

# Create Azure Virtual Network (VNet)

1. Login to the Azure Portal:
  - a. Open your web browser and navigate to the Azure Portal.
  - b. Sign in with your Azure account credentials.
2. Navigate to Virtual Networks:
  - a. In the left-hand side menu, click on "Create a resource."
  - b. In the "Search the Marketplace" box, type "Virtual Network" and select it from the dropdown.
3. Initiate VNet Creation:
  - a. Click on the "Create" button.
4. Fill in the Basic Details:
  - a. Subscription: Choose the appropriate Azure subscription.
  - b. Resource Group: Either select an existing resource group or create a new one.
  - c. Name: Provide a name for the Virtual Network. E.g., "MyVNet"
  - d. Region: Choose a region where you want the VNet to reside.
5. IP Addresses Configuration:
  - a. IPv4 Address space: Define an address range for the VNet. For this example, let's use 10.2.0.0/16.
6. Security Options:
  - a. You can leave the default options or configure DDoS protection and firewall as per your requirements.
  - b. Click on the "Review + create" button, then on the next screen, click "Create."

## Create Two Subnets within the VNet

1. Navigate to the Created VNet:
  - a. Once the VNet creation process completes, go to "Resource groups" from the left-hand side menu.
  - b. Click on the resource group where you created the VNet.
  - c. Click on the VNet (e.g., "MyVNet").
2. Open Subnets Setting:
  - a. In the VNet's overview page, under the "Settings" section, click on "Subnets."
3. Add First Subnet:
  - a. Click on the "+ Subnet" button.
  - b. Name: Provide a name for the first subnet, e.g., "Subnet1".
  - c. Address range: Define an address range for this subnet. For this example, use 10.2.1.0/24.
  - d. Configure any other settings as necessary (like service endpoints).

- e. Click "OK."
4. Add Second Subnet:
  - a. Click on the "+ Subnet" button again.
  - b. Name: Provide a name for the second subnet, e.g., "Subnet2".
  - c. Address range: Define an address range for this subnet. For this example, use 10.2.2.0/24.
  - d. Configure any other settings as necessary.
5. Click "OK."

## Create a Network Security Group (NSG)

1. In the Azure Portal, go to the left-hand side menu and click on "Create a resource."
2. In the "Search the Marketplace" box, type "Network Security Group" and select it from the dropdown.
3. Click the "Create" button.
4. Fill in the required details:
  - a. Subscription: Choose your subscription.
  - b. Resource Group: Select the resource group where your VNet and subnets reside.
  - c. Name: Provide a name for the NSG, e.g., "MyNSG".
  - d. Region: Choose the same region where your VNet is.
5. Click on "Review + create" then on the next screen, click "Create."

## Add an RDP Rule to the NSG

1. Once the NSG is created, click on "Resource groups" from the left-hand side menu.
2. Select the resource group where you created the NSG.
3. Click on the NSG you just created (e.g., "MyNSG").
4. In the settings pane on the left, click on "Inbound security rules."
5. Click the "+ Add" button to add a new rule.
6. Fill in the required details for the RDP rule:
  - a. Source: Any
  - b. Source port ranges: \*
  - c. Destination: Any
  - d. Destination port ranges: 3389
  - e. Protocol: TCP
  - f. Action: Allow
  - g. Priority: Choose a number, e.g., 100 (ensure it doesn't conflict with existing rule priorities).
  - h. Name: Give the rule a name, e.g., "Allow\_RDP".

7. Click "Add" to save the rule.

## Attach the NSG to the First and Second Subnet

1. While still in the NSG's settings, click on "Subnets" in the settings pane.
2. Click the "+ Associate" button.
3. For the "Virtual network," choose your VNet (e.g., "MyVNet").
4. For "Subnet," select the second subnet (e.g., "Subnet1").
5. Click "OK."
6. Repeat the steps for Subnet2

## Create some VMs

1. Go to Azure Portal:
  - a. Navigate to Azure Portal.
  - b. Sign in with your credentials.
2. Create a Virtual Machine:
  - a. In the left-hand side menu, click on "Create a resource."
  - b. Select "Compute," then choose "Virtual Machine."
  - c. Click "Create."
3. Fill in the Basics:
  - a. Subscription: Choose your Azure subscription.
  - b. Resource Group: Select the resource group where your VNet and subnets are.
  - c. Virtual Machine Name: Provide a name for your VM, e.g., "VM1."
  - d. Region: Ensure it's the same region as your VNet.
  - e. Availability options: Choose based on your requirements (e.g., No infrastructure redundancy required).
  - f. Image: Select an OS image (e.g. Windows 11).
  - g. Size: Pick a size that fits your needs.
  - h. Continue with the default options or adjust as necessary for the remaining fields.
4. Networking Configuration:
  - a. Virtual network: Choose your VNet, e.g., "MyVNet."
  - b. Subnet: Choose "Subnet1."
  - c. Public IP: Choose to create a new one or use an existing one based on your requirements.
  - d. Adjust other options as necessary.
5. Continue Setting up the VM:
  - a. Disks: Choose the type of OS disk (e.g., Premium SSD).

- b. Management, Advanced, Tags: Adjust these settings as necessary for your use case.
6. Review & Create:
  - a. Review your configurations.
  - b. Click "Review + create," then on the next screen, click "Create."
7. Perform same steps for the second VM but this one add it to subnet2

## Connect to VM1 using RDP

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




## Ping RDP to the second VM

1. Get the Public IP of VM2:
  - a. Navigate to the Azure Portal.
  - b. Click on "Resource groups" and select the resource group where your VMs are.
  - c. Click on VM2 from the list of resources.
  - d. Under the "Overview" tab, note down the Public IP address of VM2.
2. Use Remote Desktop Client:
  - a. On your remote machine, search for "Remote Desktop Connection" and open it.
  - b. In the "Computer" field, enter the Public IP address of VM2 you noted in the previous step.
3. Click "Connect."
  - a. When prompted, enter the username and password you set up for VM2.
  - b. Click "Yes" or "Continue" if you receive a certificate warning.

- c. Once connected, you'll be inside the VM2 Windows environment.

## 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 Storage account

1. Sign in to the Azure Portal
  - a. Go to the Azure Portal.
  - b. Sign in with your Azure account credentials.
2. Create a Storage Account
  - a. In the Azure portal's left sidebar, click on "Create a resource."
  - b. In the "Search the Marketplace" box, type "Storage Account" and select "Storage account" from the dropdown list.
  - c. In the resulting page, click the "Create" button to start the process.
3. Configure the Storage Account
  - a. Basics tab:
  - b. Subscription: Select your Azure subscription.
  - c. Resource Group: Create a new one or select an existing one.

- d. Storage account name: Enter a unique name. This name must be globally unique and can contain 3-24 lowercase letters and numbers only.
  - e. Location: Select a region where you want the storage account to reside.
  - f. Performance: Choose between Standard (HDD) or Premium (SSD). Standard is often sufficient for general-purpose use.
  - g. Account kind: Select the kind of storage account you need (e.g., General purpose v2 is commonly used as it supports blobs, files, queues, and tables).
  - h. Replication: Choose the type of replication you want, such as "Locally redundant storage (LRS)" or "Geo-redundant storage (GRS)" based on your data durability needs.
4. Step 4: Review and Create

## Install Azure Storage Explorer on VM1

1. RDP into VM1: Connect to VM1 using Remote Desktop Protocol (RDP).
2. Download Azure Storage Explorer:
  - a. Open a web browser on VM1.
  - b. Navigate to the official Azure Storage Explorer page.
  - c. Download the Azure Storage Explorer setup for Windows.
3. Install Azure Storage Explorer:
  - a. Once the setup is downloaded, run the installer and follow the installation steps.

## Connect to the Azure Storage Account

1. Open Azure Storage Explorer: Once installed, open Azure Storage Explorer on VM1.
2. Connect to your Azure Storage Account:
  - a. In the left pane, click on the plug icon (🔌) to open the Connect dialog.
  - b. Choose "Storage account or service" and click "Next."
  - c. Choose "Use a storage account name and key" or another method based on your preference.
3. If using the storage account name and key:
  - a. Obtain your storage account name and one of your access keys from the Azure portal.
  - b. Paste the storage account name and key into the respective fields in Storage Explorer.
4. Click "Next" and then "Connect."
5. Perform nslookup on the dns name of the storage account
  - a. Observe the Ip address

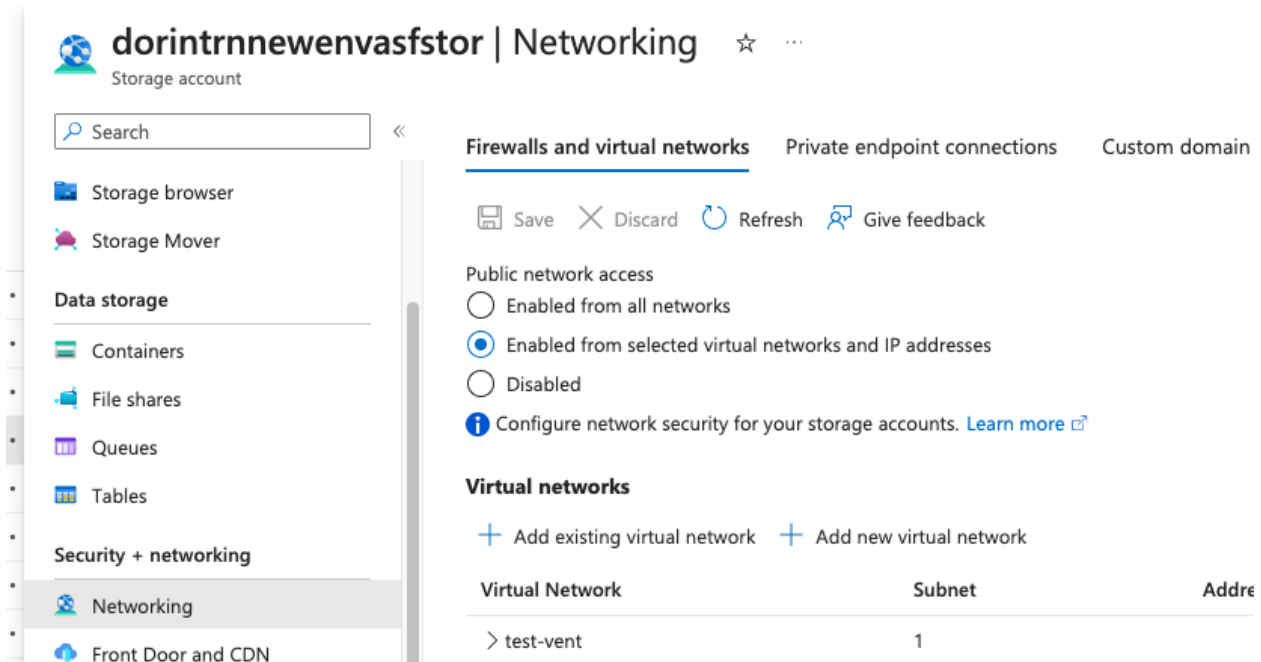
## Restrict public access to the storage account

1. Navigate to the Storage Account
  - a. Go to the Azure Portal.
  - b. In the left-hand sidebar, click on "Resource groups" and then select the appropriate resource group where your Storage Account resides.
  - c. From the list of resources, click on your Storage Account to open its settings.
2. Configure Network Access
  - a. In the Storage Account's settings pane, under the "Security + networking" section, click on "Networking."
3. In the "Networking" tab:
  - a. Allow access from: Choose "Selected networks." This will deny public access and only allow access from the networks you specify.
4. Try to connect to the storage account from VM1
5. Perform an nslookup on the url
  - a. Observe the IP address

## Create a service endpoint for your storage account

1. Navigate to Your Storage Account
  - a. Go to the Azure Portal.
  - b. From the left-hand sidebar, click on "Resource groups," then select the appropriate resource group where your Storage Account resides.
  - c. Click on your Storage Account from the list of resources to open its overview pane.
  - d. Step 2: Configure the Firewall and Virtual Networks
  - e. In the Storage Account's settings pane, under the "Security + networking" section, click on "Firewalls and virtual networks."
2. Under the "Virtual networks" section:
  - a. Choose "Selected networks" under the "Allow access from" option to ensure only your selected networks can access the storage account.
  - b. Click on the "+ Add existing virtual network" link.
3. Add the Service Endpoint
  - a. In the "Add existing virtual network" pane:
    - i. Virtual network: Select the virtual network that subnet1 is a part of.
    - ii. Subnet: After selecting the virtual network, a dropdown will appear for the subnet. Select subnet1 from the dropdown list.

- b. Under the "Service Endpoints" section of the same pane, you'll see the available service endpoints for your selected subnet. Choose "Microsoft.Storage" to enable the storage service endpoint.
  - c. Click the "Add" button to confirm and add the service endpoint to subnet1.
4. Save Changes
  - a. After adding the service endpoint, return to the "Firewalls and virtual networks" pane and click the "Save" button at the top to apply your changes.



5. Try to connect now from the VM1
6. Perform an nslookup on the url
  - a. Observe the IP address

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

1. Navigate to the NSG Associated with subnet1
  - a. Go to the Azure Portal.
  - b. 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.)
  - c. From the list of resources, click on the NSG associated with subnet1 to open its settings.
2. Add an Outbound Security Rule



- a. In the NSG's settings pane, under the "Settings" section, click on "Outbound security rules."
  - b. 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
  - a. Source: Choose "Any" (to apply to all resources in subnet1).
  - b. Source port ranges: Leave it as "\*\*".
  - c. Destination: Choose "Service Tag".
  - d. Destination service tag: Choose "Storage" (This service tag represents Azure Storage service in the same region as the NSG).
  - e. Destination port ranges: Leave it as "\*\*".
  - f. Protocol: Choose "Any".
  - g. Action: Choose "Deny".
  - h. 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.
  - i. Name: Provide a descriptive name for the rule, such as "BlockOutboundToStorageServiceTag".
  - j. Description: (Optional) Add a short description for clarity.
4. Save the Rule
  - a. 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

## Create a private endpoint for a storage account

1. Create a new storage account
2. Navigate to Your Storage Account
3. Start the Creation of the Private Endpoint
  - a. In the Storage Account's settings pane, under the "Security + networking" section, click on "Private endpoint connections."
  - b. Click on the "+ Private endpoint" button to start the creation process.
4. Set Up the Basics
  - a. Subscription: Ensure the correct subscription is selected.
  - b. Resource Group: You can choose to create a new resource group or use an existing one.
  - c. Name: Provide a name for the private endpoint.
  - d. Region: Select the region where you want the private endpoint to be located. Typically, it would be in the same region as the storage account and the VNet.

## 5. Set Up the Resource

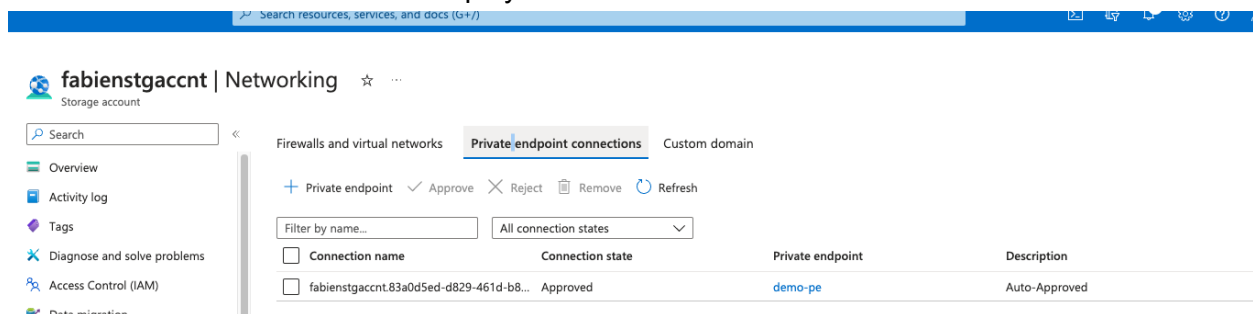
- Connection Method: Choose "Connect to an Azure resource in my directory."
- Subscription: Ensure the correct subscription is selected.
- Resource type: Choose "Microsoft.Storage/storageAccounts."
- Resource: Select your desired storage account.
- Target sub-resource: Choose "table" for Table Storage.

## 6. Configure the Private Endpoint

- Virtual Network: Choose the virtual network where you want the private endpoint to reside.
- Subnet: Choose the subnet within the virtual network where the private endpoint will be placed. Select the one where VM1 is placed.
- Private DNS integration: It's typically recommended to enable this option. When you enable Private DNS Integration, Azure will automatically create/update a private DNS zone for the storage account, making it easier to resolve the storage account's private IP.

## 7. Review and Create

- After you've filled in all the necessary details, click the "Review + create" button at the bottom of the page.
- Azure will validate your configurations. Once validation passes, click the "Create" button to start the deployment.



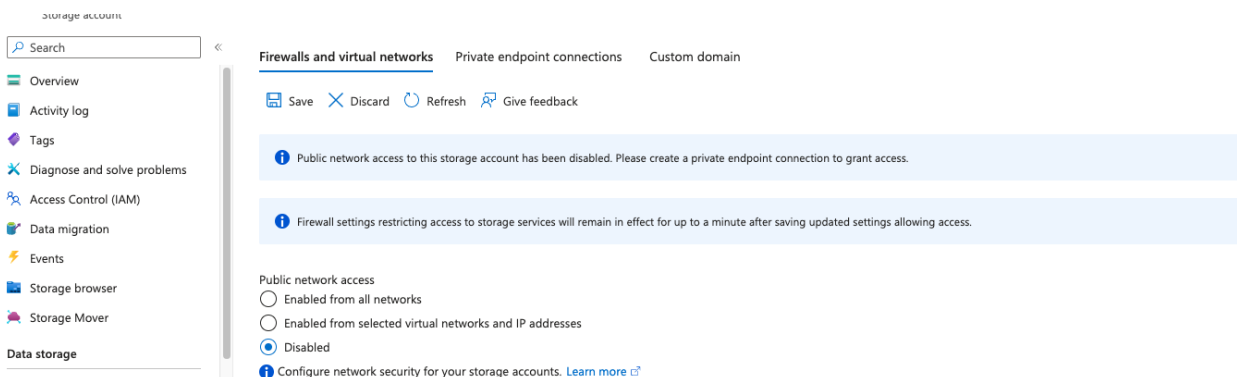
## 8. Connect to the storage account from VM1.

## 9. Perform an nslookup on the url

- Observe the IP address

## 10. Close the public access for the storage account.

## 11. Connect to the storage account from VM1.



## Create an Application Security Group

1. Go to the Azure Portal.
2. In the left-hand sidebar, click on "+ Create a resource."
3. In the search box, type "Application Security Group" and select it from the results.
4. Click on the "Create" button to start the creation process.
5. Fill in the required details:
  - a. Subscription: Choose the appropriate subscription.
  - b. Resource group: Select an existing resource group or create a new one.
  - c. Name: Give a descriptive name for the ASG.
  - d. Region: Select the region where your VM2 resides.
6. Click on the "Review + create" button.
7. After validation, click on the "Create" button.

## Add VM2 to the Application Security Group

1. Click on Virtual machines option.
2. Select the provided virtual machine.
3. Click on Networking.
4. Choose the Application security groups.
5. From the dropdown that appears, select the security group that we created. Then select Save.
6. Create NSG rule to allow RDP to the VM2 Application Security Group