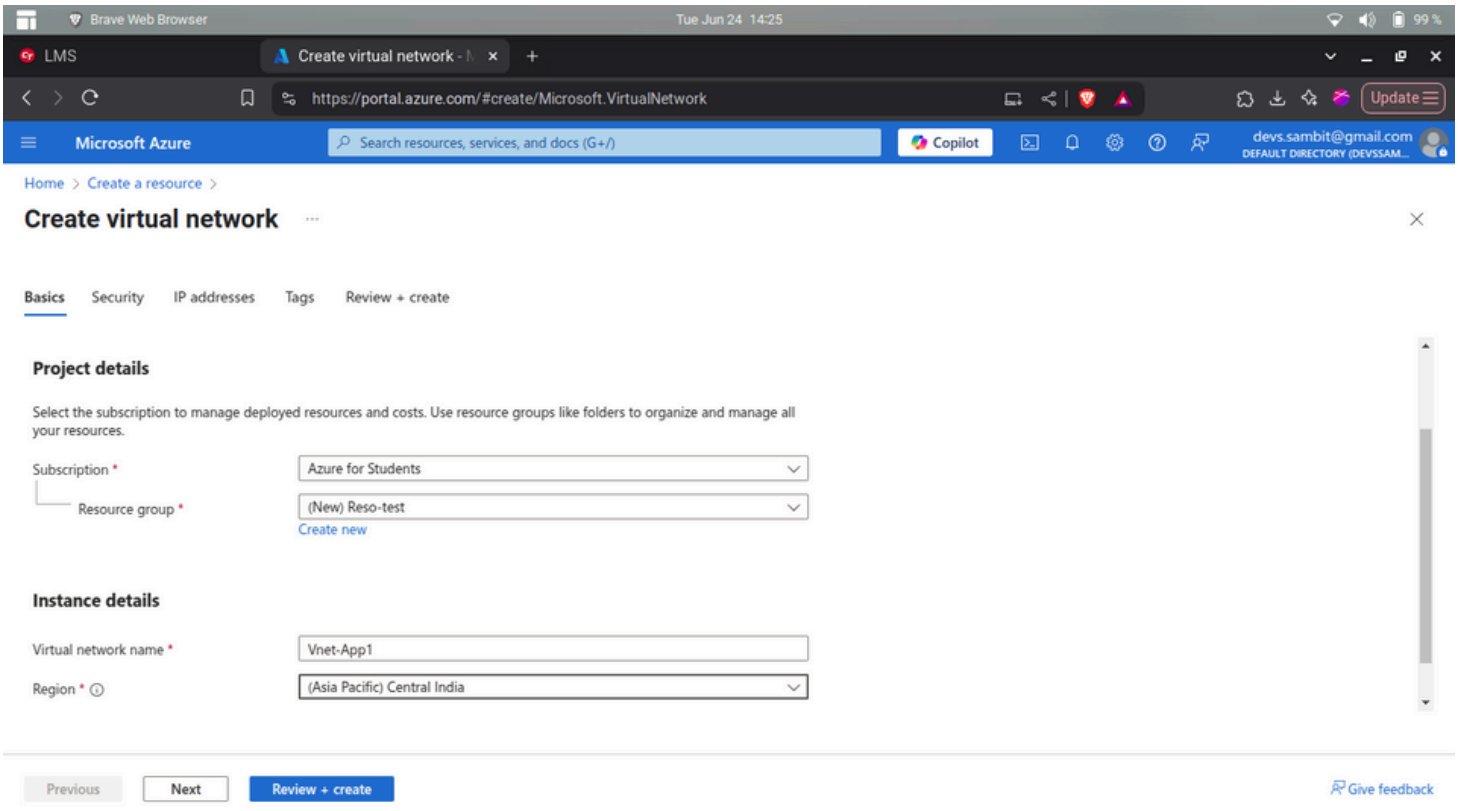
CONFIGURATION OF VNET, VM & PEERING

Step 1: Create the First Virtual Network (VNet1) and its Subnets

- Log in to Azure Portal
- Search for Virtual Networks
- Create a New Virtual Network
- **Basics Tab**

1. Subscription: Ensure your Azure for Students subscription is selected.
2. Resource Group: Click Create new and enter a name. This group will hold all our resources. Click OK.
3. Virtual network name: Enter VNet-App1.
4. Region: Choose a region close to you, e.g., Central India.



BASICS TAB

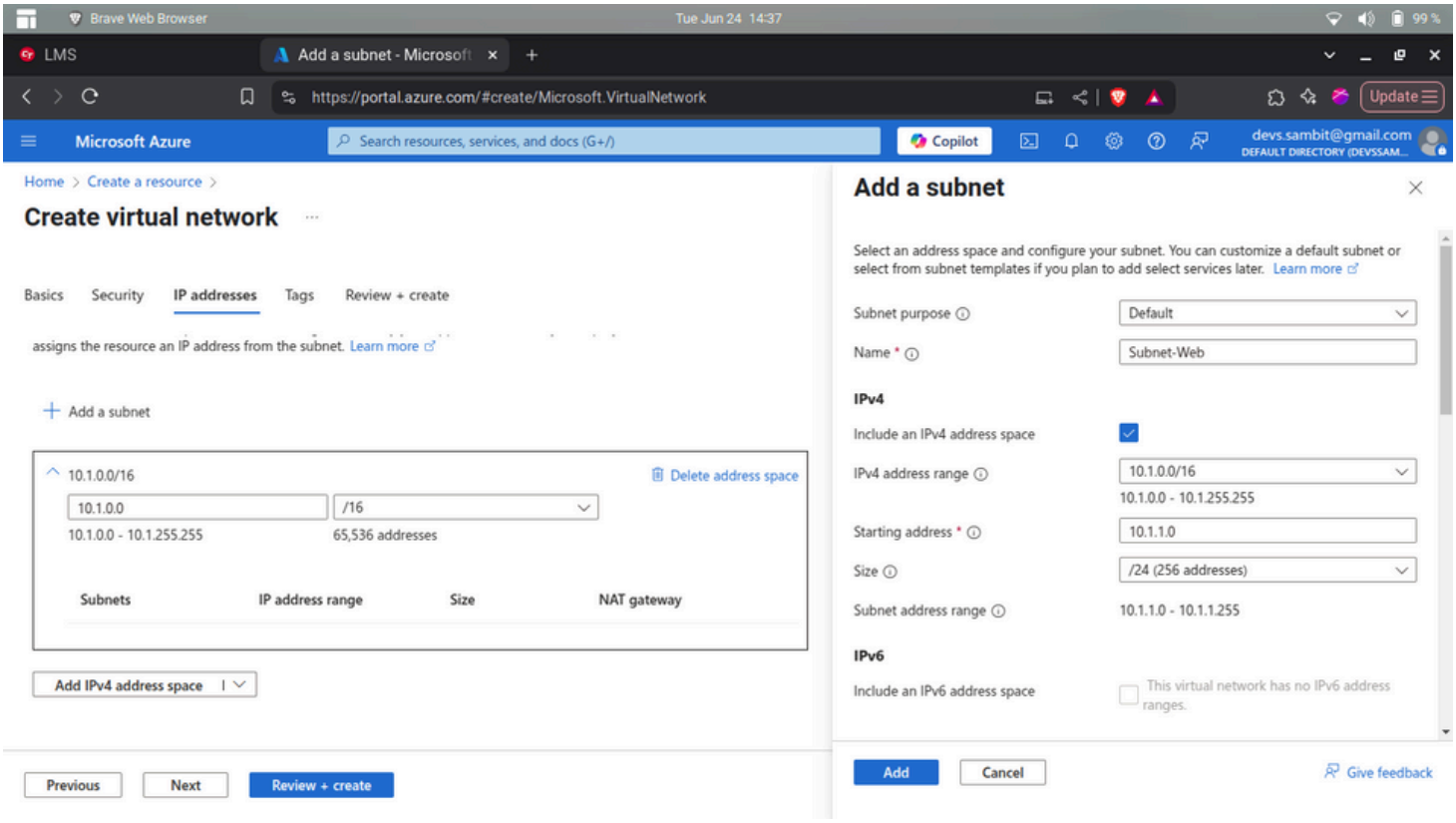
- **IP Addresses Tab:**

IPv4 address space: Enter 10.1.0.0/16.

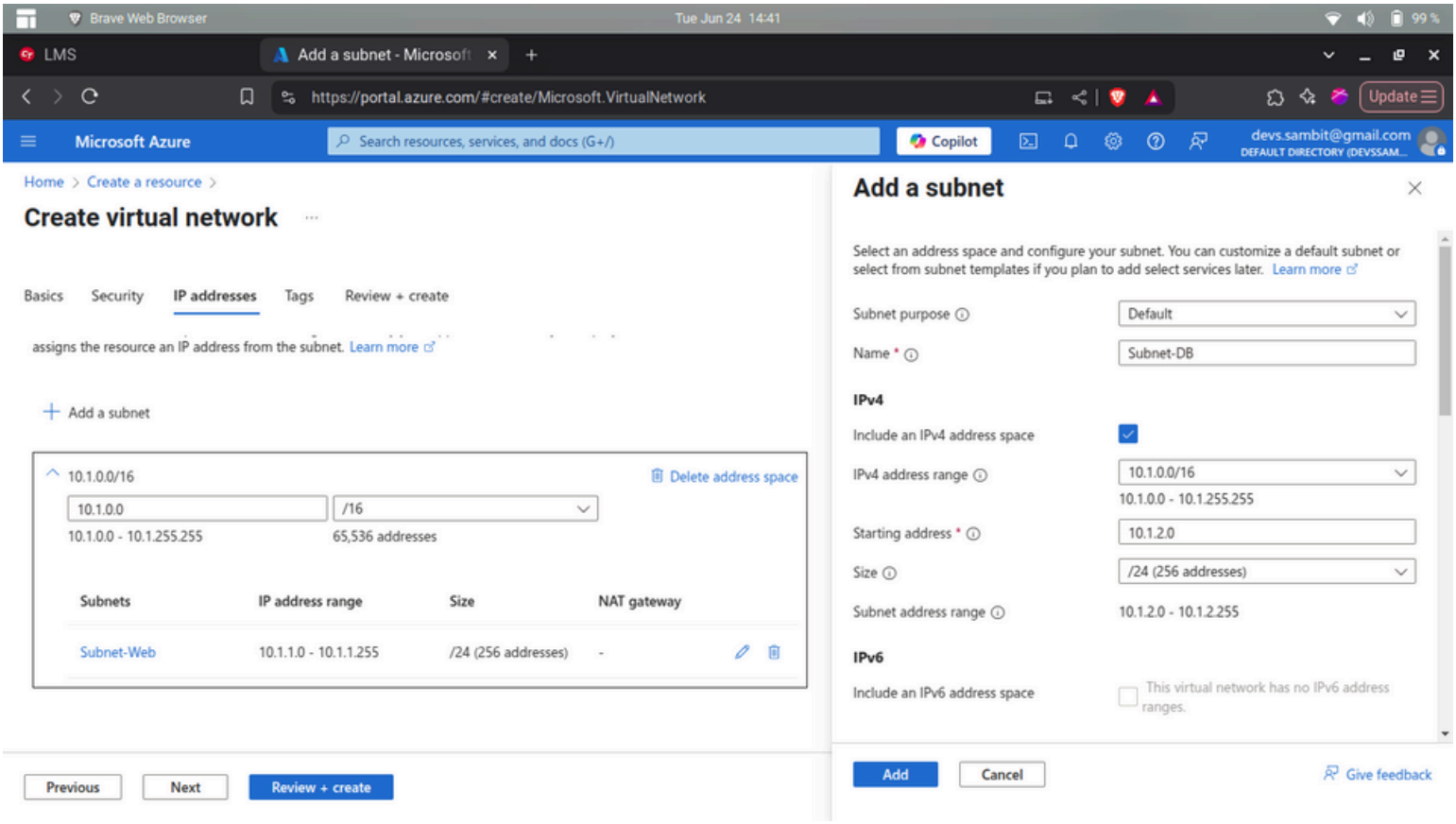
This gives your VNet a large block of private IPs.

Subnets: You'll see a default subnet. Let's configure ours:

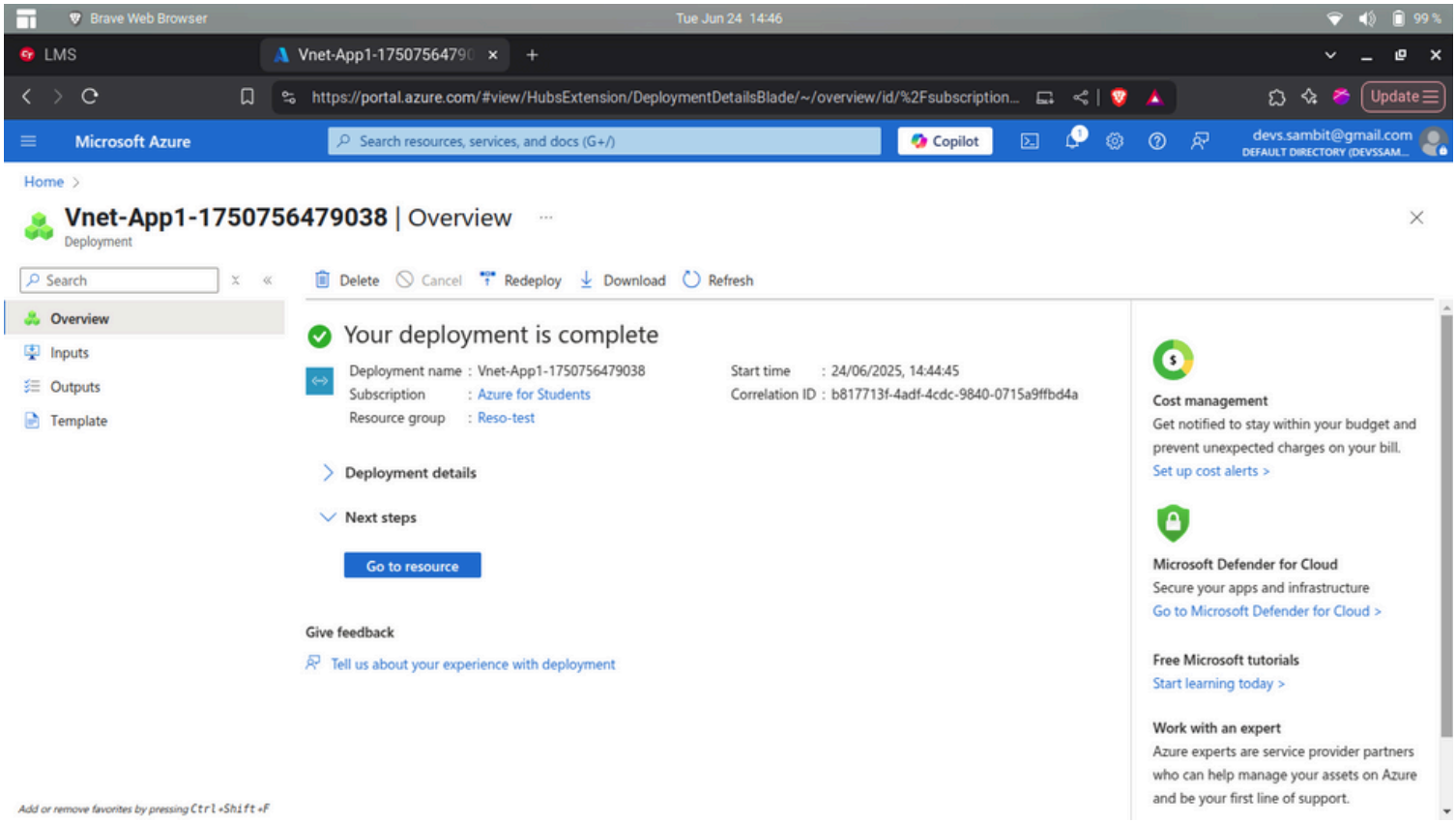
1. Click on the default subnet row.
2. Name: Change it to Subnet-Web.
3. Address range (CIDR block): Change it to 10.1.1.0/24. This will create 256 IPs, with 5 reserved by Azure, leaving 251 usable IPs.
4. Click Save.
5. Click + Add subnet.
6. Name: Enter Subnet-DB.
7. Address range (CIDR block): Enter 10.1.2.0/24.
8. Click Add.
9. Click Review + create.



IP ADDRESSES TAB : SUBNET-WEB



IP ADDRESSES TAB: SUBNET-DB

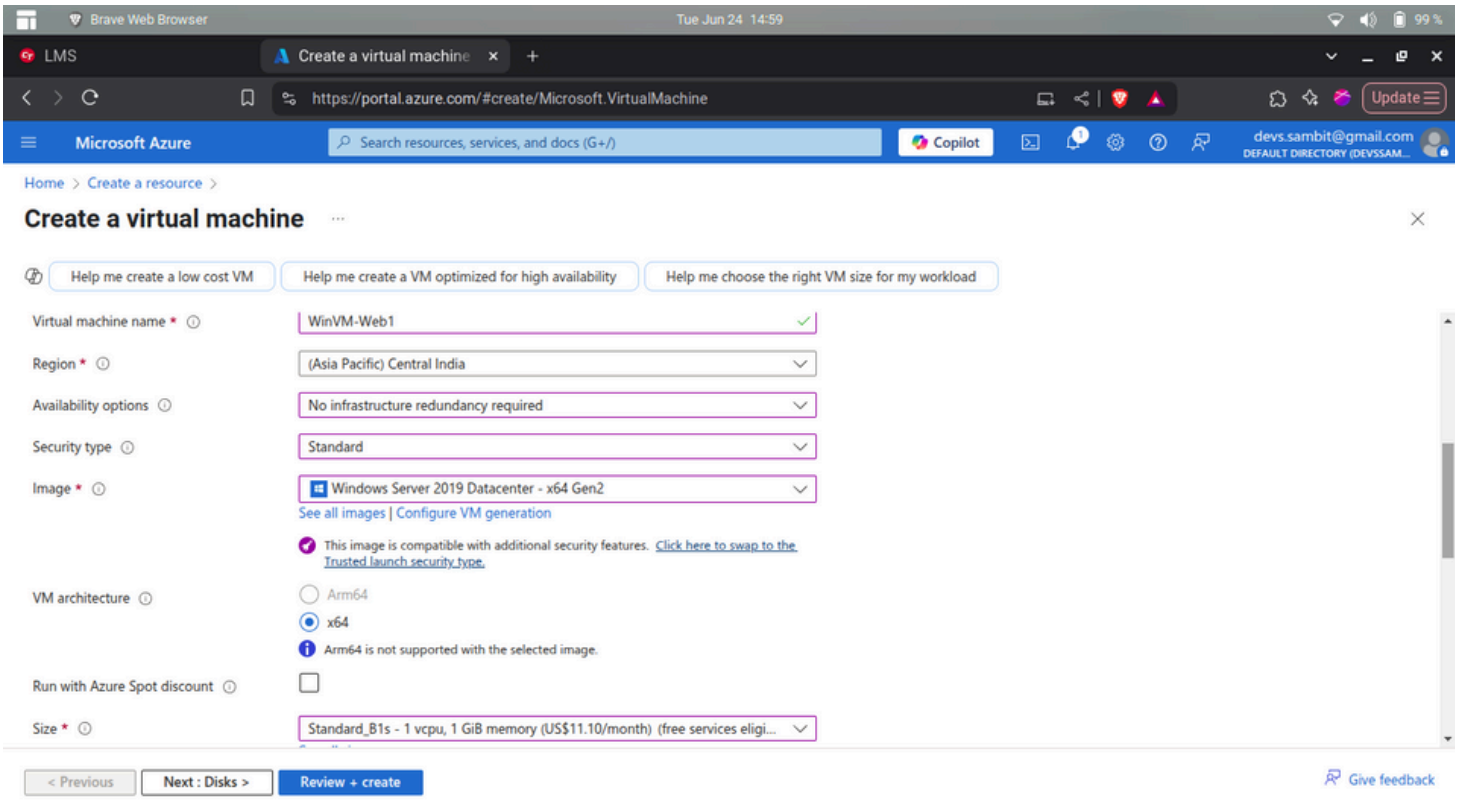


OVERVIEW PAGE

Step 2: Launch a Windows Virtual Machine (VM1) in Subnet-Web

We'll create WinVM-Web1 in VNet-App1's Subnet-Web.

- Search for Virtual Machines
- Create a New Virtual Machine
- On the Virtual machines page, click + Create > Azure virtual machine.
- Basics Tab:
- Subscription: Select your student subscription.
- Resource Group: Choose the existing RG-AzureNetworkingLab you created.
- Virtual machine name: Enter WinVM-Web1.
- Region: Select the same region you used for VNet-App1.
- Image: Select Windows Server 2019 Datacenter - Gen2.
- Size: Click See all sizes and search for B1s or B2s. Select B1s (it's very cheap for testing).



BASICS TAB

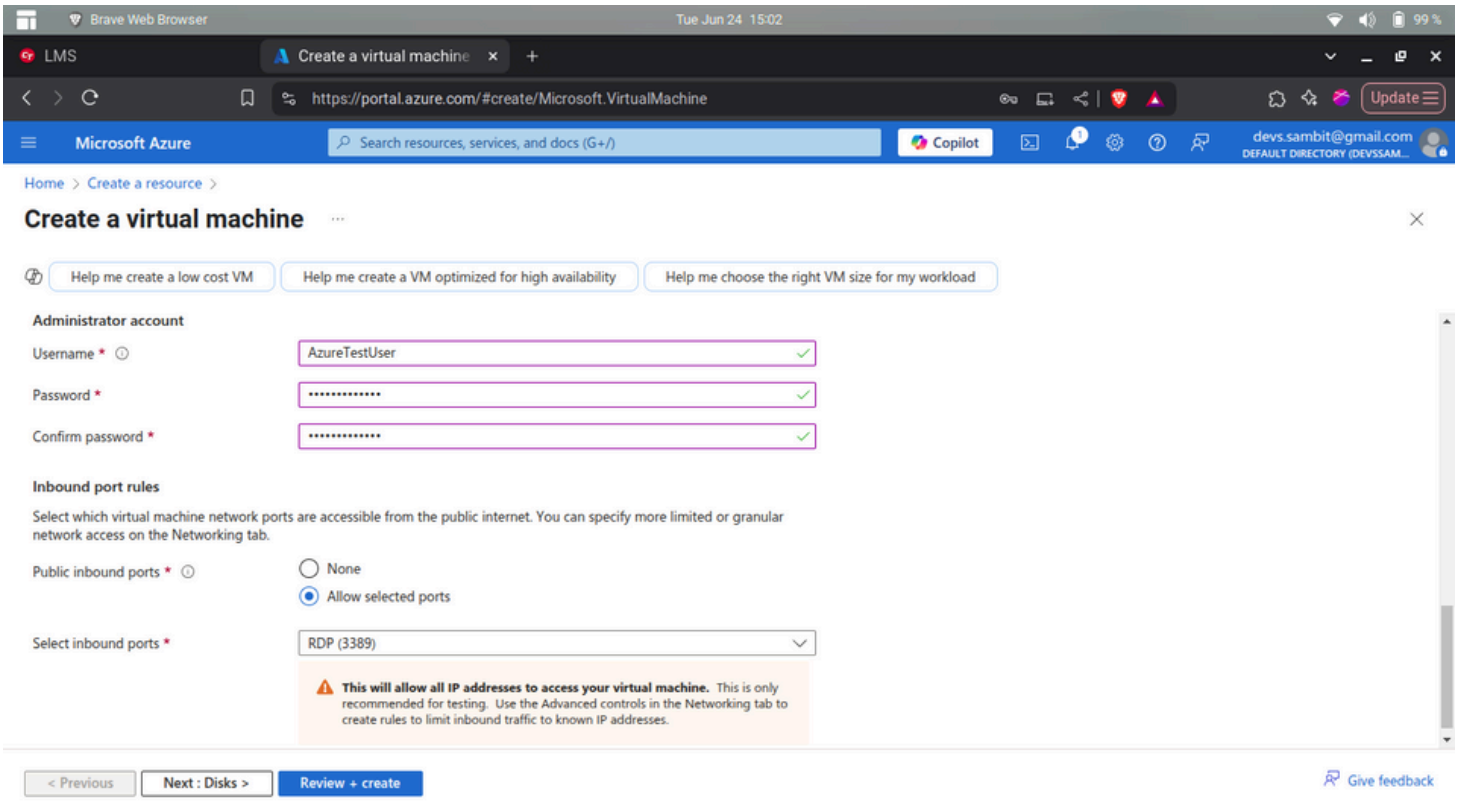
- **Administrator account:**

Username: Enter a username (e.g., AzureTestUser).

Password: Create a strong password and confirm it. Remember this username and password!

Inbound port rules:Public inbound ports: Choose Allow selected ports.

Select inbound ports: Check RDP (3389).



ADMINISTRATOR TAB

- **Disks Tab:**

Leave defaults for OS disk type.

- **Networking Tab:**

1. Virtual network: Select VNet-App1.
2. Subnet: Select Subnet-Web (10.1.1.0/24).
3. Public IP: Leave as (new) WinVM-Web1-ip. Azure will create a public IP for you to connect to the VM.
4. NIC network security group: Select Basic.
5. Click Review + create.

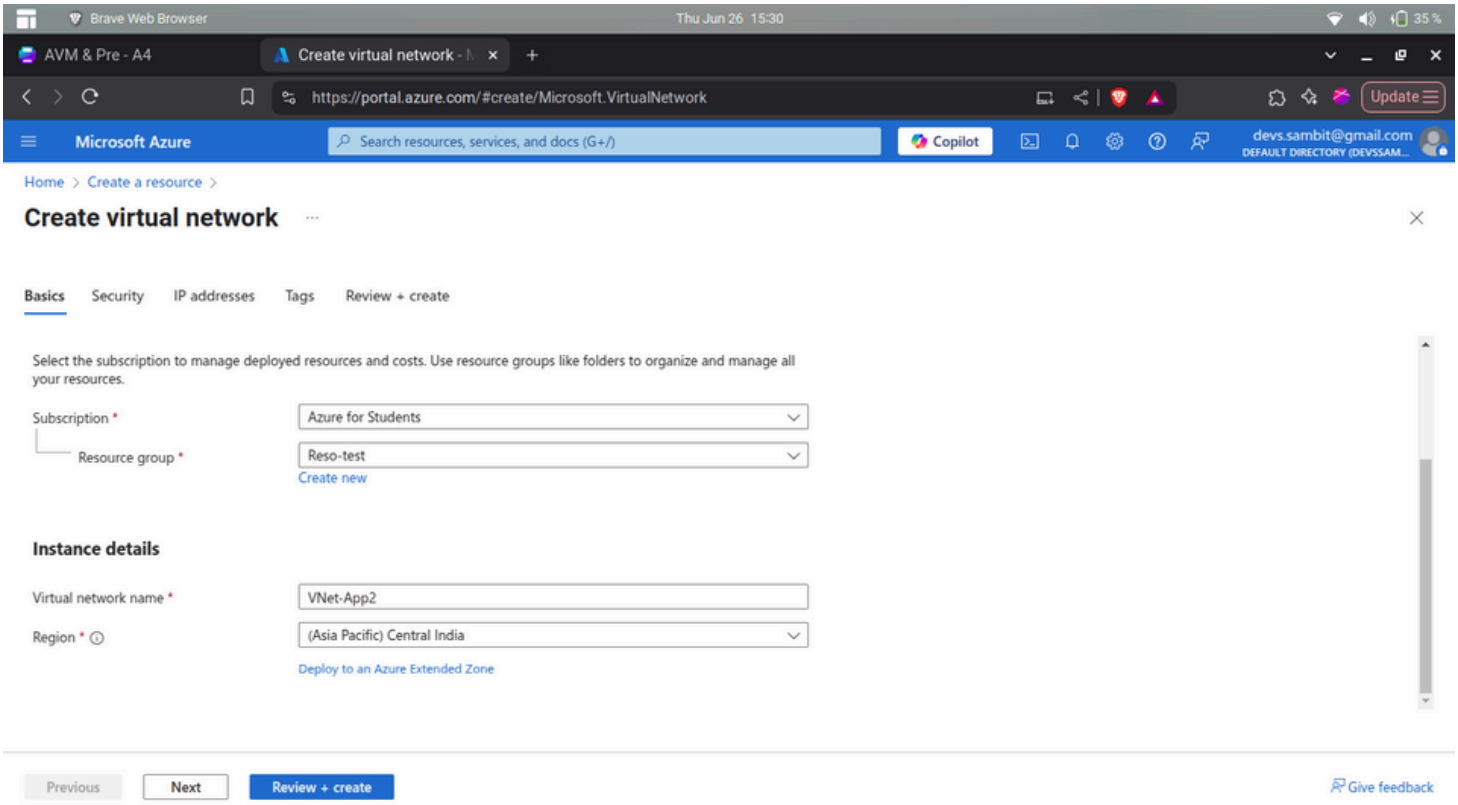
Step 3: Create the Second Virtual Network (VNet2) and its Subnets

Now, let's create VNet-App2 with Subnet-Linux and Subnet-Analytics.

Repeat Steps 1.2 to 1.3: Go back to Virtual networks and click + Create.

- Basics Tab:

1. Subscription: Your student subscription.
2. Resource Group: Select RG-AzureNetworkingLab.
3. Virtual network name: Enter VNet-App2.
4. Region: Select the same region you used for VNet-App1.



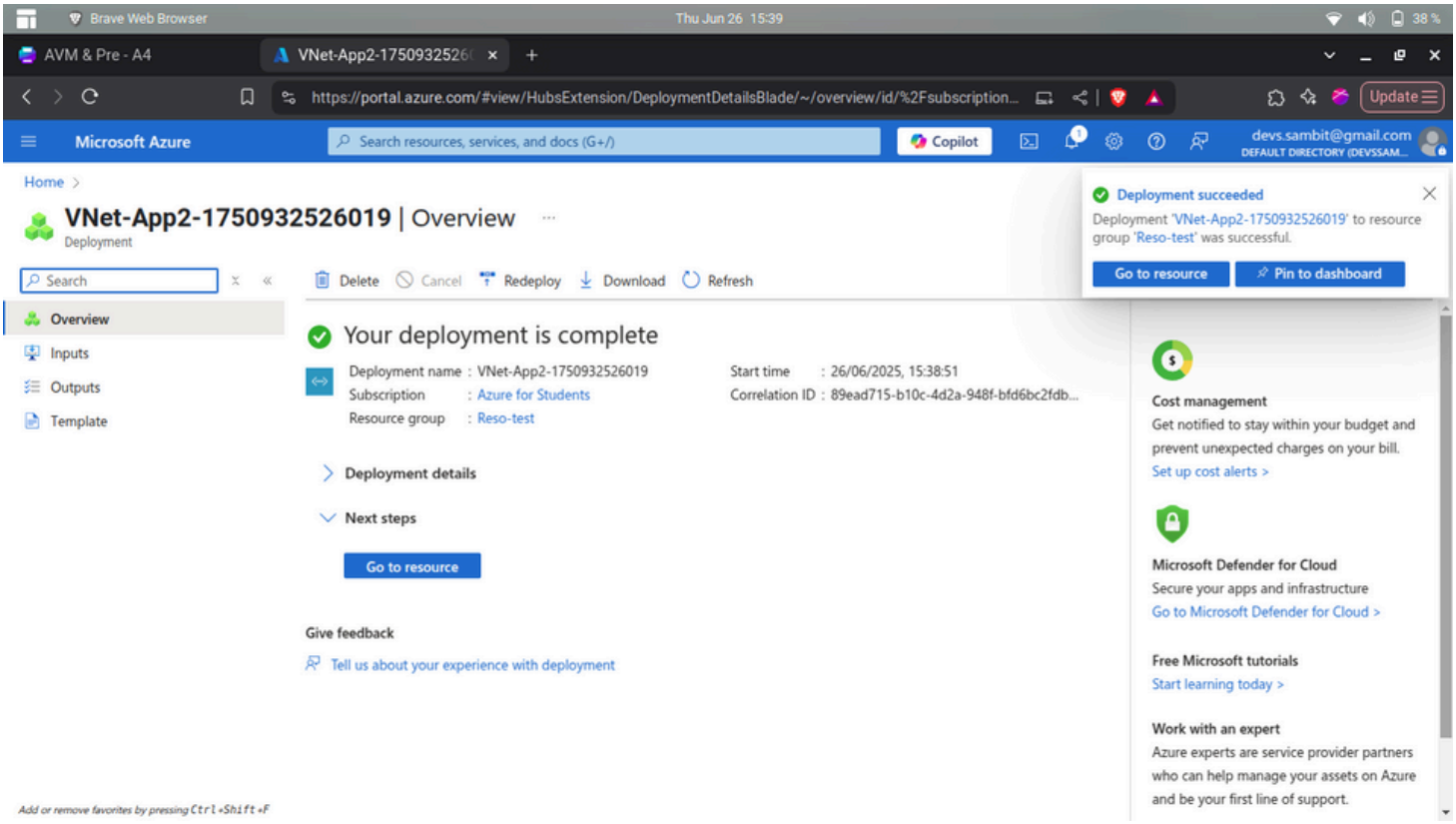
BASICS TAB OF VNET 2

- **IP Addresses Tab:**

IPv4 address space: Enter 10.2.0.0/16. Crucially, this must NOT overlap with 10.1.0.0/16 from VNet-App1.

- **Subnets**:

1. Click on the default subnet row.
2. Name: Change it to Subnet-Linux.
3. Address range (CIDR block): Change it to 10.2.1.0/24.
4. Click Save.
5. Click + Add subnet.
6. Name: Enter Subnet-Analytics.
7. Address range (CIDR block): Enter 10.2.2.0/24.
8. Click Add.
9. Click Review + create.



OVERVIEW PAGE OF VNET 2

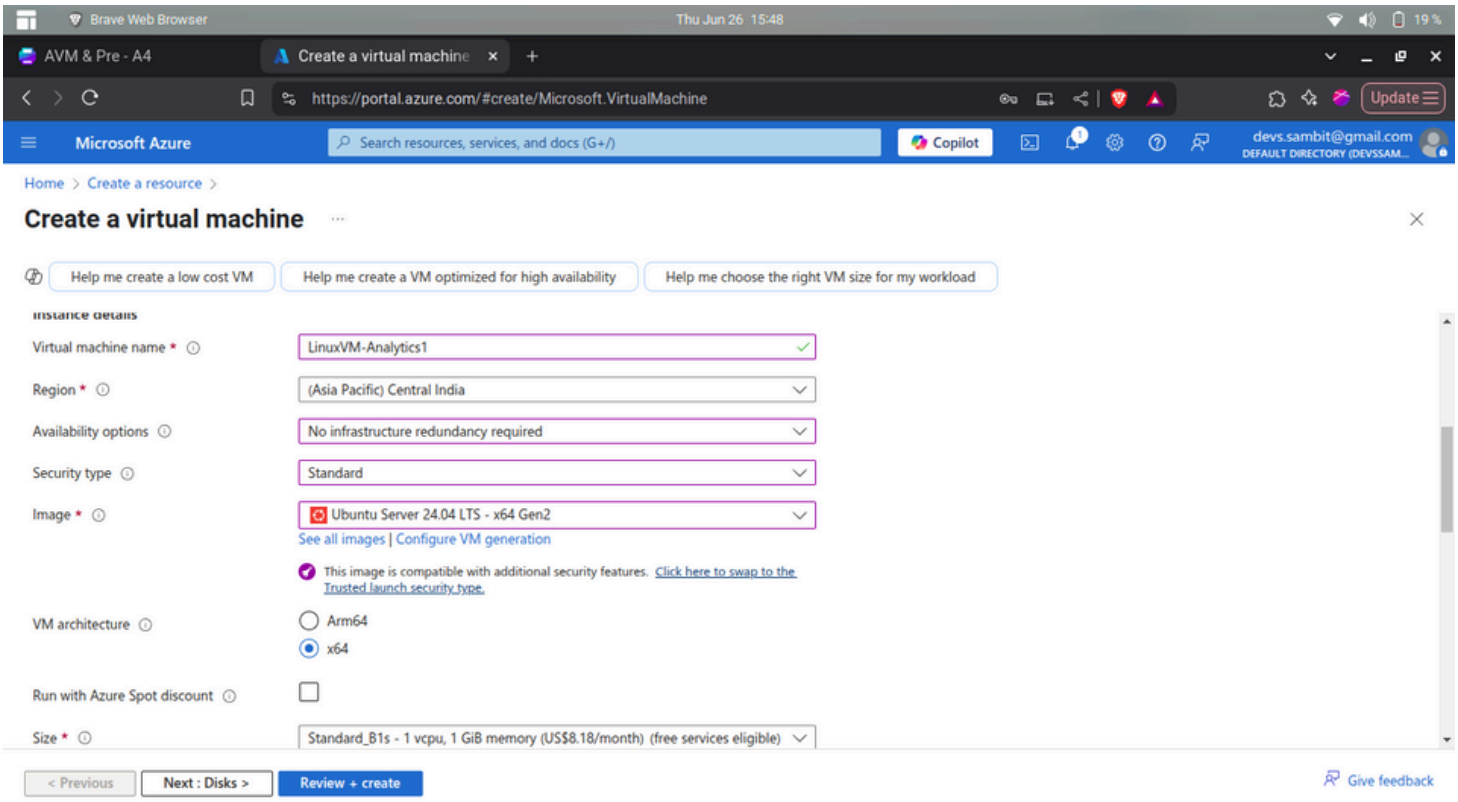
Step 4: Launch a Linux Virtual Machine (VM2) in Subnet-Linux

Create LinuxVM-Analytics1 in VNet-App2's Subnet-Linux.

Repeat Steps 2.1 to 2.2: Go back to Virtual machines and click + Create > Azure virtual machine.

- **Basics Tab:**

1. Virtual machine name: Enter LinuxVM-Analytics1.
2. Region: Select the same region as your VNets.
3. Image: Select Ubuntu Server 24.04 LTS - Gen2.
4. Size: Select B1s or B2s.



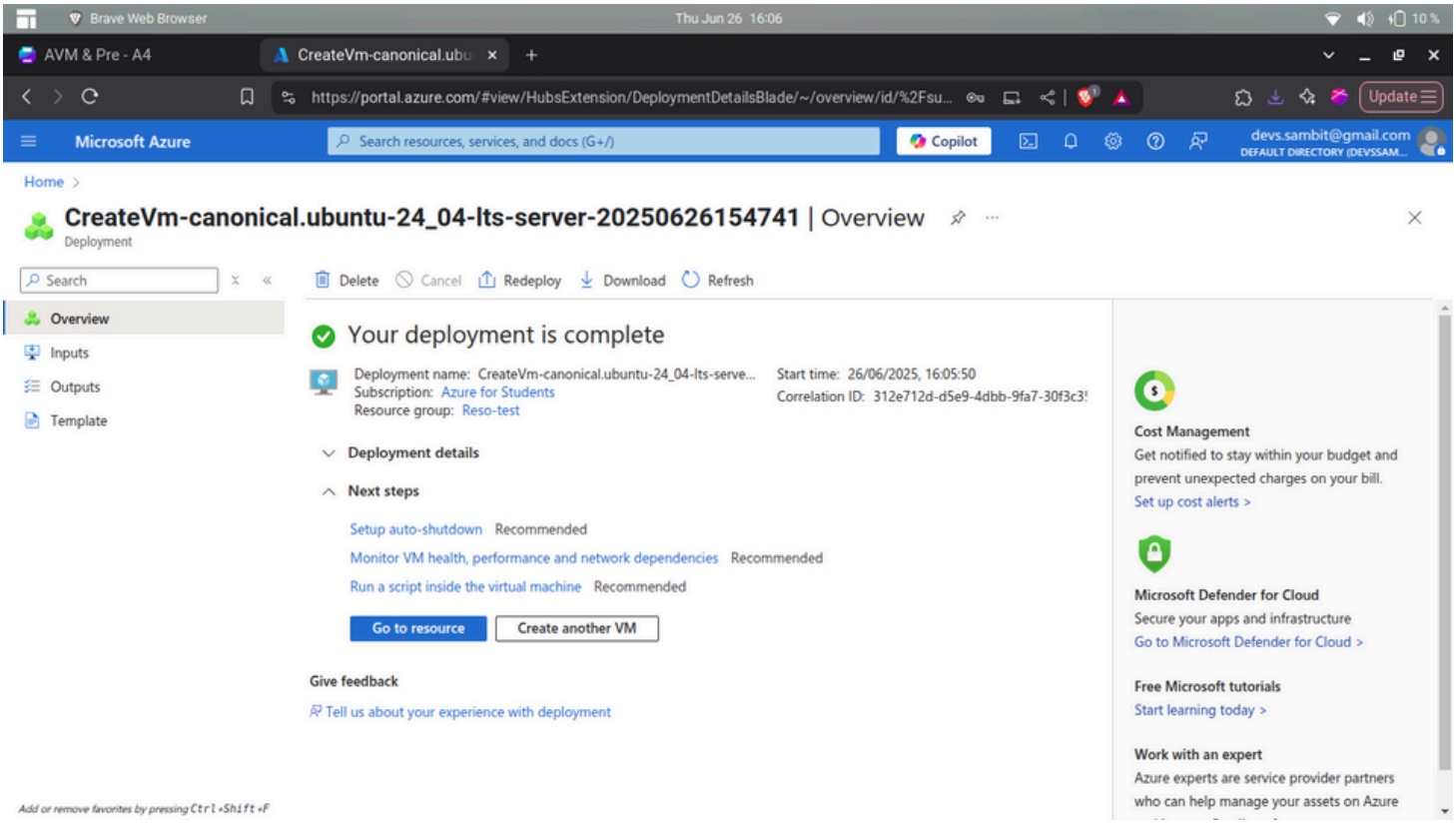
BASICS TAB OF LINUX VM

- **Administrator account:**

1. Authentication type: Choose SSH public key.
2. Username: Enter a username (e.g., azureuser).
3. SSH public key source: Select Generate new key pair.
4. Key pair name: Enter my-linux-ssh-key.
5. Important:Download private key and create resource. You'll need it to connect via SSH.

- **Networking Tab:**

1. Virtual network: Select VNet-App2. **2.362**
2. Subnet: Select Subnet-Linux (10.2.1.0/24).
3. Public IP: Leave as (new) LinuxVM-Analytics1-ip.
4. NIC network security group: Select Basic.
5. Click Review + create**.**



OVERVIEW PAGE OF LINUX VM

Step 5: Establish VNet Peering between VNet-App1 and VNet-App2

This will allow WinVM-Web1 and LinuxVM-Analytics1 to communicate directly using their private IPs.

Go to VNet-App1:

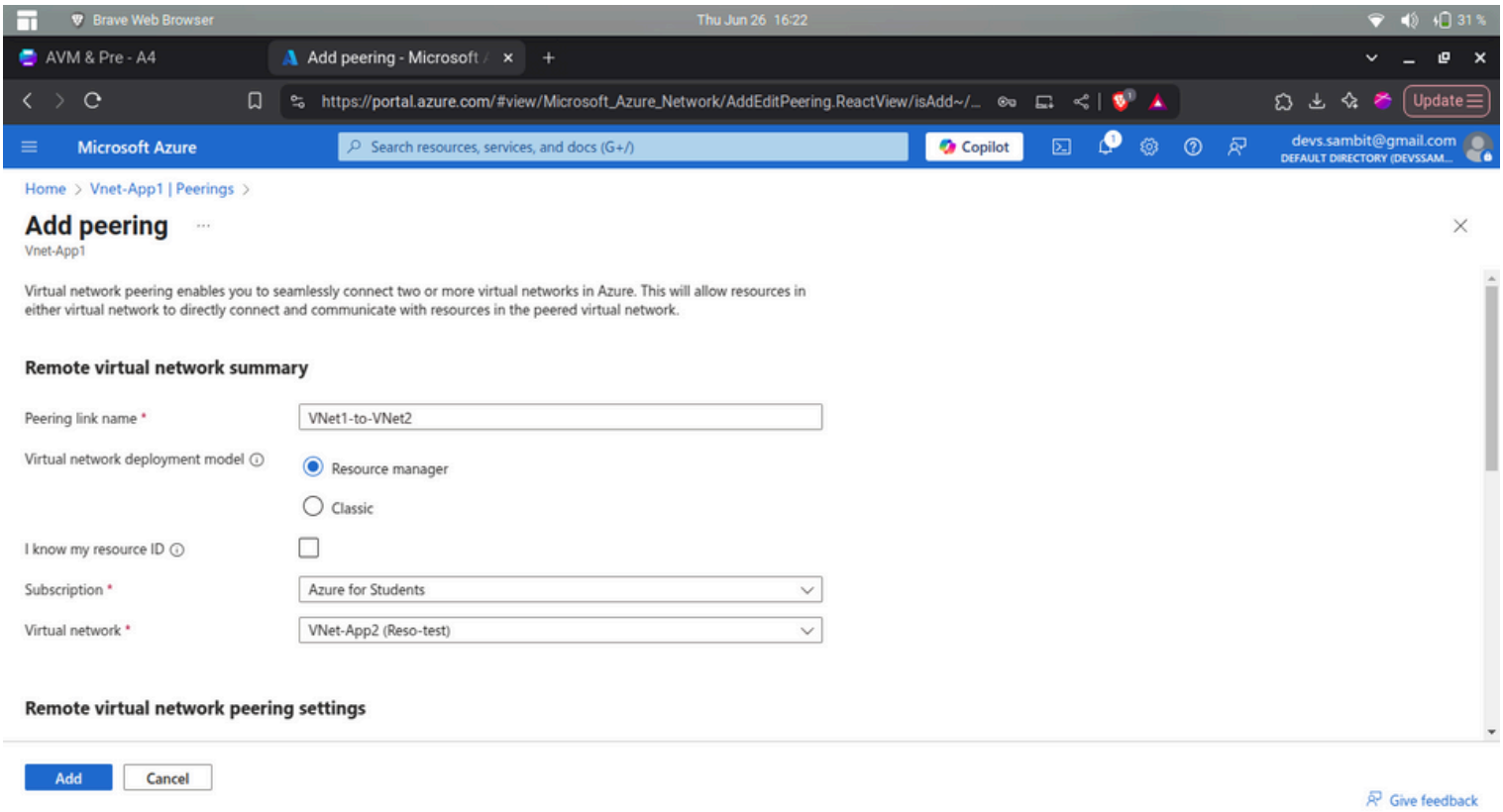
- In the Azure portal search bar, type VNet-App1 and select it from the results.
- In the left-hand menu, under Settings, click Peerings.

Add Peering:

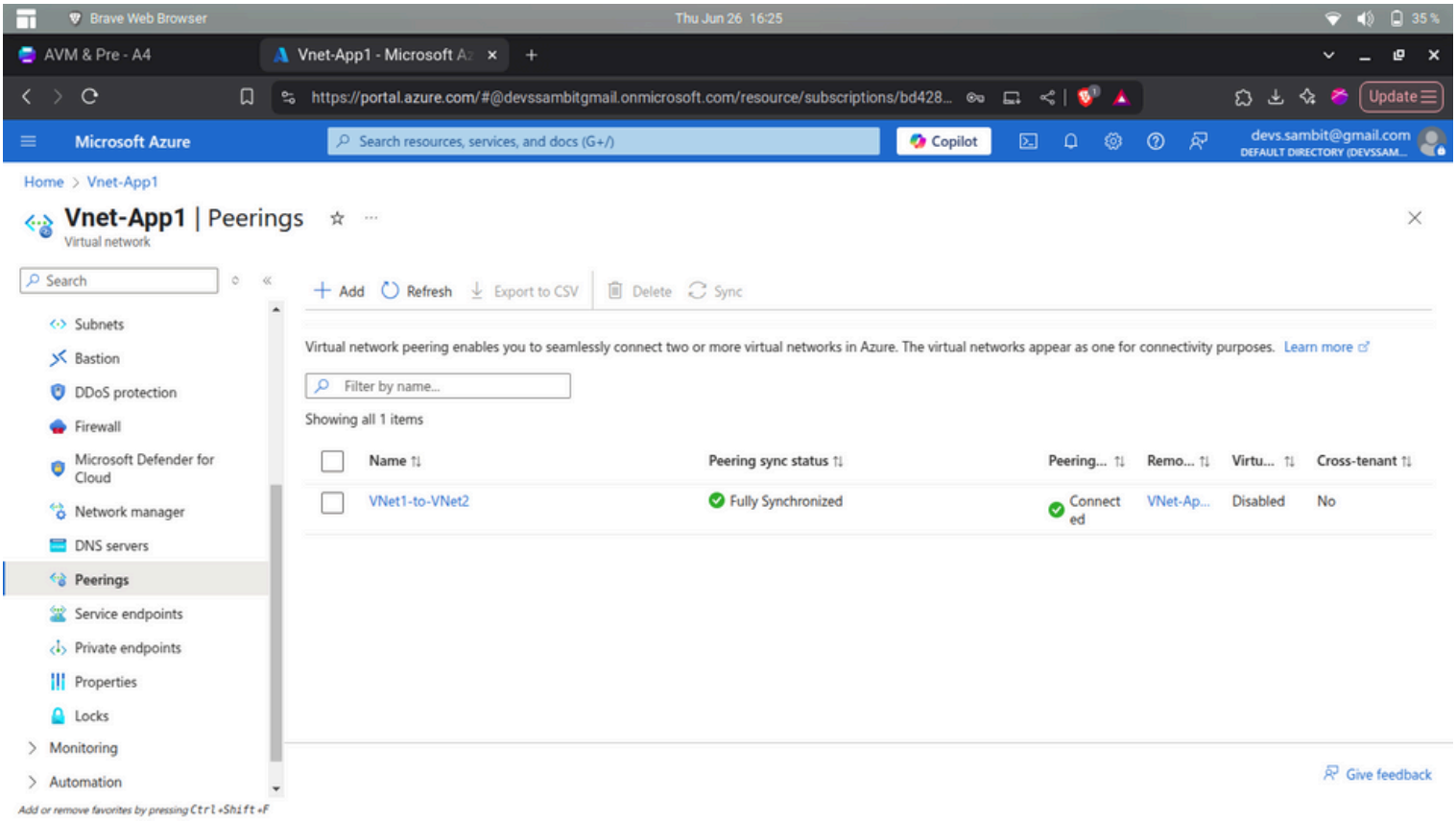
- Click + Add.
- This creates a two-way connection, so you define both sides here:

1. Local or Remote virtual network gateway: Leave defaults.
2. Peering link name from VNet-App1 to VNet-App2: Enter VNet1-to-VNet2.
3. Allow VNet-App1 to access VNet-App2: Ensure this is checked (default).
4. Allow VNet-App1 to receive forwarded traffic from VNet-App2: Check this.

- Remote virtual network:
    - Peering link name from VNet-App2 to VNet-App1: Enter VNet2-to-VNet1.
    - Subscription: Select your student subscription.
    - Virtual network: Select VNet-App2.
    - Allow VNet-App2 to access VNet-App1: Ensure this is checked (default).
    - Allow VNet-App2 to receive forwarded traffic from VNet-App1: Check this.
    - Enable VNet-App2 to use VNet-App1's remote gateway or route server: Leave unchecked for now.
- Click Add.



CONFIGURATION OF VNET PEERING



OVERVIEW PAGE OF VNET PEERING

Step 6: Test Connectivity (Ping between VMs)

IMP: There might be some variations in the whole step 6 as this version is specifically for systems running Linux OS.

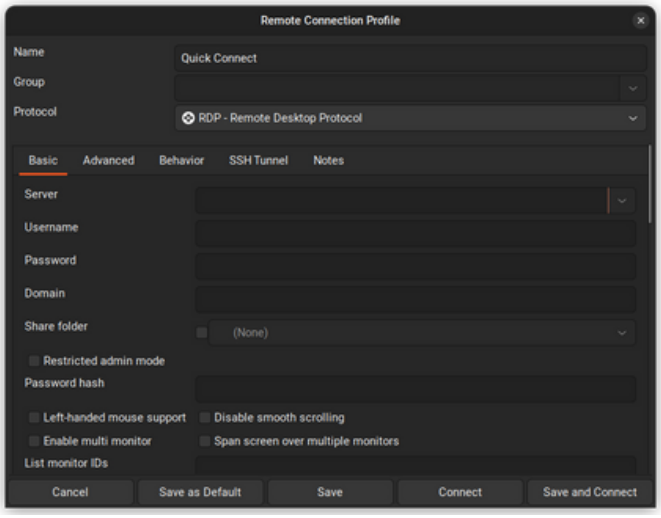
Now, let's verify if your VMs can ping each other. You'll need their private IP addresses.

To find VM Private IPs:

- Go to Virtual machines in the portal.
- Click on WinVM-Web1. On the Overview page, find its Private IP address. Note it down (e.g., 10.1.1.4).
- Go back to Virtual machines.
- Click on LinuxVM-Analytics1. On the Overview page, find its Private IP address. Note it down (e.g., 10.2.1.4).

6.a: Connect to Windows VM (WinVM-Web1) via RDP

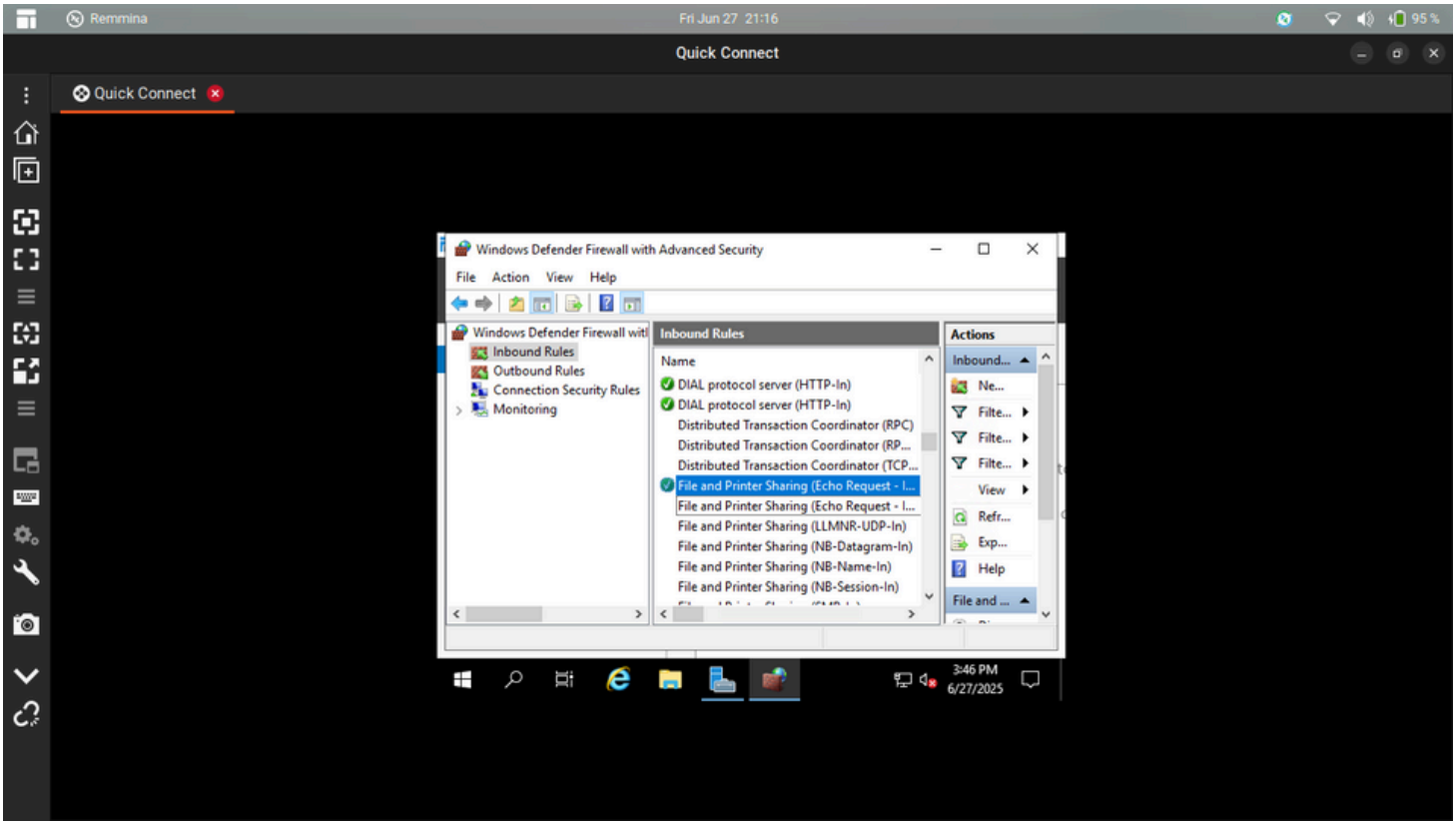
1. On WinVM-Web1's Overview page, copy its Public IP address.
2. Open Remote Desktop Connection on your local machine.
3. Paste the Public IP address and click Connect.
4. Enter the username and password you set during VM creation.
5. Accept any certificate warnings.



6.b: Prepare Windows VM for Ping (Inside WinVM-Web1)

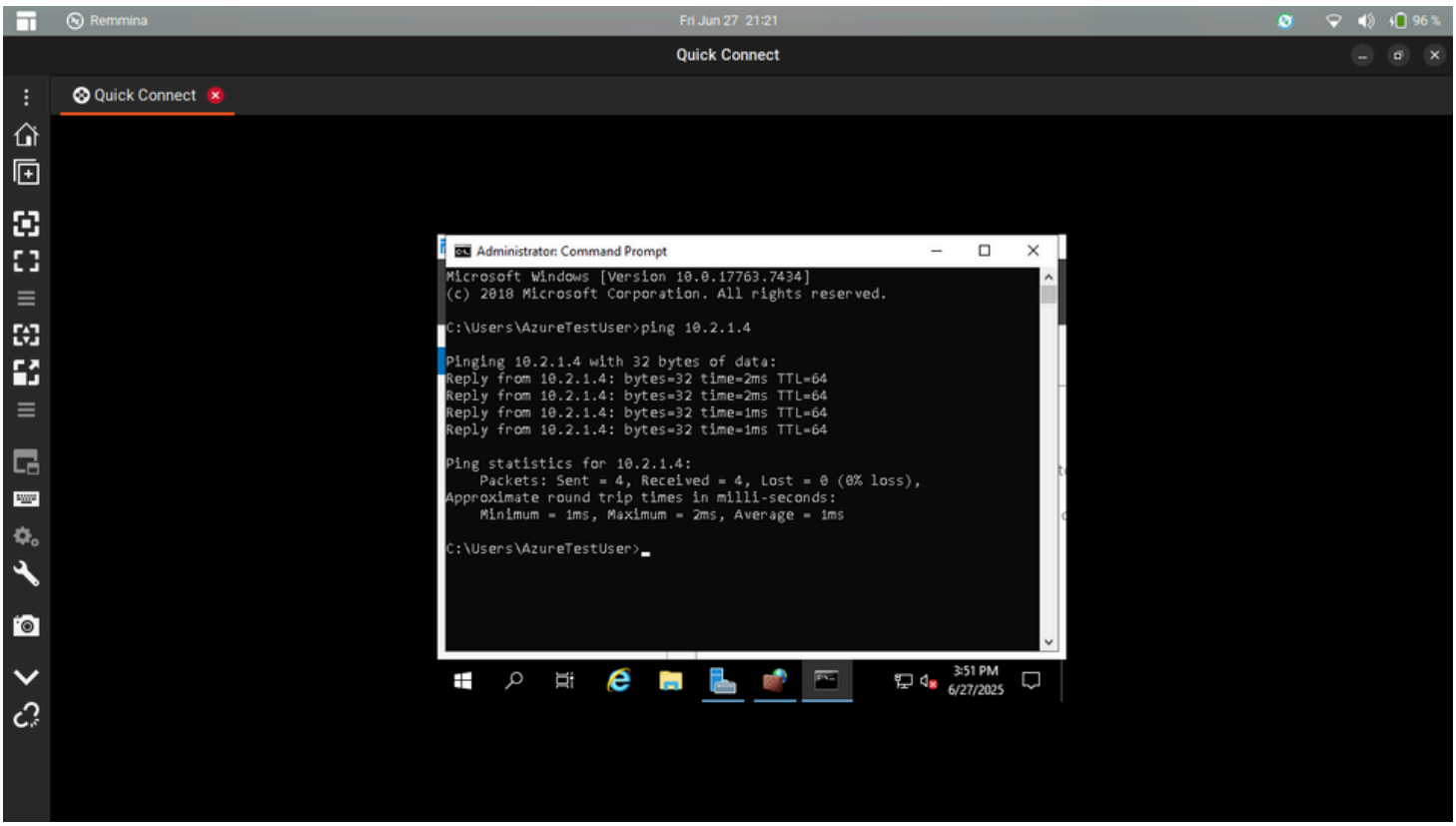
By default, Windows Firewall blocks incoming ICMP (ping) requests. You need to enable the rule for ping or temporarily disable the firewall from inside the Windows VM.

1. Once RDP'd into WinVM-Web1, open Server Manager.
2. Go to Tools > Windows Defender Firewall with Advanced Security.
3. In the left pane, select Inbound Rules.
4. Look for rules named "File and Printer Sharing (Echo Request - ICMPv4-In)". There might be several for different profiles (Domain, Private, Public).
5. Enable the rules that are disabled by right-clicking them and selecting "Enable Rule".



6.c: Ping Linux VM from Windows VM (Inside WinVM-Web1)

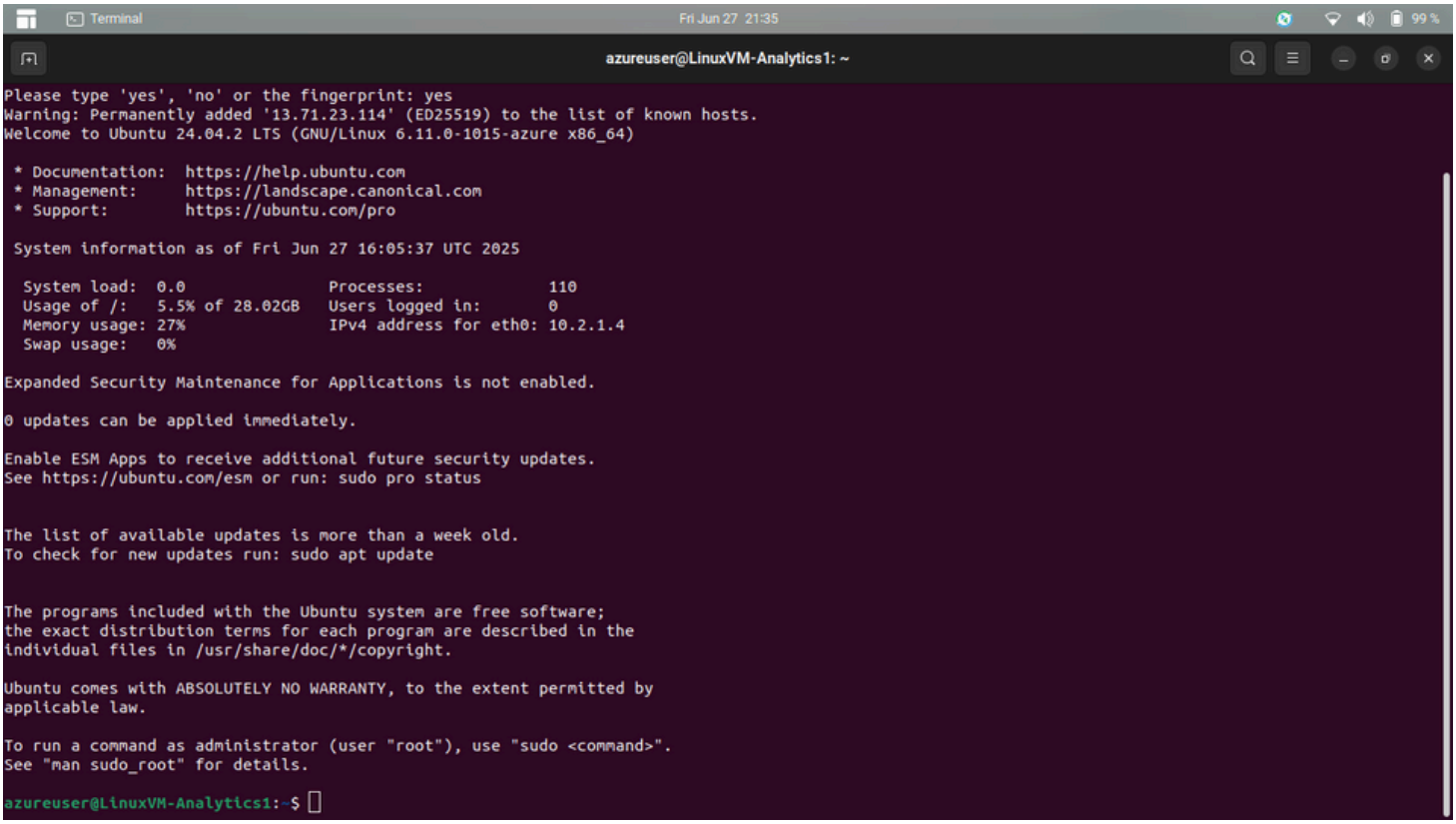
1. On WinVM-Web1, open Command Prompt or PowerShell.
2. Type ping <LinuxVM-Analytics1_Private_IP_Address> (e.g., ping 10.2.1.4).
3. You should see replies, indicating successful communication from Windows to Linux. If not, recheck peering status and firewall rules.



PING FROM WINDOWS TO LINUX

6.d: Connect to Linux VM (LinuxVM-Analytics1) via SSH from Ubuntu

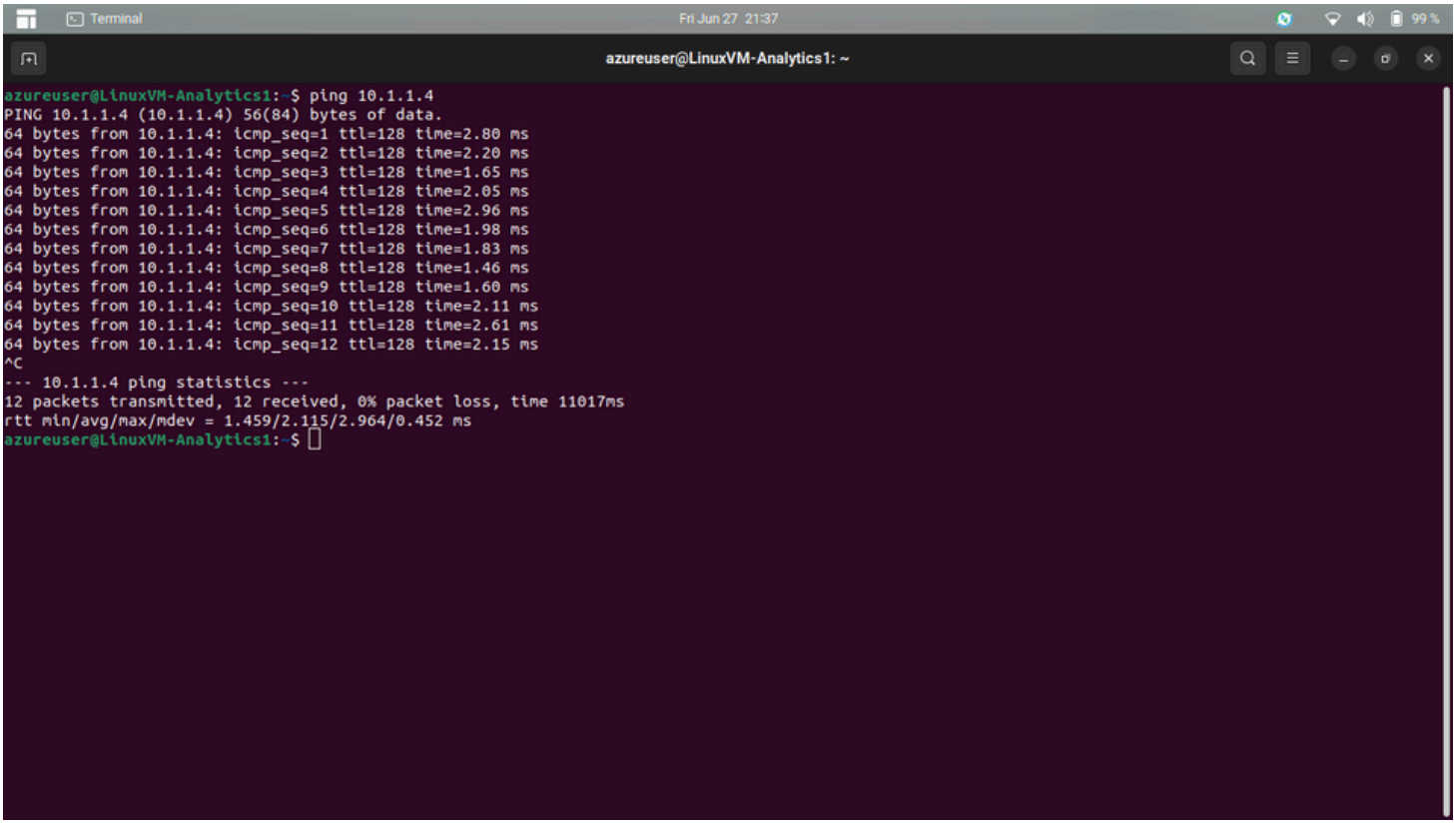
1. chmod 400 /path/to/your/my-linux-ssh-key.pem
2. ssh -i /path/to/your/my-linux-ssh-key.pem azureuser@<LinuxVM-Analytics1_Public_IP_Address>
3. The first time you connect, you might be asked to confirm the host's authenticity; type yes and press Enter.



LINUX LOGIN FROM TERMINAL

6.e: Ping Windows VM from Linux VM (Inside LinuxVM-Analytics1)

1. ping <WinVM-Web1_Private_IP_Address> (e.g., ping 10.1.1.4)
2. You should see replies, confirming bidirectional communication from Linux to Windows across the peered VNets. Press Ctrl+C to stop the ping.



PING FROM LINUX TO WINDOWS

Step 7: Clean Up Your Azure Resources (VERY IMPORTANT!)

To avoid consuming your credits unnecessarily, delete the resources when you are finished. The easiest way to do this is to delete the entire resource group.

1. Go to Resource Groups:
    - In the Azure portal search bar, type Resource groups and select it from the results.
2. Delete Your Lab Resource Group:
    - Find and click on RG-AzureNetworkingLab.
    - On the Resource Group's Overview page, click Delete resource group at the top.
    - You will be prompted to type the resource group name (RG-AzureNetworkingLab) to confirm deletion. Type it exactly as shown and click Delete.
    - This process can take several minutes as Azure deletes all resources within that group (VNets, VMs, Public IPs, etc.).

NOTE: If the resources are needed for further even after the performed task, deactivating each of them rather than deleting is a good choice.

But, it surely might keep on incurring small charges in the background due to some cost factors like disks, transfers over peerings, reserved IP addresses.

CONCLUSION

Throughout our discussion, we've explored the foundational elements of networking in Microsoft Azure:

- Azure Virtual Networks (VNets): Your isolated and secure private network in the cloud, defined by logical CIDR ranges that dictate its IP address space.
- Subnets: Smaller, segmented portions of a VNet's address space, crucial for organizing resources, applying granular security, and hosting specific Azure services.
- VNet Peering: A powerful mechanism to connect disparate VNets, allowing secure, high-bandwidth communication across the Microsoft backbone, whether within the same region (Regional Peering) or across different regions (Global Peering).

Submitted by:
Sambit Kumar Panda

References:

https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-subnet?tabs=azure-portal
https://learn.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview
https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal
https://www.google.com/search?q=https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-firewall-windows-server