Deploying Azure Infrastructure:
A Step-by-Step Guide

- Create a resource group
- Create a virtual network with 2 subnets
- Deploy a virtual machine and attach a disk
- Configure a network interface and assign private and public IPs
- Attach the NIC to the VM
- Set up a Network Security Group (NSG) with rules to allow web traffic and RDP
- Configure Virtual Network Peering

Deploying Azure Infrastructure: A Step-by-Step Guide

In this guide, you will learn how to:

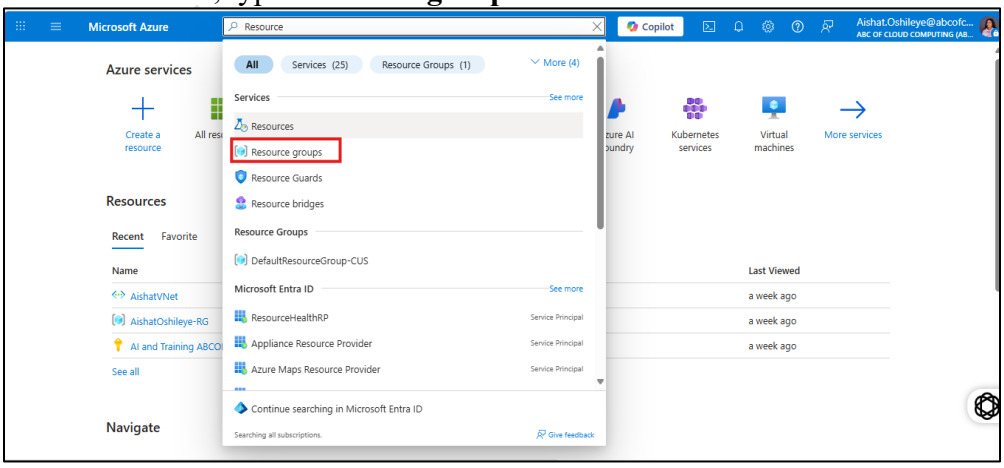
- Create a resource group
- Create a virtual network with 2 subnets
- Deploy a virtual machine and attach a disk
- Configure a network interface and assign private and public IPs
- Attach the NIC to the VM
- Set up a Network Security Group (NSG) with rules to allow web traffic and RDP
- Configure Virtual Network Peering

Prerequisites

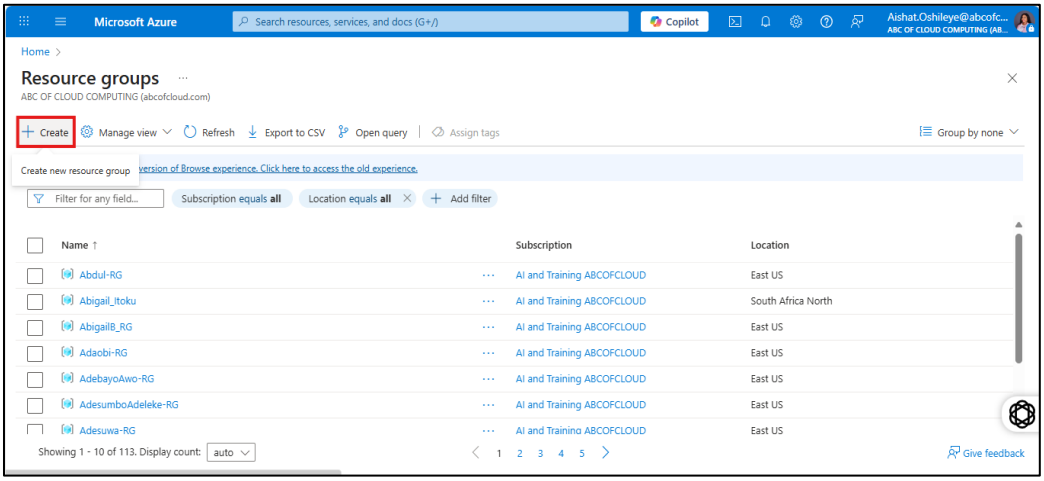
- An active Azure subscription
- Access to Azure Portal

Task 1: Create a Resource Group

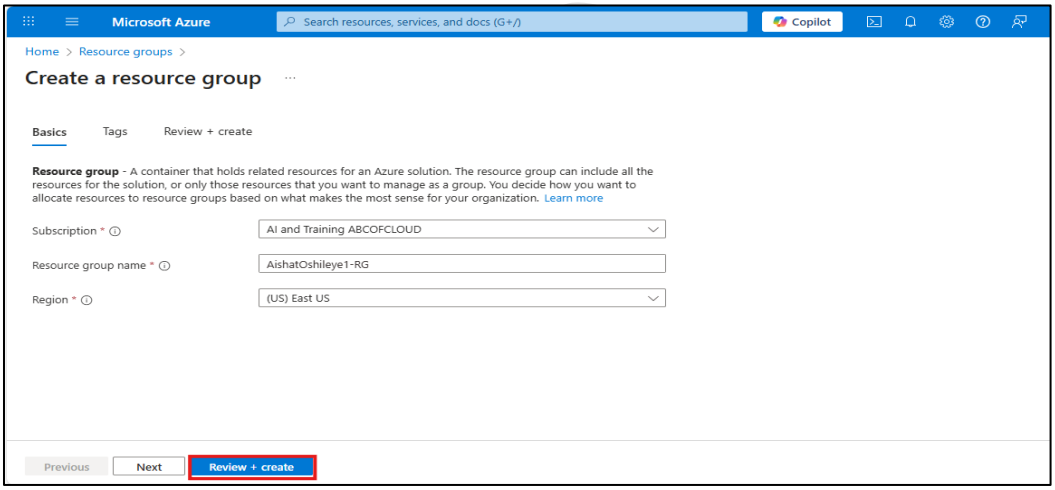
1. Log in to the Azure Portal.
2. In the search bar, type **Resource groups** and select it.

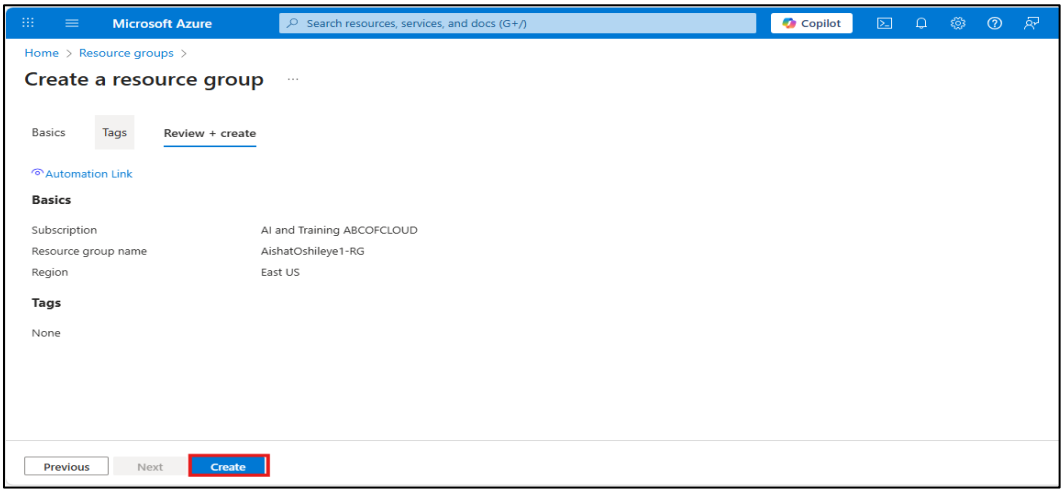


3. Click on + **Create**.



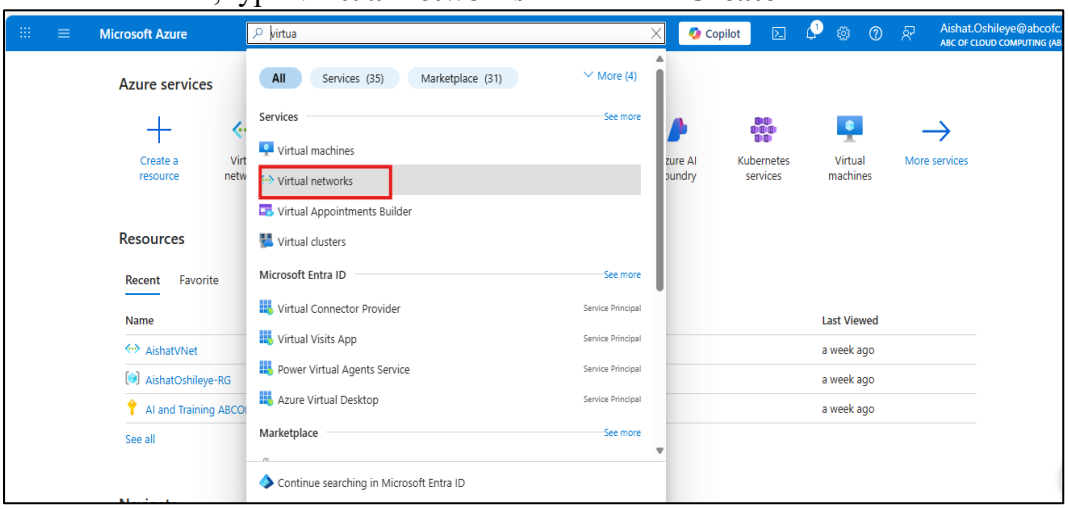
4. Choose your **Subscription**.
5. Enter a **Resource Group Name** (e.g., `MyResourceGroup`).
6. Select a **Region** (e.g., `West Europe`).
7. Click **Review + Create → Create**.

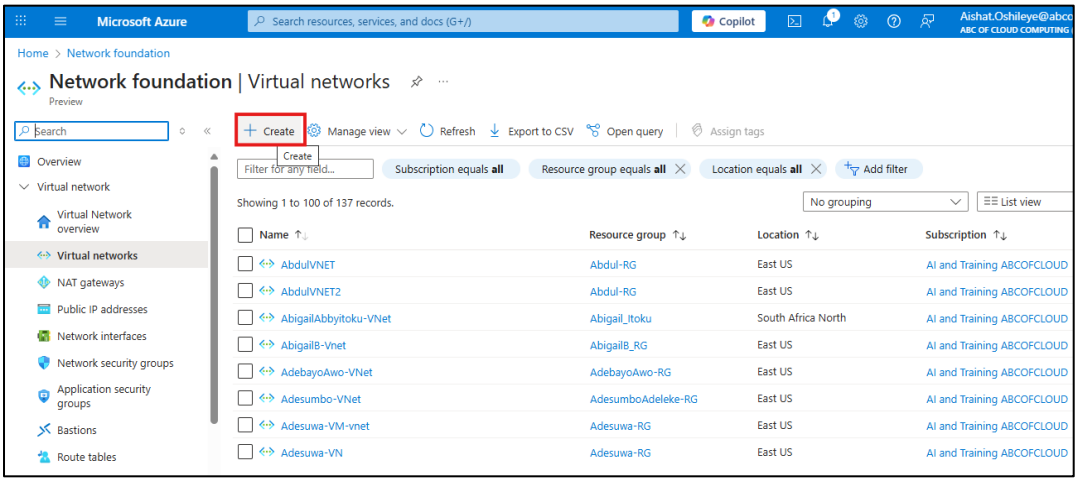




Task 2: Create a Virtual Network (VNet) with 2 Subnets

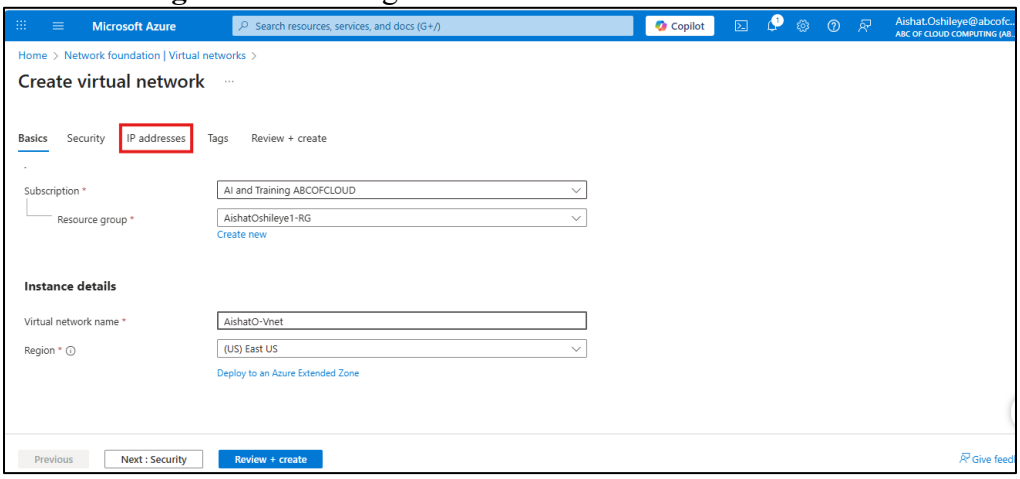
1. In the search bar, type **Virtual networks** and click + **Create**.



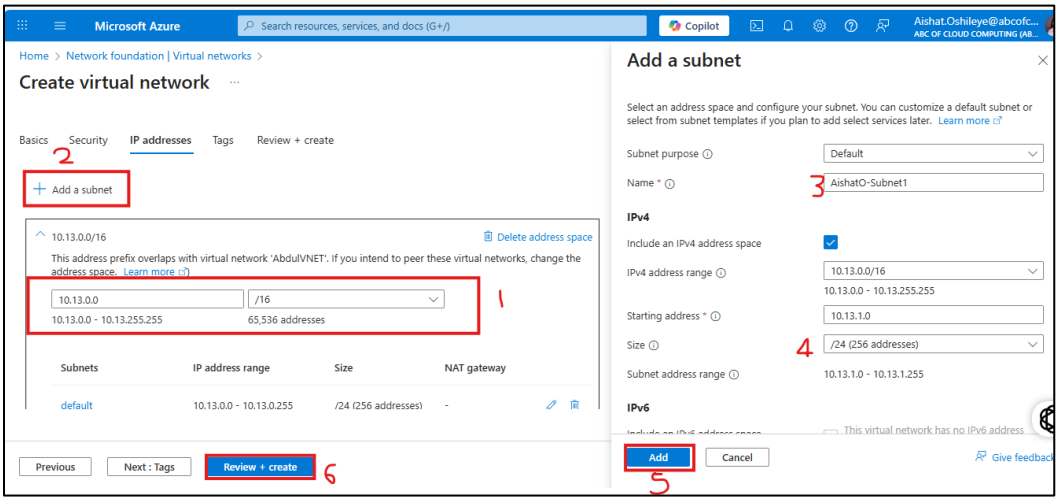


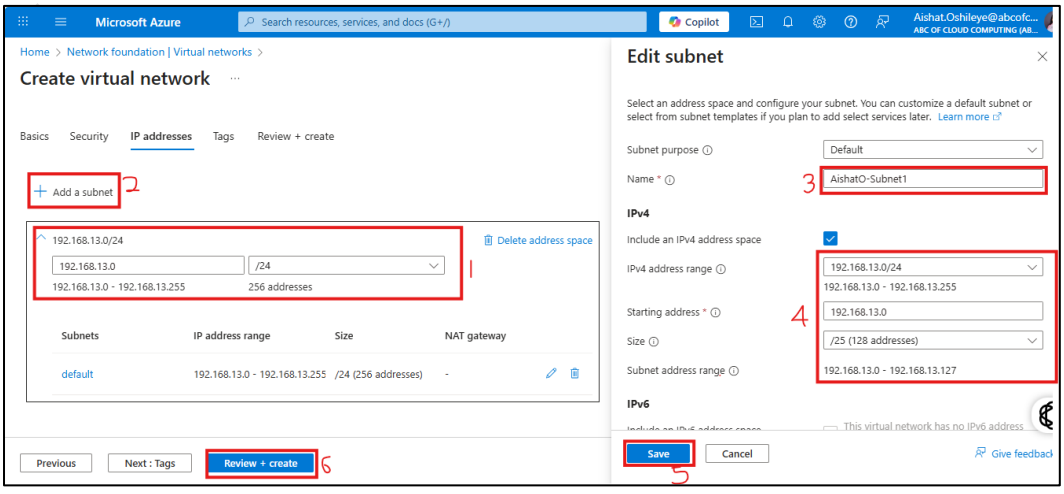
2. Choose your **Subscription** and **Resource Group**.
3. Enter a **Name** for your VNet (e.g., `MyVNet`).

4. Select the **Region**. Then Navigate to the IP Addresses tab

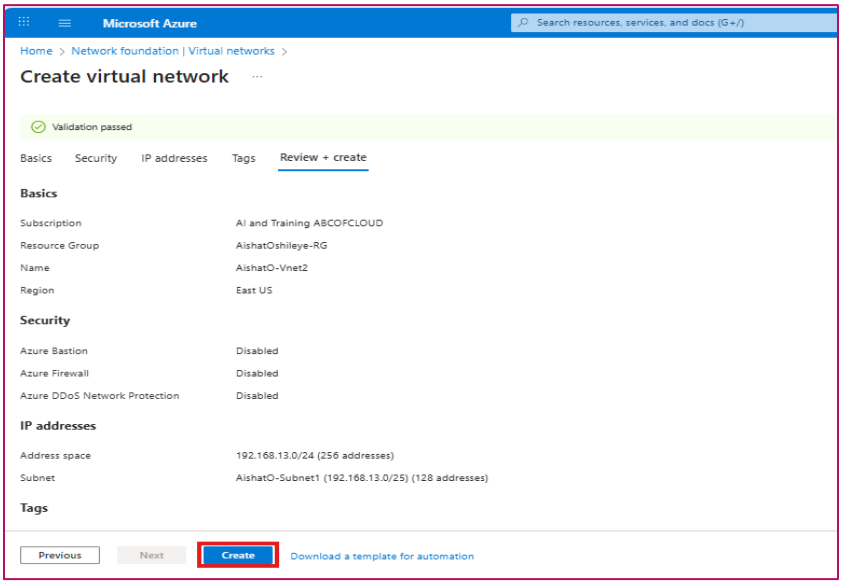


5. Under **IP Addresses**, define your **Address Space** (e.g., `10.0.0.0/16`).
6. Add **2 Subnets**: Example;
    - Subnet1: `10.0.1.0/24`
    - Subnet2: `10.0.2.0/24`



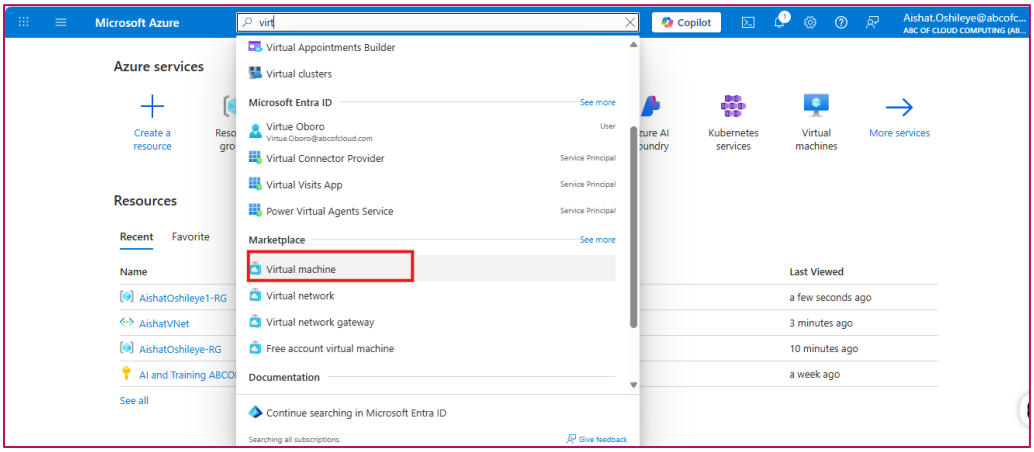


7. Click **Review + Create → Create**.

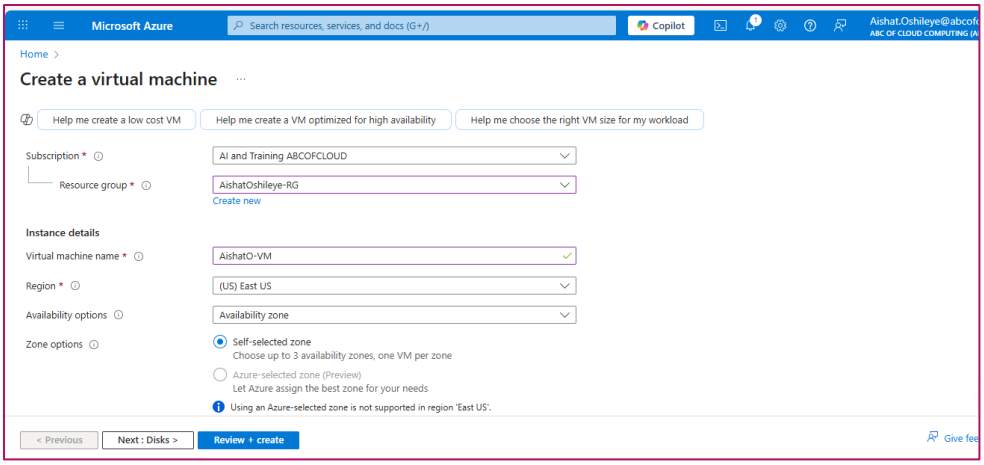


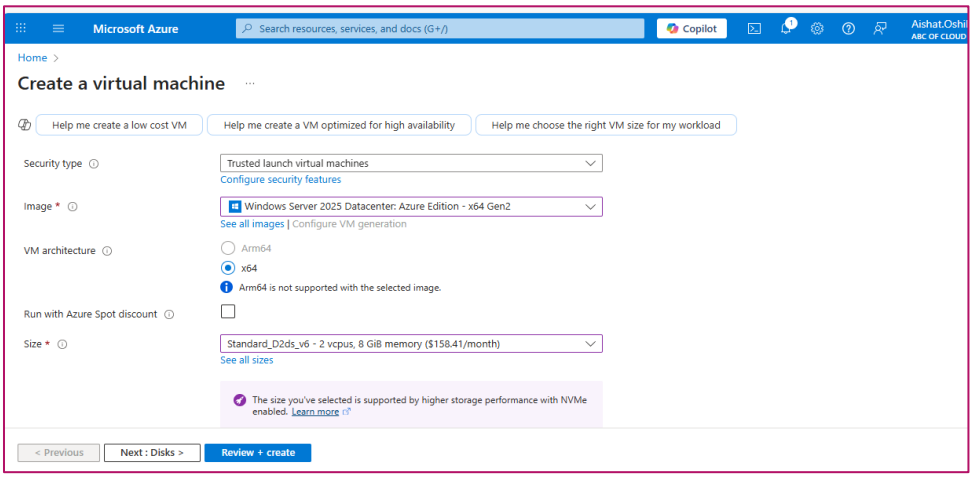
Task 3: Create a Virtual Machine and Attach an Additional Disk

1. In the search bar, type **Virtual machines** → Click **+ Create** → **Azure virtual machine**.

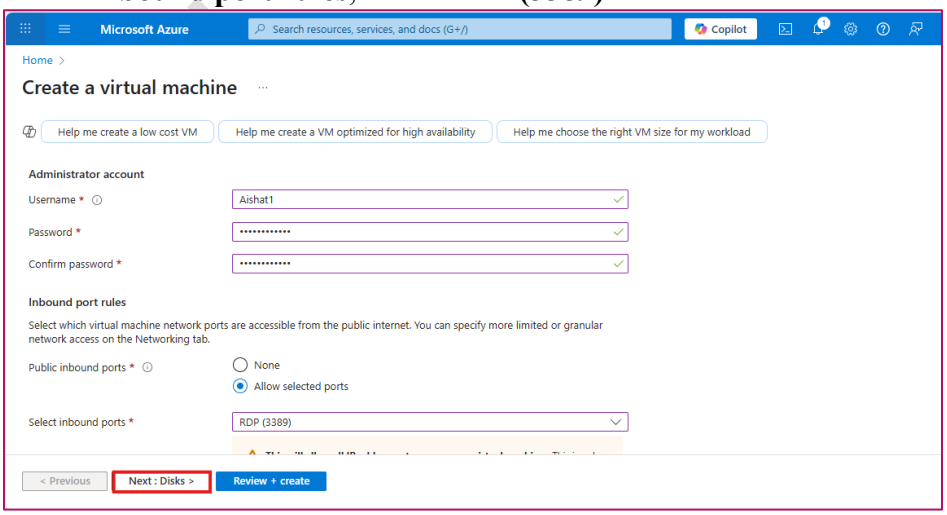


2. Select your **Resource Group**.
3. Name your VM (e.g., `MyVM`).
4. Choose the **Region** (same as your VNet).
5. Choose an **Image** (e.g., `Windows Server 2019 Datacenter`).



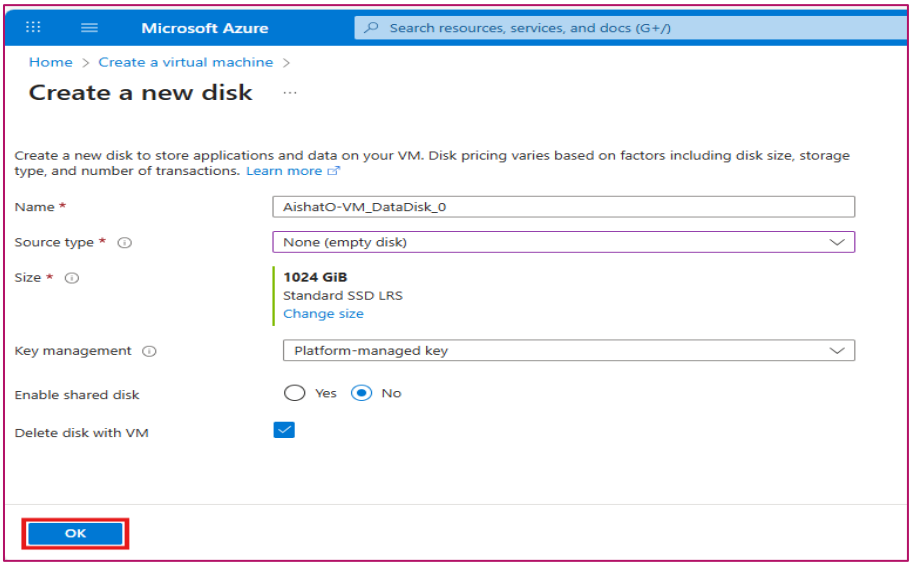


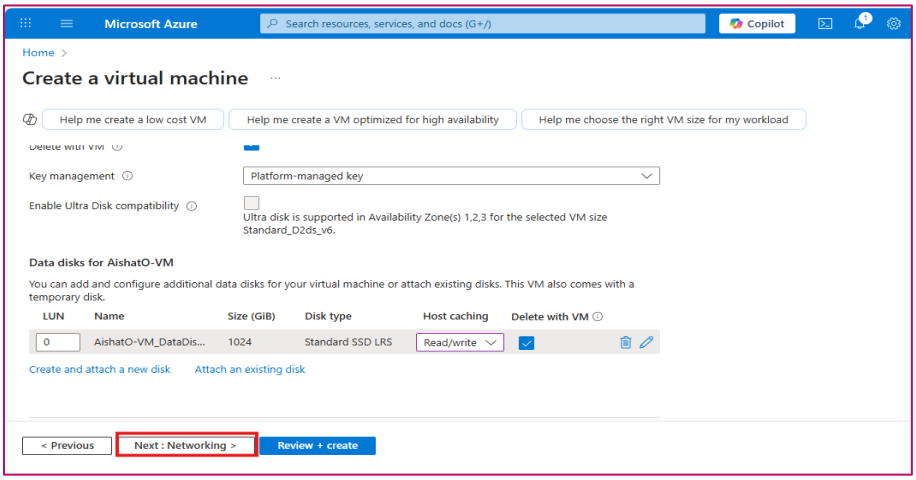
6. Create or select an **Admin username** and **Password**.
7. Under **Inbound port rules**, select **RDP (3389)**.



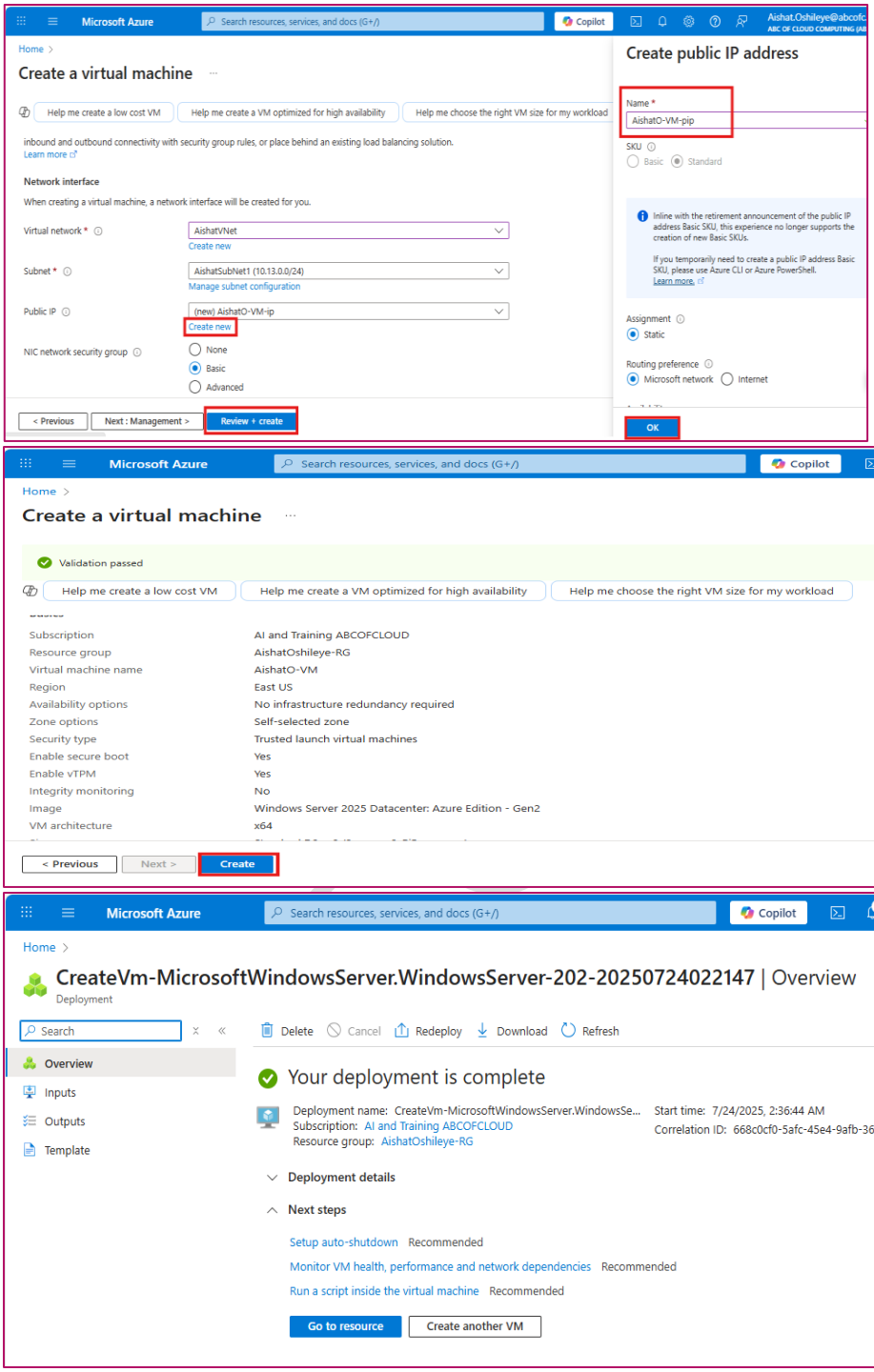
8. Click **Next: Disks** and enter disk details → **Create and Attach a New Disk**.

   Configure New Disk details, **Save** and Click **Next: Networking**





1. Under **Networking**, choose:
    - Existing **Virtual Network** and **Subnet**
    - Select **create new** under **Public IP** (optional for RDP)
    - Select an option **(Basic)** for NIC **Network Security Group**
2. Click **Review + Create → Create**.

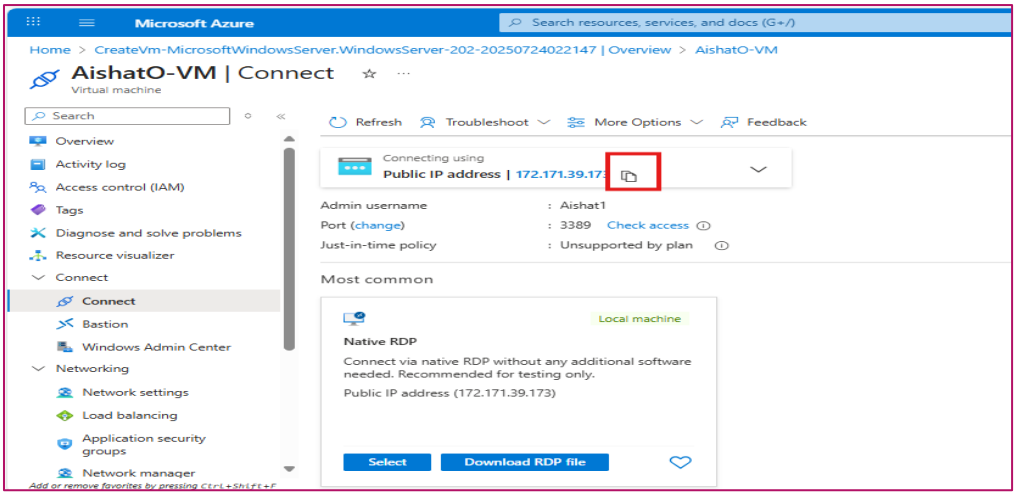


Connect to the VM Via RDP, only recommended for testing purpose. RDP exposes the VM to the public

1. In the left-hand menu, click **Virtual machines**.
2. Click on the **name of your VM**.

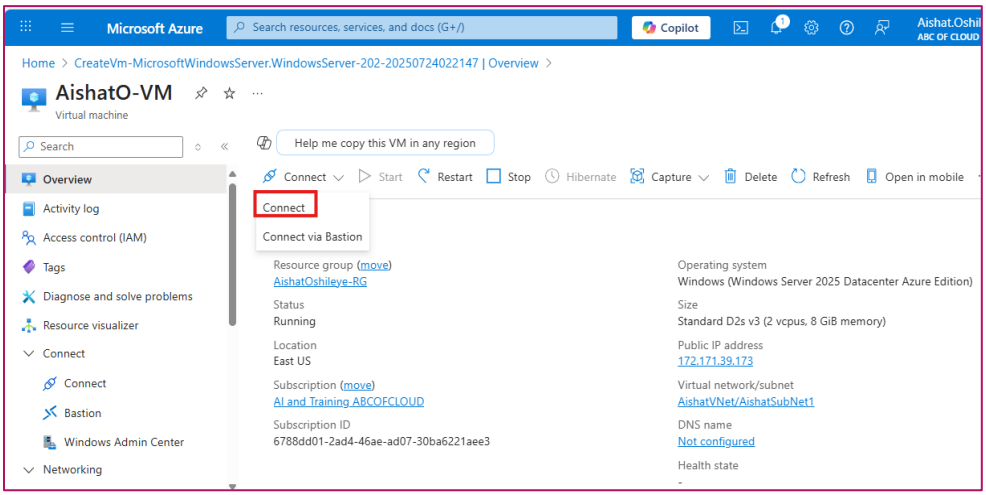
Locate the Public IP Address

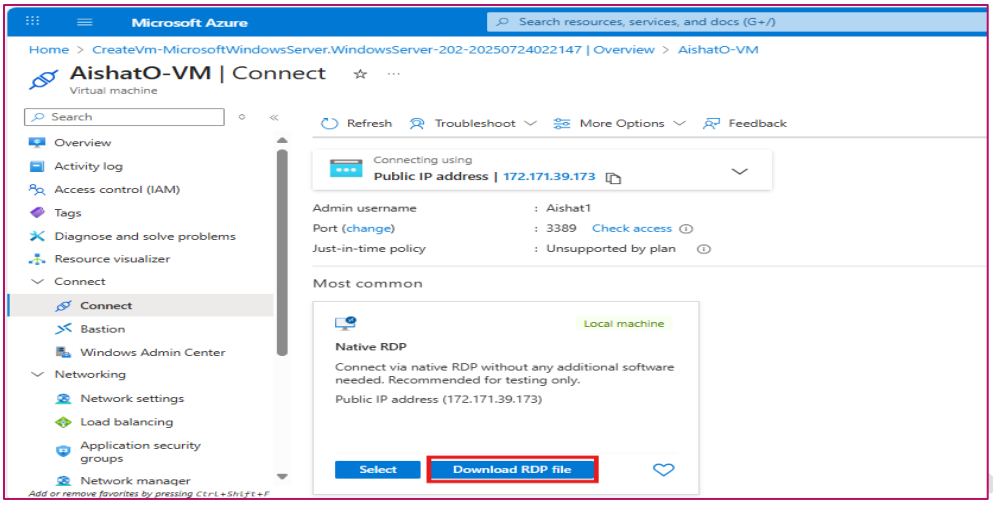
1. In the VM Overview page, look for **Public IP address**.
2. Copy this IP — you will need it for the RDP connection.

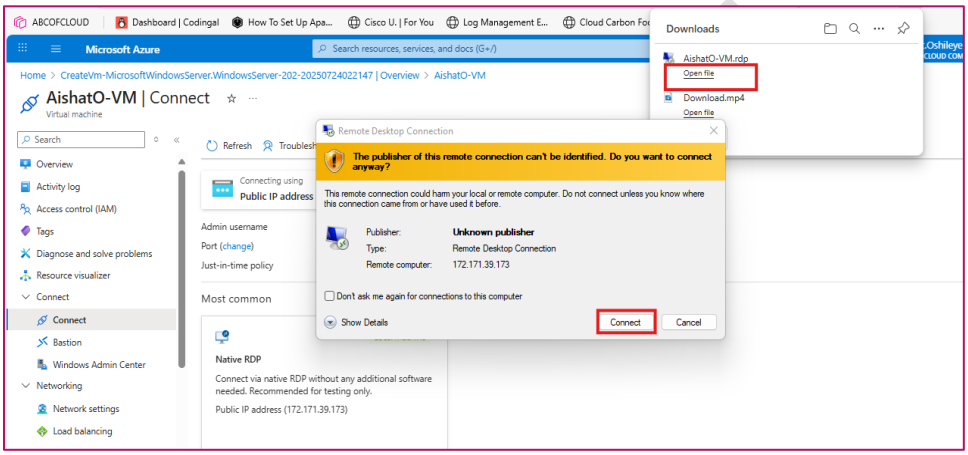


Download the RDP File (Optional Method)

1. Still on the VM Overview page, click the **Connect** button at the top.
2. Choose **RDP**.
3. In the pane that appears, click **Download RDP File**.
4. Open the downloaded `.rdp` file.



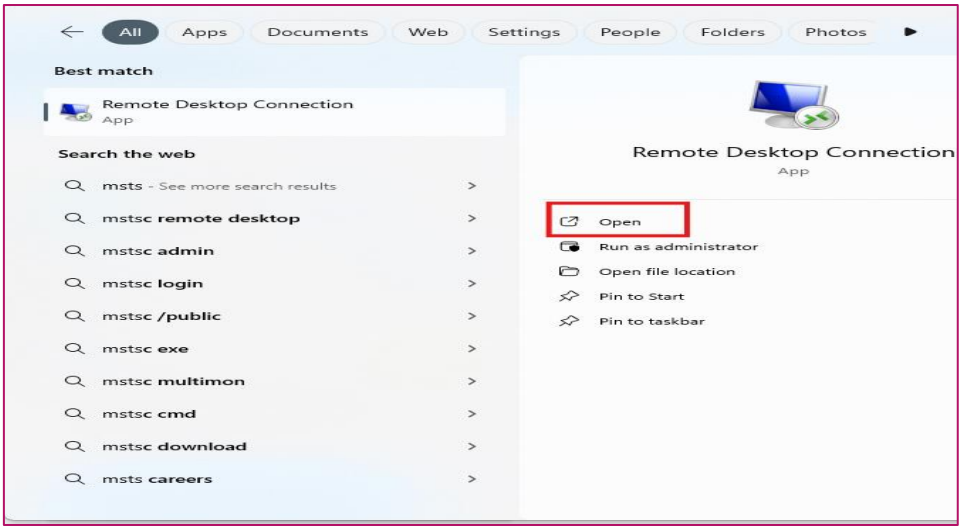




Connect Using Remote Desktop App (Manual Method)

RDP is used only for testing purposes and not recommended for use in Production environments

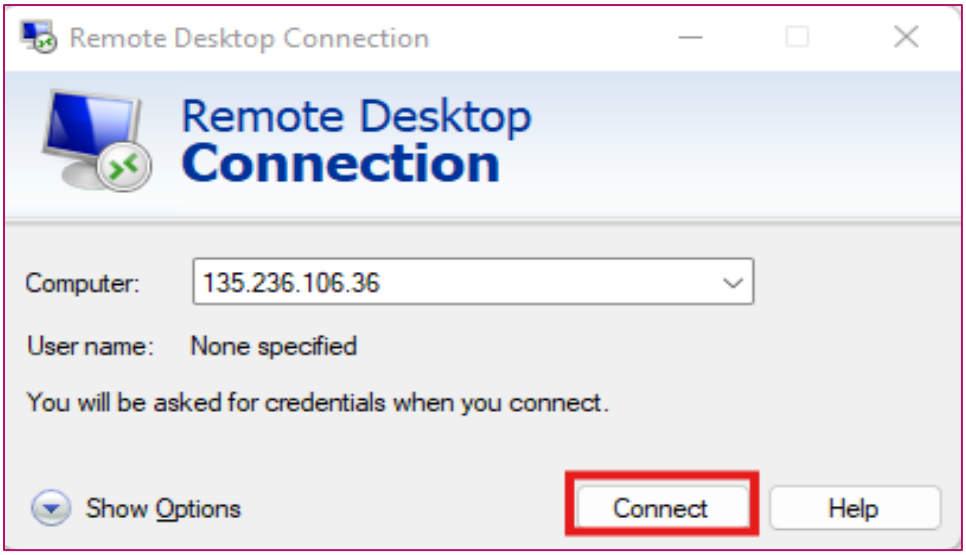
1. On your local computer, press **Windows + R**, type `mstsc`, and press **Enter**.
2. In the **Remote Desktop Connection** window:
    - Enter the **Public IP address** of your VM
    - Click **Connect**

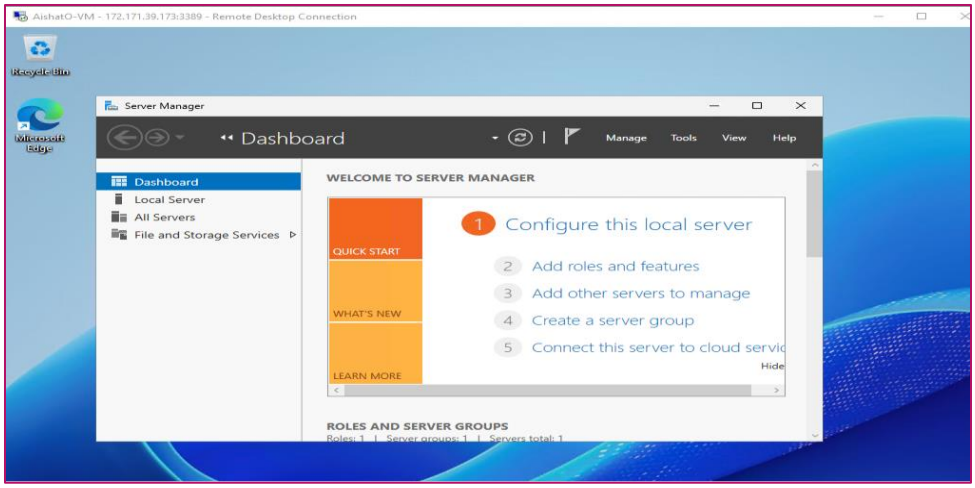


Enter Credentials

1. When prompted, enter the **admin username and password** you created when setting up the VM.

2. Click **OK**. Accept the certificate warning if prompted

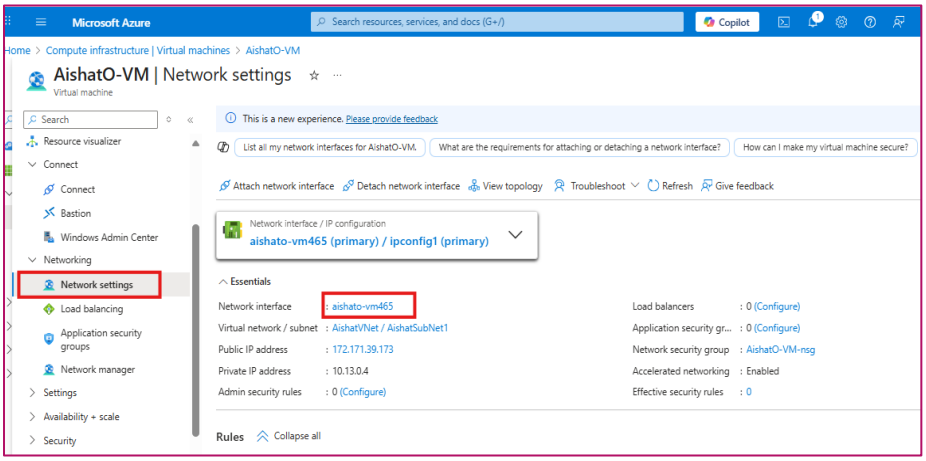


3. 

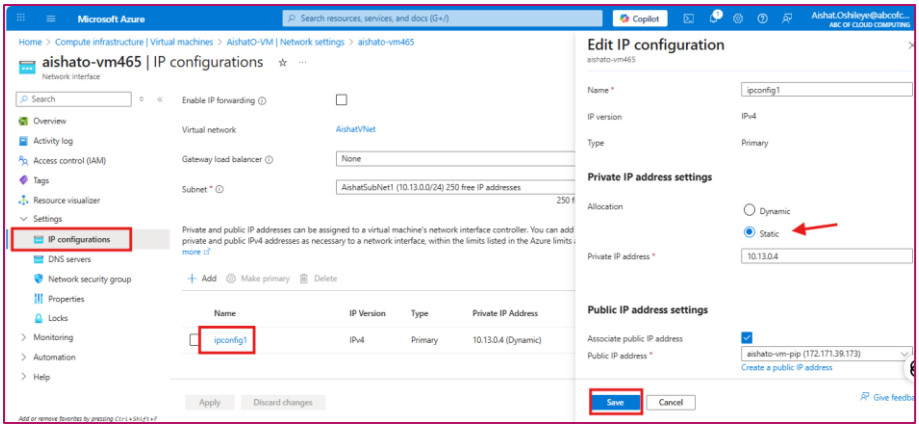
You should now be connected to your Azure VM via RDP and can interact with it like a regular Windows computer.

Step 4: Configure the Network Interface (NIC)

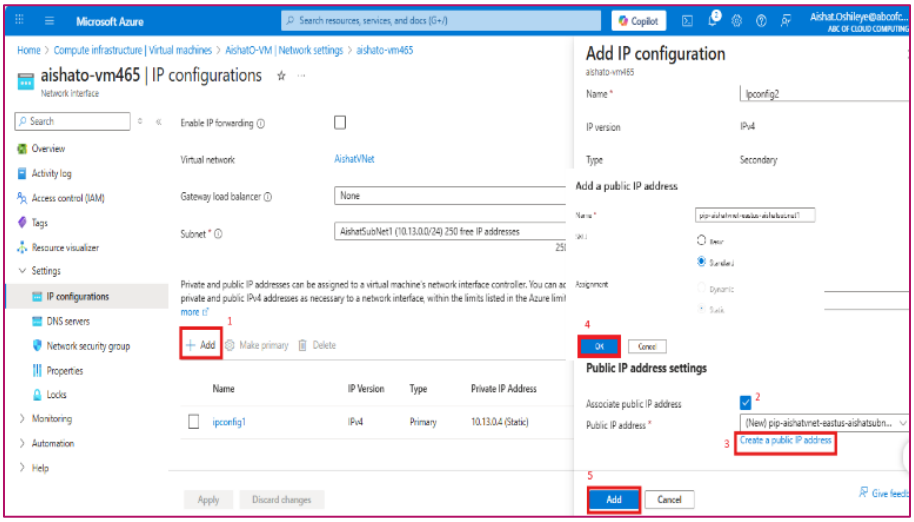
1. Go to **Virtual machines** → Select your VM.
2. In the VM blade, under **Settings**, click **Networking**.
3. Click on the **Network interface name**.



4. Under **Settings**, go to **IP configurations**.
5. Select the configuration, click **Edit**, and:
    - Set **Private IP address** to **Static**
    - Enter the IP (e.g., `10.0.1.4`)

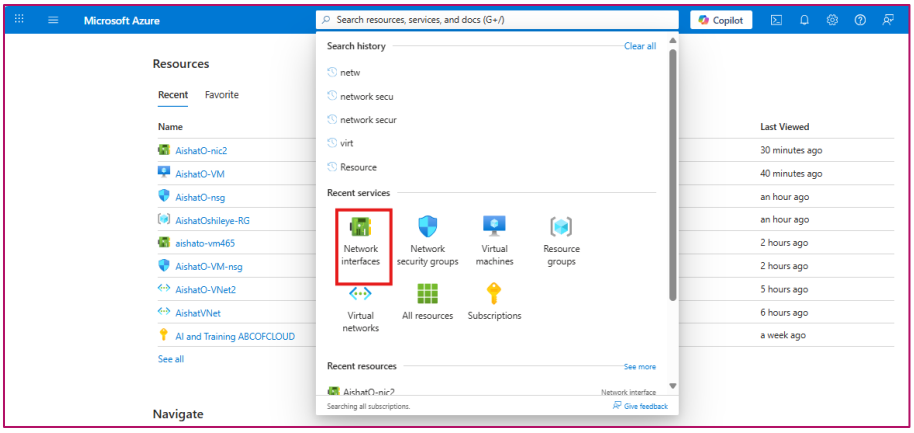


6. Save changes.
7. Create a new network interface by clicking +**Add.** This opens a new window that prompts you to Add IP configurations.
8. Add a name for the ipconfig.
9. Set private IP address to **static.**
10. Select **create a new public IP address** and configure the public IP address settings.
11. Click **OK**, then **Add**



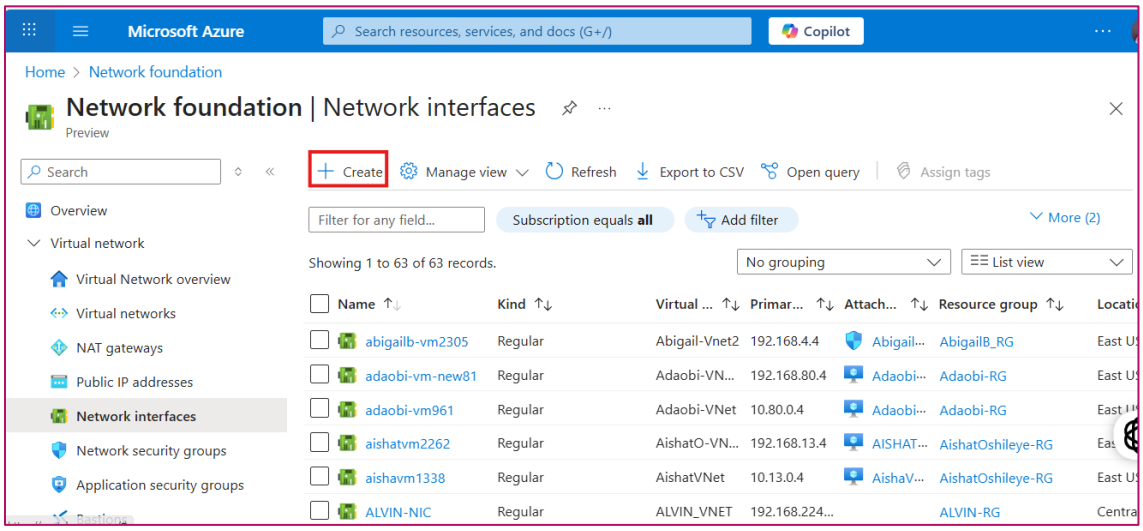
Create a New Network Interface

Step 1: Search for "Network Interfaces"



- **Step 3: Start Creating a New NIC**

1. Click on **+ Create** or **+ Add** at the top.



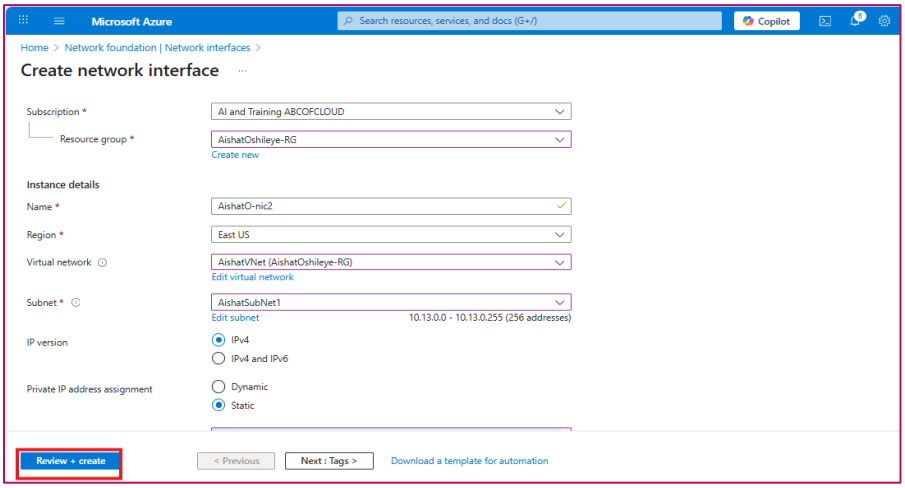
- **Step 4: Fill in NIC Details**

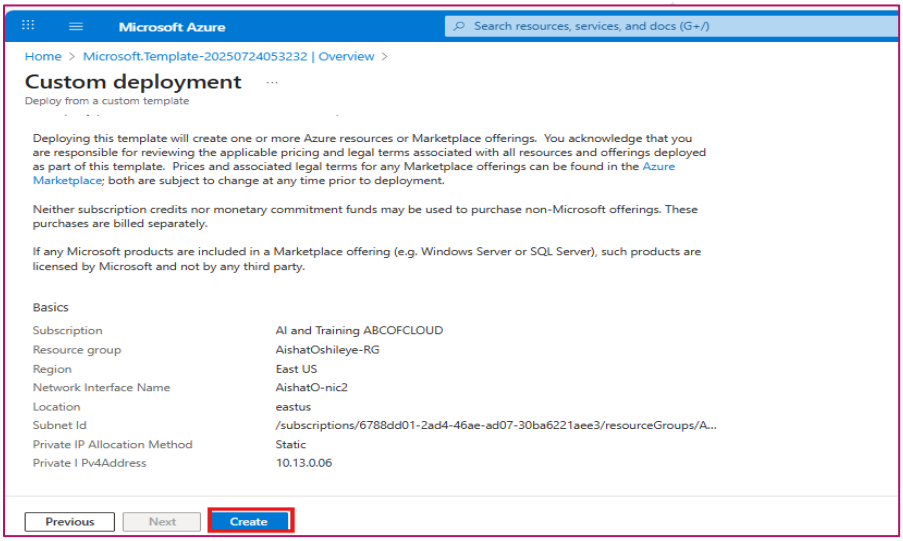
1. **Subscription**: Choose your Azure subscription.
2. **Resource Group**: Select the existing resource group (e.g., MyResourceGroup).
3. **Name**: Enter a name for the NIC (e.g., MyNIC1).
4. **Region**: Select the same region as your VM and VNet (e.g., West Europe).

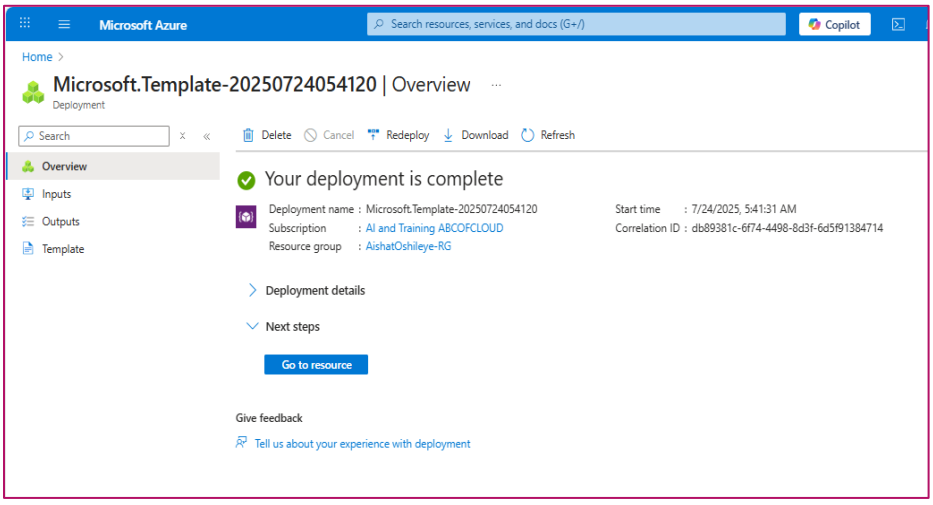
Configure Network Settings

1. **Virtual Network**: Choose the existing VNet (e.g., MyVNet).
2. **Subnet**: Select one of the subnets you created earlier (e.g., Subnet1).
3. **Private IP**: You can leave it as **Dynamic**, or choose **Static** and enter an IP (e.g., 10.0.1.5).
4. Click **Review + create**.

5. Once validation passes, click **Create**.

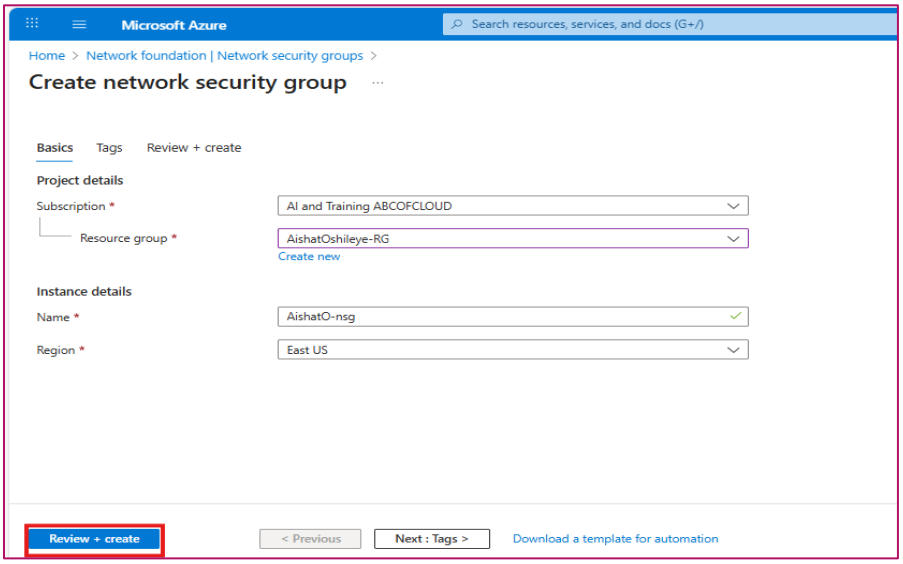


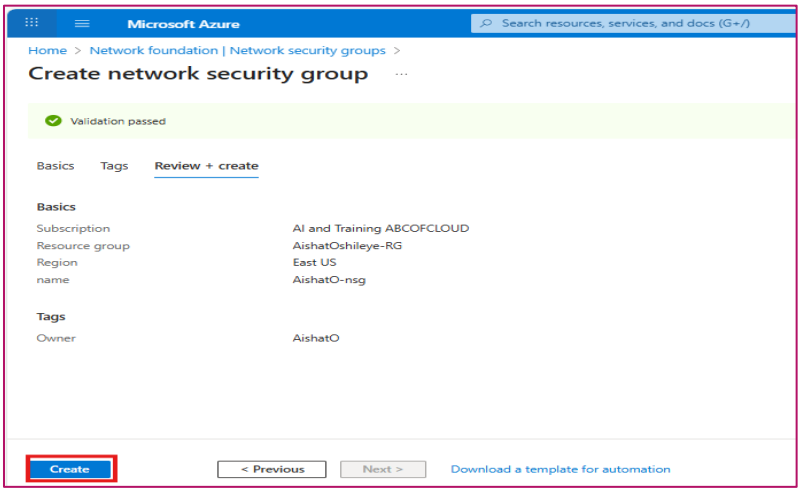




Task 5: Create and Configure Network Security Group (NSG)

1. In the search bar, type **Network security groups** → Click **+ Create**.
2. Select your **Subscription** and **Resource Group**.
3. Enter **Name** (e.g., `MyNSG`) and select the **Region**.
4. Click **Review + Create** → **Create**.



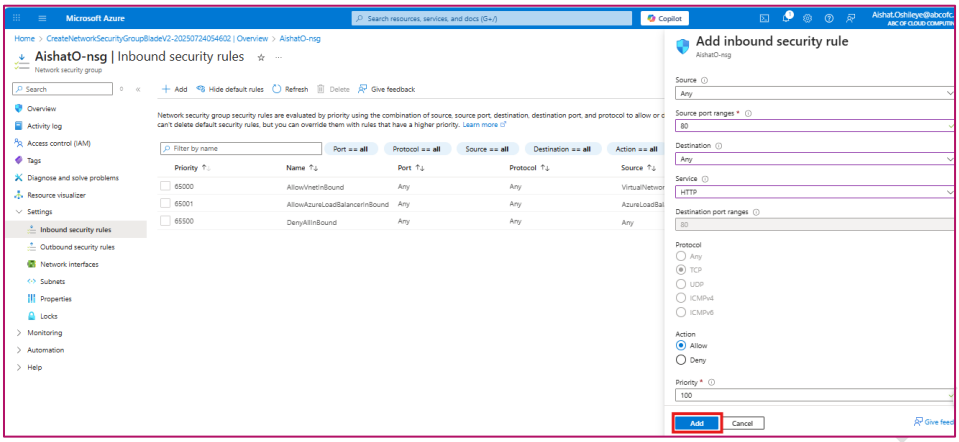


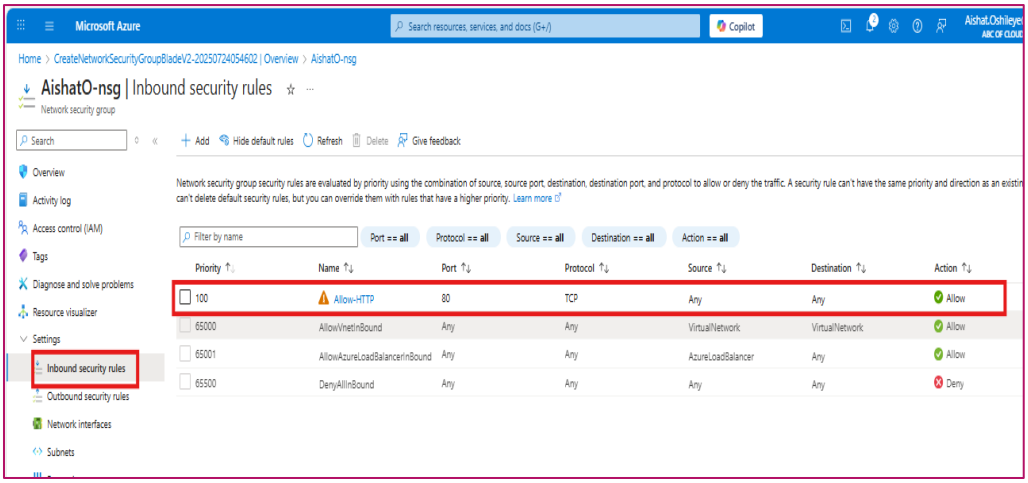
5. After creation, open the NSG → Go to **Inbound security rules** → **+ Add**:

Rule 1 – Allow Web App (HTTP)

- **Source**: Any
- **Protocol**: TCP
- **Port**: 80

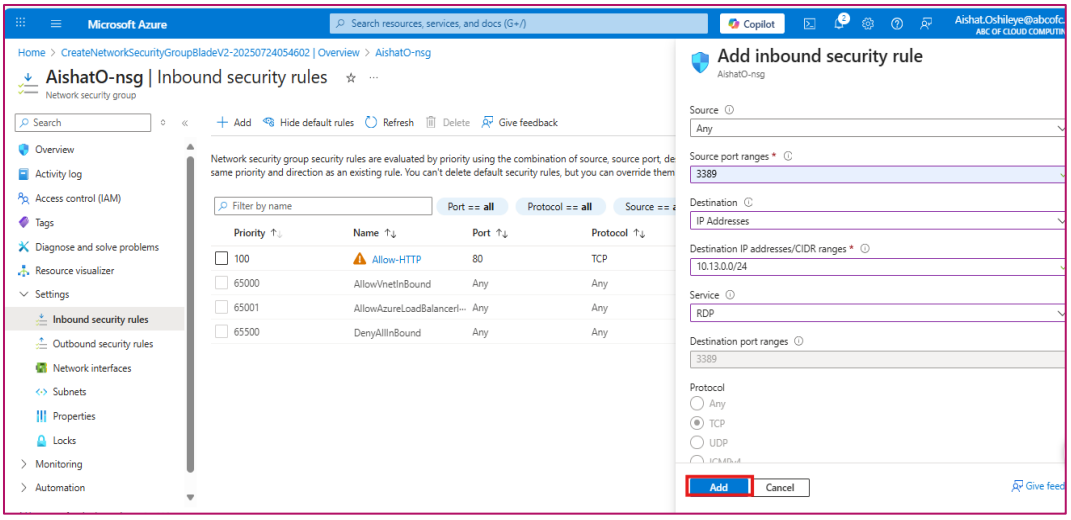
- **Action**: Allow
- **Priority**: 100
- **Name**: Allow-HTTP

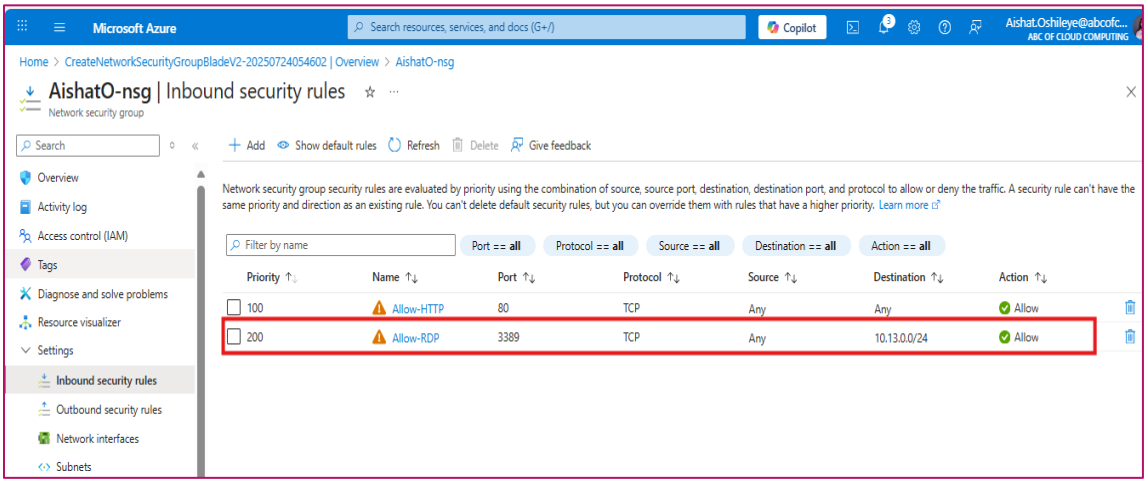




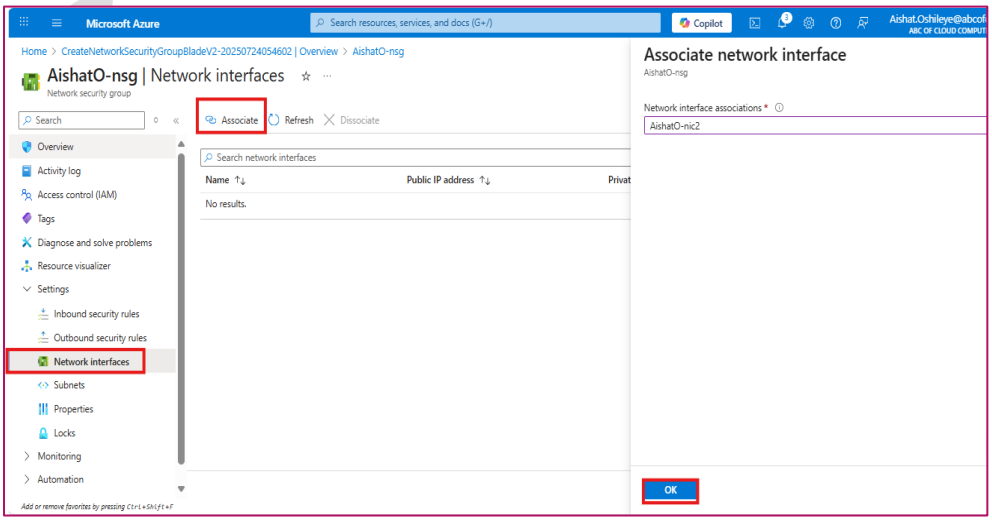
Rule 2 – Allow RDP

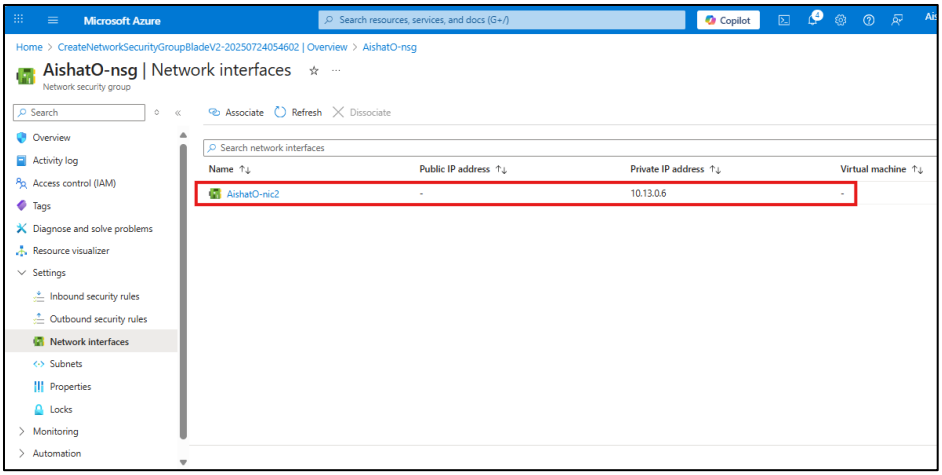
- **Source**: Any
- **Protocol**: TCP
- **Port**: 3389
- **Action**: Allow
- **Priority**: 200
- **Name**: Allow-RDP





6. Associate the NSG to your **NIC** or **Subnet** by selecting **Network interfaces** or **Subnets** under **Settings** in the NSG.

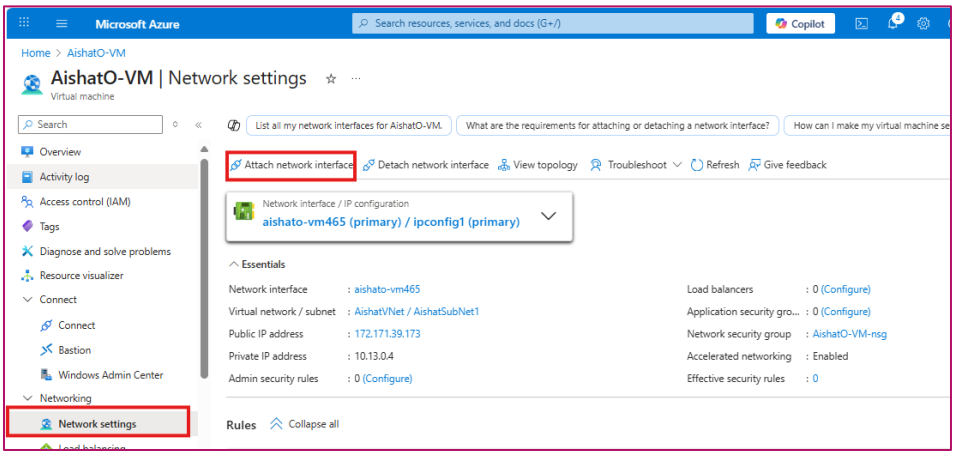


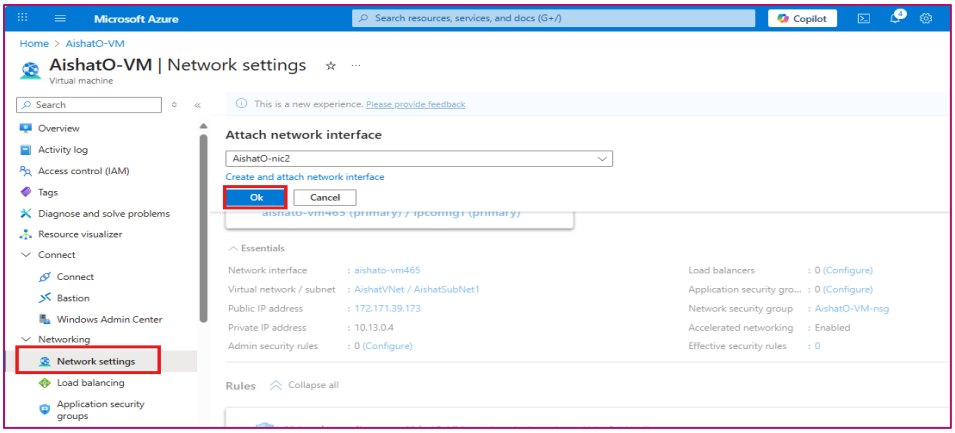


Task 6: Attach the NIC to the VM

This step applies if you created a NIC separately and want to attach it to a VM.

1. Stop the VM if running.
2. Go to the **Virtual machine → Networking → Detach network interface** (if needed).
3. Attach the new NIC via **Networking → + Attach network interface**.
4. Select the NIC → OK.

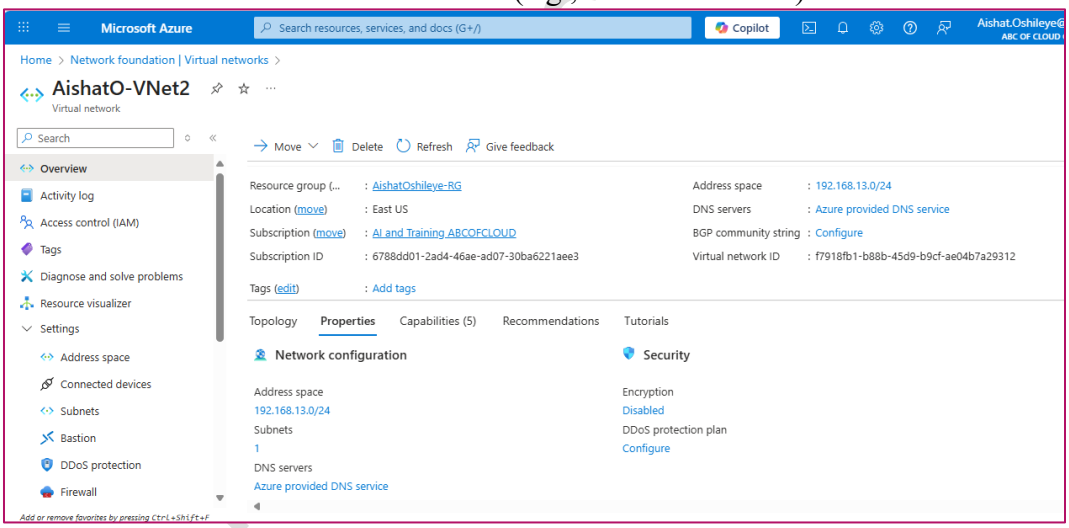


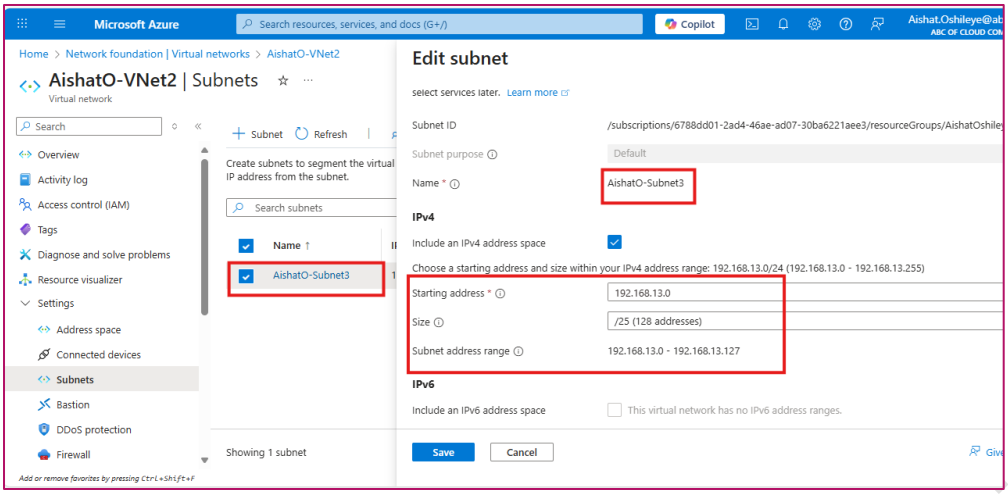


Task 7: Configure VNet Peering and Connect Two VMs

Step 1: Create a Subnet in a second Vnet

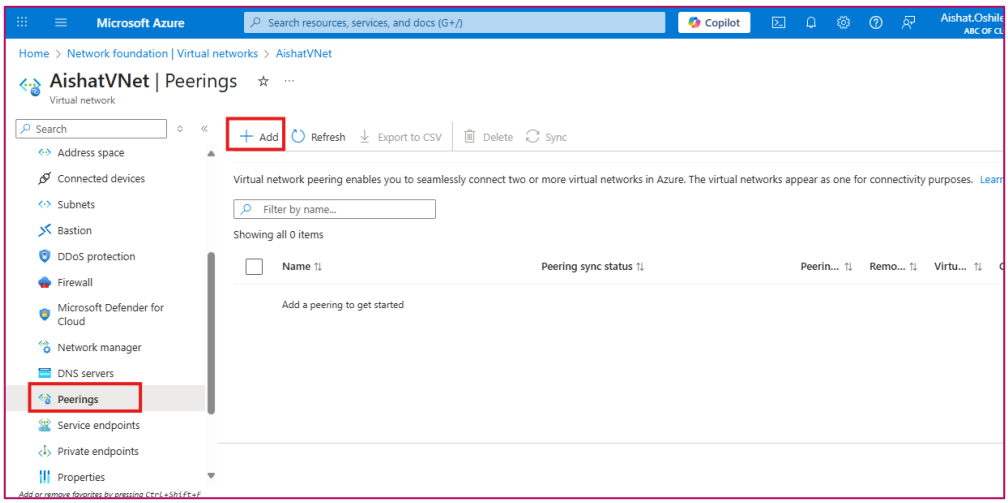
1. Go back to your second VNet
2. Add another subnet: **AishatO-Subnet3** (e.g., 192.168.13.0/25)

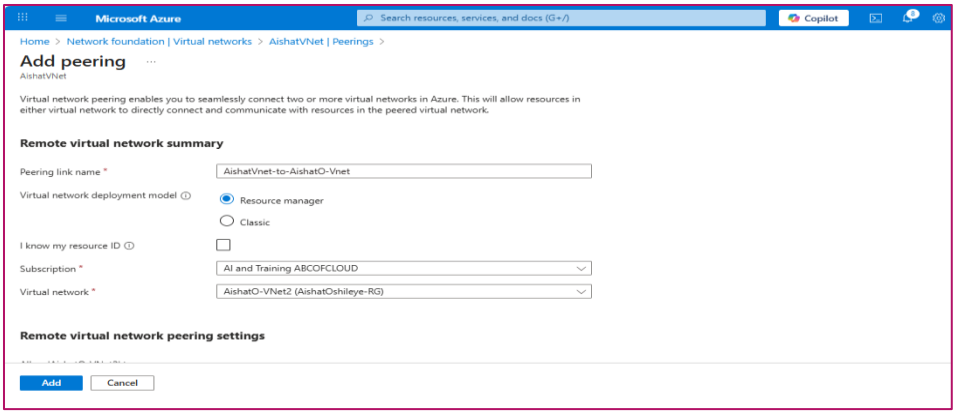


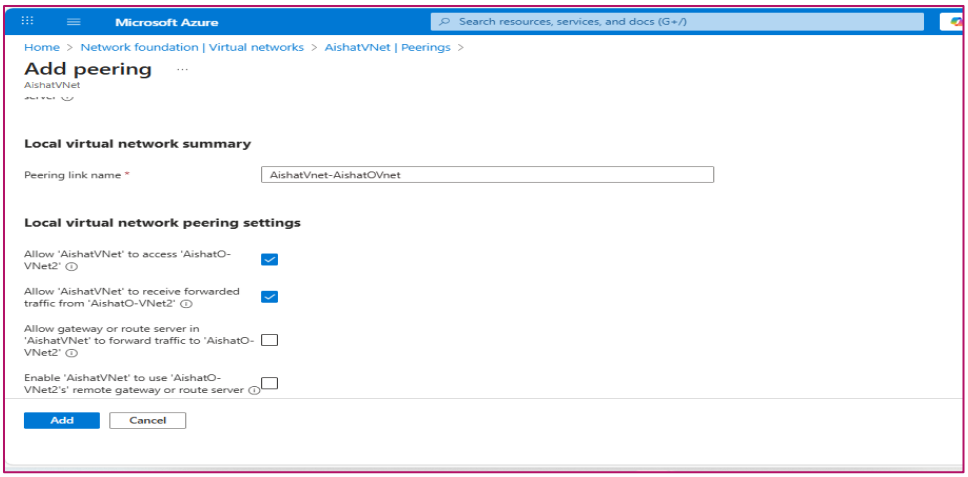


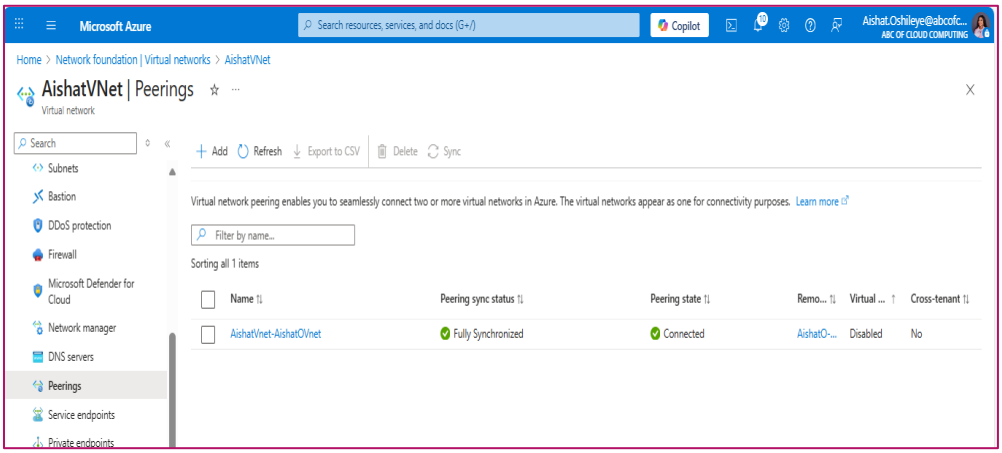
Step 2: Create Another VM in AishatO-Subnet3
Repeat **VM creation steps** and place it in **AishatO-Subnet3**. Name it **AishatOVM2**.
Step 3: Configure VNet Peering

1. Navigate Home > Virtual networks > Your VNet > Peerings > + Add
   - **Peering link name**: vnet-to-vnet (or more descriptive)
   - **Virtual network**: Same VNet or another one (in this case, another one)
   - Enable **"Allow traffic"** both ways
   - Click **"Add"**



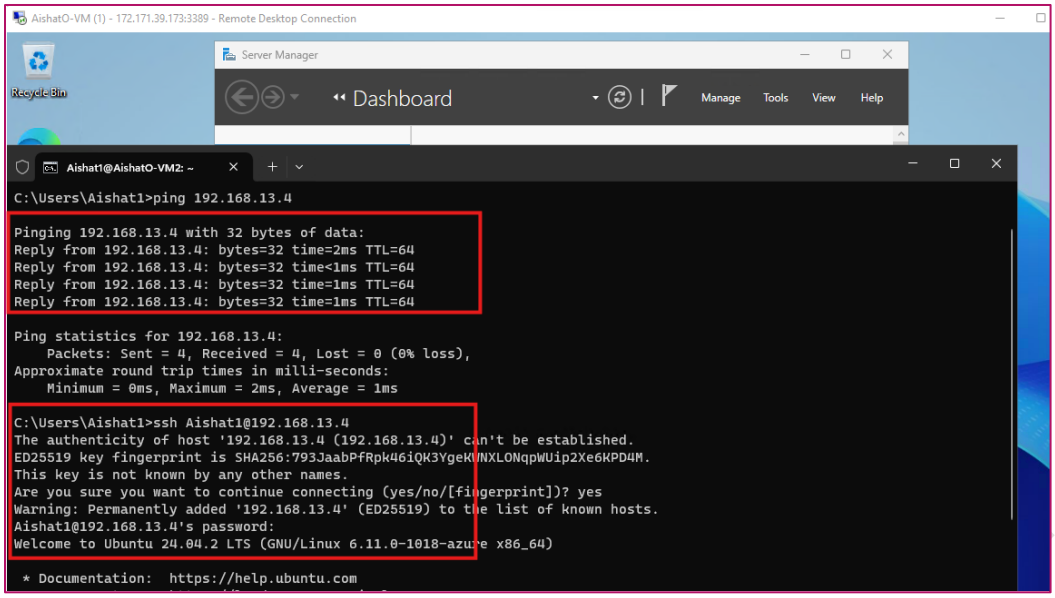






Step 4: Test VM Connectivity

- Use RDP from VM1 to SSH into the other via its **Private IP** (found in NIC or VM overview) RDP into VM1 and SSH from VM1 to VM2



Summary

Resource	Task
Resource Group	Created a Resource Group to contain all resources
Virtual Network	Created 2 Vnets in resource group
Subnet	Created two subnets in VNet2 and 1 subnet in Vnet2
VM	Created 1 each in 2 subnets
Disks	Attached to VMs
NIC + NSG	Created, configured and attached to VMs
NSG Rules	Allow HTTP and RDP
Peering	Configured between Vnets
Connection	Verified between VMs

If you have come this far, you're ready to build more advanced cloud solutions!