



Creating Virtual Network & Deploying Virtual Machine

Azure Virtual Network (VNet) is a foundational component of Azure networking, allowing you to create private networks in the cloud. It provides isolation, segmentation, and connectivity to your Azure resources, much like a traditional on-premises network.

Here are some key aspects of Azure Virtual Network:

1. **Isolation:** VNets provide network isolation for your Azure resources. Each VNet acts as a private network in the cloud, allowing you to control inbound and outbound traffic.
2. **Subnets:** Within a VNet, you can create multiple subnets to segment your resources. Subnets help organize and manage resources within the VNet and can have different access controls and security policies.
3. **Connectivity:** VNets can be connected to each other, to on-premises networks, and to the internet. Azure provides several options for connecting VNets, including Virtual Network Peering, VPN Gateway, and ExpressRoute.
4. **Network Security Groups (NSGs):** NSGs are Azure's built-in firewall capability that allows you to control traffic to and from resources within a VNet. NSGs can be applied to subnets or individual resources to enforce network security policies.
5. **Traffic Routing:** Azure VNets support custom route tables, allowing you to control how traffic is routed within the VNet and to external destinations.
6. **IPv4 and IPv6:** Azure VNets support both IPv4 and IPv6 addressing, enabling you to address your resources using either protocol.



Use cases of Virtual Network:

Azure Virtual Network (VNet) supports various use cases across different industries and scenarios. Here are some common ones:

1. **Hybrid Cloud Connectivity:** Many organizations have a hybrid cloud environment, with some resources hosted in Azure and others on-premises. VNets allow you to establish secure connections between your Azure resources and your on-premises network using VPN Gateway or ExpressRoute. This enables seamless communication and data transfer between the two environments while maintaining security and compliance.
2. **Multi-tier Applications:** VNets enable you to architect multi-tier applications with different layers (e.g., web, application, and database) deployed across separate subnets within the same VNet. This segmentation enhances security by restricting communication

between tiers and allows you to apply different network policies and access controls to each subnet.

3. Virtual Private Cloud (VPC) Replacement: Azure VNets can serve as virtual private clouds, providing isolated networking environments for your Azure resources. This is particularly useful for organizations migrating from on-premises infrastructure to the cloud, as VNets replicate the familiar network segmentation and isolation features of traditional data centers.
4. Global Application Deployment: For global-scale applications that require low-latency access from different geographic regions, Azure VNets support global VNet peering. This allows you to connect VNets across Azure regions, enabling seamless communication between resources deployed in different regions while maintaining the benefits of isolation and security.
5. Network Segmentation and Security: VNets allow you to implement granular network security controls using Network Security Groups (NSGs) and Application Security Groups (ASGs). You can define rules to allow or deny traffic based on IP addresses, ports, and protocols, helping to protect your resources from unauthorized access and potential threats.
6. Internet of Things (IoT) Solutions: Azure VNets provide a secure foundation for deploying IoT solutions by allowing you to connect IoT devices to Azure services securely. You can use VNets to establish communication between IoT devices, IoT hubs, and other Azure services while enforcing network-level security policies to safeguard sensitive data.
7. High-Performance Computing (HPC): For HPC workloads that require high-speed interconnectivity and low-latency communication between compute nodes, Azure VNets support accelerated networking and high-performance computing capabilities. This enables you to deploy HPC clusters within a VNet and achieve optimal performance for demanding computational tasks.

In this guide, we're setting up a **Virtual Network (VNet)** in Azure and deploying a **Virtual Machine (VM)** within that network. The end goal is to establish a private network environment in the cloud, where the VM can securely operate and communicate with other resources within the VNet. This setup provides isolation, segmentation, and connectivity for our Azure resources, similar to on-premises network infrastructure, enabling us to run applications, services, or workloads in a controlled and secure environment.

To begin with the Lab

Creating a Virtual Network

Login to Azure Portal,

Step 1: Search for Virtual Network in the marketplace and click on Create.

Home > Create a resource >

Marketplace ...

Get Started

Service Providers

Management

My Marketplace

Favorites

Recently created

Private plans

Categories

Networking (268)

Security (246)

Compute (159)

IT & Management Tools (125)

virtual network

Pricing : All × Operating System : All × Publisher Type : All × Product Type : All ×

Azure services only

Publisher name : All ×

Showing 1 to 20 of 690 results for virtual network: Clear search

Tile view ▾

Category	Description	Provider	Status	Create
Virtual network	Create a logically isolated section in Microsoft Azure and securely connect it outward.	Microsoft	Starts at Free	Create
Virtual network gateway	The VPN device in your Azure virtual network and used with site-to-site and VNet-to-VNet VPN connections.	Microsoft	Starts at Free	Create
CloudGuard Network Security for Azure Virtual	Delivers industry-leading threat prevention and management for Azure Virtual WAN and hybrid clouds	Check Point	Starts at Free	Create
Network interface	Create a Microsoft Azure Network Interface that allows you to connect a Virtual Machine to a Virtual Network.	Microsoft	Starts at Free	Create
Network connection				
Local network gateway				
Network Manager				
Network Connections				

Is Marketplace helpful?

Step 2: Select the resource group & enter the name for the virtual network.

- Click on next.

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 Pass - Sponsorship (9e3f0cae-8274-4931-b16b-95242092e301) ▼
Resource group *	demo-resource-group ▼
	Create new

Instance details

Virtual network name *	demo-VN
Region * ⓘ	(Asia Pacific) Central India ▼
	Deploy to an Azure Extended Zone

Step 3: In the IP addresses section, here you will see the subnets and you can add or change the name of the subnet.

- First, we are going to change the name of the subnet. So, to change the name of the subnet you need to click on the pencil icon which is highlighted and then you will see a new window has been opened on the right side of the screen. Change its name and then click on save.
- Then we are going to add a new subnet.

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 IPv4 address space | ▾

[Delete address space](#)

10.0.0.0/16

10.0.0.0 /16 10.0.0.0 - 10.0.255.255 65,536 addresses

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

[Edit](#) [Delete](#)

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-1

IPv4

Include an IPv4 address space	<input checked="" type="checkbox"/>
IPv4 address range * ⓘ	10.0.0.0/16 10.0.0.0 - 10.0.255.255
Starting address * ⓘ	10.0.0.0
Size ⓘ	/24 (256 addresses)
Subnet address range ⓘ	10.0.0.0 - 10.0.0.255

- Now to add a new subnet first you must click on Add a Subnet.
- Then from the right side you can see give it a name then the starting address will be auto filled for you. Just click on add.

The screenshot shows the Azure portal interface for creating a virtual network. On the left, the 'Create a resource > Marketplace' path is visible. The main area is titled 'Create virtual network'. The 'IP addresses' tab is selected. A note says: 'Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need.' Below this is a note about defining address space ranges. A 'Subnet purpose' dropdown is set to 'Default'. A red box highlights the 'Name' field containing 'Subnet-2'. Under 'IPv4', the 'Include an IPv4 address space' checkbox is checked. The 'IPv4 address range' dropdown shows '10.0.0.0/16' and '10.0.0.0 - 10.0.255.255'. The 'Starting address' dropdown is set to '10.0.1.0' and has a red box around it. The 'Size' dropdown is set to '/24 (256 addresses)'. The 'Subnet address range' is '10.0.1.0 - 10.0.1.255'. Under 'IPv6', there is a note that 'This virtual network has no IPv6 address ranges.' Under 'Private subnet', there is a note about enabling outbound connectivity via a NAT gateway. A red box highlights the 'Add' button at the bottom right of the dialog.

Step 4: Go on to Review + Create and click on Create.

- Virtual Network -> Vnet -> Subnets

The screenshot shows the 'demo-VN | Subnets' page. The left sidebar includes 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Address space', 'Connected devices', and 'Subnets' (which is currently selected). The main area displays a table of subnets:

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
Subnet-1	10.0.0.0/24	-	251	-	-	-
Subnet-2	10.0.1.0/24	-	251	-	-	-

Creating a Virtual Machine

- Now, let's deploy a virtual machine to our virtual network.
- So, to create a virtual machine first you go to the Create Resources section then choose to Create Virtual Machine or you can just click on the hamburger icon from the top left corner and from there choose Create a VM.
- Click on Create.
- Now while creating your virtual machine, remember to select the same resource group and same region where you have deployed your virtual network.

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 Pass - Sponsorship (9e3f0cae-8274-4931-b16b-95242092e301) ▼
Resource group * ⓘ	demo-resource-group ▼ Create new

Instance details

Virtual machine name * ⓘ	demoVM ✓
Region * ⓘ	(Asia Pacific) Central India ▼
Availability options ⓘ	No infrastructure redundancy required ▼
Security type ⓘ	Standard ▼
Image * ⓘ	Ubuntu Server 22.04 LTS - x64 Gen2 ▼ See all images Configure VM generation

This image is compatible with additional security features. [Click here to swap to the Trusted launch security type.](#)

- Now move to the networking section you will see that it is automatically picking up your virtual network and assigning it a subnet.
- If you click on the subnet, you have the option to change the subnet as per your desire.
- After that just move to review page and create your virtual machine.

Network interface

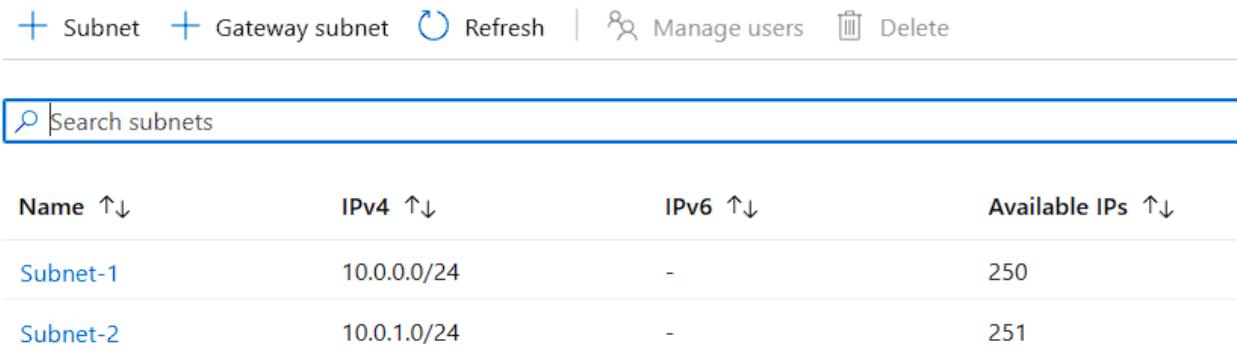
When creating a virtual machine, a network interface will be created for you.

Virtual network * ⓘ	demo-VN ▼ Create new
Subnet * ⓘ	Subnet-1 (10.0.0.0/24) ▼ Manage subnet configuration
Public IP ⓘ	(new) demoVM-ip ▼ Create new
NIC network security group ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports * ⓘ	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports

- Once your VM is deployed then click on go to resources and there you can see your virtual network and the subnet.

Operating system : Linux (ubuntu 22.04)
 Size : Standard B1s (1 vcpu, 1 GiB memory)
 Public IP address : [98.70.96.140](#)
 Virtual network/subnet : [demo-VN/Subnet-1](#)
 DNS name : [Not configured](#)
 Health state : -

- Now If you return to the virtual network and then click on subnets, you will notice that in Subnet-1, the remaining available IP addresses are 250 because 1 is being used by the virtual machines.



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
Subnet-1	10.0.0.0/24	-	250
Subnet-2	10.0.1.0/24	-	251