

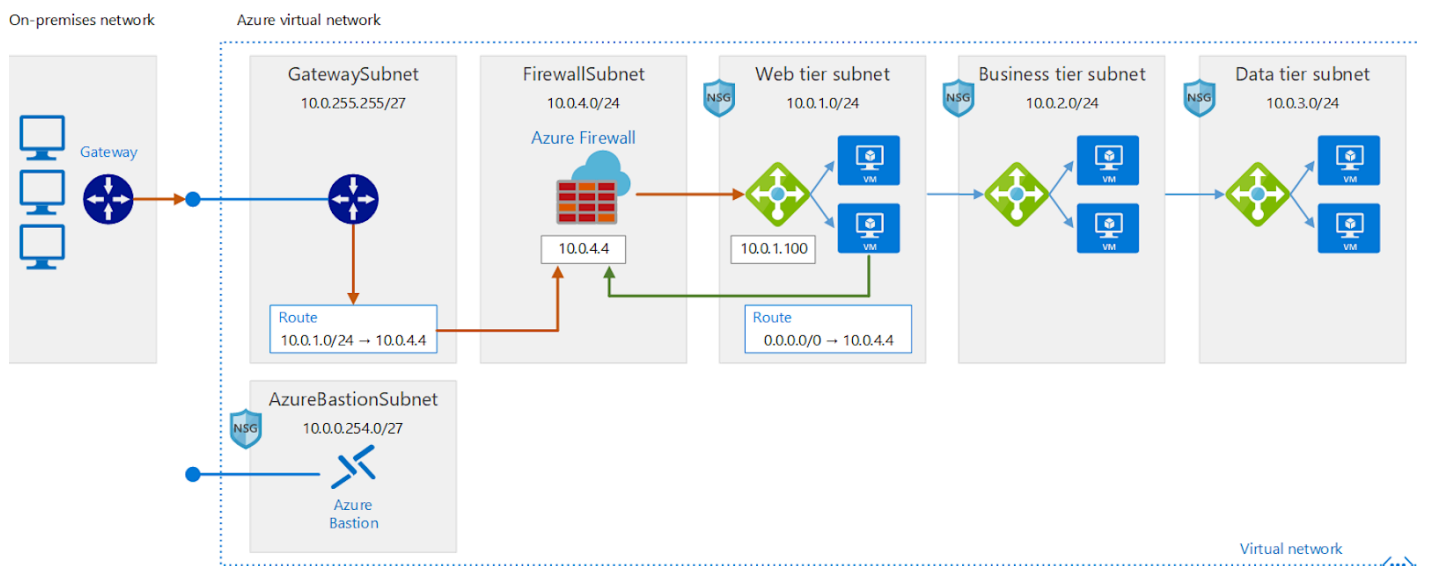
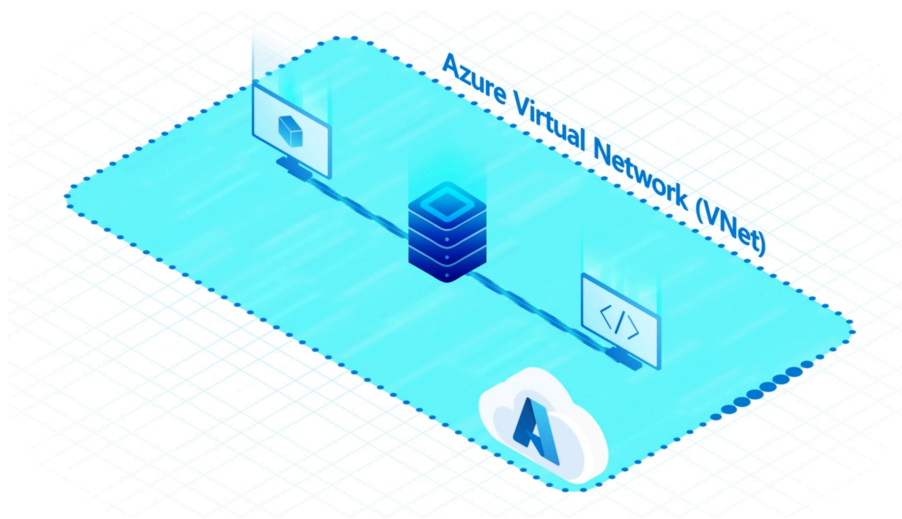
CIDR Ranges of a VNet, Subnet & VNet Peering

1. Overview

In the Azure ecosystem, **Virtual Networks (VNETs)** represent the core infrastructure layer that enables cloud-based applications and services to communicate securely and efficiently. VNETs act as a logical, isolated section of the Azure cloud, scoped to a specific subscription and region, where resources such as Virtual Machines (VMs), Application Gateways, Load Balancers, Databases, and more can be deployed and connected.

A VNet provides the same networking functionalities found in an on-premises network, such as IP addressing, name resolution, routing, and security, but with the elasticity, scalability, and cost efficiency of the cloud. With VNETs, organizations can build highly customizable network topologies tailored to specific workloads, while maintaining complete control over traffic flow and security boundaries.

VNETs are pivotal in designing hybrid and multi-cloud architectures. They support VPN Gateways and ExpressRoute connections to securely bridge on-premises environments with cloud deployments. Moreover, VNETs can be interconnected using VNet Peering, enabling a mesh of secure, high-performance communication channels between isolated environments or across different regions.



2. CIDR Ranges in VNets and Subnets

2.1 What is CIDR?

CIDR (Classless Inter-Domain Routing) is a notation method for IP address allocation and routing. It replaces the older classful addressing scheme by allowing **variable-length subnet masks**. CIDR notation uses the format: `<IP_address>/<prefix_length>`

Example: 10.0.0.0/16

2.2 CIDR in Azure VNets

- VNets in Azure **must have a defined IP address space** in CIDR format.
- CIDR blocks can range from /8 to /29.
- A VNet can have multiple **non-overlapping** address spaces (useful for peering later).
- The address space should be chosen with future subnetting and peering in mind.

2.3 CIDR in Azure Subnets

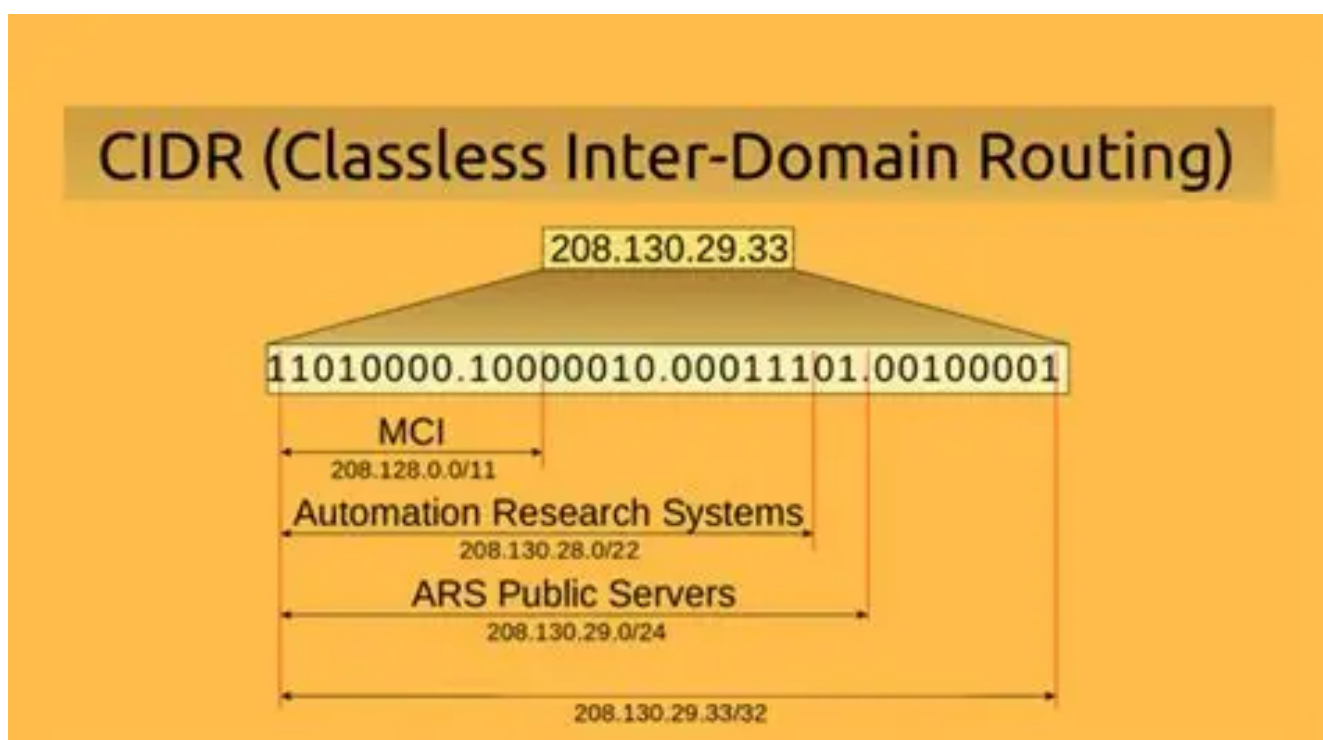
- Subnets are segments of a VNet's CIDR space.
- Each subnet requires a unique non-overlapping CIDR block within the VNet.
- Azure reserves the first four and the last IP address of each subnet, reducing usable IPs.

Example

VNet: 10.0.0.0/16

Subnet 1: 10.0.1.0/24

Subnet 2: 10.0.2.0/24



3. Subnet Architecture and Purpose

3.1 What is a Subnet?

A **Subnet**, short for *subnetwork*, is a logically defined segment of an Azure Virtual Network (VNet) that helps in organizing, isolating, and securing resources. Subnetting enables fine-grained control over traffic routing, security, and IP address management.

In Azure, a subnet is defined by a **CIDR block** that is a subset of the parent VNet's address space. All resources deployed within a subnet receive an IP address from that range.

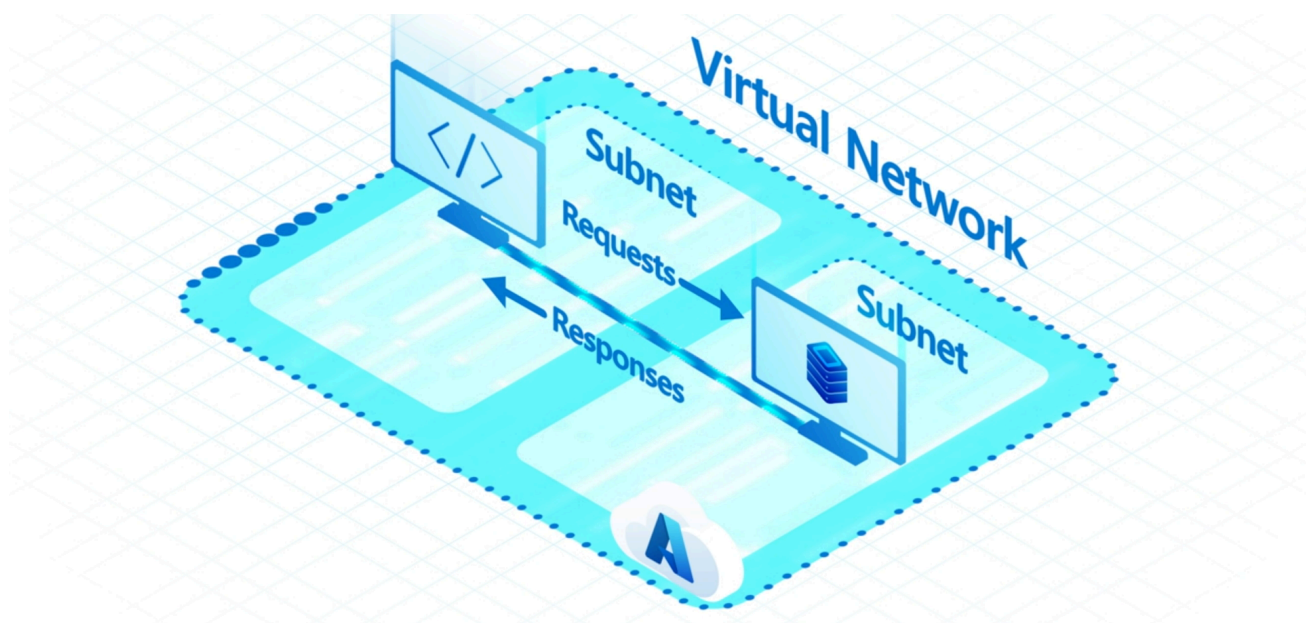
Key Capabilities of Subnets:

- **Logical Isolation:** Each subnet can represent a unique tier (e.g., web, app, database) or workload type, enhancing clarity and manageability.
- **Security Enforcement:** Apply Network Security Groups (NSGs) to subnets to control inbound and outbound traffic at Layer 3/4.
- **Custom Routing:** Attach User-Defined Routes (UDRs) to subnets for traffic redirection, inspection, or firewall enforcement.
- **Policy Enforcement:** Deploy Azure Policies at the subnet level to enforce resource tagging, allowed VM sizes, etc.
- **Network Virtual Appliances (NVAs):** Subnets can host custom routing devices for firewall, NAT, or WAN optimization.

3.2 Types of Subnets

While Azure doesn't classify subnets explicitly, they can be designed based on purpose:

- **Front-end subnet:** Hosts web servers or public-facing apps.
- **Back-end subnet:** Contains databases or internal services.
- **Gateway subnet:** Required for VPN Gateway or ExpressRoute connections.
- **Bastion subnet:** Required for Azure Bastion service.



4. VNet Peering

Virtual Network (VNet) Peering in Azure enables seamless connectivity between two VNets, allowing virtual machines and services in each network to communicate over private IP addresses. This is achieved through Azure's high-speed, low-latency backbone network, not the public internet. Peering abstracts the complexity of VPN or gateway configurations and provides a straightforward method for enabling secure cross-network communication.

Peered VNets:

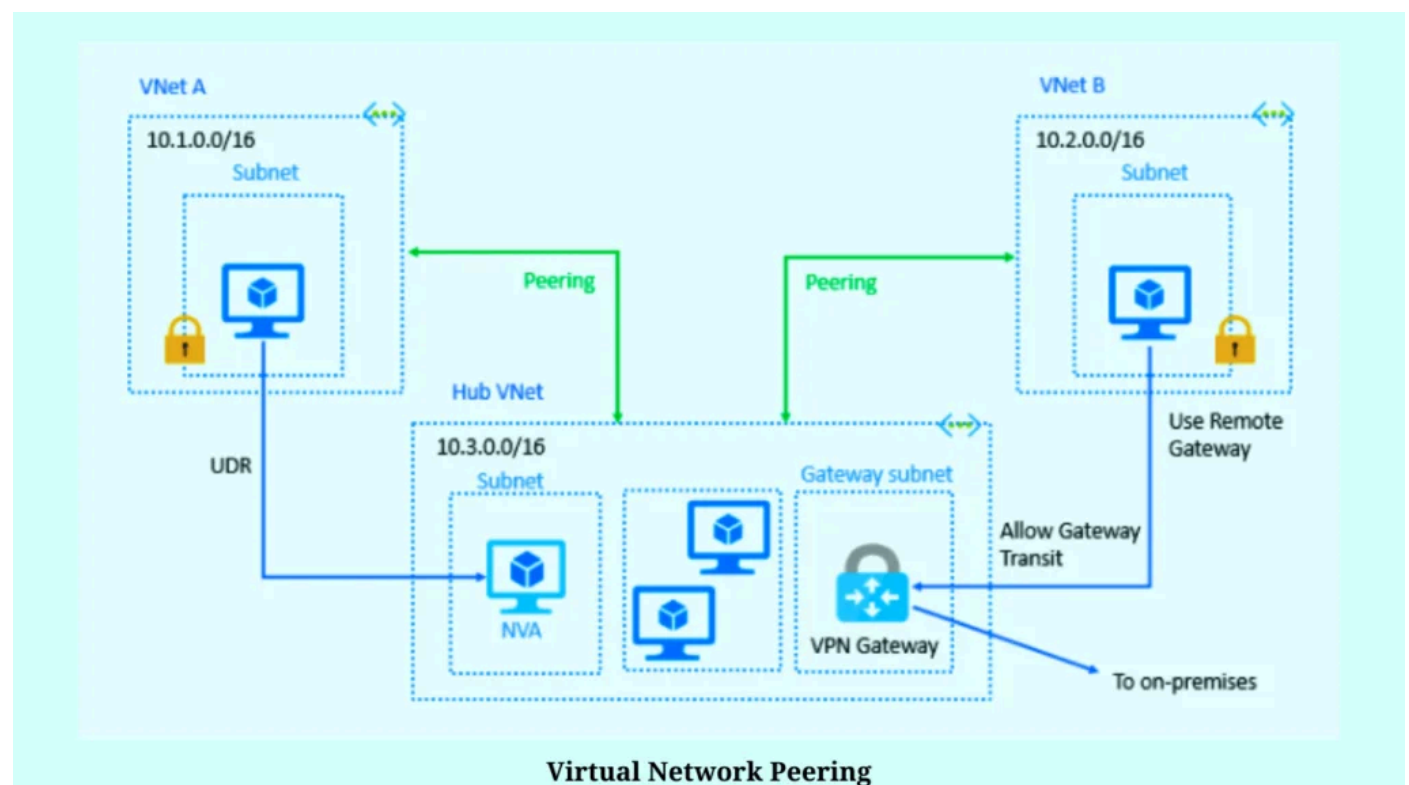
- Can be in **same or different regions**
- Must have **non-overlapping address spaces**
- Can **forward traffic** between them if explicitly configured

Types of VNet Peering

Type	Description
Intra-Region Peering	Connects two VNets in the same Azure region
Global VNet Peering	Connects VNets across different regions

Key Features

- **No public internet involvement:** Traffic stays on Azure's private backbone.
- **Low-latency & high-speed:** No bottlenecks due to NAT.
- **Transitive peering not supported:** You must manually peer each VNet that needs connectivity.
- **Network Security Group rules still apply:** Even if peered, explicit NSG rules are needed for communication.



5. Use Case: Deploying VNets, Subnets, and VMs with Peering for Cross-Network Communication

Objective Overview

To design and implement a secure, logically segmented Azure network infrastructure using Virtual Networks (VNets) and Subnets to simulate a real-world enterprise network topology. The goal is to deploy Linux-based Virtual Machines (VMs) in isolated subnets within a VNet, ensuring they can communicate with each other internally via private IPs. Additionally, establish VNet Peering between two separate VNets to enable cross-network communication without exposing resources to the public internet. This setup aims to demonstrate secure, scalable, and private intra-network and inter-network connectivity in Azure.

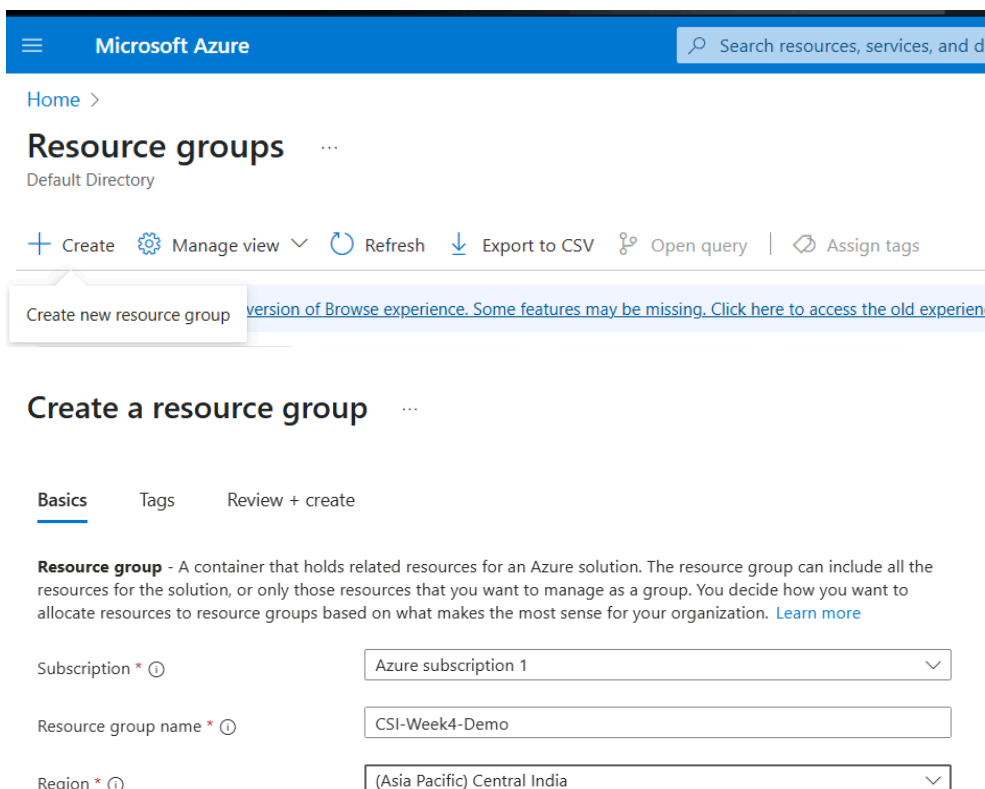
Specifically, we will:

- Create a Virtual Network (VNet1) with two subnets.
- Launch one Linux VM in Subnet-1 and one Windows VM in Subnet-2.
- Validate ping/ICMP connectivity between these VMs (within the same VNet).
- Create a second VNet (VNet2) in the same region with its own subnet and Linux VM.
- Establish VNet Peering between VNet1 and VNet2.
- Confirm cross-VNet communication by verifying ping between the VMs in both VNets.

Step-by-Step Implementation on Azure Portal

Step 1: Create a Resource Group

- Go to **Azure Portal > Resource Groups > Create**
- Provide a name and region.
- Click **Review + Create > Create**



Microsoft Azure

Search resources, services, and d

Home >

Resource groups

Default Directory

+ Create ⚙️ Manage view ▾ ↻ Refresh ⬇️ Export to CSV 🔗 Open query | 🏷️ Assign tags

Create new resource group [version of Browse experience. Some features may be missing. Click here to access the old experien](#)

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Subscription * ⓘ Azure subscription 1 ▾

Resource group name * ⓘ CSI-Week4-Demo

Region * ⓘ (Asia Pacific) Central India ▾

Step 2: Create VNet1 with Two Subnets

- Go to **Virtual Networks > Create**
- Define address space (e.g., `10.0.0.0/16`)
- Add two subnets:
 - Subnet-Linux (`10.0.1.0/24`)
 - Subnet-Windows (`10.0.2.0/24`)
- Click **Review + Create > Create**

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Network foundation | Virtual networks >

Create virtual network ...

Basics

Security

IP addresses

Tags

Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

[Learn more.](#)

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 *

CSI-Week4-Demo

[Create new](#)

Instance details

Virtual network name *

VNet1

Region * ⓘ

(US) East US

Previous

Next

Review + create

Edit 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 * ⓘ 10.0.1.0

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](#)

Save Cancel [Give feedback](#)

Add a subnet

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 * ⓘ 10.0.2.0

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

Add Cancel [Give feedback](#)

Step 3: Launch Linux VM in Subnet-Linux

- Go to **Virtual Machines > Create**
- Select Ubuntu image and place it in **Subnet-Linux** of **VNet1**
- Enable SSH access
- Deploy the VM

Microsoft Azure

Search resources, services, and d

Home >

Create a virtual machine

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me cho

Project details

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

Subscription * ⓘ Azure subscription 1

Resource group * ⓘ CSI-Week4-Demo
[Create new](#)

Instance details

Virtual machine name * ⓘ LinuxVM

Region * ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Security type ⓘ Loading...
[Configure security features](#)

Image * ⓘ Ubuntu Server 24.04 LTS - x64 Gen2 (free services eligible)
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64
☒ x64

< Previous Next : Disks > Review + create

Microsoft Azure

Search resources, services, and d

Home >

Create a virtual machine

Help me create a low cost VM

Help me create a VM optimized for high availability

Help me cho

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 co 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 * ⓘ VNet1
[Create new](#)

Subnet * ⓘ Subnet-Linux (10.0.1.0/24)
[Manage subnet configuration](#)

Public IP ⓘ Loading...
[Create new](#)

NIC network security group ⓘ ☐ None
☒ Basic
☐ Advanced

Public inbound ports * ⓘ ☐ None
☒ Allow selected ports

< Previous Next : Management > Review + create

Step 4: Launch Windows VM in Subnet-Windows

- Create a new VM using Windows Server image
- Place it in **Subnet-Windows** of **VNet1**
- Enable RDP access
- Add an NSG rule to allow **ICMP** (ping)

Microsoft Azure

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

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 * CSI-Week4-Demo

Instance details

Virtual machine name * WindowsVM

Region * (US) East US

Availability options No infrastructure redundancy required

Security type Standard

Image * Windows Server 2022 Datacenter - x64 Gen1 (free services eligible)

There is a generation 2 version of this image available which has higher feature compatibility. Click here to swap to the generation 2 version

< Previous Next > Disks Review + create

Microsoft Azure

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

Basic options

Ephemeral OS disk No

Networking

Virtual network VNet1

Subnet Subnet-Windows (10.0.2.0/24)

Public IP (new) WindowsVM-ip

Accelerated networking Off

Place this virtual machine behind an existing load balancing solution? No

Delete public IP and NIC when VM is deleted Disabled

Management

Microsoft Defender for Cloud Basic (free)

System assigned managed identity Off

Login with Microsoft Entra ID Off

Auto-shutdown Off

Backup Disabled

Enable periodic assessment Off

< Previous Next > Create

Step 5: Enable ICMP (Ping) Between VMs

- Add custom inbound NSG rule to both VMs:
 - Protocol: ICMP
 - Source: Any
 - Action: Allow

Search resources, services, and docs (G+/)

Copilot

ayush030503@gmail.com

LinuxVM | Network settings

Virtual machine

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Connect Networking

Network settings

Load balancing Application security groups Network manager

Settings Availability + scale Security Backup + disaster recovery Operations Monitoring Automation Help

Private IP address 10.0.1.4

Admin security rules 0 (Configure)

Rules Collapse all

Network security group LinuxVM-nsg

Impacts 0 subnets, 1 network interface

Search rules

Priority 1 Name

Inbound port rules (4)

300 SSH

65000 AllowVne

65001 AllowAzu

65500 DenyAllI

Outbound port rules (3)

Add inbound security rule

Source Any

Source port ranges *

Destination Any

Service Custom

Destination port ranges * 3389

Protocol Any

TCP

UDP

ICMPv4

ICMPv6

Action Allow

Deny

Priority * 1000

Name * AllowRDP

Add Cancel

Add inbound security rule

Source Any

Source port ranges *

Destination Any

Service Custom

Destination port ranges * *

Protocol Any

TCP

UDP

ICMPv4

ICMPv6

Action Allow

Deny

Priority * 1010

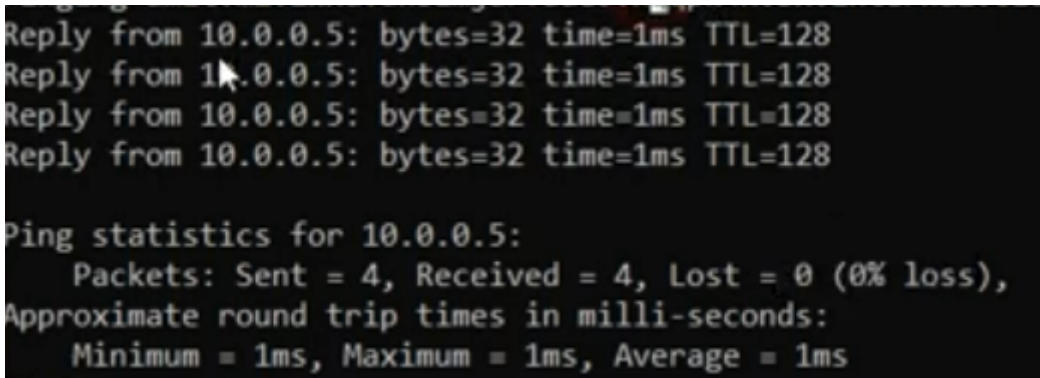
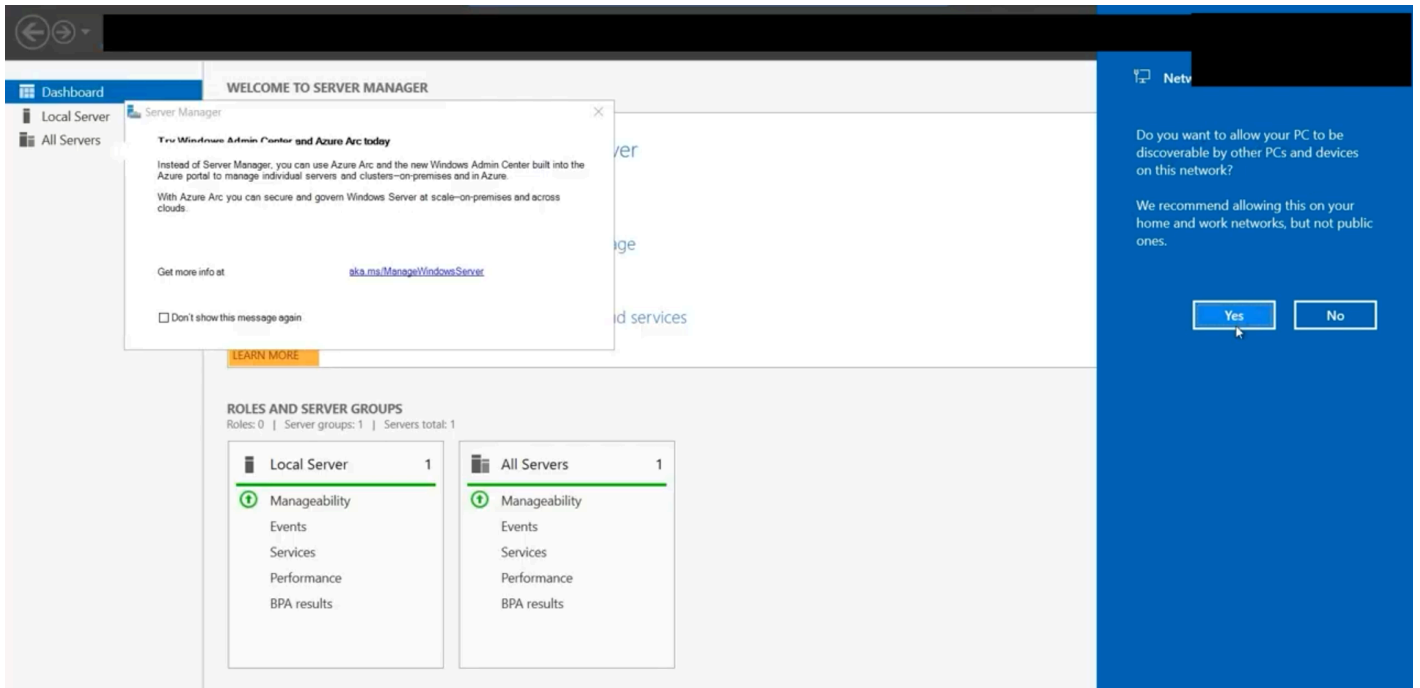
Name * AllowICMP

Add Cancel

Give feedback

Step 6: Test Intra-VNet Communication

- SSH into Linux VM and ping Windows VM, use `ping <WindowsVM Private IP>`
- Or RDP into Windows VM and ping Linux VM
- Confirm successful ping response



Step 7: Create VNet2 and a Linux VM

- Create **VNet2** with a non-overlapping address space (e.g., `10.1.0.0/16`)
- Add a subnet (e.g., `10.1.1.0/24`)
- Launch a **Linux VM** in this subnet
- Enable SSH and ICMP via NSG

LinuxVM2
Virtual machine

Search

Help me copy this VM in any region

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

Connect

Start

Restart

Stop

Hibernate

Capture

Delete

Essentials

JSON View

Resource group (move) : [CSI-Week4-Demo](#)
Status : Running
Location : East US
Subscription (move) : [Azure subscription 1](#)
Subscription ID : 3251632f-6d31-406a-aca0-f03541ebe8f4
Operating system : Linux (ubuntu 24.04)
Size : Standard D2s v3 (2 vcpus, 8 GiB memory)
Public IP address : [172.191.129.50](#)
Virtual network/subnet : [VNet2/Subnet-Linux-2](#)
DNS name : [Not configured](#)
Health state : -
Time created : 29/6/2025, 11:12 am UTC
Tags (edit) : [Add tags](#)

Step 8: Configure VNet Peering

- In **VNet1**, create peering to **VNet2**
- In **VNet2**, create peering to **VNet1**
- Enable traffic in both directions

Microsoft Azure

Upgrade

Search resources, services, and docs (G+/)

Copilot

ayush030503@gmail.com

Home > VNet1

VNet1 | Peerings

Virtual network

Search

Add

Refresh

Export to CSV

Delete

Sync

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. [Learn more](#)

Filter by name...

Showing all 0 items

Name	Peering sync status	Peering state	Remo...	Virtu...	Cross-tenant
Add a peering to get started					

Microsoft Azure

Upgrade

Search resources, services, and docs (G+/)

Copilot

ayush030503@gmail.com

Home > VNet1

VNet1 | Peerings

Virtual network

Search

Add

Refresh

Export to CSV

Delete

Sync

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

Address space

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. The virtual networks appear as one for connectivity purposes. [Learn more](#)

Filter by name...

Showing all 1 items

Name	Peering sync status	Peering state	Remote virtual network name	Virtual network gateway or route server	Cross-tenant
VNet1-to-VNet2	Fully Synchronized	Connected	VNet2	Disabled	No

Step 9: Test Cross-VNet Communication

- SSH into either Linux VM and ping the other's private IP
 - Confirm connectivity

Home > Compute infrastructure

Compute infrastructure | Virtual machines

Search

Overview

All resources

Infrastructure

Virtual machines

Virtual machines Get started

Name ↑	Subscription	Resource Group	Location	Status	Operating syst...	Size	Public IP addre...	Disks
LinuxVM1	Azure subscript...	CSI-Week4-De...	East US	Running	Linux	Standard_B1s	172.191.118.40	1
LinuxVm2	Azure subscript...	CSI-Week4-De...	East US	Running	Linux	Standard_B1s	172.203.164.145	1

Switch to PowerShell Restart Manage files New session Editor Web preview Settings Help

```
$ ping -c 4 172.203.164.145
PING 172.203.164.145 (172.203.164.145) 56(84) bytes of data.
64 bytes from 172.203.164.145: icmp_seq=1 ttl=58 time=1.56 ms
64 bytes from 172.203.164.145: icmp_seq=2 ttl=58 time=1.66 ms
64 bytes from 172.203.164.145: icmp_seq=3 ttl=58 time=1.73 ms
64 bytes from 172.203.164.145: icmp_seq=4 ttl=58 time=1.64 ms

--- 172.203.164.145 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.557/1.646/1.727/0.060 ms
$
```

```
$ ping -c 4 10.0.1.4
PING 10.0.1.4 (10.0.1.4) 56(84) bytes of data.
64 bytes from 10.0.1.4: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 10.0.1.4: icmp_seq=2 ttl=64 time=0.032 ms
64 bytes from 10.0.1.4: icmp_seq=3 ttl=64 time=0.040 ms
64 bytes from 10.0.1.4: icmp_seq=4 ttl=64 time=0.039 ms

--- 10.0.1.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.023/0.033/0.040/0.006 ms
$
```