Tiwari.chandan08@outlook.com

[Email address]

MICROSOFT AZURE

1-: Network Operating System (Run On server computer)

**Server-:** A server is a computer program or device that provides the functionality for other programs or device, called clients. For example (Web Server, File Server, SAP HANA, Database server, Backup server, Domain controller, Tally server etc.)

**Windows network Operating System-:** windows server 2008, windows server2012, windows server2016 and windows server2019

**Linux network operating system-:** Redhat Linux, SUSE Linux

**Processor**-Xeon Processor

**2-: Client Operating System-:**

**Client-:** A client is a piece of computer hardware or software that access a service made available by a server. For example, web browser are client that connect to web server and retrieve web pages for display.

**Windows-:** Windows7, windows8, windows10

**Linux-:** Ubuntu Centos

**Processor:** Corei3, corei5, corei7

**Traditional IT**

Switch

Primary Data Centre

Xeon Processor

Xeon Processor

Xeon Processor

Xeon Processor

Xeon Processor

Xeon Processor

File Server

SAP Server

Tally Server

Web Server

DC Server

Backup Server

* In Tradition IT we purchase hardware for each application
* In Traditional IT hardware cost increase.
* In Traditional IT OS cost Increase
* DR(Disaster Recovery)

**Virtualization**

For virtualization, purchase high configuration hardware and enable virtualization technology,

There are two organization which is work on virtualization.

1-Microsoft-Hyper V

2-

* VM Ware-ESXI

VM Ware-Work Station

DB Server

2GB RAM

Back up Server

2GB RAM

XEON

HR Server

2GB RAM

File Server

2GB RAM

File Server

2GB RAM

VM WARE Work Station

Windows server 2012

10TB HDD

256GB RAM

XEON Processor

**\*In Virtualization Hardware cost decrease.**

**\*OS cost Increase**

**Draw Back of Virtualization**

**\*Electricity Increase**

**\*DR Costly**

**\*On Premise Computing-Physically Operated(mouse,laptop,switch)**

**\*Cloud Computing-Manage by Microsoft**

**Overview of Cloud Technology**

**Cloud Computing**: Cloud computing is the delivery of computing service-servers, storage, database, networking, software, analytics and more-over the internet.

There are three types of cloud computing.

1-Public cloud

2-Private cloud

3-Hybrid cloud

**Public Cloud-**Public clouds are owned and operated by third party cloud service provider, which deliver their computing resource like servers and storage over the internet.

Microsoft azure is an example of public cloud. With a public cloud all hardware, software and other supporting infrastructure’s owned managed by the cloud provider. You access and manage your account using web browser.

For example, a customer who wants such a cloud so that my users can access over the internet from anywhere and the environment that is made is cheaper.

1-Multitenant ID (Two or more than Organization): HCL, IBM, JIO

2-Shared Hardware:

3: Isolate

5: Cheaper

5: you can access over the internet.

**Private Cloud:** A private cloud refers to cloud computing resource used exclusively by a single business or organization. A private cloud can be physically located on the company’s on-site data Centre. Some companies also pay third party service providers to host their private cloud. A private cloud is one in which the service and infrastructure are maintained on a private network.

For example, a customer who wants such a cloud so that my users can access only within the organization and the hardware on which the data is being stored, the data of any other organization should not be stored on it.

1-Single Tenant ID (Single Organization): HDFC

2-Reserved Hardware

3-Isolate (no one can access the data)

4-Costly

5-you can access within intranet.

Front End Application (Net banking).

Back-end application (in house application).

**Hybrid Cloud**: hybrid clouds combine public and private cloud, bound together by technology by that allows data and application to be shared between them. By allowing data and application to move between private and public cloud, hybrid cloud gives business greater flexibility and more deployment option.

For example, , a customer who wants such a cloud so that my users can access within the organization and over the internet. and the hardware on which the data is being stored, the data of any other organization should not be stored on it.

1-Single tenant ID: WB

2-Reserved Hardware

3-Isolate

4-Costly

5-Internet+Intranet=Hybrid cloud

Public cloud Private cloud=Hybrid cloud

**Difference between on premise and cloud computing**

Multi-tenant, shared,

Technical Model

Single tenant, selfish static

Interna network or internet corporate client

Internet, any device

Access Model

Pay as you go and for what you use

Buy assets and build technical architecture

Business Model

Buy Services

Acquisition Model

Buy assets and build technical architecture

Traditional Computing

On-premise

Cloud Computing

\*On-premise solutions has all the required physical devices installed in customer premises. Cloud solutions, on the other hand, are access via the internet, and typically hosted by a third-party vendor.

\*Second big difference is the ”pay as you go” or on demand usage service model(cloud) versus the traditional upfront capital expenditures(on-premises)

\*In cloud computing, low CAPEX cost, no hardware cost while in premise. The larger the enterprise, the grater the CAPAX costs.

Server Provisioning Cloud Provisioning

Time

Demand

Time

Demand

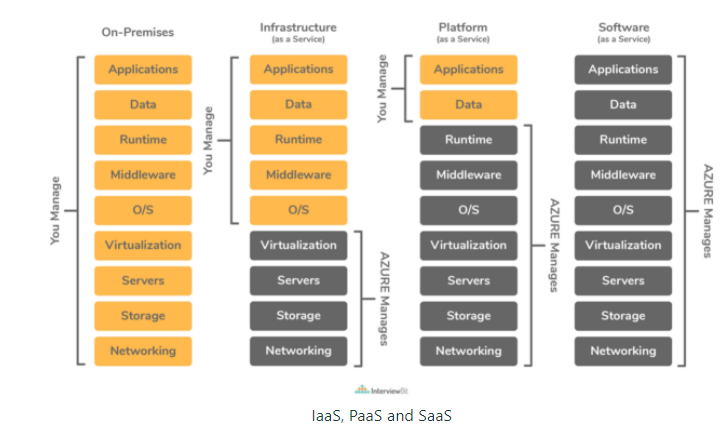
**What is a ”cloud”**

Cloud on demand, scalable, multitenant, self -service computer and storage resource.

“Cloud computing works by enabling client devices to access data and cloud applications over the internet from remote physical servers, databases and computers.”

Model types of cloud services

* Infrastructure-as-a service (IaaS)-the most important and widely used category of cloud computing services. With IaaS, you rent IT infrastructure-servers, virtual machine (VMs)storage, network, operating system-from a cloud provider on a pay-as-you go basis.
* Platform as a service (PaaS)-platform as a service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivery and managing mobile app, without worrying about setting up or managing the underlying infrastructure of servers, storage, network and database needed for development.
* Software as a service (SaaS)- Software as a service (SaaS) is method for delivering software application over the internet. On demand and typically on subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure and handle any maintenance, like software upgrades and security patching. Users connect to the application over the internet.

****

**Resource Group**

**Resource group is a container that holds all related resources for an Azure solution. The resource group includes those resources that you want to manage as a group.**

Resource Group

Storage Account

Virtual Machine

Virtual Network

Backup

Database

Automation

To hold all resources

**IP(Internet Protocol)**

**IP stand for internet protocol and its port no is 0. IP is a unique identification of host, for each host we assign a unique identification(IP).If we assign a same IP for multiple host, they are conflict and they are out of network.so for good practice we assign a unique identification for each host.**

**IPv4(Internet Protocol version 4)-IPv4 is a 32 Bit and its divide in 4 equal parts(Octat) and each parts(Octat) contains 8 bit. After 8 bit we represent of dot(.)**

**IPv4 Range(Value)-In IPv4 the min value is 0 and max value is 255.if we wright 256 the show error.**

**IPv4 Address-IP address means full range. if we divide a big network to a small network we called subnet.**

**Class of IPv4-**

**Class A (Default Range 0-127)**

**Class B (Default Range 128-191)**

**Class C (Default Range 192-223)**

**Class D**

**Class E**

**Class D and Class E are used for R&D and multicasting purpose.**

**we cannot judge a class by default range (Remember)**

**Class A is used for enterprise network (big network). This is used for Appx 1 crore host and this is addressing space of Class A.**

**In class A by default 8 bit is full.**

**11111111.00000000.00000000.00000000**

**255. 0 . 0 . 0**

**Class B is used for medium network, this is used for max 65535 host.65535 is a address space of class B.**

**In class B by default 16 bit is full.**

**11111111.11111111.00000000.00000000**

**255 . 255 . 0 . 0**

**Class C is used for small network. this is used for max 255 host and this is address space(Full range) of Class C.**

**In class C by default 24 bit is full.**

**11111111.11111111.11111111.00000000**

**255 . 255 . 255 . 0**

**in first Octate value is between 1 and 223 and rest three octate value is between 0 and 255.**

**Calculation of Subnet address**

**Sr No Host (32bit-Sr no.)**

**1 2**

**2 4**

**3 8**

**4 16**

**5 32**

**6 64**

**7 128**

**8 256**

**9 512**

**10 1024**

**11 2048**

**2n-2-----1**

**0---By default network address**

**1—Reserved for default gateway**

**2-Reserverd for DNS**

**3-- Reserved for DNS**

**255—Reserved for broadcast**

**classless interdomain routing-CIDR**

**Network security group (NSG)**

NSG basically a firewall. NSG contains rules to allow /block an inbound/outbound network traffic. NSG can be associated with subnet or individual virtual machine instance within that subnet.

there are two types of NSG rules

1-Inbound rule (By default Deny)

2-Outbound rule (By default Allow)

**How to create NSG-**

**1-Go to Network security group---Click on create**

* **Name-**
* **Subscription**
* **Resource group**
* **Region**
* **Create**

**Deploy NSG with particular subnet-**

**Go to Network security group—click on Subnet-click on associate-select virtual network-Select Subnet---OK**

**For Inbound Security rule-(Allow 3389)**

**Click on Inbound Security rule—**Click on add

**Source-**Any

**Source port range-\***

**Destination-**Any

**Service-**RDP

**Protocol-**TCP

**Port no-**3389

**Action-**Allow

**There are many rules in NSG.**

**Rule1- (Any person access to server from anywhere)**

**Source: Any**

**Destination: Any**

**Port:3389**

**Port Name:RDP (Remote Desktop Protocol)**

**Action: Allow**

**Rule2- (No one person access to server)**

**Source: Any**

**Destination: Any**

**Port:3389**

**Port Name:RDP (Remote Desktop Protocol)**

**Action: Deny**

**Rule3- (Only one person access to server)**

**Source: IP (Public IP)122.161.75.20**

**Destination: Any**

**Port:3389**

**Port Name:RDP (Remote Desktop Protocol)**

**Action: Allow**

**Rule4- (more than one to access the server)**

**Source: IP (Public IP)122.161.75.20,146.196.32.78**

**Destination: Any**

**Port:3389**

**Port Name:RDP (Remote Desktop Protocol)**

**Action: Allow**

**Rule5- (Block the internet)**

**Source: IP Any**

**Destination: Any**

**Port:80,443**

**Port Name: HTTP, HTTPS**

**Action: Deny**

**Rule6- (Allow to internet)**

**Source: IP Any**

**Destination: Any**

**Port:80,443**

**Port Name: HTTP, HTTPS**

**Action: Allow**

**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.**

**Virtual Network Lab**

Go to All Services----Virtual Network----Click on Add

* Name-
* Address space
* Subscription
* Resource group
* Location-
* Subnet Name-
* Subnet Address range-
* DDOS protection-Basic
* Service Endpoint-Disable
* Firewall-Disable

**Click on Create**

**Virtual Machine**-Azure Virtual machine will let us create and use virtual machines in the cloud as Infrastructure as a Service. Azure Virtual Machine**provides the flexibility of virtualization without the need to purchase and maintain the physical hardware to run it.**

**Following are the configuration choices that Azure offers while creating a Virtual Machine**.

* Operating system (Windows and Linux)
* VM size, which determines factors such as processing power, how many disks we attach etc.
* The region where VM will be hosted
* VM extension, which gives additional capabilities such as running anti-virus etc.
* Compute, Networking, and Storage elements will be created during the provisioning of the virtual machine.

**There are two types of Virtual machine**

**1-Window Virtual Machine**

**2-Linux Virtual Machine**

**In windows Virtual Machine network operating system is windows server 2012, windows server2016, windows server2019.Client operating system in windows virtual machine is windows7, windows10In windows virtual machine RDP protocol is used and RDP port no. is 3389.For access of windows virtual Machine, we use Win+R=run>mstsc=>public Ip**

**IP=>username and password=>ok**

**Administrator, admin and root these are reserved username in windows virtual machine.**

**Linux Virtual Machine**

In Linux Virtual machine network operating system is Red hat Linux and SUSE Linux.

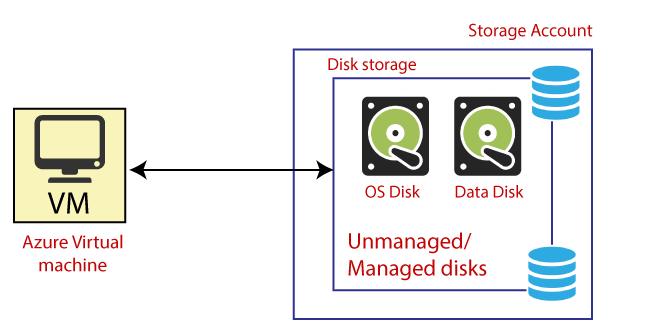
In Linux virtual machine client operating system is Ubuntu and centos.

In Linux virtual machine SSH secure shell protocol is used and port no is 22.

For access of Linux virtual Machine, we use Putty (App)=>IP and port no=>username and password.

Administrator, admin and root these are reserved username in Linux virtual machine.

**Disk-** Virtual machine uses disks as a place to store an operating system, applications, and data in Azure. All virtual machines have at least two disks- a Windows operating system disk and a temporary disk. Both the operating system disk and the Temporary disk are virtual hard disks (VHDs) stored in an Azure storage account. The VHDs used in Azure is .vhd files stored as page blobs in a standard or premium storage accountin Azure. Virtual machines can also have one or more data disks that are also stored as VHDs.



## **Types of Disk**

**Different kinds of disks that are offered by Azure:**

**Unmanaged disks:**It is a traditional type of disk that has been used by VMs. With these disks, we can create our storage account and specify that storage account when we create the disk. We must not put too many disks in the same storage account, resulting in the VMs being throttled.

**Managed disks:**It handles the storage account creation/management in the background for us and ensures that we do not have to worry about the scalability limits of the storage account. We specify the disk size and the performance tier (standard/premium), and Azure creates and manages the disk for us.

* **Standard HDD disks:** Best for backup, non-critical, infrequent access.
* **Standard SSD disks:**Best for web servers, lightly used enterprise application dev/test.
* **Premium SSD disks:**Best for production and performance sensitive workloads.

**In virtual Machine there are three types of Disks-**

**1-OS disk**-- Every virtual machine has one attached operating system disk. That OS disk has a pre-installed OS, which was selected when the VM was created. All files of Operating system is save on OS disk. Min size of OS disk is 127GB

**2-Temporary disk-** The temporary disk provides short-term storage for applications and processes, and is intended to only store data such as page or swap files. Data on the temporary disk may be lost during a [maintenance event](https://docs.microsoft.com/en-us/azure/virtual-machines/understand-vm-reboots) or when you [redeploy a VM](https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/redeploy-to-new-node-windows?toc=%2fazure%2fvirtual-machines%2fwindows%2ftoc.json).

**3-Data Disk-** A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. max size is 32 TB.

**Azure VM Family**

**A-**series (Entry Level economical VMs for development/testing)

Exp-Development and test server, Low traffic web server, small to medium server.

**B-series-** (Use for Testing purpose)

**D series-** (General purpose compute)-Use for database certified VM(SQL)

**E Series-** (Used for Application Server-Tally, SAP, ERP, Navision, Inhouse app)

**F series-** (Use for domain controller)

**N series-**Used for movies maker, Graphics designer)

**M series-**used for high compute power-Google, FB, You tube

**L-series-**used for big data, Hadoop

**Note----D2as\_v4(s is show, then premium disk is supported. If s is not show then premium disk is not supported)**

**For addition of new disk--**Go to Virtual Machine>go to disk>create and attached a new disk>save

use Command----diskmgmt.msc

go to disk 2. right click on disk2>initialize disk

**(Master boot record)-**At user end we use MBR. for example-Laptop, Computer. Maximum 4TB partition can be made in MBR.

**GPT (Guid partition table**)-where ever we deploy application by using network operating system we use GPT.

Maximum 32TB partition can be made in GPT.

for example, server (windows server 2012,2016,2019), database, Application**.**

**Availability set**- Availability set is a logical grouping of virtual machine which protect from hardware failure within a datacentre. Availability set is basically Hardware level Patch Management. During VM creation you will select an availability set, after VM creation you can't select an availability set. Availability set provide 99.95% SLA (service Level Agreement). And it is work on only single region.

An availability set does not protect your application from operating system or application specific failures.

There are two types of domains in availability set.

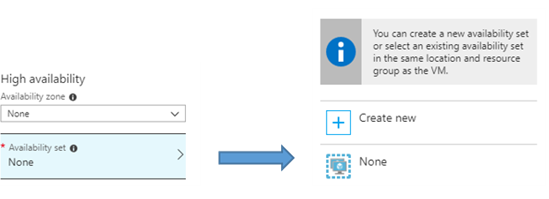
* **Fault Domain:** Fault domain define the group of virtual machinesthat share a common power source and network switch. Fault domain is max 3 and its count on 0,1, 2.its represent a rack

**Update Domain**-An Update domain is group of resources that can be updated and rebooted if required at the same time.

Virtual machines that share an update domain can undergo maintenance or be rebooted at the same time. Update domain is maximum 20.

**Configure an Availability Set**

We can configure an Availability Set ONLY when we deploy a New Virtual Machine, we can't add an existing Virtual Machine to an Availability Set.  
At the image below we can see the Availability Set Option on Azure Portal.

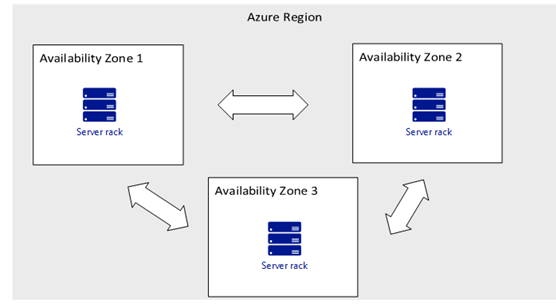
****

# **Availability Zones**

This is the next level of Azure Virtual Machines high-availability, because Virtual Machines are in different physical locations within an Azure Region. Minimum three availability zone available in an azure region and each zone has one or more data centre. Each zone has independent power, cooling and network infrastructure. Availability zones offer 99.99% SLA. **There are two categories of Availability Zones:**

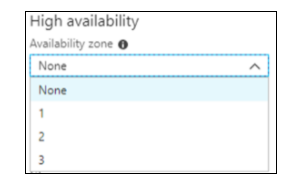
* **Zonal Services (Add the resource to a specific zone, for example VMs, Managed Disks, IP Addresses )**
* **Zone-redundant services (Automatic replication across zones is enabled for SQL Database, zone-redundant storage)**

**At the image below we can see a scenario with three Availability Zones on the same region.**

****

## **Configure an Availability Zone**

**Configuring an Availability Zone is very easy, especially from the Azure Portal. Select the Availability Zone for the Virtual Machines using the Availability Zone drop-down. Your managed disk and, if you have one, your public IP will be deployed into the same zone. Note that for 99.99% SLA, you must deploy at least two virtual machines into at least two different zones.  
The next image shows this option.**

****

# **Differences between Availability Set and Availability Zone**

**At the table below we can see the two main differences between Availability Set, Zone**

|  |  |
| --- | --- |
| **Availability Set** | **Availability Zone** |
| **Protect from Hardware failures within data centres.** | **Protect from entire data centre failure** |
| **SLA 99.95 %** | **SLA 99.99%** |

# **Azure VM SLA**

Below are the SLAs for the Azure Virtual Machines.

* 99.9%, Single VM
* 99.95%, 2 or more VMs in an Availability Set
* 99.99%, 2 or more VMs into Availability Zone

**Reginal Pair-**We ensure high availability of resources through regional pair.

A regional pair consists of two regions within the same geography. Azure serialize platform updates (Planned maintenance) across regional pairs, ensuring that only one region in each pair updates at a time. If an outage affects multiple regions, at least one region in each pair will be prioritised for recovery.

Azure provides several storage solutions that take advantage of paired regions to ensure data availability.

For example, azure Geo-redundant storage replicate data to secondary region automatically, ensuring that data is durable even in the event that the primary region isn’t recoverable.

Not all azure resources automatically replicate data, nor do all azure services automatically fallback from a failed region to its pair. In such cases, recovery and replication must be configured by the customer.

**Special Azure Region-**

1-US Gov Virginia and US Gov Lowa

2-China East and China North

3-Germany central and Germany northeast

**Virtual Machine Extension-**Virtual machine extension provide post deployment configuration and automation.

**Lab**

**Create Virtual Machine-**

**Basic—Disk—Networking—Management—Advance---**

**Extension—Select an extension to install----Custom script extension—Upload script file in azure storage or create a new storage**

**Review and create.**

**Virtual network Peering-** It is used to established private connection between two or more different virtual network of same region or also across the global Azure region through Microsoft backbone infrastructure, not through a gateway, or over the public internet.

* Vnet peering is two-way peering enabled from any one of the virtual networks.
* Its provide lower latency and higher bandwidth.

How to established connection b/w two Vms in a single network

-Create Virtual network

-Create two virtual machines in same virtual network

-RDP

-windows firewall-Off (Because Ping is work on ICMP protocol and window is by default block this protocol.)

-CMD-Ping private IP

* **VNet Peering Types**1. **Virtual Network Peering:** Connecting VNets within the same Azure region.  
  2. **Global VNet Peering (Vnet to Vnet VPN)**: Connecting VNets across Azure regions.

If we have a virtual network in azure that exists in different regions, then we can use Global peering. Gateway transit is supported for Global VNet Peering.

It works on geographic location. With the help of VNET to VNET VPN we communicate different network in geographic locations. Any data transfer through VPN gateway and data transfer through tunnel (this is a private path). It transfers Data with 256-bit encryption. And data transfer in encryption form gateway uses IKEV1 or V2 protocol

### IKEV1 or V2(Internet key enhance version 1 or version2 Currently version2 is used.

Benefits of peering-

1-Network traffic between peered virtual network is private.

2-Low latency and higher bandwidth

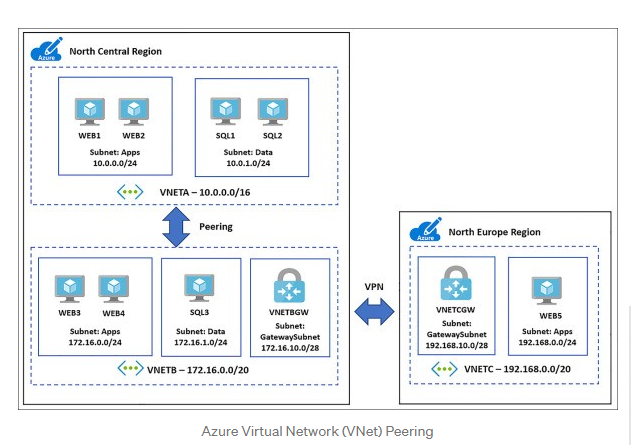
3-Ability to communicate transfer data across azure region, subscription

4-The traffic between virtual machine is peered virtual network is routed directly through the Microsoft backbone infrastructure, not through a gateway or over the public internet

5-Peering are not transitive.

For Example-Vnet1-Vnet2

Vnet2-Vnet3



## **Virtual Network peering in same region**

Lab

Create two Virtual networks

Create two virtual machines

Go to one of these virtual networks------select peering---Add peering

This virtual network

Peering link name

Traffic to remote virtual network

* Allow (default)
* Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

* Allow (default)
* Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server

* Use this virtual network's gateway or Route Server
* Use the remote virtual network's gateway or Route Server
* None (default)

Remote virtual network

Peering link name

Virtual network deployment model

* Resource manager
* Classic

I know my resource ID

Subscription

Azure subscription 1



Virtual network



Traffic to remote virtual network

* Allow (default)
* Block all traffic to the remote virtual network

Traffic forwarded from remote virtual network

* Allow (default)
* Block traffic that originates from outside this virtual network

Virtual network gateway or Route Server

* Use this virtual network's gateway or Route Server
* Use the remote virtual network's gateway or Route Server
* None (default)

Add

**Vnet to Vnet connection in different region Lab**

1-Create two vnet in two different regions

2-Create subnet gateway

3-Create two virtual network gateways in two vnet

## Create virtual network gateway

**Basics**

**Project details**

Subscription

Azure subscription 1

**Instance details**

Name

Region

Gateway type

* VPN
* ExpressRoute

VPN type

* Route-based
* Policy-based

VPN type

* Route-based
* Policy-based

SKU-VpnGw2AZ

Generation-Generation2

Virtual network

[Create virtual network](https://portal.azure.com/)

Only virtual networks in the currently selected subscription and region are listed.

**Public IP address**

Public IP address

* Create new
* Use existing

Public IP address name



Public IP address SKU-Standard

Assignment

* Dynamic
* Static

Availability zone-The value must not be empty.

Enable active-active mode

* Enabled
* Disabled

Configure BGP

* Enabled
* Disabled

**Create**

Same step follows on 2nd virtual network gateway

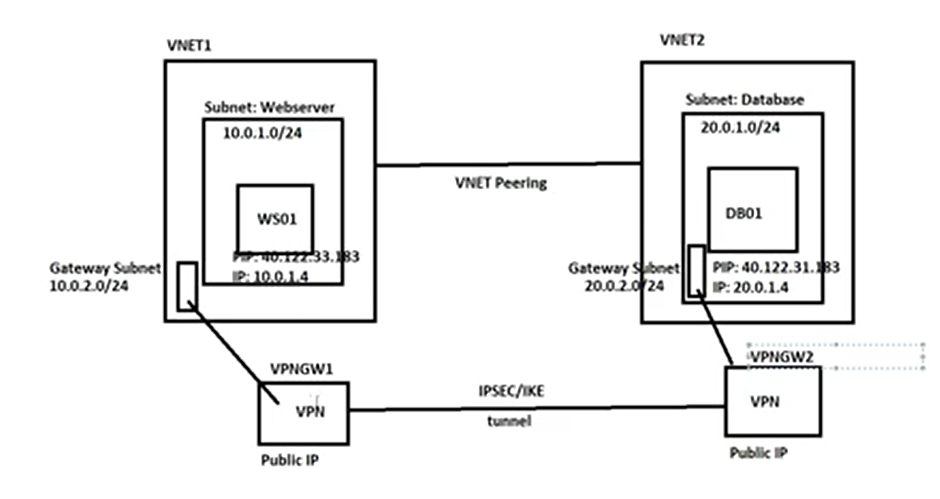
3-Go to virtual network gateway-click on connection—Add

Connection type-Vnet to vnet

First vnet gateway

Second vnet gateway

Shared key



**Gateway Type-The two gateway types are:**

**1-VPN Gateway**

**2-Express route Gateway**

## **VPN Gateway:** A VPN gateway is a specific type of virtual network gateway, which is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet. Site to Site, point to site and Vnet to Vnet connection all use a VPN gateway.

When we are planning to deploy a VPN gateway into Azure, we can configure the number of settings related to it:

* **Gateway SKUs:** We need to select the SKU that satisfies our requirements based on the types of workloads, throughputs, features, and SLAs.
* **Zone-redundant gateways:** We can get benefits from zone-resiliency to access your mission-critical, scalable service on Azure when we use zone-redundant gateways.
* **Connection types:** Connection type can be IPsec, Vnet2Vnet, ExpressRoute, VPNClient.
* **VPN types:** The VPN type that we choose depends on the connection topology that we want to create and the VPN device. It can be a policy-based VPN or Route-based VPN.
* **Gateway subnet:** Before you create a VPN gateway, you must create a gateway subnet with the name 'GatewaySubnet' and do not deploy anything else into that subnet.
* **Local network gateway:** Local network gateway usually represents your on-premises location, i.e., VPN devices, and address prefixes.
* **Connection topologies:** Site to site, multi-site, point-to-site, Vnet-to-Vnet, and express route.
* **Monitoring and Alerts:** Monitors the key metrics and configure alerts.

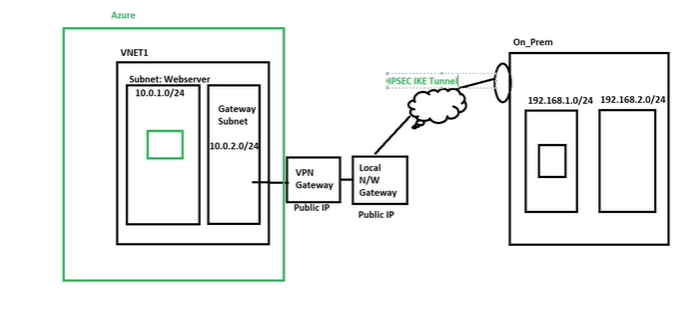
**Site to Site VPN:** With the help of Site-to-Site VPN you established the connection between On-premise VPN device and azure VPN gateway that is deployed in azure network.

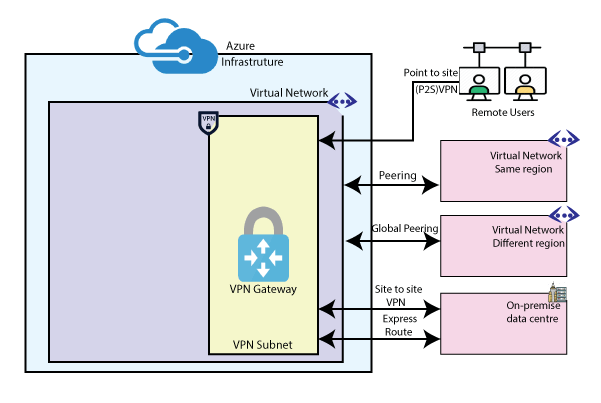
* **The communication between On-**premise VPN device and azure VPN gateway is sent through an encrypted tunnel over the internet.
* **VPN type**

**1--**Policy based – (One to one) Static

**2-**Route based- (one to many) Dynamic

* **Add gateway subnet to virtual network**
* **Deploy virtual network gateway with VPN as gateway type route based as VPN type and add new public IP address name.**
* **Now check configuration of on-premise VPN device with new public IP assignment, enter shared key, use of IKEv2 protocol and associate public IP of azure virtual network gateway.**





**Site to Site VPN Lab**

### 1-Create Virtual Network

### 2-Create Virtual Machine

### 3-Create Gateway subnet---

### Go to virtual network---click on subnet---click on subnet gateways---

### mention address range---click ok

### 4-Virtual network gateways----

### Go to virtual network Gateways---Click on add

### Name-

### Region-

### Gateway Type-1-VPN 2- Express route

### VPN Type---1-Route based 2-Policy based

### SKU

### Generation

### Public IP address—-1-Create New 2-Uses existing

### Public IP address Name

### 5-Local network Gateway-Click on Add

### Name-

### IP address- (Specify public IP address)

### Address space

### Subscription-

### Resource group

### Location-

### Create

### For established connection between Virtual Network Gateways and Local Network Gateways-

### Go to Virtual Network gateways-

### Click on created Virtual Network gateway-Go to connection-Click on Add

### Name-

### Connection Type- 1- Vnet to Vnet 2- Site to Site 3- Express route

### Virtual network gateways

### Local network Gateways-Add local network gateways

### Shared Key

### IKE Protocol—1- IKEv1 2-IKEv2

### Subscription

### Resource Group

### Location

### OK

### For connection established between VPN gateway and Onprem-

### Click on Connection-(click on Created site to site)- Click on Download Configuration—Select Device Vendor—Select Device Family—Select Firmware Version—And download configuration

### Review and Create

**Point to Site VPN-** With the help of Point to site VPN gateway you create a secure connection between virtual (Azure)network and individual remote users.

* The communication between a virtual network and user computer is sent through an encrypted tunnel over the internet.
* Gateway subnet-The gateway subnet is part of virtual network IP address range. It contains the IP address that the virtual network gateway resources and services use.
* VPN gateway is specific type of virtual network gateway that is used to send and receive encrypted traffic between an azure vnet and on-premise location over the public internet.
* Add gateway subnet to virtual network.
* **Deploy virtual network gateway with VPN as gateway type route based as VPN type and add new public IP address name.**
* Configure P2S VPN with address pool and past route certificate data then download VPN client certificate and install this on remote user computer.
* Now remote user access azure service using private IP address of Vnet.

Point-to-site VPN can use one of the following protocols:

* **OpenVPN Protocol**,
* **Secure Socket Tunnelling Protocol (SSTP)**
* **IKEv2 VPN**

## How are P2S VPN clients authenticated?

Before Azure accepts a P2S VPN connection, the user has to be authenticated first. There are different mechanisms that Azure offers to authenticate a connecting user.

### 1-Authenticate using Azure certificate authentication

### 2-Authenticate using Azure Active Directory authentication

### 3-Radius authentication

### 

### Lab

### 1-Create Virtual Network

### 2-Create Virtual Machine

### 3-Create Gateway subnet---

### Go to virtual network---click on subnet---click on subnet gateways---

### mention address range---click ok

### 4-Virtual network gateways----

### Go to virtual network Gateways---Click on add

### Name-

### Region-

### Gateway Type-1-VPN 2- Express route

### VPN Type---1-Route based 2-Policy based

### SKU

### Generation

### Public IP address—-1-Create New 2-Uses existing

### Public IP address Name

### Review and Create

### 5-Go to Created Virtual network gateways—

### User VPN configuration-Point to site not configured—for configuration of VPN—Click on configuration---Address pool—Give the address range

### Tunnel Type-1-Open to VPN 2- SSTP 3- IKEv2

### Authentication Type—1-Azure certificate 2-Radius authentication 3-Azure active directory

### Root certificate—Paste root certificate

### Download VPN client- for this software user connect to azure virtual network.

### Save

### For user connection—Open network connection(ncpa.cpl)

### Icon show (Vnet-1)—click on vnet1—connect

### Download Self signed root certificate & Client certificate-

### Generate and export certificate for P2S—Copy of power shell command and open power shell and paste and enter.

### For check of where certificate is create-certmgr.msc—Go to personal—Click on certificate—Export P2S certificate-save (in the form of cer)

### For Client certificate-

### Copy of power shell command and open power shell and paste and enter. Export client certificate-save (in the form of cer)

**Express Route**: To send network traffic on private connection, you use the gateway type ‘Express route’**. Express route is providing the Private connectivity from On-**premise data centre to azure virtual network. Express route connection do not go over the public internet and the data transfer in express route through a private path and data is not encrypted form but it is secure.

**Each virtual network can have only one virtual network gateway per gateway type.** For example, you can have one virtual network gateway that uses -Gateway type VPN, and one that uses-Gateway type Express route.

**All azure region is connected to Microsoft backbone private network.** And Microsoft backbone network are connected to Meet me/peering location/Microsoft edge. When we configure the express route, two types of edge are created.

**1-**Partner edge

**2-**Microsoft edge

**Express route Lab**

### 1-Create Virtual Network

### 2-Create Virtual Machine

### 3-Create Gateway subnet---

### Go to virtual network---click on subnet---click on subnet gateways---

### mention address range---click ok

### 4-Virtual network gateways----

### Go to virtual network Gateways---Click on add

### Name-

### Region-

### Gateway Type-1-VPN 2- Express route

### Select Express route

### VPN Type---1-Route based 2-Policy based

### SKU—1-Standard 2-High Performance 3-Ultra performance

### When you select a higher gateway SKU more CPU and bandwidth are allocated to the gateway

### Virtual network-Select Virtual network (When we Deploy a virtual network gateway in gateway subnet, two or more VMs are created in backend.)

### Public IP address—-1-Create New 2-Uses existing

### Public IP address Name

**Review and Create**

**5-Express route circuit-**

**Go to express route circuit-click on create**

* Resource group-
* Region-
* Name-

**Click on configuration-**

* **Port Type- 1-**Provider  **2-** Direct
* **Create new or import from Classic- 1-**Create new **2-** Import
* **Provider-**
* **Peering location-**
* **SKU—1-Local** (Local SKU gives access to only 1-2 azure region in the same geo region)

**2-Standard** (Standard SKU gives access all region in same geo location)

**3- Premium** (Premium SKU gives access all region in all geo location.)

* **Billing Model-**

**1-Meterd-**Inbound data transfer is free but we pay for outbound data transfer.

We pay as predefined rate for outbound data transfer

**2-Unlimited-**On monthly basis we pay for outbound data transfer.

* **Allow Classic operation-1-**Yes  **2-**No

**Review and create**

**6-Integrate (Connection) to express route circuit to express route Gateway-**

Before integration, express route circuit should be provisioned by service provider. After that express route integrate with express route gateway.

**For Integration—**

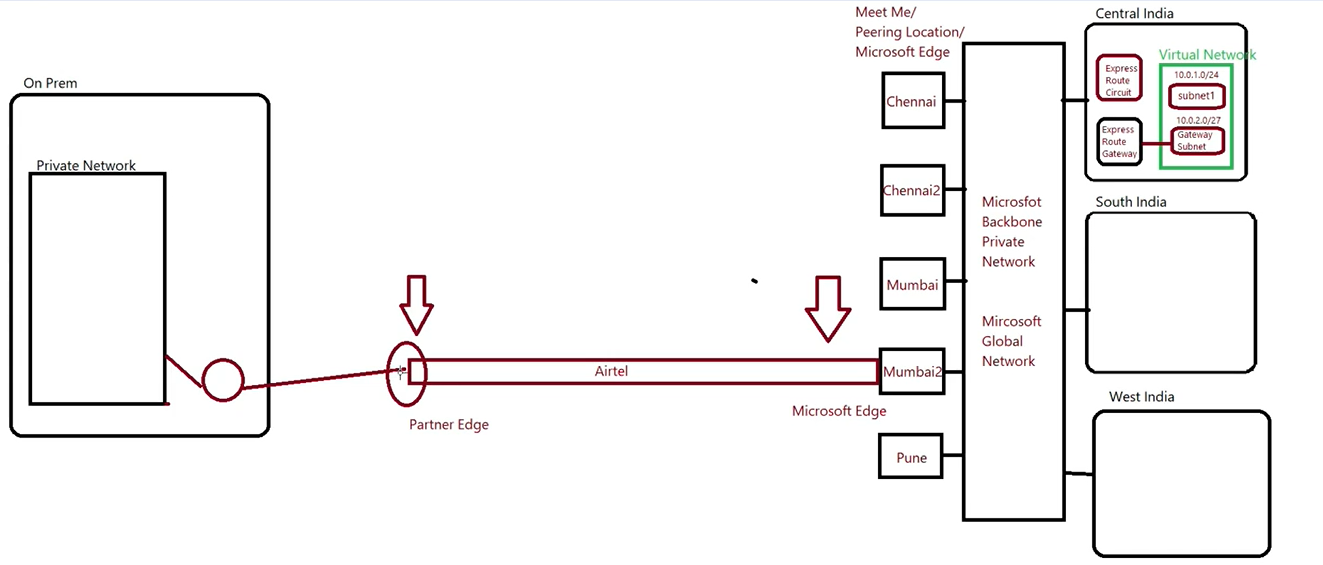
Go to virtual network gateway

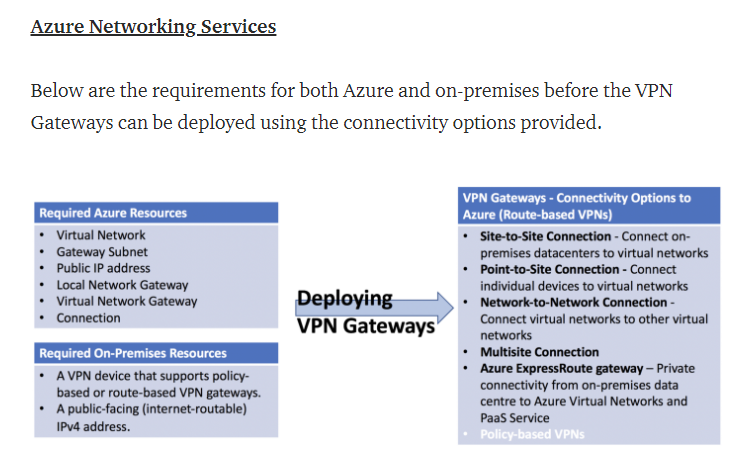
Click on created virtual network gateway (Express route gateway)

**Connection-**Click on add

* **Name-**
* **Connection type-**Express route
* **Select virtual network gateway (Express route gateway)**
* **Select express route circuit**
* **Subscription**
* **Resource Group**
* **Location**

**OK**





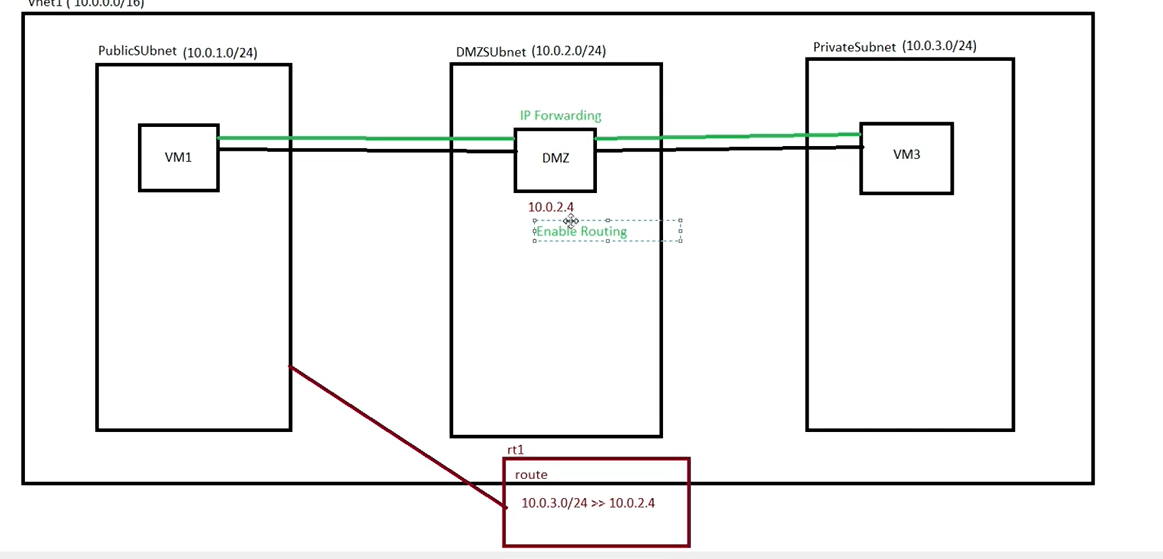
**Route Table-Azure automatically creates a route table for each subnet within an azure virtual network and adds system default route to the table.**

**There are two types of routes on azure-**

**1-System route-**Azure automatically creates system routes and assigns the routes to each subnet in a virtual network. You can't create system routes, nor can you remove system routes, but you can override some system routes with custom routes. Azure creates default system routes for each subnet, and adds additional optional default routes to specific subnets.

**2-User defined route** **(UDR):** You can create custom, or user-defined(static), routes in Azure to override Azure's default system routes, or to add additional routes to a subnet's route table. In Azure, you create a route table, then associate the route table to zero or more virtual network subnets. Each subnet can have zero or one route table associated to it.

User defined routes are custom routes that controls network traffic by defining routes that specify the next Hop of the traffic flow. The next Hop can be a virtual a virtual network gateway, virtual network, intenet,or virtual appliance.



**Route Table lab**

**1-Search for route table-Select it then creates and configure the following settings:**

* Name-
* Subscription-
* Resource group-
* Location-

**Review and create**

**2-Go to created route table-Click on Route-**

* Name-
* Address prefix (10.0.3.4-This is 2nd VM IP)
* Next Hop Type-Select virtual machine alliance
* Next Hop Address-Enter Virtual machine appliance IP address

**Click OK**

**3-Go to Created Route table-click on subnet**

* Click on associate
* Select virtual Network
* Subnet(Source subnet)

**Click OK**

**4-For enable of IP forwarding (For forward the traffic to next VM)**

* Go to Virtual Machine appliance
* Networking-
* Network Interface
* IP configuration
* Enable IP forwarding

**Save**

**5-Enable Routing-Using PowerShell command**

****

**6-Reboot the VM**

**Note- For checking of data transfer use this command-tracert IP**

**Load Balancer-** An Azure Load balancer is layer 4(TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs.It works in single region.

By default, load balancer uses a 5-tuple hash-

1-Source IP

2-Source port

3-Destination IP

4-Destination port

5-IP protocol

Azure Load Balancer distribute traffic flow arrives at the LB frontend IP to Backend pool VMs based on configured load balancing rule. And health probe rules.

* **Azure Load balancer components-**
* **Frontend IP**: Frontend IP is must to configure to access the application as the application request will directly come tin to the Frontend IP rather than VMs.This can be public IP or private IP.
* **Backend Pool-** Associate all VMs to backend pool that is the part of availability set, then only Vms added to backend pool.
* **Health Probe-**To check the health of Vms associated in the backend pool.
* **Load Balancing rule:** It is define used to define how incoming traffic distribute to all healthy Vms with in the backend pool and associate frontend IP to load balancing rule.
* **Inbound NAT Rule:**

## **Azure Load Balancer Types-**

In Azure, you can create two types of the **load balancer**

* Public load balancer
* Internal/ private load balancer

**Public Load Balancer:** A **public load balancer** can be used to load balance **internet traffic** to virtual machines. It can provide**outbound connections** for virtual machines (VMs) inside your virtual network. This connection is accomplished by translating this private IP address to public IP address. It is used to load balance internet traffic to Healthy Vms. Public load balancer is commonly used for web server.

**Lab**

1-Create Resource group

2-Create Virtual Network

3-Create Availability set

4-Cerate two virtual Machine-----Create-New---Public inbound port-HTTP, RDP

5-Create Load balancer ---All services—networking---load balancer-

Name-

Type-Public

SKU-Basic

Public IP

Create

Open load balancer—Frontend IP co configuration, Backend Pool-Add

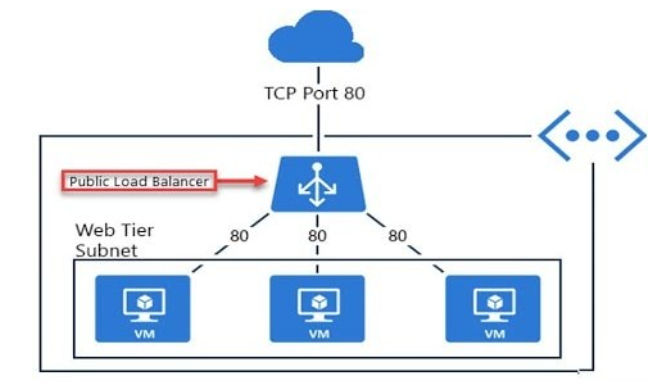
Name, Associated to availability set

Add target-Target---Target VM. Network IP configuration

6-Health Probe-+Add, protocol—HTTP---OK

7-Add balancing rule

7-Install IIS server



**Internal/ Private Load Balancer:** It is used where private IP are needed at the frontend only. It is used to load balance traffic inside a Vnet. It is commonly used for database server as it is directly not exposed to internet.

Load Balancer SKU-

|  |  |  |
| --- | --- | --- |
| **Load Balancer SKU-** | **Standard Load Balancer** | **Basic Load Balancer** |
|  | This is chargeable | This is free |
| Backend pool size | Up to 1000 instances | Up to 300 Instances |
| Health probes | TCP, HTTP, HTTPs  TCP connections stay alive in all situation even all probes down | TCP, HTTP  TCP connections terminate when all probes down |
| Availability Zone | Available | Not available |

While using standard Load balancer we must use standard public IP in load balancer and in all VMs.

**Lab**

1-Create Resource group

2-Create Virtual Network

3-Create Availability set

4-Cerate two virtual Machine-----Create-New---Public inbound port-HTTP, RDP

Create another Vm for testing

5-Create Load balancer ---All services—networking---load balancer-

Name-

Type-Interna

SKU-Basic

Select Virtual network

Select Subnet

Create

Open load balancer—Frontend IP co configuration, Backend Pool-Add

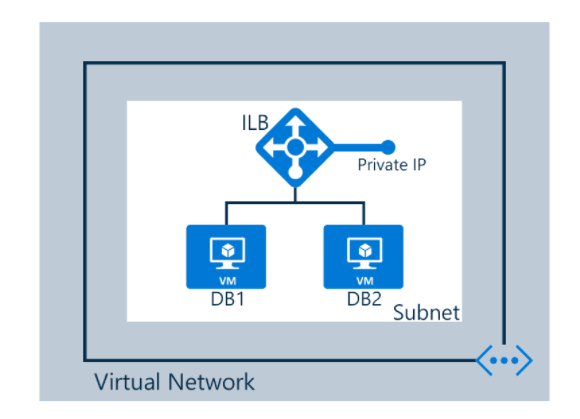
Name, Associated to availability set

Add target-Target---Target VM. Network IP configuration

6-Health Probe-+Add, protocol—HTTP---OK

7-Add balancing rule

7-Install IIS server



**Traffic Manager-**Azure Traffic Manager is a DNS-based traffic load balancer that enabled to distribute traffic across global azure region. Traffic Manager uses DNS to direct the client requests to the appropriate service endpoint based on a traffic-routing method and health of the Azure endpoint.

Traffic Manager also provides your public endpoints with high availability and quick responsiveness.

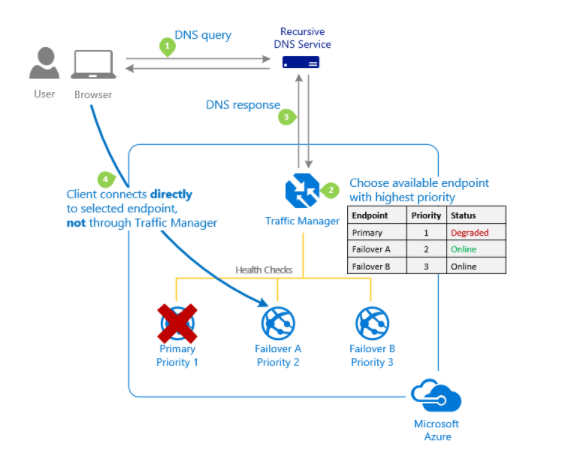
Traffic manager also provides health monitoring for every endpoint. The endpoint can be any Internet-facing service hosted inside or outside of Azure.

## **Azure Traffic Manager Routing Methods-**

These following **traffic routing methods** which are available

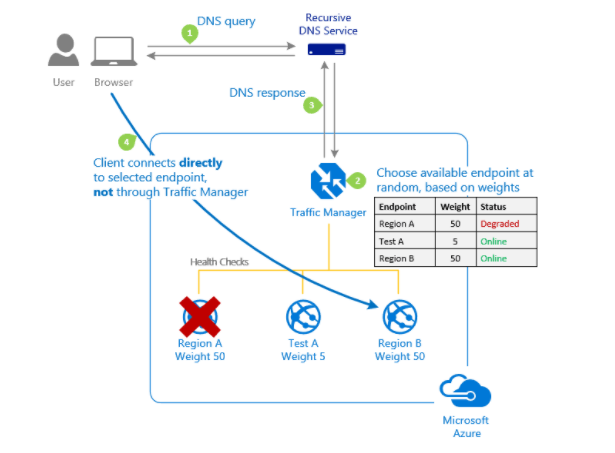
### ****1.) Priority****

When you select the **priority routing method**, it contains a prioritized list of service endpoints where the primary service endpoint has the highest priority for all traffic. If the primary service endpoint is unavailable, it redirects the traffic to the second priority endpoint and so on.

****

### ****2.) Weighted-****

The weighted routing method is used when you want to **distribute traffic**evenly or to use **pre-defined** weightsacross a set of endpoints. In this traffic-routing method, you allocate a weight which is an integer from 1 to 1000, to each endpoint in the Microsoft Azure Traffic Manager profile configuration.

****

### ****3.) Performance:** Route the traffic to closest endpoint in terms of the lowest latency.**

### **4—**Geography**-Route the traffic to specific node based on the source location.**

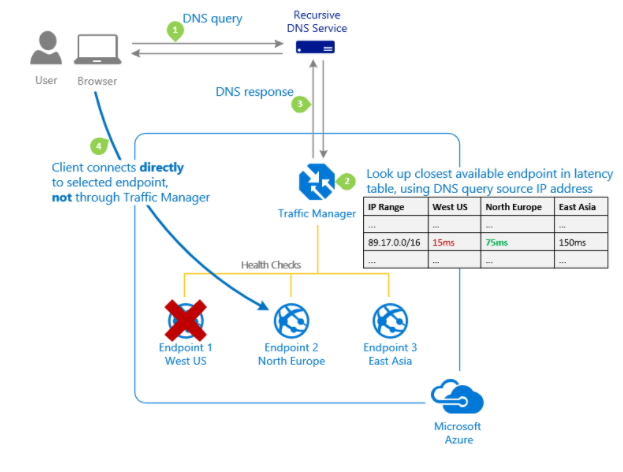
### **5-**Subnet-**Route the traffic nodes based on the source IP address range.**

### **6-Multivaluve-Route the traffic to multiple healthy endpoints but response comes from nearest location.**

### **Add endpoints-**

### **Azure endpoint-endpoint host in azure cloud.**

### **External endpoint-Endpoint host outside the azure i.e., in on-premise.**



## **Features Of Azure Traffic Manager-**

### 1-**Improve application performance**

### **2-Perform service maintenance without downtime**

### ****Application Gateway-**** Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Application Gateway can make routing decisions based on additional attributes of an HTTP request.

This type of routing is known as application layer (OSI layer 7) load balancing and can-do URL-based routing and more.

Components:

**Frontend IP Address-**Configure frontend IP (Public or private IP) andUser will connect the application gateway via frontend IP address.

**Backend pool**-Associate all instances to backend pool.it can be VM (NIC card), VMss, VM Public IP or private IP and on-prem web apps.

**Listener-**It check for the incoming connection request, you can configure a multiple listener.

**There are two types of listeners-**

**1-Basic-**If you want all of your request (for any domain) to be accepted and forwarded to backend pools, choose basic.

**2- Multisite-**If you want to forward request to different backend pool based on the host header or host name, choose multisite listener, where you must also specify a host name that match with the incoming request.

**Routing rules-**It is used to route the traffic from listener to backend pool.

**There are two types of rules-**

**1-Basic-**All request are routed to backend pool directly.

**2-Path Based--**All request are routed to backend pool based on the URL.

**Health probes**-It will monitor the health of resources of backend pool configured in application gateway.

Configure routing rule for listener and associate frontend IP and also configure routing rule for backend target and create new HTTP setting rule.

**Azure Storage-**Azure Storage is a Microsoft-managed cloud service that provides storage that is highly available, secure, durable, scalable and redundant. It is a service to store files, messages, tables, and other type of information.

Azure storage also used for virtual machines which include disks and files.

Azure storage is generally used in 3 categories

Storage for Virtual Machine-Disk and file share

Unstructured Data-Blobs and data lake storage

Structured Data-Tables, cosmos DB, Azure SQL DB

Note-NAS (Network attached storage) --In NAS multiple hard disks are attached. This type of hard disk is used in organization.

**Standard and Premium storage account-**

**Standard-:**

**-) Backed by Magnetic drives (HDD)**

**-) Lowest Cost per GB**

**Premium:**

**-) -) Backed by Solid state drives (SSD)**

**Can only be used with Azure VM disk**

**Azure Storage account types- Azure provides the storage services with the help of storage account. There are 4 types of storage uses.**

**1-Azure Blobs-**

Azure blob storage is service of storing large amount of unstructured object data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world, or to store application data privately.

Blobs stand for binary large object. In Azure blobs we access the data through HTTP or HTTPS protocol.

Maximum size of Blob storage is 500TB.

**Blob storage is used for:**

1-Server images are documents directly to a browser.

2-Storing files for distributed access.

3-Streaming video and Audio

4-Storing data for backup and restore, disaster recovery and archiving.

5-Storing data for analysis by an on-premises or azure -hosted services.

**Blob Containers and categories-**

**Containers-**A container organized a set of blobs, similar to a directory in a file system**.** You can create multiple blobs under container and multiple containers in one storage account.

**Blob storage are categories in 3 types:**

**Block blob:** Any files, videos, images etc. saved in blob storage are default saved with the type as “Block Blob”.

It stores text or binary data up to about 4.7TB. Block blobs are made up of block of data that can be managed individually.

**Page Blob: It** stores random access files up to 8TB in size. Page blobs store virtual hard drive (VHD) files and serve as disks for azure virtual Machine.

Eg-Azure SQL DB uses Page Blob.

**Append blob:** Append blob are made up of blocks like block blobs, but are optimizes for append operation. Append blobs are ideal for scenarios such as logging data for virtual machine.

**Azure files-(Max size-5TB)**

Azure files enables you to set up highly available network file share that can be accessed by using the standard server message block (SMB- Also known as common internet file system or CIFS) protocol from anywhere in the world.

That means that multiple VMs can share the same files with both read and write accesses cases for this if you want to migrate the application or the data in to azure.

It uses server message block (SMB) Protocol and SMB port no is 445.

File share can be used in may scenarios-

1-Replace or supplement On-premise file shares.

2-Lift and shift operation.

**Benefits**

1-Shared accessed

2-Fully Managed-Update, replacing faulty disk is managed by azure.

**Maximum size of Azure file is 5TB**

**Azure Tables-**

It stored structured NO SQL in the cloud. Which accept authenticateed calls from inside and outside the cloud.

You can use table storage to store flexible datasets like user data for web application address books or other metadata.

Azure table storage is now part of Azure Cosmos DB.

Common use of Table storage are-

1-Storing TBs of structure data capable of serving web scale application.

2-Quickly quering data using a cluster index.

The main Difference between SQL DB and NO SQL DB is NO SQL DB is Scalable while SQL DB is not scalable. Other difference is NO SQL is fast responsive comparison to SQL.

**Azure queues-**

The Azure queue services is used to store and retrieve messages. Queue messages can be up to 64KB in size, and a queue can contain millions of messages. Queue are generally used to store lists of messages to be processed asynchronously.

Message can be remained in queue for 7 days. (Maximum)

**Common uses-**

1-Creating a backlog of work to process asynchronously.

2-Passing message from an azure web role to azure worker role.

**Storage account performance-**

**1-Standard Account-**

**Are backed by HDD (magnetic drives)**

**Lowest cost per GB**

**Best for application that require bulk storage**

**Data is accessed infrequently**

**1-Premium Account-**

**Are backed by SSD (Solid state drive)**

**Offer consistent low -latency performance**

**Use with azure virtual Machine disk**

**Best for I/O intensive application like database**

**Storage Kinds**

**General purpose v1-**

Legacy account type for Blobs, files, queue and tables. Use general purpose v2accounts instead when possible and it may not have all the latest features.

It supports services only like Blob, File, Queue, Table and disk.

It does not support any access tier like Hot, Cool.

It supports only replication like LRS, GRS, RA-GRS.

It supports both standard and premium performance tiers.

**General purpose v2-**

Basic and latest storage account type for Blob, file, Queue, and table. Recommended for most scenarios using Azure storage and Microsoft recommend to using this type of account.

It supports services only like Blob, File, Queue, Table, disk and Data Lake Gen2.

It supports access tier like Hot, Cool and archive.

It supports replication like LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS

It supports both standard and premium performance tiers**.**

**Blob Storage-**

The Blob storage is used f or storing unstructured data

It supports only services of Blob (block blob, append blob)

It supports only standard performance tier.

It supports access tiers like Hot, Cool, Archive.

It supports only replication like LRS, GRS, RA-GRS.

**Access Tiers-**

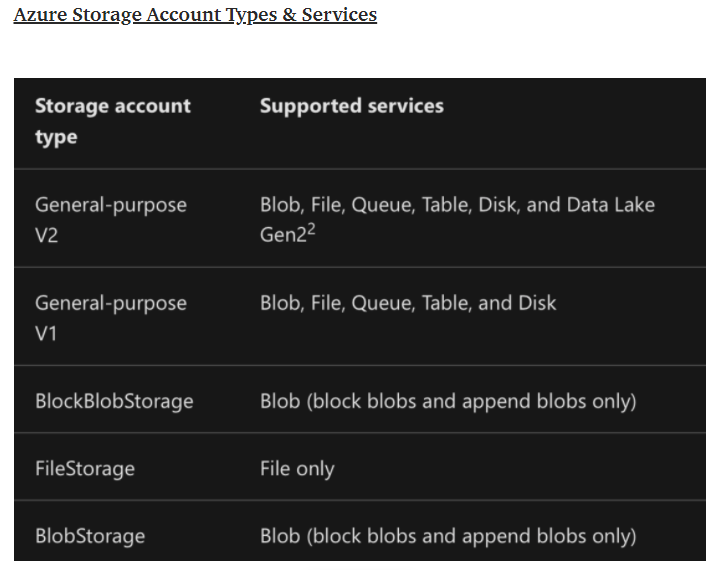
**Hot-**Optimized for storing data that is accessed frequently like virtual machine, files, images, videos that are in regular use.

Hot tier has higher storage cost and lower read cost.

**Cool-**Optimized for storing data that is infrequently accessed and stored for at least 30 days like backup data that will be stored in storage and are not use frequently.

In this storage cost is lower however read cost is higher than Hot tier.

**Archive-**Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours) like you have yearly report or data which is not in use but you keeping it for long term like 15 or 99 years.

In this storage cost is lower than Cool tier however access cost is higher than cool storage.

**Storage replication:**

Mostly big companies used to keep more than 1 storage devices for redundancy purpose or high availability or for mirroring if incase one storage device goes to down then data can be accessible from other storage device. IN same way azure also has same kind of concept with advance version which will replication the storage in to multiple regions for mirroring purpose and this replication is managed by Microsoft itself.

**There are 6 types of replications in storage:**

**Locally redundant storage (LRS):**

If we select LRS, the 3 copies of data will be stored in 3 storage boxes within the same data center.

**Zone redundant storage (ZRS):**

If we select ZRS, the 3 copies of data will be created in multiple datacenters in same region.

**Geo-redundant storage:**

If we select GRS, the 3 copies of data will be created in primary region and 3 copies of data created in other secondary geo location. It means it creates 6 copies of your data.

**Read Access Geo-redundant storage (RA-GRS):**

This option is same like GRS but here we have read only access to the secondary datacenter. We can access the data with the secondary URL any time.

**Geo-Zone redundant storage (GZRS):**

It copies your data synchronously across three azure availability zone in the primary region using ZRS.It then copies your data asynchronously to a single physical location in the secondary location.

**Read Access Geo-Zone redundant storage (RA-GZRS):**

This option is same like GZRS but here we have read only access to the secondary datacenter. We can access the data with the secondary URL any time.

**Lab**

**Step**1---Create Resource group

**Step2**--Storage account>Create a storage account

**Account kind**-General purpose v1

General purpose v2

Blob Storage

**Replication**-LRS

GRS

RA-GRS

ZRS

GZRS

RA-GZRS

**Access tier**-Cool

Hot

**Review and create**

**Step3**---File share

Create file share--shalesfileshare

Click on create

**Step4**----Containers

**Azure storage explorer**

**Azure SQL database**

**What is SQL**

SQL stands for structured query language. It is used for accessing an manipulating database such as insert,update,delete,retrive.

**What is Database**

Database is collection of data that is organized so that it is can be easily accessed and managed.

Database management system (DBMS)-Database management system is software which is used for creating and managing different databases.

**With the help of DBMS, we take care of following task-**

1-Data security

2-Data backup

3-managed huge amount of data

4-Data import and export

**Types of DBMS-**

There are various types of DBMS but here we categorized only two important DBMS which is mostly used:

1-Relational database

2-non-relational database

**Relational Database-**Relational database is known as RDMBS and stand s for relational database management system.RDBMS is database management system that data is stored in form of tables and each table contains row and columns.

Example of non-relational database is MY SQL server, Microsoft access.

**Non-relational database-** Data is not organized in the form of tables. Data is stored in form of key and value paires.the example of non-relational database are JSON and XML.

SQL database is a general purpose relational database managed services in Microsoft azure that support structures such as relational data,JSON,XML etc.

In Azure SQL DB we managed only application and OS managed by Microsoft. This is only PASS service. (while in on-premise we manage APPLICATION as well as OS).

**Azur SQL Database DTU(Database throughput unit)calculator-** This calculator will help you determine the number of DTUs for your existing SQL Server database(s) as well as a recommendation of the minimum performance level and service tier that you need before you migrate to Azure SQL Database. Knowing the minimum service tier will allow you to get the performance you need while minimizing your costs.

**Measure resource utilization**

Measure the following utilization metrics for at least an hour so the calculator can analyze utilization over time to provide you the best recommendation:

* Processor - % Processor Time
* Logical Disk - Disk Reads/sec
* Logical Disk - Disk Writes/sec
* Database - Log Bytes Flushed/sec

To assist in capturing the correct performance metrics, use one of the following utilities (Command Line EXE or PowerShell Script) to capture your database utilization. The utility and script are configured to capture the above performance counters for a one hour period.

* Before running the utility/script, ensure that no processes other than SQL are utilizing CPU, memory, and disk.
* Click the link and download the zip file on to your SQL server and extract the contents.
* If you are using the command line utility, right-click the .exe file and select "Run as administrator."
* If you are using the PowerShell script, navigate to the Windows PowerShell ISE and right-click to "Run as administrator." Within Windows PowerShell ISE, browse to the sql-perfmon.ps1 script file and click 'F5' to run the script.

### Upload the CSV file and Calculate

Once the script completes, enter the number of cores for your server and upload the CSV file generated by the script. Click the **Calculate** button to view your recommended Service Tier/Performance Level and DTUs.

**Lab**

Resource group----TCS-RG

SQL Database

databasename-tcsdb01

create server-tcsserverdb01

authentication method-use SQL authentication

server admin login-dbadmin01

password-admin@123456

go to microsoft SQL server managment studio

Before login, go to set server firewall after that add client IP and save.

Backup>retention policies>configure policies

point-in-point restore (Minimum 1 day and maximum 7 days backup)

Long term retention---

1-weekly long-term retention(if we want weekly backup)

2-Monthly Long term retention(If we want monthly backup)

3-Yearly long term retention(If we want yearly backup)

Go to restore database

Database name-dbrestoredrill

**Azure Backup and Site recover**

The Azure Backup service provides simple, secure, and cost-effective solutions to back up your data and recover it from the Microsoft Azure cloud.

* Backup of Azure Vms, SQL server, on-premise server. Azure backup service can take the back of VM level, file level, and disk level. In azure backup taken through recovery service vault.
* By default, the backup policy is retention period is set to 30 days but can change as per requirement.
* Configure the backup policy like schedule time and date, retention period, backup frequency.
* Configure the alert for backup.
* Restore the file, complete VM or disk only.
* If backup deleted accidently, the backup will retain for the period of 14days and still chance the restore the data.
* Once 14 days will be over, the deleted file will be deleted permanently.
* **Azure VM backup-**Backup of azure Vms, can take the backup file, folder**,** OS, disk.
* Azure backup offers 3 types of replications:
  1. LRS
  2. GRS
  3. ZRS
* RSV in backend used blob storage to store the backup data.
* Deploy RSV in same region.
* In RSV, update backup configuration and configure backup policy like schedule time and date retention period, backup frequency and add Vms for backup then enable backup.
* Also configure alert for the backup and email address in notification.
* If client required immediate backup, then go through backup now and this will retain the backup till. By default, 30 days from the date of backup performed
* In case of VM crash down, then restore the full vm through RSV, but before restoring full vm create a storage account, now restore VM by selecting the latest restore point and also select create new VM for restore configuration in same RG, then click on restore.
* Once restoration of VM done then take RDP access of restore VM which having all data.
* In case if file and folder deleted from VM remote server, then recover through RSV by selecting backup, items of VM and then start file recover by selecting latest recover point and download script and copy generated password.
* Now drive mount in this PC’ of VM server from where we can lift and shift deleted file and then unmount disk from portal (RSV).
* Backup VMs once a day.
* First time full backup then after do incremental/modified data backup.
* Work in same region.
* Size of RSV is unlimited and the backup data in RSV is maintained by Microsoft.
* NO data transfer from one RSV to another RSV.
* In single region we create a maximum 500 RSV.
* **Mars Backup**: Backup from on-premise server to Azure.
* First time full backup then after do the modified data backup.
* MARS agent support backup of

1-File and folder

2-Volume level

3-System level.

* Work in same region.
* Deploy RSV and prepare infra by downloading recovery service agent and vault credential key.
* Install MARS agent in on-premise server and process registration using vault key.
* Now open MARS agent console in on-premise server.
* Backup now option not available, first configure the schedule backup, for selected backup item and then configure the retention policy.
* If client required immediate backup, go to backup now and select backup item for backup then click on backup.
* In case if backup data deleted from on-premise server, then recover data through MARS agent console.
* Select the server from which data recover but data will recover till the last backup, then click on mount.
* New drive mount on the on-premise server now recovers the data from drive.
* Now click on unmount in mars agent console.
* Maximum 3 backup frequency allowed in a day.

**Azure Backup delivers these key benefits:**

* **on-premises backup**:
* **Back up Azure IaaS VMs**:
* **Scale easily** -
* **Get unlimited data transfer**:
* **Keep data secure**:
* **Centralized monitoring and management**:
* **Retain short and long-term data**: You can use [Recovery Services vaults](https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview) for short-term and long-term data retention.
* **Multiple storage options** - Azure Backup offers three types of replications to keep your storage/data highly available.
  + [Locally redundant storage (LRS)](https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#locally-redundant-storage) replicates your data three times (it creates three copies of your data) in a storage scale unit in a datacentre. All copies of the data exist within the same region. LRS is a low-cost option for protecting your data from local hardware failures.
  + [Geo-redundant storage (GRS)](https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#geo-redundant-storage) is the default and recommended replication option. GRS replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS costs more than LRS, but GRS provides a higher level of durability for your data, even if there's a regional outage.
  + [Zone-redundant storage (ZRS)](https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy#zone-redundant-storage) replicates your data in [availability zones](https://docs.microsoft.com/en-us/azure/availability-zones/az-overview#availability-zones), guaranteeing data residency and resiliency in the same region. ZRS has no downtime.

**Azure Backup Components:**

**1-Mars Agent (Microsoft Azure recovery service)-**

* No separate backup server
* On-premise backup
* Max 3 times per day
* Only RSV for backup

**2**- **System Centre DPM-**

* System Centre DPM can backup of VMware VM. also, backup of windows and Linux
* It cannot backup of Oracle workload.
* It is used locally attached disk and RSV for Backup.

**3- Azure Backup server-**

* Flexible when to take backup
* *It* can backup of VMware VM.
* It is used locally attached disk and RSV for Backup.

**4-Azure Iaas VM backup-**

* No agent required for backup.
* Backup VMs once a day.
* Cannot backup on-premise.
* No locally attached disk, only RSV.

**NOTE-**In on Region we can create 500 Recovery service vault.

[**Recovery Services vault**](https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview) is a logical container that stores backup data for protected resources, such as Azure VMs. When a backup job runs, it creates a recovery point inside the Recovery Services vault. You can then use one of these recovery points to restore data to a given point in time.

**Lab-Azure Backup-**

**Create Recovery service vault**

**(Name, Subscription and location)**

**Now Recovery Service Vault- Click on Backup**

**Where is your workload Running?**

**1-Azure**

**2-On-premise**

**What do you want to backup?**

**1-File & Folder**

**2-Hyper-V VM**

**3-Vmware VM**

**4-Microsft SQL server**

**5-Microsoft share point**

**Prepare Infrastructure**

**Install recovery service agent(40mb)**

**Download vault credential**

**Now open icon shown on desktop**

**Register server-enter vault credential**

**Once register-Now click on schedule backup**

**Now select item to backup**

**Schedule a backup everyday**

**Backup Now**

**Delete some file and recover data**

* **Site Recovery service**: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages.
* **s**ite Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
* **Backup service**: The [Azure Backup](https://docs.microsoft.com/en-us/azure/backup/) service keeps your data safe and recoverable.

Site Recovery can manage replication for:

* Azure VMs replicating between Azure regions.
* On-premises VMs, Azure Stack VMs, and physical servers.

**Azure Active Directory**

**A Group Policy Object (GPO) is a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor. GPOs can be associated with single or numerous Active Directory containers, including sites, domains, or organizational units (OUs). The MMC allows users to create GPOs that define registry-based policies, security options, software installation, and much more. Active Directory applies GPOs in the same, logical order; local policies, site policies, domain policies and OU policies.*GPOs that are in nested OUs work from the OU closest to the root first and outwards from there.***

**Work Group-In work group all host connected in peers means they are controlled itself.In work group each users setup account means the computer you are logging in should have an account.User can use his login credentials only on his system and not others**

**Server opareating system,network operating system or client operating system this is by default member of work group (Each computer by default member of work group).**

**Domain Network-In domain network each host are connected to server and server managed by network administrator**

**Domain Controller-.On Microsoft server,a domain controller is a server computer that respond to security authentication request(logging in,checking permission etc)within a window domain.**

**Use of Domain controller-**

**\*Centralized management of network resource, user groups, computer and printer**

**\* Better password management**

**\*Software deployment**

**Organizational unit(OU)-An OU is container that represent a logical grouping of resource that have similar securities or administrative guidelines.**

**Single sign on(SSO)-SSO is an authentication process that allows a user’s to access multiple application with on set of login credential.**

**Active Directory-Azure AD is a cloud-based service for identity and access management (**[**IAM**](https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system))**. For an organization, Azure AD helps employees sign up to multiple services and access them anywhere over the cloud with a single set of login credentials.**

**With Azure AD, the administrators can handle multiple user logins without any issue. Administrators need to assign a single username and password to access all the services they want.**

### Security in Azure AD

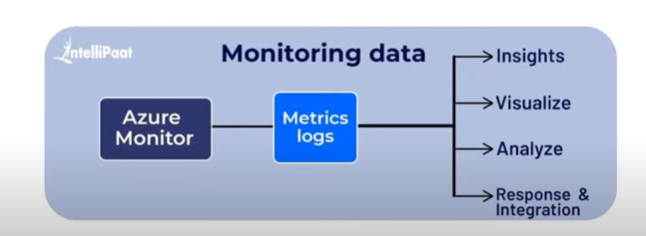
**Azure AD contains a number of features to secure and protect organizational data. Azure AD's security features include MFA, SSO for cloud-based SaaS applications, context-based adaptive policies,**[**identity governance**](https://www.techtarget.com/searchsecurity/definition/identity-governance)**, an**[**application proxy**](https://www.techtarget.com/searchwindowsserver/definition/Web-Application-Proxy)**to secure remote access and protective machine learning (to guard against stolen credentials and suspicious log-on attempts).**

### Azure AD features and licensing

* **Unlimited single sign-on**
* **User provisioning**
* **Federated Authentication (Active Directory Federation Services or third-party identity provider)**
* **Users and group management**
* **Device registration**
* **Cloud authentication (Pass-Through Authentication, Password Hash synchronization, Seamless SSO)**
* **Azure AD Connect sync, which extends an organization's on-premises directories to Azure AD**
* **Self-service password change**
* **Azure AD Join (desktop SSO and administrator BitLocker recovery)**
* **Password protection**
* **Multifactor authentication**
* **Basic reporting for security and usage**
* **Azure AD features for guest users**

**Azure Monitor-**

Microsoft Azure Monitor is tools that collect and analyses the data about of various azure resources and infrastructure on which azure resources are run and the data collect in the form of metrics and logs. This data can then be processed to perform various functions such as analysis, visualization, alerting, automation and integrations.”

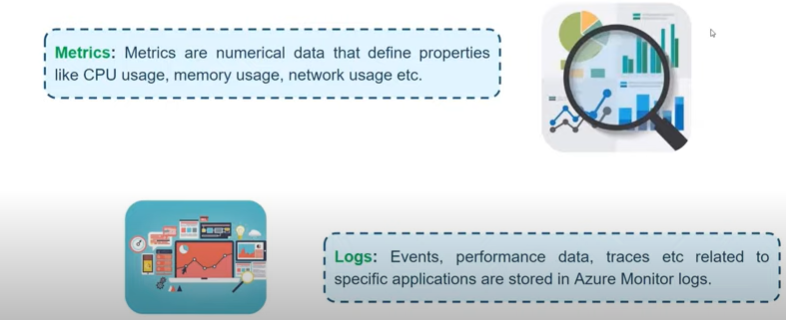


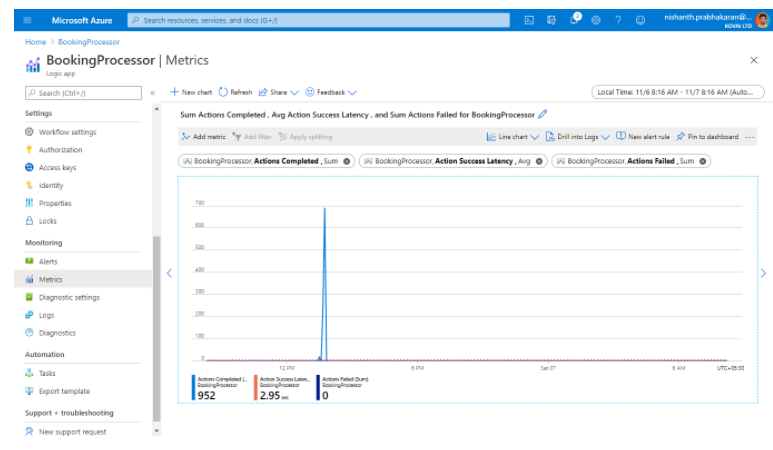
### ****Metrics and Logs seem to be at the core of Azure Monitor, so what are they?****

### ****2.1 Metrics****

Metrics are numerical data that defines properties like CPU utilisation, memory utilisation, network utilisation These are usually real-time, and as they’re stored as values with a regular collection interval, they’re perfectly suited to being displayed as graphs to help you view performance over time.

* The focus for metric-based data types ids the numerical time-sensitive values that represent some aspect of the target resource.

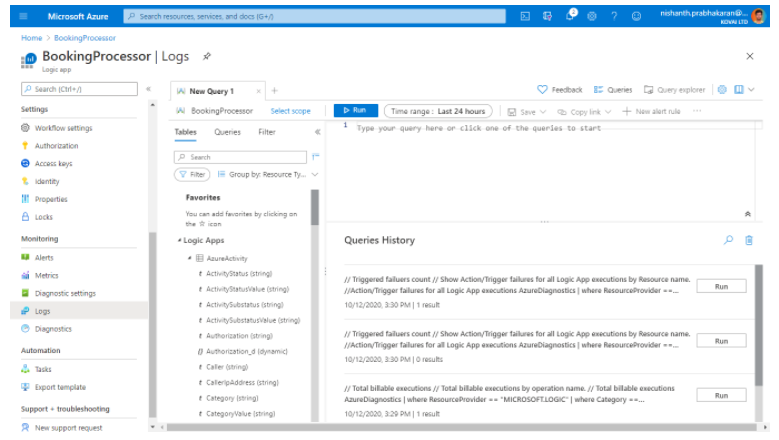




### Logs-

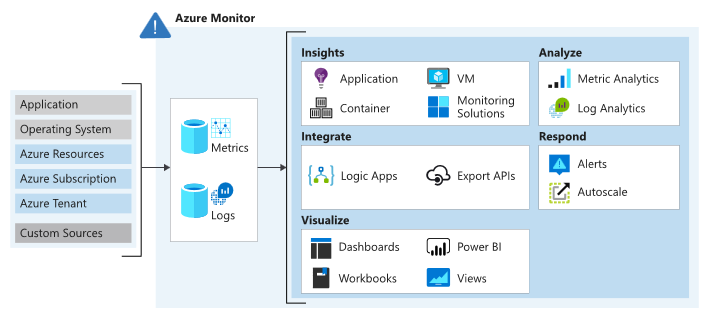
Events, performance data and traces etc related to specific application are stored in azure monitor logs. The logs can include numeric values such as Azure Monitor metrics, but most include text data rather than numeric values.

* The focus for log-based data types is the querying of content data held in structured, record-based log files that are relevant to the target resource.



## **What data types does Azure Monitor collect?**

The following diagram gives a high-level view of Azure Monitor. On the left are the sources of monitoring data: Azure, operating systems, and custom sources. At the center of the diagram are the data stores for metrics and logs. On the right are the functions that Azure Monitor performs with this collected data, such as analysis, alerting, and streaming to external systems.

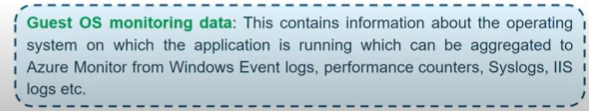


Data can be obtained from a range of sources through Azure Control. Users can opt for monitoring data at different levels across the application, any operating system, and resources it depends on, including the platform itself. For each of the following levels, Azure Monitor collects the data:

**Application data:**



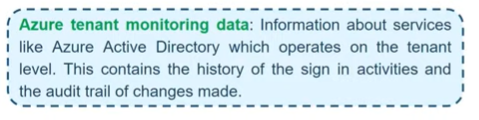
**Operating System data:** Data regarding the operating system in which the application is running i.e., data from the Windows or Linux virtual machines that host your application. It could be run on Azure, another cloud, or on-premises.



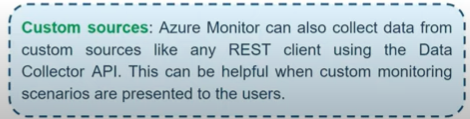
**Azure resource data:** Data that relates to the operations of an Azure resource, such as a web app or a load balancer.

**Azure subscription monitoring data:** Data that relates to the subscription and it also includes data about [Azure health](https://www.serverless360.com/blog/azure-health-monitoring) and availability.

**Azure tenant monitoring data:** Data on the Azure organization-level services, such as Azure Active Directory.



**Custom sources**-



Since Azure Monitor is an automatic system, it begins to collect data from these sources as soon as you create Azure resources such as virtual machines and web apps. You can extend the data that Azure Monitor collects by:

* **Enabling diagnostics**: For some resources, such as [Azure SQL Database](https://www.serverless360.com/azure-sql-database-monitoring-management), you receive full information about a resource only after enabling diagnostic logging for it. You can use the Azure portal, the Azure CLI, or PowerShell to enable diagnostics.
* **Adding an agent**: For virtual machines, you can install the Log Analytics agent and configure it to send data to a Log Analytics workspace. This agent increases the amount of information that’s sent to Azure Monitor.

### Alerts

In Azure Monitor, alerts proactively notify you when issues are detected with your infrastructure or application using your monitoring data. Before the users of your system notice them, they allow you to identify and address issues. Alert rules are detached from alerts and the actions taken when an alert fire. The alert rule manages to capture the alert target and the alert criteria. It is possible to have the alert rule in an enabled or disabled state. Alerts fire only when enabled.

#### **Metric Alerts**

Metric alerts are used to achieve regular threshold monitoring of Azure resources. Azure Monitor runs metric alert trigger conditions at regular intervals. When the evaluation is true, Azure Monitor sends a notification. Metric alerts are stateful, and Azure Monitor will send a notification only when the prerequisite conditions are met. Metric alerts can be useful if, for instance, you need to know when your server CPU utilization is reaching a critical threshold of 90%. You can be alerted when your database storage is getting too low, or when network latency is about to reach unacceptable levels.

#### **Log Alerts**

Log alerts use log data to assess the rule logic and, if necessary, trigger an alert. This data can come from any Azure resource: server logs, application server logs, or application logs. By its nature, log data is historical thus usage is focused on analytics and trends. These types of logs can be used to assess if any of your servers have exceeded their CPU utilization by a given threshold during the last 30 minutes. Or, you can evaluate response codes issued on your web application server in the last hour.

#### **Activity Log Alerts**

Activity log alerts enable you to be notified when a specific event happens on some Azure resource. For example, you can be notified when someone creates a new VM in a subscription. An activity log can also include alerts for Azure service health. Activity log alerts are designed to work with Azure resources. Typically, you create this type of log to receive notifications when specific changes occur on a resource within your Azure subscription.

## **Native Azure Monitoring tools**

Azure itself offers hands-on native monitoring tools to ensure that you built your Azure integration and get it monitored under the same roof. Listed below are the native monitoring tools offered by Azure,

### Activity Logs

The Azure Activity Log is a Subscription log that gives knowledge into Subscription level events that have been created in Azure. It incorporates a scope of information, from Azure Resource Manager operational information to refreshes on Service Health events. You might need to Archive the Azure Activity Log in case you retain your Activity Log longer than 90 days for governance, investigation and backups.

### Log Analytics

Azure Log Analytics Workspace is the logical storage unit where log data is collected and stored. It can be considered as the primary management unit of Azure Monitor Logs. It is used to collect data from various sources such as Azure Virtual Machines, Windows or Linux Virtual Machines, Azure Resources in a subscription, etc. It facilitates an assured monitoring service to fulfil the monitoring needs of the user.

### Azure Alerts

Alert is a monitoring service offered by Azure Monitor that proactively notifies the user when issues are found with your infrastructure or application using your monitoring data in Azure Monitor. There are three types of Azure Alerts available:

* **Metric Alerts:**These alerts will monitor the Azure resources based on Metrics that are specific to Azure resources and alerts the user whenever there is a Violation with the configured threshold value. E.g., Count of Dead-Letter messages metric for Service bus, Run Succeeded for Azure Logic Apps.
* **Log Alerts:**These alerts allow users to monitor the Log Analytics queries by evaluating resource logs every set frequency, and trigger a notification based on the values returned from the query.
* **Activity Log Alerts:**Activity log alerts will send an alert report whenever there is a new activity log event occurs that matches the specified condition.

### Azure Diagnostics

Azure Diagnostics offers capabilities to export to metrics and activity to logs to other resources for Custom monitoring and manipulation. These diagnostic logs can be passed to resources like Azure Storage, Log Analytics workspace, and Event hubs for further processing.

### Azure Metrics

Metrics are numerical values that describe some aspect of a system at a particular time. Metrics are collected at regular intervals that can be used for analysis, visualization, and monitoring. Every Azure resource offers an extensive set of metrics specific to that resources which can be used to create charts and alerts.

### Service Health-

### Provides personalized views of the health of azure services, region and resources. Events includes: Service issues, planned maintenance event and health advisories.

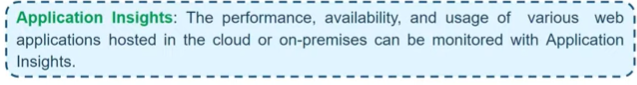
[Azure Service Health](https://www.serverless360.com/blog/azure-health-monitoring) keeps you informed on any planned downtime. Due to maintenance some resources and regions may have some impact, and this will be intimated to the users in advance so that they can act accordingly.

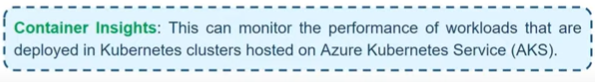
Azure service health contains three Events that help you understand better some unexpected errors and planned downtimes.

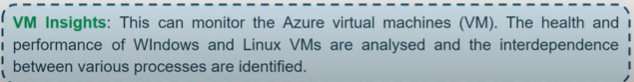
* Service Issues – Contains reports of the current issues happening in Azure like service outages, etc. and even the solution from the Azure development team can also be found here
* Planned maintenance – Contains reports of planned maintenance service scheduled by Azure and even reports of some solution on how you could achieve less impact on this downtime
* Health advisories – reports issues that require your action to avoid service interruption

### Azure Application Insights

Application Insights are used to monitor live applications and to Detect and Analyse issues in the applications. It can do anomaly detections and designed to improve performance and usability.







**Azure autoscaling-** Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. Auto scale allows you to have the right amount of the resources running to handle the load on your application. It allows you to add resources to handle increases in load and also save money by removing resources that are sitting idle.

You specify a min or max instance to run and add or remove VMs automatically based on a set of rules.

Scale Out (+)-Increase the VMs

Scale In (-)-Decrease the VMs

**Types of scaling-There are two types of scaling-**

**1-Horizontal Scaling-**Horizontal means increase or decrease no. of VMs according to situation.

2-**Vertical Scaling**-Vertical scaling keeps the same no. of VMs, but makes the VM more or less powerful power in terms of memory, CPU, speed & disk space require VM to stop and restart.

**Public IP address and Private IP address-**

When we create virtual machine there are two types of IP address are assigned.

**1-Public IP address**-With the help of public IP address we connect the resources to external resources via internet. Two types of public Ip address

* **Dynamic-**Dynamic Assignment is provided temporary public IP address. This type of public IP address will be changed if VM is stopped.
* **Static-**Static assignment provide the fixed public IP address. Static Public IP address will not be change if VM are stopped.

**Static Public IP address are commonly used in the following scenarios:**

1-When you must update firewall rules to communicate with your azure resources

2-DNS name resolution, where change in IP address would require updating A records**.**

**2-Private IP address-**This used for local network.

Private IP address is automatically assigned in Vm but public IP address is optional. By default, private IP address is dynamic assignment, but we can change to manually if we select static.

For Change of Dynamic assignment to static assignment-

Go to network interface card---Click on IP configuration-Change dynamic to static

**Lab Public IP address**

**1-Search Public IP address-Select IP address--- Assignment-1-Dynamic-(Temporary)**

**2-Static-(Permanent)**

**Create**

**2-Select created public IP address-**

* **IP version-**

1-IPv4 2-IPv6 3-Both

If we select IPv4 then we use this public IP in Virtual machine and load balancer.

If we select IPv6 then we use this IP in only load balancer.

* **SKU-**
* 1-Standard 2-Basic

If we select standard SKU then only static assignment available in IP address assignment. Dynamic assignment is disable.

* **Tier-**

1-Regional 2- Global

If we create cross region load balancer then we select Global tier.

* **Name-**
* **IP address assignment**

1-Dynamic 2- Static

* **Routing preference-**

1-Microsoft Network 2-Internal

* **Idle time out-**

Maximum-30 min

Minimum-4 min

* **DNS name label-**
* **Subscriptions**
* **Resource group**
* **Location**
* **Availability zone-**

**1-**No zone **2-** Zone redundant **3-**1 **4-**2 **5-**3

If we select Standard SKU availability zone option available. In the case of Zone redundant, public IP address advertise in three availability zone. In case anyone zone is down then the public IP address is available in next two zone.

**Create**

If we change Public IP address then go to IP address Configuration, change public IP address and save.

**PIP Basic SKU and Standard SKU**

**Basic SKU public IP address**-In basic SKU by default all port is open. In Basic SKU NSG is optional so that Basic SKU is less secure.

For IPv4-can be assigned using the dynamic or static allocation method.

For IPv6-can only assigned using the dynamic allocation method.

Have an adjustable inbound originated flow idle time out of 4-30 min with default of 4 min and fixed outbound originated flow idle time out of 4 min.

Are open by default, Network security groups are recommended but optional for restricting inbound or outbound traffic.

Don’t support availability zone scenarios.

**Standard SKU public IP address**- In standard SKU by default all port is secure(closed), also for standard SKU NSG is mandatory so that this is secure as compare to basic.

Have an adjustable inbound originated flow idle time out of 4-30 min with default of 4 min and fixed outbound originated flow idle time out of 4 min.

Are open by default, Network security groups are recommended but optional for restricting inbound or outbound traffic.

You Can associate a public IP address resource with-

1-Virtual Machine network interface

2-Internet facing load balancer

3-Virtual Network gateway.

4-NAT gateway

5-Application gateway

6-Azure firewall

7-Bastion host