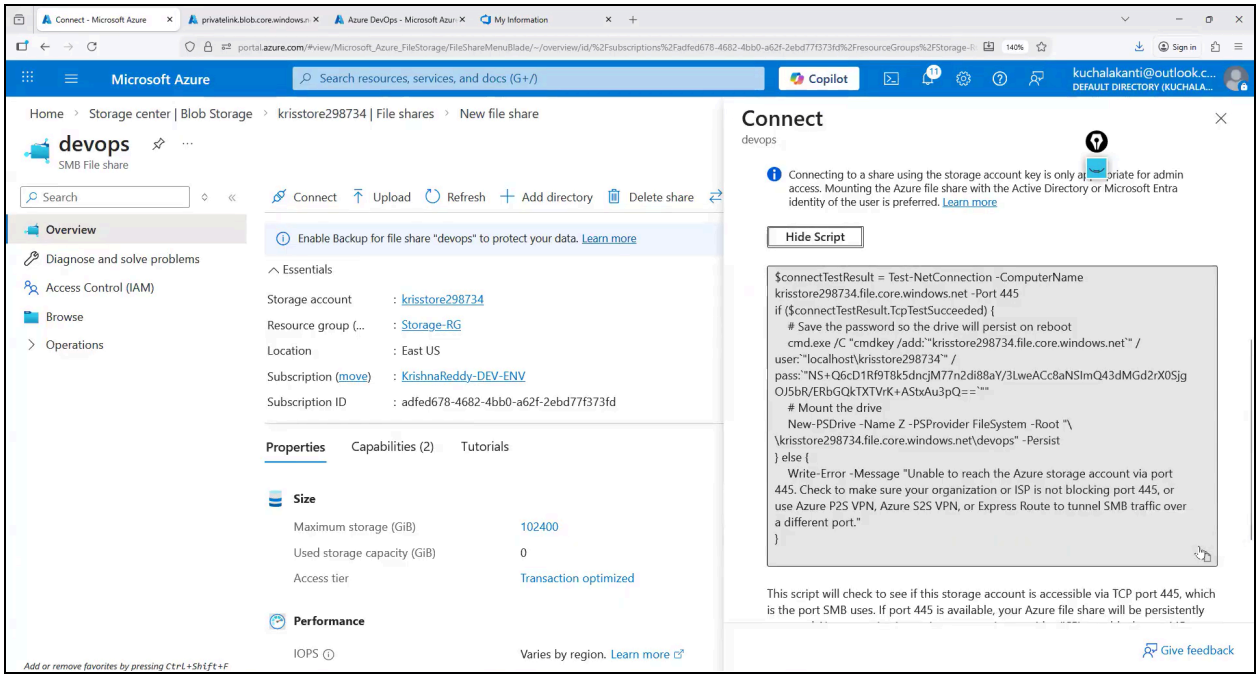
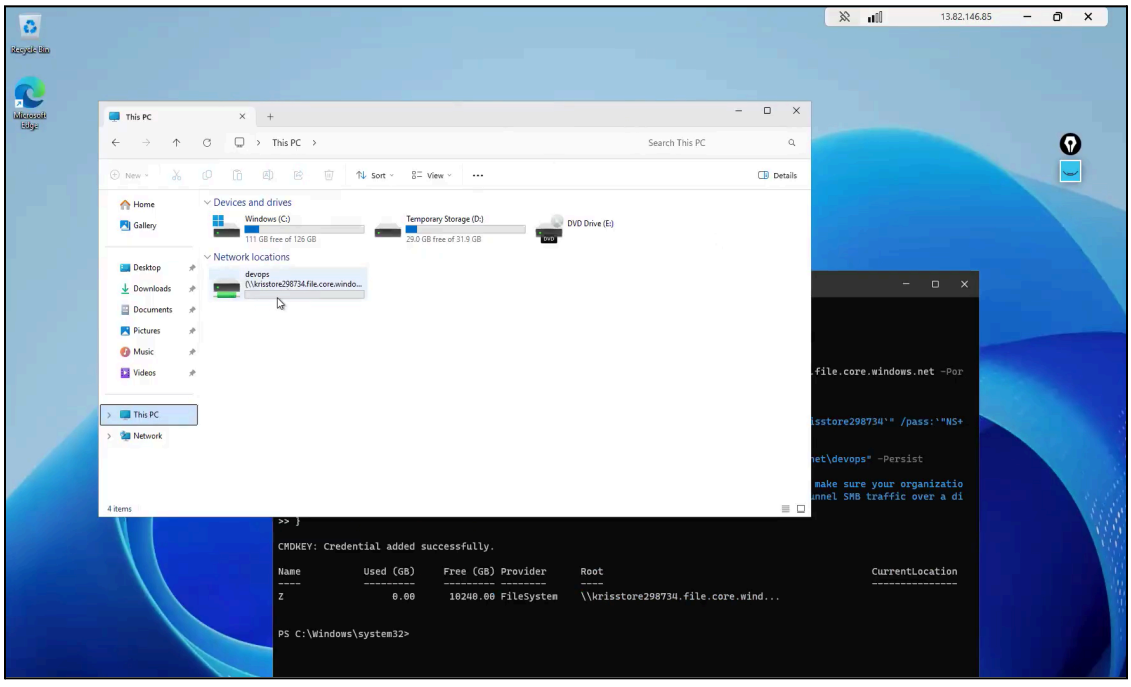


Fig (17) creating a z drive in the windows machine.

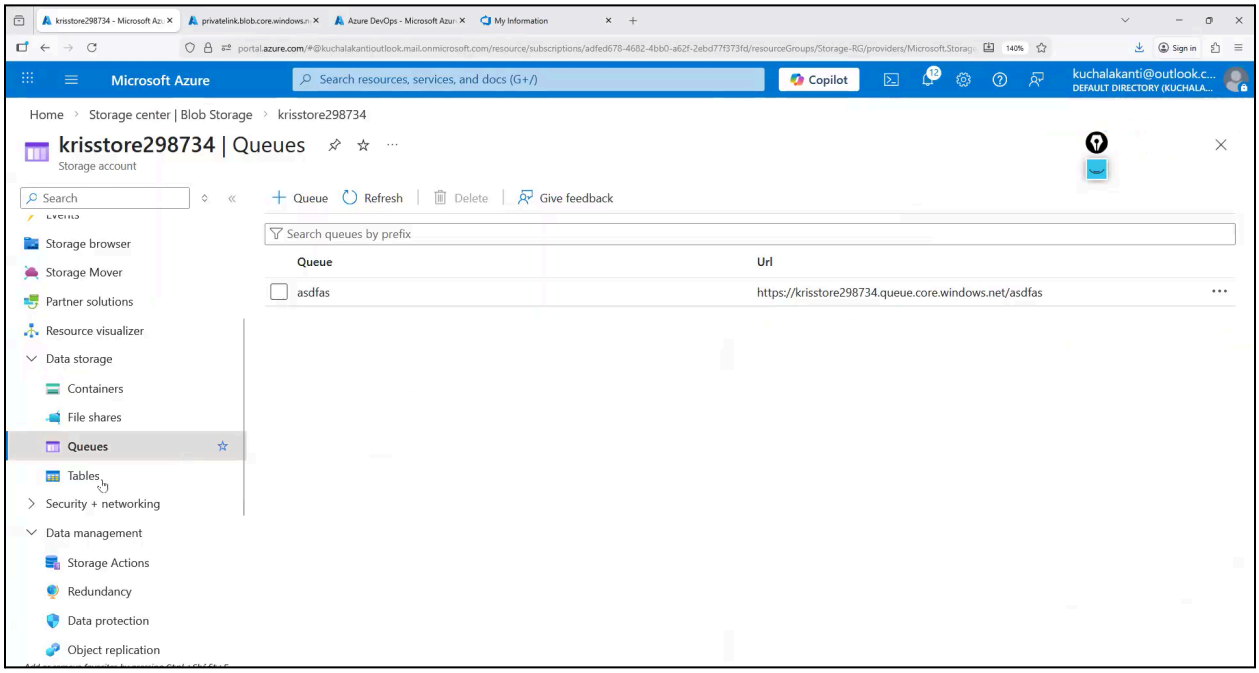
→ copy & paste the above script [fig(17)] in the windows machine powershell to create a Zdrive.



fig(18) created a z drive in the windows machine.

→ QUEUES :-

- When we create a queue we get an endpoint, this endpoint is given to the sql developer,he will add in the database, so that all the data will be store in the Queues.



fig(19) created a queue.

→ TABLES :-

- When we create a Table we get an endpoint, this endpoint is given to the sql developer,he will add in the database, so that all the data will be store in the Tables.

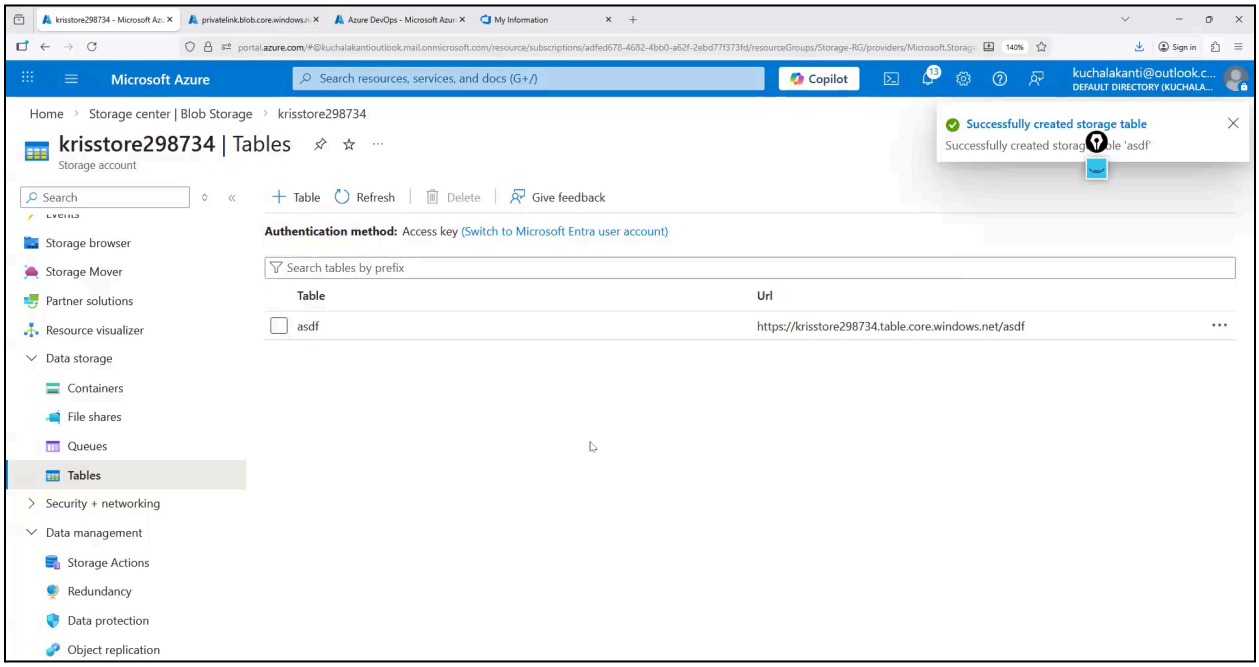


Fig (20) a table is created.