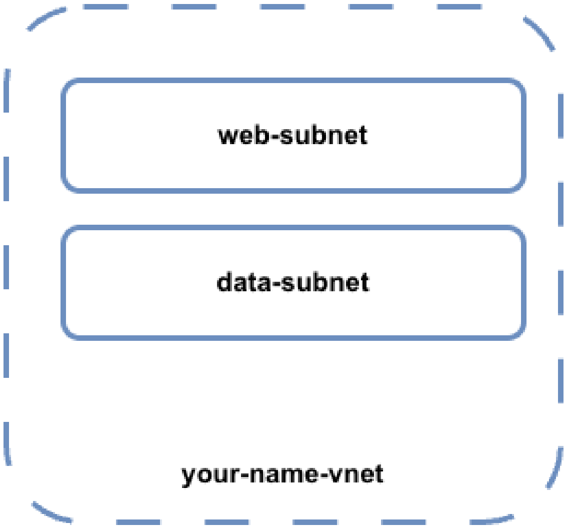
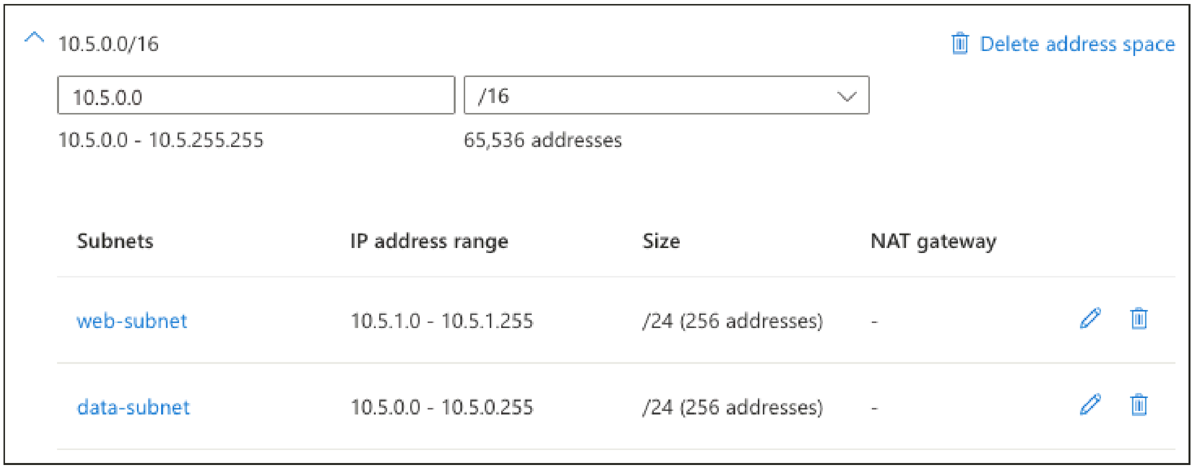
Create a VNet with Two Subnets

1. Create a resource group
    - Go to Resource groups
    - Click **Create**
    - Name: **your-name-rg**
    - Choose a region
    - Click **Review + create** → **Create**
2. Create a virtual network
    - Go to Virtual networks
    - Click **Create**
    - Resource group: **your-name-rg**
    - Name: **your-name-vnet**
    - Choose the same region





10.5.0.0/16

10.5.0.0 | /16

10.5.0.0 - 10.5.255.255 | 65,536 addresses

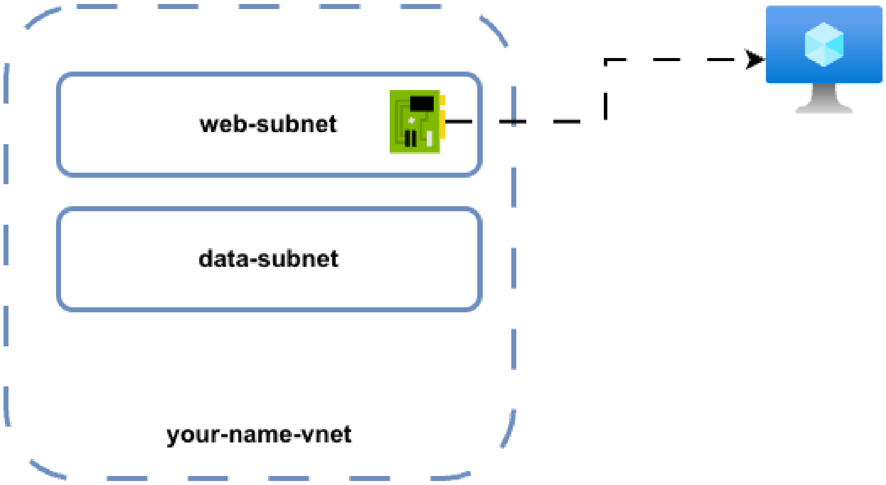
Subnets	IP address range	Size	NAT gateway
web-subnet	10.5.1.0 - 10.5.1.255	/24 (256 addresses)	-
data-subnet	10.5.0.0 - 10.5.0.255	/24 (256 addresses)	-

3. Add subnets
    - Go to the **IP addresses** tab
    - Click **Add subnet**
        - Name: **web-subnet**
        - Choose an address range
            - Replace X with a number between 5-255
            - Make sure X is unique across the room
    - Click **Add subnet** again
        - Name: **data-subnet**
        - Choose an address range
4. Finish creation
    - Click **Review + create**

- Click **Create**

5. Verify
    - Open **your-name-vnet**
    - Go to **Subnets**
    - Confirm **web-subnet** and **data-subnet** are listed
6. **Restore a Virtual Machine from a Backup Vault** and place it in web-subnet

Steps to Restore a Virtual Machine from a Backup Vault

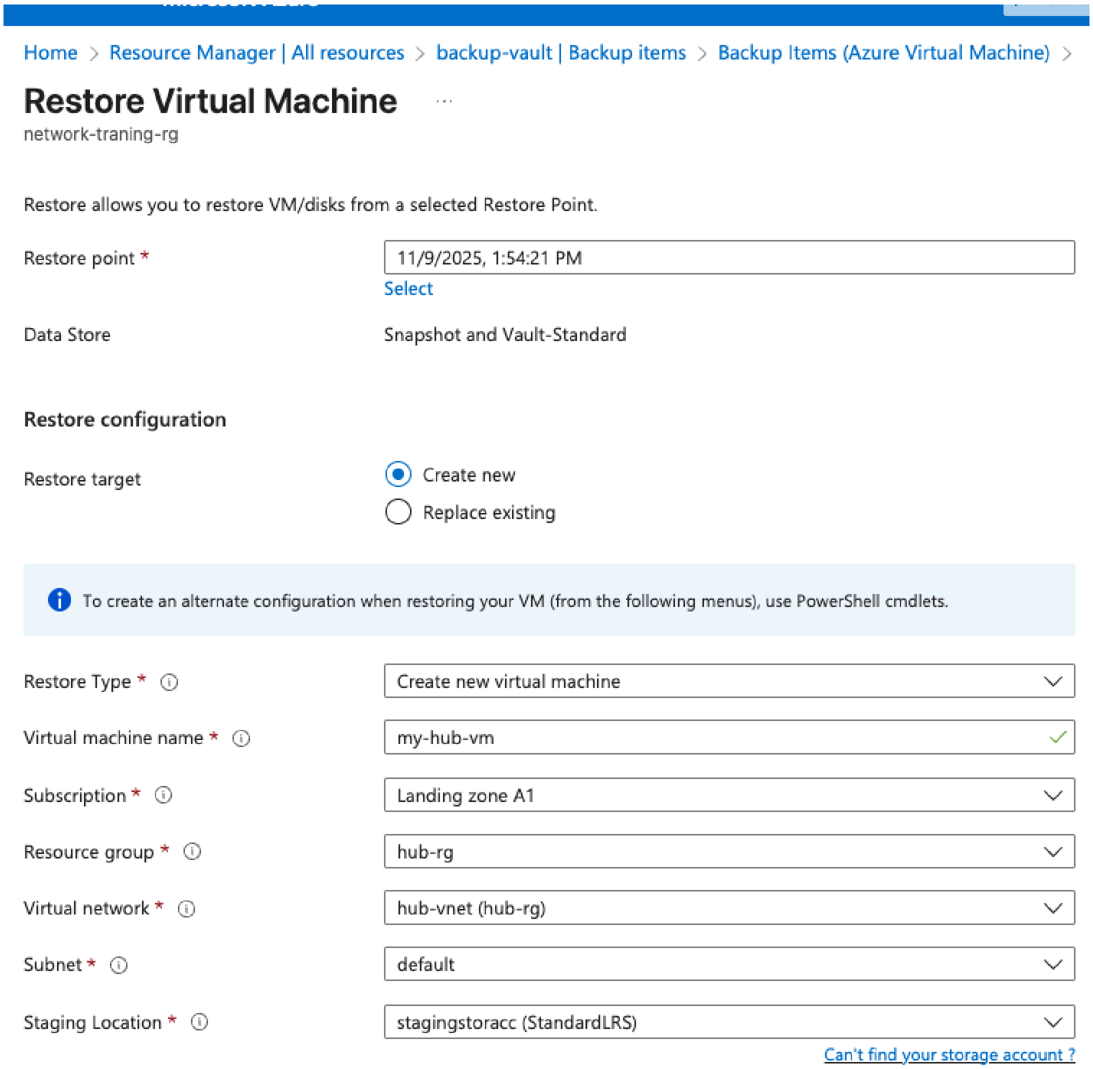


1. **Recovery Services vaults**
    - Go to **Recovery Services vaults** → **Backup items** → **Azure Virtual Machine**.
    - Select the VM you want to restore.
2. **Choose a Restore Point**
    - Click **Select** next to *Restore point*.
    - Pick the date/time you want to restore from.
3. **Choose Restore Target**
    - Select **Create new** (or **Replace existing**, if you want to overwrite the VM).
4. **Configure Restore Settings**
    - **Restore Type:** Choose *Create new virtual machine*.
    - **Virtual machine name:** Enter the new VM name.
    - **Subscription:** Select your subscription.
    - **Resource group:** Choose where to create the VM.
    - **Virtual network:** Pick the VNet for the restored VM.
    - **Subnet:** Select the **web-subnet**.
    - **Staging location:** Choose the storage account for temporary restore data.

5. **Start Restore**
    - Review the settings.
    - Click **Restore**.

      Verify the Restored VM

      After the job completes, go to **Virtual Machines**, find your new VM, and start it.
    - Use RDP to connect:
        i. User: **azureuser**
        ii. Pass: **Baga1BunaBozz**!
        iii. Make sure you have a public IP attached
        iv. Make sure RDP is allowed in the NSG



Home > Resource Manager | All resources > backup-vault | Backup items > Backup Items (Azure Virtual Machine) >

Restore Virtual Machine ...

network-traning-rg

Restore allows you to restore VM/disks from a selected Restore Point.

Restore point *	11/9/2025, 1:54:21 PM Select
Data Store	Snapshot and Vault-Standard

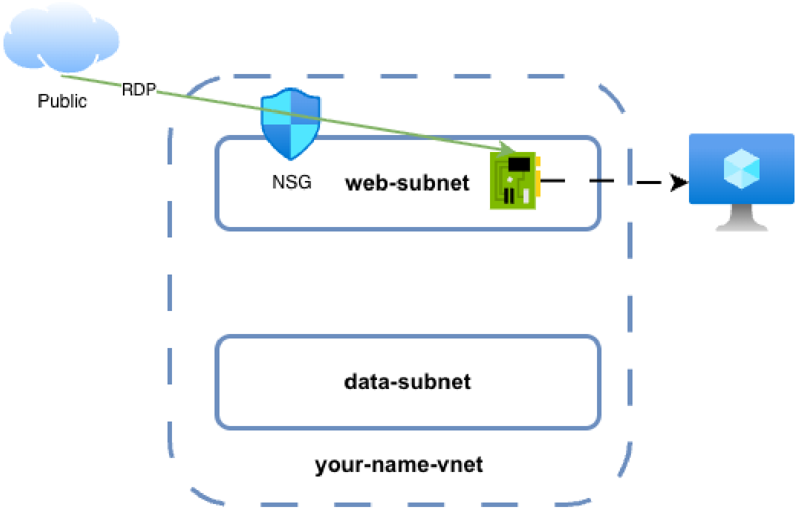
Restore configuration

Restore target: ● Create new ○ Replace existing

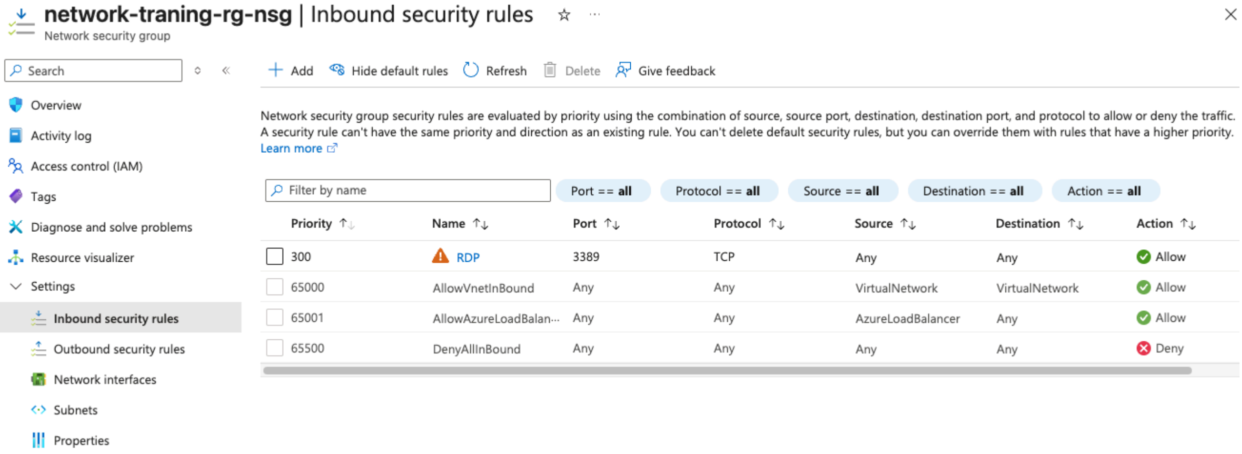
To create an alternate configuration when restoring your VM (from the following menus), use PowerShell cmdlets.

Restore Type *	Create new virtual machine
Virtual machine name *	my-hub-vm ✓
Subscription *	Landing zone A1
Resource group *	hub-rg
Virtual network *	hub-vnet (hub-rg)
Subnet *	default
Staging Location *	stagingstoracc (StandardLRS) Can't find your storage account ?

Create a Network Security Group (NSG)



1. Create a Network Security Group (NSG)
    - Go to **Network security groups**
    - Click **Create**
    - Resource group: **your-name-rg**
    - Name: **your-name-nsg**
    - Region: same as your VNet
    - Click **Review + create** → **Create**
2. Add an inbound rule to allow RDP
    - Open **your-name-nsg**
    - Go to **Inbound security rules**
    - Click **Add**
        - Source: **Any**
        - Source port: *****
        - Destination: **Any**
        - Destination port ranges: **3389**
        - Protocol: **TCP**
        - Action: **Allow**
        - Priority: **1000** (or an available value)
        - Name: **Allow-RDP**
    - Click **Add**

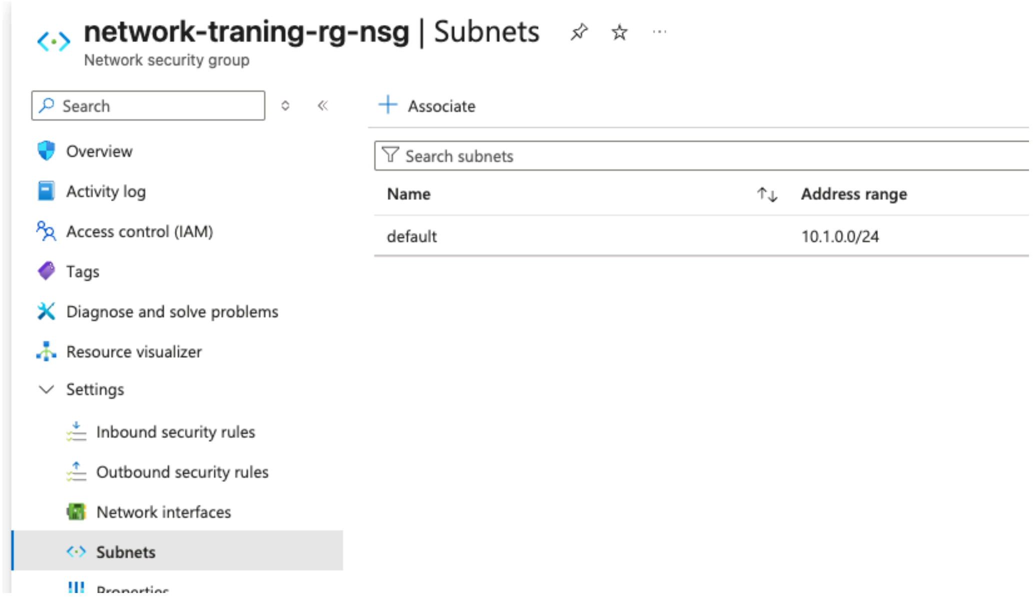


Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority	Name	Port	Protocol	Source	Destination	Action
□ 300	⚠ RDP	3389	TCP	Any	Any	✓ Allow
□ 65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□ 65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	✓ Allow
□ 65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

3. Associate the NSG with the web-subnet
    - Open **your-name-vnet**
    - Go to **Subnets**
    - Select **web-subnet**

    - Under **Network security group**, choose **your-name-nsg**
    - Click **Save**
4. Verify
    - Open the **web-subnet** again
    - Confirm **your-name-nsg** is listed under **Network security group**



network-traning-rg-nsg | Subnets

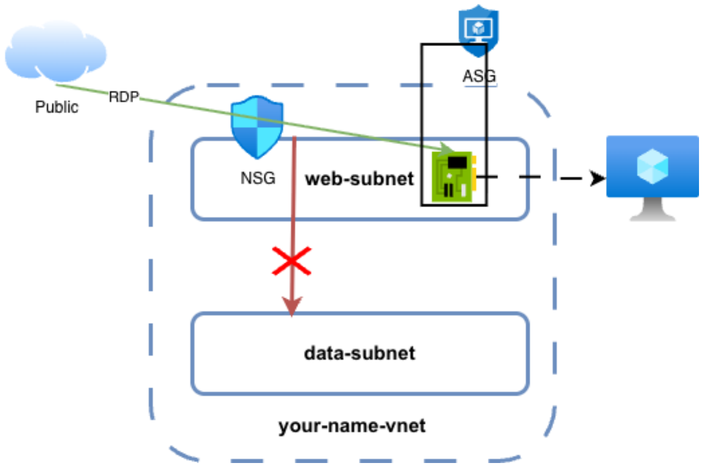
Network security group

Name	Address range
default	10.1.0.0/24

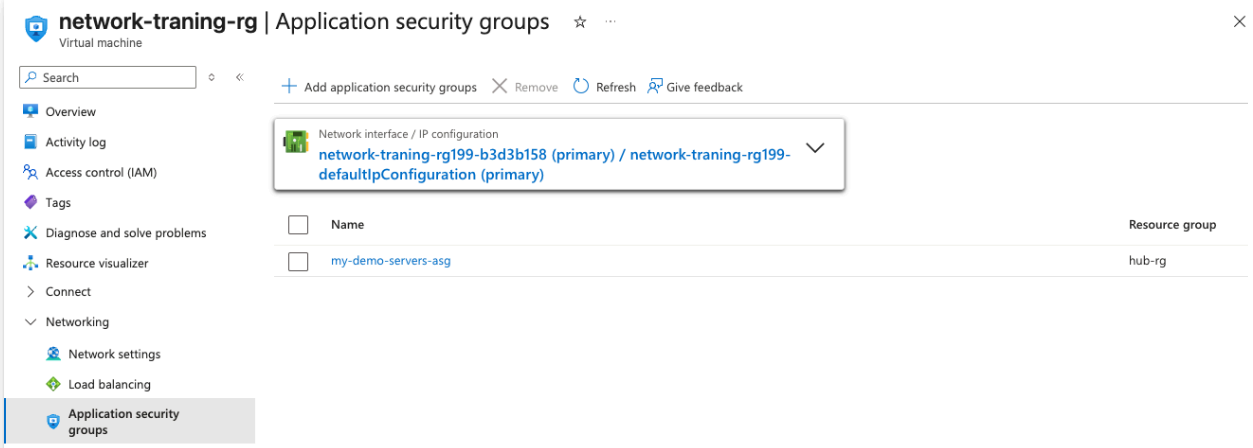
Connect to VM1 using RDP

1. Get the Public IP of VM1:
    - Navigate to the Azure Portal.
    - Click on "Resource groups" and select the resource group where your VMs are.
    - Click on VM1 from the list of resources.
    - Under the "Overview" tab, note down the Public IP address of VM1.
2. Use Remote Desktop Client:
    - On your local machine, search for "Remote Desktop Connection" and open it.
    - In the "Computer" field, enter the Public IP address of VM1 you noted in the previous step.
    - Click “Connect."
    - When prompted, enter the username and password you set up for VM1.
    - Click "Yes" or "Continue" if you receive a certificate warning.
3. Once connected, you'll be inside the VM1 Windows environment.

Create an Application Security Group



1. Create an Application Security Group (ASG)
    - Go to **Application security groups**
    - Click **Create**
    - Resource group: **your-name-rg**
    - Name: **your-name-servers-asg**
    - Region: same as your VM
    - Click **Review + create** → **Create**
2. Add the VM to the ASG
    - Go to **Virtual machines**
    - Open the VM you restored or created earlier
    - Select **Networking**
    - **Application security groups**
    - Click **Add ASG**
    - Select **your-name-servers-asg**
    - Click **Save**



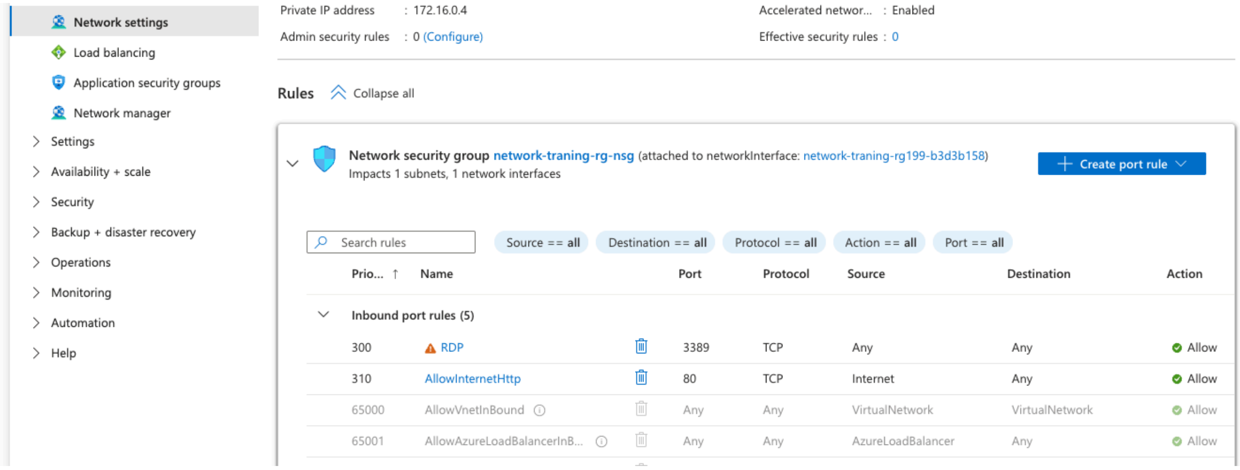
Network interface / IP configuration
network-traning-rg199-b3d3b158 (primary) / network-traning-rg199-defaultIpConfiguration (primary)

Name	Resource group
my-demo-servers-asg	hub-rg

4. Create NSG rules to allow HTTP and HTTPS

- Open **your-name-nsg**
- Go to **Inbound security rules**
- Click **Add**
    - Source: **Service Tag - Internet**
    - Source port ranges: *
    - Destination: **Application security group**
    - Select **your-name-asg**
    - Destination port ranges: **80/443**
    - Protocol: **TCP**

- Action: **Allow**
- Priority: **1001/2**
- Name: **Allow-HTTP/3**
- Click **Add**



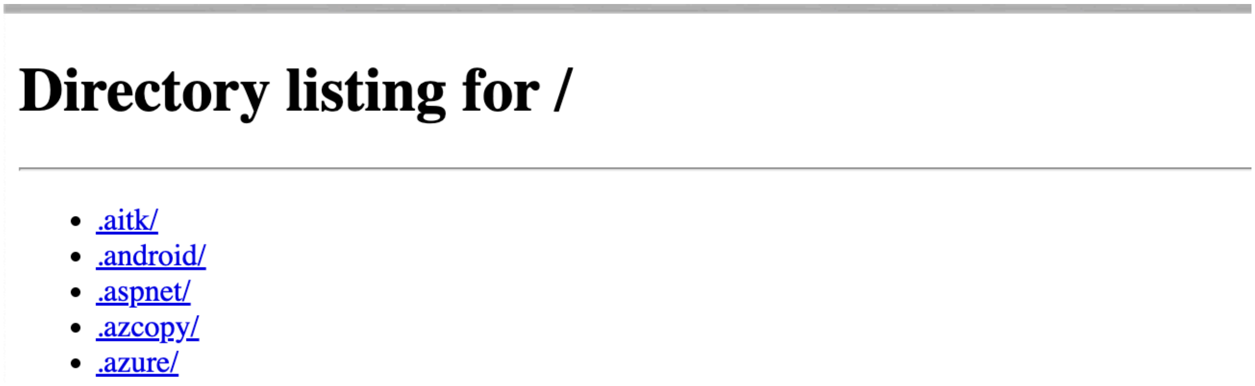
Private IP address : 172.16.0.4
Admin security rules : 0 (Configure)
Accelerated networ... : Enabled
Effective security rules : 0

Network security group network-traning-rg-nsg (attached to networkInterface: network-traning-rg199-b3d3b158)
Impacts 1 subnets, 1 network interfaces

Prio... ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	RDP	3389	TCP	Any	Any	Allow
310	AllowInternetHttp	80	TCP	Internet	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow

5. Verify

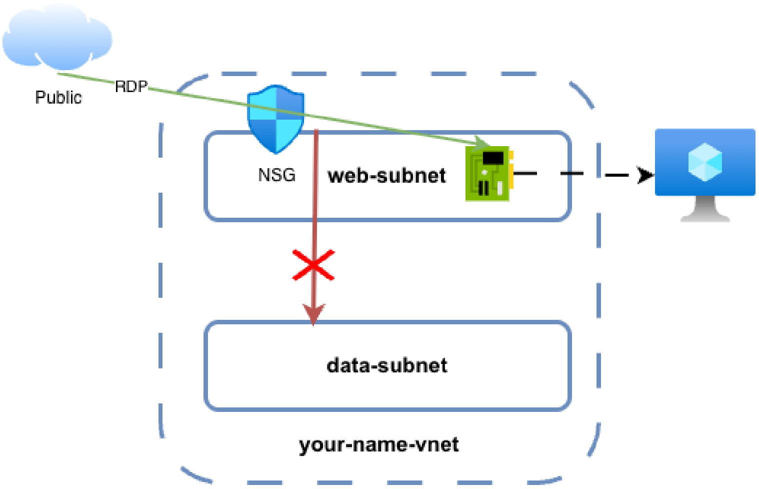
- Open **your-name-nsg**
- Check **Inbound rules** for **Allow-HTTP** and **Allow-HTTPS**
  Open the VM → **Networking** and confirm it is assigned to **your-name-asg**
- On your VM RDP session
  - Open a terminal run:
  - python3 -m http.server 8000 --bind 0.0.0.0
  - Open your VM Public IP in the browser



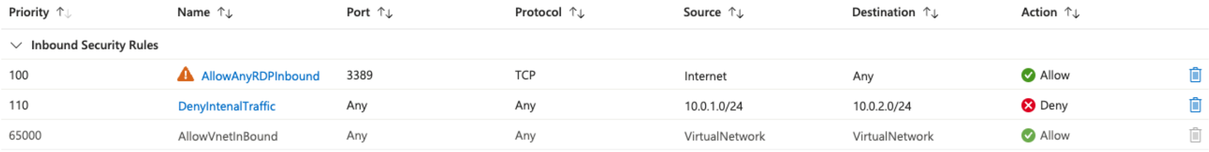
Directory listing for /

- .aitk/
- .android/
- .aspnet/
- .azcopy/
- .azure/

Block traffic between subnets

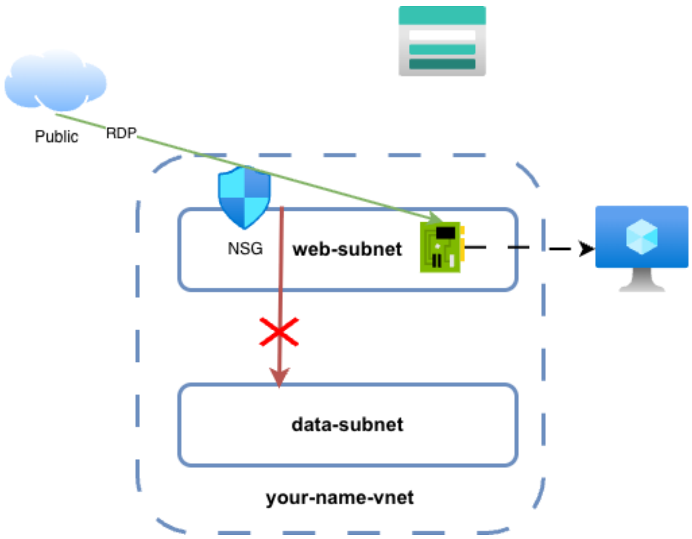


1. Configure the Rule to Block Traffic from Subnet1 to Subnet2:
    a. Source: CIDR block
    b. Source IP addresses/CIDR ranges: 10.0.1.0/24 (address range of Subnet1)
    c. Destination: CIDR block
    d. Destination IP addresses/CIDR ranges: 10.0.2.0/24 (address range of Subnet2)
    e. Protocol: Any
    f. Action: Deny
    g. Priority: Choose a unique priority value (e.g., 100). Ensure it doesn't conflict with other rule priorities and is higher (numerically lower) than any allowed rules you want to override.
    h. Name: Give the rule a descriptive name, e.g., "Block_Subnet1_to_Subnet2".
    i. Click "Add" to save the rule.
2. (Optional) Create a Reverse Rule:
    a. If you want to block traffic from Subnet2 to Subnet1 as well, repeat the steps above, but reverse the source and destination CIDR ranges.



Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
100	⚠ AllowAnyRDPInbound	3389	TCP	Internet	Any	✓ Allow
110	DenyIntenalTraffic	Any	Any	10.0.1.0/24	10.0.2.0/24	✗ Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow

Create a Storage account



1. Sign in to the Azure Portal
    - Open the Azure Portal
    - Sign in with your Azure credentials
2. Start creating a Storage Account
    - Click **Create a resource**
    - Search for **Storage account**
    - Select **Storage account**
    - Click **Create**

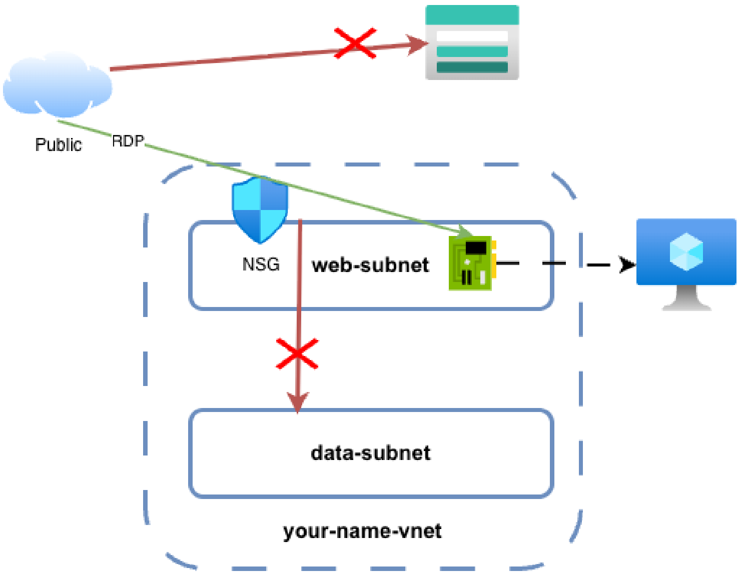
3. Configure the Storage Account
    - **Subscription:** choose your subscription
    - **Resource group:** select **your-name-rg**
    - **Storage account name:** enter **your-name-sa**
    - **Location:** choose the same region as your other resources
    - **Performance:** choose **Standard**
    - **Account kind:** select **General purpose v2**
    - **Replication:** choose **LRS** (Locally Redundant Storage) unless told otherwise
4. Review and create
    - Click **Review + create**
    - Click **Create**

Connect to the Azure Storage Account

1. Connect to the **restored** VM using RDP
    - Open **Remote Desktop Connection**
    - Enter the public IP of your restored VM
    - Sign in with the VM username and password
2. Open Azure Storage Explorer on VM
    - In the Start menu, search for **Azure Storage Explorer**
    - Open the application
3. Start the connection wizard
    - Click the **plug icon (🔌)** in the left pane
    - Select **Storage account or service**
    - Click **Next**
4. Choose the authentication method
    - You may use **any of the following**:
        - **Storage account name and key**
        - **SAS (Shared Access Signature)**
        - **Azure AD / RBAC**
    - Click **Next**
5. Perform an nslookup on the storage account
    - Open **Command Prompt** on VM1
    - Run:

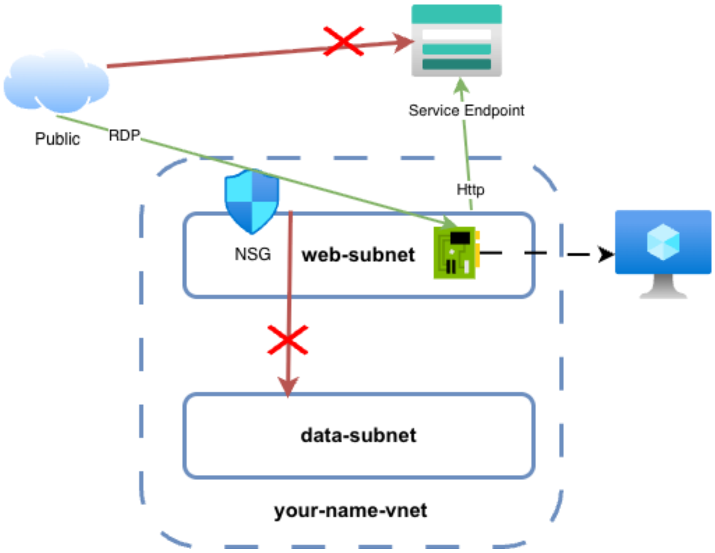
      ```
      nslookup yournamesa.blob.core.windows.net
      ```
    - Observe the **IP address** returned

Restrict public access to the storage account



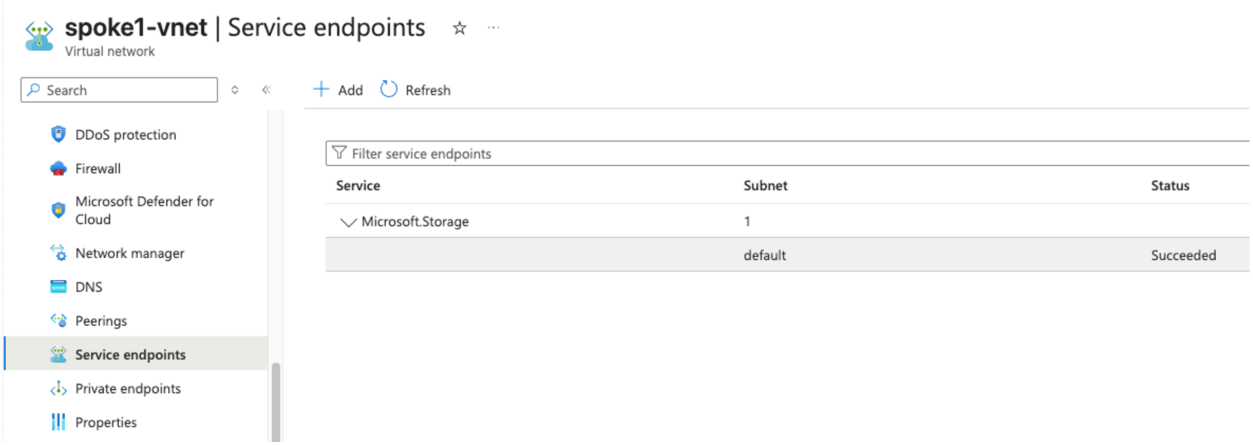
1. Open your storage account (your-name-sa)
    a. Go to Storage accounts
    b. Select your-name-sa
2. Configure Network Access
    a. In the Storage Account's settings pane, under the "Security + networking" section, click on "Networking."
    b. Click on “Manage” Public network access
3. In the "Networking" tab:
    a. Allow access from: Choose "Selected networks." This will deny public access.
    b. Don’t add any networks
4. Try to connect to the storage account from VM
5. Perform an nslookup on the URL
    a. `nslookup yournamesa.blob.core.windows.net`
    b. Observe the IP address

Create a service endpoint for your storage account



1. Open your virtual network (**your-name-vnet**)
    - Go to **Virtual networks**
    - Select **your-name-vnet**
2. Open the **web-subnet** (or the subnet you want to secure)
    - Go to **Subnets**
    - Click **web-subnet**
3. Enable the Service Endpoint
    - Scroll to **Service endpoints**
    - Click **+ Add service endpoint** (or **Add** depending on UI)
    - In the service list, select **Microsoft.Storage**
    - Ensure the **subscription** and **region** match your storage account
    - Click **Add**
4. Save the configuration

    - Click **Save** on the subnet
5. Verify
    - Reopen **web-subnet**
    - Confirm Microsoft.Storage appears under Service endpoints
    - Try to connect to the Storage account
    - Discuss the results


spoke1-vnet | Service endpoints

Virtual network

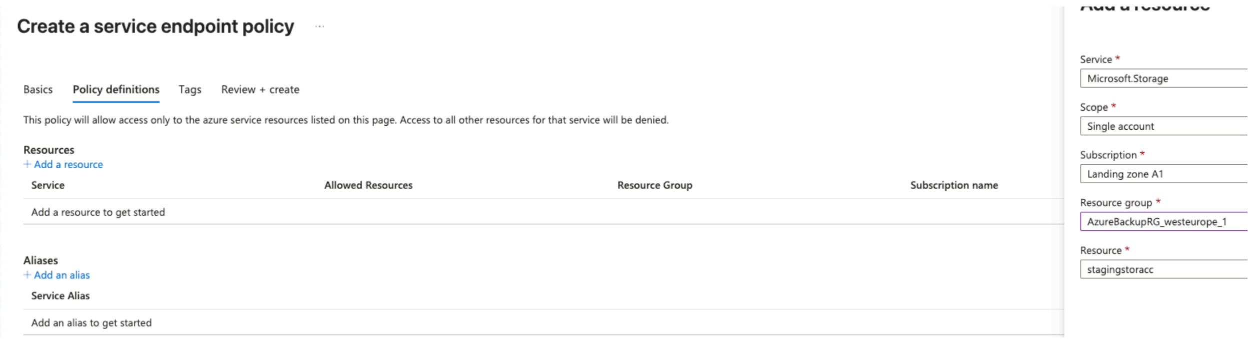
Service	Subnet	Status
Microsoft.Storage	1	
	default	Succeeded

Allow Vnet to the storage account

1. Open your storage account (your-name-sa)
    - Go to Storage accounts
    - Select your-name-sa
2. Go to networking settings
    - In the left menu, click Networking
    - Under Firewall and virtual networks, choose Selected networks
3. Add the VNet
    - Scroll to Virtual networks
    - Click + Add existing virtual network
    - Select your VNet: your-name-vnet
    - Select the subnet where you enabled the service endpoint (for example web-subnet)
    - Click Add
4. Save the configuration
    - Click Save at the top
5. Verify
    - Under Virtual networks, confirm that your-name-vnet and the selected subnet appear in the allowed list
    - Connect from your Vnet to your Storage account
    - Discuss the results

Create a Service Endpoint Policy for a Storage Account

1. Open Service Endpoint Policies
    - Go to the **Azure Portal**.
    - Search for **Service endpoint policies**.
    - Click **Create**.
2. **Fill in Basic Details**
    - **Subscription:** Select your subscription.
    - **Resource Group:** Choose the one used by your VNet or create a new one.
    - **Name:** Enter a policy name (e.g., *sep-storage-allow*).
    - **Region:** Select the same region as your **VNet**.
3. **Add Policy Definition**
    - Click **Add a policy definition**.
    - **Service:** Choose **Microsoft.Storage**.
    - Select your storage account from your resource grup
    - Add.
4. **Create the Policy**
    - Review your settings.
    - Click **Create**.



Create a service endpoint policy ···

Basics | Policy definitions | Tags | Review + create

This policy will allow access only to the azure service resources listed on this page. Access to all other resources for that service will be denied.

Resources

+ Add a resource

Service	Allowed Resources	Resource Group	Subscription name
Add a resource to get started			

Aliases

+ Add an alias

Service Alias
Add an alias to get started

Add a resource

Service *: Microsoft.Storage

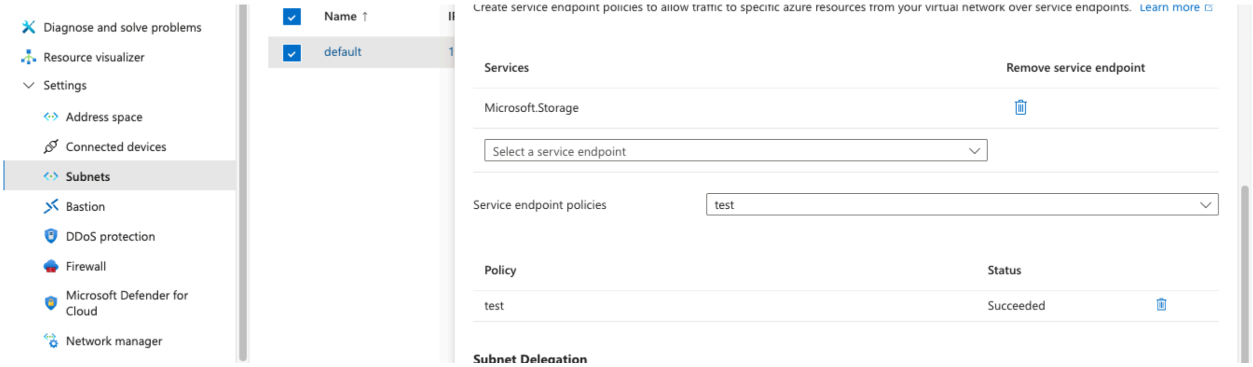
Scope *: Single account

Subscription *: Landing zone A1

Resource group *: AzureBackupRG_westeurope_1

Resource *: stagingstoracc

5. **Assign Policy to Your VNet Subnet**
    - Go to your **Virtual Network**.
    - Open **Subnets**.
    - Select the subnet that needs access.
    - Under **Service endpoints**, enable **Microsoft.Storage**.
    - Under **Service endpoint policies**, select the policy you just created.
    - Click **Save**.



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	🗑

Select a service endpoint

Service endpoint policies: test

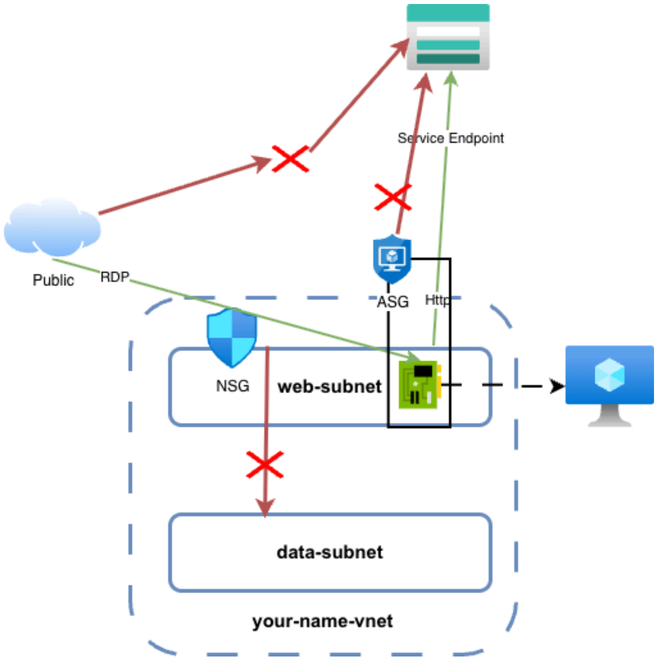
Policy	Status	
test	Succeeded	🗑

Subnet Delegation

6. Verify the Configuration

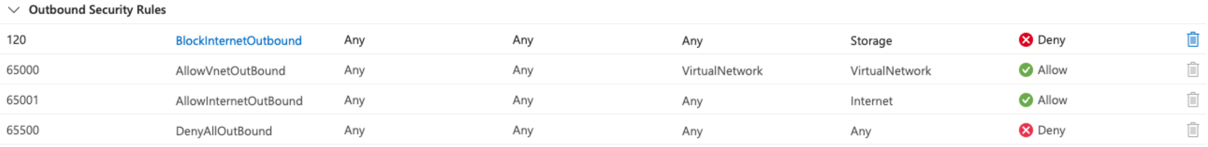
- Return to the subnet view.
- Confirm that:
  - **Microsoft.Storage** service endpoint is enabled.
  - Your **Service Endpoint Policy** is attached.

Create NSG rule for subnet1 to block outbound traffic to storage accounts using the Service Tag



1. Navigate to the NSG Associated with subnet1
   - Go to the Azure Portal.
   - In the left-hand sidebar, click on "Resource groups" and then select the appropriate resource group where your NSG resides. (If you don't already have an NSG associated with subnet1, you'll need to create one first.)
   - From the list of resources, click on the NSG associated with subnet1 to open its settings.
2. Add an Outbound Security Rule
   - In the NSG's settings pane, under the "Settings" section, click on "Outbound security rules."
   - Click on the "+ Add" button to start the process of adding a new rule.
3. Configure the Rule to Block Outbound Traffic to Azure Storage Accounts
   - Source: Choose "Application Security Group"
   - Source port ranges: Leave it as "*".
   - Destination: Choose "**Service Tag**".

    - Destination service tag: Choose "Storage" (This service tag represents Azure Storage service in the same region as the NSG).
    - Destination port ranges: Leave it as "*".
    - Protocol: Choose "Any".
    - Action: Choose "Deny".
    - Priority: Set a value (e.g., 110). Ensure this value is lower (numerically) than any allow rules you might have for outbound traffic to ensure this block rule takes precedence.
    - Name: Provide a descriptive name for the rule, such as "BlockOutboundToStorageServiceTag".
    - Description: (Optional) Add a short description for clarity.
4. Save the Rule
    - Click the "Add" button at the bottom of the pane to add the rule.

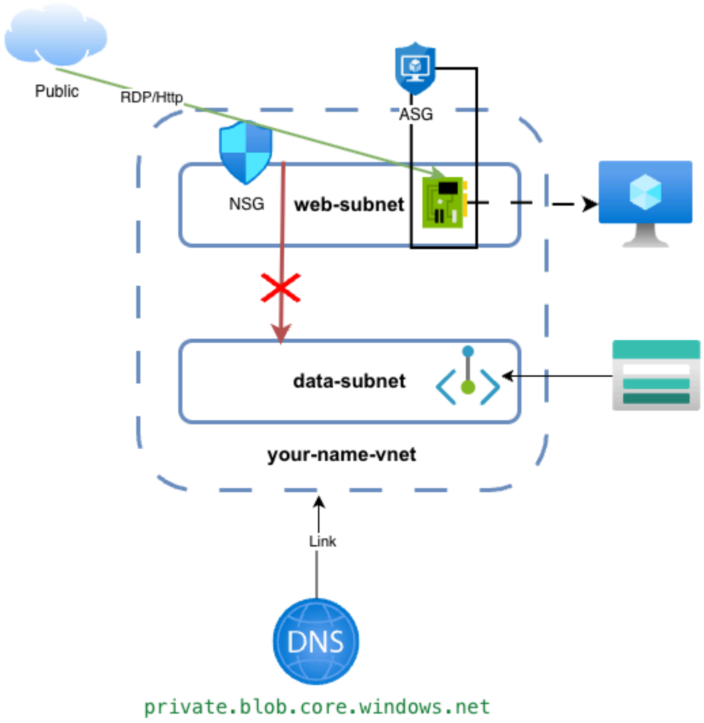


Outbound Security Rules

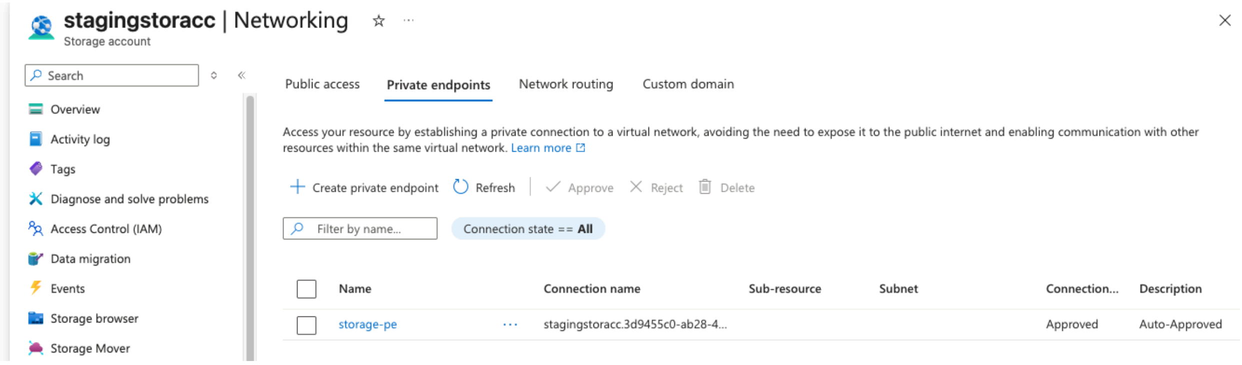
120	BlockInternetOutbound	Any	Any	Any	Storage	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

5. Try to connect to the storage account
6. Discuss Results

Create a Private Endpoint



1. **Open the Storage Account**
    a. Go to the **Azure Portal**.
    b. Search for your **Storage Account**.
    c. Open it.
2. **Go to Private Endpoint Connections**
    a. In the left menu, select **Networking**.
    b. Click the **Private endpoint connections** tab.
    c. Select **+ Private endpoint**.
3. **Fill in Basic Details**
    a. **Subscription:** Select your subscription.
    b. **Resource group:** Choose the same RG as your VNet (recommended).
    c. **Name:** Enter a name for the private endpoint (e.g., *pe-storage*).
    d. **Region:** Must match the region of the **VNet**, NOT required to match storage account.
4. **Choose the Resource to Connect**
    a. **Resource type:** Select **Microsoft.Storage/storageAccounts**.
    b. **Resource:** Choose your storage account.
    c. **Target sub-resource:** Select what you want (typically **blob**, or **file**, or multiple endpoints created separately).
5. **Select the VNet and Subnet**
    a. Choose the **Virtual Network** you created.
    b. Select the **subnet** for the private endpoint.
        i. data-subnet
6. **Integrate with Private DNS (recommended)**
    a. On the **DNS Integration** step, choose:
        i. **Yes** → integrate with **Private DNS Zone**.
        ii. Pick the recommended zone (e.g., `privatelink.blob.core.windows.net`).
    b. If your zone doesn't exist, Azure will create it automatically.



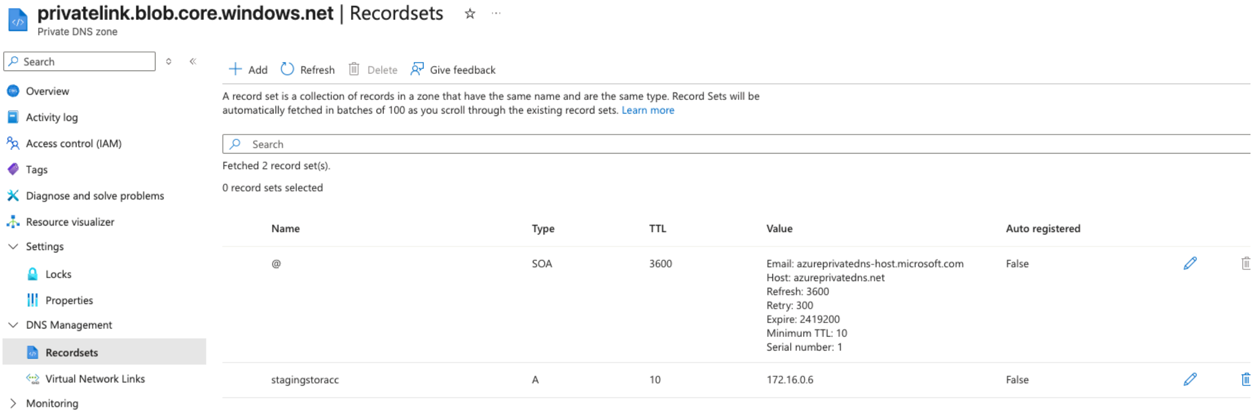
stagingstoracc | Networking

Storage account

Access your resource by establishing a private connection to a virtual network, avoiding the need to expose it to the public internet and enabling communication with other resources within the same virtual network. Learn more

□	Name		Connection name	Sub-resource	Subnet	Connection...	Description
□	storage-pe	···	stagingstoracc.3d9455c0-ab28-4...			Approved	Auto-Approved

7. **Review and Create**
    a. Review the configuration summary.
    b. Click **Create**.
    c. Wait for deployment to complete.
8. **Verify the Private Endpoint**
    a. Return to the **Storage Account** → **Networking** → **Private endpoint connections**.
    b. Confirm the status shows **Approved**.
    c. From a VM inside the VNet:
        i. Access the storage account using its **private** endpoint FQDN.
        ii. Confirm traffic does not use the public endpoint.
        iii. `nslookup yournamesa.blob.core.windows.net`



privatelink.blob.core.windows.net | Recordsets

Private DNS zone

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

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
stagingstoracc	A	10	172.16.0.6	False