

Deployment of Azure Infrastructure

1. **Create Resource Group and Virtual Network**

1.1 Create the Resource Group – Chaitra_RG_Assignment at EastUS region and create First VNET Chaitra-VNET-Core with CIDR 192.168.0.0/16 at EastUS region.

Create a resource group

BasicsTagsReview + create

[Automation Link](#)

Basics

Subscription	Azure for Students
Resource group name	Chaitra_RG_Assignment
Region	East US

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<div>Azure for Students</div>
Resource group *	<div>Chaitra_RG_Assignment</div> Create new

Instance details

Virtual network name *	<div>Chaitra-VNET-Core</div>
Region * ⓘ	<div>(US) East US</div> Deploy to an Azure Extended Zone

Click on Next to Assign CIDR with 192.168.0.0/16 and create two subnets as:

- WebTier subnet: 192.168.10.0/24
- MgmtSubnet subnet: 192.168.20.0/24

192.168.0.0/16 [Delete address space](#)

192.168.0.0 /16
192.168.0.0 - 192.168.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
WebTier	192.168.10.0 - 192.168.10.255	/24 (256 addresses)	-
MgmtSubnet	192.168.20.0 - 192.168.20.255	/24 (256 addresses)	-

Click Next to review and create

Basics	Security	IP addresses	Tags	Review + create
Subscription		Azure for Students		
Resource Group		Chaitra_RG_Assignment		
Name		Chaitra-VNET-Core		
Region		East US		
Security				
Azure Bastion		Disabled		
Azure Firewall		Disabled		
Azure DDoS Network Protection		Disabled		
IP addresses				
Address space		192.168.0.0/16 (65,536 addresses)		
Subnet		WebTier (192.168.10.0/24) (256 addresses)		
Subnet		MgmtSubnet (192.168.20.0/24) (256 addresses)		

1.2 Create the Second VNET in the Name of Chaitra-VNET-Services with CIDR 10.10.0.0/16

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Resource group * [Create new](#)

Instance details

Virtual network name *

Region * [Deploy to an Azure Extended Zone](#)

Click on Next to Assign CIDR with 10.10.0.0/16 and DataSubnet subnet: 10.10.1.0/24

10.10.0.0/16 [Delete address space](#)

10.10.0.0 /16
10.10.0.0 - 10.10.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
DataSubnet	10.10.1.0 - 10.10.1.255	/24 (256 addresses)	-

Click Next to review and create

Basics

Subscription	Azure for Students
Resource Group	Chaitra_RG_Assignment
Name	Chaitra-VNET-Services
Region	East US

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.10.0.0/16 (65,536 addresses)
Subnet	DataSubnet (10.10.1.0/24) (256 addresses)

Once the Deployment of both VNET is done, go under the VNets to check Subnets and confirm.

Chaitra-VNET-Core | Subnets

Virtual network

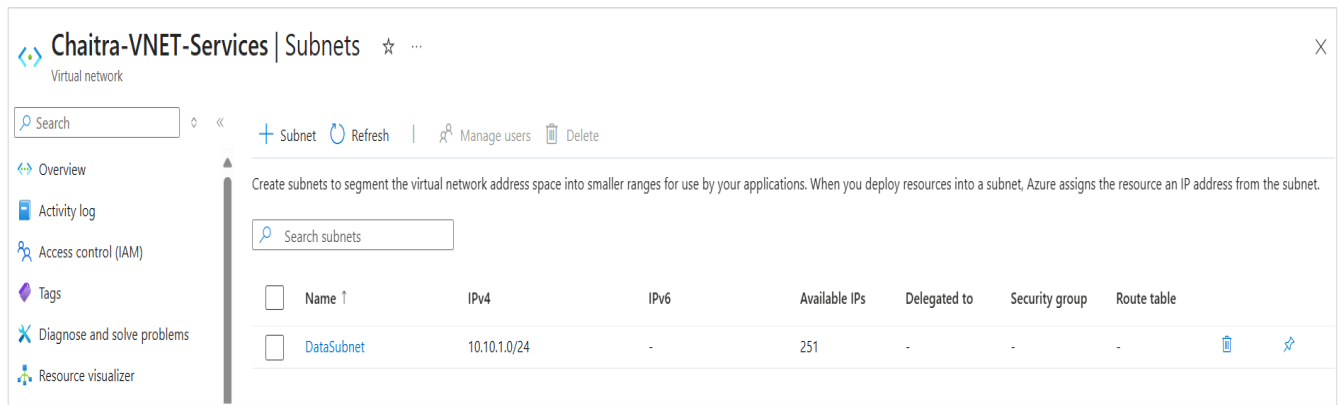
Search

+ Subnet Refresh Manage users Delete

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Search subnets

	Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
<input type="checkbox"/>	WebTier	192.168.10.0/24	-	251	-	-	-
<input type="checkbox"/>	MgmtSubnet	192.168.20.0/24	-	251	-	-	-



2 VNet Peering

To Establish bidirectional peering between the two VNets.

- We need to select any one Vnet that is created.
- Then select Peering option from the service menu.
- Click on Add to Peer a Vnet
- Here peering name is given as "VNETCore-VNETServices"

VNETCore-VNETService

Chaitra-VNET-Core

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

Remote virtual network summary

Remote Vnet Id	/subscriptions/7a368cae-b6fe-4543-8fec-7358b1643da7/resourceGroups/C...
IP address space	10.10.0.0/16

Local virtual network summary

Peering link name *	VNETCore-VNETService
Peering state	✓ Connected

3 Creating VMs

- Create “Chaitra-MgmtVM” in MgmtSubnet:
- Selected Windows Server 2022,
- RDP access only from current public IP

Create a virtual machine ...

[Help me create a low cost VM](#) [Help me create a VM optimized for high availability](#) [Help me choose the right VM size for my workload](#)

your resources.

Subscription * ⓘ

Resource group * ⓘ
[Create new](#)

Instance details

Virtual machine name * ⓘ ✓

Region * ⓘ

Availability options ⓘ

Security type ⓘ
[Configure security features](#)

Image * ⓘ
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ
☐ Arm64
☒ x64
Arm64 is not supported with the selected image.

- Click next for selecting mgmt-subnet and new public ip.

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ
[Create new](#)

Subnet * ⓘ
[Manage subnet configuration](#)

Public IP ⓘ
[Create new](#)

NIC network security group ⓘ
☐ None
☒ Basic
☐ Advanced

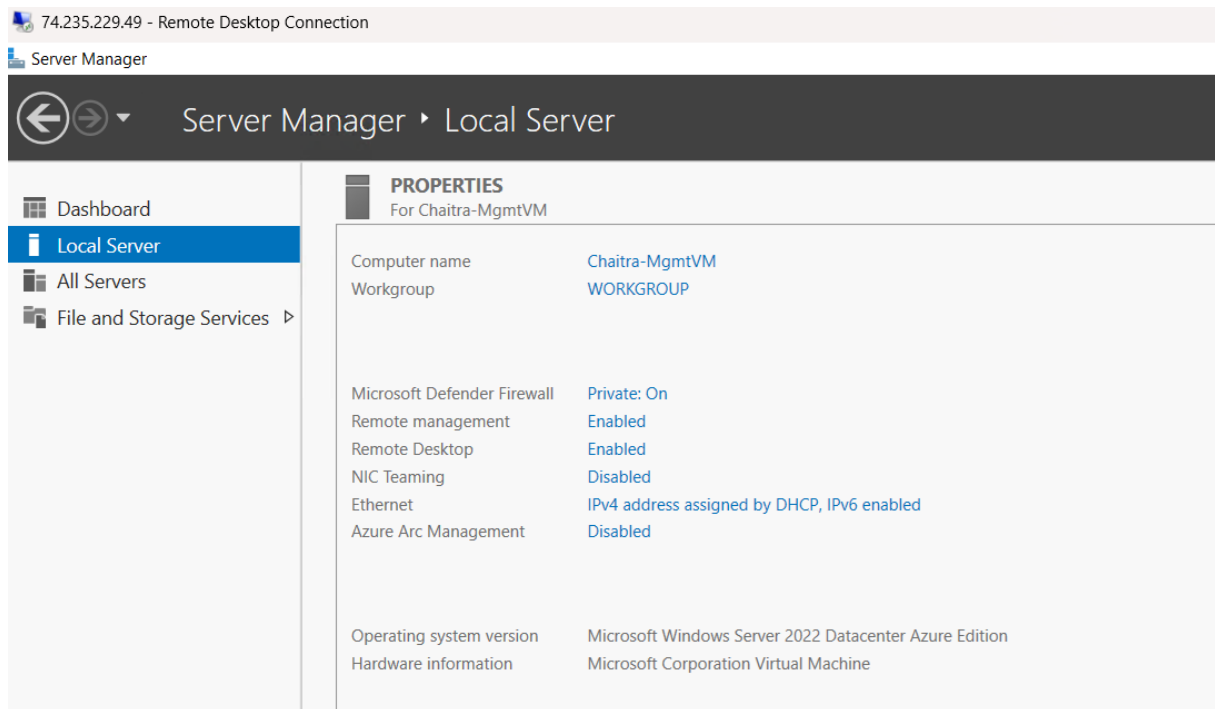
Public inbound ports * ⓘ
☐ None
☒ Allow selected ports

Select inbound ports *

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

- Review and create.

Access the VM using Public ip via RDP



Create second VM Ubuntu with NGINX, No ssh and allow Http and https

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ Chaitra-VNET-Core ▼
[Create new](#)

Subnet * ⓘ WebTier (192.168.10.0/24) ▼
[Manage subnet configuration](#)

Public IP ⓘ (new) Chaitra-WebVM-ip ▼
[Create new](#)

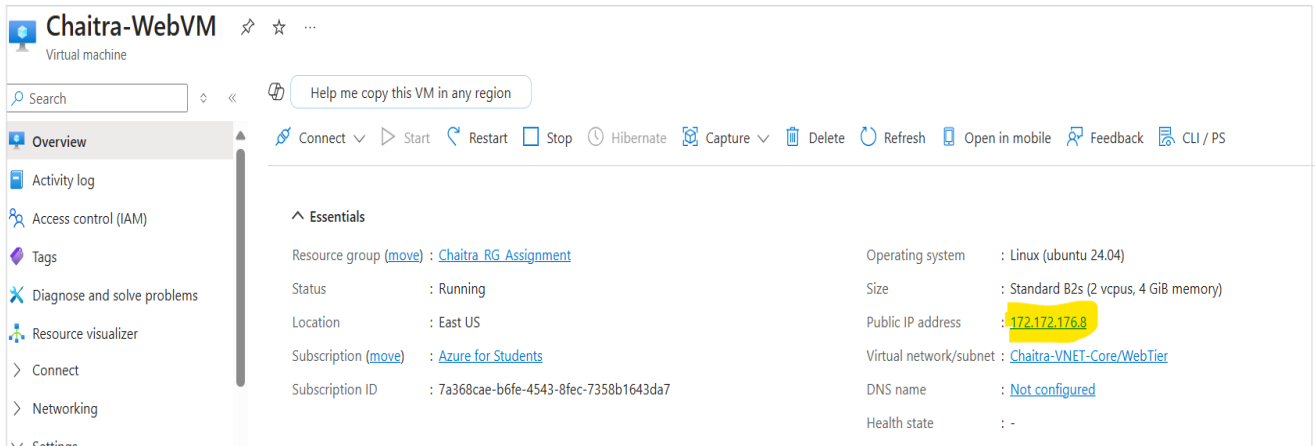
NIC network security group ⓘ ☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ ☐ None ☒ Allow selected ports

- Click next to select webtier subnet and create public ip
- Click on advanced tab to add Custom script data and review and create.
- Below is the script

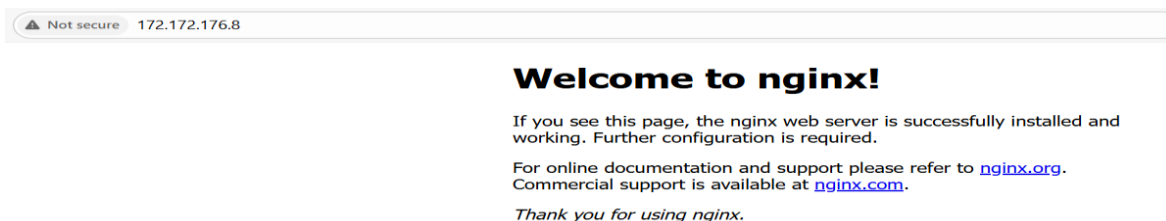
```
#!/bin/bash
# Update package list
sudo apt update
# Install nginx
sudo apt install nginx -y
# Start nginx
sudo systemctl start nginx
```

After the deployment of Ubuntu vm, note the public ip of the VM to access the nginx default website via browser. (172.172.176.8)



Go to NSG “chaitra-webvm-nsg” and add inbound security rules -> add ->allow http(80) and https(443)

Lets access the nginx default website from a browser via public ip. <172.172.176.8>



Create third VM(Ubuntu), without public ip

- In the networking tab, disable public ip and select the Vnet as Chaitra-VNET-Services and the subnet DataSubnet

Create a virtual machine ...

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my workload

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * [Create new](#)

Subnet * [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group ☐ None ☒ Basic ☐ Advanced

- Review and create.

4 Creating NSG

Go to NSG settings of mgmtvm ->click inbound security rules ->add

Select source ip and enter public ip, select destination port as 3389(RDP) and ADD.

Chaitra-MgmtVM-nsg Network security group

Search Move Delete Refresh Give feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
- Monitoring
- Automation
- Help

Essentials

Resource group (move) : [Chaitra_RG_Assignment](#) Custom security rules : 1 inbound, 0 outbound

Location : East US Associated with : 0 subnets, 1 network interfaces

Subscription (move) : [Azure for Students](#)

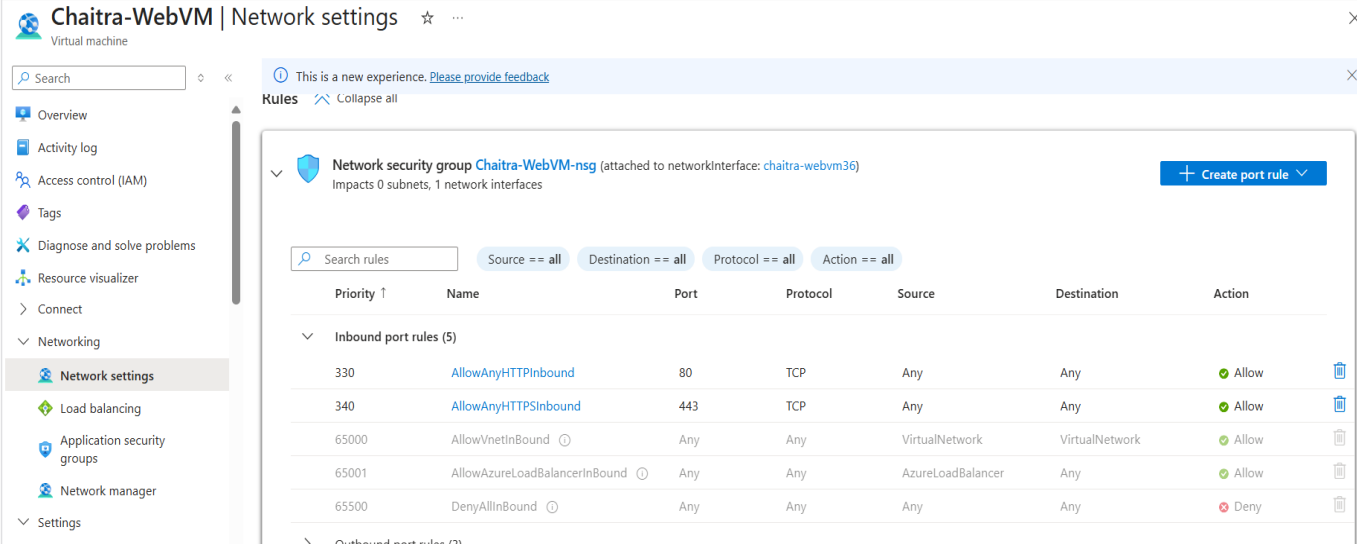
Subscription ID : 7a368cae-b6fe-4543-8fec-7358b1643da7

Tags (edit) : [Add tags](#)

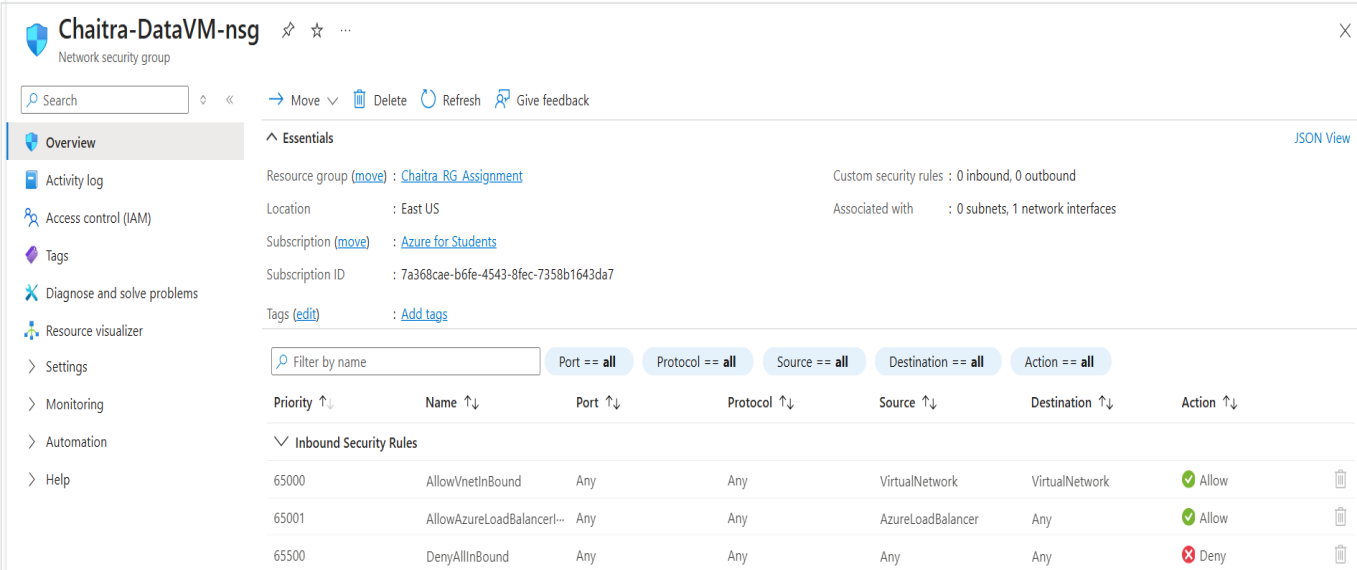
Filter by name Port == all Protocol == all Source == all Destination == all Action == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
310	AllowCidrBlockRDPInbou...	3389	TCP	74.235.229.49	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancer...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Go to Ubuntu(nginx) NSG settings and allow only http and https

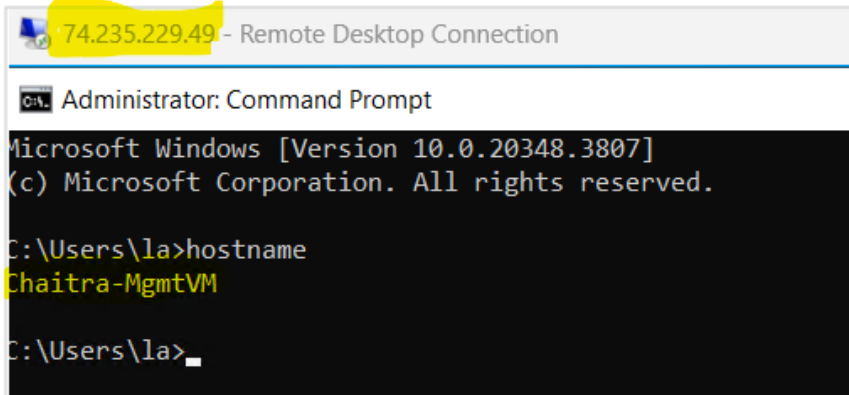


Data VM NSG settings



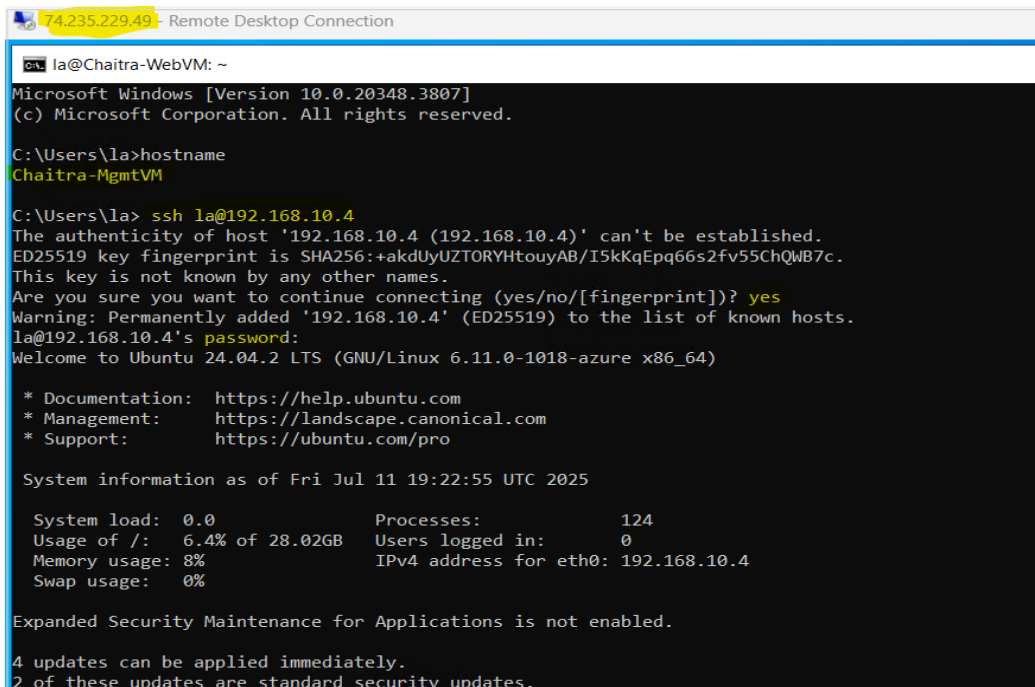
FINAL OUTPUT

- Accessing Chaitra-MgmtVM via RDP by using public ip
- Enter Username and Password to login, login successful




A screenshot of a Remote Desktop Connection window titled "74.235.229.49 - Remote Desktop Connection". The window shows a Windows Command Prompt with the title "Administrator: Command Prompt". The text in the prompt reads: "Microsoft Windows [Version 10.0.20348.3807] (c) Microsoft Corporation. All rights reserved. C:\Users\la>hostname Chaitra-MgmtVM C:\Users\la>".

- SSH access to Chaitra-WebVM is performed internally from Chaitra-MgmtVM using the VM's private IP address (192.168.10.4). This confirms that internal connectivity is functioning correctly, while public SSH access remains restricted as per the configured NSG rules.
- Open Powershell in MgmtVM RDP and Type the command `ssh la@192.168.10.4`, enter the password and login



A screenshot of a Remote Desktop Connection window titled "74.235.229.49 - Remote Desktop Connection". The window shows a Windows Command Prompt with the title "la@Chaitra-WebVM: ~". The text in the prompt reads: "Microsoft Windows [Version 10.0.20348.3807] (c) Microsoft Corporation. All rights reserved. C:\Users\la>hostname Chaitra-MgmtVM C:\Users\la> ssh la@192.168.10.4 The authenticity of host '192.168.10.4 (192.168.10.4)' can't be established. ED25519 key fingerprint is SHA256:+akdUyUZTORYHtousyAB/I5kKqEpq66s2fv55ChQWB7c. This key is not known by any other names. Are you sure you want to continue connecting (yes/no/[fingerprint])? yes Warning: Permanently added '192.168.10.4' (ED25519) to the list of known hosts. la@192.168.10.4's password: Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1018-azure x86_64) * Documentation: https://help.ubuntu.com * Management: https://landscape.canonical.com * Support: https://ubuntu.com/pro System information as of Fri Jul 11 19:22:55 UTC 2025 System load: 0.0 Processes: 124 Usage of /: 6.4% of 28.02GB Users logged in: 0 Memory usage: 8% IPv4 address for eth0: 192.168.10.4 Swap usage: 0% Expanded Security Maintenance for Applications is not enabled. 4 updates can be applied immediately. 2 of these updates are standard security updates."

- SSH access to Chaitra-DataVM is performed internally from Chaitra-WebVM using the VM's private IP address (192.168.10.4). This confirms that internal connectivity is functioning correctly via NSG rules.
- Enter the Username and Password for the VM and login

 la@Chaitra-DataVM: ~

See "man sudo_root" for details.

la@Chaitra-WebVM:~\$ ssh la@10.10.1.4

The authenticity of host '10.10.1.4 (10.10.1.4)' can't be established.

ED25519 key fingerprint is SHA256:CkDQMLWiKYhn/jXzm0jAwqkK9BFvjp+vnBo17Uom7yM.

This key is not known by any other names.

Are you sure you want to continue connecting (yes/no/[fingerprint])? yes

Warning: Permanently added '10.10.1.4' (ED25519) to the list of known hosts.

la@10.10.1.4's password:

Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.11.0-1018-azure x86_64)

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro
```

- Accessed DataVM via private ip through SSH from the WebVM.

SSH access to **Chaitra-WebVM** was successfully tested from **Chaitra-MgmtVM** using its **private IP address**, confirming internal network connectivity. Since SSH access is **blocked via public IP** as per the NSG rules, this validates that access is only permitted through the internal VNet.

Additionally, connectivity from **Chaitra-WebVM** to **Chaitra-DataVM** using its **private IP** was successful, confirming that the Data VM is securely isolated from public networks and accessible only through internal tiers.