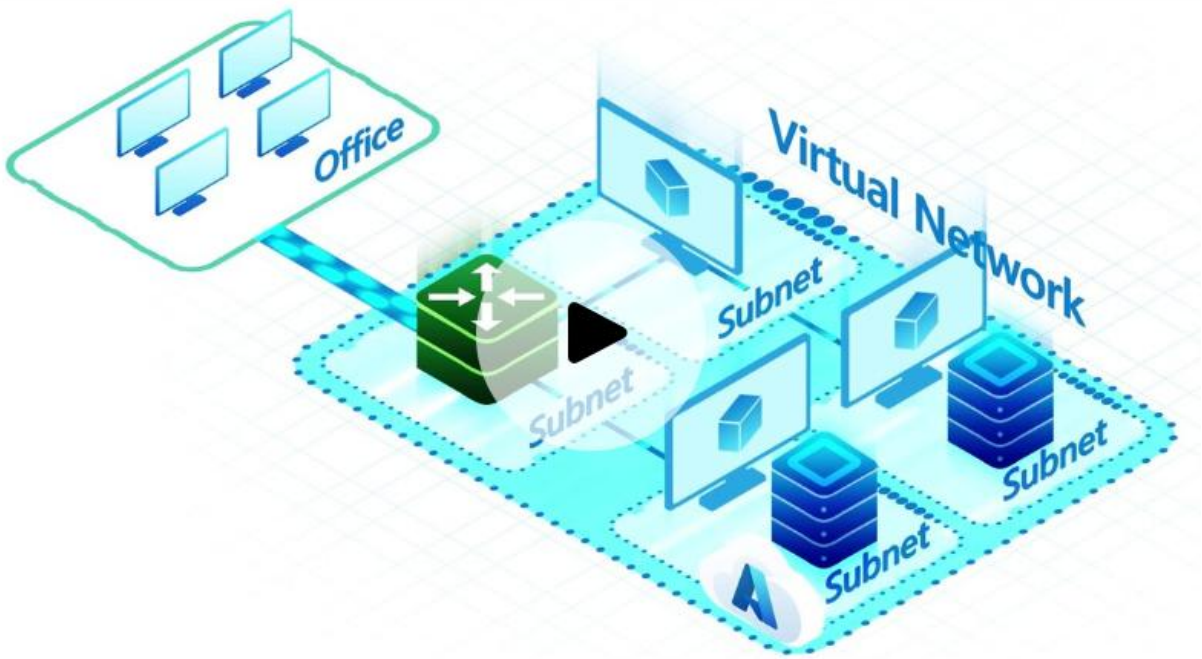
1. Objective:

- ✓ Prepare a R&D document on the working of NSG & ASG, allowing specific IPs to access VMs and Deny Internet using NSG, Public IPs and Types, Static and Dynamic IP, Service tags, Allocate Static IPs to all VM's, creating a Network Security Group, Creating Public IP, Associating/De-associating Public IP with virtual machine, Creation of Network Interface

2. Introduction

Microsoft Azure, or just **Azure** is the cloud computing platform developed by Microsoft.
It has management, access and development of applications and services to individuals, companies, and governments through its global infrastructure.

Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure. An instance of the service (a virtual network) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. These Azure resources include virtual machines (VMs).



A virtual machine is like a physical computer, but it is a digital version of it. Actually, it is not so much different from physical computers because they have also memory, CPU, as well as they have disks to store our data or various files and one more interesting thing is that they can also connect to the internet.

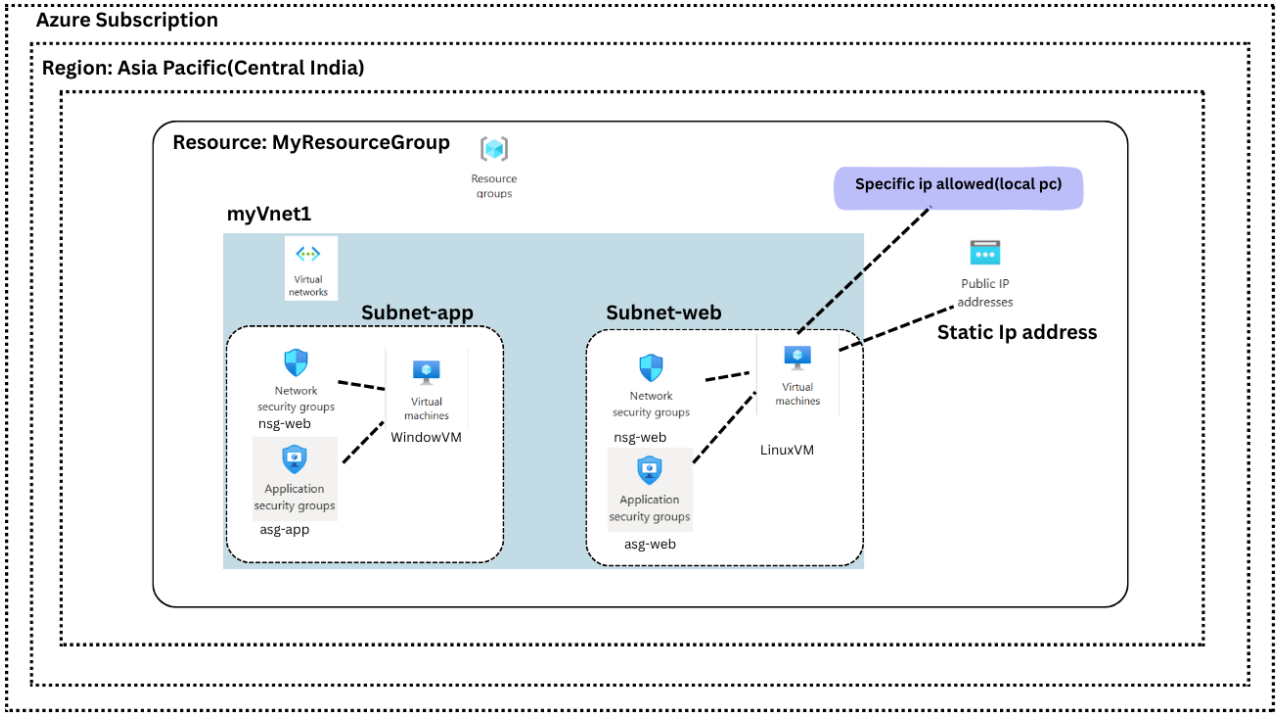
You can create a virtual network in the cloud dedicated to your Azure account. It is the fundamental building block where you can launch Azure resources.
Azure VNet is the networking layer of Azure VMs.
A VNet spans all the Availability Zones in the region. After creating a VNet, you can add one or more subnets in each Availability Zone.

A **virtual network** (VNet) allows you to specify an IP address range for the VNet, add subnets, associate network security groups, and configure route tables.

A **subnet** is a range of IP addresses in your VNet. You can launch Azure resources into a specified subnet. Use a **public subnet** for resources that need to connect to the Internet and a **private subnet** for resources that won't be connected to the Internet.

To protect the Azure resources in each subnet, use **network security groups**.

3. Architecture



Points to Note:

1. Azure subscription: Azure for Students

2. Azure Region selected: Asia Pacific (Central India)

3. myVnet hosts a Windows VM (WindowVM) in Subnet-app.

- 4. myVnet hosts a Linux VM (LinuxVM) in Subnet-web.

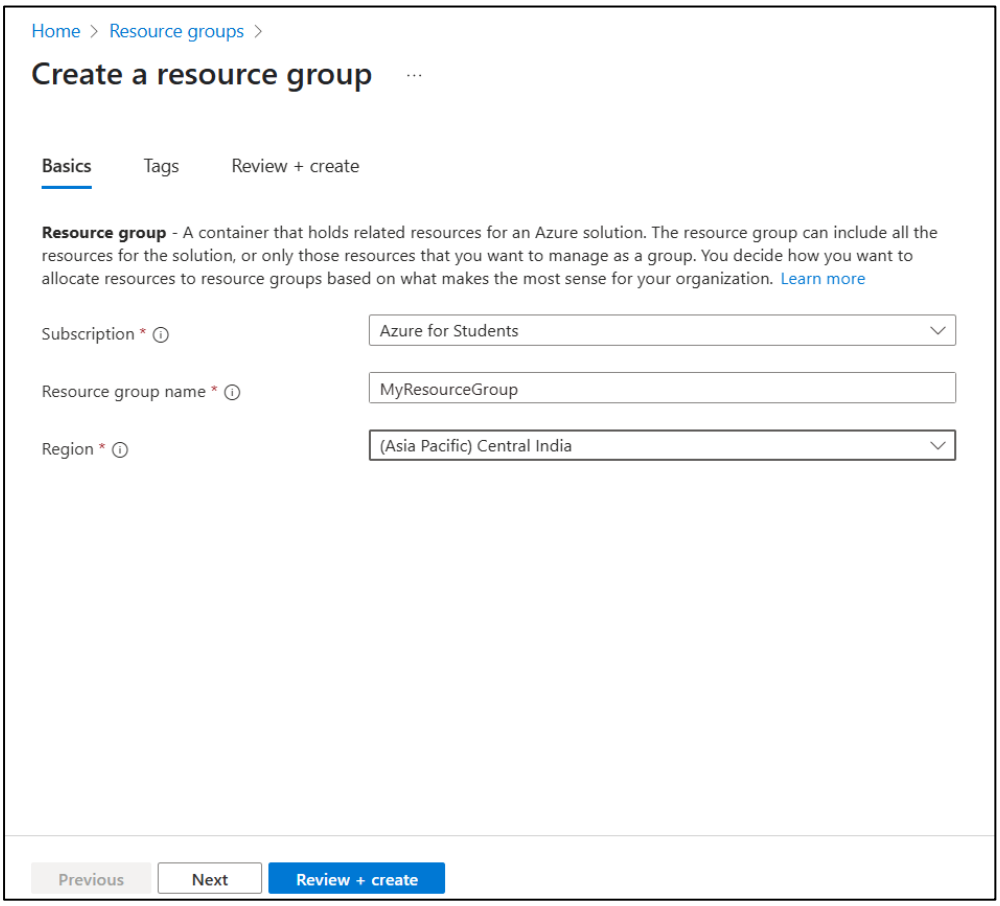
5. Network Security Groups (NSGs) with specific ip, static ip allowed , internet access denied.

6. asg-app and asg-web attached to vms respectively.

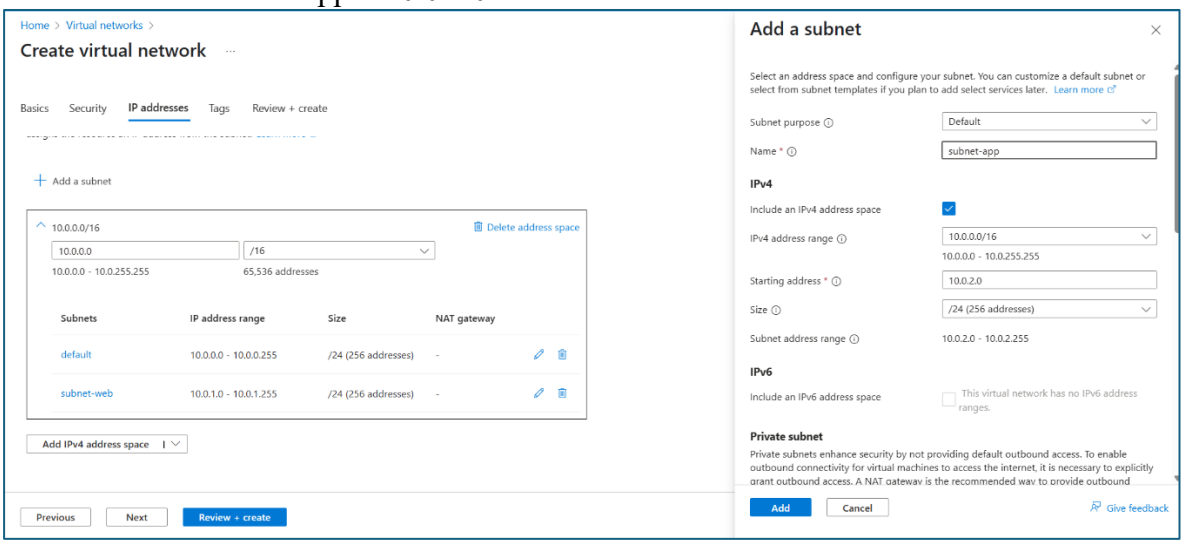
4. Deployment and Configuration

i. Login to Azure Account.

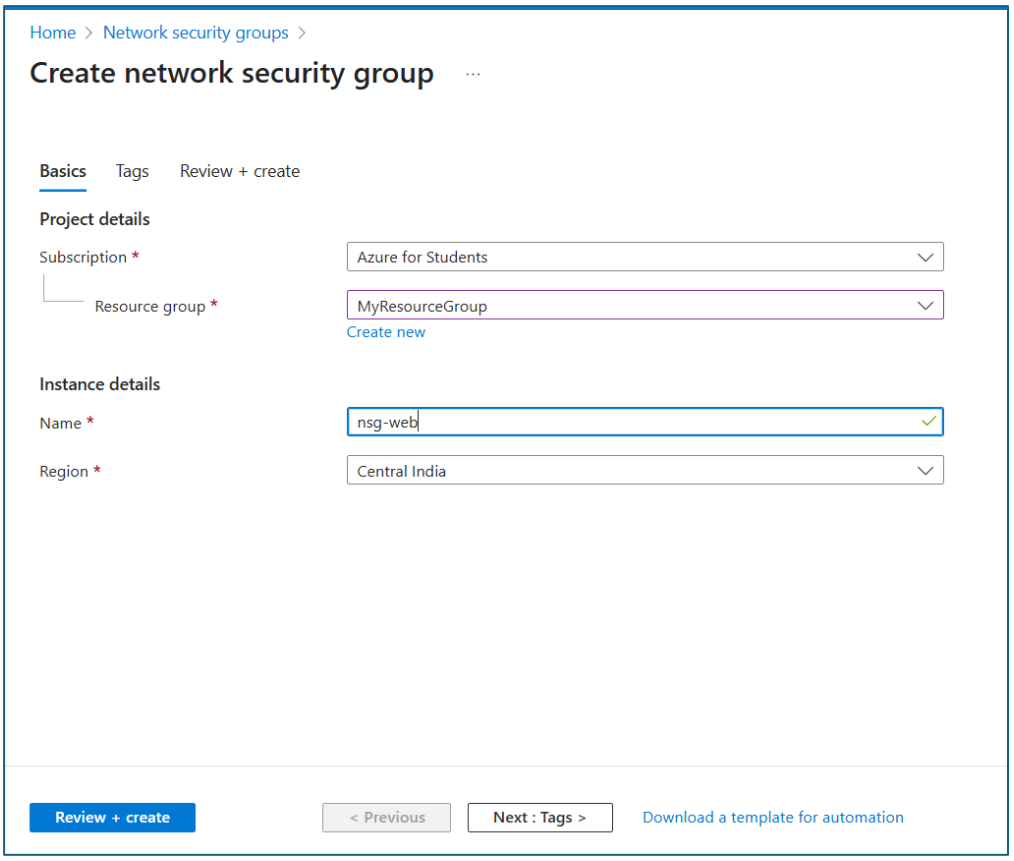
ii. Created a resource group named **MyResourceGroup**.
Selected region Central India



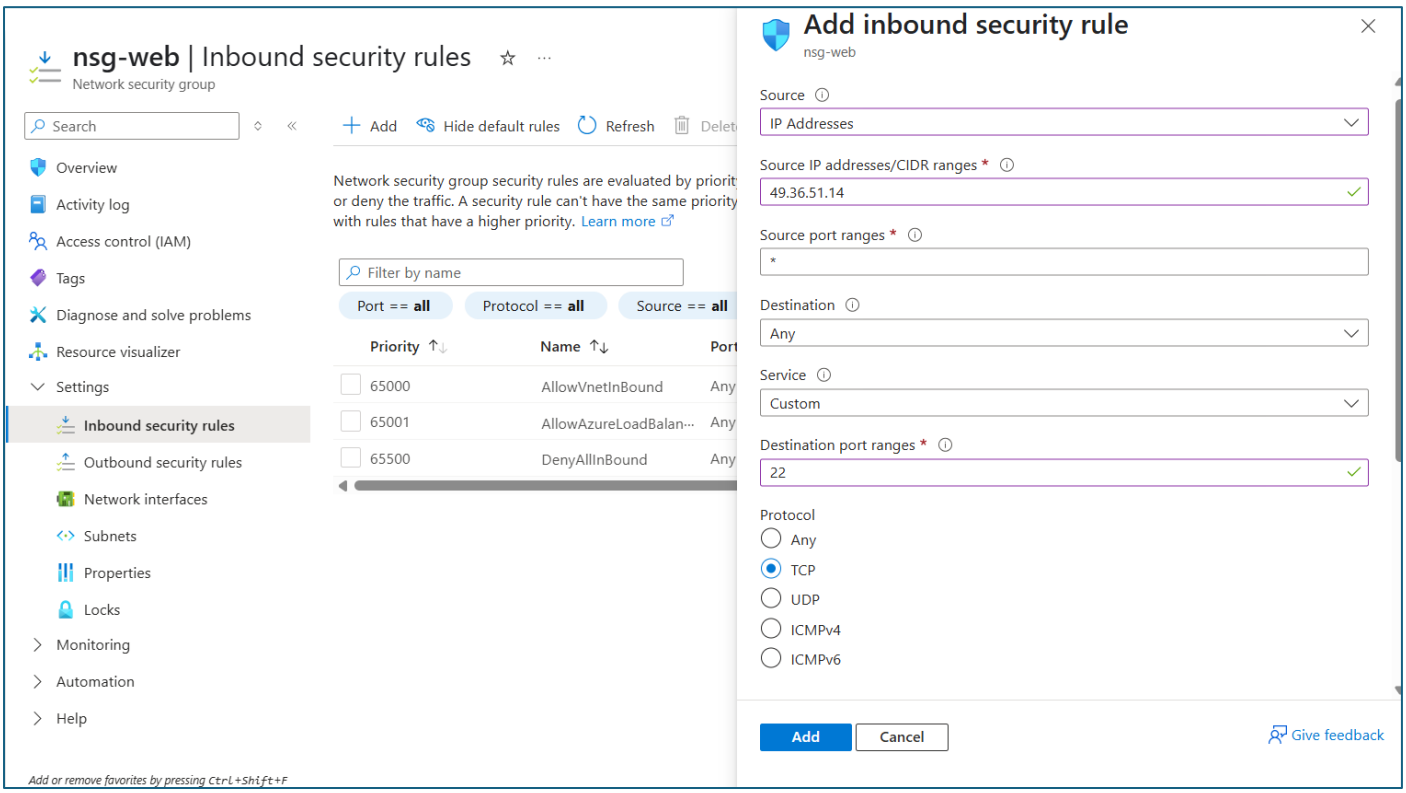
iii. Created 2 Virtual Networks named myVnet in the same region withing same resource group.
myVnet: Address Space: 10.0.0.0/16
Subnet: name – default - 10.0.0.0/16
subnet-web – 10.0.1.0/24
subnet-app - 10.0.2.0/24

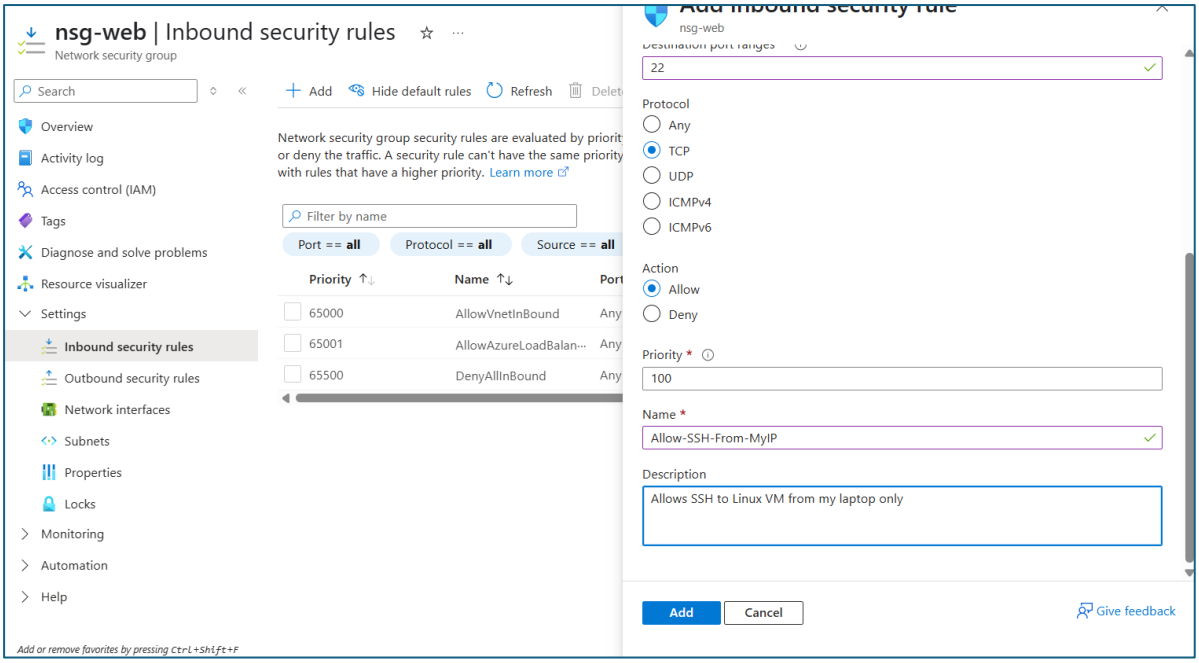


iv. Create network security group named nsg-web under the same region as resource group.

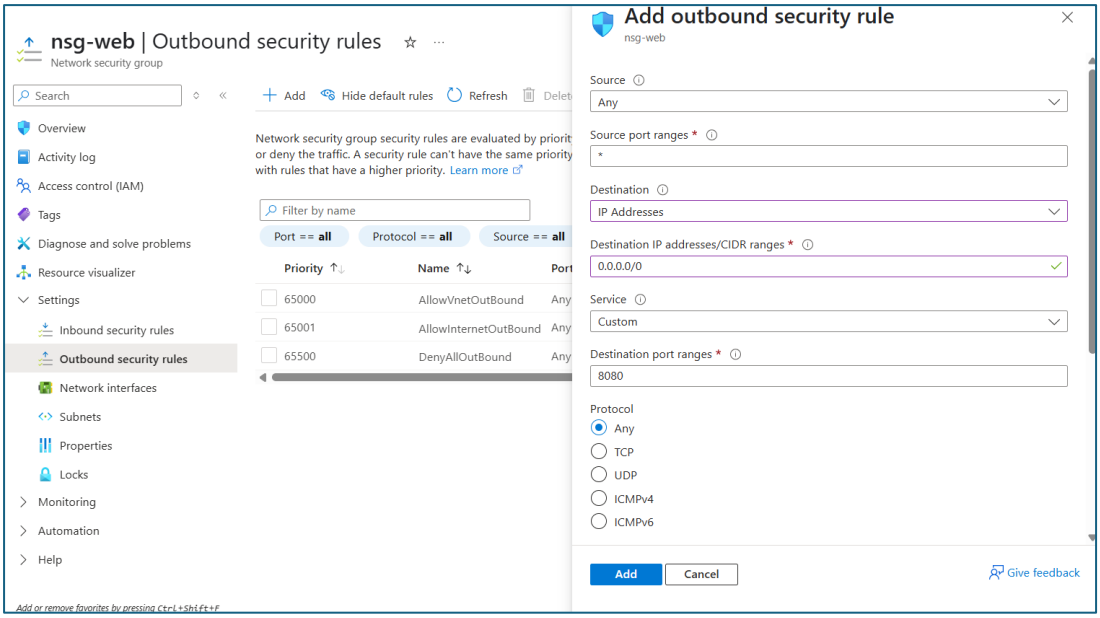


v. Go to the nsg-web and go to inbound security rules and make the changes as follows (allowing specific ip address access):

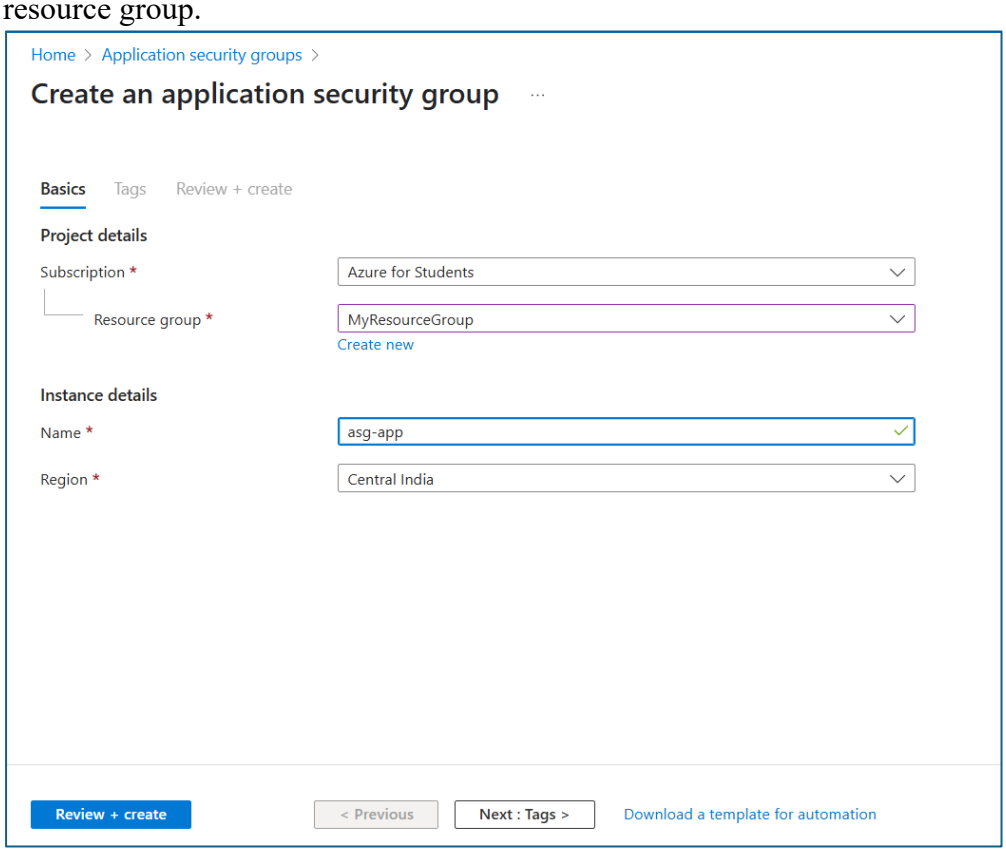




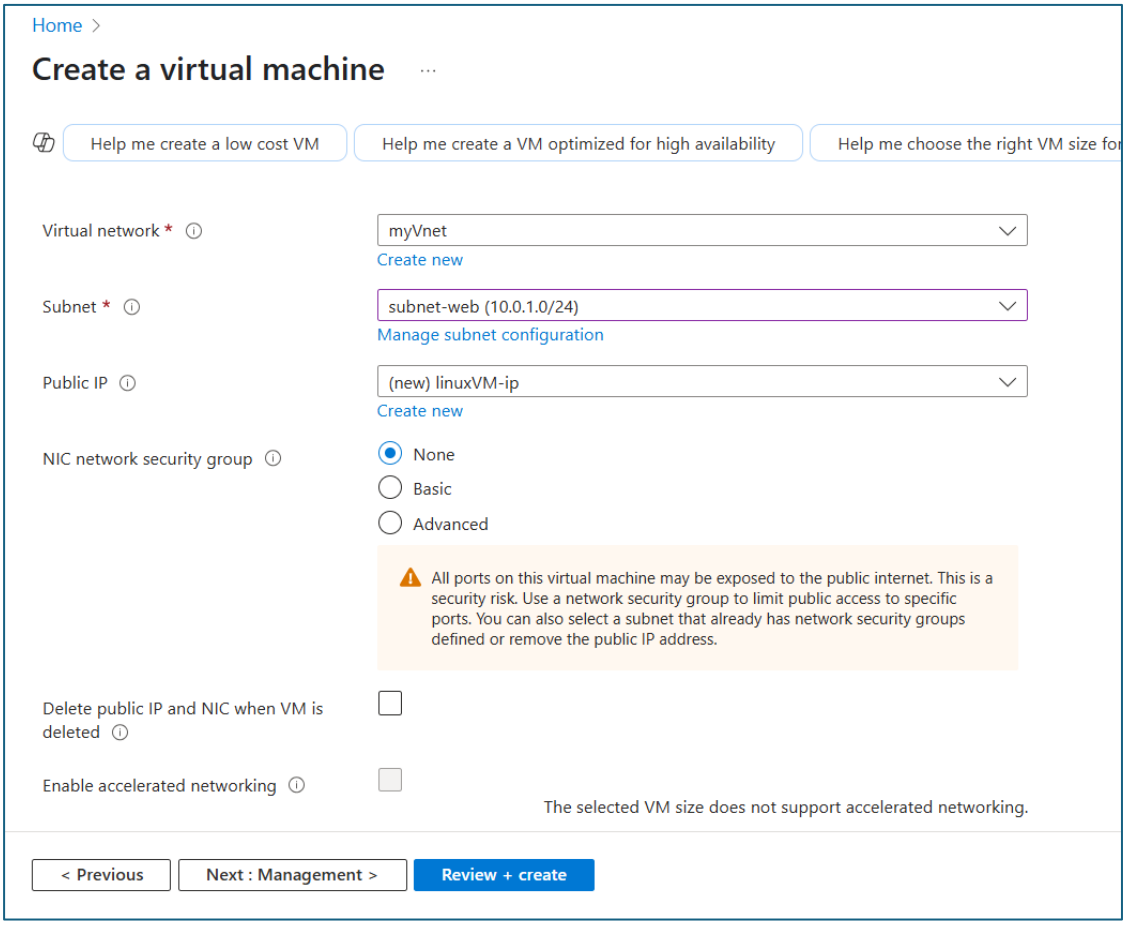
vi. Go to the outbound rules and deny internet permission:

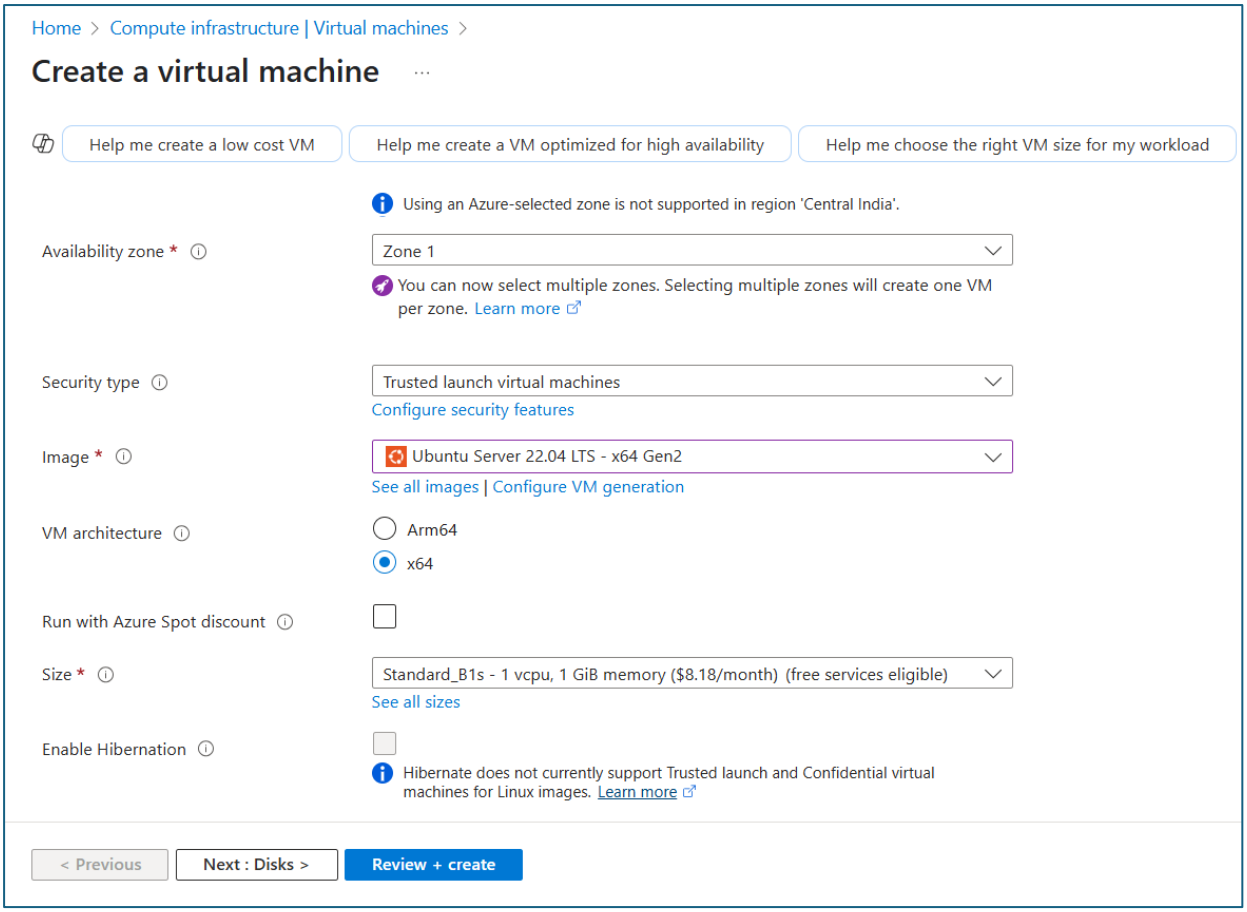


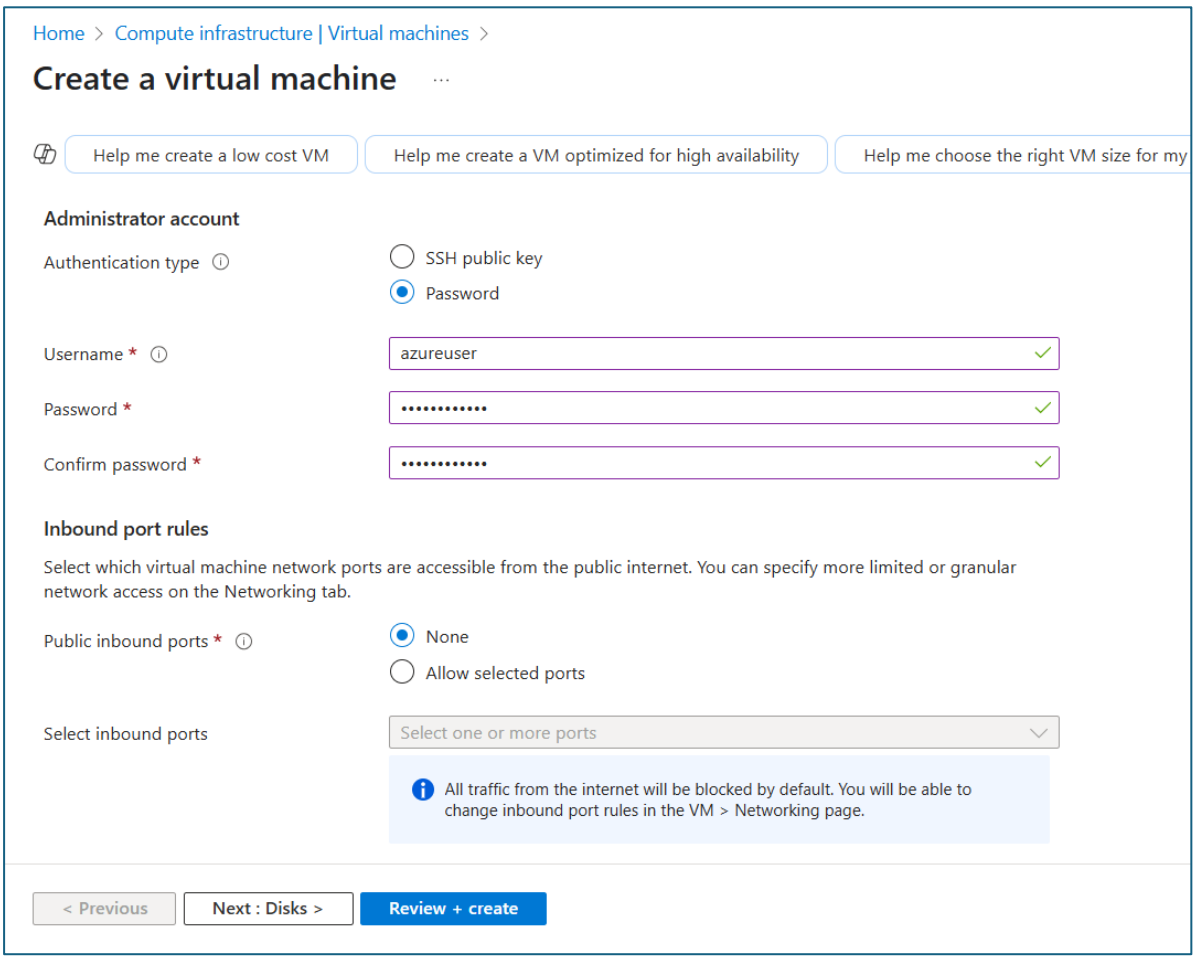
vii. Create Application Security group named asg-web and asg-app under the same region as resource group.

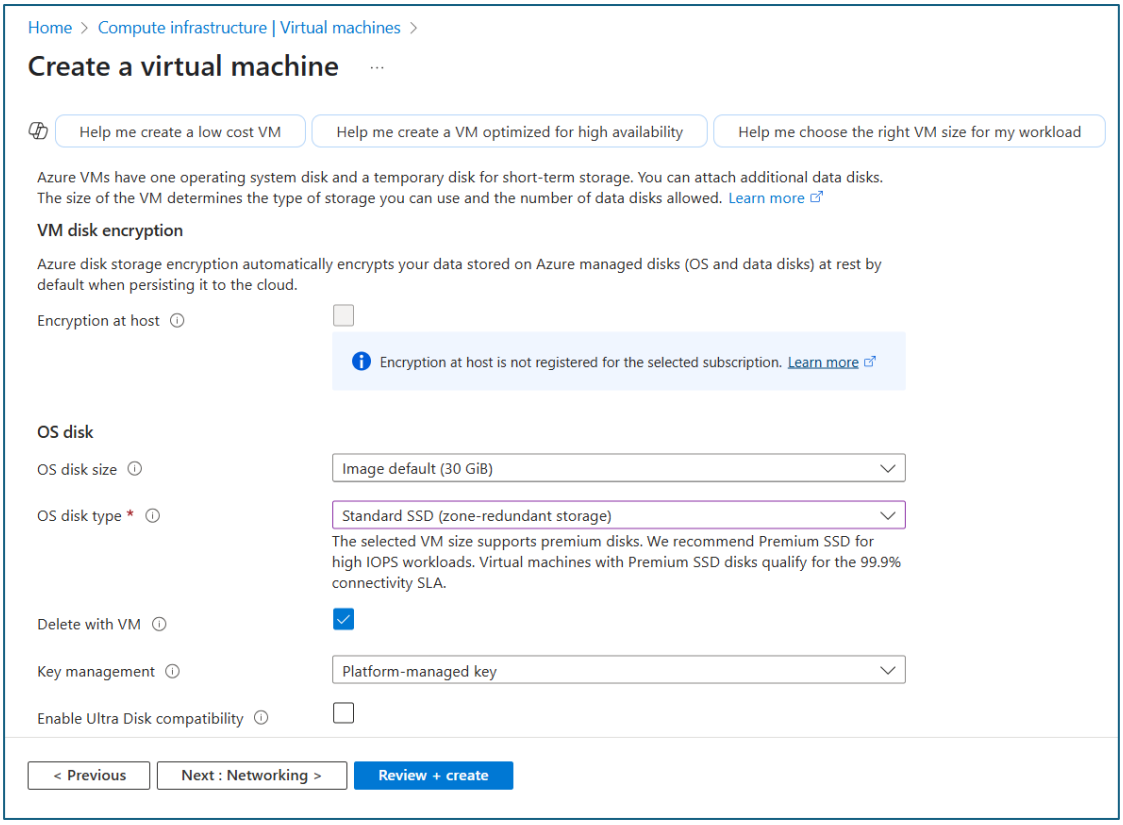


viii. Create linux virtual machine in subnet-web and windows virtual machine in subnet-app with the following configurations.

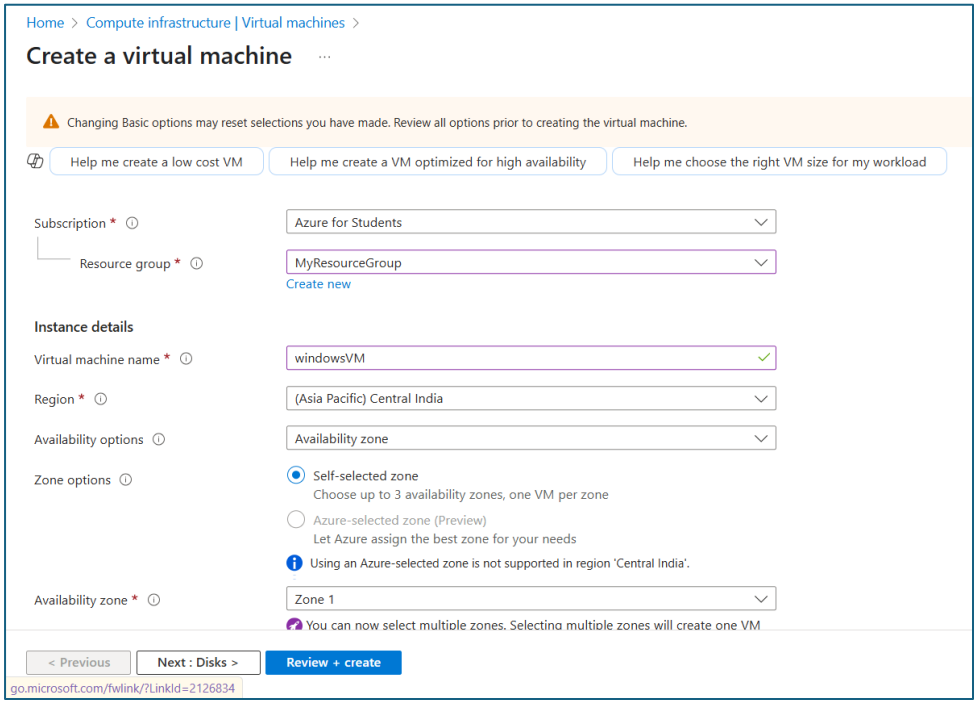


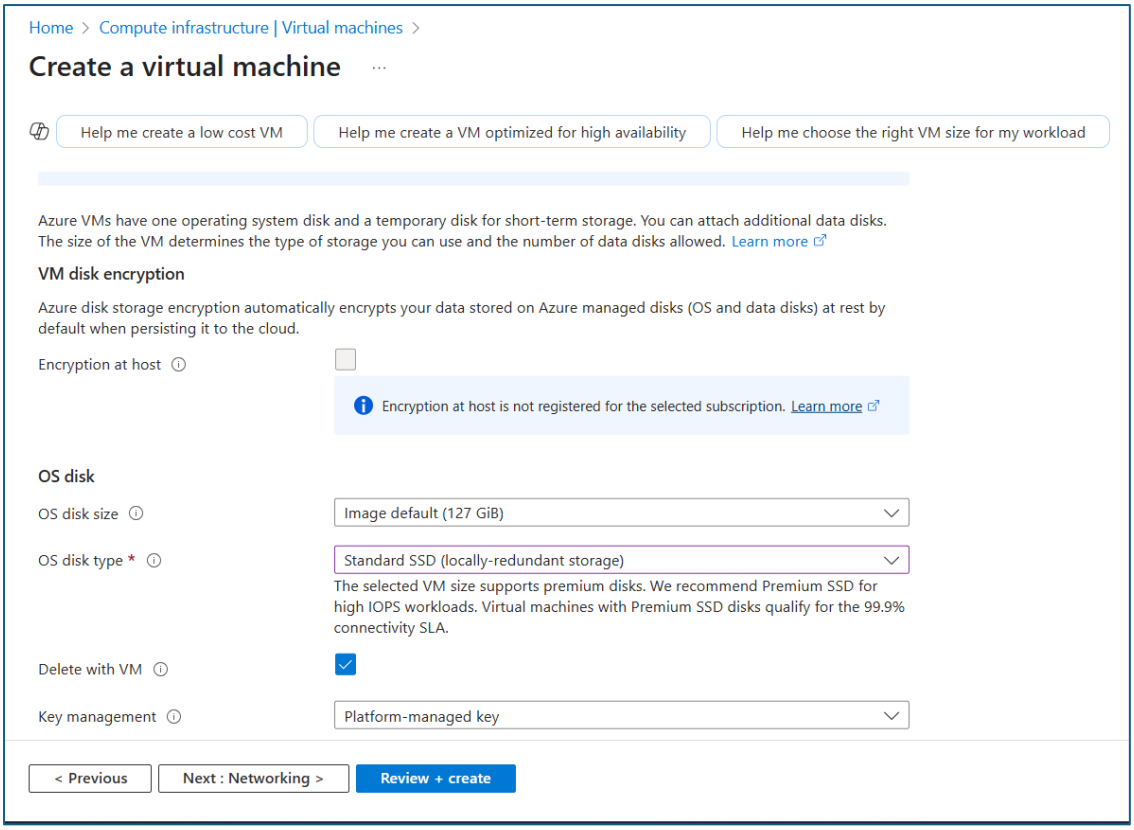

Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Using an Azure-selected zone is not supported in region 'Central India'.
Availability zone *
Zone 1
You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more
Security type
Trusted launch virtual machines
Configure security features
Image *
Ubuntu Server 22.04 LTS - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Run with Azure Spot discount
Size *
Standard_B1s - 1 vcpu, 1 GiB memory ($8.18/month) (free services eligible)
See all sizes
Enable Hibernation
Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more
< Previous
Next : Disks >
Review + create

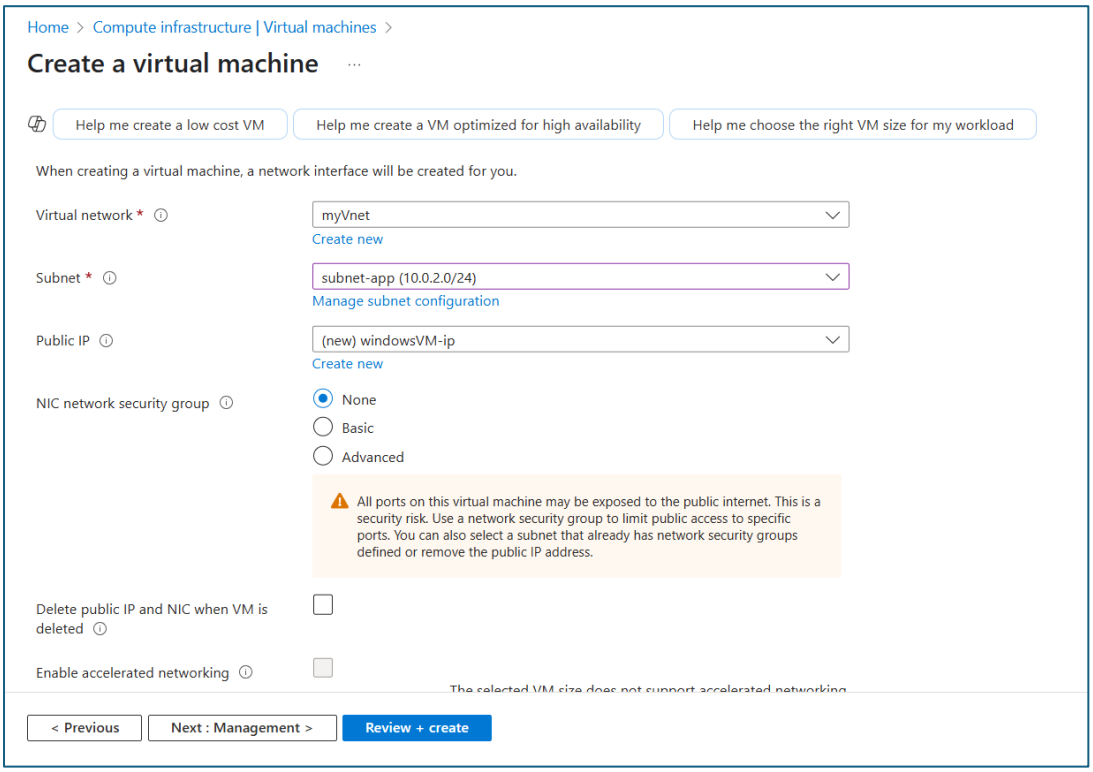

Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my
Administrator account
Authentication type
SSH public key
Password
Username *
azureuser
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.
Public inbound ports *
None
Allow selected ports
Select inbound ports
Select one or more ports
All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.
< Previous
Next : Disks >
Review + create



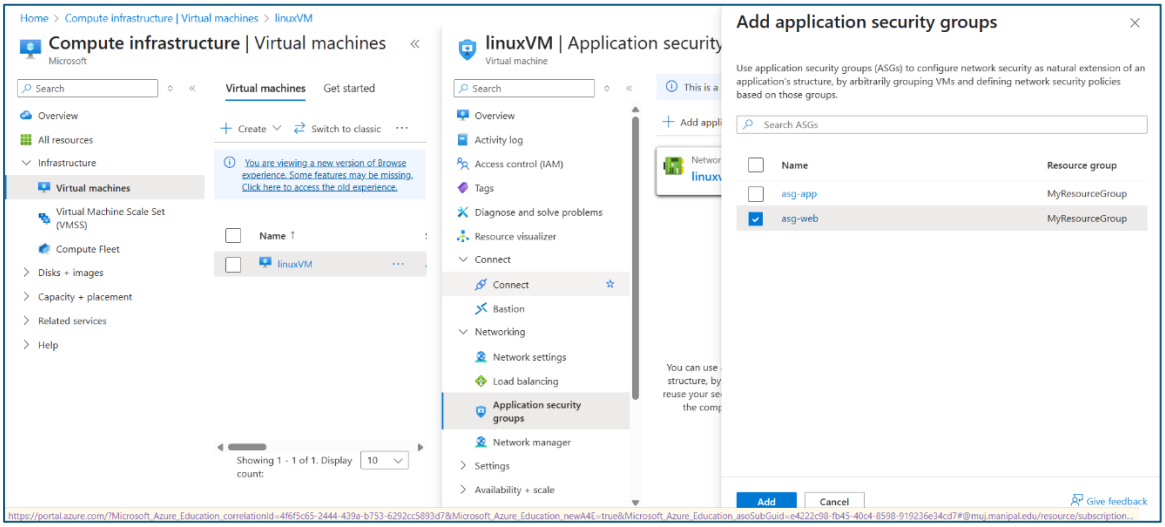
Windows virtual machine:

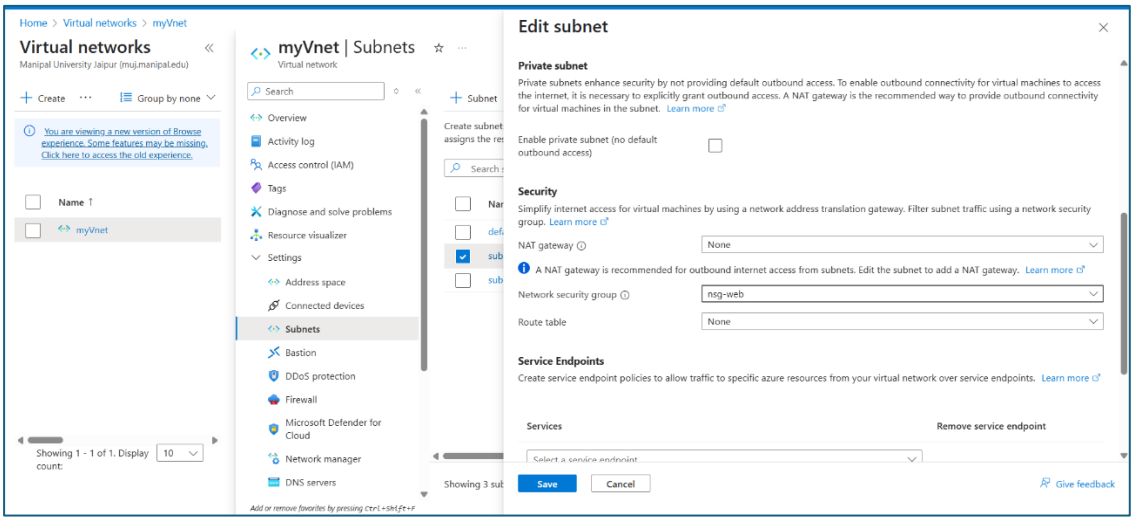



Home > Compute infrastructure | Virtual machines >
Create a virtual machine ...
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more
VM disk encryption
Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.
Encryption at host
Encryption at host is not registered for the selected subscription. Learn more
OS disk
OS disk size
Image default (127 GiB)
OS disk type *
Standard SSD (locally-redundant storage)
The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.
Delete with VM
Key management
Platform-managed key
< Previous
Next : Networking >
Review + create

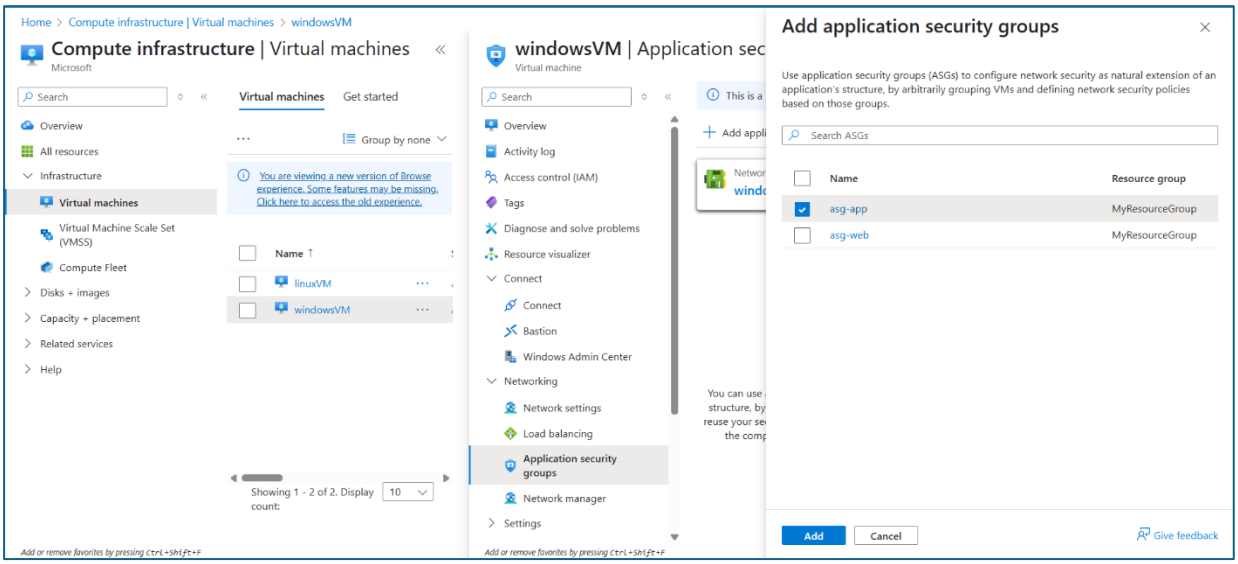

Home > Compute infrastructure | Virtual machines >
Create a virtual machine ...
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
When creating a virtual machine, a network interface will be created for you.
Virtual network *
myVnet
Create new
Subnet *
subnet-app (10.0.2.0/24)
Manage subnet configuration
Public IP
(new) windowsVM-ip
Create new
NIC network security group
None
Basic
Advanced
All ports on this virtual machine may be exposed to the public internet. This is a security risk. Use a network security group to limit public access to specific ports. You can also select a subnet that already has network security groups defined or remove the public IP address.
Delete public IP and NIC when VM is deleted
Enable accelerated networking
The selected VM size does not support accelerated networking
< Previous
Next : Management >
Review + create

ix. Attach nsg-web to linux vm and asg-web to linux vm.

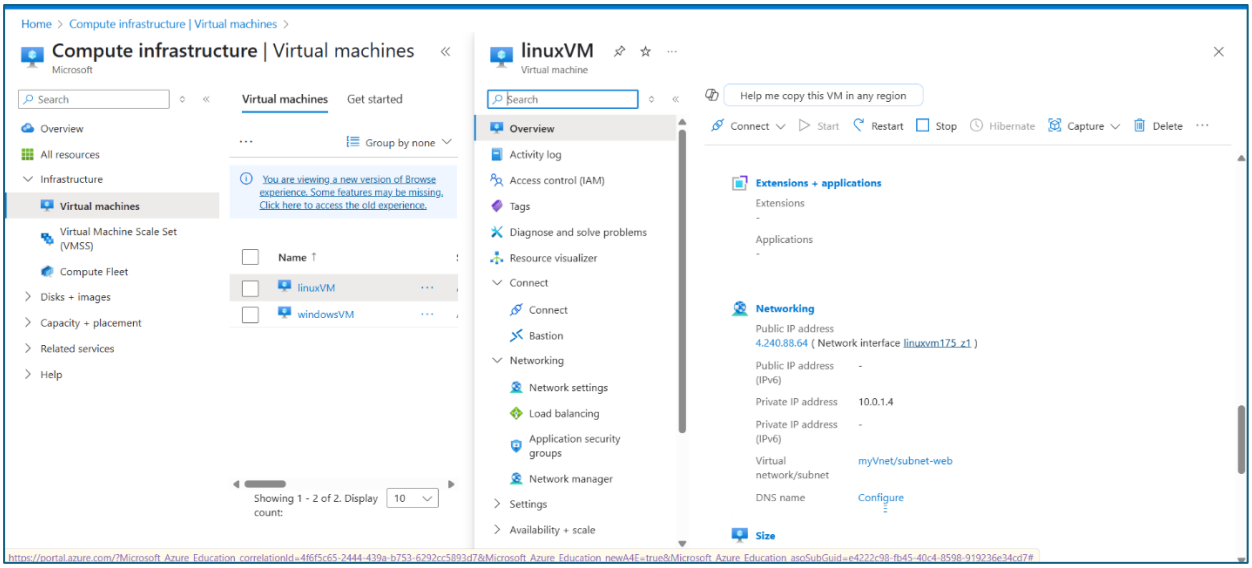


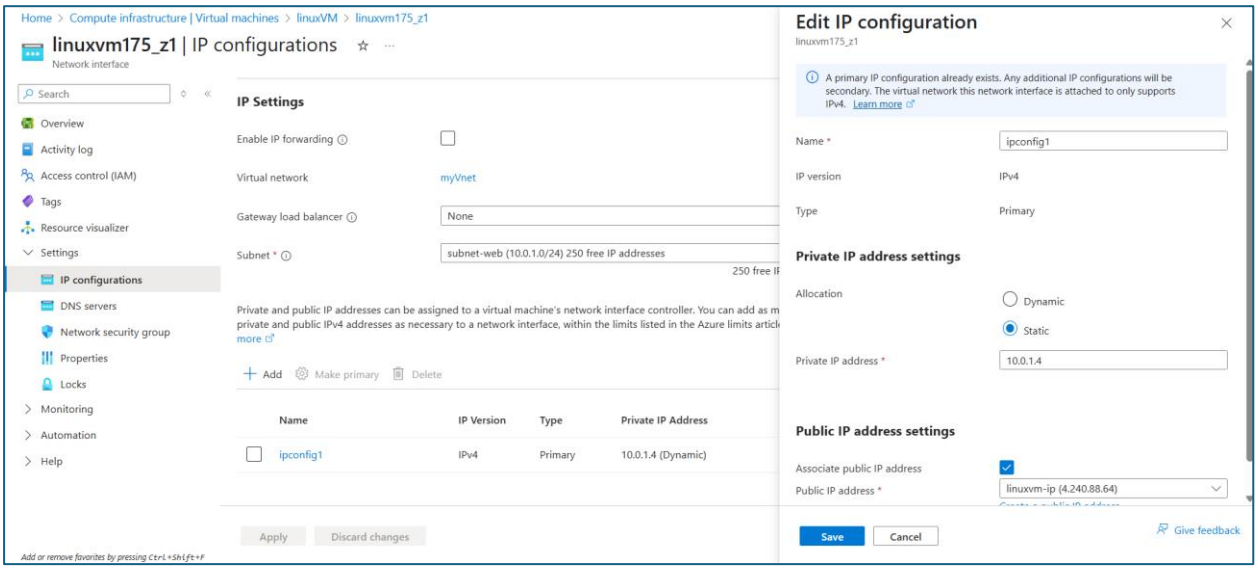


x. Similarly attach asg-app to windows vm.

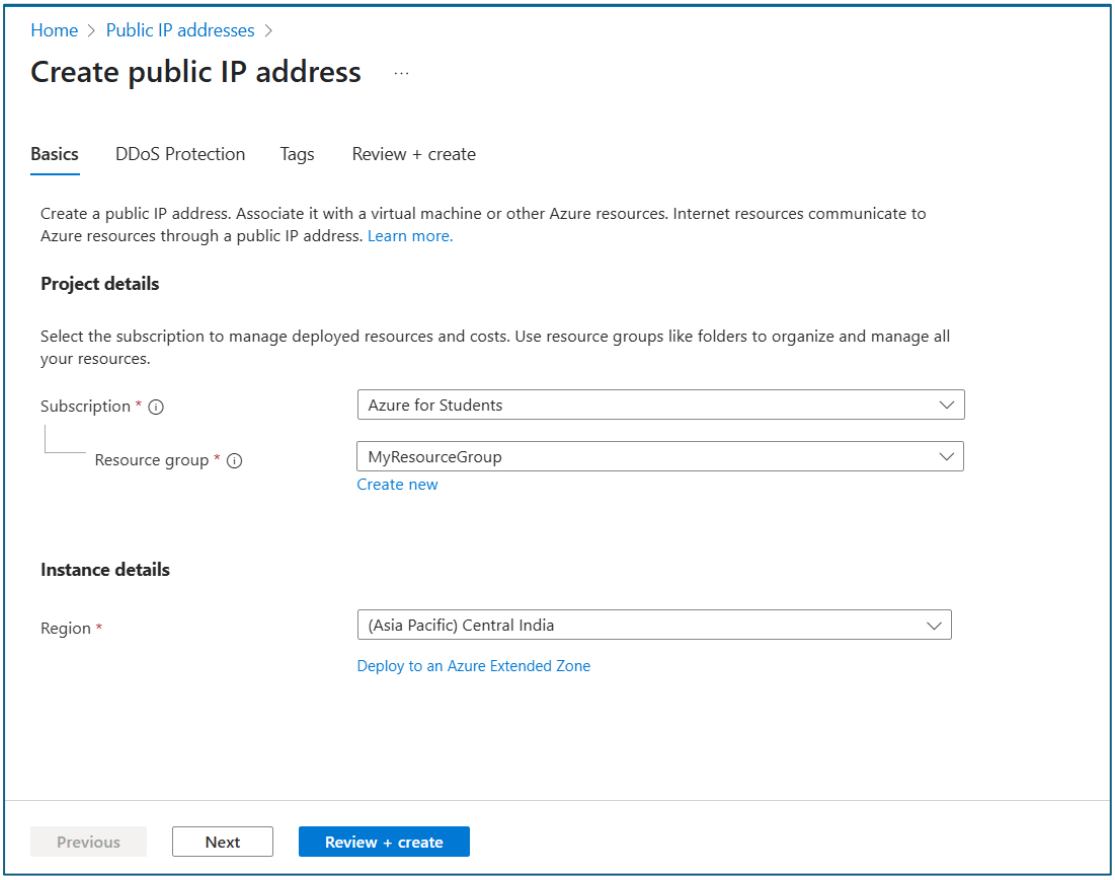


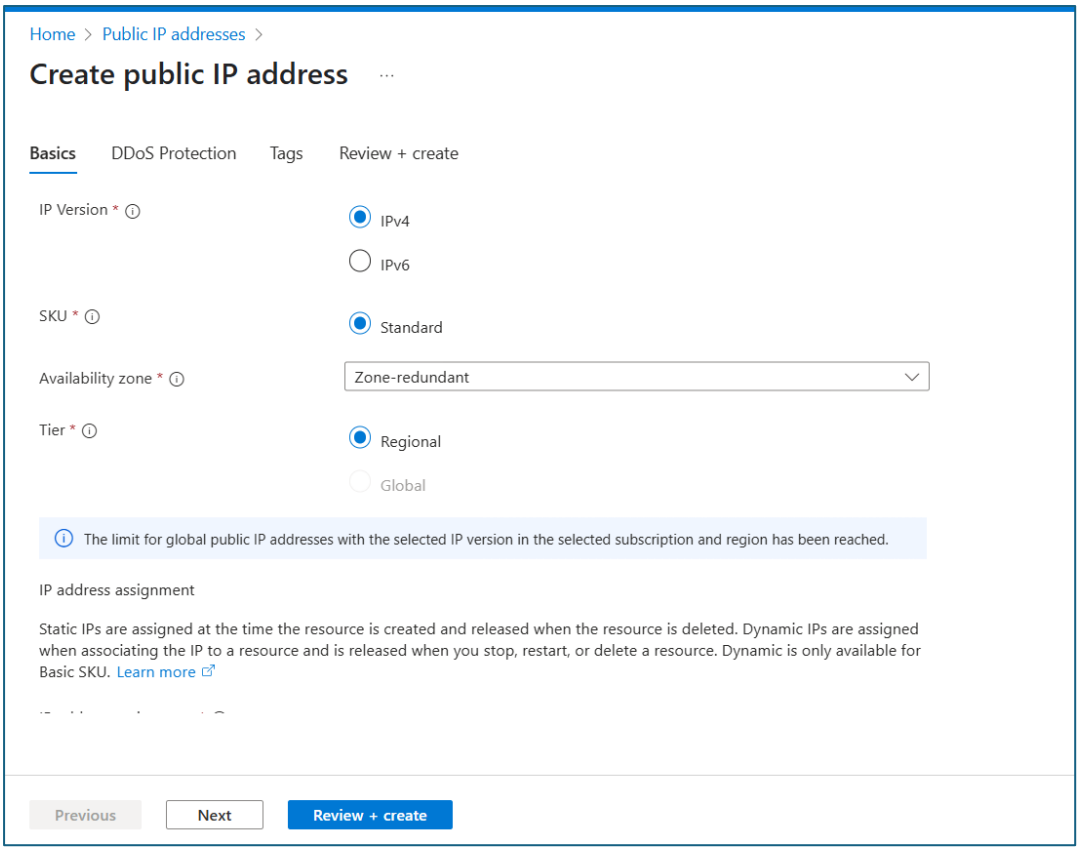
xi. Create static ip (10.0.1.4) for linux vm.

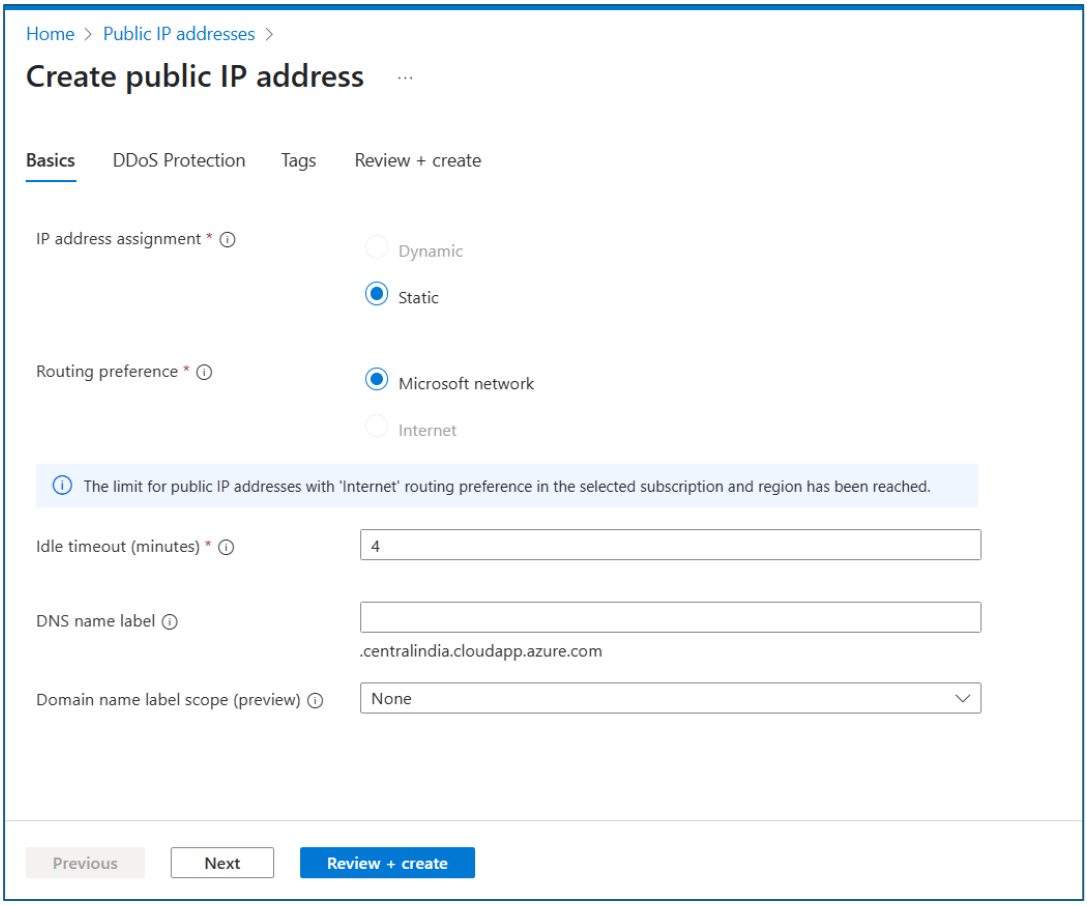

Home > Compute infrastructure | Virtual machines >
Compute infrastructure | Virtual machines
Microsoft
Search
Overview
All resources
Infrastructure
Virtual machines
Virtual Machine Scale Set (VMSS)
Compute Fleet
Disks + images
Capacity + placement
Related services
Help
Virtual machines
Get started
Group by none
You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.
Name
linuxVM
windowsVM
Showing 1 - 2 of 2. Display count:
10
linuxVM
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Connect
Bastion
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Availability + scale
Help me copy this VM in any region
Connect
Start
Restart
Stop
Hibernate
Capture
Delete
Extensions + applications
Extensions
-
Applications
-
Networking
Public IP address
4.240.88.64 (Network interface linuxvm175_z1)
Public IP address (IPv6)
-
Private IP address
10.0.1.4
Private IP address (IPv6)
-
Virtual network/subnet
myVnet/subnet-web
DNS name
Configure
Size

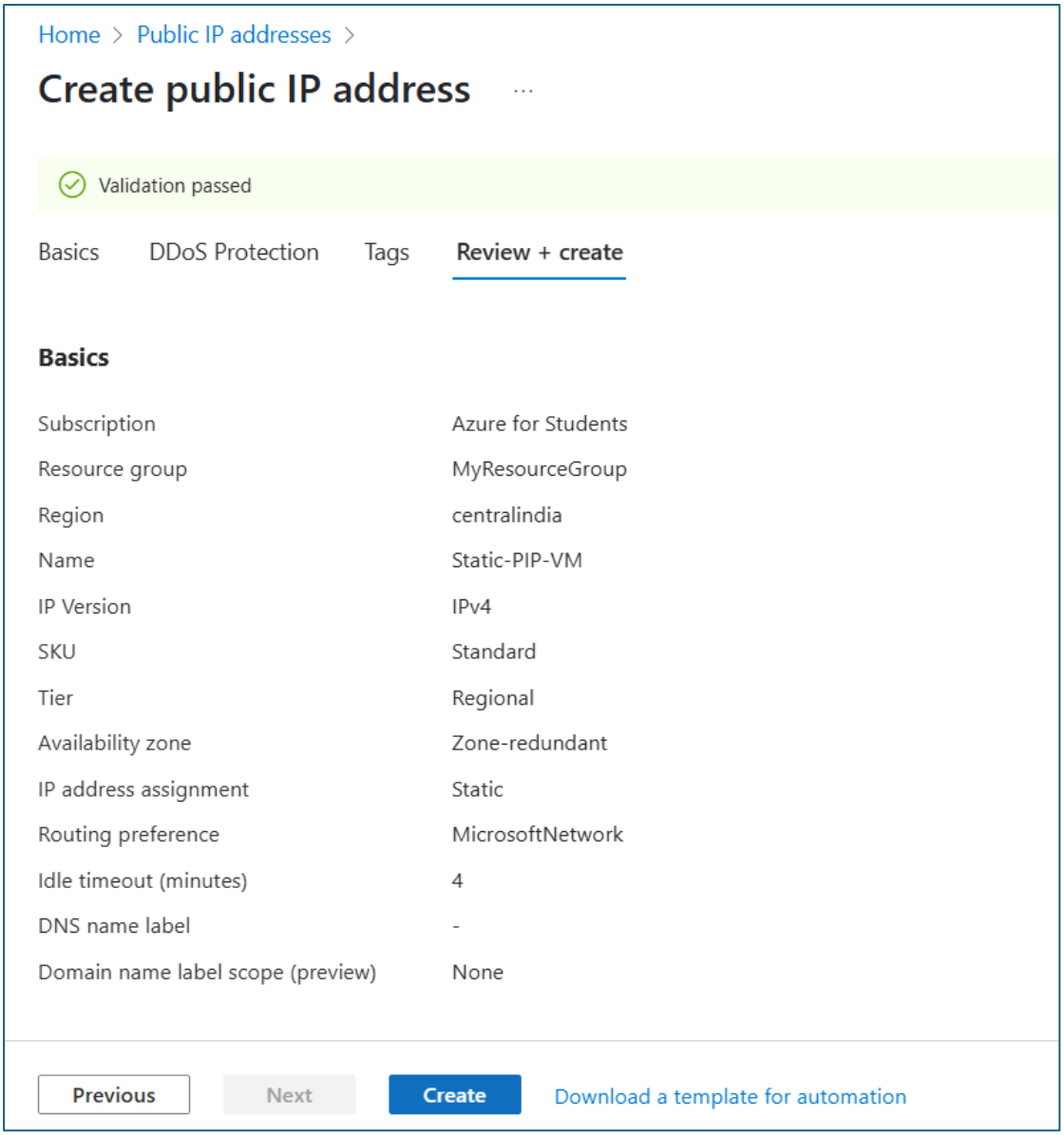

Home > Compute infrastructure | Virtual machines > linuxVM > linuxvm175_z1
linuxvm175_z1 | IP configurations
Network interface
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
IP configurations
DNS servers
Network security group
Properties
Locks
Monitoring
Automation
Help
IP Settings
Enable IP forwarding
Virtual network
myVnet
Gateway load balancer
None
Subnet *
subnet-web (10.0.1.0/24) 250 free IP addresses
Add
Make primary
Delete
Name
IP Version
Type
Private IP Address
ipconfig1
IPv4
Primary
10.0.1.4 (Dynamic)
Apply
Discard changes
Edit IP configuration
linuxvm175_z1
A primary IP configuration already exists. Any additional IP configurations will be secondary. The virtual network this network interface is attached to only supports IPv4. Learn more
Name *
ipconfig1
IP version
IPv4
Type
Primary
Private IP address settings
Allocation
Dynamic
Static
Private IP address *
10.0.1.4
Public IP address settings
Associate public IP address
Public IP address *
linuxvm-ip (4.240.88.64)
Save
Cancel
Give feedback

xii. Now, create public ip address in the same resource group.

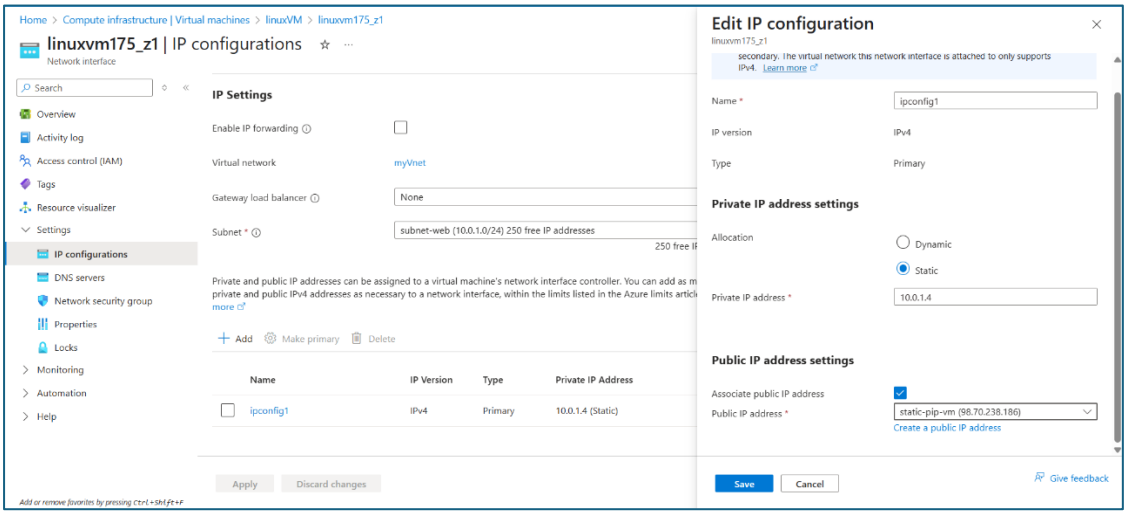


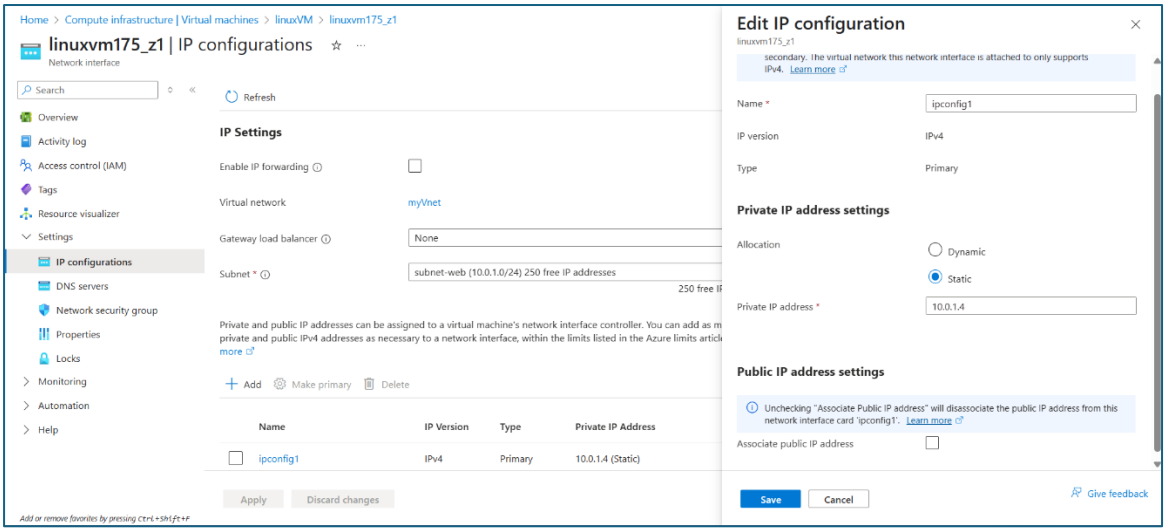



Home > Public IP addresses >
Create public IP address ...
Basics
DDoS Protection
Tags
Review + create
IP address assignment *
Dynamic
Static
Routing preference *
Microsoft network
Internet
The limit for public IP addresses with 'Internet' routing preference in the selected subscription and region has been reached.
Idle timeout (minutes) *
4
DNS name label
.centralindia.cloudapp.azure.com
Domain name label scope (preview)
None
Previous
Next
Review + create

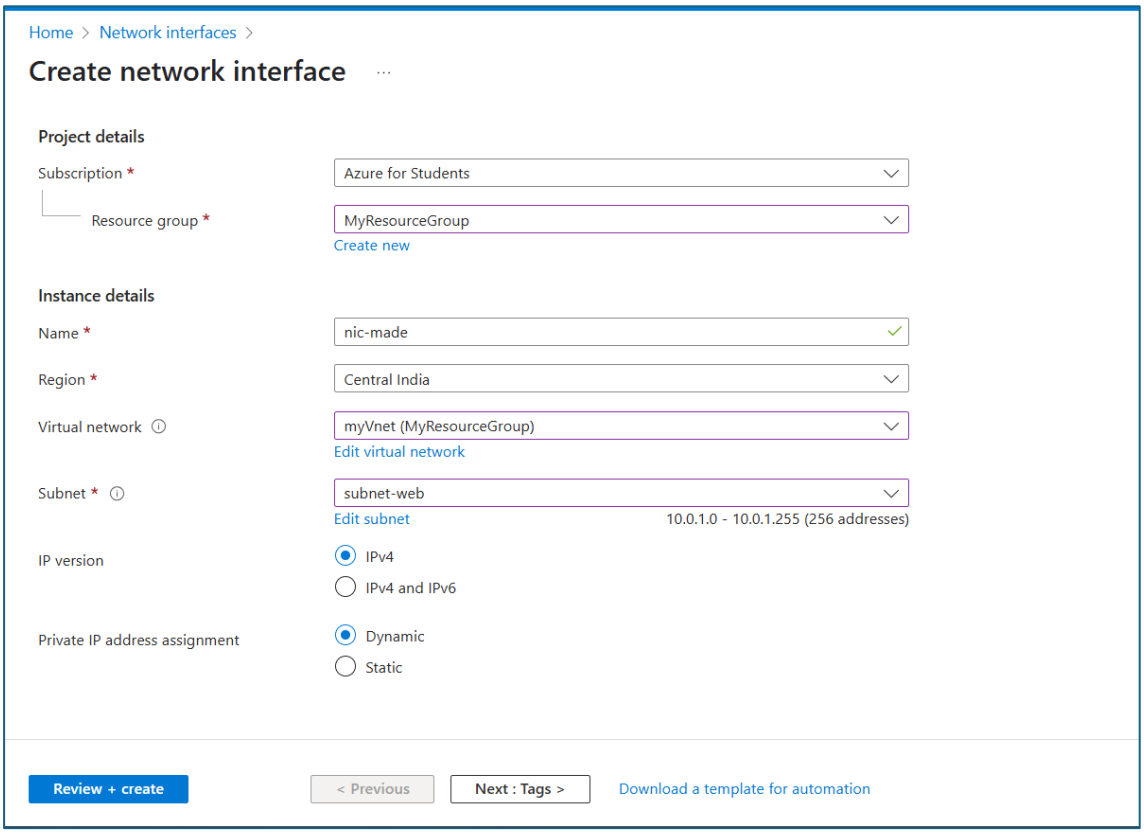


xiii. Associate the public ip to linux vm. And dissociate it too.





xiv. Create network interface card for myVnet in the same region.

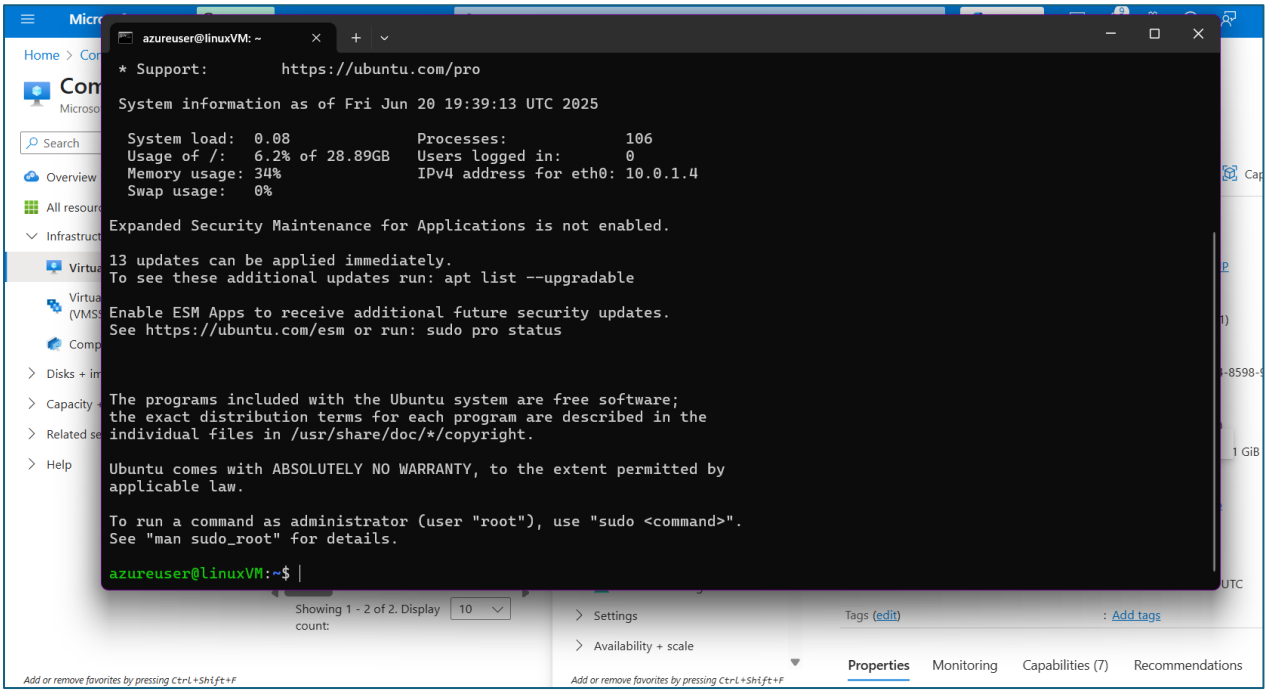


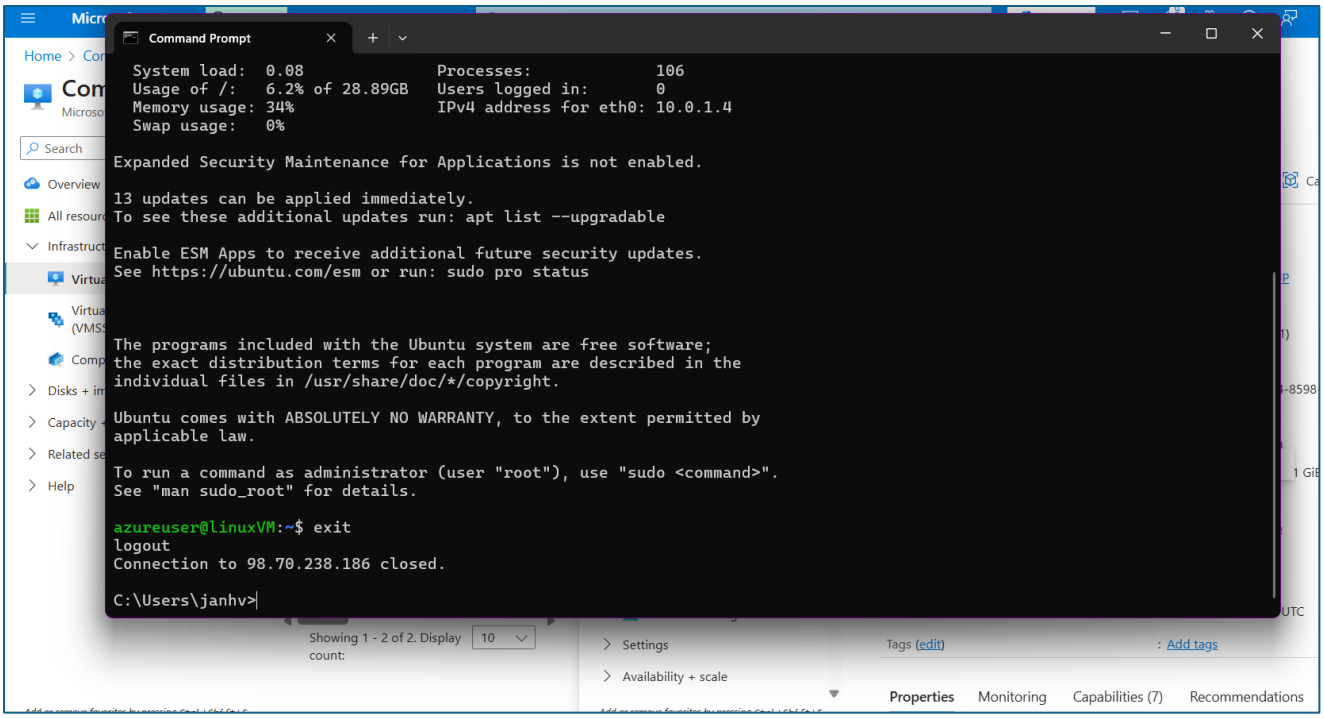
5. Result

- ✓ Successfully created network security group and application security group.
- ✓ Successfully attached the nsg and asg to the virtual machines.
- ✓ Successfully allowed inbound rules (specific ip address)
- ✓ Successfully denied outbound rules(internet access)
- ✓ Created static ip and successfully attached to linux vm.

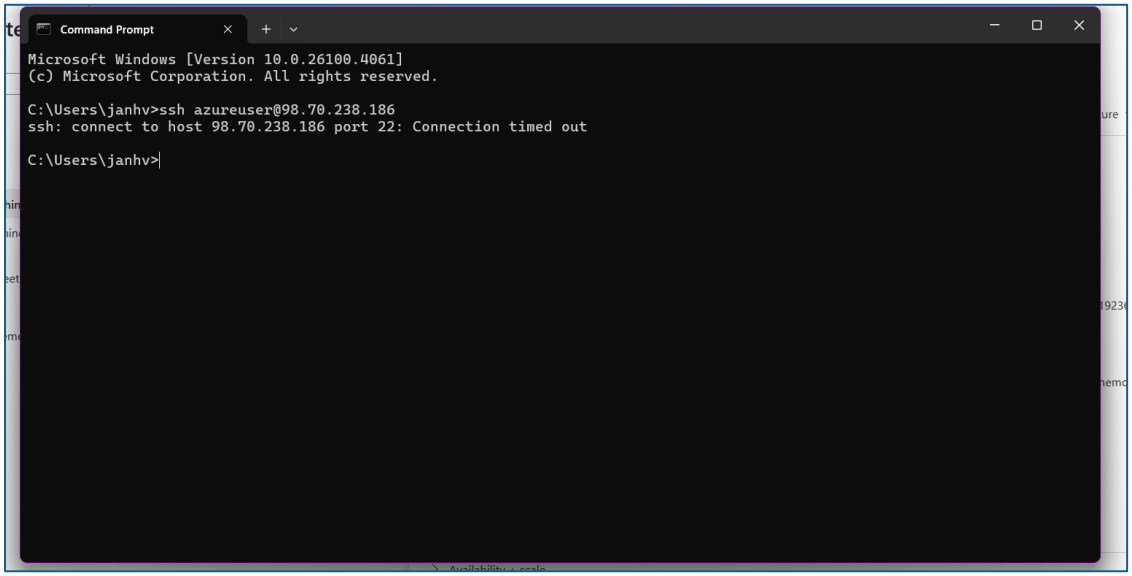
✓ Successfully associated and disassociated the ip address accordingly.

Accessed the linux virtual machine by the machine of specific address.

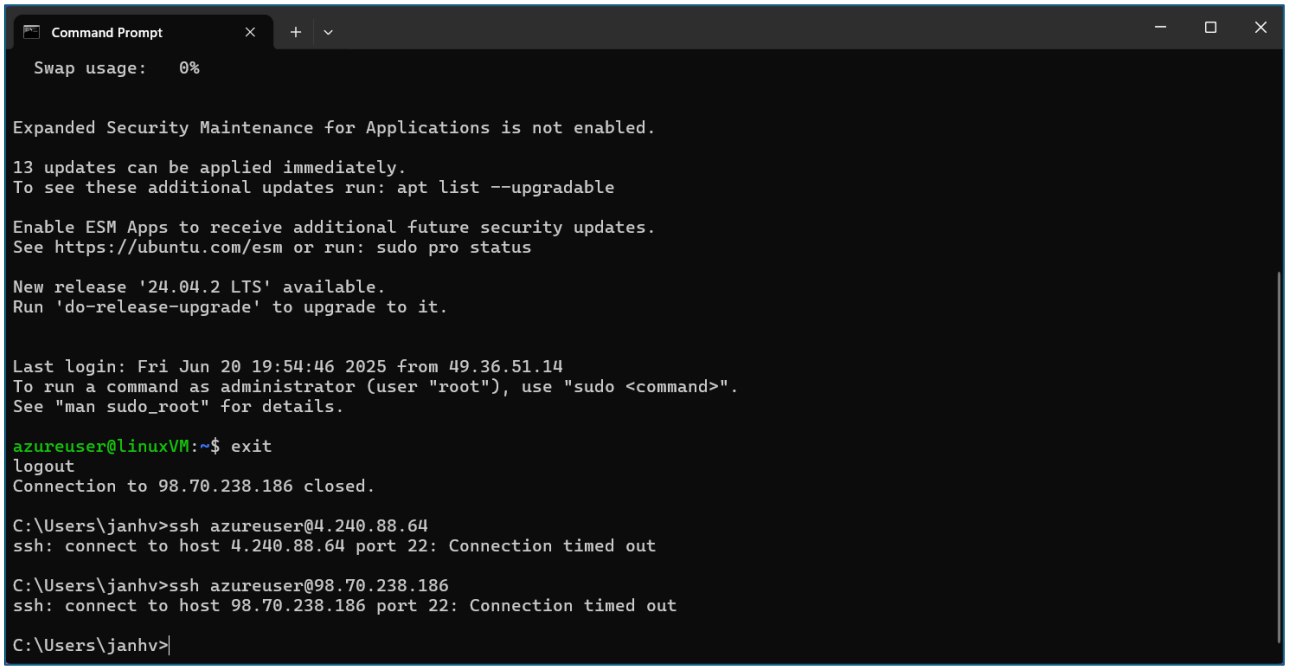




Access denied by other ip address machine



Accessing machine using the static ip address , denied access after dissociation.



6. Troubleshooting

Issue 1: When VM is being created, it is not visible. Solution: The VM and the chosen Virtual Network (VNet) are located in different regions.
Make sure the VM and VNet are in the same region when they are created by going to VNet → Overview then Region.

Issue 2: 'None' is shown for the public IP Solution: "None" appears if no public IP was assigned when the virtual machine was created.
To fix, navigate to VM → Networking → Click NIC → IP Configurations → Associate Public IP.

Issue 3: SSH/Ping Not Working Solution: By default, NSG blocks SSH and ICMP (ping).
Depending on the use case, add rules to NSG → Inbound Rules to permit either TCP or ICMP on port 22/3389.

Issue 4: ASG Doesn't Show Up When Creating a VM Solution: If ASG was created after the VM tab loaded or is located in a different region, it is not visible.
Make sure the ASG and the VM are in the same region, or manually attach the ASG using the NIC settings after the VM has been created.

Issue 5: Internet Access Remains Functional Following the Deny Rule Solution: The priority of the Outbound Deny rule is too low.
Make sure the priority is less than 65000 and that it is correctly connected to the subnet or NIC by going to NSG → Outbound Rules.

Issue 6: NSG Regulations Not Applying Solution: No association with NSG.
Make sure the NSG is truly connected by going to VNet → Subnets or NIC → NSG.
To debug the final rule set, use the NIC's "Effective Security Rules" feature.

7. References:

- **https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview**
- **https://learn.microsoft.com/en-us/azure/virtual-network/network-security-group-how-it-works**
- **https://learn.microsoft.com/en-us/azure/virtual-network/application-security-groups**
- **https://www.cloudthat.com/resources/blog/difference-between-application-security-groups-asgs-and-network-security-groups-nsgs**
- **https://tutorialsdojo.com/network-security-group-nsg-vs-application-security-group/**
- **https://www.geeksforgeeks.org/computer-networks/difference-between-static-and-dynamic-ip-address/**