**Basics in Azure**

* **Virtual machines**
* **Storage :** types,managed, unmanaged,storage accounts
* **Network** : vnet,subnet,virtual network gateway, Traffic Manager
* **Firewall** : NSG, Azure Firewall
* **Access Manager** : IAM, roles and authentication

**VNET**

* Azure vnet is the backbone of the azure infra CIDR (classless inter domain routing)
* Primary used for machine -to- machine communication & Outbound & inbound internet
* Subnet is the smalled chunk of vnet
* Gateway subnet : Main moto is to establish communication between two different networkswhere public ip might be involved.

We cannot create multiple gateway subnets

* Private ip is a non routable ip address
* Azure reserves 5 Ip (0-network address, 1-az gateway,2,3- az dns server,255-broadcast ip)
* Every new machine ip which starts with .4
* In azure vnet we can add our own dns server VNET>>dns server>>custom
* Address space : 10.0.0.0/16 where we can add the CIDR range here.
* Connected devices : where we can see all the NIC cards here
* DDos :distributed denial of service attack
* Locks: are primarily used to prevent the accidental deletion or modifications
* Azure Event Hub: which is used to store the events in that hub
* Connection monitor : which is used to have all the network info about the client machine(P2S)VPN
* NSG : it acts as a basic first level of firewall at the subnet level  
  It primarily used to control the inbound and outbound traffic  
  Rules created in the NSG will be applicable to all instances with in the subnet  
  Rules are created along with their own priority (lowest first)
* Network interfaces: in NSG where we can write or customize all NSG rules for each VM’s
* Effective security rule : which is used to find the conflicts btw the NSG rules with in the Network interface and the subnet level and gives the consolidated data
* Route table : it simply defines the path of the network from source to destination
* Route table (adding the route rule to block the dest CIDR range and hop type as none) which blocks the traffic to that CIDR range network.
* Virtual network gateway route propagation: which is used to enable and detects automatically all the routes for the gatewaysubnet.
* Vnet peering : its to establish the communication btw the different networks of the same region
* Global Vnet peering :its to establish the communication btw the different networks of the different region
* Transit gateway : its to dedicate a VNet as a bridge to pass the traffic through it and to peer through it
* Service endpoint : creating a connecting string for the service with in the network

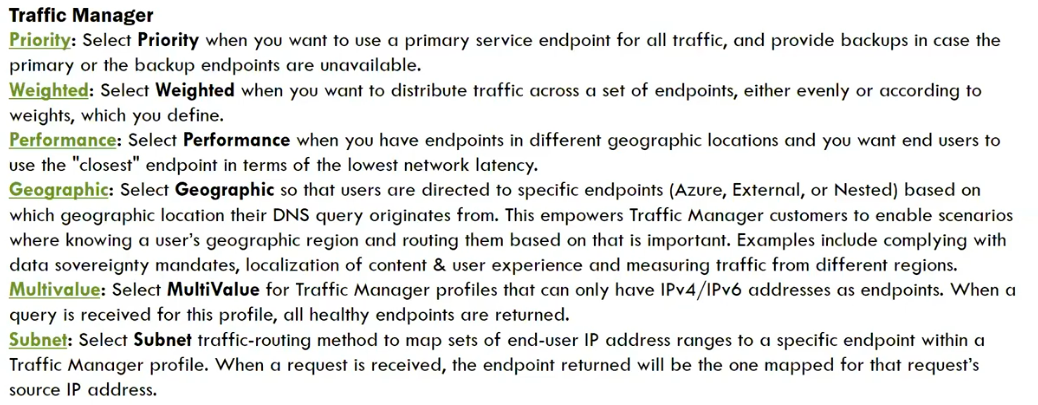
**Virtual Machines**

* Its a compute service simply system within a system (using VMware,hypervisor,Virtualbox)
* Azure vm’s backup are with **vhd & VHDX**files
* If the vhd or vhdx size is greater then 8TB its recommend to use Azure data box (snow ball) where page blob supports only 8TB of data.
* **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.
* If we shutdown the vm with in the VM then in the console it would reflect as the stopped state only
* **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.
* **VM sizes** : general purpose and compute optimized (F series) Memory optimized (E series)
* Networking : NSG rules (inbound,outbound, App security groups, LB) and association to network interface cards and to the subnets and effective security rules and topology (network diagram)
* Disk: managed(encryption) unmanaged(no encryp) we can add data disk (d drive) and can able to swap OS disk with other (snapshot or custom disk)  
  We can also export disk by SAS(shared access signature) for some duration
* **Size** : where we can resize the VM (vm will be re-deployed) restart will happen
* **Security** : security center free is default (which shows the vulnerabilities and recommended settings in VM)  
  Just-in-time access: which allows us to give access to VM for some duration based on token authentication
* **Extensions** : we can install the additional external 3rd party Microsoft tie up agents
* **Bastion** : uses static public ip which hides and can able to access vm using browser
* Disaster recovery : which is use to create a replica on the cloud and if same region will maintain sync with the primary and replica if not same region then its async with(max 1min delay) btw the primary and replica.  
  On-prem then it download ASR agent (azure site recovery) which collects and creates the replica in azure
* Update management : which is used for the patch updates with in the server which will be monitored by the Microsoft monitoring agent.(where we can schedule the updates as well)
* Guest level monitoring : which is used to maintain the heart beats for monitoring the health status of it which help in system diagnostics
* Connection monitor: which is used to make the connections for the other network or the domain it tries to communicate the destination IP or the server based on the time interval
* Service health : which is used to specify the service and region heath status respectively.
* Perform diagnostics : which is used to perform the diagnostics in the end machine
* Reset password : where we can reset the password & the reset the configurations only
* Redeploy : which is used to redeploy the vm on a new hardware without data loss (unable to boot or connect to the vm or some Bluescreen error )
* Serial console: SAC(special administration console)
* Connection troubleshoot : which is used to test the network connectivity inbound and outbound

**Azure Load Balancer**

* Efficiently distributing of the loads or distributing the incoming network traffic.
* Vm should be in the availability set (inorder to distribute between the FD and UD)  
  FD(rack level network and power issues) UD
* Backend pools : used to manage the websites with in the all vm’s
* Health probes : it used to perform the check run for the service or the connection establishment coninuously
* Frontend ip config : which is used to have the public ip details
* Session persistence : (it allows us to goes to the same vm which the frequently used server )

**Application Gateway**

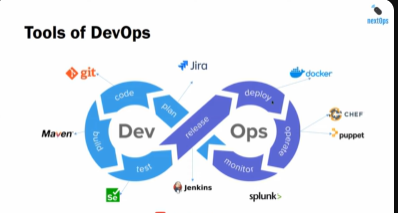
* Its only defined to distribute the web traffic which helps us to manage the application.(http & Https)
* Http settings : which are used to modify the header content
* Cookie based affinity : which is used to hit the same vm server all the time
* Connection draining : during maintenance it prevents in the abnormal connection of the machine based on the duration of the seconds
* Webapplication firewall : additional layer of security for the web apps
* Frontendpublicip : where we can add one public ip only and multiple listeners
* Pathbased rule : which is used to route to the listener based on the URL path.
* Rewrite set : we need to enable to rewriting capability of the LB (header path)  
    
   **Traffic Management (Route 53)**
* Its a DNS based traffic LB which enables us to distribute traffic to services(or VM) with in global regions of azure VM’s.  
  
* Azure endpoint : which allows you to use the app services and public ip address and app service slots
* External endpoint : which can able to access the onprem vm ip’s using S2S vPN
* Nested Endpoint : which allows you to add the custom profiles (shown in img)
* Realusermeasuremnts : which gives the info while using the website similar to header info

**Azure Firewall**

* In order to create an azure firewall it should have AzureFirewallSubnet (subnet should be their in the VNET)
* AZ firewall should have the separate public ip for it
* We need to define the inbound and outbound firewall rules

**Azure Storage**

* Queue : used for the mobile notification and for the push notifications and stores the transactions
* Tables : Nosql file types uses tables
* Fileshares : similar to network drives
* Containers: VHD disks
* Blobs: a massive scalable objects store for text and binary data.
* Storage explorer : is a stand-alone tool to integrate with azure and can able to access the storage account
* Datatransfer: to tarnsfer the data from source to destination which recommend you the options based on the data size and bandwidth speed   
  AZcopy : azure standalone CLI tool its a slow tool  
  AZstorgaeExplorer: GUI interface tool to  
  Az rest API :   
  AZ databox : primary for the VHD files recommended
* Events : which acts as alerts when something is modified ( trigger action)
* Access keys : which are simply connection strings used for the authentication purpose.
* CORS : its a http feature that enables web application which is running under one domain can access resources in other domain.(Cross Origin Resource Sharing)  
  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
* Large fileshares : which provides max file share upto 100TB of data
* Block Blob : Can be managed individually stores text and data upto 4.7TB
* Append Blob : similar to block blob but stores the log data on it
* Page Blob : stores random access files upto 8TB especially for VHD files
* Custom domain : where we can add the custom domain details to it.
* Data protection : its a default retention policy 7days once we delete the files.
* AzureCDN : content delivery network used for the streaming purpose
* Addsearchsite : which is used as web search engine for the designed app.
* LifecycleManagement : where we can manage the tiers by adding the rule conditions.
* Manage disks : its a disk space where it has the feature of having availability sets.  
    
    **Azure DevOps  
   **
* (Plan)Azure Boards: which are simply a todo tasks /work items which helps in planing (we can integrated jira ticketing tool  
  Which is primarily used to track the work  
  Backlog : if the task/work iteam is over due it will be in backlog.  
  Sprint : usually a 15days of time to complete the given task  
  Query : where its used as a filter by using query to obtain the results
* (Build) Azure Repos: its a centralized repository where we can store the code  
  Commit : its a place where we can modify the changes  
  Branches: its a similar to folder where the code is present  
  Push: we can see who pushed the code and what was the latest pushed code  
  Pull request : we can see who pulled the code and what was the latest pulled code
* (CI &CD)Azure Pipelines:  
  Triggers: which is used to monitor and enable continue integrity   
  Build : which is used to build the applications from the source code.  
  Options: its the primary option which gives the features and options about the laguage the application is written(.net)  
  Scheduled : its a also a feature where we can schedule the build by giving the time frame if not we can go by enabling continuous integration in triggers  
  Task: its an action that need to be performed on it (like archiving files…etc)  
  Release : where it releases the pipelines we can enable the continuous deployment trigger when the changes made will be deployed accordingly.
* (Testing)Test Plans:
* (Library)Artifacts
* Deveploment slot : azure provides the 5 development slots where we can clone the app and can do required modifications  
  In-order to prevent the business impact of the production environment If everything is fine in this we can swap it as the main production at any time.  
    
   **ARM Templates**
* Its a Json type coded file where we can deploy infrastructure with the help of these ARM Templates
* The primary ARM templates **azuredeploy.json , azuredeploy.parameters.json**
* Json(java script object notation) where we can write objects between { Key : value } we should not give **comma** for the last value.
* We can use **defaultvalue** as something in our main file if in case if we forget to give the inputs to the paraments so that it takes the default content value as the input.
* Most of the cases resources will start with the [ which means an array
* The dependency parameters we can write as **dependson** in the json file so that block will execute first
* Validation of the ARM template will happen from the second deployment only if the resource was already created it skips if not it will execute.  
    
   **Azure Key Vault**
* Its primarily used to store any kind of sensitive information (passwords, ssh keys, certificates )
* Soft delete is already enabled on it (min 7 days max 90 days) for the accidental deletion
* Keys: in order to connect to the linux machine we need the SSH key where we can use from here
* Secret : will the windows machines and passwords can be store here
* Certificates : where we can store import certificates and can able to generate the self signed certificates as well