**Azure Cloud**

Microsoft Azure is a service that provides cloud computing for building, managing, deploying and testing applications and services.

There are usually three models of cloud services

**1. Software as a Service (SaaS)**

**2. Platform as a Service (PaaS)**

**3. Infrastructure as a Service (IaaS)**

**1. Software as a Service (SaaS) -** software that’s available via a third-party over the internet.

**2. Platform as a Service (PaaS) -** PaaS is a complete development and deployment environment in the cloud.

PaaS includes infrastructure—servers, storage and networking—but also middleware, development tools, business intelligence (BI) services, database management systems and more.

PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing and updating.

PaaS is an environment in which developers can create different applications. It supports many program languages, and it provides the hardware so users can develop and test applications.

The advantage is that it is a complete environment, which lets developers jump into the action by giving them all that they need, including testing tools. It is secure too.

**3. Infrastructure as a Service (IaaS) -** cloud-based services, pay-as-you-go for services such as storage, networking, and virtualization.

SaaS examples: Big Commerce, Google Apps, Salesforce, Dropbox, MailChimp, ZenDesk, DocuSign, Slack, Hubspot.

PaaS examples: AWS Elastic Beanstalk, Heroku, Windows Azure (mostly used as PaaS), Force.com, OpenShift, Apache Stratos, Magento Commerce Cloud.

IaaS examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean, Magento 1 Enterprise Edition\*.

**Regions, Geography and Availability Zones:**

Availability Zones is a high-availability offering that protects your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

**VNet**- Azure Virtual Network (VNet) is the fundamental building block for our private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in our own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

**Subnets**- Subnets enable you to segment the virtual network into one or more sub-networks and allocate a portion of the virtual network's address space to each subnet. You can then deploy Azure resources in a specific subnet. Just like in a traditional network, subnets allow you to segment your VNet address space into segments that are appropriate for the organization's internal network. This also improves address allocation efficiency. You can secure resources within subnets using Network Security Groups.

Subnet is a range of IP addresses in the VNet, you can divide a VNet into multiple subnets for organization and security.

**Network Interface:**

A network interface enables an Azure virtual machine to communicate with internet, Azure, and on-premises resources. A VM can have one or more network interfaces.

A Network Interface (NIC) is an interconnection between a Virtual Machine and the underlying software network. An Azure Virtual Machine (VM) has one or more network interfaces (NIC) attached to it. Any NIC can have one or more static or dynamic public and private IP addresses assigned to it.

**VNet Peering:**

We can connect virtual networks to each other with virtual network peering. These virtual networks can be in the same region or different regions (also known as Global VNet peering).

Once peered, the VNets appear as one, for connectivity purposes. The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same VNet, through *private* IP addresses only. No public internet is involved. You can peer VNets across Azure regions, too – all with a single click in the Azure Portal.

Azure supports the following types of peering:

* Virtual network peering: Connect virtual networks within the **same Azure region.**
* Global virtual network peering: Connecting virtual networks **across Azure regions.**

**The benefits of using virtual network peering:**

* A low-latency, high-bandwidth connection between resources in different virtual networks.
* The ability for resources in one virtual network to communicate with resources in a different virtual network.
* The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
* The ability to peer virtual networks created through the Azure Resource Manager.

**VPN Gateway:**

A VPN gateway is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public Internet.

We can also use a VPN gateway to send encrypted traffic between Azure virtual networks over the Microsoft network. Each virtual network can have only one VPN gateway. However, you can create multiple connections to the same VPN gateway. When we create multiple connections to the same VPN gateway, all VPN tunnels share the available gateway bandwidth.

**Azure Storage:**

Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers a massively scalable object store for data objects, a file system service for the cloud, a messaging store for reliable messaging, and a NoSQL store.Azure Storage includes these data services:

* [Azure Blobs](https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction): A massively scalable object store for text and binary data.
* [Azure Files](https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction): Managed file shares for cloud or on-premises deployments.
* [Azure Queues](https://docs.microsoft.com/en-us/azure/storage/queues/storage-queues-introduction): A messaging store for reliable messaging between application components.
* [Azure Tables](https://docs.microsoft.com/en-us/azure/storage/tables/table-storage-overview): A NoSQL store for schemaless storage of structured data.

**Virtual Machine:**

A virtual machine is a computer file, typically called an image that behaves like an actual computer. It is creating a computer within a computer.

This gives us a flexibility that can run multiple machines in a physical computer.

It can be used for various ways like,

* Development and Test
* Applications in the Cloud
* Extended Datacenter

**Application Security Group (ASG):**

Application Security Groups helps to manage the security of Virtual Machines by grouping them according the applications that runs on them. It is a feature that allows the application-centric use of Network Security Groups.

ASGs are used within a NSG to apply a network security rule to a specific workload or group of VMs — defined by ASG worked as being the “network object” & explicit IP addresses are added to this object. This provides the capability to group VMs into associated groups or workloads, simplifying the NSG rule definition process.

* All network interfaces used in an ASG must be within the same VNet
* If ASGs are used in the source and destination, they must be within the same VNet.

**Network Security Group (NSG):**

A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).

When an NSG is associated to a subnet, the rules apply to all resources connected to the subnet. Traffic can further be restricted by also associating an NSG to a VM or NIC.

NSG’s control access by permitting or denying network traffic in a number of ways, whether it be:-

* Communication between different workloads on a vNET
* Network connectivity from on-site environment into Azure
* Direct internet connection

**Load Balancer:**

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

An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. A load balancer health probe monitors a given port on each VM and only distributes traffic to an operational VM.

Virtual machines connect to a load balancer using their virtual network interface card (NIC). To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer.

There are mainly 3 load balancing components available in Azure.

* Azure Load Balancer
* Azure Application Gateway
* Azure Traffic Manager

## Azure Load Balancer

Azure Load Balancer is a Load Balancer in a more classical sense as it can be used balancing load for VMs in the same way we were using traditional load balancers with our on-premise servers. Now since Azure load balancer is designed for cloud applications it can also be used to balance load to containers and PaaS applications along with VMs.

Azure Load Balancer can be used in two configuration modes:

* **External —** Public load balancing
* **Internal —** Internal load balancing

### **External — Public Load Balancing**

In this mode, load balancer is assigned a public IP address to ensure that the load balancer can accept requests coming in from the internet. The load balancer will get called from the internet by the client applications and services, and then based on the configured rules it will distribute the incoming traffic over VMs, containers, or apps.

### **Internal — Internal Load Balancing**

The internal Load Balancer is essentially the same as external, but it uses a private IP address and thus it can be called only from the applications within the virtual network to which it is attached.

## Azure Application Gateway

Azure Application Gateway is a level 7 load balancer and thus it has access to application and session payload which makes it possible for the application gateway to provide much more feature-packed load balancing like sticky sessions, connection affinity, etc. Since application gateways have more information compared to the Azure load balancer, more complex routing and load balancing can be configured. Application gateway acts as a reverse proxy service. It terminates the client connection and forwards request to back endpoints.

## Azure Traffic Manager

Traffic Manager uses DNS to redirect requests to an appropriate geographical location endpoint. Traffic Manager does not see the traffic passing between the client and the service. It simply redirects the request based on most appropriate endpoints. Geographical location endpoints are internet facing reachable public URLs.

Azure Traffic Manager works at the DNS level, i.e. it distributes the load over multiple regions and data centers using the rules configured at the DNS level. The client makes a DNS request and, based on the location of the DNS, Azure Traffic Manager will find the nearest region and sends that back to the client via a DNS response.

**Virtual Machine Scale Set:**

Azure virtual machine scale sets let us create and manage a group of identical, load balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to our applications, and allow us to centrally manage, configure, and update a large number of VMs. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

## Availability set

An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.

When two or more servers are in a single availability set, even if one or more of servers becomes unavailable due to any reason, rest of servers in an Availability set will provide the service.