* Azure was initially called the **Project Red Dog** in the year **2008**
* Officially launched in 2010 on feb 1st.
* **56 Regions and 140+ countries**
* Regions is a geographical area which may contain one or more availability zones.
* The primary purpose of the paired region is for the HA
* Region >>Availability zones >> Data Centers >> Racks >> servers >> virtual Machines
* Azure users by default Azure provided DNS.
* activity log is used to record all activities performed in azure rg along with time stamp
* Connected devices (VNET)where you can see all the NIC cards and the Virtual Machines
* Azure reserves the 5 subnets they are **Network IP, gateway ip , DNS IP’s and the Broadcast IP**
* Vertical scaling means increasing the configurations
* Horizontal scaling means increasing the instance/VM count
* **Gateway Subnet** to establish the external communication
* **DDOS (Distributed denial of service)** which is used to help and be able to handle multiple requests from multiple end users by writing the rules in the basic or in the standard where we can customize it (eg: flipkart sales, Amazon.)
* In the **NSG** by default **Outbound internet is allowed**.
* Route Table is used to define the path of the network communication.
* **CIDR** (Classless Inter-Domain Routing) -- also known as super netting -- is a method of assigning Internet Protocol (IP) addresses.
* **VM** are of three types (ON-Demand, reserved, spot VM’s)
* **On-Demand :** create use and terminate
* **Reserved :** To give the commitment to the microsoft for the 1year or 3years (for termination also have to pay fee)
* **Spot VM:** Azure uses unused space for the creation of the VM and based on the amount for the bidding VM will be deallocated automatically if the bidding is high.
* **Availability set >> Update domain(20) parallel>> fault Domain (3) series**
* **Fault Domain :** it’s a logical group of underlying hardware share common power and network source
* **Update Domain :** It’s a logical group of underlying hardware that undergoes maintenance & rebooted sametime.
* **VM Generation :** Gen1 (Boot BIOS) VHD Gen2 (UEFI) VHDX
* **Host Group :** it’s a collection of the dedicated hosts.
* **Cloud Init :** it is used to install the software’s and the packages and configuration initially after the first boot (linux)
* **Snapshot :** can be only created only for the OS disk itself.
* **Azure Hybrid Benefit:** it's used to save the licensing cost of the machine.

To create a virtual Machine the following are the processes.

First need to create a Resource Group

Second need to create a Virtual Network

Third need to create a NSG group

* TO create a Custom Image

First we have to run the cmd (**sysprep/generalize**) in the launched instance or in the VM. (if we won't run the cmd then it won’t turn on)

Second we need to click on the capture and then need to add those

* **Bastion :** you can connect to the VM from the browser itself and public IP is assigned but not visible
* **Auto-Shutdown :** we can schedule the shutdown time of the VM along by sending the notification to the email
* **VNET peering :** It’s a concept in which we can connect 2 VNETs.

Open the first vnet and then click on the peering and then add the peering and establish peering from both the ends and click on save.

To verify login to the VM’s and then take the RDP of other VM’s Private IP.

We can peering between the regions as well which is known as the Global VNET peering.

* Express Route : connecting to Azure Vpn through a dedicated tunnel provided by the ISP
* Virtual Network Gateway : it’s a separate entity and needs to be created in order to create a VPN.
* VPN is of two types they are : Point2 Site (endpoint laptop) and Site2Site(route)
* Active-Active mode : which act as a backup tunnel to enable active mode we need other public IP
* **Point-2 -site configuration :**   
  initially we need to run the PowerShell script to generate the certificate.

Second now open the cert manager and then export the root and the client certificate from the personal folder in the cert manager

Third now click on the point-to-site configuration in the virtual Network gateway click on configure tab give the IP address range and choose the tunnel type (IKEv2) Authentication type (Azure certificate)

4th write the root certificate name and then paste the content in the public certificate data the powershell code of the generated root certificate and click save and download the VPN client extract and install it and import the client certificate. Then click on **connect**

* **Site-to-Site VPN :**

1st it’s a continuous VPN where we have to check the path

2nd open the virtual network gateway and in that open connections click on add name Eg: Azure2onprem

Connection type is site-to-site **Local Network gateway** click add give the name and the IP and IP range address of the onprem server and ADD

3rd click on the shared Key (PSK) and enable the IKEv2 and click **OK**

4th check open the Onprem server and from that ping Azure VM private IP and connect the RDP.

Storage

Azure storage is of two types: they are storage accounts and the other is the managed disks.

Storage types.

**Blobs : (**Binary Large objects**)** its a massively scalable object which is used to store the text and the binary data

**Files :** which are used to managed file shares for the cloud and for the on-prem deployments

**Queues:** it’s a messaging store for reliable messaging between application components. And used for sending the notifications to mobiles anything under the pipeline can be handled using queues.

**Tables :** it’s a NOSQL db used for the less storage of structured data.

Storage AccessTires:

HOT : it’s a data which we can access frequently is placed in the HOT tire

COOL : it’s a data which we can access infrequently is placed in the Cool tire, which is of minimum 30days

ARCHIVE: it’s a data which we can access rarely is placed in the Archive tire, which is of minimum 180days

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Instance Types

**General Purpose** : CPU : Memory = (standard d64-V3 256GB Ram 1600 GB ROM) for testing and development

**Compute optimized :** high CPU : Memory (standard F72-V2 144GB Ram 576 GB ROM) for app servers and web server

**Memory optimized :** CPU : Memory high (standard M128-V3 3892GB Ram 14336 GB ROM) for in-memory analytics to large cache.

**Storage Optimized :** provide high disk IO(standard L32-V3 256GB Ram 5630GB ROM) for Big Data NoSQL,SQLDB

**GPU** : (standard ND24rs 448GB Ram 2948 GB ROM 4 GPU and 96GB memory) for high graphic and video editing **High performance compute :** (standard L32 224GB Ram 2000 GB ROM) faster and powerful

Route table >> routes >>address range and then next hop address

Azure

**Capture**: which creates the custom image of the ISO

Service Endpoints

The primary moto of the service endpoints is that to restrict the public accessing URL (like mapped drives)

* Create a storage account in the Same region
* In the storage account create some files in (blob, files,tables,queues) and upload the files.
* To restrict the access storage account>> networking>>allow access from>>selected network
* Then need to give access to the private Vnet access so write a rule in the NSG to allow for the Azure Storage account
* Then open storage account>>private endpoint>>add>>connect to resource in my directory>>resource type>>Microsoft storage account >>give the private vnet>>create
* Now open the storage acc>>open the file that you have created and then click on connect it will generate a PowerShell script and then open the private VM and PowerShell and then paste the copied script and then execute it so that you are able to MAP and access the file storage.

Load Balancer

Load balancer which is used to route the traffic to the backend pools. Operates in layer 4

If simultaneously requests can be able to handle by using the different hosts in the backend pools

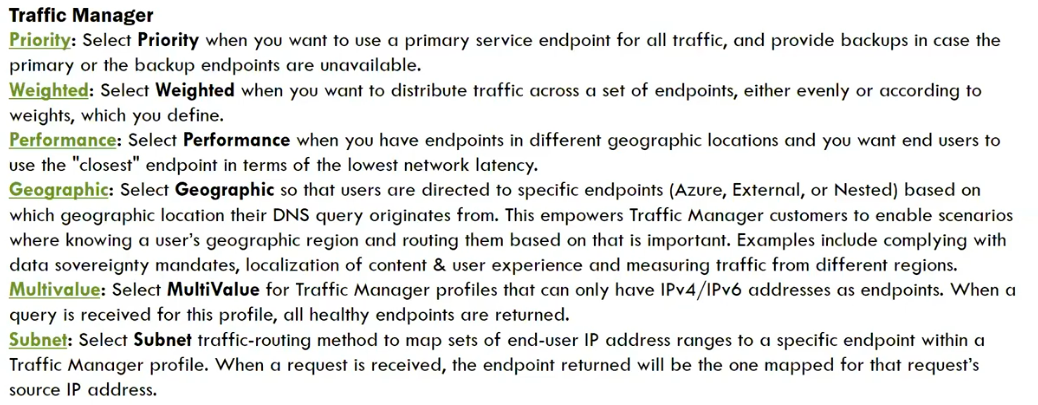
* Create a load balancer
* Enable the IIS web server in both the VM and in the LB>>backend pools>>add>>name, vnet, virtual machine, give the machine within the available set.
* Health probes (check run) add those either in TCP or HTTP
* Need to write the load balancer rule give the backend pool and health probe
* Browse the public IP which will hit the web server

Table

Description automatically generated

Application Gateway

* It can only handle the HTTP and HTTPS traffic only. Operate in layer 7
* Built in auto scaling and SSL termination at the gateway (offline SSL loader)
* Create an application gateway and select the tire (standard, WAF, WAFv2(autoscaling enabled and firewall)) and set it in the separate subnet and set the backend pools >> configuration add the routing rules (listeners and backend target) and create HTTP settings and then review+create.
* Traffic manager profile (geographical based on the region) can able to manage the load





**ONprem>>Azure Migrate**

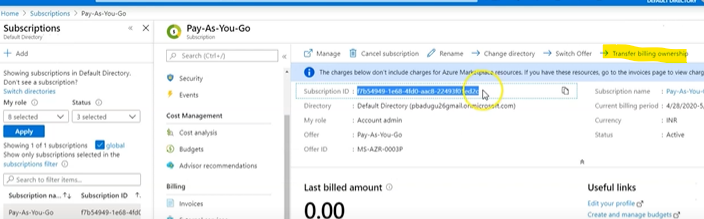
Onprem Prerequisites:



Azure Prerequisites:

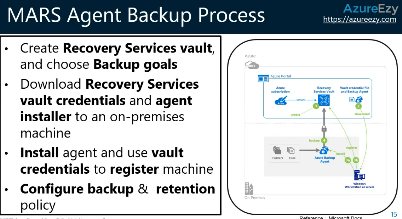
subscription>>network>>storage>> azure recovery service vault

**EA to CSP migrate**

* online billing transfer go to the subscription and then transfer billing membership  
  
* we need to give the other account email id and we will receive an email and then we need to accept it
* It will be route to the payment info like credit card info upon entering the details the transfer will start
* Then upon successful transfer you can able to see the subscription details in the subscription section

onprem-azure

* MARS for the backup (or the data box) we can take backup of files, everything, system, volume
* MARS process (create recovery service vault by choosing backupgoals) (Key vault & MARS agent)
* **MARS need to config>> enter key vault cred>> it register the VM in the recovery service vault**
* **then need to specify the backup & retention policy.**
* MABS and DPM (data protection manager)



Migrate Process

* Azure Migrate >> create a new project>>
* Server assessment >> discover >> generate migrate project key >>download migrate appliance>>import in Hyper V
* Then open azure appliance config manager>>registering with the VM project key>>share the Hyperv and host details >> validate>>start discovery
* IT would register the VM’s and will enable the access, overview and servers will be discovered
* create an assessment by selecting the servers (which we want to migrate)
* we need to replicate the VM >>select the group>> and the VM>>target account is the storage account>> and select the Vnet.>>>replicate it
* Under replicating machines, wait for status to be changed to protected
* Then click on Migrate>>>select the VM>>Migrate  
  status can be seen in the **Jobs** section

Backup of VM

* create a recovery service Vault>>new Backup >>choose the workload running (onprem, azure,stack)>> vm>>set the backup policy and retention policy>> add the VM>> backup

**Onprem**

* create a recovery service vault>>new backup>>choose the workload>>what u want to backup(files,folders,system volume,hyper v, vmware..etc)>>prepare infrastructure>>then download MARS agent and vault key.
* Install the MARS agent on the on-prem (it registers to azure account with the help of the recovery vault key)>>set the passphrase (for encrypt)>>finish.
* Azure backup console >>we can schedule backup based on the backup policies>>chose the files or folders to backup >>finish

**ARM TEMPLATE**

* cloud shell deployment of the arm template command(az deployment group create –resource-group optimized-vm-rg –template-file template.json - - parameters paraments.json
* To see the status using the cloud shell bash   
  Az provider show - - namespace microsoft.insights -o table (to see the status of microsoft insight o/p in table)