**AZURE ZERO TO HERO**

**Basic of Cloud Computing:**

A developer develops an application in local computer. After that he host the application in a server.

A local computer has CPU,RAM , Storage and Display, graphic card etc.

A server is also a computer has CPU, RAM, and storage and the purpose of the server is to run application

**Data Centre:**

A bunch of servers at one place is called a data centre.

**Public cloud:**

The cloud services(virtual machines) are provided by the cloud providers like AWS, GCP and Azure.

**Private Cloud:**

The companies maintain their own data centres for security regions like finace, banking companies will do. These cloud services are called private cloud.

**Hybrid Cloud:**

It is mix of private cloud and public cloud. The companies request compute services from the cloud provider and they keep the data in their on premises data centre(private cloud).

**Multi Cloud:**

Requesting cloud services from multiple cloud providers like storage for azure, compute for AWS and database in GCP.

**Virtualization:**

A hypervisor software is used to logically partitioning the big server into multiple virtual servers called virtual machines.

**API:**

Accessing the application programmatically is called Application Interface. We can interact with the Azure through Console, CLI and API. The API is program that has the requirements of the resources we want and can run this code in the URL of the Azure to get the services.

**Regions:**

Each region has multiple availability zones. US-east-1 is region and us-east-1a &east-1b are the availability zones

**Availability Zones (Data centres):**

These are the data centres available in that particular regions.

**Services Models**

**IaaS:**

If you take VM, storage and network from cloud provider and use them to deploy applications and install software then it is IaaS.

**PaaS**:

If you take Database from the cloud provider for your use then it is called PaaS. Here we need not to think about the network, security, vm and storage. The configuration is required to use the PaaS.

**SaaS:**

Email, gmail, outlook, teams is a software service where we directly use the service we simply create an account to use it. No need for configuration.

**Day-3**

A resource is an instance of a service. Azure has various services and if you give the requirements then a resource is created.

**Azure Resource Manager:**

The requirements for a particular service are taken from user by the Azure Resource Manager. Then the ARM will create a resource for the user.

Just like the requirements for the VM like storage, OS, network etc. are taken by the ARM and it creates a resource.

**Resource Group:**

A resource group is mandatory to create any resource in Azure.

Its is grouping of resources under one name is called Resource Group. It is a combination of different resources.

If you group the resources then you can track them easily.

Listing Access, permissions, security , auditing, cost & billing can be tracked and managed & changes for the group of resources through the Resource Group. We can mange these things simply.

Grouping of the resources is one of the best practices so that we can manage the access, security, auditing etc for all the resources in that group. This is very easy.

In a company they have different teams and each team has different resources. To track them using tags is easy but creating a resource group and keeping the resources under one group as per the teams is best practice.

Upi group

2 VM, 3 DB

Transaction group

10 vm, 5 DB, 4 EKS

Payments group

(5 vm, 2 DB, 3 EKS)

Azure Resource Group

If your organization is using only one azure account then the best practice is to use the resource groups

Payment\_prod, payments\_QA, payments\_dev, etc. in this way we can track and manage the resources usage, configuration, security, access, network, etc for the resources belonging to that particular group.

One resource can go to one resource group only. Grouping can be done by project name and also environment name.

**Azure Networking:**

**3 Tier Architecture**:

The 3 tier architecture has front end applications, back end applications and Database.

**2 Tier Architecture**:

A 2 tier architecture has front end and back end applications only.

Database subnet

NSG

Bussiness logic App subnet

NSG

Azure Load Balancer

Web App subnet

NSG

8.8.8.8

App Gateway subnet

Azure DNS

Azure

Firewall



DNS

ISP

User



* Here the Virtual Network (Vnet) range is decided based on the resources we use in that Vnet by using the CIDR.
* The Vnet is split inton multiple subnets like application gateway subnet, Web application subnet, Business app subnet, Database subnet.
* The application copies are deployed in multiple availability zones of the same region so that is one zone goes down the other will work without interruption.
* The users request to a domain like google will go through our home wifi to the ISP where it has the DNS records and the domain name will resolved into the IP address of the google.
* It will enter the Vnet through the Firewall.

**Firewall:**

It will restrict the unauthorized entry into the Vnet.

* The IP address of the google is the IP address of the Load Balancer in the Application Gateway.
* The load balancer will decides the request path to the web application based on the traffic and also the health of the application. It will decide where to send and how many requests to be sent to that particular Web application.
* The Azure DNS resolves the domain name to the IP of the Load Balancer.

**App Gateway Load Balancer:**

It is a L7 layer Load balancer where the requests are distributed based on the http url of the request. Ex: google/login, google/logout. The routing is based on the url of the request.

**Azure Load Balancer:**

The routing is based on the L4 layer load balancing. Where the app gateway routing will determine the backend application load balancer routes.

* The App gateway load balancer will send the request based on the http url of the web application.
* The web application request to the backend application is also determined by the Azure Load balancer.
* Each Subnet will have a NSG so that the request will be checked before accessing the applications inside the subnet.

**Virtual Network Peering:**

To establish a communication between two Vnet we need the Vnet peering where we modify the route tables of the Vnets and allow the communication requests between the two Vnets. But for this we need the administration access to both the Vnets.

**VNet Gateway:**

It is similar to the VNet Peering.

**VPN Gateway:**

We can establish a communication between your organizational network and azure cloud network. This is mostly used in the Hybrid cloud where the requests from your organizational private cloud have to communicate with the azure cloud database or instances, etc.

**Demo Project:**