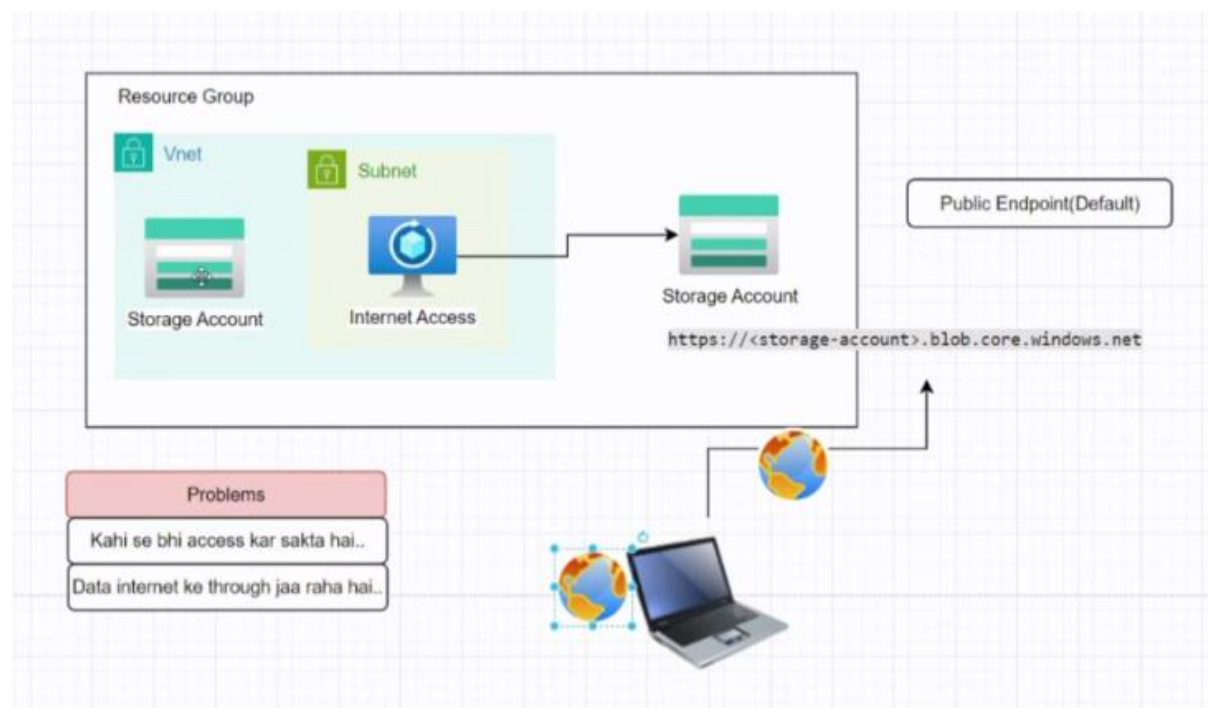


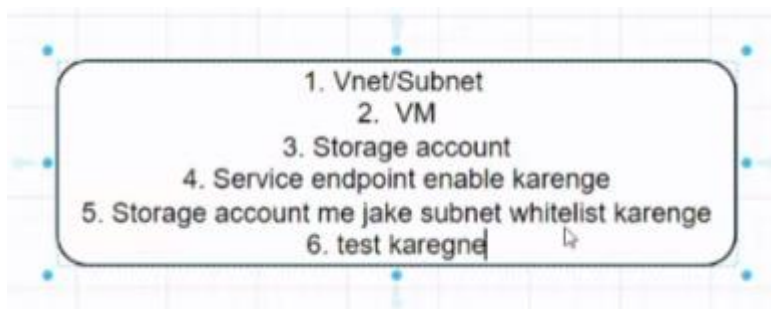
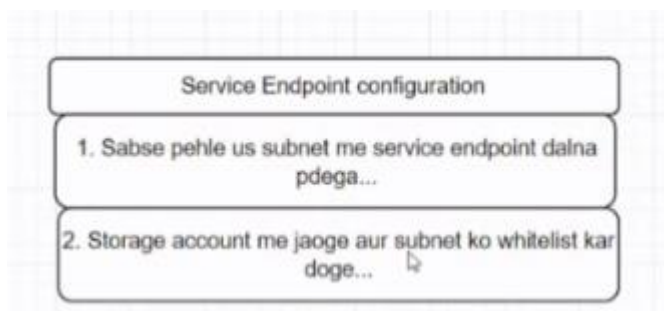
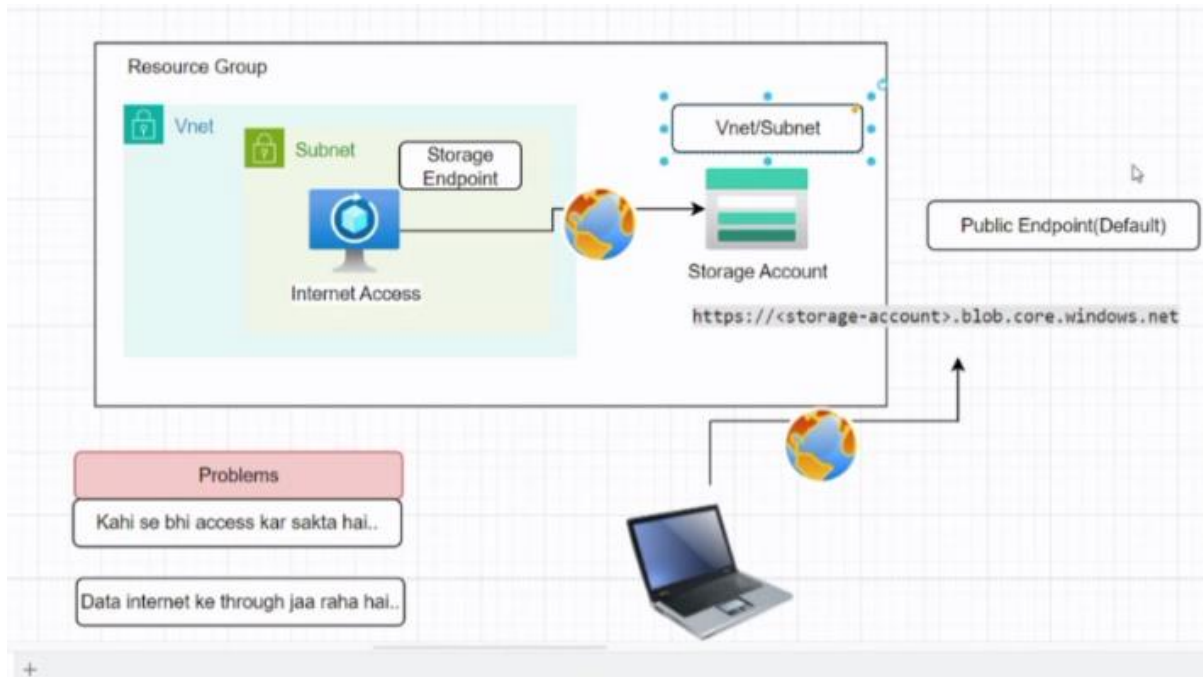
## Assignment - Azure Firewall + UDR Rules

### NSG - Network Security Group

### ASG - Application Security Group

### Difference between Loadbalancer, Application Gateway, Frontdoor, Traffic Manager

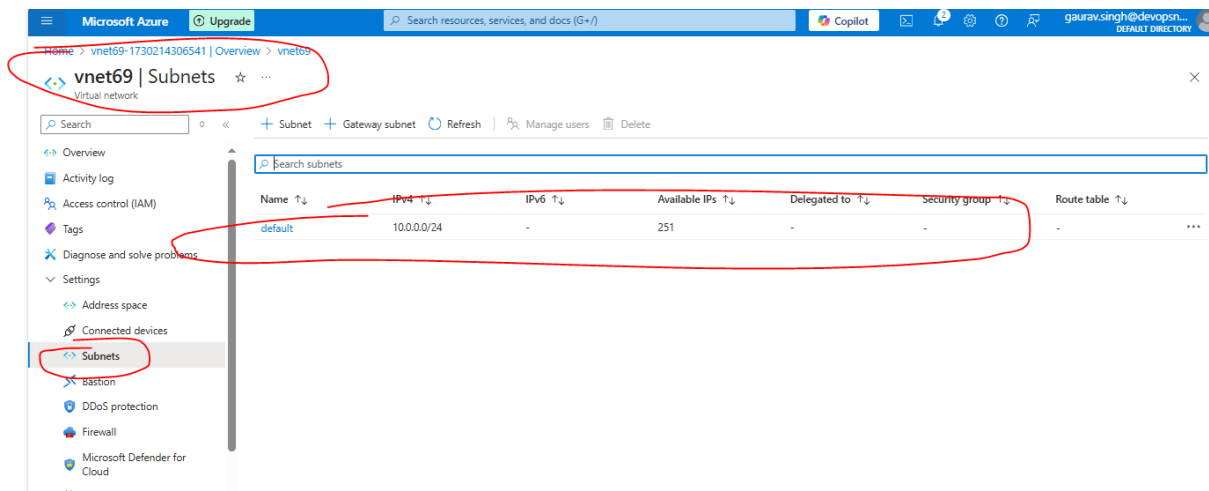




+++++

## AGENDA – Create vnet + subnet

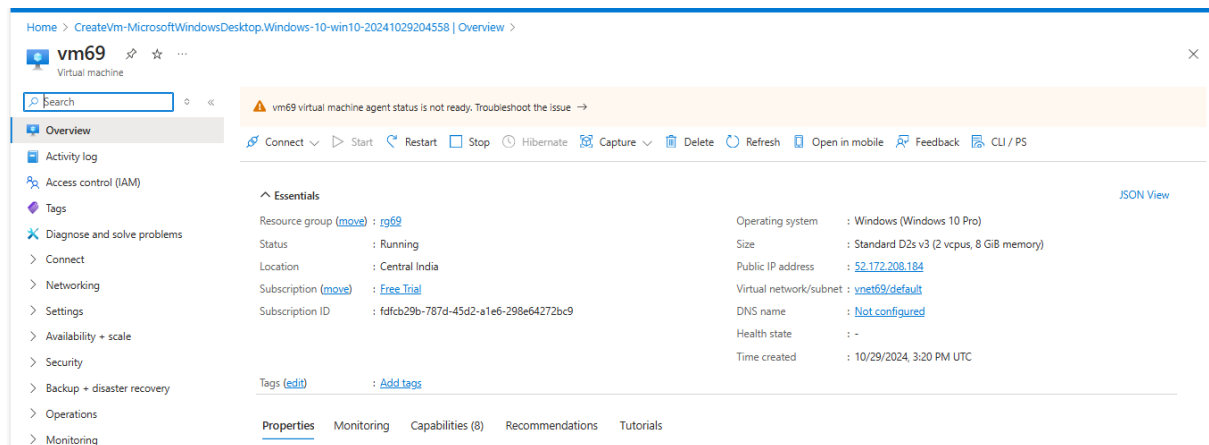
1)



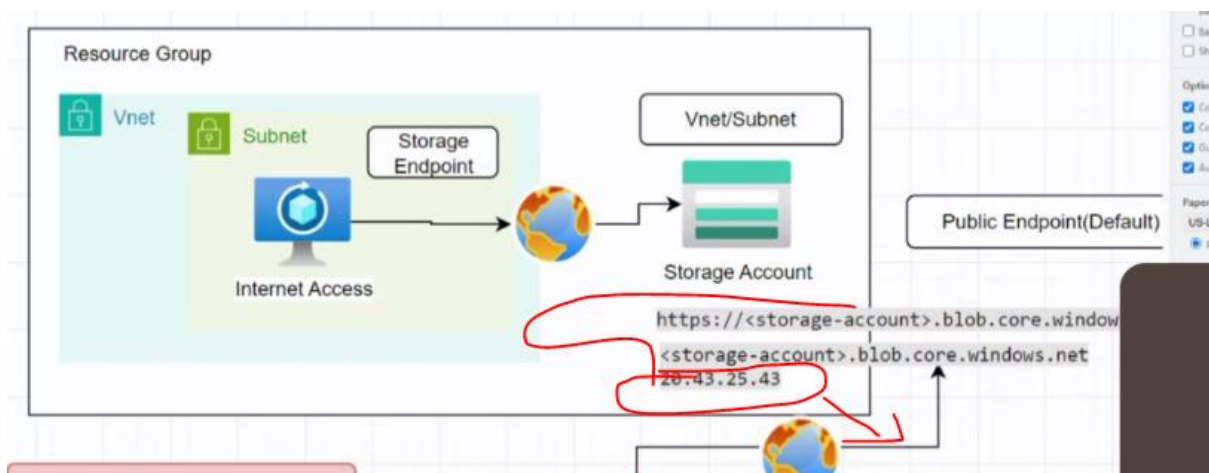
+++++

## AGENDA – Create vm of vm image (OS)

1)



2) The IP we have in url is public only whether its service end point or private end point



+++++

## AGENDA – Create storage account +container+ sas url

1)

The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The breadcrumb trail indicates the user is in the 'Home' view, specifically looking at the 'st69' storage account (ID: 1730216238387) in the 'Overview' section. The 'st69' storage account is highlighted with a red circle. The left sidebar contains a list of navigation options, including 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage browser', 'Storage Mover', 'Partner solutions', 'Data storage', 'Security + networking', 'Data management', 'Settings', 'Monitoring', and 'Monitoring (classic)'. The main content area displays the 'Overview' page for the 'st69' storage account. It includes a search bar, a list of actions (Upload, Open in Explorer, Delete, Move, Refresh, Open in mobile, CLI / PS, Feedback), and a 'Tags' section. The 'Essentials' section provides key information: Resource group (rg69), Location (centralindia), Primary/Secondary Location (Primary: Central India, Secondary: South India), Subscription ID (fd1cb29b-787d-45d2-a1e6-298e64272bc9), Disk state (Primary: Available, Secondary: Available), Performance (Standard), Replication (Read-access geo-redundant storage (RA-GRS)), Account kind (StorageV2 (general purpose v2)), Provisioning state (Succeeded), and Created date (29/10/2024, 9:07:34 pm). The 'Properties' section is expanded, showing 'Blob service' settings: Hierarchical namespace (Disabled), Default access tier (Hot), Blob anonymous access (Disabled), Blob soft delete (Enabled (7 days)), Container soft delete (Enabled (7 days)), and Versioning (Disabled). The 'Security' section shows 'Require secure transfer for REST API operations' (Enabled), 'Storage account key access' (Enabled), 'Minimum TLS version' (Version 1.2), and 'Infrastructure encryption' (Disabled). The 'Networking' section is also visible.

2) Search – DNS checker – takes out ip address of website

The screenshot shows a DNS checker tool interface. At the top, it displays the search result for 'GOOGLE.COM'. Below this, there are buttons for 'Expand All' and 'Download Records'. The 'Jump to:' section lists various record types: A Records, AAAA Records, CNAME Records, MX Records, NS Records, PTR Records, SRV Records, SOA Records, TXT Records, CAA Records, DS Records, and DNSKEY Records. The 'A' record section is expanded, showing a table with columns: Type, Domain Name, TTL, and Address. The table contains one record for 'google.com' with a TTL of 300 and an IP address of 142.250.176.206. The IP address is circled in red. Below the 'A' record section, the 'AAAA' record section is also expanded, showing a table with columns: Type, Domain Name, TTL, and Address. The table contains one record for 'google.com' with a TTL of 24 and an IPv6 address of 2607:f8b0:4006:820::200e. The IP address is also circled in red. At the bottom of the page, there is a 'CNAME' section and a privacy policy notice: 'By clicking "Accept" or continuing to use our site, you agree to our Website's Privacy Policy'. An 'Accept' button is visible.

Storage service	Endpoint
Blob Storage	<code>https://&lt;storage-account&gt;.blob.core.windows.net</code>
Static website (Blob Storage)	<code>https://&lt;storage-account&gt;.web.core.windows.net</code>
Data Lake Storage	<code>https://&lt;storage-account&gt;.dfs.core.windows.net</code>
Azure Files	<code>https://&lt;storage-account&gt;.file.core.windows.net</code>
Queue Storage	<code>https://&lt;storage-account&gt;.queue.core.windows.net</code>
Table Storage	<code>https://&lt;storage-account&gt;.table.core.windows.net</code>

### 3) Create container

Home > st69

**st69 | Containers**

Storage account

Search

+ Container Change access level Restore containers Refresh Delete Give feedback

Search containers by prefix

Name	Last modified	Anonymous access level	Leas
\$logs	10/29/2024, 9:08:05 PM	Private	Avai
container69	10/29/2024, 9:10:19 PM	Private	Avai

### 4) Now put file into it

Microsoft Azure Upgrade

Search resources, services, and docs (G+)

Copilot

Home > st69 | Containers >

**container69**

Container

Search

Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Crea

Overview

Diagnose and solve problems

Access Control (IAM)

Settings

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

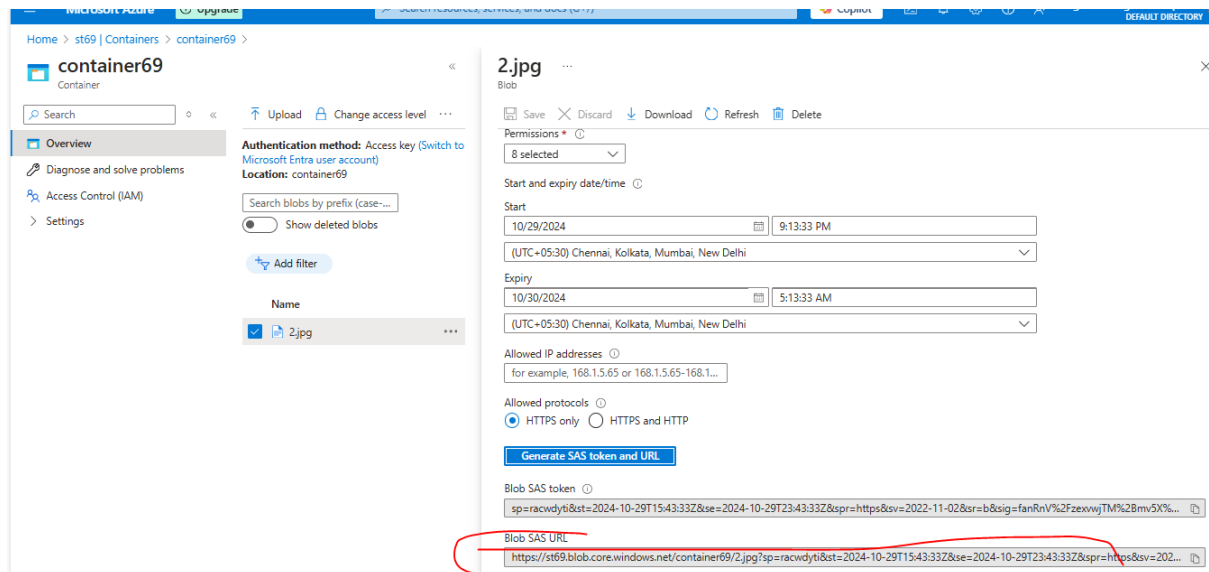
Location: container69

Search blobs by prefix (case-sensitive)

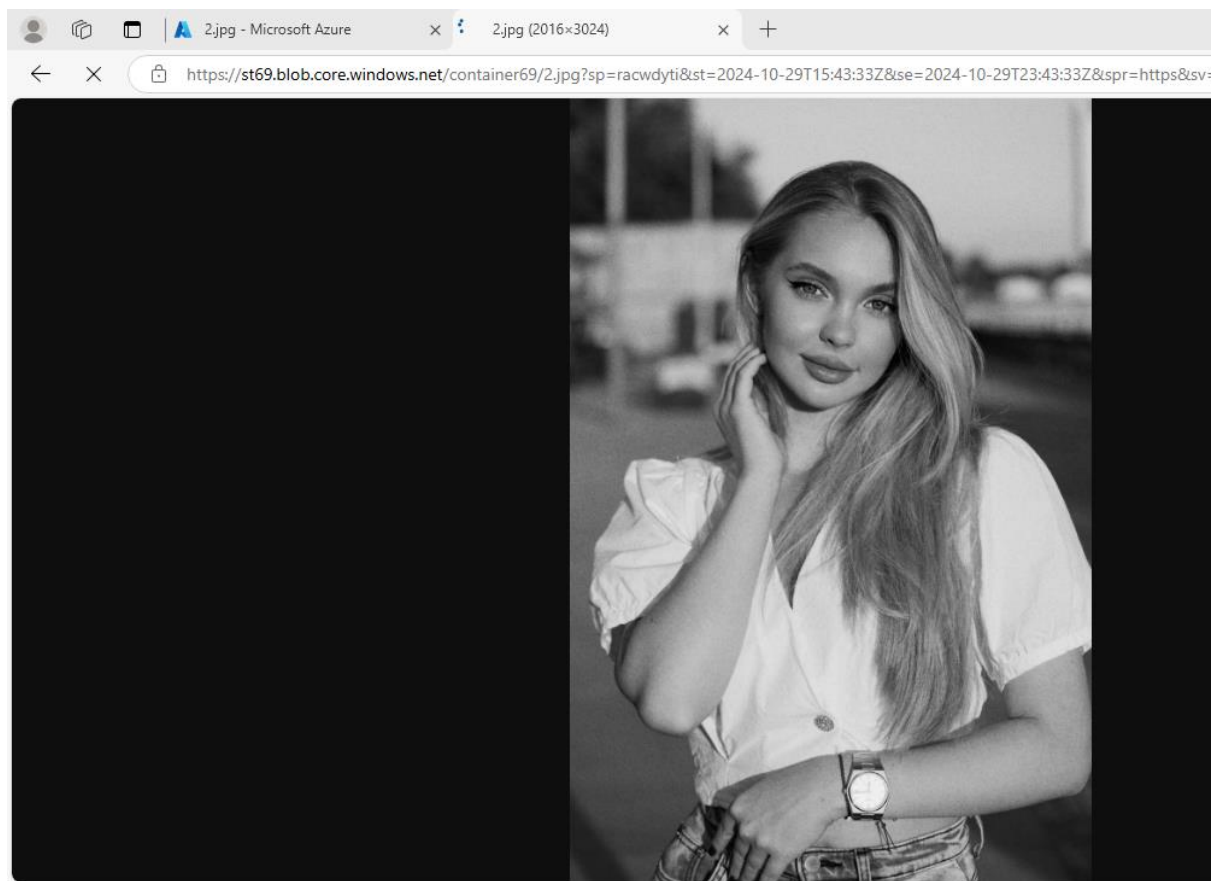
Add filter

Name	Modified	Access tier	Archive status	Blob type	Size
2.jpg	10/29/2024, 9:12:55 ...	Hot (Inferred)		Block blob	575.

### 5) Generate sas



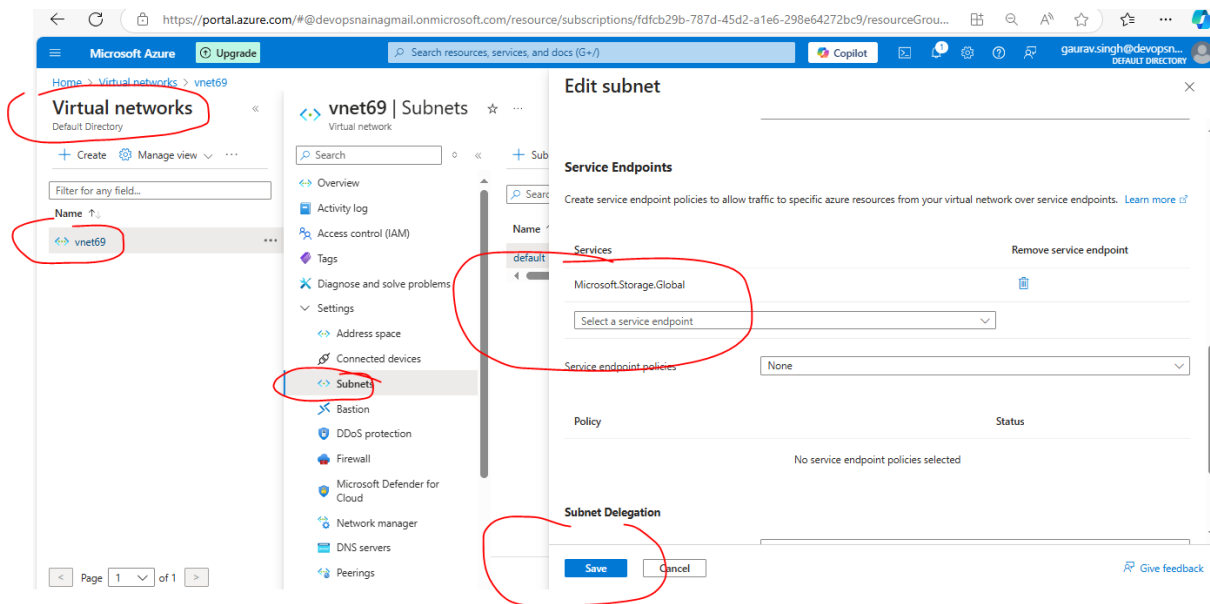
## 6) Access url on browser



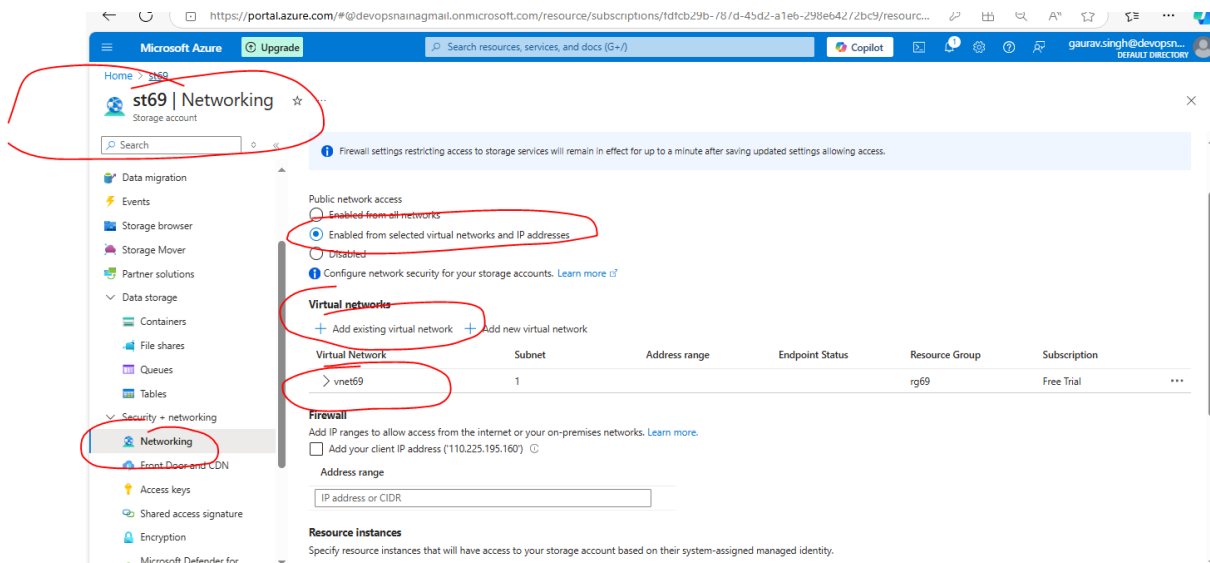
+++++

**AGENDA – Want that above blob url should access only by that subnet which is inside out vnet**

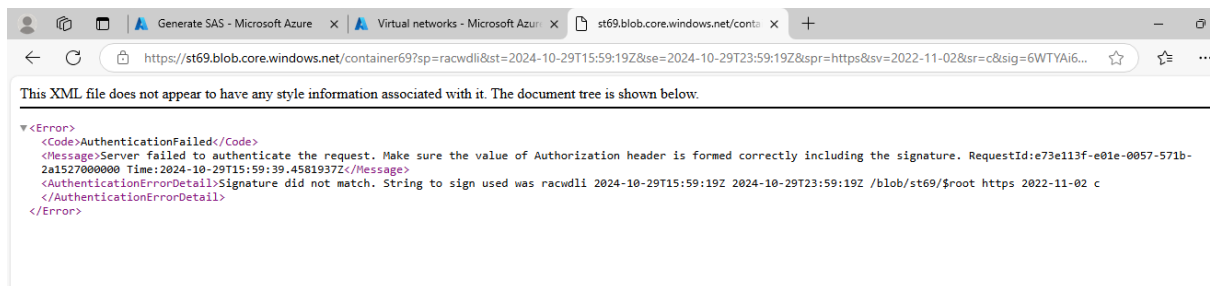
1) For Enabling service point -> Go to vnet -> subnet -> default -> Service endpoints -> Microsoft.service.global -> save



2) Go to storage account -> networking -> Enabled from selected virtual networks and IP addresses -> Enable service point -> Add existing virtual network – save. So service end point is put at subnet level



3) Now again try to access blob url of uploaded image in container, so its not accessible because we have restricted to as specific subnet in vnet



4) We checked in dns look up, still blob url has public ip

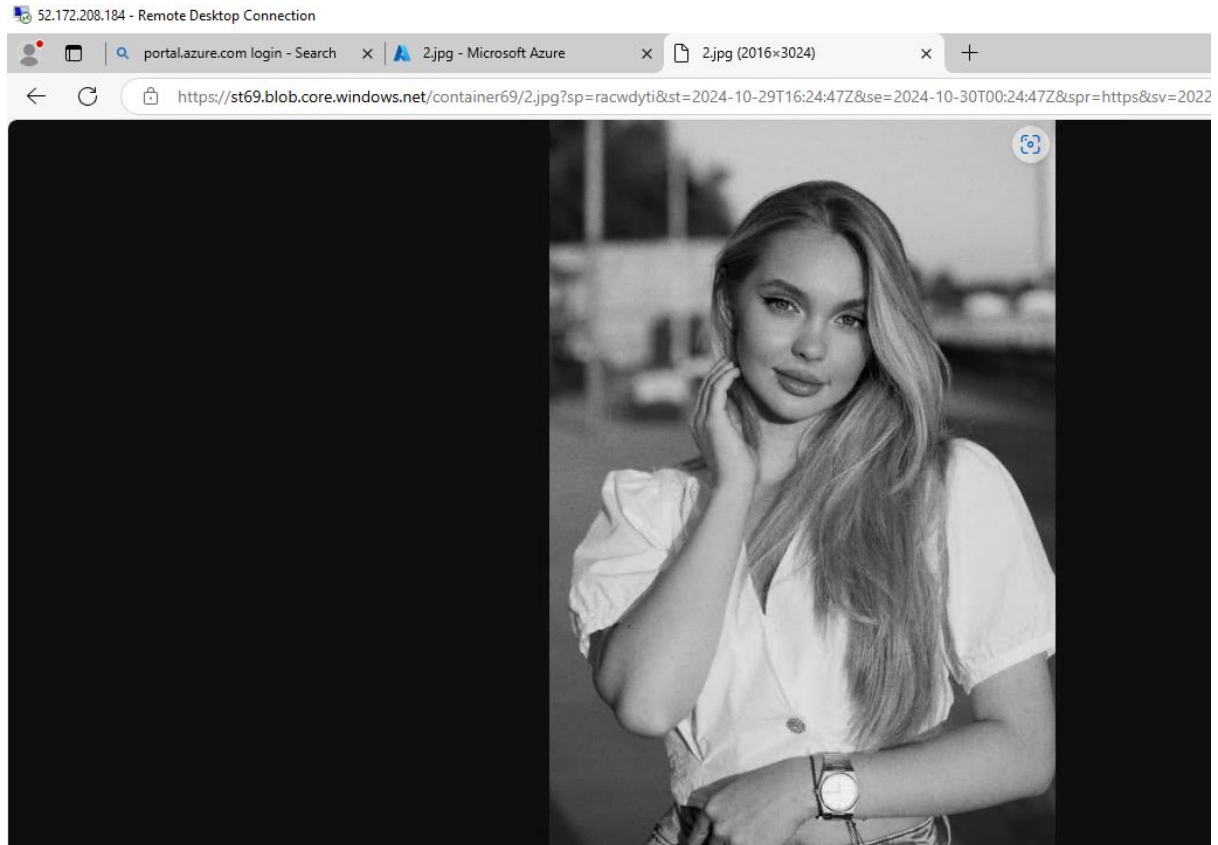
+++++

## **AGENDA – CONNECT TO VM NOW**

1) Do rdp in vm

2) Run same blob url then it will run inside vm

3)



+++++

## **AGENDA – disable public endpoint**

1) Go to storage end point and Now disable public end point



Home > st69

## st69 | Networking

Storage account

Search

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)

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh Give feedback

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
vnet69	1			rg69	Free Trial

**Firewall**

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

☐ Add your client IP address (110.225.195.160) ⓘ

Address range

IP address or CIDR

Firewalls and virtual networks Private endpoint connections Custom domain

Save Discard Refresh Give feedback

Public network access to this storage account has been disabled. Please create a private endpoint connection to grant access.

2) Now inside vm also we will not be to access blob url

52.172.208.184 - Remote Desktop Connection

portal.azure.com login - Search x 2.jpg - Microsoft Azure x st69.blob.core.windows.net/cont x +

https://st69.blob.core.windows.net/container69/2.jpg?sp=racwdyti&st=2024-10-29T16:24:47Z&se=2024-10-30T00:24:47Z&spr=https&sv=2022...

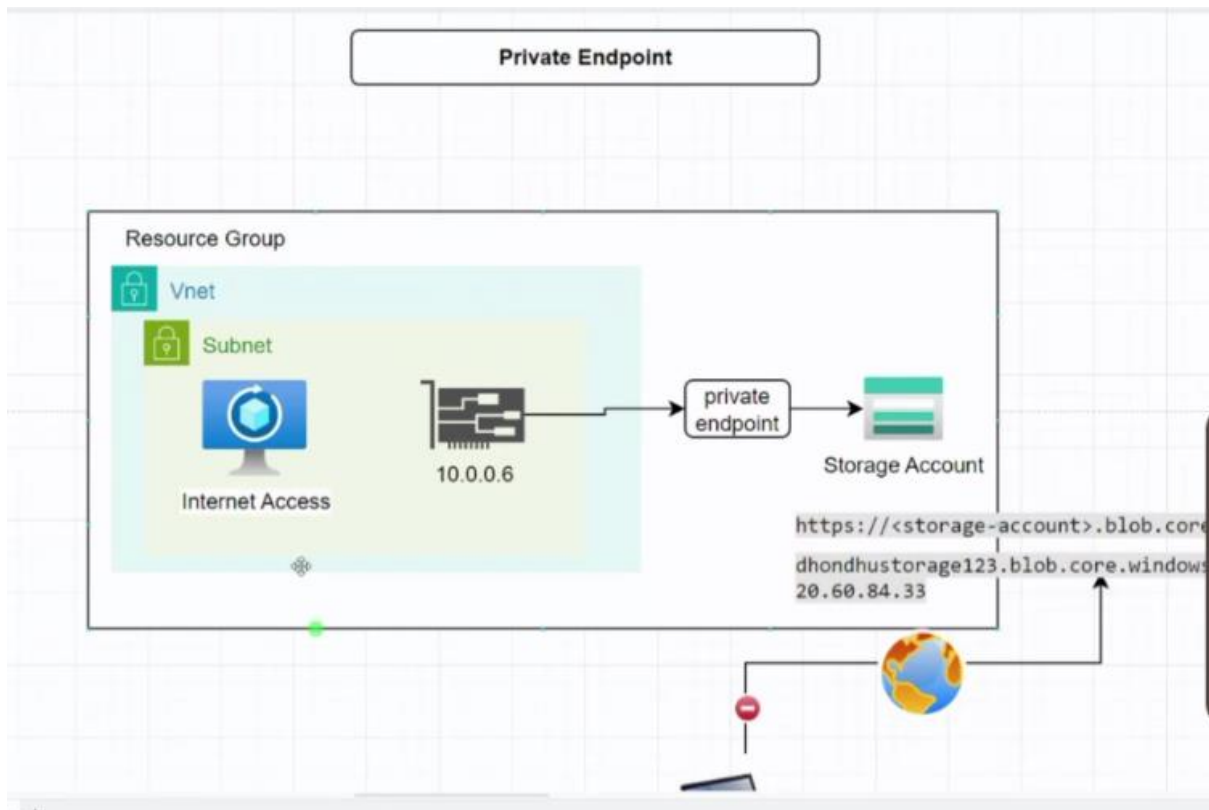
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Error>
  <Code>AuthorizationFailure</Code>
  <Message>This request is not authorized to perform this operation. RequestId:8d7656be-a01e-0024-5f22-2a4db4000000 Time:2024-10-29T16:51:56.9166645Z</Message>
</Error>
```

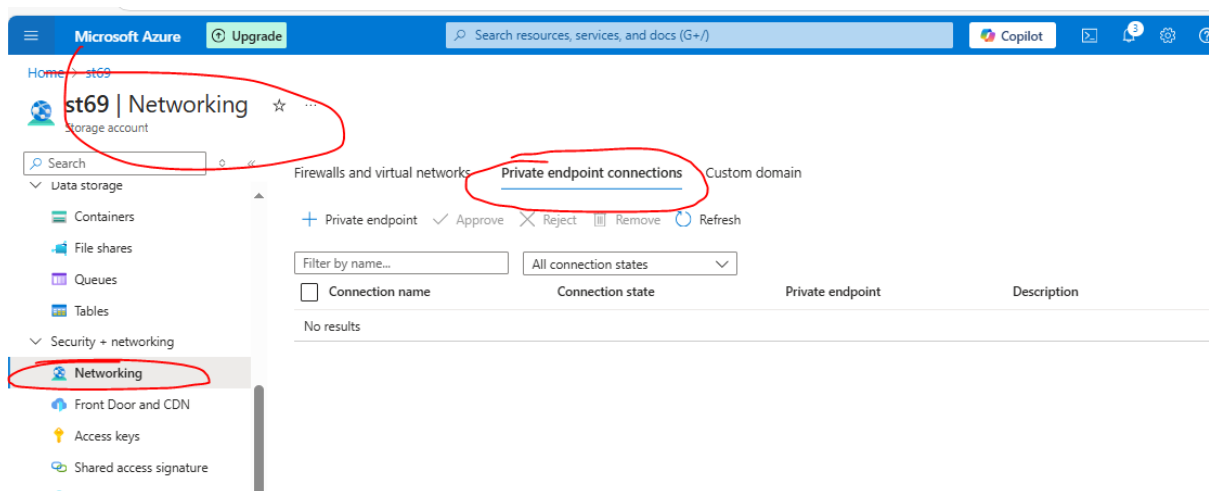
+++++

## AGENDA – CREATE private endpoint

1) When we enable private endpoint, then a nic card is created in vet and an ip address is allocated on this nic card



2) go to st acc -> private end point connections



3) nslookup tool

```
Windows PowerShell
PS C:\Users\aaes> nslookup dhondhustorage123.blob.core.windows.net
Server:  reliance.reliance
Address: 205:201:301c:5901::c0a8:1d01

Non-authoritative answer:
Name:    blob.pn1prdstr10a.store.core.windows.net
Address: 20.60.84.33
Aliases: dhondhustorage123.blob.core.windows.net

PS C:\Users\aaes> nslookup dhondhustorage123.blob.core.windows.net
Server:  reliance.reliance
Address: 2405:201:301c:5901::c0a8:1d01

Non-authoritative answer:
Name:    blob.pn1prdstr10a.store.core.windows.net
Address: 20.60.84.33
Aliases: dhondhustorage123.blob.core.windows.net

PS C:\Users\aaes>
```

4) Now create private end point

## Create a private endpoint

✓ Basics **2 Resource** ③ Virtual Network ④ DNS ⑤ Tags ⑥ Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription Free Trial (fdfcb29b-787d-45d2-a1e6-298e64272bc9)

Resource type Microsoft.Storage/storageAccounts

Resource st69

Target sub-resource \* ⓘ blob

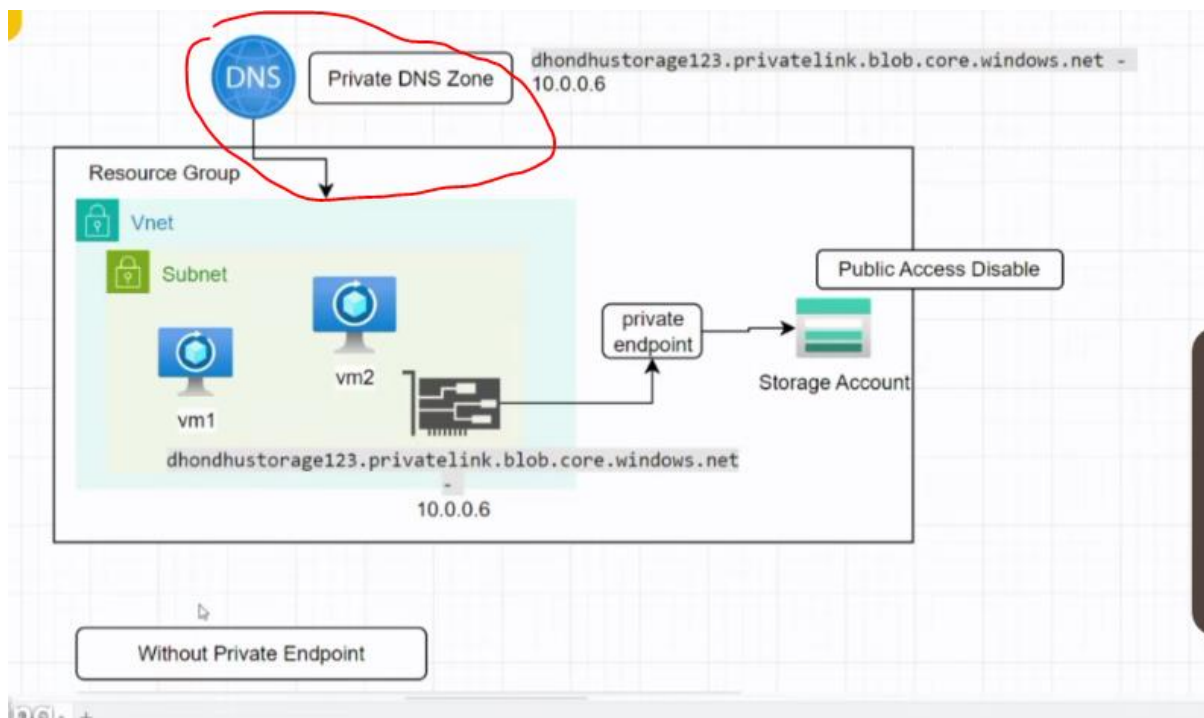
Without Private Endpoint

```
dhondhustorage123.blob.core.windows.net - (A) 20.60.84.33
```

With Private Endpoint

```
dhondhustorage123.blob.core.windows.net - (CNAME) - dhondhustorage123.privatelink.blob.core.windows.net
dhondhustorage123.privatelink.blob.core.windows.net - 20.60.84.33
```

5) A private DNS zone is need to be created. Just click yes it will be made



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

Home > st69 | Networking >

## Create a private endpoint ...

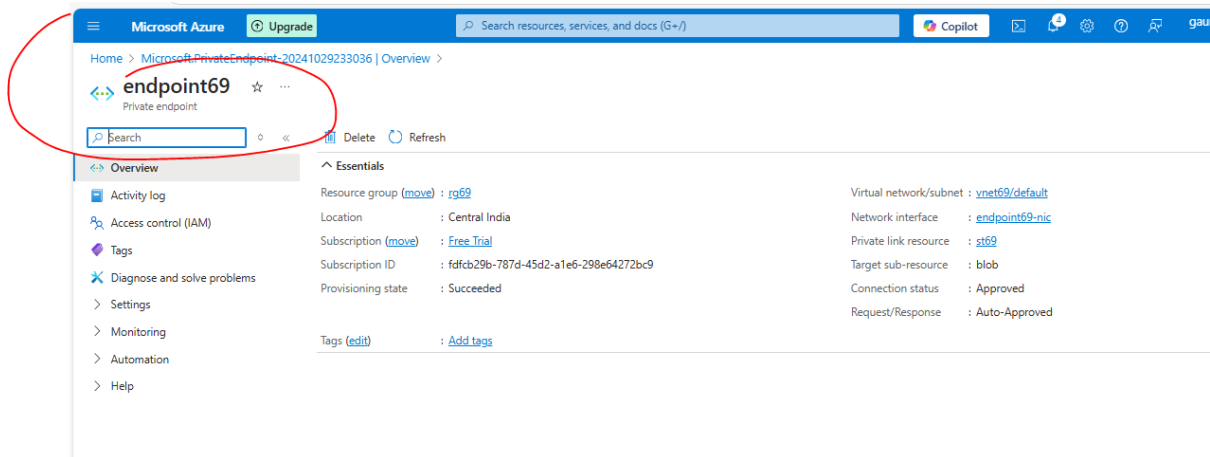
✓ Basics ✓ Resource ✓ Virtual Network **✓ DNS** ⑤ Tags ⑥ Review + create

### Private DNS integration

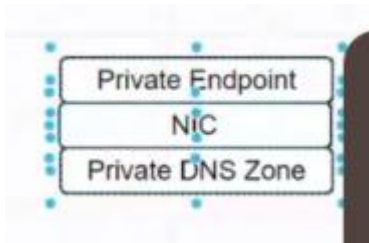
To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-blob-core-win...	Free Trial	rg69	(new) privatelink.blob.cor...

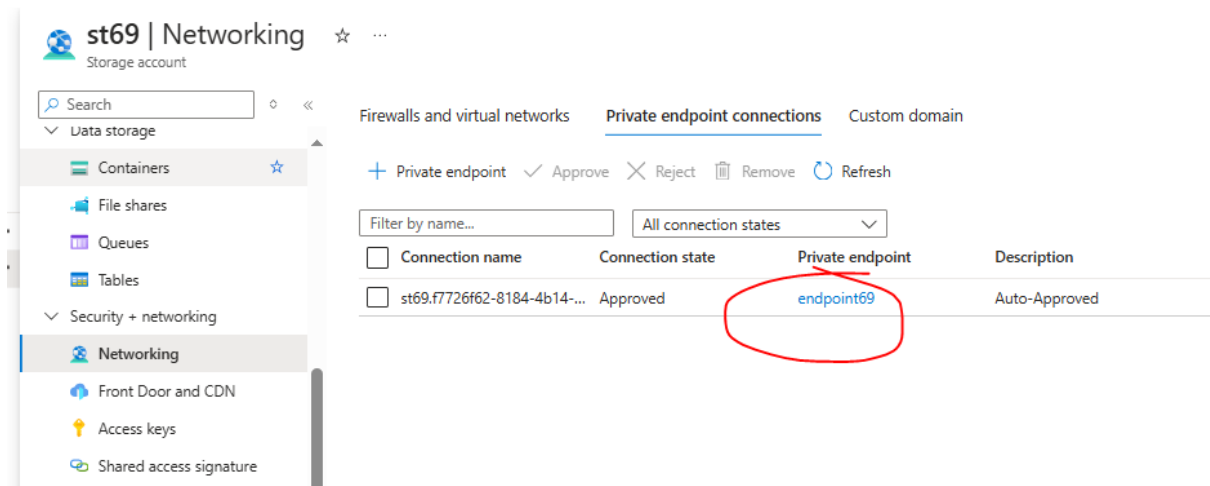


6) So now resources created will be



7) Basically dns zone is optional but then we have to set up private ip and other things manually

8) Now go to storage account -> networking -> private end point -> click on name -> DNS configuration ->



**endpoint69 | DNS configuration**

Private endpoint

Search

+ Add configuration Refresh

endpoint using a private DNS zone. You can also utilize your own DNS servers. [Learn more](#)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Application security groups

**DNS configuration**

Properties

Locks

Monitoring

Automation

Help

**Customer Visible FQDNs**

DNS records visible to the customer

Network Interface	IP addresses	FQDN
endpoint69-nic	10.0.0.5	st69.blob.core.windows.net

Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
privatelink-blob-c...			Free Trial	privatelink.blob.core.windows...	default
st69.privatelink.blob.core.windows...		10.0.0.5			

9) Go to private dns zones – so there is one created

**Private DNS zones**

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags Delete

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 1 of 1 records.

Name	Num...	Max n...	Num...	Num...	Resource group
privatelink.blob.core.windows.net	1	25,000	0 / 1000	0 / 100	rg69

**privatelink.blob.core.windows.net | Recordsets**

Private DNS zone

Search

+ Add Refresh Delete

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Properties

Locks

DNS Management

**Recordsets**

Virtual Network Links

Monitoring

Automation

Help

A record set is a collection of records in a zone that have the same name and are the same type. Record Sets will be automatically fetched in batches of 100 as you scroll through the existing record sets. [Learn more](#)

Search

Fetched 2 record set(s).

0 record sets selected

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host@microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
st69	A	10	10.0.0.5	False

10)

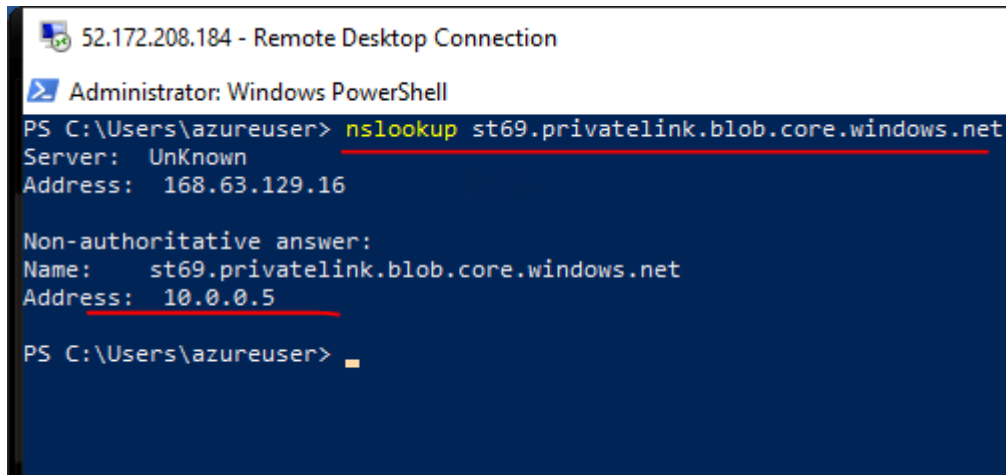
privatelink.blob.core.windows.net

st69 - 10.0.0.5

=> st69.privatelink.blob.core.windows.net

11) Go inside vm and open powershell

**nslookup st69.privatelink.blob.core.windows.net**

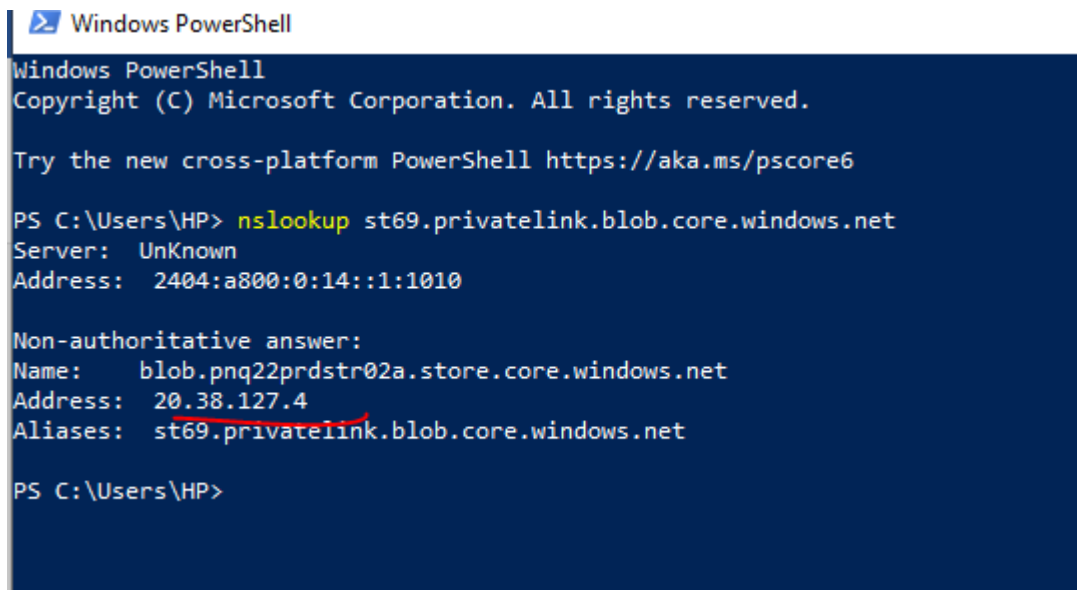


```
52.172.208.184 - Remote Desktop Connection
Administrator: Windows PowerShell
PS C:\Users\azureuser> nslookup st69.privatelink.blob.core.windows.net
Server: UnKnown
Address: 168.63.129.16

Non-authoritative answer:
Name: st69.privatelink.blob.core.windows.net
Address: 10.0.0.5

PS C:\Users\azureuser>
```

12) Now do in local comp which shows public ip



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

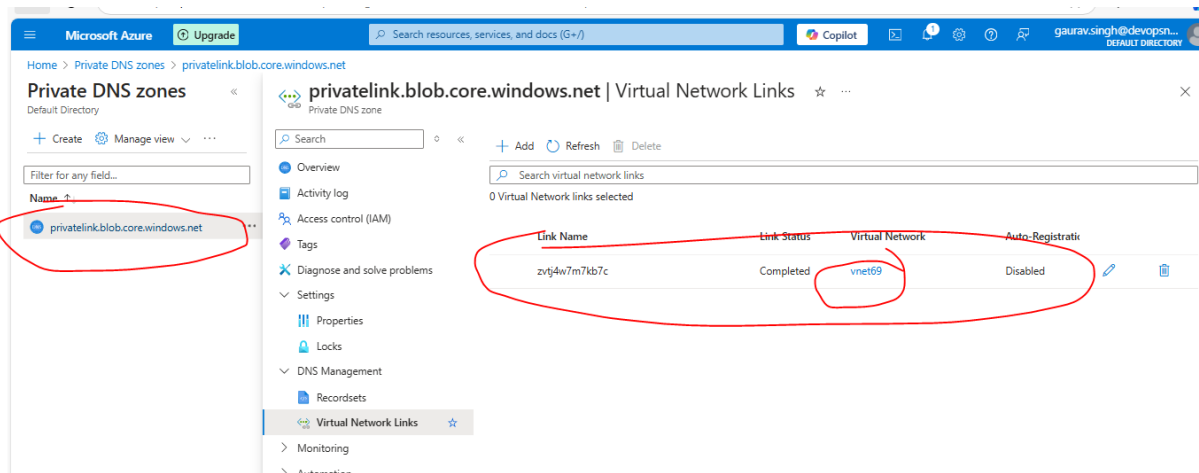
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\HP> nslookup st69.privatelink.blob.core.windows.net
Server: UnKnown
Address: 2404:a800:0:14::1:1010

Non-authoritative answer:
Name: blob.pnq22prdstr02a.store.core.windows.net
Address: 20.38.127.4
Aliases: st69.privatelink.blob.core.windows.net

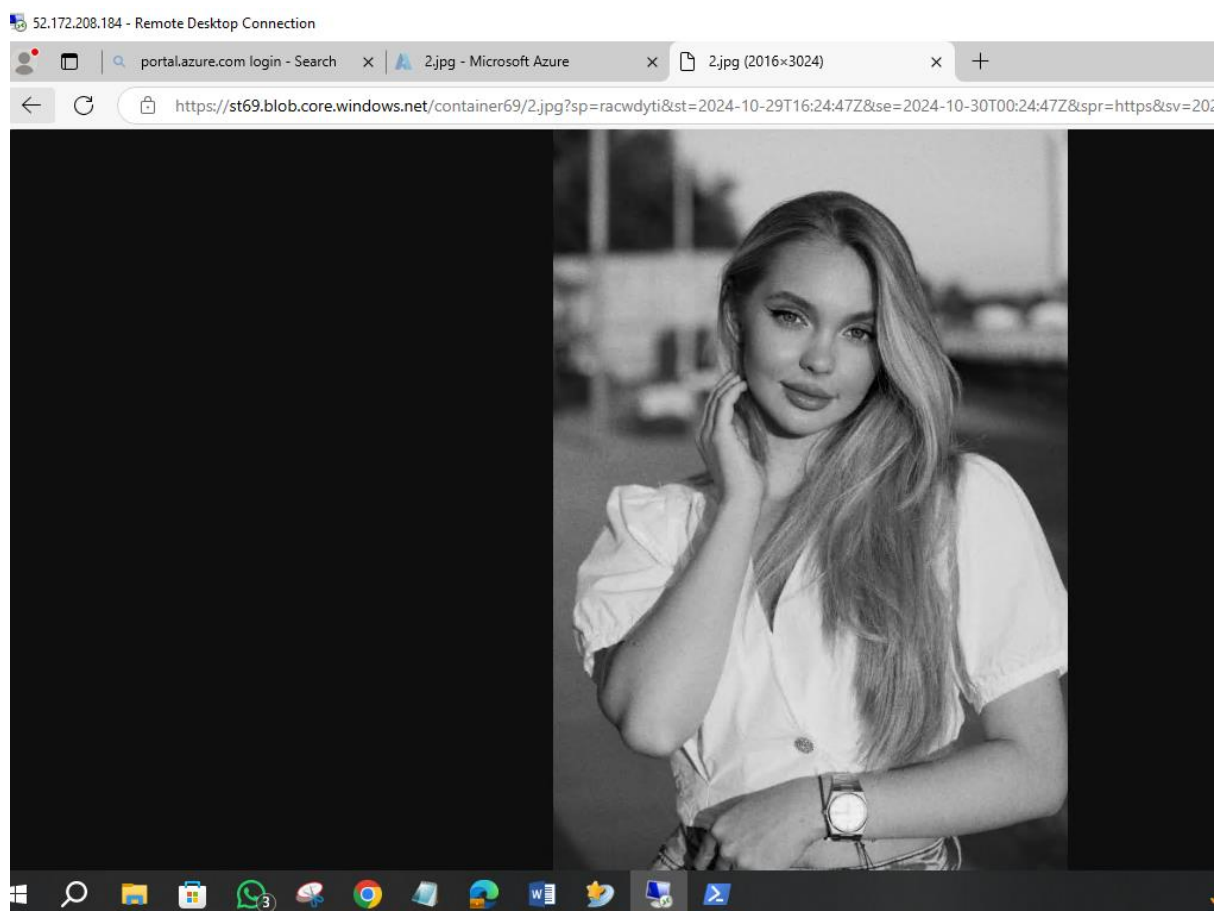
PS C:\Users\HP>
```

12) Checknig private dns zone is linked to vnet



13) Now same blob url again works in vm

<https://st69.blob.core.windows.net/container69/2.jpg?sp=racwdyti&st=2024-10-29T16:24:47Z&se=2024-10-30T00:24:47Z&spr=https&sv=2022-11-02&sr=b&sig=J4cP7d7ilhOfY3%2B6ZvMrkvwwgn1tiB4p7qa%2B82ADp4%3D>





### Interview Questions

Private endpoint banate samay kya kya banta hai?

Service Endpoint banate samay kya kya banta hai?

Private endpoint vs service endpoint ke beech difference?

### Question of the Weeek

Highly Available, Highly Secure, Highly Scalable...Sab kuch highlly wala environment