A

MINOR PROJECT

ON

CREATING A VNET USING VNET SERVICES IN MICROSOFT AZURE

SUBMITTED IN FULLFILLMENT OF THE INTERNSHIP IN CLOUD COMPUTING

Submitted By

R.S.Dharsan

(963321104020)

ROHINI COLLEGE OF ENGINEERING AND TECHNOLOGY

ANNA UNIVERSITY:CHENNAI

OCTOBER 2023

ABSTRACT

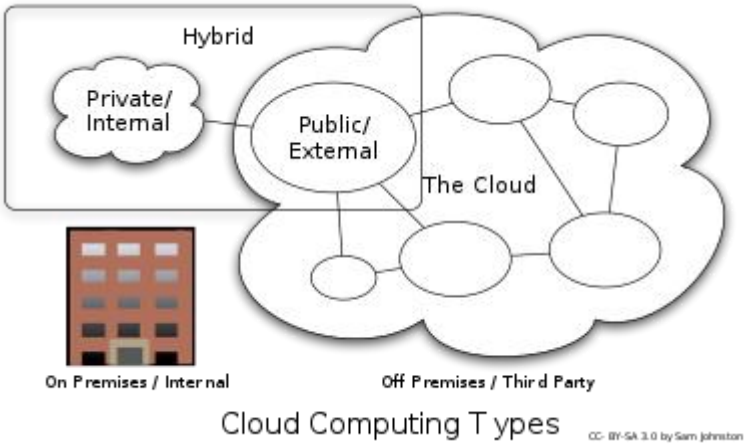
Using this Virtual network we can enable communication between multiple computers, virtual machines (VMs), virtual servers, or other devices across different office and data center locations.

Network virtualization helps organizations achieve major advances in speed, agility, and security by automating and simplifying many of the processes that go into running a data center network and managing networking and security in the cloud.

CLOUD COMPUTING

Cloud computing is the on-demand availability of computer system resources, especially data storage (cloud storage) and computing power, without direct active management by the user.[2] Large clouds often have functions distributed over multiple locations, each of which is a data center. Cloud computing relies on sharing of resources to achieve coherence and typically uses a "pay as you go" model, which can help in reducing capital expenses but may also lead to unexpected operating expenses for users, securely with other networks and maintain a cost-efficient cloud environment. Thus, adding another feather to Microsoft's hat.

Deployment Models



Public Cloud:

Overview: In a public cloud deployment model, cloud infrastructure and services are owned, operated, and maintained by a cloud service provider (CSP) and are made available to the general public or a broad customer base. The CSP hosts multiple tenants on shared physical resources.

Characteristics:

Accessibility: Services are accessible over the public internet.

Cost-Efficiency: Typically, you pay on a pay-as-you-go or subscription basis, reducing upfront capital expenses.

Scalability: Public clouds offer dynamic scalability to meet varying resource demands.

Shared Resources: Resources are shared among multiple tenants.

Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), and IBM Cloud.

Use Cases:

- Web hosting and development environments.
- SaaS applications.
- Test and development environments.
- publicly accessible websites and applications.

Private Cloud:

Overview: In a private cloud deployment model, the cloud infrastructure and services are dedicated to a single organization. The organization may own and operate the infrastructure on its premises (on-premises private cloud) or have a third-party provider manage it (hosted private cloud).

Characteristics:

Isolation: Resources are not shared with other organizations.

Control: The organization has full control over the infrastructure and configurations.

Security: Enhanced security and compliance options.

Customization: The organization can tailor the cloud environment to its specific needs.

Examples: VMware Cloud, OpenStack, Azure Stack, and Oracle Cloud at Customer.

Use Cases:

- Highly regulated industries (e.g., finance, healthcare) with stringent security requirements.
- Organizations with legacy applications requiring cloud-like flexibility.
- Government agencies and institutions with data sovereignty requirements.

Hybrid Cloud:

Overview: A hybrid cloud deployment combines elements of both public and private clouds, allowing data and applications to be shared between them. It provides greater flexibility and optimization of resources by integrating on-premises infrastructure with public cloud services.

Characteristics:

Interoperability: Data and applications can move seamlessly between on-premises and cloud environments.

Scalability: Bursting to the public cloud during peak demand.

Data Portability: Data synchronization and replication between environments.

Complexity: Managing two different environments can be more complex.

Examples: AWS Outposts, Azure Arc, and Google Anthos.

Use Cases:

- Data backup and disaster recovery solutions.
- E-commerce websites with variable traffic.
- Applications that require on-premises data processing and cloud-based analytics.

Multi-Cloud:

Overview: Multi-cloud is a deployment model where an organization uses multiple public cloud providers or a combination of public and private clouds for various workloads. It aims to avoid vendor lock-in, optimize costs, and leverage best-of-breed services.

Characteristics:

Diversity: Utilizing multiple cloud providers for different services or regions.

Risk Mitigation: Redundancy across providers reduces the impact of outages.

Complexity: Managing multiple cloud providers can be challenging.

Cost Optimization: Choosing the most cost-effective services from different providers.

Examples: A combination of AWS, Azure, GCP, and private cloud environments.

Use Cases:

- Risk mitigation by avoiding reliance on a single provider.
- Leveraging specialized services from different providers.
- Regulatory compliance by using providers with data centers in specific regions.

Azure Virtual Network

- An Azure Virtual Network (VNet) is a network or environment that can be used to run VMs and applications in the cloud.
- When it is created, the services and Virtual Machines within the Azure network interact securely with each other.

Advantages of Using Azure Virtual Network

Some of the major advantages of using Microsoft Azure VNet are as follows:

- It provides an isolated environment for your applications
- A subnet in a VNet can access the public internet by default
- We can easily direct traffic from resources
- It is a highly secure network
- It has high network connectivity
- It builds sophisticated network topologies in a simple manner
- Moving on, let have a look at the components of Azure VNet.

Components of Azure VNet

Azure networking components provide a wide range of functionalities that can help companies build efficient cloud applications that meet their requirements.

The components of Azure Networking are listed below, and we have explained each of these components in a detailed manner:

1. Subnets
2. Routing
3. Network Security Groups

Subnets

- Subnets let users segment the virtual network into one or more sub-networks.
- These sub-networks can be separated logically, and each subnet consists of a server.
- We can further divide a subnet into two types:

1. Private
2. Public

- Private - Instances can access the Internet with NAT (Network Address Translation) gateway that is present in the public subnet.
- Public - Instances can directly access the internet.

Routing

- It delivers the data by choosing a suitable path from source to destination.
- For each subnet, the virtual network automatically routes traffic and creates a routing table.

Network Security Groups

- It is a firewall that protects the virtual machine by limiting network traffic.
- It restricts inbound and outbound network traffic depending upon the destination IP addresses, port, and protocol.

Everything You Need to Know About Microsoft Azure Virtual Network

How to Launch an Instance using Azure VNet?

Step- By-Step Creating Azure Virtual Machine and Virtual Network

Earlier, while developing and deploying software applications, companies had been facing common issues like network attacks, data leaks, poor network connectivity, time-consuming processes in building network topologies, and inadequate diversion of network traffic.

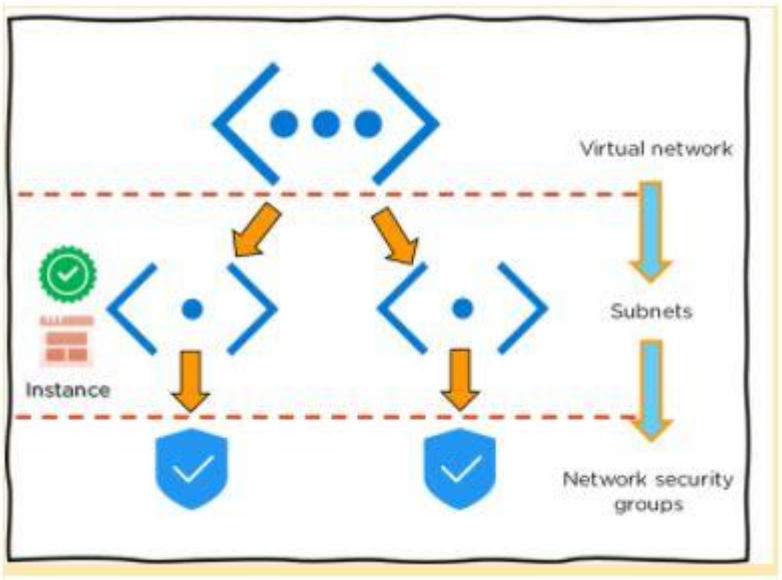
With this going on, Microsoft saved the day, right on time Microsoft Azure addressed these issues and launched Azure Virtual Network, which helped companies communicate securely with other networks and maintain a cost-efficient cloud environment. Thus, adding another feather to Microsoft's hat.

This article will help you understand the concept of how to secure your application using Azure VNet.

Network Security Groups

- It is a firewall that protects the virtual machine by limiting network traffic.
- It restricts inbound and outbound network traffic depending upon the destination IP addresses, port, and protocol.

How to Launch an Instance using Azure VNet?



- First, create a virtual network in the Azure cloud
- Next, create subnets into each virtual network
- Now, assign each subnet with the respective instance or Virtual Machine
- After which you can connect the instance to a relevant Network Security Group
- Finally, configure the properties in the network security and set policies
- As a result, you will be able to launch your instance on Azure

Moving forward, we will see a demonstration on creating an Azure virtual machine and virtual network step-by-step.

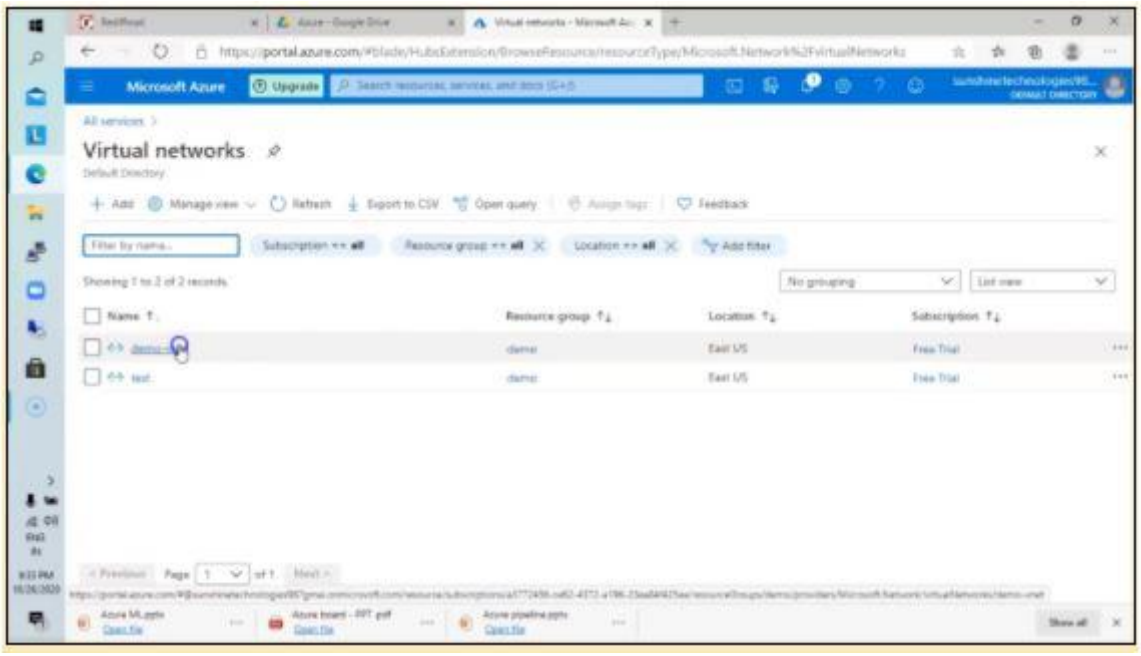
Step-By-Step Creating Azure Virtual Machine and Virtual Network

Step 1 − First, log into your Azure Management Portal, select 'New' at the bottom left corner.

Step 2 − Next, on the Network Services go to Virtual Network -> Quick create.

Step 3 - Now, enter the name and leave all other fields empty and click 'next'.

Step 4 − Finally, click on 'Create a Virtual Network,' and it is done.



Note: Now, in the same VNet, create a Virtual machine

Step 5 - First, select ‘create’ to build a new Virtual Machine with Windows Server 2012 R2 Datacenter.

Step 6 - Once the fields are entered, select the existing resource group that you had created for the virtual network and select OK.

Step 7 - Now, choose a desired size and configuration by selecting DS1_V2 Standard type

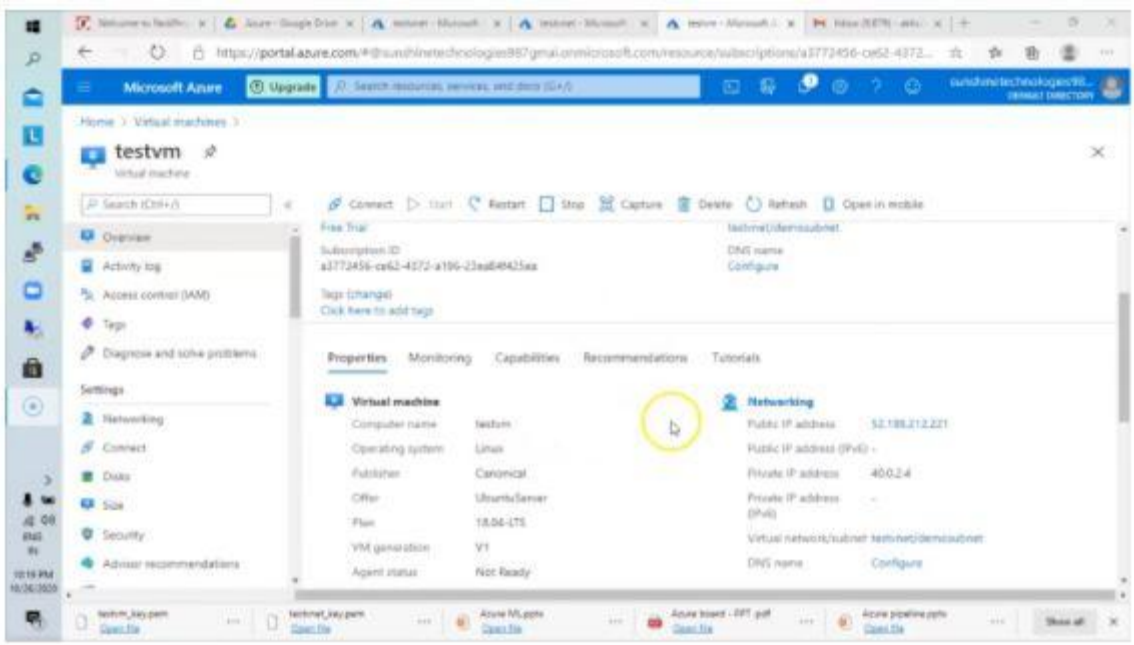
Note: By default, we would choose a Virtual Network.

Step 8 - Now select the subnet as FrontEndSubnet and do not change the public IP address. Also, keep the Network Security Group as none.

Step 9 - Create a new availability set and set a new name to it.

Next, set the fault domains as 2 and then disable the Guest OS Diagnosis section.

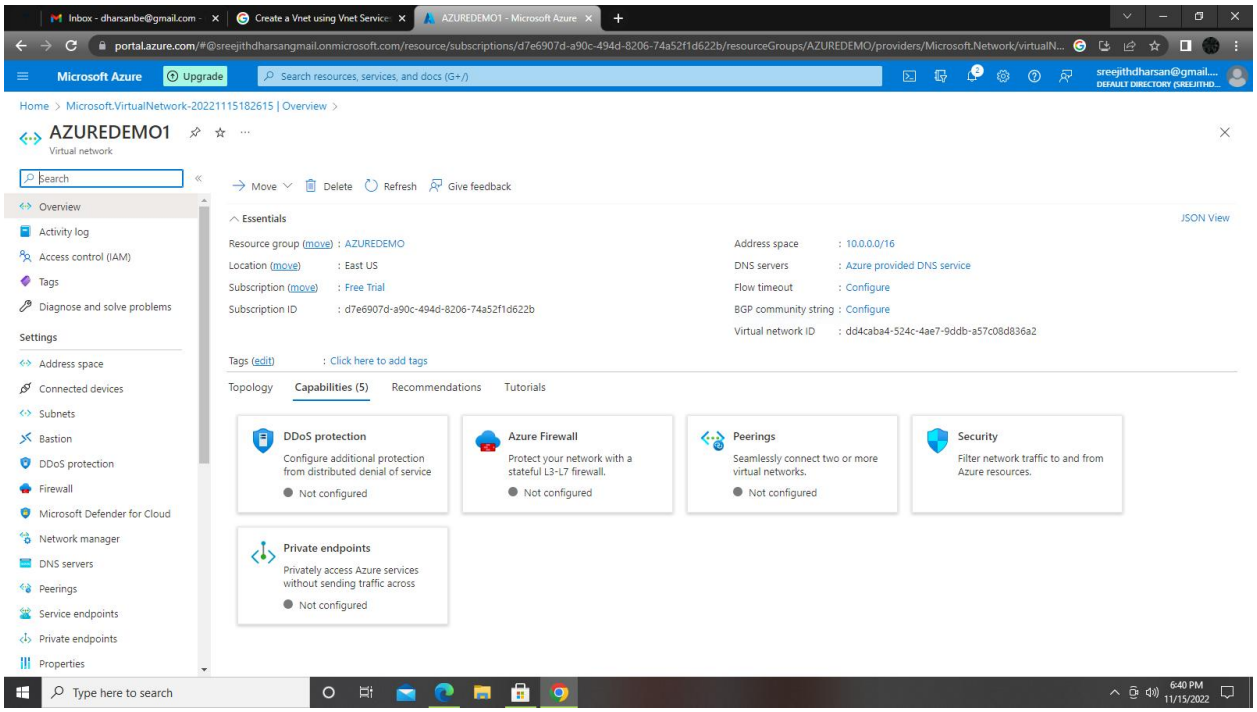
Step 10 - Finally, click and select ‘create’.



Congratulations, you have successfully created a VM.

This is all the basic information you need to know about Microsoft Azure Virtual Network.

OUTPUT



Conclusion

We explored all about Microsoft Azure VNet and its benefits, Components of Azure VNet, how Machine Learning works with SageMaker, how to Launch an instance using Azure VNet, and finally, we also saw a demo on how to create an Azure virtual machine and virtual network.

Whether you're an experienced AWS Architect or you're aspiring to break into this exciting industry, enrolling in our Cloud Architect Master's program will help you with all levels of experience in master AWS Cloud Architect techniques and strategies.

.