Vnet

A. R7D Document: CIDR Ranges, VNet, Subnets, and Vnet Peering

1. Purpose

To document and understand the fundamentals and best practices regarding CIDR Ranges of a Virtual Network (Vnet), its subnets, and the mechanisms and types of Vnet Peering in cloud environments such as Microsoft Azure.

---

2. Scope

- Design considerations for IP Addressing with CIDR
- Subnetting within Vnets
- Configuration and planning of Vnet Peering
- Security, routing, and performance considerations

---

3. Key Concepts

3.1. CIDR (Classless Inter-Domain Routing)

- CIDR is a method for allocating IP addresses and routing IP packets.
- CIDR notation: <IP_address>/<prefix_length>
  Example: 10.0.0.0/16
- It allows flexible IP address allocation:
  - 10.0.0.0/8 = 16,777,216 addresses
  - 10.0.0.0/16 = 65,536 addresses
  - 10.0.0.0/24 = 256 addresses

---

4. Virtual Network (Vnet) CIDR Range

4.1. Definition

- A Vnet is a logical isolation of the Azure cloud dedicated to a subscription.
- Each Vnet must have a non-overlapping CIDR block.

4.2. Best Practices

- Use private IP ranges defined in RFC 1918:
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Plan for scalability: Use 10.0.0.0/16 for large deployments

---

5. Subnets

5.1. Definition

- A subnet is a segmented block of a Vnet's address space.
- Subnets are used to isolate workloads and enforce security.

5.2. CIDR within a Subnet

- A subnet's CIDR must fall within the Vnet CIDR.
- Example:
  - Vnet: 10.0.0.0/16
  - Subnet1: 10.0.1.0/24
  - Subnet2: 10.0.2.0/24

5.3. Subnet Sizing Guidelines

- /24 (256 addresses) is common
- Azure reserves 5 Ips per subnet:

- First: Network address
- Last: Broadcast address
- 3 Reserved by Azure

---

6. Vnet Peering

6.1. Definition

- Vnet peering connects two Vnets so that resources in each can communicate with each other using private Ips.
- Provides high-bandwidth, low-latency connectivity.

6.2. Types of Vnet Peering

Type	Description
Intra-region Peering	Vnets in the **same Azure region**
Global Peering	Vnets in **different regions**
Cross-Subscription Peering	Vnets in **different subscriptions**, same or different regions
Cross-Tenant Peering	Vnets in **different Azure AD tenants** (requires extra config)

6.3. Peering Features

Feature	Supported
Private IP communication	✅
Resource Manager support	✅
Transitive Routing	❌

Feature	Supported
Gateway Transit	✅ (with config)
Bandwidth limit	No extra charge for bandwidth, but data transfer charges apply

---

7. Vnet Peering: Routing and Security

7.1. Routing

- Automatically updates the routing table.
- Custom routes or UDRs (User Defined Routes) are needed for special paths.

7.2. Security

- NSGs (Network Security Groups) apply at subnet/nic level
- Traffic between peered Vnets can be filtered using NSGs and ASGs

---

8. Use Cases

- Isolating environments (Dev, Test, Prod) but allowing inter-communication
- Multi-region HA deployments
- Connecting Vnets across departments or business units

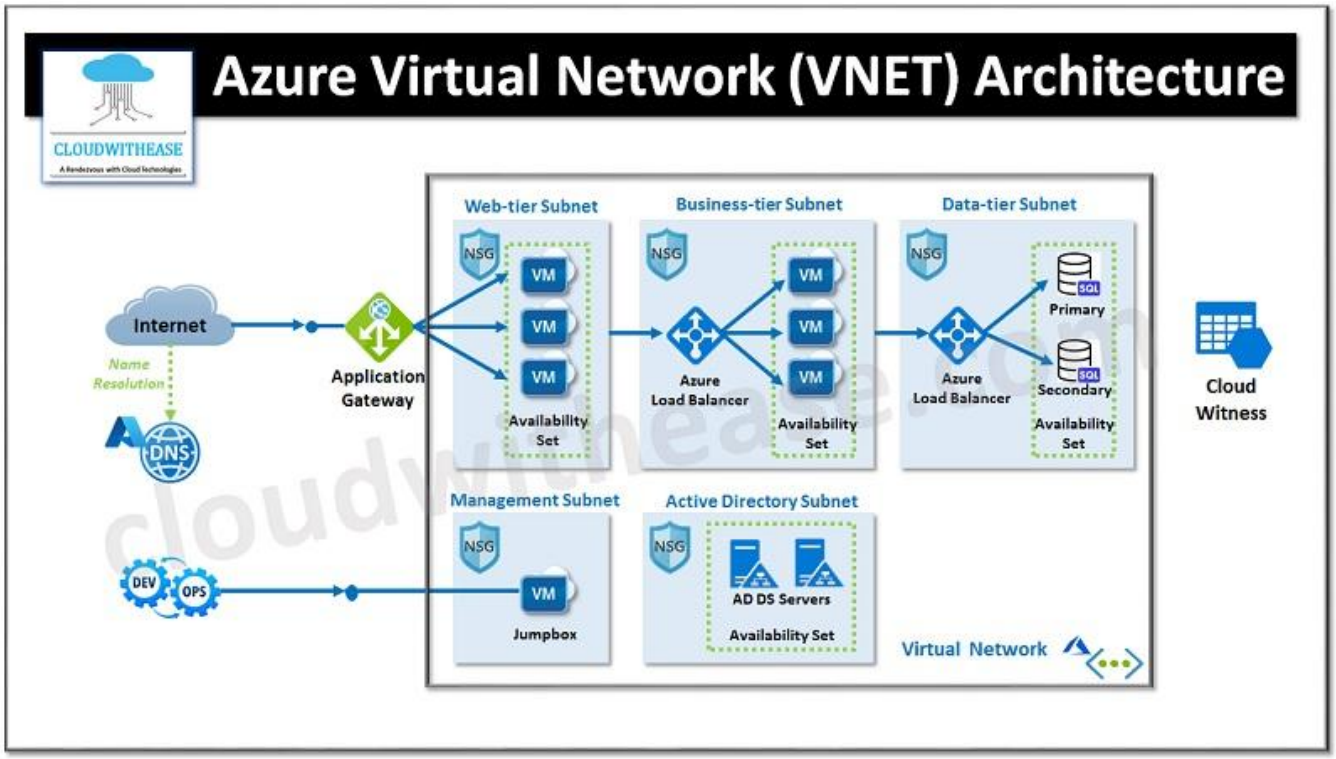
---

9. Limitations and Considerations

- **Overlapping CIDRs** not allowed for peering
- **Transitive peering** is not supported: Vnet A → B → C does not imply A → C
- **Peering limits** per Vnet: 500 (soft limit, subject to region

10. Diagrams

- Vnet/Subnet Hierarchy



- Vnet Peering Topology (Hub & Spoke, Mesh)

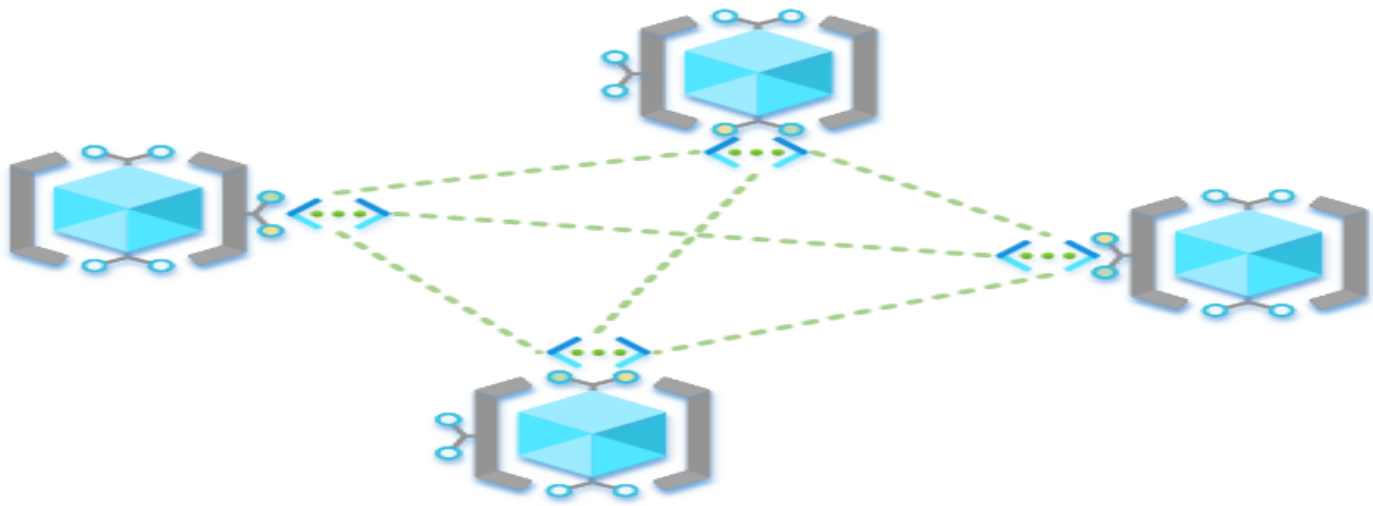


Fig : Mesh

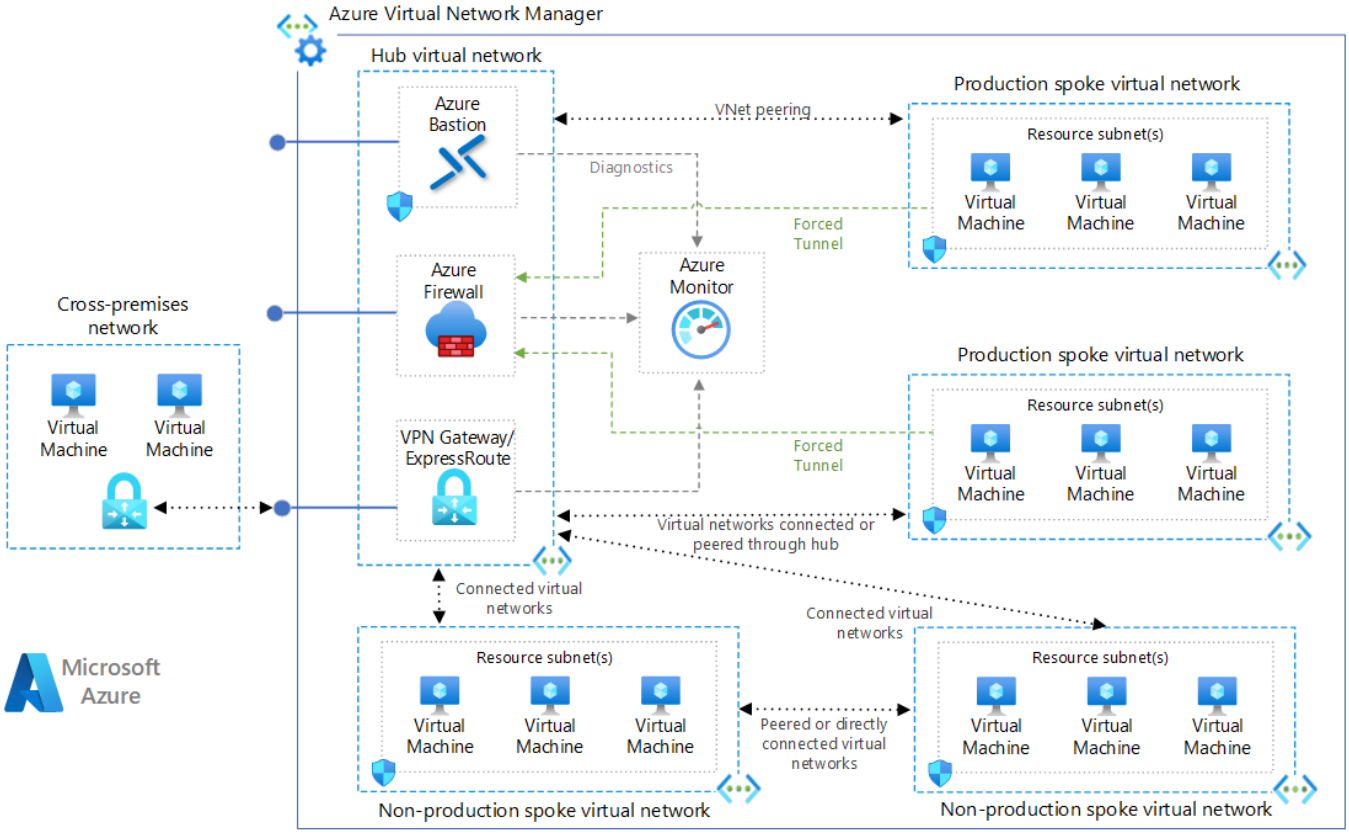


Fig : Hub and Spoke

B. R&D Document: Azure Virtual Network & VNet Peering Use Case

Use Case:

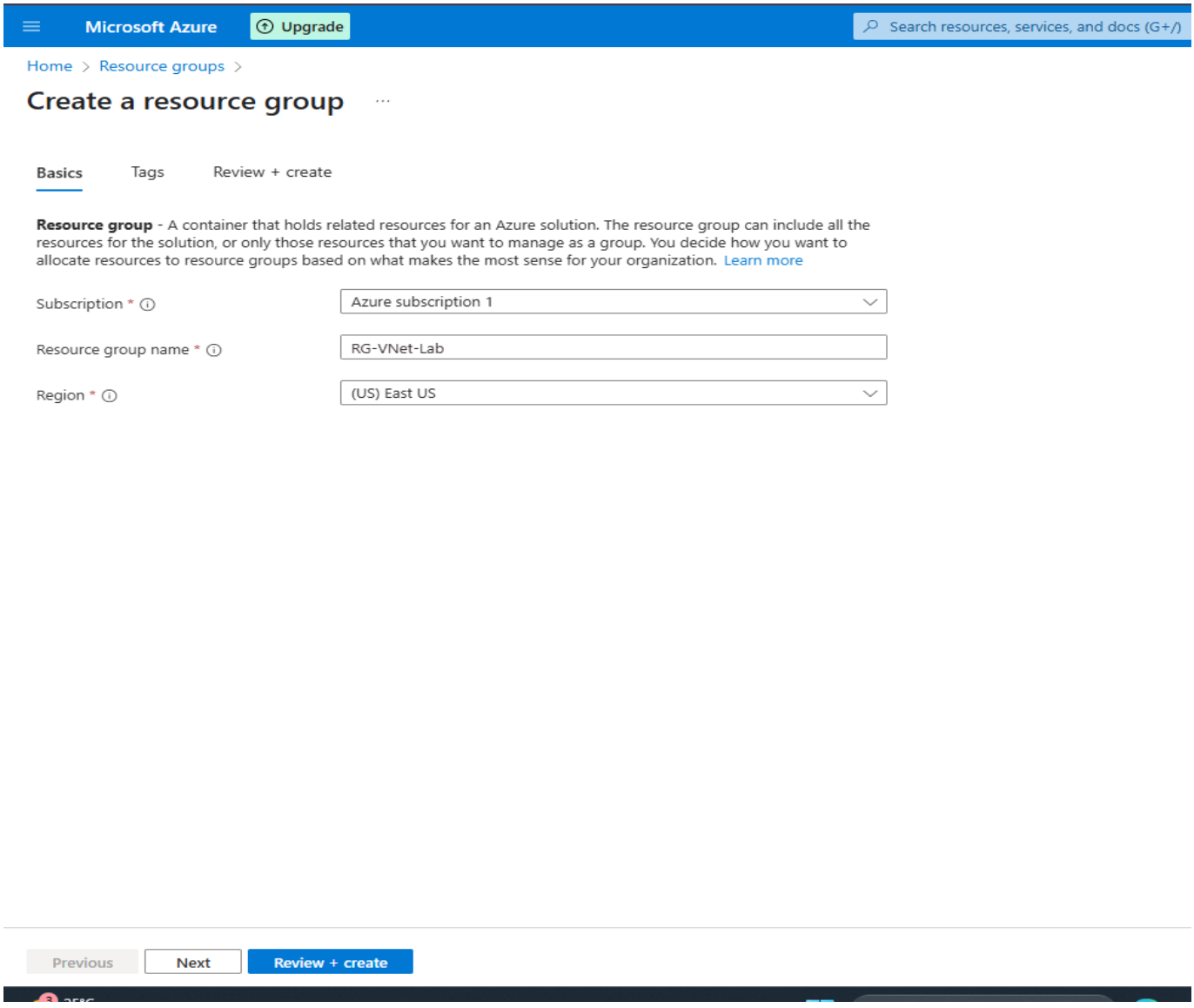
Create two VNets with subnets. Launch one Windows VM and one Linux VM (in different subnets of the same VNet). Ensure they can communicate with each other. Then create another VNet and connect both VNets using VNet peering. Verify cross-VNet VM communication.

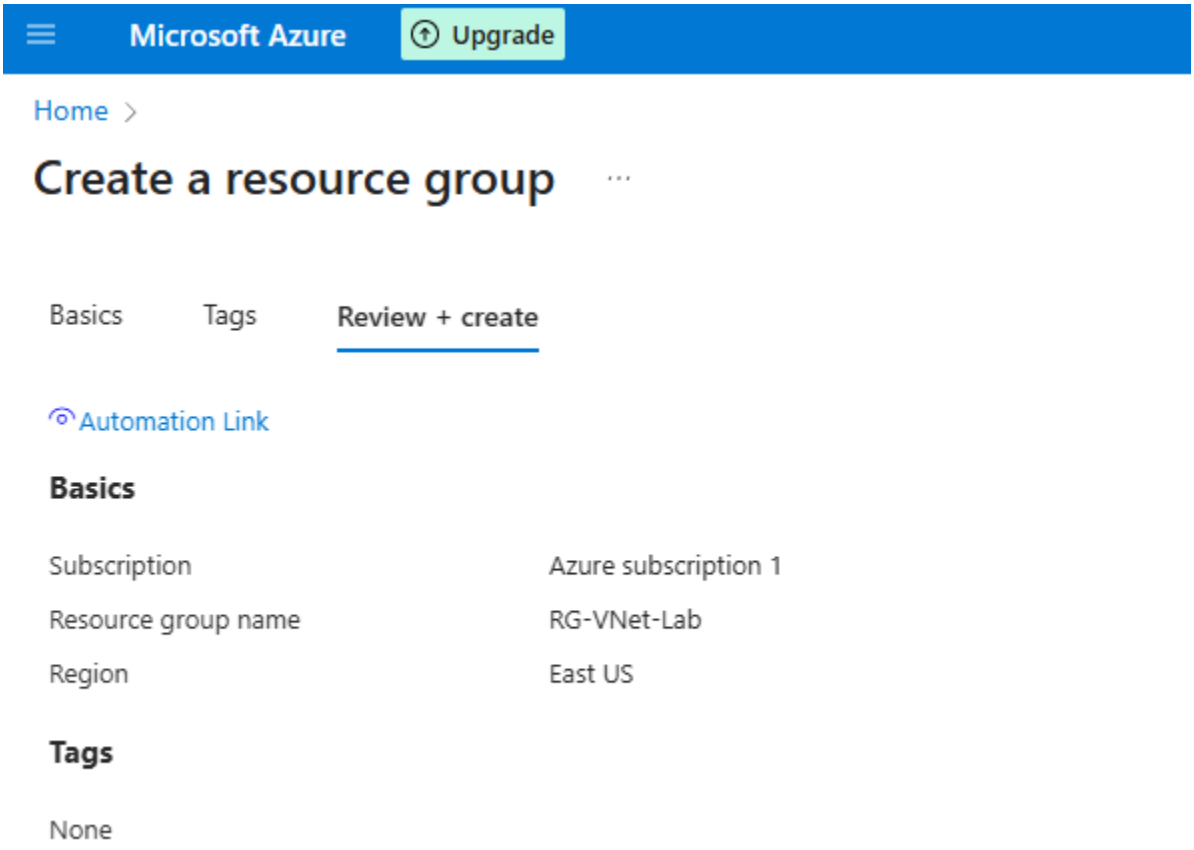
Step 1: Create a Resource Group

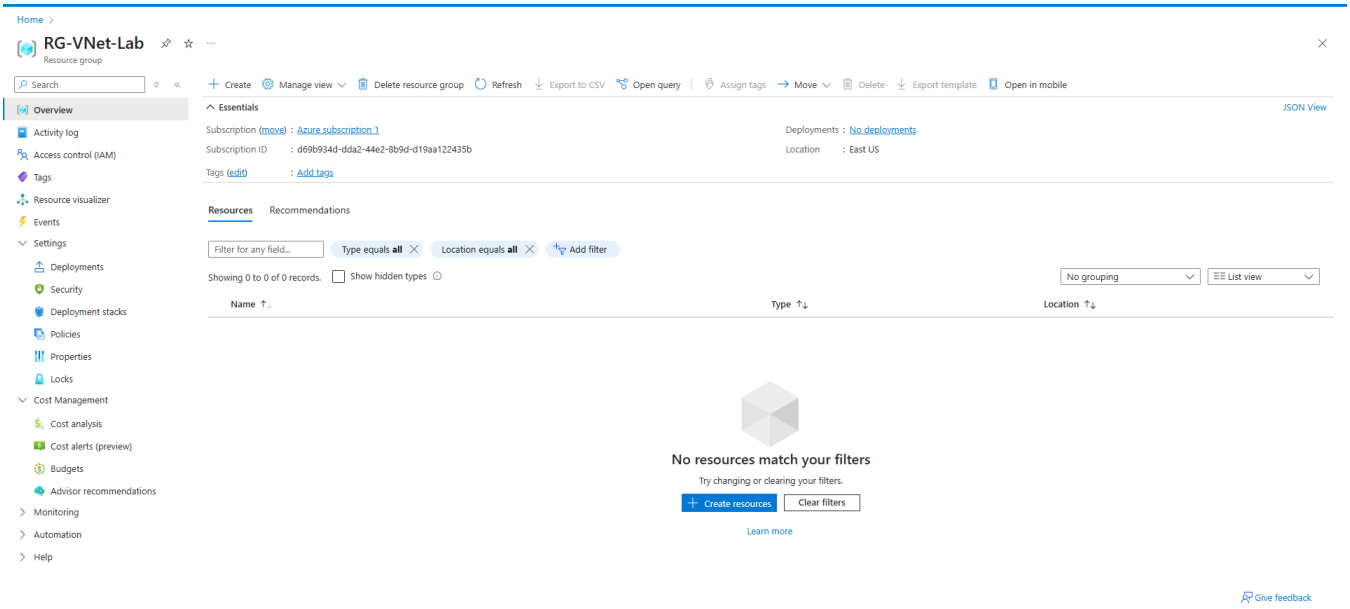
1. Navigate to Azure Portal:
    - Open the Azure Portal.
2. Create a Resource Group:

- In the left-hand menu, select Resource groups.
- Click on + Create at the top.
- Enter a name for the Resource Group (e.g., RG-VNet-Lab).
- Select a Region (for this example, choose any region like East US).
- Click Review + Create and then Create.

Purpose: Resource groups are used to organize related resources, including Virtual Networks, VMs, and other resources.




Microsoft Azure
Upgrade
Home
Create a resource group
Basics
Tags
Review + create
Automation Link
Basics
Subscription
Azure subscription 1
Resource group name
RG-VNet-Lab
Region
East US
Tags
None


Home
RG-VNet-Lab
Resource group
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Events
Settings
Deployments
Security
Deployment stacks
Policies
Properties
Locks
Cost Management
Cost analysis
Cost alerts (preview)
Budgets
Advisor recommendations
Monitoring
Automation
Help
Create
Manage view
Delete resource group
Refresh
Export to CSV
Open query
Assign tags
Move
Delete
Export template
Open in mobile
Essentials
JSON View
Subscription (move) : Azure subscription 1
Subscription ID : d69b934d-dda2-44e2-8b9d-d19aa122435b
Tags (edit) : Add tags
Deployments : No deployments
Location : East US
Resources
Recommendations
Filter for any field...
Type equals all
Location equals all
Add filter
Showing 0 to 0 of 0 records.
Show hidden types
No grouping
List view
Name
Type
Location
No resources match your filters
Try changing or clearing your filters.
Create resources
Clear filters
Learn more
Give feedback

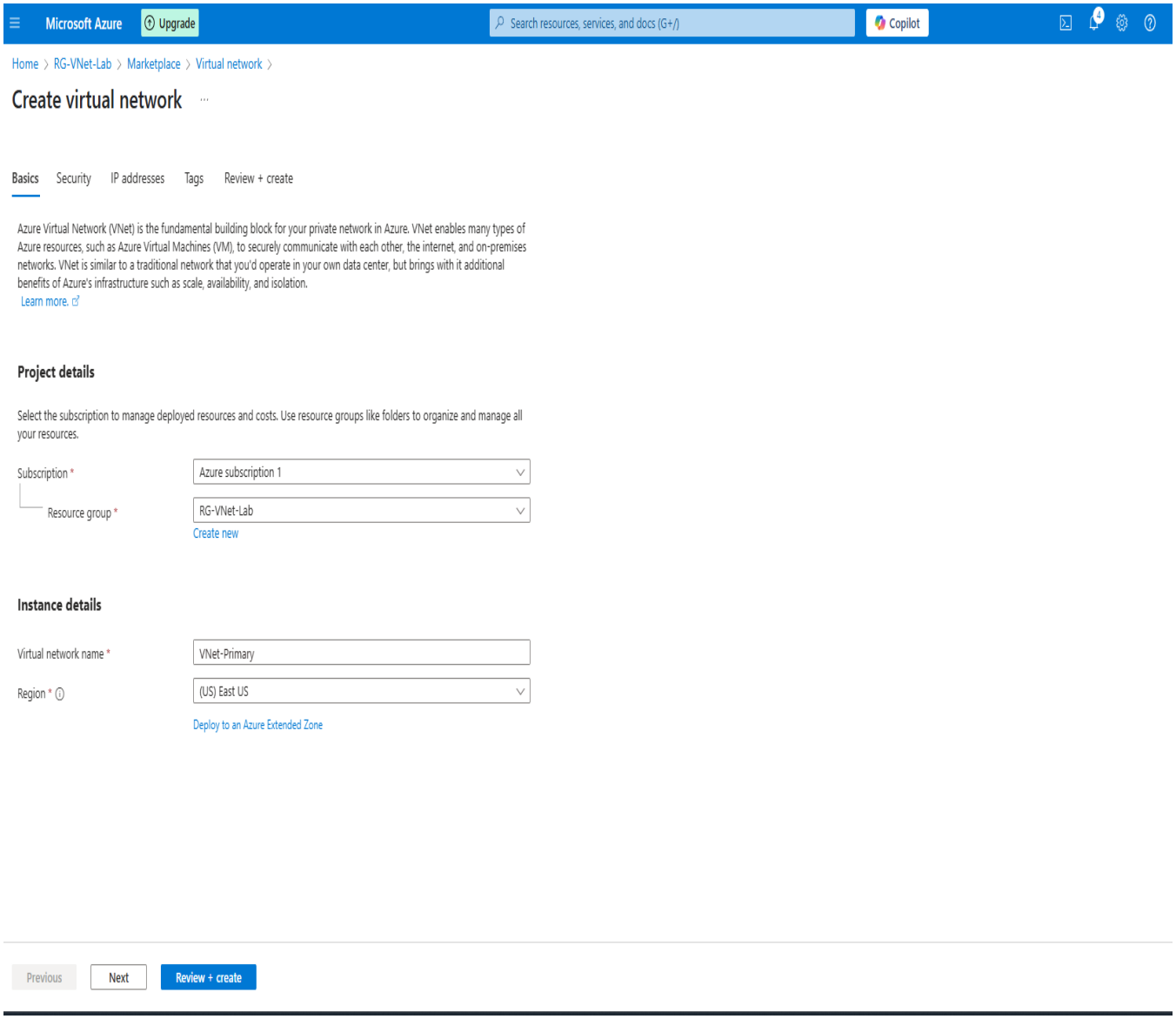
Step 2: Create the First Virtual Network (VNet) and Subnets

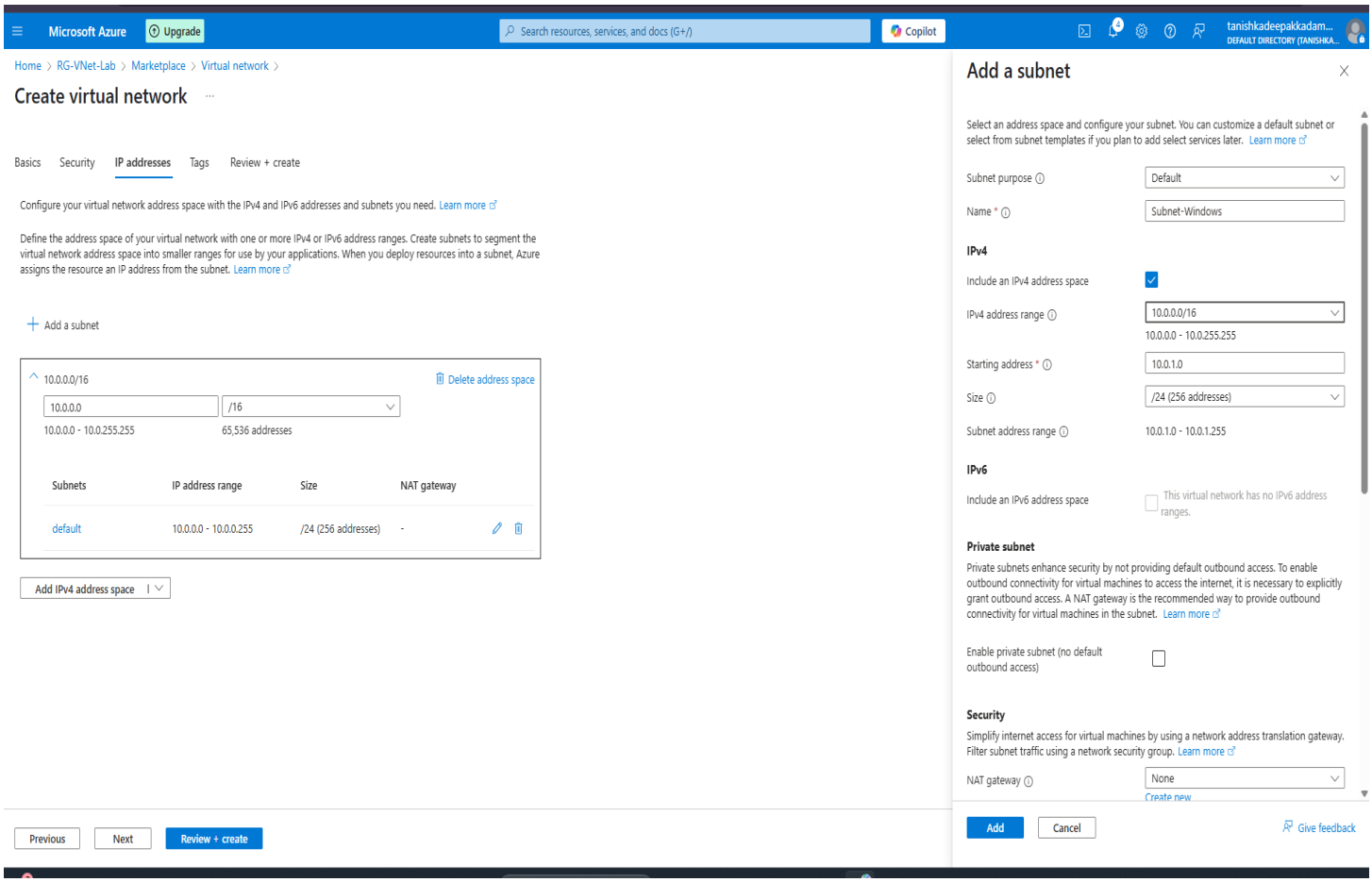
1. Navigate to Virtual Networks:
    - In the Azure Portal, click on Create a resource.
    - Search for Virtual Network, then click on Create.
2. Configure VNet:
    - Subscription: Select your subscription.
    - Resource Group: Select the one created in Step 1 (RG-VNet-Lab).
    - Name: VNet-Primary
    - Region: Choose the same region as the resource group (e.g., East US).
    - Address space: 10.0.0.0/16 (this will allow for up to 65,536 IP addresses).
3. Add Subnets:
    - Scroll down to the Subnets section and click + Add subnet.
        - Subnet Name: Subnet-Windows
        - Subnet Address: 10.0.1.0/24 (for up to 256 addresses)
    - Click + Add subnet again for the second subnet:
        - Subnet Name: Subnet-Linux
        - Subnet Address: 10.0.2.0/24 (for up to 256 addresses)
4. Review and Create:
    - Click Review + Create and then Create.

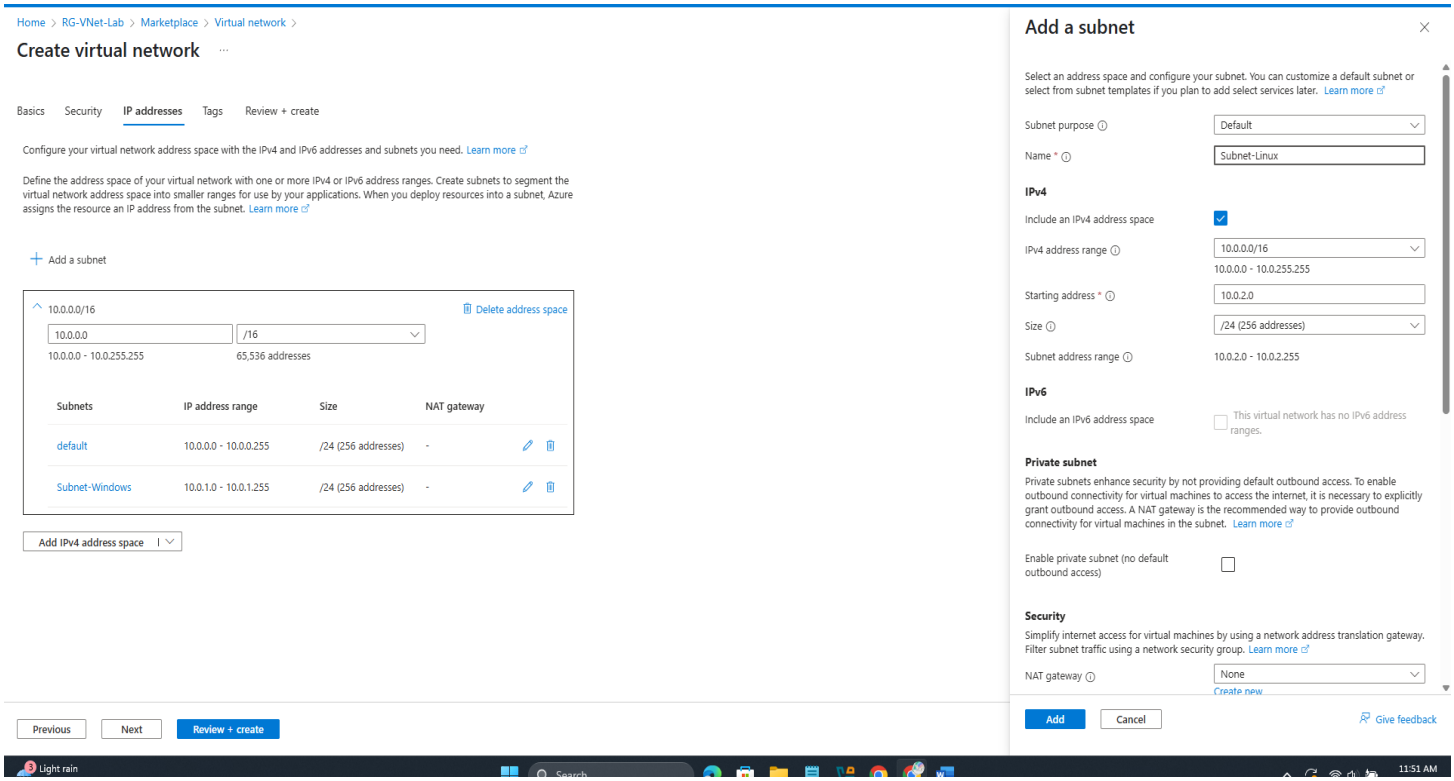
Explanation:

- This creates a Virtual Network (VNet) with two subnets: one for Windows VMs (Subnet-Windows) and one for Linux VMs (Subnet-Linux).

- The address range 10.0.0.0/16 is large enough to accommodate several subnets.




Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
tanishkadeepakkadam...
DEFAULT DIRECTORY (TANISHKA...
Home > RG-VNet-Lab > Marketplace > Virtual network >
Create virtual network
Basics Security IP addresses Tags Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. 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. Learn more
Add a subnet
10.0.0.0/16
Delete address space
10.0.0.0
/16
10.0.0.0 - 10.0.255.255
65,536 addresses
Subnets
IP address range
Size
NAT gateway
default
10.0.0.0 - 10.0.0.255
/24 (256 addresses)
-
Add IPv4 address space
Previous
Next
Review + create
Add a subnet
Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more
Subnet purpose
Default
Name *
Subnet-Windows
IPv4
Include an IPv4 address space
IPv4 address range
10.0.0.0/16
10.0.0.0 - 10.0.255.255
Starting address *
10.0.1.0
Size
/24 (256 addresses)
Subnet address range
10.0.1.0 - 10.0.1.255
IPv6
Include an IPv6 address space
This virtual network has no IPv6 address ranges.
Private subnet
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more
Enable private subnet (no default outbound access)
Security
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more
NAT gateway
None
Create new
Add
Cancel
Give feedback


Home > RG-VNet-Lab > Marketplace > Virtual network >
Create virtual network
Basics Security IP addresses Tags Review + create
Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. 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. Learn more
Add a subnet
10.0.0.0/16
Delete address space
10.0.0.0
/16
10.0.0.0 - 10.0.255.255
65,536 addresses
Subnets
IP address range
Size
NAT gateway
default
10.0.0.0 - 10.0.0.255
/24 (256 addresses)
-
Subnet-Windows
10.0.1.0 - 10.0.1.255
/24 (256 addresses)
-
Add IPv4 address space
Previous
Next
Review + create
Add a subnet
Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more
Subnet purpose
Default
Name *
Subnet-Linux
IPv4
Include an IPv4 address space
IPv4 address range
10.0.0.0/16
10.0.0.0 - 10.0.255.255
Starting address *
10.0.2.0
Size
/24 (256 addresses)
Subnet address range
10.0.2.0 - 10.0.2.255
IPv6
Include an IPv6 address space
This virtual network has no IPv6 address ranges.
Private subnet
Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more
Enable private subnet (no default outbound access)
Security
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more
NAT gateway
None
Create new
Add
Cancel
Give feedback
Light rain
11:51 AM

Home > RG-VNet-Lab > Marketplace > Virtual network >

Create virtual network ...

Basics | Security | **IP addresses** | Tags | Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. Learn more

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. 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. Learn more

+ Add a subnet

10.0.0.0/16 Delete address space

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-
Subnet-Windows	10.0.1.0 - 10.0.1.255	/24 (256 addresses)	-
Subnet-Linux	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

Add IPv4 address space

Previous Next Review + create

3 Light rain

Step 3: Deploy VMs in Each Subnet

Create Windows VM in Subnet-Windows:

1. Navigate to Virtual Machines:
    - In the Azure Portal, click on Create a resource.
    - Search for Virtual Machine and select Create.
2. Configure Windows VM:
    - Subscription: Select your subscription.
    - Resource Group: Select RG-VNet-Lab.
    - VM Name: WinVM
    - Region: Choose the same region as before (e.g., East US).
    - Image: Choose Windows Server 2022.
    - Size: Select B2s (Standard).
    - Authentication Type: Choose Password and provide username (e.g., admin) and a strong password.
    - Network Interface: Choose VNet-Primary → Subnet-Windows.
    - Public IP: Select None (for private communication within the VNet).
3. Create the VM:
    - Review the settings and click Create.

Create Linux VM in Subnet-Linux:

1. Navigate to Virtual Machines:
    - In the Azure Portal, click on Create a resource.
    - Search for Virtual Machine and select Create.
2. Configure Linux VM:
    - Subscription: Select your subscription.

- Resource Group: Select RG-VNet-Lab.
- VM Name: LinuxVM
- Region: Choose the same region (e.g., East US).
- Image: Choose Ubuntu 20.04.
- Size: Select B1s (Standard).
- Authentication Type: Choose SSH public key or Password.
- Network Interface: Choose VNet-Primary → Subnet-Linux.
- Public IP: Select None (for private communication within the VNet).

3. Create the VM:
    - Review the settings and click Create.

Explanation:

- These steps create two VMs: WinVM in Subnet-Windows and LinuxVM in Subnet-Linux under the same VNet. They can now communicate within the VNet using private IPs.

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Changing Basic options may reset selections you have made. Review all options prior to creating the 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

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

Project details

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

Subscription * : Azure subscription 1

Resource group * : RG-VNet-Lab

Create new

Instance details

Virtual machine name * : WinVM

Region * : (US) East US

Availability options : Availability zone

Zone options :

- (•) Self-selected zone
  Choose up to 3 availability zones, one VM per zone
- ( ) Azure-selected zone (Preview)
  Let Azure assign the best zone for your needs

Using an Azure-selected zone is not supported in region 'East US'.

< Previous | Next : Disks > | Review + create

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Changing Basic options may reset selections you have made. Review all options prior to creating the 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

You are in the free trial period. Costs associated with this VM can be covered by any remaining credits on your subscription. Learn more

Size * : Standard_B1s - 1 vcpu, 1 GiB memory (US$10.22/month) (free services eligib...
See all sizes

Enable Hibernation : Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Username * : Admins

Password * : ••••••••••••

Confirm password * : ••••••••••••

Inbound port rules

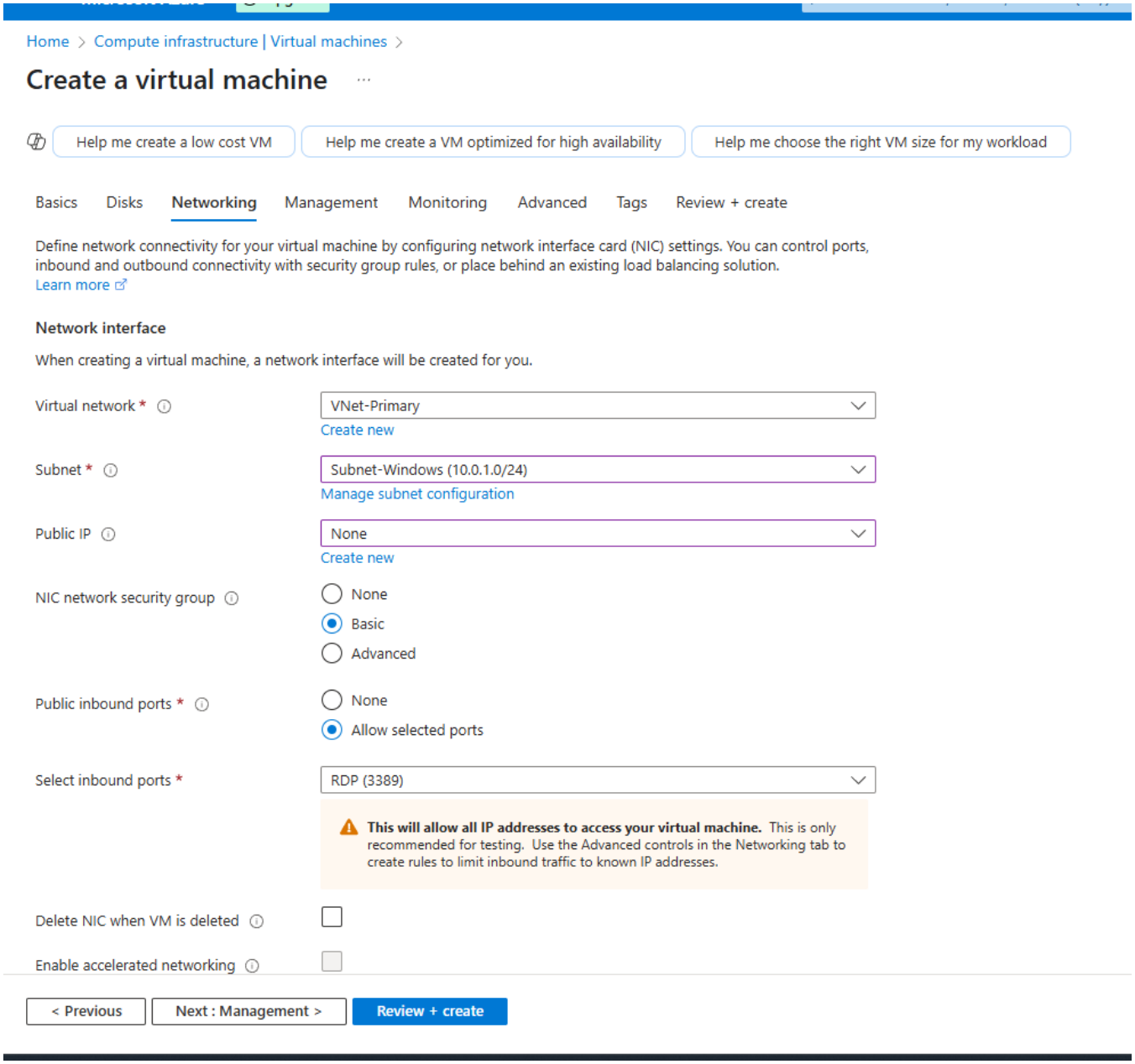
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * : None / Allow selected ports

Select inbound ports * : RDP (3389)

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.

< 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 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 *
VNet-Primary
Create new
Subnet *
Subnet-Windows (10.0.1.0/24)
Manage subnet configuration
Public IP
None
Create new
NIC network security group
None
Basic
Advanced
Public inbound ports *
None
Allow selected ports
Select inbound ports *
RDP (3389)
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.
Delete NIC when VM is deleted
Enable accelerated networking
< Previous
Next : Management >
Review + create

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Validation passed

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 workl

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

You have set RDP port(s) open to the internet. This is only recommended for testing. If you want to change this setting, go back to Basics tab.

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Virtual machine name	WinVM
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Username	Admins
Public inbound ports	RDP

< Previous | Next > | Create

27°C
Partly sunny

Search

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Validation passed

Help me create a low cost VM | Help me create a VM optimized for high availability | Help me choose the ri

Basics

Subscription	Azure subscription 1
Resource group	RG-VNet-Lab
Virtual machine name	LinuxVM
Region	East US
Availability options	Availability zone
Zone options	Self-selected zone
Availability zone	1
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Ubuntu Server 24.04 LTS - Gen2
VM architecture	x64
Size	Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation	No
Authentication type	SSH public key
Username	azureuser
SSH Key format	RSA
Key pair name	Password
Public inbound ports	SSH
Azure Spot	No

Disks

OS disk size	Image default

< Previous | Next > | Create

Home > Compute infrastructure | Virtual machines >

Create a virtual machine ...

Validation passed

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 workl

OS disk type	Premium SSD LRS
Use managed disks	Yes
Delete OS disk with VM	Enabled
Ephemeral OS disk	No

Networking

Virtual network	VNet-Primary
Subnet	Subnet-Linux (10.0.2.0/24)
Public IP	None
Accelerated networking	Off
Place this virtual machine behind an existing load balancing solution?	No
Delete NIC when VM is deleted	Disabled

Management

Microsoft Defender for Cloud	None
System assigned managed identity	Off
Login with Microsoft Entra ID	Off
Auto-shutdown	Off
Enable periodic assessment	Off
Enable hotpatch	Off
Patch orchestration options	Image Default

Monitoring

Alerts	Off
Boot diagnostics	On

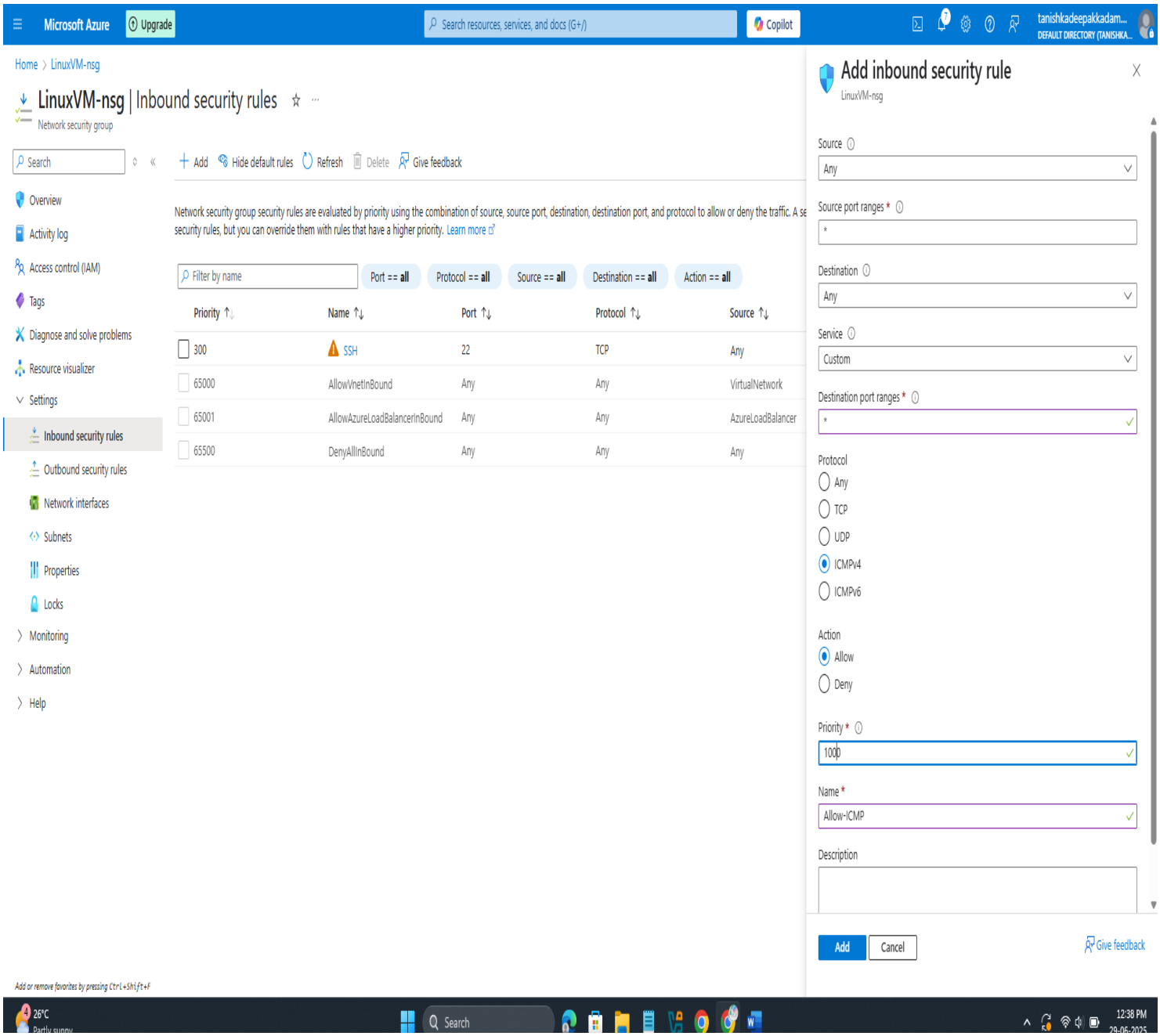
< Previous | Next > | Create

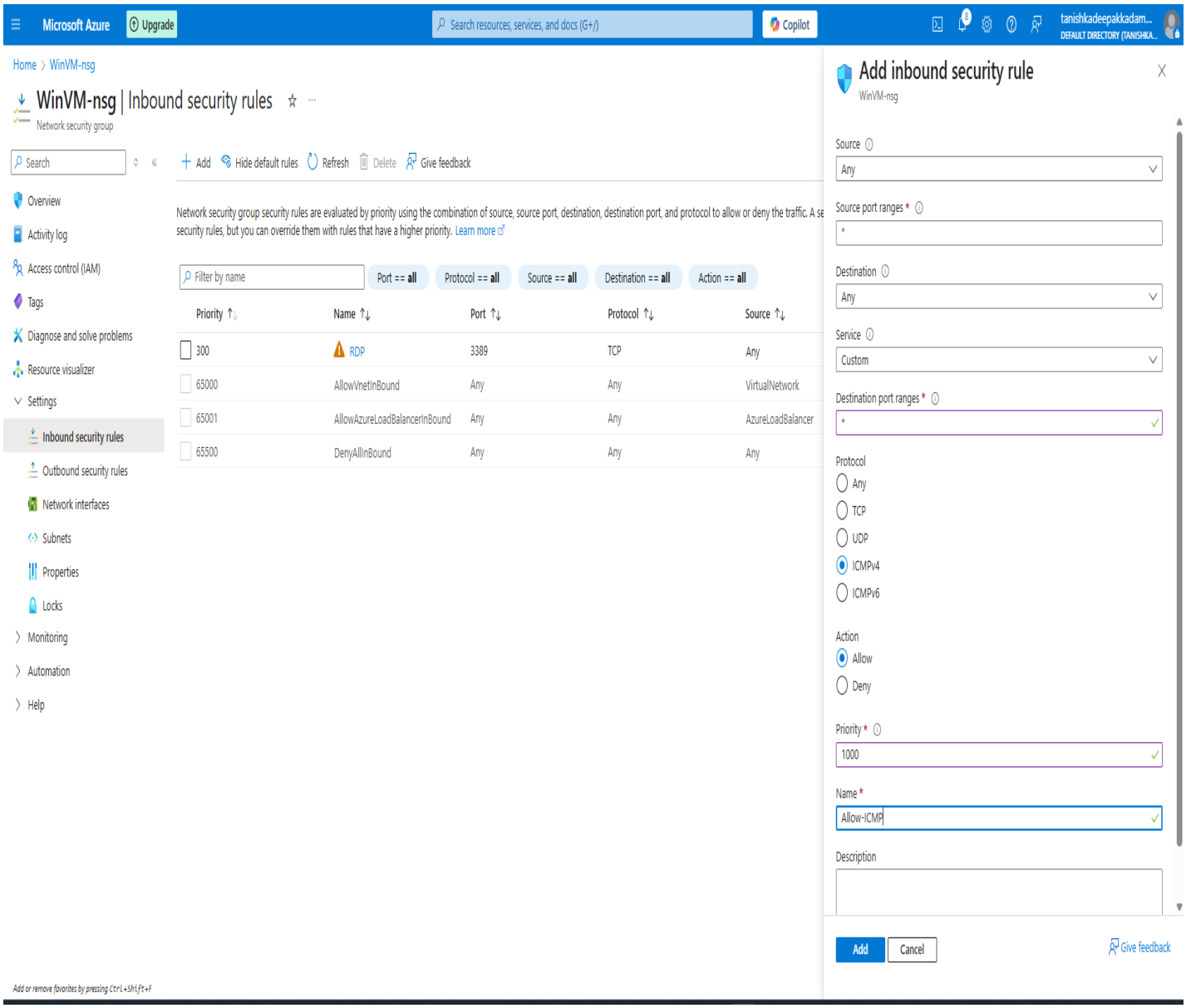
Step 4: Configure Network Security Groups (NSGs) to Allow ICMP (Ping)

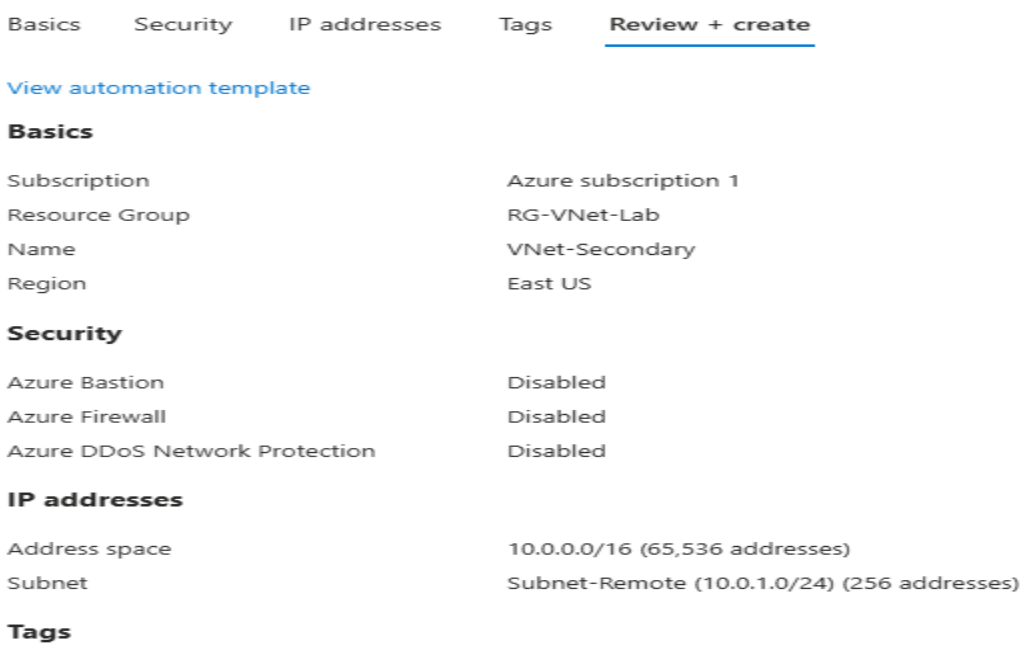
1. Navigate to Network Security Groups:
    - In the Azure Portal, click on Create a resource.
    - Search for Network Security Group and select Create.
2. Configure NSGs:
    - For each subnet (Windows and Linux), create a Network Security Group (NSG) and associate it with the respective subnet.
3. Add an Inbound Rule for ICMP:
    - Go to Inbound security rules.
    - Click on + Add to create a new rule:
        - Source: Any
        - Source port ranges: *
        - Destination: Any
        - Destination port ranges: *
        - Protocol: ICMP
        - Action: Allow
        - Priority: 1000
        - Name: Allow-ICMP
4. Apply NSG to Subnets:
    - Go to Virtual Networks → Select VNet-Primary → Subnets.
    - Apply the newly created NSGs to Subnet-Windows and Subnet-Linux.

Explanation:

- These steps configure the NSGs to allow ICMP (ping) traffic to ensure that VMs can communicate via ping.


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
tanishkadeepakkadam...
DEFAULT DIRECTORY (TANISHKA...
Home > LinuxVM-nsg
LinuxVM-nsg | Inbound security rules
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add
Hide default rules
Refresh
Delete
Give feedback
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A se
security rules, but you can override them with rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
300
SSH
22
TCP
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwork
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
65500
DenyAllInBound
Any
Any
Any
Add or remove favorites by pressing Ctrl+Shift+F
Add inbound security rule
LinuxVM-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMPv4
ICMPv6
Action
Allow
Deny
Priority *
1000
Name *
Allow-ICMP
Description
Add
Cancel
Give feedback
26°C
Partly sunny
Search
12:38 PM
29-06-2025


Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
tanishkadeepakkadam...
DEFAULT DIRECTORY (TANISHKA...
Home > WinVM-nsg
WinVM-nsg | Inbound security rules
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add
Hide default rules
Refresh
Delete
Give feedback
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A se
security rules, but you can override them with rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
300
RDP
3389
TCP
Any
65000
AllowVnetInBound
Any
Any
VirtualNetwork
65001
AllowAzureLoadBalancerInBound
Any
Any
AzureLoadBalancer
65500
DenyAllInBound
Any
Any
Any
Add or remove favorites by pressing Ctrl+Shift+F
Add inbound security rule
WinVM-nsg
Source
Any
Source port ranges *
*
Destination
Any
Service
Custom
Destination port ranges *
*
Protocol
Any
TCP
UDP
ICMPv4
ICMPv6
Action
Allow
Deny
Priority *
1000
Name *
Allow-ICMP
Description
Add
Cancel
Give feedback



Step 5: Verify Internal Connectivity

1. Test Ping Between VMs:
    - Windows VM (RDP): RDP into the WinVM (using Remote Desktop Protocol).
        - Open Command Prompt and type ping <Private IP of LinuxVM>.
    - Linux VM (SSH): SSH into the LinuxVM (using SSH client or Cloud Shell).
        - Open terminal and type ping <Private IP of WinVM>.
2. Check Connectivity:

- Ensure both VMs can successfully ping each other.

Step 6: Create Second Virtual Network (VNet2) and Subnet

1. Navigate to Virtual Networks:
    - In the Azure Portal, click on Create a resource.
    - Search for Virtual Network and click Create.
2. Configure VNet2:
    - Subscription: Select your subscription.
    - Resource Group: Select RG-VNet-Lab.
    - Name: VNet-Secondary
    - Region: Choose the same region as VNet-Primary (e.g., East US).
    - Address space: 10.1.0.0/16.
3. Create a Subnet in VNet2:
    - Click on + Add subnet.
    - Subnet Name: Subnet-Remote
    - Subnet Address: 10.1.1.0/24 (for up to 256 addresses).
    - Click Create.

Explanation:

- This creates VNet-Secondary with a subnet (Subnet-Remote) where you can add additional VMs.

Step 7: Configure VNet Peering

1. Peer VNet-Primary with VNet-Secondary:
    - In the Azure Portal, go to Virtual Networks → VNet-Primary.

- Under Settings, click Peerings → + Add.
  - Name: PrimaryToSecondary
  - Peering Link: Select VNet-Secondary.
  - Traffic: Enable traffic in both directions (from VNet-Primary to VNet-Secondary and vice versa).
- Click OK to create the peering.

2. Configure Peering on VNet-Secondary:
   - Go to Virtual Networks → VNet-Secondary → Peerings → + Add.
     - Name: SecondaryToPrimary
     - Peering Link: Select VNet-Primary.
     - Enable traffic in both directions.
   - Click OK to confirm.

Explanation:

- This establishes a peering connection between VNet-Primary and VNet-Secondary, allowing traffic to flow between the two VNets.

Step 8: Verify Cross-VNet Connectivity

1. Test Ping Between VNets:
   - From the Windows VM in VNet-Primary, ping the private IP of a VM in VNet-Secondary (or create a new VM in VNet-Secondary).
   - From the Linux VM in VNet-Primary, ping the private IP of a VM in VNet-Secondary.
2. Check Peering Status:
   - Ensure that the peering status is Connected and that traffic flows as expected.