**Azure Network Service**

The most fundamental building block of Azure network services is the virtual network. Using a virtual network, we can deploy our isolated network on Azure. And we can divide the virtual network into multiple parts using subnets. For example - webserver subnet, App servers1 subnet, App servers2 subnet, Database subnet, Gateway subnet, Virtual Appliance subnet, etc. These are the typical examples, but we can create different kinds of subnets based on our requirements.

And once we create subnets, we can deploy different types of Azure services into these subnets. We can deploy a virtual machine into these subnets. But in addition to virtual machines, we can also deploy some specialized environments. i.e., some PaaS environments that are capable of being implemented into a virtual network. For example - in an app service environment, we can able to deploy in its own subnet. Similarly, there is something called managed SQL instance and also managed integration environment, all these kinds of environments we can able to deploy within a virtual network.

**Azure Virtual Network**

The Azure Virtual Network is a logical representation of the network in the cloud. So, by creating an Azure Virtual Network, we can define our private IP address range on Azure, and also deploy different kinds of Azure resources. For Example - Azure virtual machine, App service environment, Integration service environment, etc.

**Azure Vnet Capabilities**

Following are the capabilities of the Azure Vnet:

**Isolation and segmentation:** To deploy resources such as virtual machines into virtual networks, they will be isolated from other resources. By putting the virtual machine into your virtual network, it cannot be reached from the Internet or other Azure resources unless we enable communication in between. We can also use subnets within virtual networks to further segment our resources within the network.

**Communication with the Internet:** All resources in a virtual network can communicate outbound to the Internet by default. But it needs to establish an inbound connection from the Internet. We can either use public IP or load balancers.

**Communication between resources:** Communication between the number of resources inside the virtual network or with other resources through service endpoints.

**Communication with on-premises resources**: By establishing either point to site VPN or site to site VPN or Express route, your workloads within Azure virtual network can seamlessly communicate with workloads within our on-premises data center.

There are lots of capabilities within the Azure virtual network that we can use to control the traffic.

**Filter network traffic:** We can use Network Security Groups, Application Security Group, Azure firewall, or third-party network virtual appliance to filter the traffic coming to the resources in the virtual network.

**Route network traffic:** We can route the network traffic using the routing tables, we can configure user-defined routes to route all the outbound traffic, let's say via a firewall.

**Monitor network traffic:** By network security groups and traffic analytics monitoring solution, you'll be able to carry out extensive monitoring on both inbound and outbound communications.

**Subnet:**

Subnet plays a vital role because many configurations will be done at a subnet level. It is a range of IP addresses in the VNet. Vnet can be divided into multiple subnets based on different design considerations, for example - we can deploy a virtual machine, App services environment, integration service environment, etc. VMs & PaaS services deployed to subnets n the same VNet and can communicate with each other without any extra configuration. Route tables, NSG, Service endpoints, and policies are configured to the subnets.

**Azure Availability Zones and Sets**

To deliver high availability, Azure provides two more important features.

**Availability Zone**: It is a high availability offering that protects your application and data from data center failures. Generally, every Azure region consists of multiple data centers located at different physical locations. When you are deploying your services into Azure, you can able to select into which availability zone you want to deploy your service.

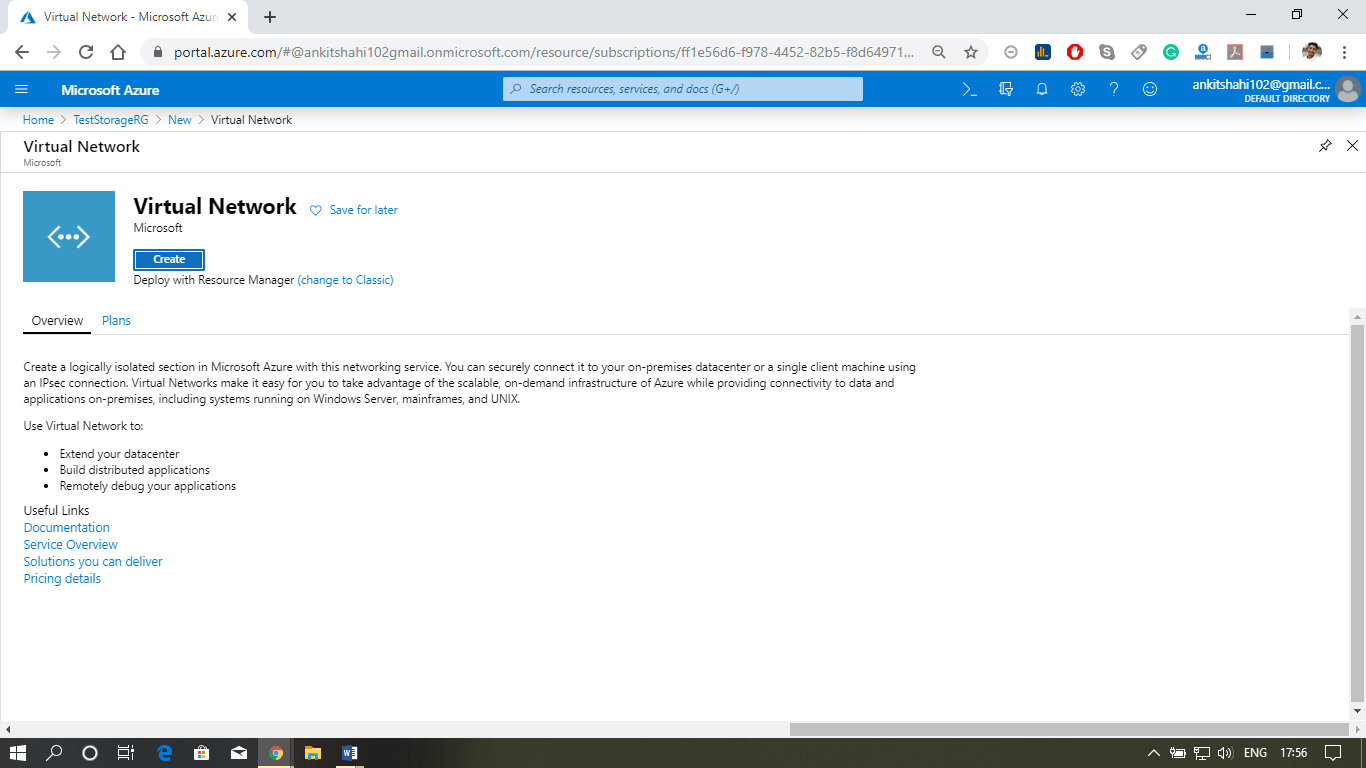
**Availability Set:** It works at a rack level. It is a logical grouping of the virtual machine within the data center that allows Azure to understand how your application is built to provide for redundancy and availability. The availability set consists of two domains one is fault domain, and another is the update domain.

* **Fault Domain:** It is a logical group of the underlying hardware that share a common power source and network switch similar to a rack within an on-premises data center. So, if we are deploying all the virtual machines into the same fault domain, then any hardware failure will knock out all the virtual machines in that particular rack or fault domain.
* **Update Domain:** It is a logical group of the underlying hardware that can undergo maintenance or be rebooted at the same time because Azure will do infrastructure management.

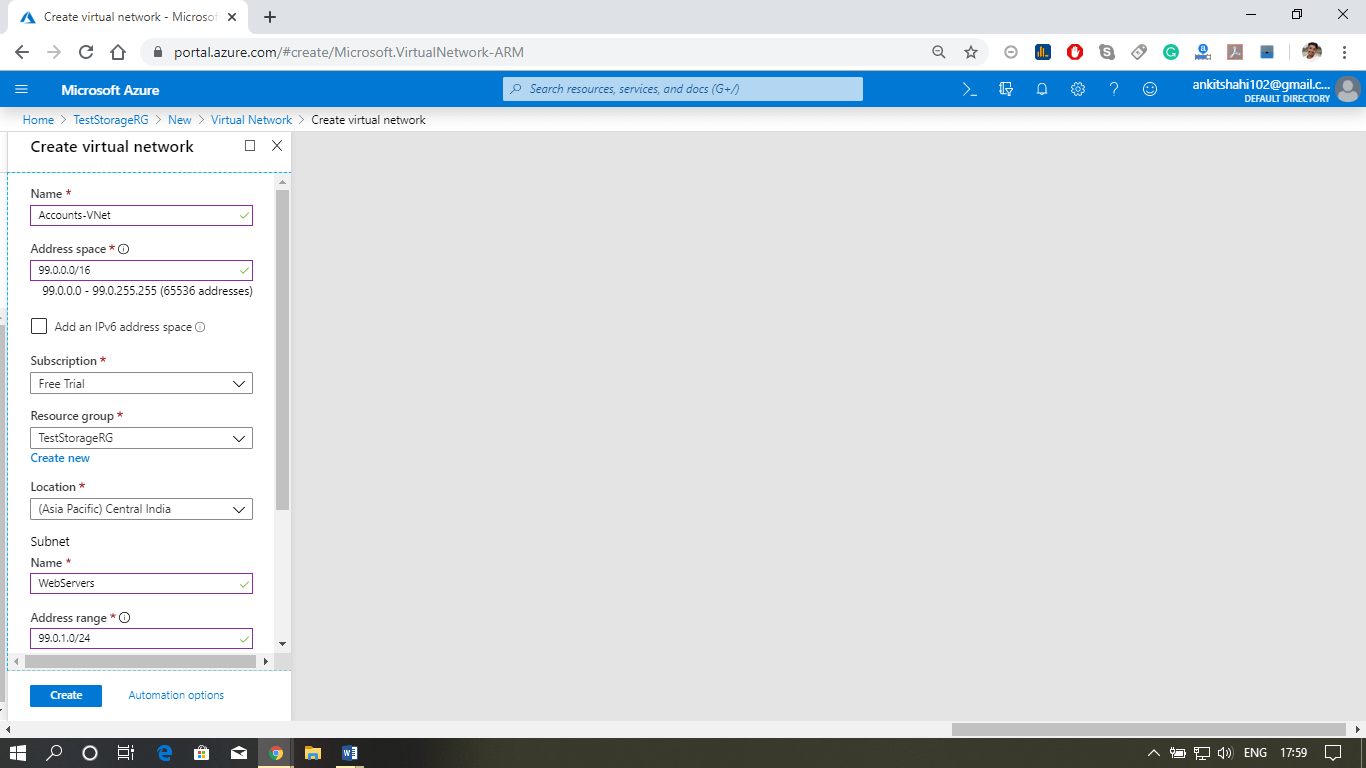
**Managed Disk fault domains**: For VMs using Azure Managed Disks, VMs are aligned with managed disk fault domains when using a managed availability set. This alignment ensures that all the managed disks attached to a VM are with the same managed disk fault domain.

**Creating Azure Virtual Network and subnets**

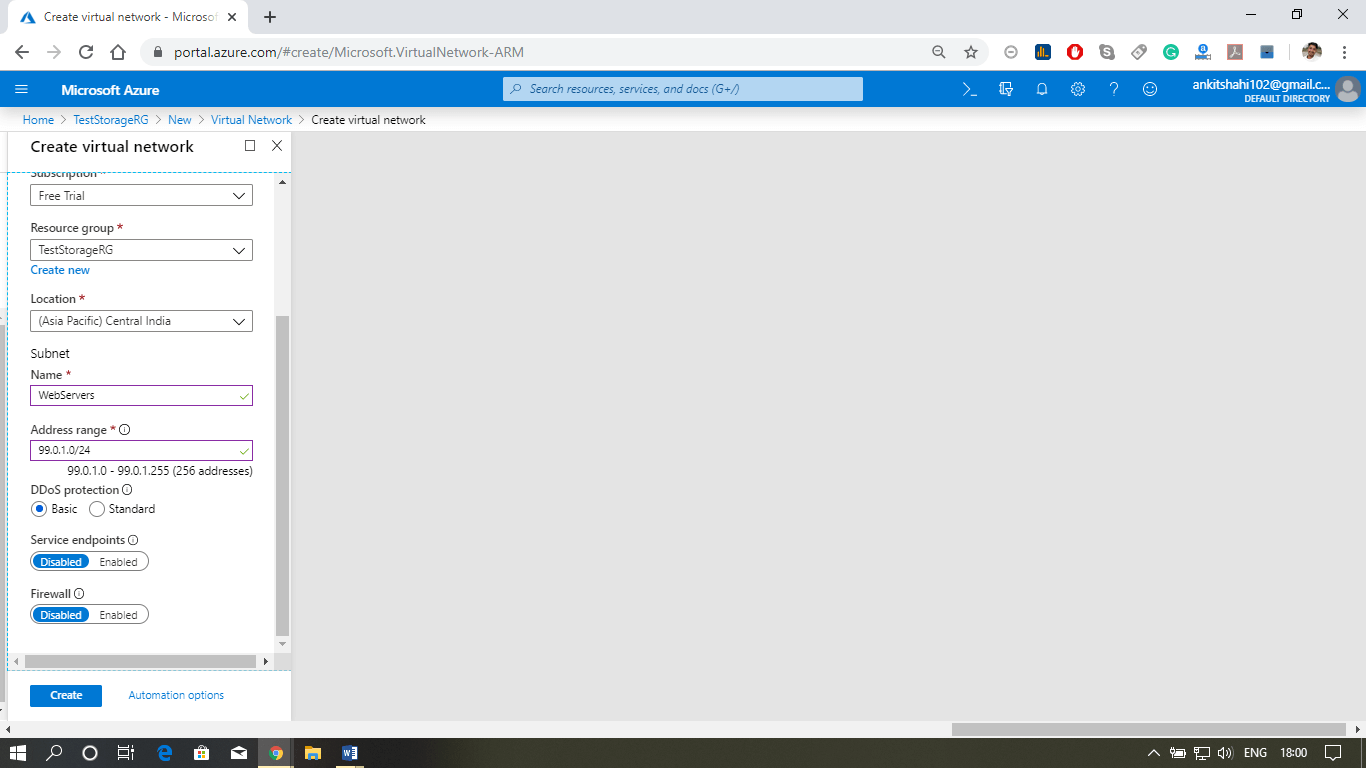
**Step 1:** Select your existing resource group, or you can create a new resource group.



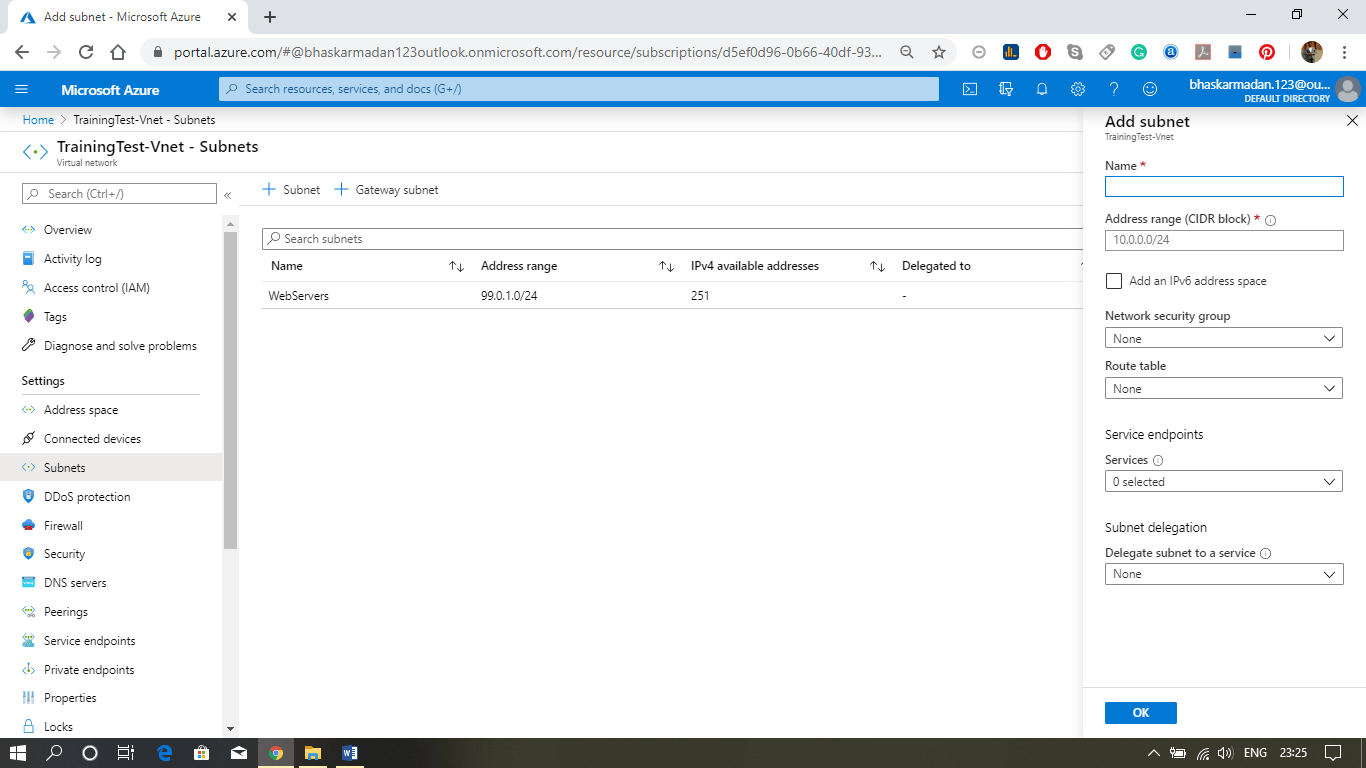
**Step 2:** After opening your resource group, click on Add then type in Virtual network in the search box. Click on Create.



**Step 3:** A new window will appear, where you need to fill the details like - name, address space (e.g., 99.0.0.0/16), Name of the subnet, subnet address space (e.g., 99.0.1.0/24). Leave everything as it is and click on create.



**Step 4:** Now, your Vnet is created. Let's add a subnet into it. Click on the subnet, then click on add subnet.



**Step 5:** On the next slider window, give a name to the subnet you want to create, provide the address range (if the address range is currently in use, you cannot change it). Then click on the ok button to create the subnet.

**Azure Network Security**

A network security group consists of security rules that allow or deny inbound/Outbound network traffic to or from different types of Azure resources that we will host in our Azure virtual network.

**Default Rules**

Some default rules are created by default when we create NSG. There are two types of default rules.

**Inbound Security rules**

* **Allow VNet Inbound**: Traffic is allowed from any resources within the VNet
* **Allow Azure LoadBalancer Inbound:** Any traffic originating from Azure load-balancer to any of the virtual machines within the network is permitted.
* **Deny All Inbound:** By default, virtual machines in the virtual network can communicate with each other, and also Azure load balancer can communicate with virtual machines within the virtual network.

**Outbound Security rules**

* **Allow VNet OutBound:** Traffic is allowed through any resources within the VNet
* **Allow Internet OutBound:** Traffic originating from any resources in the VNet to the Internet is allowed.
* **Deny All OutBound:** By default, virtual machines in a virtual network can communicate with each other, and also Azure load balancer can interact with the virtual machine within the virtual network.