Assignment on DevOps

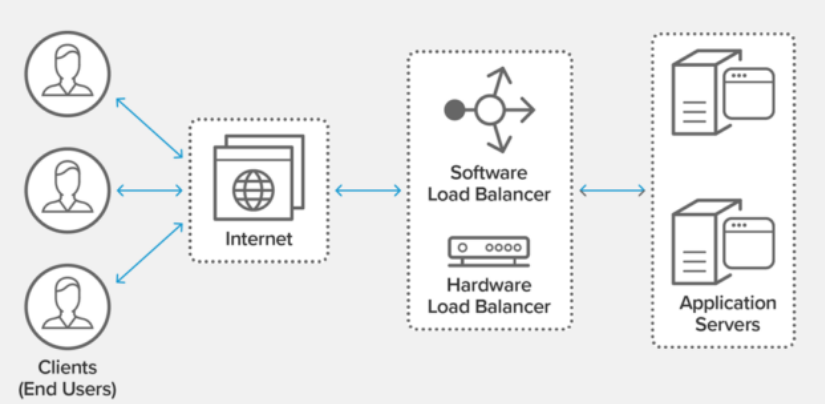
Date: 13-06-2021

1. What is Load balancer?

The role of load balancer is to balance the load of virtual machine or incoming traffic which is able to communicate with our servers. This is used for to increase capacity and reliability of applications.

A load balancer acts as the "traffic cop" sitting in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

Example: If SSC results/flipkart offers released in website, n no.of students are trying to open the same website on a same time, due to heavy load/server low the site will not help you.
This load balancer helps to share the work to n no.of servers and response get in quick way.



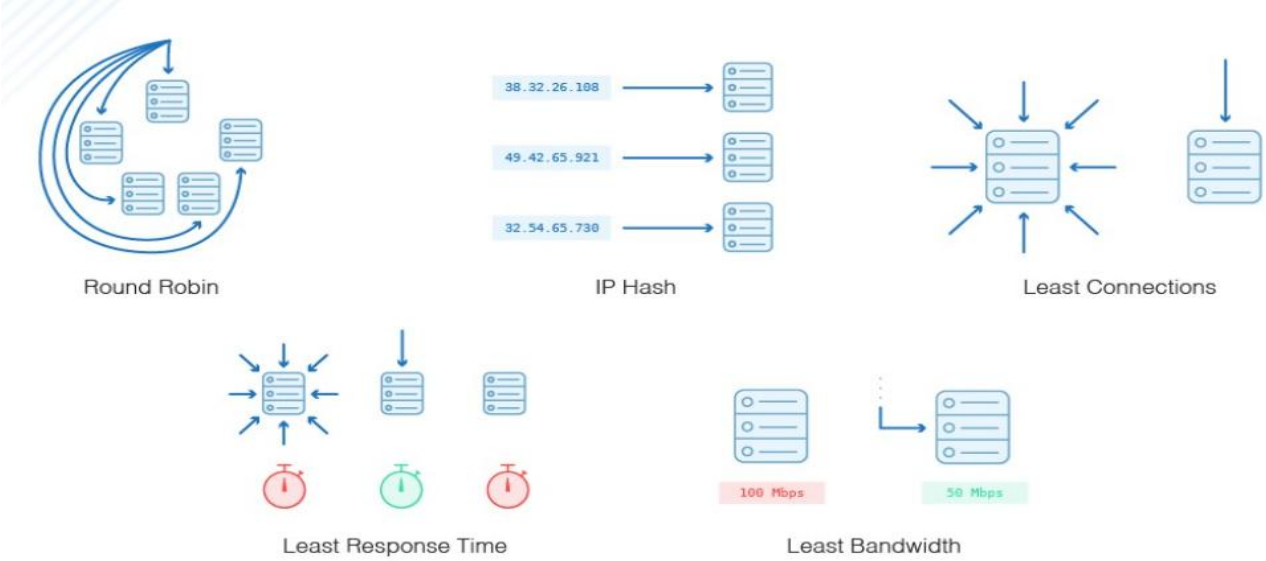
Fig(a) load balancer between client & server

2. Types of Load balancer?

There are many kinds of load balancer. The primary differentiating feature between load balancers is the load balancing algorithm used. Some of the popular loads balancing algorithms are as follows: Round Robin, IP Hash, Least Connections, Least Response Time, and Least Bandwidth.

- **Round Robin:** Sometimes the some requests are heavier than the other service, load is not correctly balance, In this Round Robin - Requests are distributed across the group of servers sequentially.
- **IP Hash:** In this straightforward load balancing technique, the client's IP address simply determines which server receives its request.
- **Least Connections:** As its name states, the least connection method directs - traffic to whichever server has the least amount of active connections. This is helpful during heavy traffic periods, as it helps maintain even distribution among all available servers.

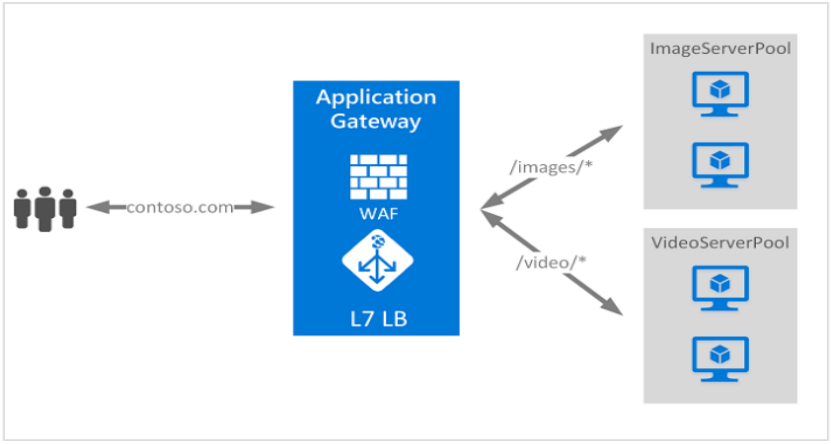
- **Least Response Time:** The least response time method directs - traffic to the server with the least amount of active connections and lowest average response time.
- **Least Bandwidth:** This application load balancer method measures traffic in megabits (Mbps) per second, sending client requests to the server with the least Mbps of traffic.



3. What is application gateway?

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications. Traditional load balancers operate at the transport layer (OSI layer 4 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.

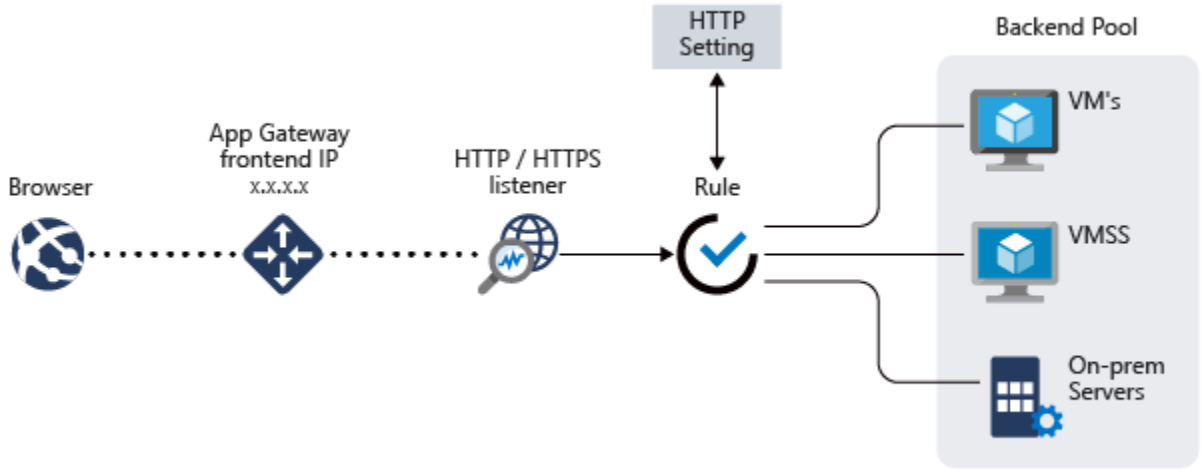
Application Gateway can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos. This type of routing is known as application layer (OSI layer 7) load balancing. Azure Application Gateway can do URL-based routing and more.



4. Difference between Load balancer and Gateway ?

Application Gateway (AGW) is a web traffic manager for your web applications (one or multiple).

1. With AGW, on top of load balancing your workloads, you can make routing decisions based on URI path or host headers. **For example**, you can route traffic based on the incoming URL. If /images are in the inbound URL, you can route traffic to a specific set of servers (or pool) configured for images. If /video is in the URL, that traffic is routed to another pool.
2. It can be used to do TLS/SSL termination. TLS/SSL termination can be useful to allow unencrypted traffic between AGW and backend servers saving some of processing load needed to encrypt and decrypt said traffic. However, sometimes unencrypted communication to the servers is not acceptable because of security requirements, compliance requirements, or application may only accept a secure connection. In these situations, Application Gateway also supports end-to-end TLS/SSL encryption.
3. It includes a web application firewall (WAF) that protects your workload from common exploits like SQL injection attacks or cross-site scripting attacks, to name a few.
4. It provides application delivery controller (ADC) as a service, offering various Layer 7 load-balancing capabilities. Use it to optimize web farm productivity by offloading CPU-intensive SSL termination to the gateway.

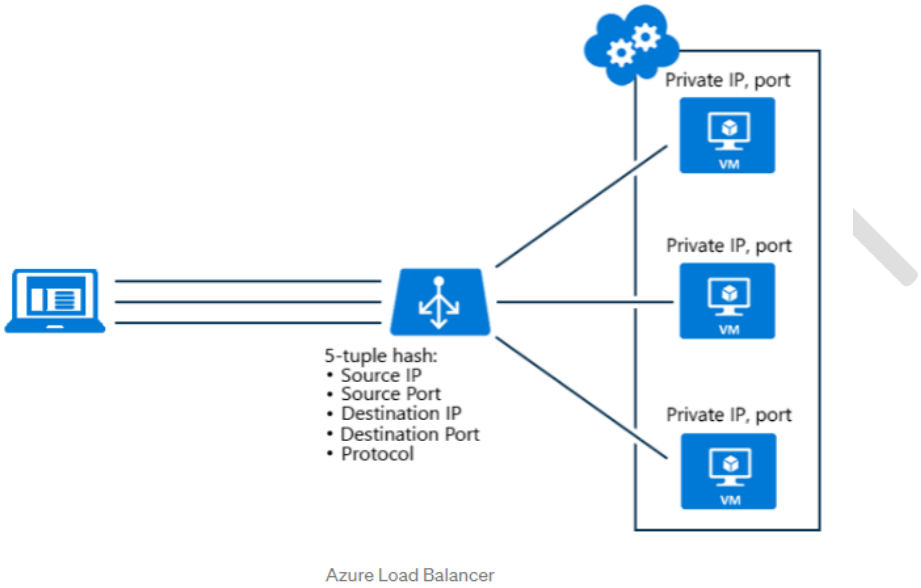


Azure Application Gateway — Backend Pools

Azure Load Balancer: - Load balancing refers to evenly distributing load (incoming network traffic) across a group of backend resources or servers. Azure Load Balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.

1. It can also provide outbound connections for virtual machines inside your virtual network by translating their private IP addresses to public IP addresses.

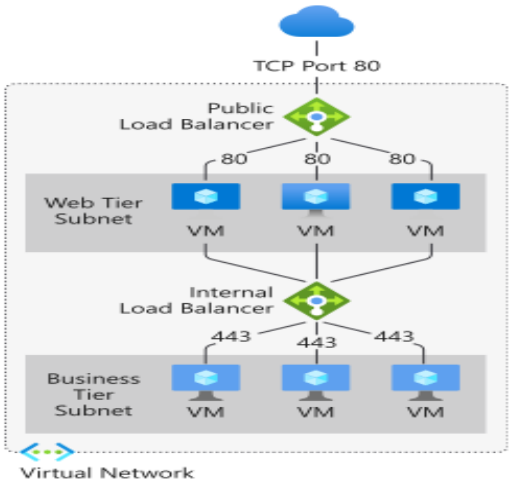
2. It is a TCP/UDP load balancing and port forwarding engine only. It does not terminate, respond, or otherwise interact with the traffic. It simply routes traffic based on source IP address and port, to a destination IP address and port.
3. Azure Load Balancer is a high-performance, low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. It is built to handle millions of requests per second while ensuring your solution is highly available. It is zone-redundant, ensuring high availability across Availability Zones.



Azure Load Balancer

A **public load balancer** can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

An **internal (or private) load balancer** is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.



Azure Load Balancer

5. How do you configure IIS Web server in your windows server? Why it is important.

IIS is a windows service that allows you to host and manage websites on windows system.

Developer creates a website it can be asp.net website, static HTML website or any type of websites. And you want to make this website publicly available to everyone on this planet – so anyone go to your website name and access this, all operation is called website hosting– for all these you need a server a computer and this server will have a public IP & now you put this website inside the server and your website is online in the internet.

Login to the portal (Microsoft Azure)
Goto virtual machine – create VM's (VM1)
Click on VM1 and connect (it will download the RDP file)
Open the RDP file with windows security user name, password

Create a resource – windows server 2019 datacenter
New resource group (name: webserverRG)
Instance details VM name: (VM1)
Region: (UK south)

Administrator username (localadmin)
Password (******)
Confirm password (******)

Select inbound port (RDP 3389)

Review+caste (deployment is completed)

Goto resource – copy the public Ip address

Goto to windows & open Remote Desktop Connection

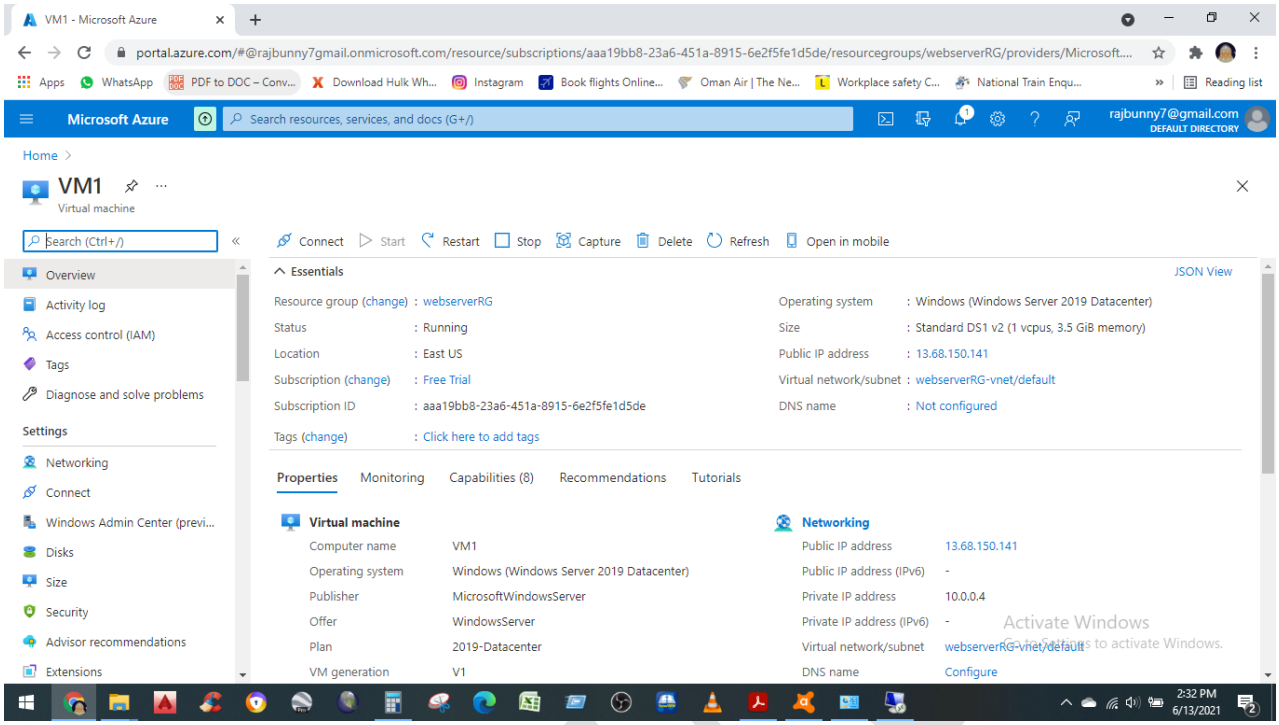
Paste the ip address in name & connect

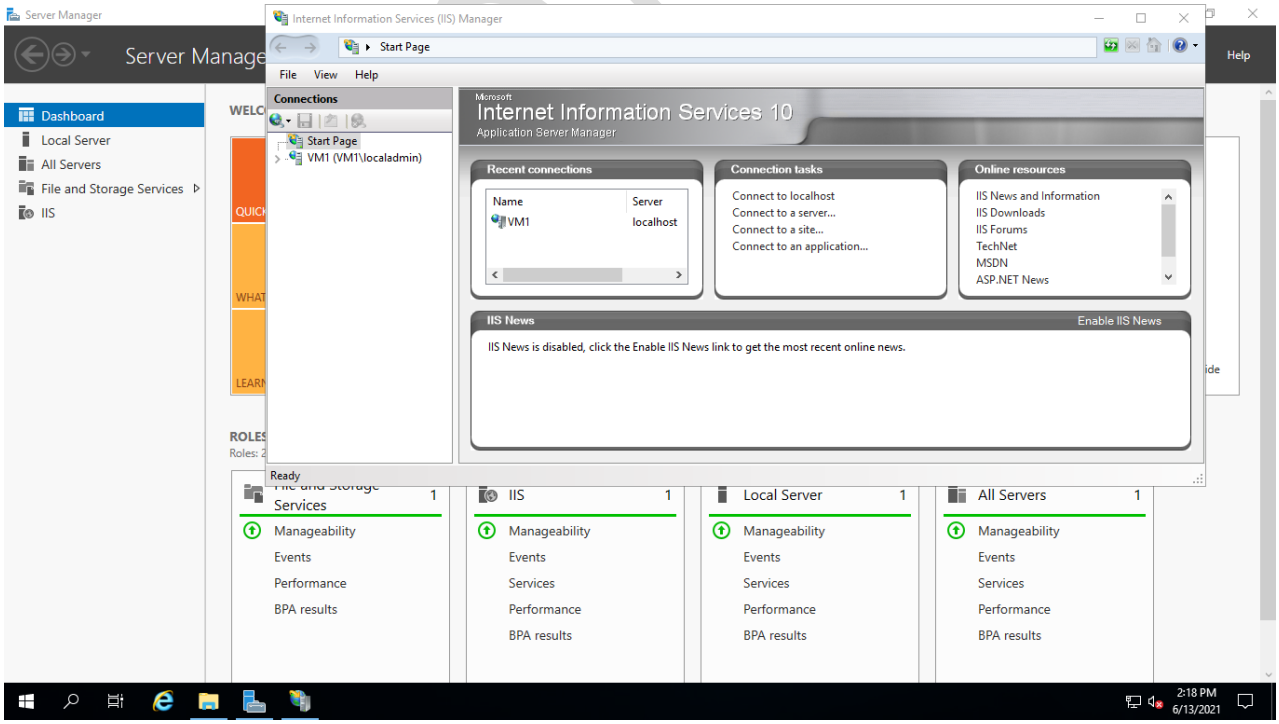
Type user name as given in portal (localadmin & password****)

System will get popup & built the software server

Goto server manager – click on add roles & features (select roles as a **Web server IIS** -add feature, select ftp server service) the install

IIS installed in server manager


VM1 - Microsoft Azure
portal.azure.com/#@rajbunny7gmail.onmicrosoft.com/resource/subscriptions/aaa19bb8-23a6-451a-8915-6e2f5fe1d5de/resourcegroups/webserverRG/providers/Microsoft....
Microsoft Azure
Search resources, services, and docs (G+/)
rajbunny7@gmail.com
DEFAULT DIRECTORY
Home
VM1
Virtual machine
Search (Ctrl+/)
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center (previ...
Disks
Size
Security
Advisor recommendations
Extensions
Essentials
JSON View
Resource group (change) : webserverRG
Status : Running
Location : East US
Subscription (change) : Free Trial
Subscription ID : aaa19bb8-23a6-451a-8915-6e2f5fe1d5de
Tags (change) : Click here to add tags
Operating system : Windows (Windows Server 2019 Datacenter)
Size : Standard DS1 v2 (1 vcpus, 3.5 GiB memory)
Public IP address : 13.68.150.141
Virtual network/subnet : webserverRG-vnet/default
DNS name : Not configured
Properties
Monitoring
Capabilities (8)
Recommendations
Tutorials
Virtual machine
Computer name VM1
Operating system Windows (Windows Server 2019 Datacenter)
Publisher MicrosoftWindowsServer
Offer WindowsServer
Plan 2019-Datacenter
VM generation V1
Networking
Public IP address 13.68.150.141
Public IP address (IPv6) -
Private IP address 10.0.0.4
Private IP address (IPv6) -
Virtual network/subnet webserverRG-vnet/default
DNS name Configure
Activate Windows
Go to Settings to activate Windows.
2:32 PM
6/13/2021


Server Manager
Server Manage
Dashboard
Local Server
All Servers
File and Storage Services
IIS
Help
Internet Information Services (IIS) Manager
Start Page
File View Help
Connections
Start Page
VM1 (VM1\localadmin)
Microsoft
Internet Information Services 10
Application Server Manager
Recent connections
Name Server
VM1 localhost
Connection tasks
Connect to localhost
Connect to a server...
Connect to a site...
Connect to an application...
Online resources
IIS News and Information
IIS Downloads
IIS Forums
TechNet
MSDN
ASP.NET News
IIS News
Enable IIS News
IIS News is disabled, click the Enable IIS News link to get the most recent online news.
Ready
Services 1
IIS 1
Local Server 1
All Servers 1
Manageability
Events
Performance
BPA results
Services
2:18 PM
6/13/2021

6. What is Public IP & Private IP?

Public IP address:- is the IP address that is logged by various servers or devices when you connect to them through your Internet connection. Like postal address used to deliver a postal mail to your home, the public IP address is the globally unique IP address assigned to a computing device. So, the web browser, email server or any other server device directly from the Internet could be the public IP address.

Any public accessibly network hardware such as a home router, or the servers hosting websites requires the public IP address.

Private IP address:- is the same as a public IP address. It is a unique identifier for all the devices behind a router or other devices that servers IP address.

With the private IP address, the devices in your home are able to have the same private IP address as anyone else around the world. Due to the private IP address are non-routable-hardware devices on the Internet and programmed to prevent devices with a private IP address from communicating directly with any other IP beyond the router that they are connected to.

The private IP address has the following three ranges.

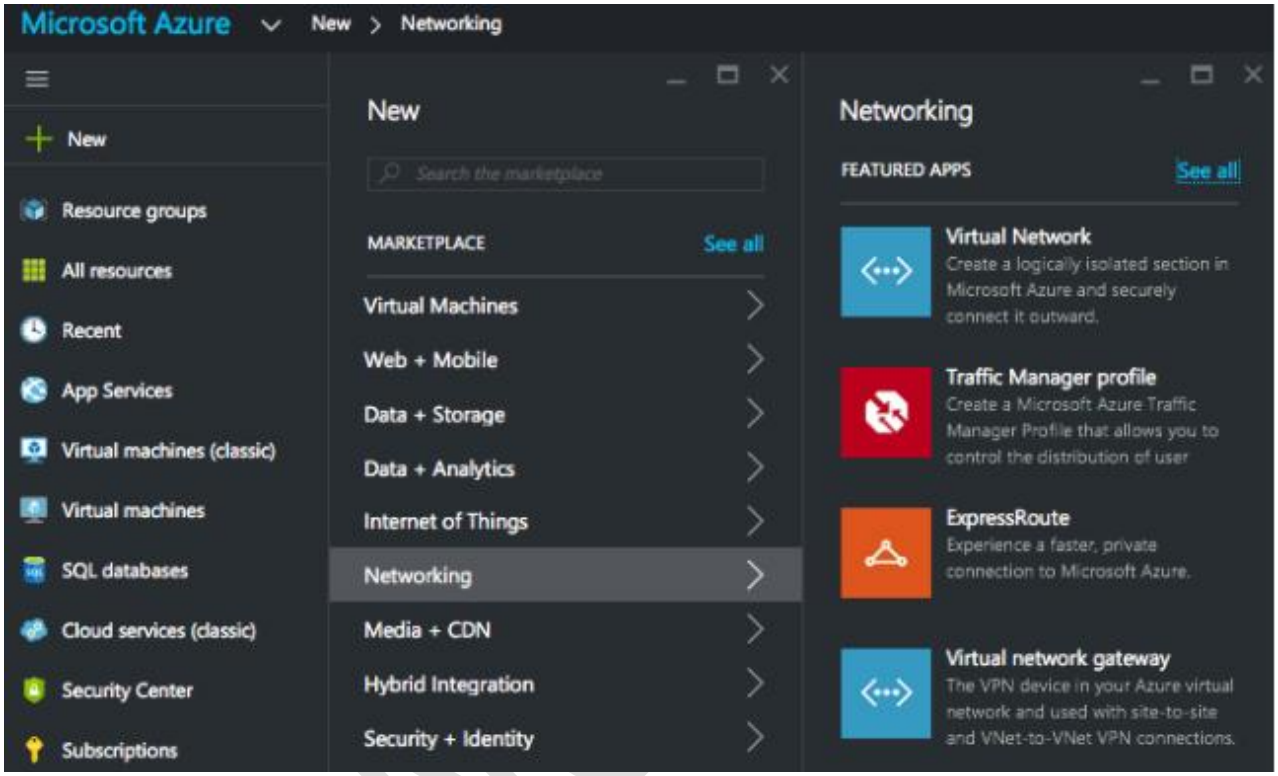
1. 10.0.0.0 - 10.255.255.255
2. 172.16.0.0 – 172.31.255.255
3. 192.168.0.0 -192.168.255.255

As for the public IP address, the rest of private IP addresses are public

Private IP	Public IP
Used with LAN or Network	Used on Public Network
Not recognized over Internet	Recognized over Internet
Assigned by LAN administrator	Assigned by Service provider / IANA
Unique only in LAN	Unique Globally
Free of charge	Cost associated with using Public IP
Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255	Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255

7. What is Vnet & subnet?

A **Virtual Network**, also known as a VNet is an isolated network within the Microsoft Azure cloud. VNets are synonymous to AWS VPC (Virtual Private Cloud), providing a range of networking features such as the ability to customize DHCP blocks, DNS, routing, inter-VM connectivity, access control and Virtual Private Networks (VPN).



A **subnet** is a range of IP addresses in the VNet, you can divide a VNet into multiple subnets for organization and security. Additionally you can configure VNet routing tables and Network Security Groups (NSG) to a subnet

Under the VNet, we must understand what Subnet is and how it works.
Subnetting is the process of dividing a network into small networks,

- We can divide the VNet IP Range into multiple Parts of unique Subnet IP ranges.
- Resources within the subnet will communicate with each other and also communicate across the subnets in the same VNet with the help of Network Security Groups, so communication between the Subnets is up to our choice.

For Example,
There are two classrooms in a school. Consider a classroom as a subnet.
Class A leader wants to get a duster from Class B, but the class was enclosed, he can go by open door.
Here the Door is a Network security group, it will act as a firewall for subnets as well as resources in the subnet.

- Resources in different VNets can't communicate with each other.

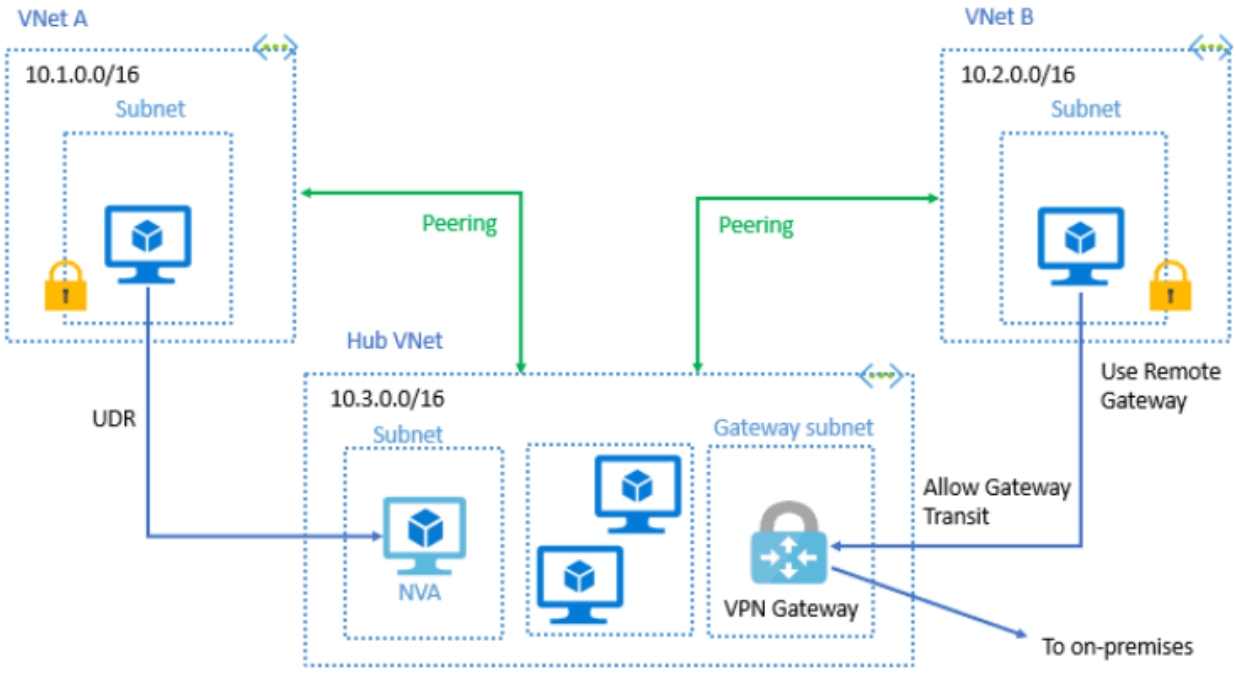
8. What is vnet peering ?

Azure Virtual Network is used for the Virtual Network Peering empowers users to flawlessly communicate with virtual networks in Azure. **VNet Peering in Azure** allows the traffic of one virtual network to communicate to another virtual network. This is basically used for database failover, disaster recovery, or cross-region data replication.VPN gateways are used in an encrypted connection in the region but VNet Peering provides connection sharing in different regions.

- VNet peering is similar to an inter-VLAN Routing in VLAN of On-premise networks so it works similarly to inter-VLAN connect to one VLAN to another VLAN for communication.
- In Azure infrastructure, need to connect to virtual networks to each other for sharing traffic which can be applications, backup, replication, recovery, or information sharing.
- The virtual machines of virtual network connections to other virtual machines of different Virtual network via connection of VNet Peering in the same region or across the region

Types of VNet Peering

- **Default VNet Peering:** it empowers the connectivity between various VNets within the same Azure region.
- **Global VNet Peering:** it allows Virtual networks to connect across different Azure regions. It provides private peering with low latency and high bandwidth in Azure backbone infrastructure.



9. How to monitor you services in Azure is(healthy or not)/ Is working properly or not

Whether you run Linux or Windows on Azure, you will want to monitor certain basic VM-level metrics to make sure that your servers and services are healthy. Four of the most generally relevant metric types are **CPU usage**, **disk I/O**, **memory utilization** and **network traffic**.

- **CPU usage** is one of the most commonly monitored host-level metrics. Whenever an application's performance starts to slide, one of the first metrics an operations engineer will usually check is the CPU usage on the machines running that application.

Name	Description	Metric type
CPU percentage	Percentage of time CPU utilized	Resource: Utilization
CPU user time	Percentage of time CPU in user mode	Resource: Utilization
CPU privileged time	Percentage of time CPU in kernel mode	Resource: Utilization

- **Monitoring disk I/O** is critical for understanding how your applications are impacting your hardware, and vice versa. For additional visibility beyond the VM-level metrics covered here, you can also collect metrics from your Azure storage accounts to determine if your storage is being throttled or has availability issues that could impact performance.

Name	Description	Metric type
Disk read	Data read from disk, per second	Resource: Utilization
Disk write	Data written to disk, per second	Resource: Utilization

- **Monitoring memory** usage can help identify low-memory conditions and performance bottlenecks.

Name	Description	Metric type
Memory available	Free memory, in bytes/MB/GB	Resource: Utilization
Memory pages	Number of pages written to or retrieved from disk, per second	Resource: Saturation

- Azure's default metric set provides data on **network traffic** in and out of a VM. Depending on your OS, the network metrics may be available in bytes per second or via the number of TCP segments sent and received. Because TCP segments are limited in size to 536 bytes each, the number of segments sent and received provides a reasonable proxy for the overall volume of network traffic.

Name	Description	Metric type	Availability
Bytes transmitted	Bytes sent, per second	Resource: Utilization	Linux VMs
Bytes received	Bytes received, per second	Resource: Utilization	Linux VMs
TCP segments sent	Segments sent, per second	Resource: Utilization	Windows VMs
TCP segments received	Segments received, per second	Resource: Utilization	Windows VMs

10. what are different types of disks we have when you create vm ?

Following is a summary comparing Azure Disk types.

Disk Type	Premium SSD	new Standard SSD	Standard HDD
Summary	Designed for IO intensive enterprise workloads. Delivers consistent performance with low latency and high availability.	Designed to provide consistent performance for low IOPS workloads. Delivers better availability and latency compared to HDD Disks.	Optimized for low-cost mass storage with infrequent access. Can exhibit some variability in performance.
Workload	Demanding enterprise workloads such as SQL Server, Oracle, Dynamics, Exchange Server, MySQL, Cassandra, MongoDB, SAP Business Suite, and other production workloads	Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test	Backup storage
Max IOPS	7,500 IOPS provisioned	Up to 500 IOPS	Up to 500 IOPS
Max Throughput	250 MBPS provisioned	Up to 60 MBPS	Up to 60 MBPS