**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.

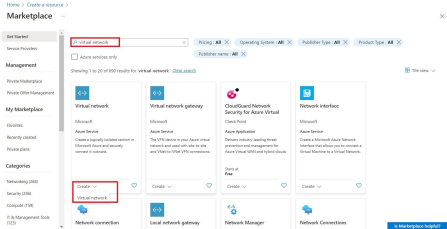
7. High-Performance Computing (HPC): For HPC workloads that require high-speed interconnectivity and low-latency communication between compute nodes, Azure VNets support accelerated networking and high-performance computing capabilities. This enables you to deploy HPC clusters within a VNet and achieve optimal performance for demanding computational tasks.

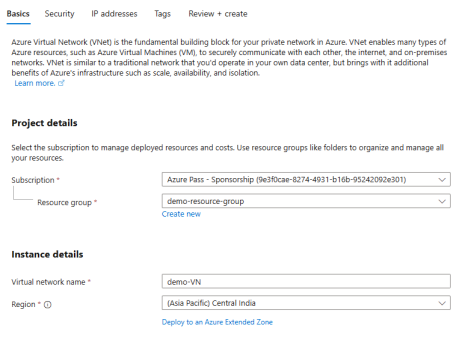
**In this guide, we're setting up a Virtual Network (VNet) in Azure and deploying a Virtual Machine (VM) within that network. The end goal is to establish a private network environment in the cloud, where the VM can securely operate and communicate with other resources within the VNet. This setup provides 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,

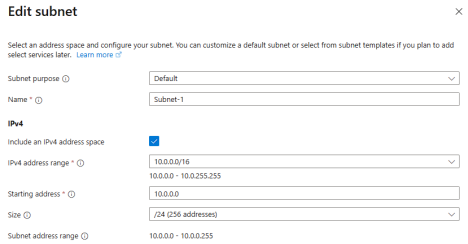
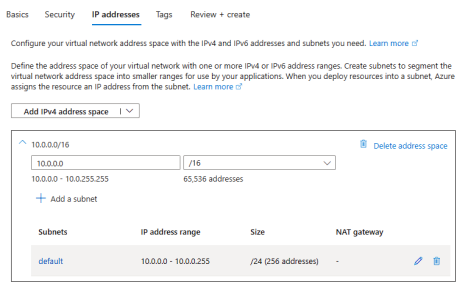
Step 1: Search for Virtual Network in the marketplace and click on Create. Step 2: Select the resource group & enter the name for the virtual network. ● Click on next.



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

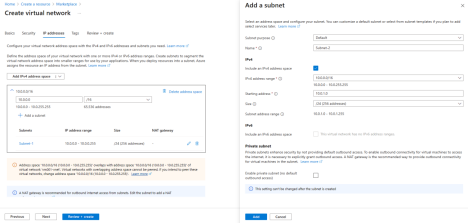
• First, we are going to change the name of the subnet. So, to change the name of the subnet you need to click on the pencil icon which is highlighted and then you will see a new window has been opened on the right side of the screen. Change its name and then click on save.

• Then we are going to add a new subnet.

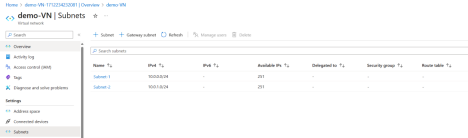


● Now to add a new subnet first you must click on Add a Subnet.

● 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.

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

● Virtual Network -> Vnet -> Subnets

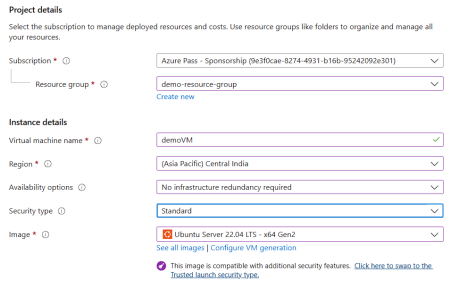
 **Creating a Virtual Machine**

• 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.

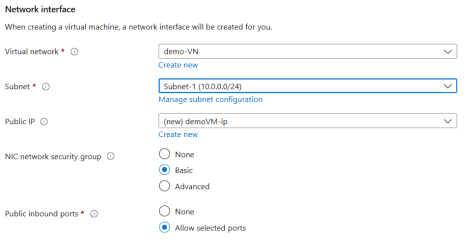
• Click on Create.

• Now while creating your virtual machine, remember to select the same resource group and same region where you have deployed your virtual network.

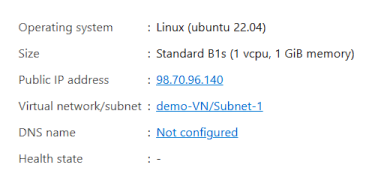


• Now move to the networking section you will see that it is automatically picking up your virtual network and assigning it a subnet.

• 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.



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



• 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.

