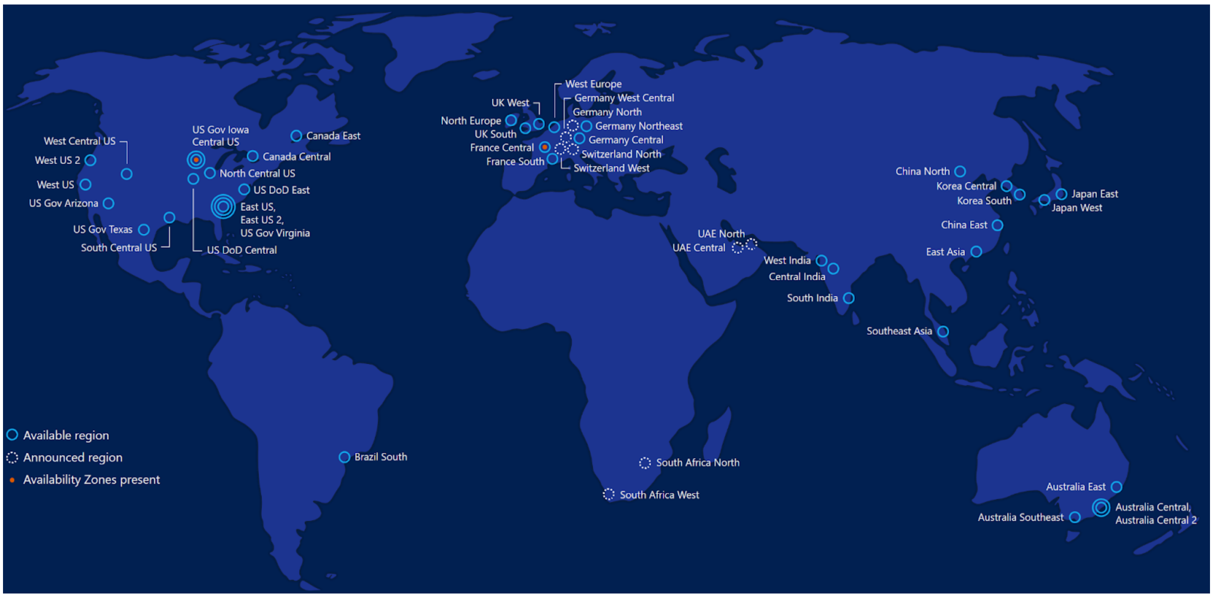
Storie 6 : Networking in Azure

Owner	ⓜ mubeen
Tags	
Created time	@February 23, 2024 12:44 PM

Azure Cloud Networking

Azure Cloud Computing resources(servers, storage, databases etc) are available across the world.

Datacenter's are available in different geographical locations

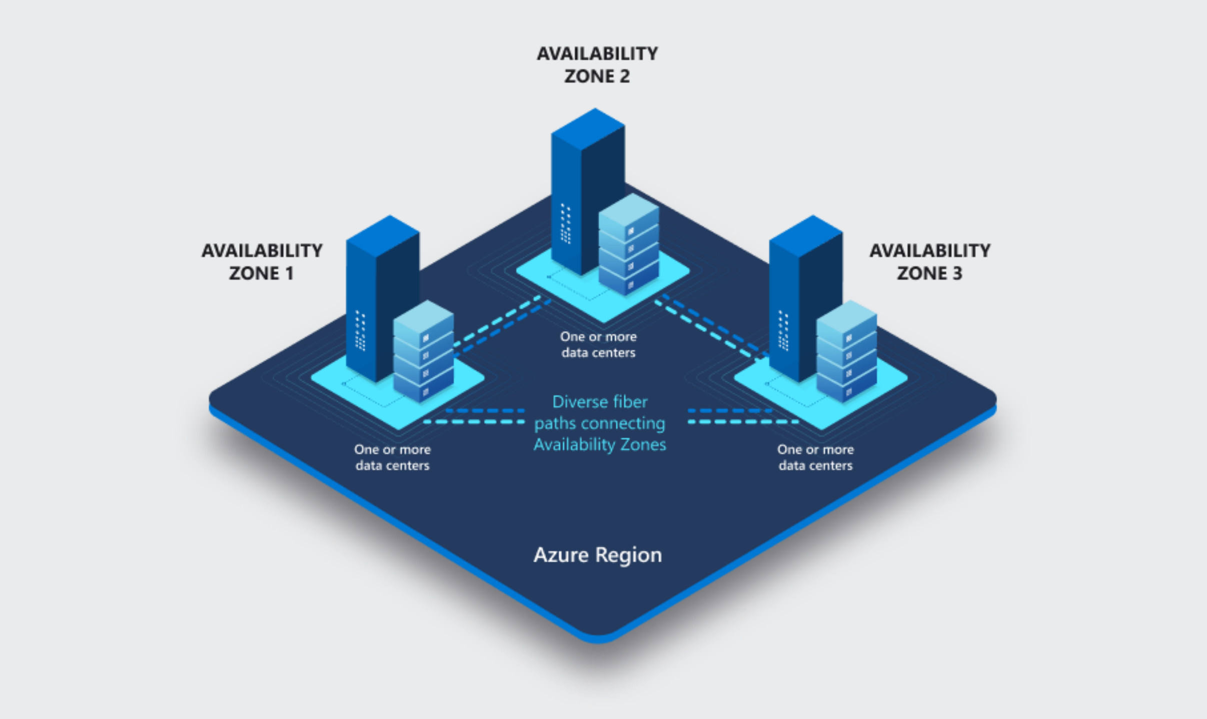


Regions

- Azure Cloud Computing Resources or Data Centers are available in different Geographical Locations, which are termed as **REGIONS**.
- Region selection is based on the client location, always select the nearest location to the client to avoid any latency issues.

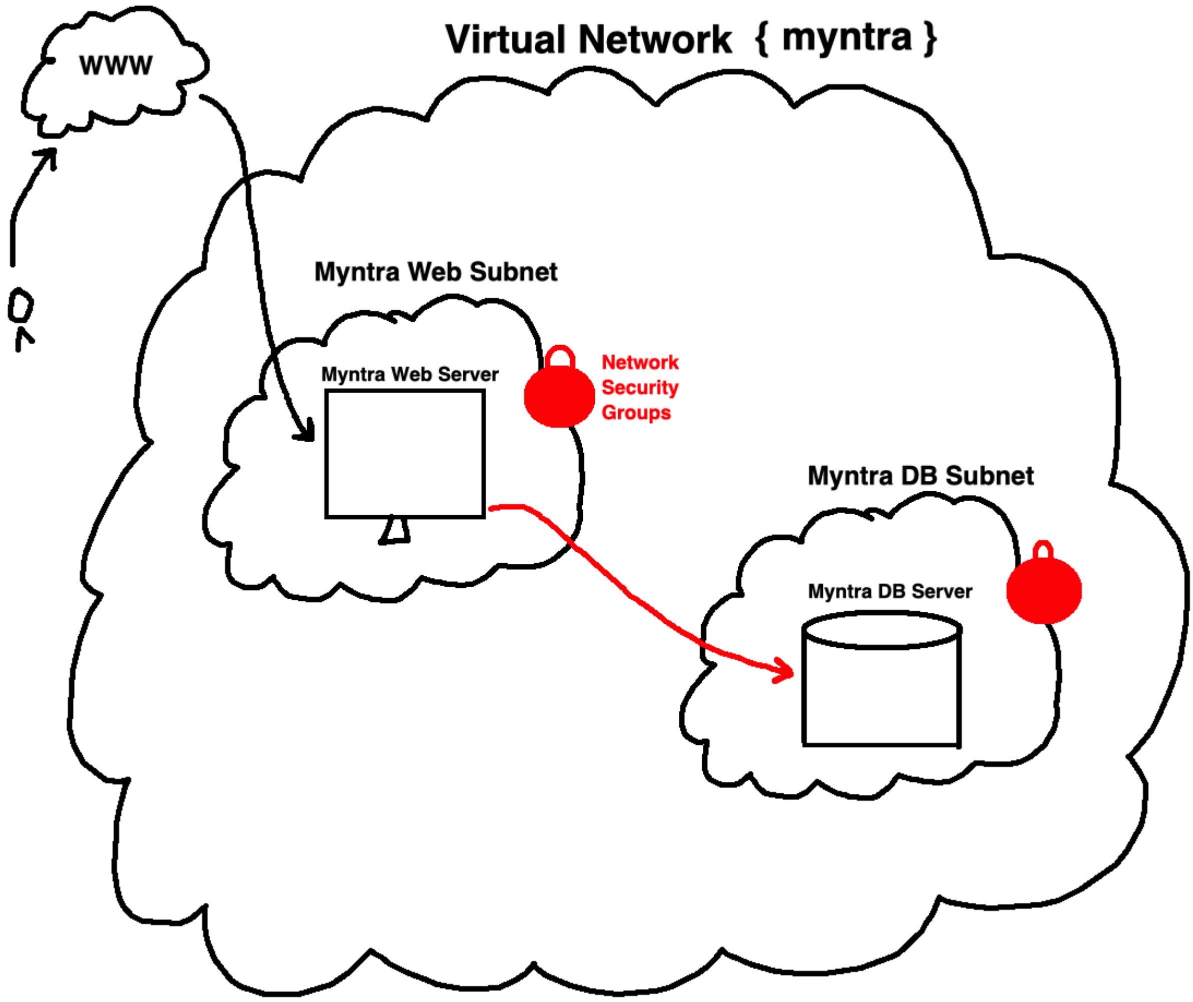
Availability Zones

- **Availability Zones are unique physical locations** within an Azure region.

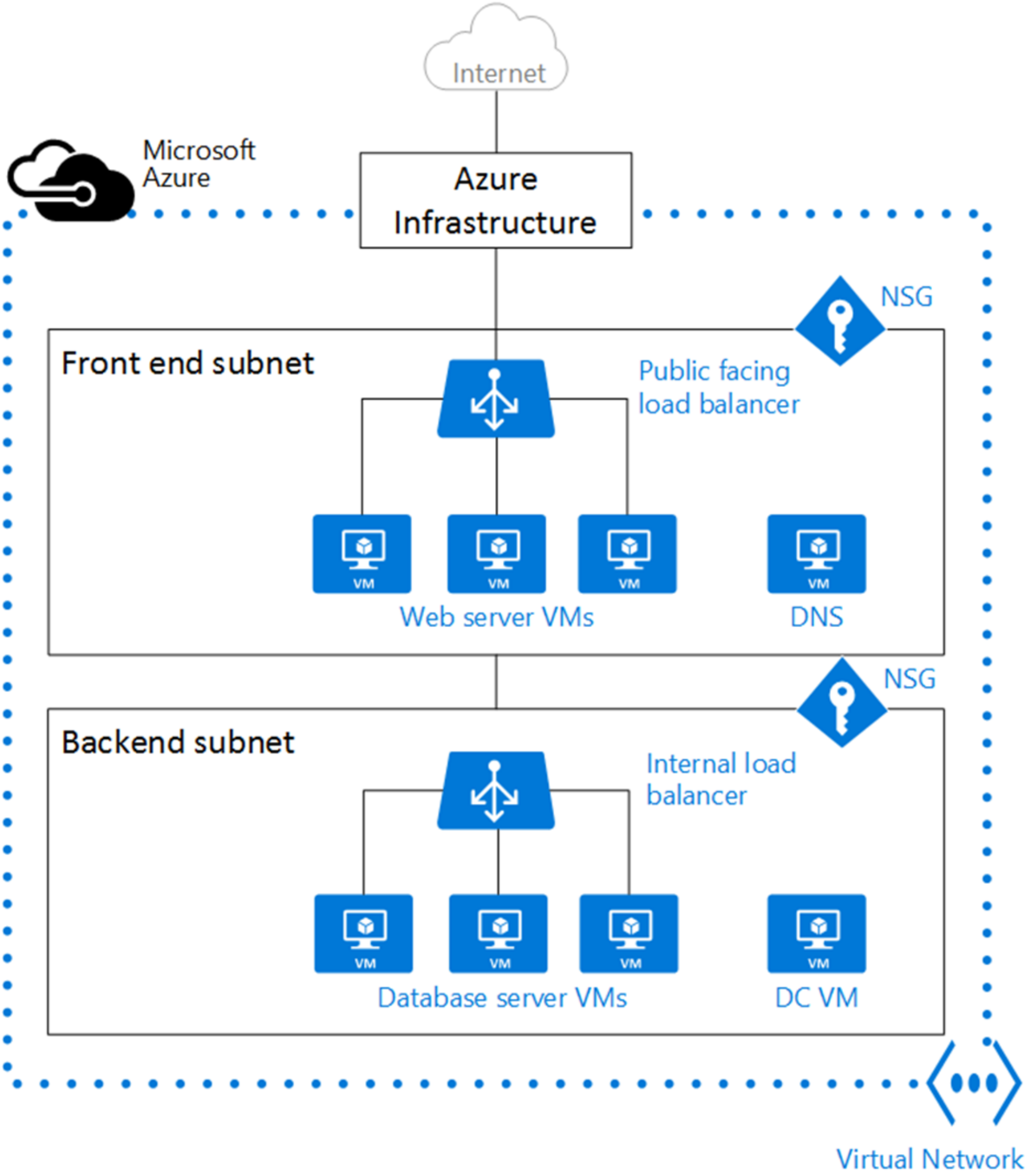


Azure Virtual Networks - VNET

- Azure Virtual Network (VNET) is a service that **lets you launch AZURE resources (servers, databases, applications etc) in a logically isolated virtual network** that you define.
- **It is similar to having your own data center inside AZURE**. The resources are completely isolated from other VNETS on AZURE

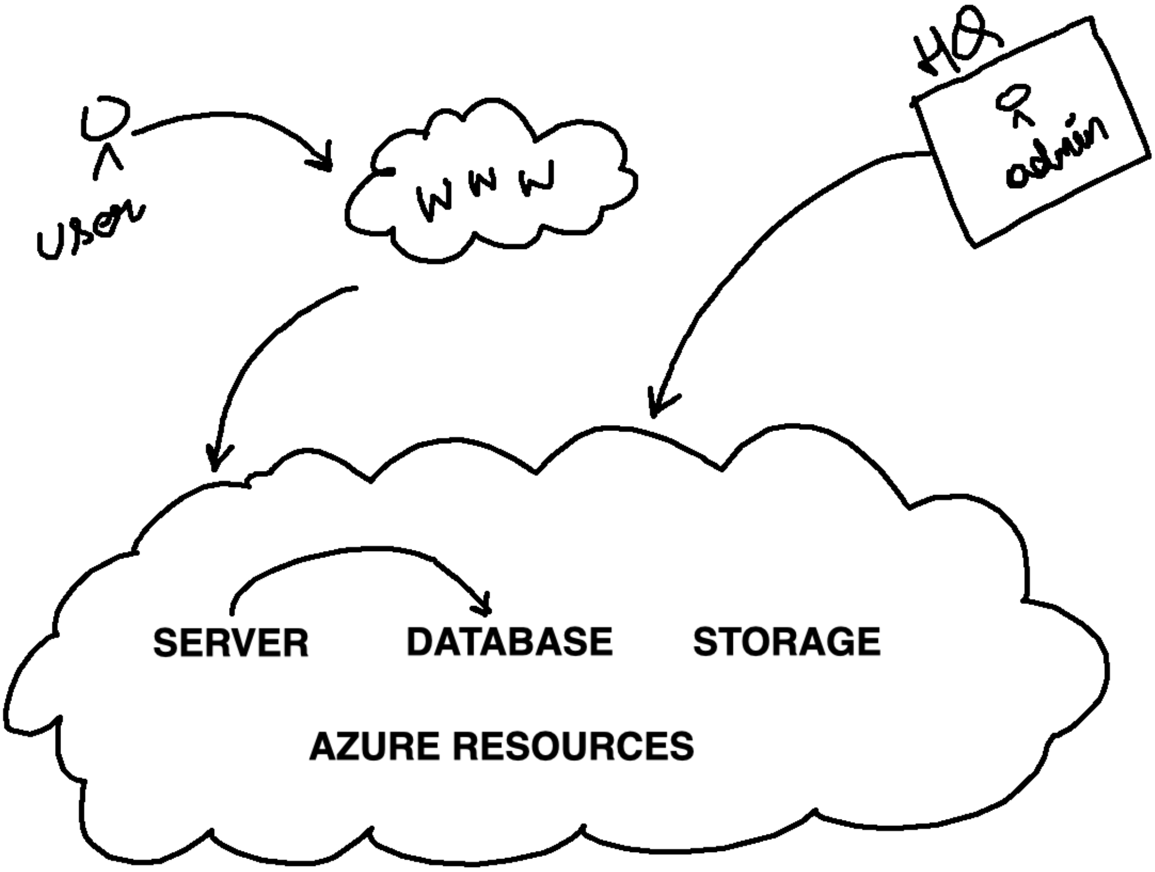


Azure VNET Components



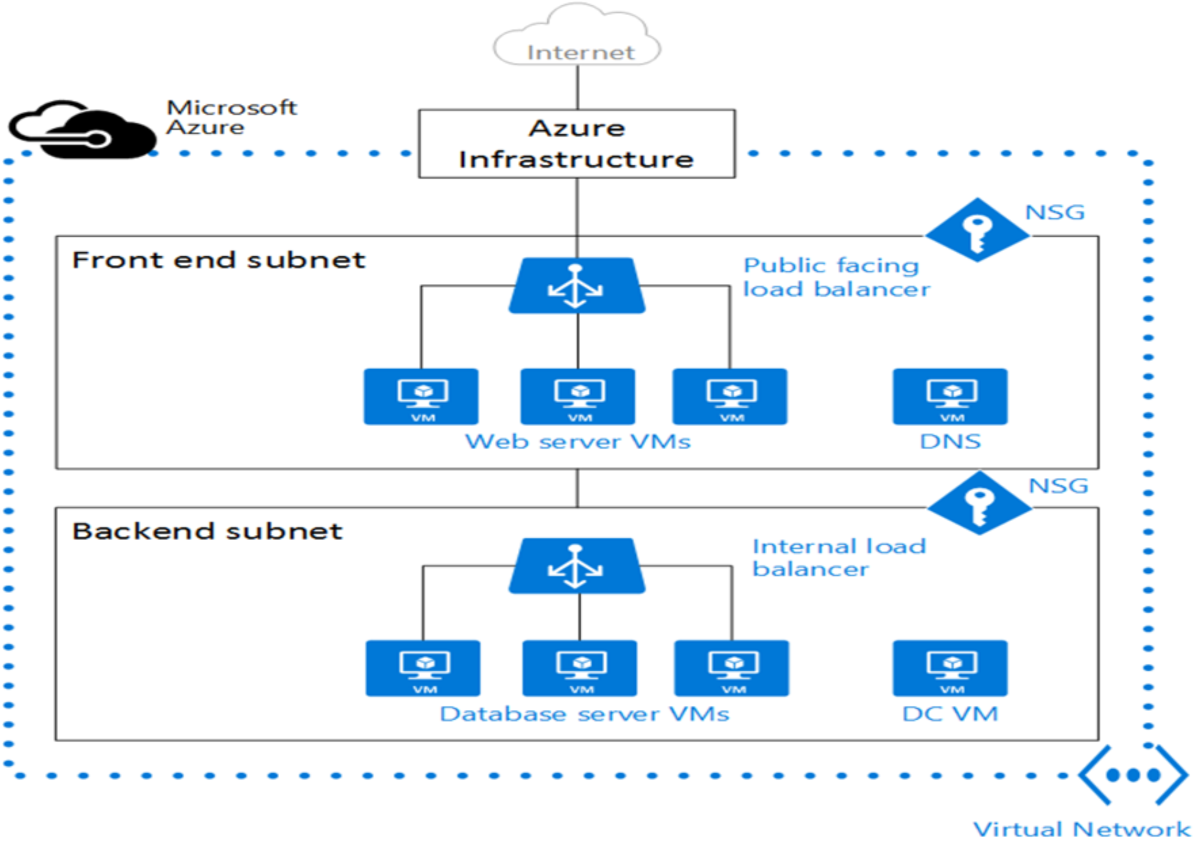
Azure VNET

- 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.



Azure Subnet

- A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for better organising and security.

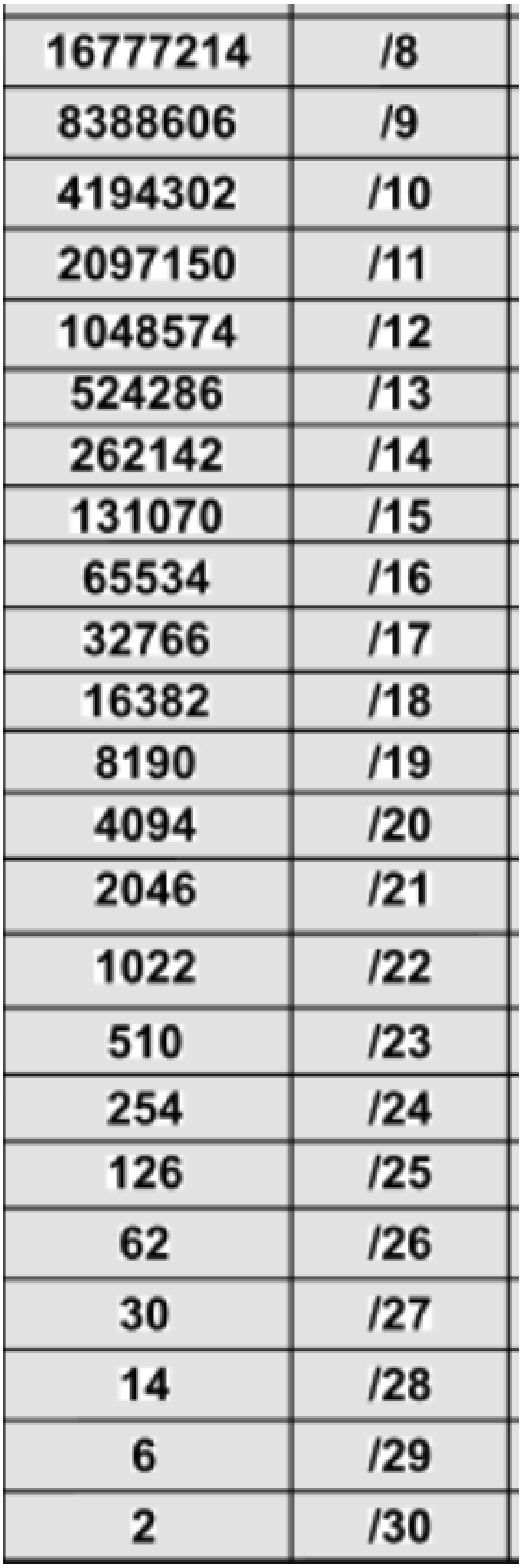


- When you set up a virtual network, you specify the topology, including the available address spaces and subnets. Select address ranges that don't overlap if the virtual network is connected to other virtual networks or on-premises networks. The IP addresses are private and can't be accessed from the Internet.
- When you create a VNET & Subnets, you must specify a **CIDR** block **(Classless Inter Domain Routing) (Determine size of VNET & Subnets)** for the VNET.

ADDRESS SPACE

- An IP is **32 bit number** & **4 Octets**, 1 octet being 8 Bits
- An IP Address looks like 10.0.0.0
- Total Bits - 32
- Netmask - X
- Result = Total Bits - Netmask
- Number Of Devices/IP's = 2 ^ Result

- /8 (Netmask) - 16 Million IP’s / Devices
- 8 - Result = Total Bits - Netmask → 32 - 8 = 24 → Number Of Devices/IP’s = 2 ^ Result → 2 ^ 24 = 16 Million IP’s / Devices



16777214	/8
8388606	/9
4194302	/10
2097150	/11
1048574	/12
524286	/13
262142	/14
131070	/15
65534	/16
32766	/17
16382	/18
8190	/19
4094	/20
2046	/21
1022	/22
510	/23
254	/24
126	/25
62	/26
30	/27
14	/28
6	/29
2	/30

Azure Reservation

- Azure reserves the first four and last IP addresses for a total of **5 IP addresses within each subnet**.
- For example, the IP address range of 10.0.1.0/24 has the following reserved addresses:

10.0.1.0 : Network address

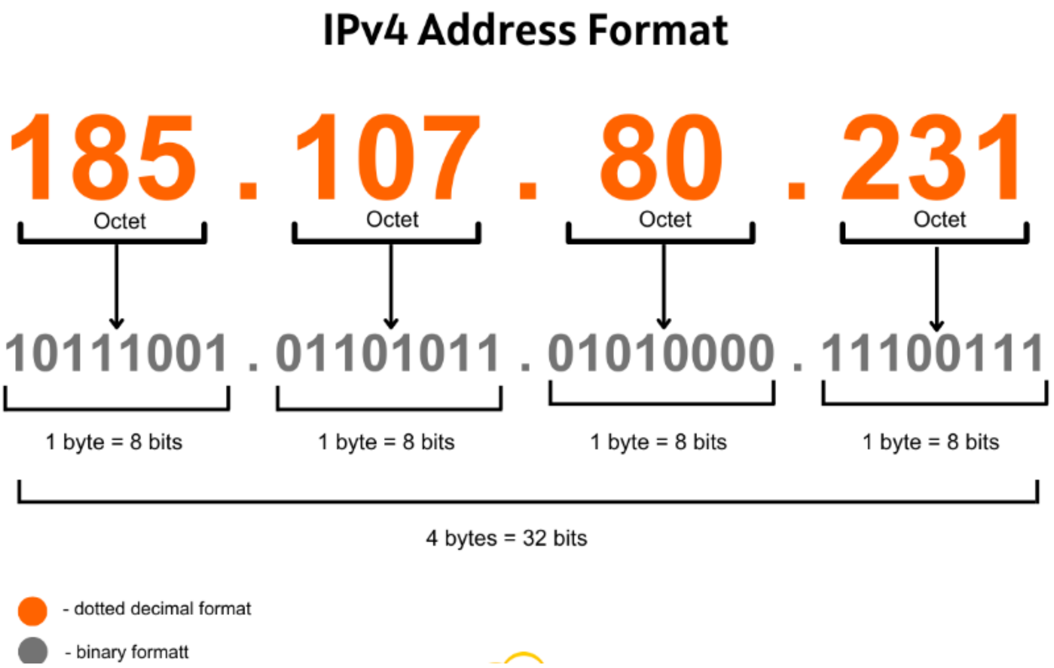
10.0.1.1 : Reserved by Azure for the default gateway

10.0.1.2, 10.0.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space

10.0.1.255 : Network broadcast address.

Ex: vnet : 10.0.0.0/16 = 65536
subnetA : 10.0.1.0/24= 251(5 ip reserved)
ADDRESS
SPACE

- An IP Address looks like 10.0.0.0
- An IP is **32 bit number** & **4 Octets**, 1 octet being 8 Bits



- Total Bits - 32

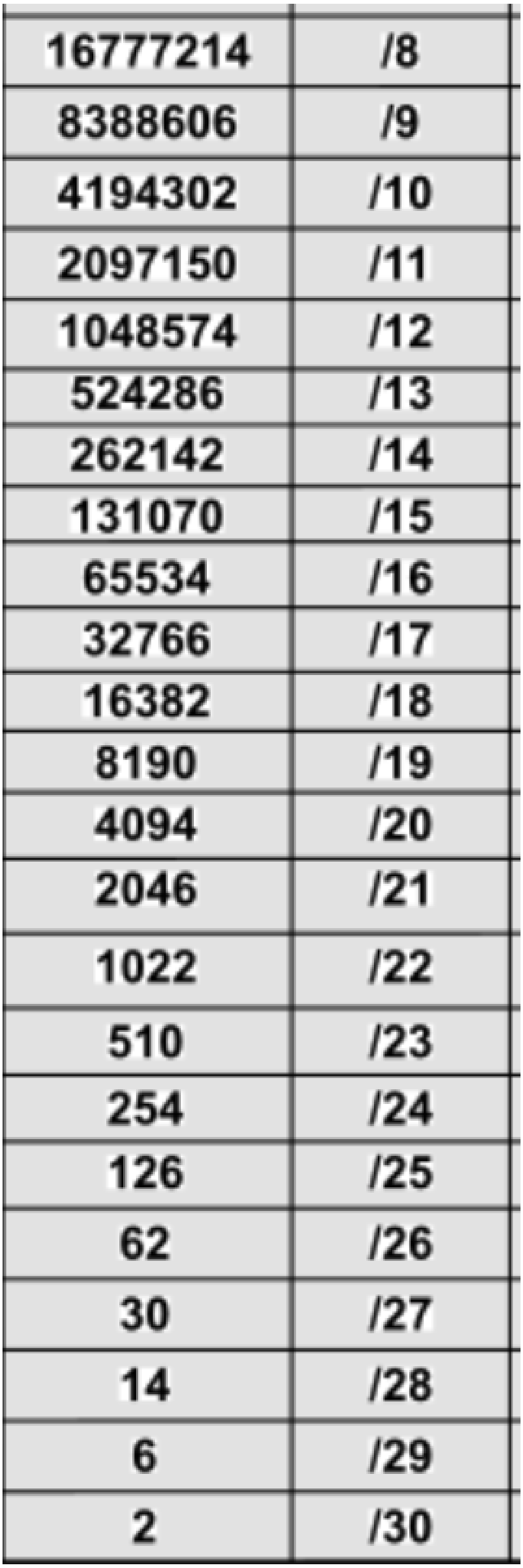
- Netmask - X
- Result = Total Bits - Netmask
- Number Of Devices/IP’s = 2 ^ Result

  Total bits - netmask (ex /24) = 2n

- If Netmask is /20 → Result = 32 - 20 = 12 i.e No Of IP’s = 2 ^ 12 = 4k
- If Netmask is /16 → Result = 32 - 16 = 16 i.e No Of IP’s = 2 ^ 16 = 65k
- If Netmask is /24 → Result = 32 - 24 = 8 i.e No Of IP’s = 2 ^ 8 = 256

  Website to calculate subnet mask

https://jodies.de/ipcalc?host=10.0.0.0&mask1=19&mask2=



16777214	/8
8388606	/9
4194302	/10
2097150	/11
1048574	/12
524286	/13
262142	/14
131070	/15
65534	/16
32766	/17
16382	/18
8190	/19
4094	/20
2046	/21
1022	/22
510	/23
254	/24
126	/25
62	/26
30	/27
14	/28
6	/29
2	/30

Azure Network Security Group (NSG)

- You can use an Azure network security group to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

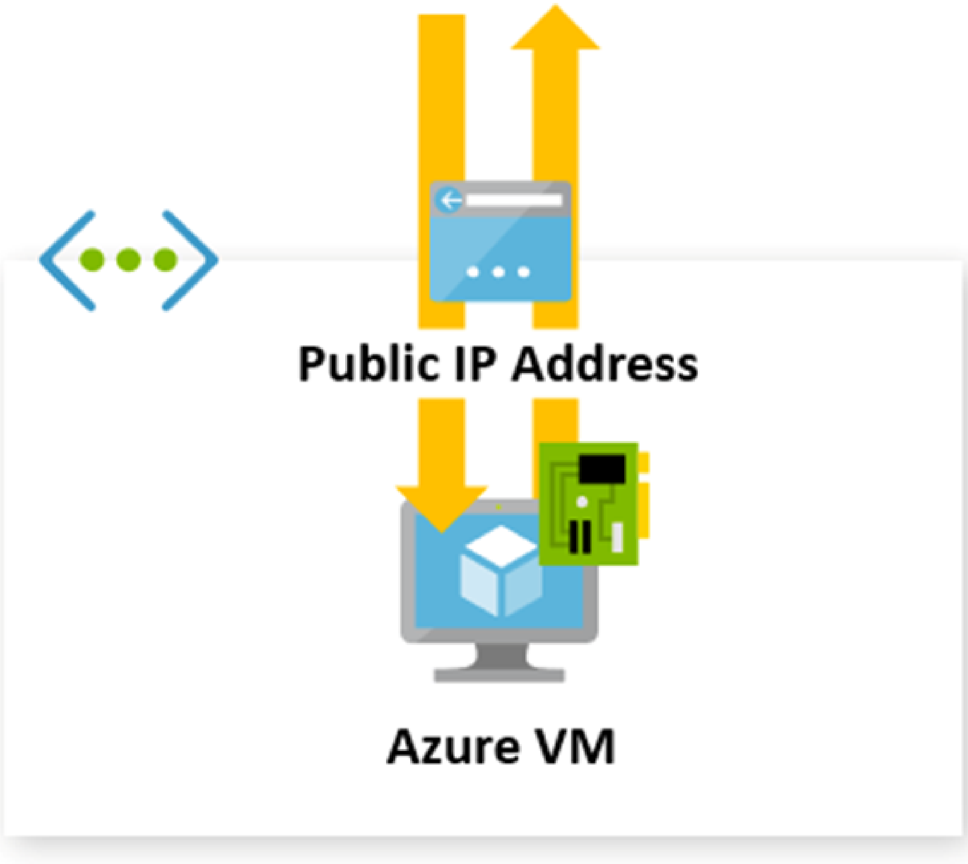
Azure Public IP

- Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses enable Azure resources to communicate to Internet and public-facing Azure services.

Azure NIC

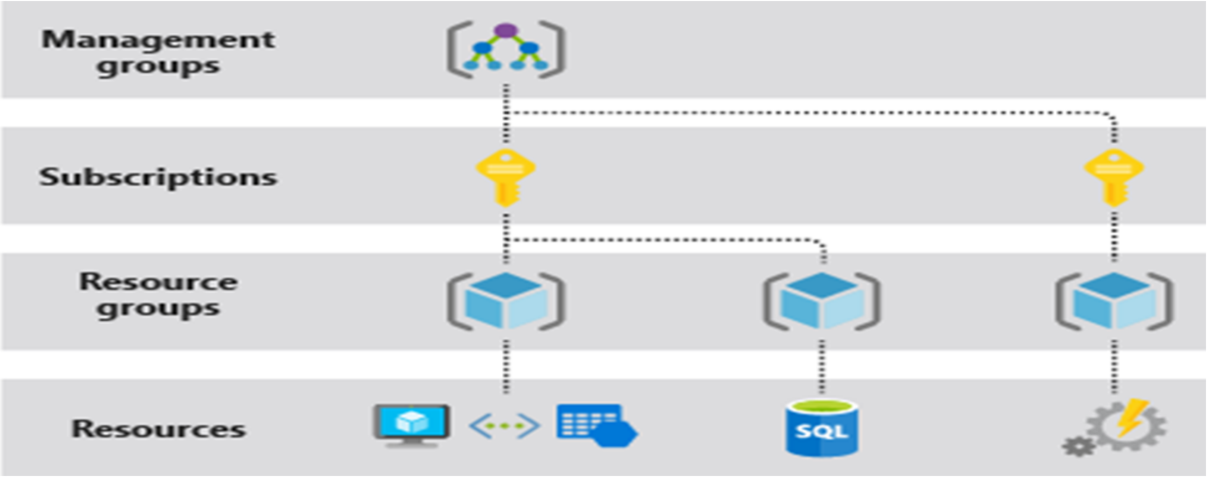
- A network interface enables an Azure Virtual Machine to communicate with internet, Azure, and on-premises resources. A virtual machine created with the Azure portal, has one network interface with default settings. You may instead choose to create network interfaces with custom settings and **add one or more network interfaces t**o a virtual machine when you create it.

Azure Public IP



- Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses enable Azure resources to communicate to the Internet.

Azure Resource Group



Azure, a resource group is a fundamental concept used to manage and organize Azure resources. A resource group is a logical container for resources deployed in Azure, and it helps you manage and organize these resources in a more efficient and consistent manner. Here are some key points about Azure resource groups:

Logical Container: A resource group is essentially a logical container that holds related Azure resources for an application or a solution. These resources can include virtual machines, storage accounts, virtual networks, web apps, databases, and more.

Azure Virtual Machines - VM’s

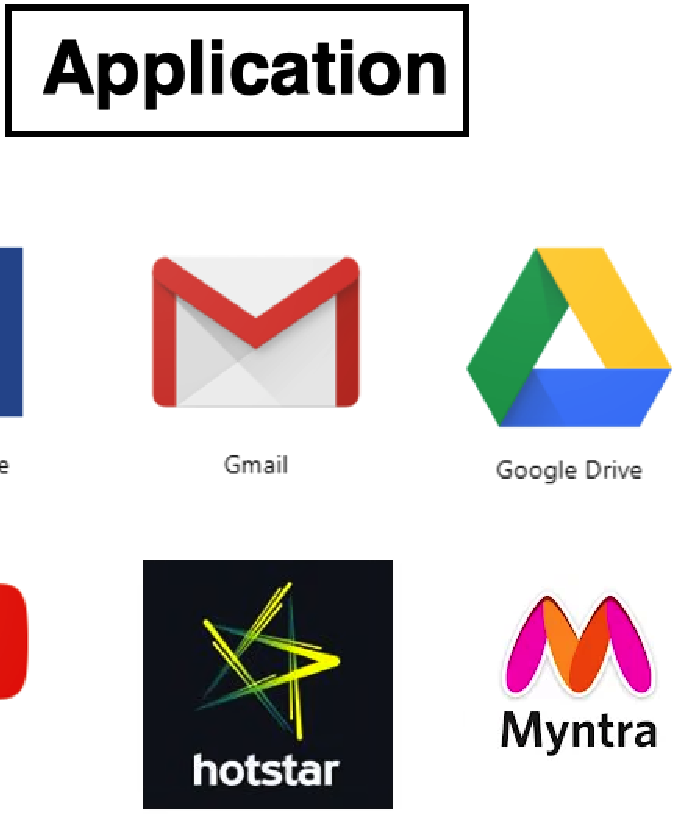
Azure VM Intro

- Azure virtual machines are one of several types of on-demand, scalable computing resources that Azure offers. Typically, you choose a virtual machine when you need more control over the computing environment than the other choices offer.
- An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it. However, you still need to maintain the virtual machine by performing tasks, such as configuring, patching, and installing the software that runs on it.

Create a VM

Application

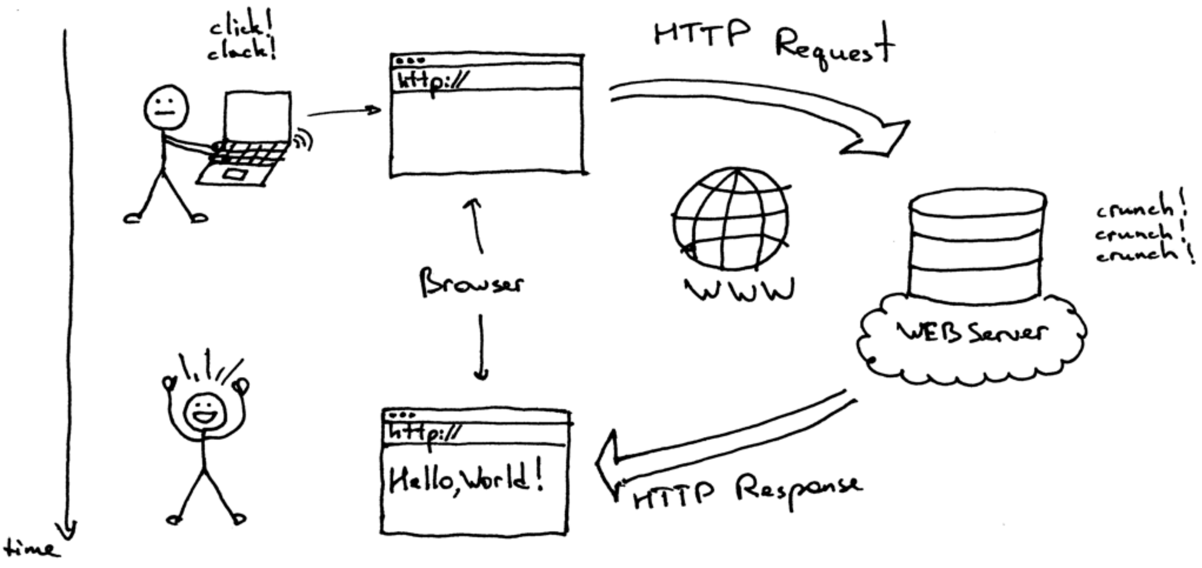
- An **application** is a **computer program** that is **designed for a particular task** typically to be used by end-users.



web server nginx
lms architecture
lms frontend backend deploy in vm

Web Server

WEB SERVER - A web server is computer software [**Nginx HTTP Server**] and underlying hardware [**AZURE VM**] that accepts requests via HTTP/HTTPS to distribute web content.



- **All computers that host websites must have web server programs**.

Installing Nginx Web Server

Nginx Web Server is not installed by default , the package name of Nginx HTTP Server - **nginx**

```
sudo apt install nginx -y
sudo systemctl status nginx
```

When troubleshooting issues related to web servers, it can be helpful to check the status of the server's processes. One way to do this is by using the command line interface and running the command `sudo systemctl status nginx`. This command will display information about the status of the Nginx web server, including whether it is running, any errors that may have occurred, and other iagnostic information.

```
sudo ss -ntpl | grep 80
sudo apt -y update
```

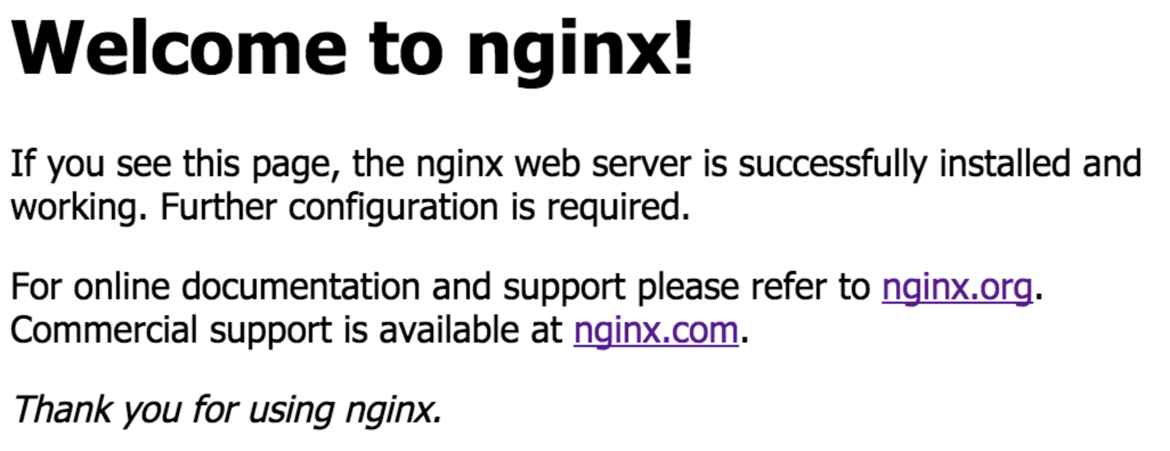
```
sudo apt -y install nginx
```

nstall Nginx by executing the command "sudo apt -y install nginx". This will automatically install Nginx and its dependencies. Once the installation is complete, you can configure Nginx to meet your specific needs. With Nginx insalled, you can take advantage of its powerful features to host web applications, serve static files, or act as a reverse proxy. So, start using Nginx today and discover why it is one of the most popular web servers in the world!

```
sudo systemctl status nginx
sudo ss -ntpl | grep 80
```

Test Web Server

> **Browse - http://public-ip**



Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.

Thank you for using nginx.

> If you are the website administrator: You may now add content to the directory **DocumentRoot** - **/var/www/html/**

The **/var/www/html/** directory is a critical component of the file system in a Linux operating system. It is the default directory where web server files are stored, such as HTML, CSS, and JavaScript files. The files stored in this directory are accessible via a web browser and are used to render web pages. Additionally, backups of this directory should be performed regularly to ensure that critical web server files are not lost in the event of a system failure or other disaster.

To **host a custom application** you can update the content of your site to **DocumentRoot**

i.e **/var/www/html**

```
ls /var/www/html
```

Private IP

- When you create a virtual machine in Azure, it's assigned a private IP address from the virtual network subnet it's connected to.
- This private IP address is used for communication between the virtual machine and other resources within the same virtual network.
- Use Case - Web Server to Database Server communication will happen over Private IP

Static IP

- Having a static IP in Azure means that your IP address does not change.
- Static IP can be useful when connecting to other services or applications that require a fixed IP address.
- Use Case - Web Server to Domain Mapping (DNS) will happen over Static IP

DNS

- DNS is a naming system that translates domain names to IP addresses, making it easier to access websites and internet services without having to remember specific IP addresses.

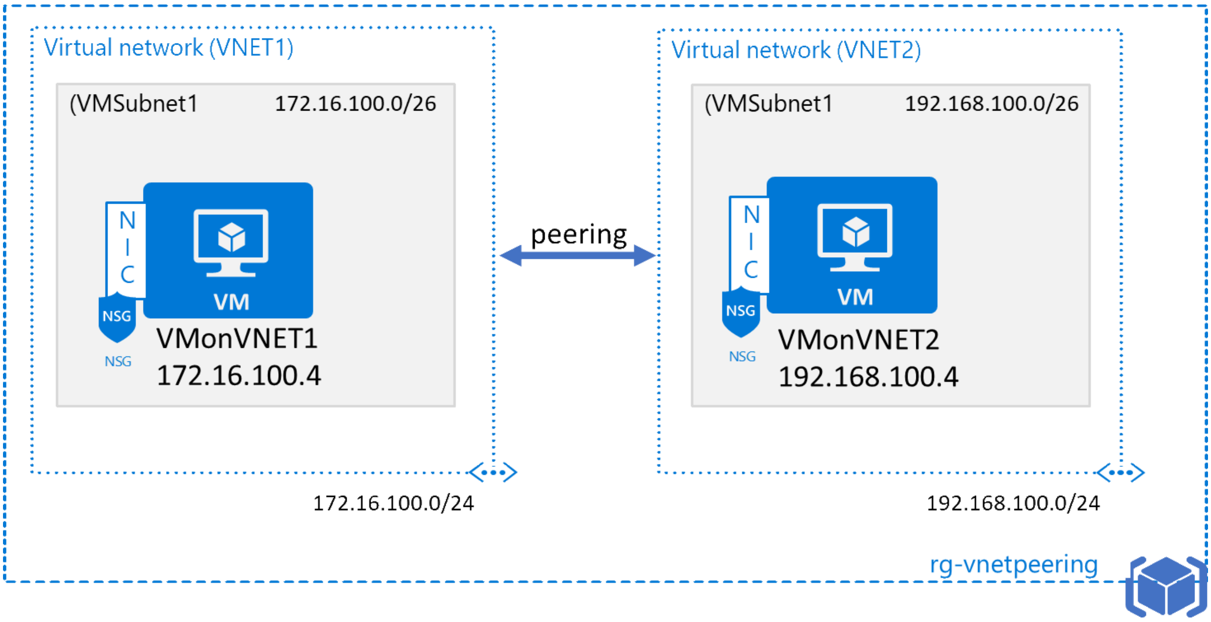
HTTPS

- HTTPS is a secure way to transmit data over the internet. It is a protocol that encrypts the data being transmitted and verifies the authenticity of the server before the data is sent.
- HTTPS is used to protect sensitive information such as passwords, credit card numbers, and personal information. This technology has become increasingly important in recent years due to the rise of cybercrime and the need for secure communication online.

Azure VNET Peering

- Virtual network peering enables you to seamlessly **connect two or more Virtual Networks in Azure**. The virtual networks appear as one for connectivity purposes.
- The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.
- Azure supports the following types of peering:
    - **Virtual network peering**: Connecting virtual networks within the same Azure region.
    - **Global virtual network peering**: Connecting virtual networks across Azure regions.
- The benefits of using virtual network peering, whether local or global, include:
    - A low-latency, high-bandwidth connection between resources in different virtual networks.

  - The ability for resources in one virtual network to communicate with resources in a different virtual network.
  - The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
  - The ability to peer virtual networks created through the Azure Resource Manager.
  - The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model. To learn more about Azure deployment models, see Understand Azure deployment models.
  - No downtime to resources in either virtual network when creating the peering, or after the peering is created.
- Network traffic between peered virtual networks is **private**. Traffic between the virtual networks is kept on the Microsoft backbone network. No public Internet, gateways, or encryption is required in the communication between the virtual networks.



```
wget http://repo.mysql.com/mysql-community-release-el7-5.no
arch.rpm
```

```
sudo rpm -ivh mysql-community-release-el7-5.noarch.rpm
```

```
sudo yum -y install mysql-server
```

```
sudo systemctl start mysqld
```

```
sudo systemctl enable mysqld
```

```
sudo systemctl status mysqld
```

```
sudo mysql_secure_installation
```