**Virtual Machines**

Components to create virtual machine are

1)VNet

2)NIC

3)NSG

4)Public IP(optional)

Vm has two ip’s

public(internet)

private (intranet)

While creating vm we can chose following options

Can be opt to this options only while creation

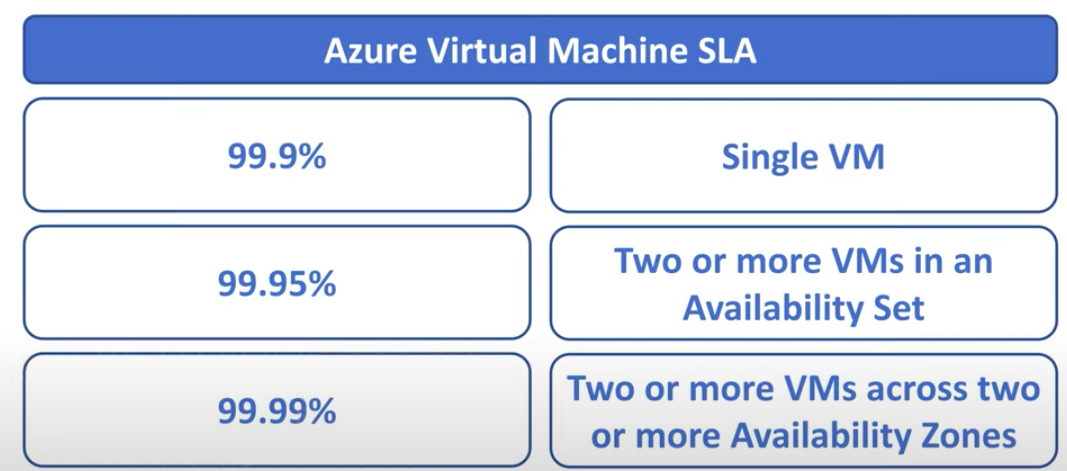
1)No infra redendency - no changes in configuration even if the cpu reaches to 100%

2)Availability set - an availability set is concept with in data centre that grouped with fault domains and updated domains(logical groups)

to eliminate single point of failure it has

a)Fault domains(3 vm’s can be created) - VM’s in it will share the configuration of rack like cpu , power , ram , memory - grouping multiple servers in multiple racks(eg 5 servers in 3 racks) - if rack has power or memory failure only those servers will get effected

b)updated domain(20) - it is logical grouping - for example if we want to update the patches of servers then we will group set of servers in updated domain and will reboot them so that other servers will available and these update domain servers will down for 30 min

3)Availability Zone - to overcome data centre failures , even though one region gets failed we can use from the other region data centre - SLA service level availability



4)VMSS - can increase configuration of vm based on cpu and memory

**horizontal scaling vs vertical scaling**

Horizontal scaling means scaling by adding more machines to your pool of resources (also described as “scaling out”), whereas vertical scaling refers to scaling by adding more power (e.g. CPU, RAM) to an existing machine (also described as “scaling up”).

NSG(network security group)

security rules

Inbound policy - accessing vm from internet (incoming request)

3389 port - it should be enabled for window

22 - linux

http(80)(with out ssl certificate) - web calls

An SSL certificate is **a digital certificate that authenticates a website's identity and enables an encrypted connection**. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.

https(443)(ssl certificate enabled)

outbound policy - accessing from vm to internet

**DISKS**

**OS Disk - Hard disk(HDD) - managed disk - stored in the vm - performance will be slow**

**Data disk (SSD) - unmanaged disk - stored in storage account high performance - we can extend the storage**

**Networking**

**Own representation of private environment**

Address space - range of ip’s in network is configured under Address space based on **CIDR( class less inter domain routine)**

CIDR - A record - private network - 0-127 (0.0.0.0 - 127.255.255.255)

- B record - On premises network - 128-191 (128.0.0.0 - 191.255.255.255)

-C record - 192-223(most of public ip’s)

-D record - 224- 239

-E record - 240 - 255

IPv4 - 32 bit - 2^32-n - suffix of ipv4 - 2^32-16 - 65536 adresses

IPv6 - 128 bit - 2^128-16

Subnet - default subnet range 10.0.0.0/24 - this indicated this subnet has 2^32-24 = 2^8 = 256

in this **5 will be reserved for azure** (network address , default gateway , DNS , network broadcast , azure netscale)

scenario - if you want to create subnet of having 10 ip addresses then will keep subnet range as 10.0.0.0/28

2^32-28 = 2^4 =16

as 5 are reserved , here we will get 11 addresses

Public IP address

Static IP - Constant ip(for server)

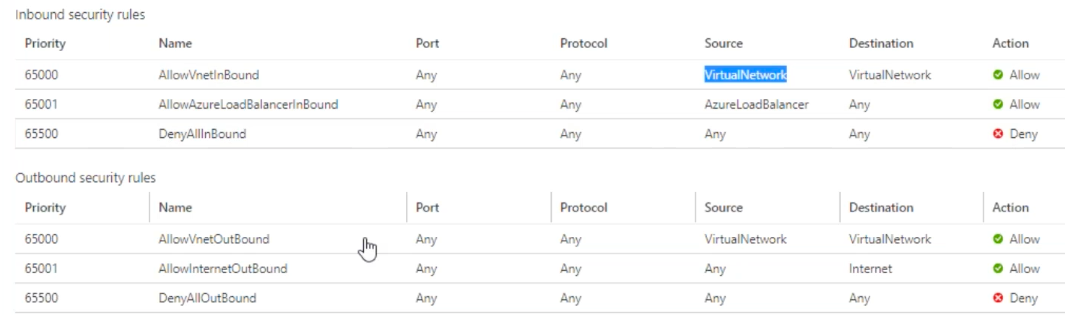
Dynamic IP - not a fixed ip … when ever we are restarting it will assign new ip

**NSG**

internet —>NSG —>n/w—->VM

inbound rules - incoming request - request from internet to internal vm

outbound rules - vm to internet

default rules

Priority

lowest number has highest priority

NSG can not be bind in VNET level , it can be bind in subnet level only

Peering(connection between two vnets)

#Peering is of two types

1)Vnet to Vnet Peering— Both Vnet should be on the same region

establishing connection between two vnets with in a same regions

2)Global Vnet Peering- Both Vnet can be in a different regions

establishing connection between two vnets with in a different regions

Practical procedure for establishing Peering between two Vnet’s in Azure portal:

Need two Vnets like below

**Vnet to Vnet Peering**

1. Vnet - Own representation of private environment
2. Adress
3. subnet
4. Region

**Global Vnet Peering**

1.vnet

2.address

3.subnet

4.gatewaysubnet

5.virtual gateway n/w

Public cloud - azure

private cloud - own network

hybrid cloud - both

class 42

**Point to sight**

when the connection has to be established from public to secured private VNet then point to sight is used.

public —————-> private Vnet

i)client certificate

ii)root certificate

iii)VPN

public

i)client certificate

ii)root

iii)VPN

private net

Site to site

**Traffic manager**

—>Routes the traffic from the client to appropriate endpoint(web app or app service running outside azure)

here azure traffic manager uses dns to direct the request to appropriate endpoint using one of the following routing methods

routing methods —>

i)performance - to use the nearest endpoint for the lowest n/w latency

ii)priority - to have a primary service endpoint for all traffic

iii)weightage - to distribute traffic across set of endpoints (eg 70 , 30 or 20 , 20 ,20,20,20)

iv)Geography -to direct to specific endpoint based on where the request originated from geographically( eg- when india ola app has to use only from india only .. other than india it will show service not found)

end points can be three types

1)azure endopoint

2)external endpoints

3)nested endpoints

**Azure load balancer**

*Load balancing* refers to evenly distributing load (incoming network traffic) across a group of backend resources or servers.

Azure Load Balancer operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. 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.

A [public load balancer](https://learn.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) 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](https://learn.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) 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.