Azure

Describe cloud Concepts (25-30%) =====================================

1. Describe Cloud Computing

2. Describe Benefits using Cloud Services ----------------------------------------

-- HA, FT, DR

-- **Fault Tolerance**:

* Continue to operate in the event of component failures.
* It ***does not provide*** the same level of failover and business continuity capabilities.
* Changing/Shifting VMs if any disaster occurs.
* Both the VMs sync simultaneously.
* Here there is no interruption or downtime but costly.

-- **High Availability**:

* If the VM goes with any wrong or component stopped working, the user will be redirected to the new VM (few seconds of delay happened). Servers and Replicated Servers (Available if needed), here redundancy is done.
* HA ***protects against data center, server, and network and storage subsystem failures*** to ***keep your business running without downtime***.
* They are also ***resilient, meaning that they can simply handle*** ***failure*** ***without service disruption or data loss***, and seamlessly recover from such failure. Azure provides
* HA features such as ***redundancy***, ***load balancing, auto-scaling*** and provisioning across ***Availability Zones (AZ)***, representing ***isolated parts of an Azure data center.***
* In a year, downtime as per SLA is ***3 seconds***.
* ***No Downtime***

-- **Disaster Recovery**: If any disaster occurs, application will be changed to other location in seconds.

-- **Reliability**: The ability of a system to recover from failuresar and continue to function. It may have minimal downtime.

-- **Scalability**:

* Scalable architectures provide the ability to grow your environment when this is needed (increase in number of users, traffic throughput).
* Example - Workload increased as business expanded over a period of time.
* Two types of Scalability - Horizontal and Vertical.
* Vertical Scalability - Increasing a capacity of current server- a larger hard drive, a faster CPU, More RAM, CPU, I/O, or networking capabilities. Here there's a limit over that we cannot add or increase.
* Horizontal Scalability - Deploying multiple instances of application/db. Here we are increasing VMs instead of components. Here there's no limit, we can increase multiple VMs. Horizontal Scalability needs additional infrastructure like Load Balancers, Auto Scaling, Group etc.

-- **Elasticity**: Ability to ***automatically expand*** or compress the infrastructural resources on a ***sudden-up and down*** in the requirement so that the workload can be managed efficiently. For example - Workload increases during festive season like Christmas.

-- **Agility**: *Rapidly deploy and config*ure cloud resources as your app's needs change. Speed and flexibility of scaling in the cloud.

-- **Azure Site Recovery** –

* Ensure business continuity by orchestrating the failover of apps and ***workloads to a secondary location*** during outages.
* It helps maintain productivity and minimize downtime by keeping critical services running in the event of a disaster at the primary site.
* Specifically designed for ***orchestrating failover during outages***.

**-- Azure Site Recovery (ASR) vs Fault Tolerance (FT) –**

* ASR - ***Disaster recovery and business continuity***, FT - ***High availability*** and resilience against ***hardware failures***.
* ASR - ***Replicates*** workloads to a secondary region or site, FT - Uses ***redundancy across VMs***, zones, and regions.
* Think of **ASR** as your ***emergency evacuation plan*** (replicate and recover), while **fault tolerance** is your ***fireproof building design*** (resilient and self-healing).

-- **Capital Expenditure (CapEx)**: Upfront cost. Spending money ahead on physical infrastructure and then deducting that cost over time from your tax bill. Ex - Deploying your own data center, server, storage, network, backup and archive, disaster recovery, datacenter infrastructure. CapEx requires significant up-front financial costs as well as ongoing maintenance and support expenditures.

-- **Operational Expenditure (OpEx)**: pay-as-you-go pricing. There is no up-front cost, as you pay for a service or product as you use it. OpEx is a consumption-based model, so company is only responsible for the cost of the computing resources that it uses.

3. Describe cloud service types -----------------------------------------------

-- Computing Models: IaaS, PaaS, and SaaS.

-- **SaaS**: Bus. You need to pay and configure the solution only rests will providers do. You - use only. Example - Outlook email, Calendar, Office 365.

-- **PaaS**: Taxi/Uber. You need to pay and check the location only. Rests Other will do. You - Only development and Data. Minimize the administrative effort. Example - Azure App Service, Azure SQL Databases, Azure Cosmos DB, Azure Synapse Analytics.

-- **IaaS**: Rented Car. You will provide something and rests are provided by providers. Car is not mine, means infrastructure is not mine. You - Development, Data Runtime, Middleware, OS. The most suited to a lift and shift migration from an on-premises datacenter to a cloud deployment. You can control "Operating System" only in IaaS computing model. If you need to install some software, prerequisite applications or services. Example - Azure Virtual Machine.

-- On-premises : Your own car. You are responsible for every things.

-- On-Premises > IaaS > PaaS > SaaS (Customer responsibility)

-- Shared Responsibility Model : Responsibilities shared between you and providers (cloud) in the Computing Models. Always your responsibility in all - Information and data, Devices (Mobile and PCs), Accounts and Identities. PaaS has the largest shared between both. No share in On-Premises.

-- Deployment Models : Public, Private, Hybrid.

-- **Public Cloud**: Cloud resources are those that are owned and managed by a third-party cloud service provider and are provided through the Internet. Advantages - No maintenance, Near unlimited scalability, High Reliability. Disadvantages - Less control. Examples - Deploy website quickly, focus on development.

-- **Private Cloud**: Cloud services that are utilized by a particular organization and are not accessible to the general public. Advantages - No legal obligation, control, strict security and compliance. Disadvantages - Infrastructure cost, difficult to elasticity, IT Skills. Examples - Government policy requires specific data to be kept in-country.

-- **Hybrid Cloud**: Combination of public and private cloud with automation and orchestration between the two. Advantages - Use your own equipment to meet security, compliance, or legacy scenarios. Disadvantages - Expensive, Complicated. Examples - Medial data can't expose to public. Application runs on old hardware.

-- **Cloud Pricing Model**: Free, Time, Data, Operations, Execution, Other metrics, Other Parameters.

Always Free - virtual Network, Azure Policy, Azure Active Directory, ***Azure Migrate***, Azure Open Datasets, Azure Lighthouse, Azure Private Link, Azure Data Catalog, Azure Service Fabric.

Pay for the Time - VMs (per second), App Services, SQL Database, Load Balancer.

Pay based on Data - Database Storage, Storage Service, Network traffic (between regions).

Pay based on Operations - Storage services (read, write, delete operations), Cosmos DB.

Pay based on Execution - Serverless offerings. Azure Function, Serverless Database, Logic Apps.

Other metrics - Premium Tier. Charge based on number of user licenses.

Other Parameters - Regions/Location, How you purchase service (through Enterprise Agreement, from web, from cloud Solution Provider), Support options, Programs and offers, and so on....

Describe Azure architecture and services (35–40%) ===============

1. Describe the core architectural components of Azure --------------------------

-- Region : Which is a physical location around the world where we cluster data centers. How to choose regions ? - Compliance, Proximity, Available services, Pricing. Each Regions has some availability Zones and each Zone has some Data Centers. Replication is fast because two availability zones are near and not so very far. All AZ traffic is encrypted. Not every Region has AZ.

-- **Region Pairs**: Two regions are paired for ***disaster purpose*** ***within the same geography***. Automatic replication and failover for some azure services. Replicates resources across regions that are at least 300 miles away fazurerom each other.

-- **Resource Group**: Logical container for resources. It groups together resources (some or all as you wish). We can create RG seperately also. RG only stores metadata and so it does not depend on Region(s). We can create RG based on usage, type, location, ets. Each resource can exist in only one RG. You can move a resource from one RG to another. RG can't be nested. Ther resources in a RG can be located in different regions than the RG. RG is created at location - to store metadata. A RG can be used to scope access control for administrative actions. To manage a RG, you can assign Azure Policies, Azure Roles, or resource locks.

* You can apply locks to a resource group or subscription to prevent deletion or make contained resources read-only.
* You can also apply locks directly to a resource. You can apply tags to a RG. The resource in the RG don't inherit those tags.
* Life cycle - then you delete a RG, all resources in the group are also deleted. To create a RG, you can use the Portal, PowerShell, Azure CLI, or an ARM template.
* What happens to the resources within a resource group when an action or setting at the Resource Group level is applied? - The setting is applied to current and future resources.
* Any resource, at the same time, can only be in the same RG and not shared.

-- **Hierarchy**:

1. Management Groups (Organization)
2. Subscriptions (Environments - dev/test/staging)
3. RGs (group resources)
4. Resources.

-- **Azure Resource Manager (ARM)**: Using Export template, we can create **JSON** file and use this template to deploy any environment.

* Here we *don't need to move one-by-one file from staging to production or moving from one RG to another RG*.
* ARM ***automates resource deployments*** (create, update, and delete) using template.
* ARM template is a ***JSON*** file that defines what you want to deploy to Azure. Integrates with Azure portal, PowerShell, CLI, and REST API to perform deployment and management tasks.
* Easy way to *deploy multiple resource instances or reliably redeploy resources*. AR template can be used to deploy the resources consistently and repeatedly.
* *ARM templates define the* ***dependencies*** *between resources so they're deployed in the* ***correct order***.
* Whenever, we create/configure any resources that is transferred to the ARM where it creates a template with the provided information and dependencies and creates/configure the same using that Template JSON file.
* Resources from various resource groups may interact with each other.
* ***ARM templates and Bicep*** *are two examples of using* ***infrastructure as code*** *with* ***the Azure Resource Manager*** *to maintain your environment*. **Bicep** files provide a more user-friendly and concise way to define Azure resources compared to the JSON format used in **ARM templates**. The Bicep language offers a cleaner syntax that is easier to read and write, making it simpler for developers and operators to work with Azure resources efficiently.

-- **Azure Blueprints** –

* It is a ***repeatable set of governance tools*** that helps development teams ***quickly build and create new environments while adhering to organizational compliance*** to speed up development and ***deployment***.
* What permissions required to delete the Blueprints –

1. $> Blueprints/version/delete -- Un-assign then
2. $> Blueprints/artifacts/delete -- ready then
3. $> Blueprints/delete -- lastly delete.

**-- Azure Subscription**: How you are billed for resource usage. AS is required to select while creating any resource anywhere. It defines two things - Billing and Access. You can create multiple AS for different purposes - Environment, Organizational structures (IT, HR, Admin, etc), Billing (production, Test, Dev). Using Azure requires as Azure Subscription, without Subscription, nothing can be done. An AS is a logical unit of Azure services that links to an Azure account. It also allows you to provision resources. It provides you with authenticated and authorized access to Azure products and services. Azure generates separate billing reports and invoices for each subscription. Different types - Free, Pay-Per-Use, Enterprise, Student.

-- **Management Groups**:

* ***Organize multiple subscriptions as a single management entity***.
* ***Any conditions applied to a MG apply to all subscriptions contained in that MG object***.
* Each MG and subscription can support ***only one parent*** - means a subscription can have only one parent MG.
* Each MG can have ***many children*** - means a MG can have many Subscriptions.
* The Root MG can't be moved or deleted, unlike other MGs.
* Azure Management Groups provide c***entralized management for access, policy, and compliance across multiple subscriptions***.

-- **Azure Sovereign Regions**: Completely new and different from other Regions - specific regions of azure that were created to meet high security and other regulatory and compliance requirements for specific market. Examples - Azure Government (only for US government), Azure China (only for China government). These regions datacenters are completely separate because of high security and Government data. These are operated directly by Microsoft. These are not publicly use.

2. Describe Azure compute and networking services -------------------------------------

-- **Compute**: Azure VM, App Service, Container Instances, Kubernetes Service, Functions, Virtual Desktop.

-- **Virtual Machine**: Important options to choose - Type of image (OS, Software), Size of VM (CPU, RAM, Storage), Availability options. Uses - During testing and deployment, to handle fluctuations in demand, During disaster recovery, Move to the cloud with VMs. When you create a VM, some other resources are automatically created - Public IP address, Network security group, Network interface, Disk, Virtual network.

-- **Deploy Webpage on VM**: RDP the VM --> Open Server Manager --> Under Default (Dashboard) click "Add roles and features" and then Next --> Select Web Server IIS and then Next --> Finally install. After installation, click on Tool (top right header) and click on IIS Manager, it will open IIS Manger. Default root of IIS folder is C/inetpub/wwwroot.

-- **VM Load Balancer**: Deliver high availability and network performance to your apps. It distributes traffics to other VMs. It does two things - Distribute traffic (High Availability) and Check health of VMs (Network Performance). Whenever it will find VM unhealthy, it will not send request to that VM. LB - Public and Private (Internal). Components - Frontend IP which defines IP address for the LB, Backend pool which contains the VMs, Health probes which monitor health of resources in backend pool, Rules that how to distribute the incoming traffic. Frontend IP is the public IP address which is assigned to LB and exposed to user for using, here users access this IP address instead of VM IP Address. Backend pool is the area where all the VMs are added so here LB distributes the traffic in all the VMs of Backend pool.

-- **Availability Sets**: make use of two key concepts - Fault Domains, and Update Domains.

* Update domains define the ***group of VMs that are going to be patched/maintained/rebooted at the same time***.
* Fault domains define the ***group of VMs that share a common power source and network switch***.
* It save from rack-wide failure, or rack-wide maintenance window that can take down all VMs hosted on this signal point of failure.
* Availability sets are free to use! You only pay for the VMs being created.
* It ***does not protect your application from operating system or application-specific failures***, it downs limit the impact of potential physical hardware failures, network outages, or power interruptions.

-- **VM Scale Sets**:

* ***Create and manage a group of load balanced VMs***.
* Allows your application to ***automatically scale*** as resource demand changes - the number of VM instances can ***automatically increase or decrease in response to demand or a defined schedule***.
* All VM instances are created from the ***same base OS image and configuration - size, disk, configuration, and application***.
* Provides high availability and application resiliency.
* There is no cost for the scale set itself, you only pay for each VM instance that you create.

-- **Azure File Sync:** Azure File Sync is a service that ***syncs files between on-premises servers and Azure*** File Shares.

-- **Azure Data Factory:** Azure Data Factory is a cloud-based data integration service that allows users to ***create, schedule, and manage data pipelines***.

-- **Azure App Service**:

* Allows developers to ***build, deploy, and scale web applications and APIs***.
* Enables you to host and manage your web applications. This is PaaS environment so - Focus on the business value and logic, Azure handles the infrastructure, Automatic scaling and high availability.
* Programming language of your choice. Supports Windows and Linux.
* ***Automatic deployment from GitHub or Azure DevOps***. Pay only for compute resources your app uses.
* Types - Web aps, API apps, Web Jobs, Mobile apps. For Ruby and Python only Linux is available.
* Within the ***same App Service Plan***, you have ***multiple web apps***.
* ***Fully managed platform*** that allows ***hosting various types of applications***, including web applications, APIs, background tasks, and mobile apps ***without*** worrying about the ***underlying infrastructure***.

-- **Azure DevTest Labs:**

* It is a service specifically designed to ***quickly provision development and test*** environments by ***using Azure Resource Manager Quickstart Templates***.
* It allows you to ***create environments with pre-configured templates***, manage costs, and integrate with Azure services for testing and development purposes.

-- ***Containers***: A package of application+dependencies+files everything. So that after sharing to another environment, everything works perfectly.

* Azure Container Instance - Containers are deployed on ACI.
* ACI is used for less containers and for testing purposes.
* Azure Kubernetes Service is used for complex and multiple containers and production also.
* Containers are a way to ***wrap up an application into its own isolated package***. This is the modern era solution for transferring your projects to friends, family, colleagues, clients etc without worrying about their system configuration to run the project. Features - Portability, Consistency, No maintenance related to infrastructure, Deployment and maintenance are efficient, Auto scaling.
* ***VMs*** *provide a full virtualization of the hardware, including CPU, memory, storage, and network interfaces, allowing each VM to run its own operating system.* ***Containers****, on the other hand, virtualize the operating system, sharing the OS kernel among multiple containers while isolating the application processes*.

-- **Azure Container Registry (Docker)**: All images are stored here. Template --> Image --> Container --> Container Registry.

-- **Azure Kubernetes Services (AKS)**: Azure's container management system. Scale your application to meet demands by adding and removing container instances. Monitor the deployed containers and resolving any issues that may come. Groups of containers are called Pods. VMs are called Nodes. To use images, connect with Azure Container Registry. AKS is integrated with Azure Monitor in order to monitor the performance in health of your cluster.

-- **Docker**: A docker container is a standard that describes the format of containers and provides a runtime for Docker containers. Docker is an open source project that automates and evolves the technology, and they work in collaboration with cloud vendors like Microsoft. The result from adopting Docker, or container, is that application can be deployed or un-deployed faster, start and stop faster, change to another "image" faster, process and do many things faster. Apps run the same, regardless of where they're run - any machine, No compatibility issues, Predictable behavior, works with any language, any OS, any technology.

-- **Windows Virtual Desktop**: Like VDI. It is connected with url and from any device - Windows, iOS, Mac. It supports Windows 10 multi-session. It has Host pools which can allocate users to sets of VMs. Scale the VMs up and down. Secure - Authentication using Azure AD, Azure Multi-factor Authentication, Role-based access controls (RBACs) to users, No confidential data on personal device, User sessions are isolated in both single and multi-session environments.

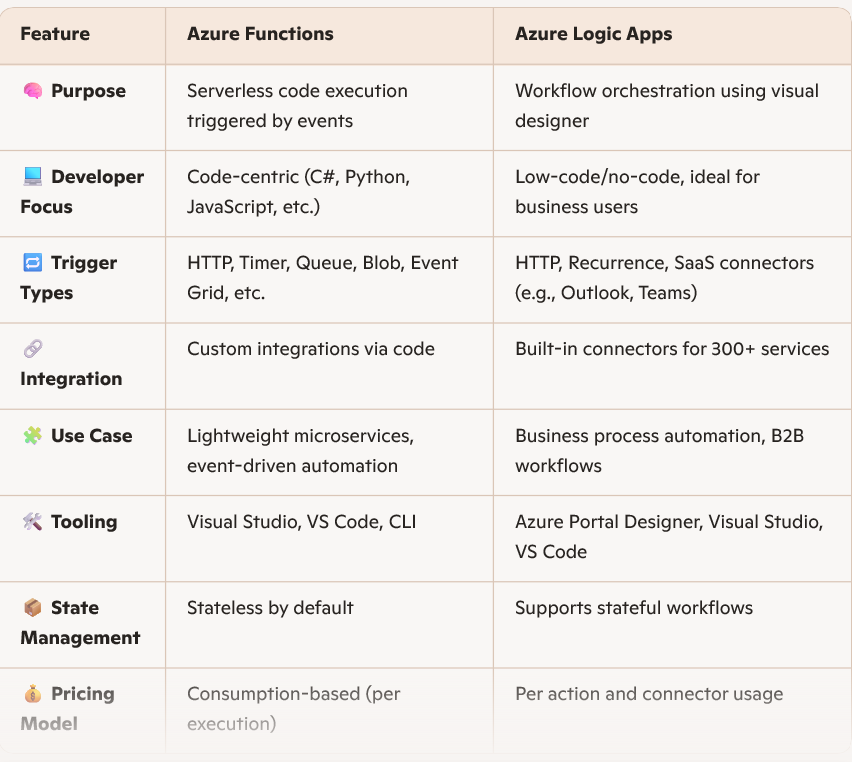
-- **Route-based VPN gateway**: If you need connections between virtual networks, point-to-site connections, multisite connections, or coexistence with an Azure ExpressRoute gateway, which type of VPN gateway should you use?

-- **Azure Functions:**

* It is a ***Serverless*** platform.
* Execute your code when needed.
* ***Event-driven solution*** - execution of your code is triggered by a specific type of event. Pay only for the time spent running your code.
* Azure Functions can be triggered by various event types, including HTTP, request. Functions scale automatically based on demand.
* Functions can be either stateless or stateful.
* Use cases - Process file uploads, Build a web API, Respond to database changes.

-- **Azure Logic Apps**: Designed to ***automate business scenarios***.

* ***Logic apps execute workflows***.
* ***Workflow*** includes actions like ***data conversions*** and ***flow controls***, such as ***conditional statements***, ***switch statements***, ***loops*** and ***branching***.
* Design using visual designer on the Azure portal or in Visual Studio.
* Build from predefined logic blocks. More than 200 different connectors and processing blocks to interact with different services.
* Starts with a trigger.
* ***Two types-Standard and Consumption***. ***Standard*** based LA choose when wants your logic apps ***always up and running***. ***Consumption*** based when you want for a ***particular task***.
* This is designer based where we can set value (***schedule***) like date etc. after/at which resource to be deleted/other purpose.



**Networking: ------------------------------------------------------------------**

-- **Azure Virtual Network (VNet):** Your own ***isolated network*** in Azure.

* Region can have multiple VNets but each VNet belong to same Region.
* Within a VNet, ***network traffic is isolated (not visible)*** from network traffic in all other Azure VNet. Y
* You maintain ***complete control over all traffic entering and leaving a VNet***.
* Region has VNet and VNet has all the Resources. VNet is assigned a range of IP Address called CIDR Range. Each IP Address defines the address of that resource, hence anyone wants to communicate with that resource it needs that IP Address. The number of resources cannot go beyond the number of IPs.
* ***Whenever you create multiple VNets under Region***, they will ***not communicate each other by default***.
* You can add more VNets or more addresses on existing VNet.

-- **Network Security Groups (NSGs):**

* Used to ***control inbound and outbound traffic*** to network interfaces, VMs, and subnets.
* You can ***allow or deny traffic to specific ports, such as ports 80 and 443***, to ensure that your web application is accessible from the internet while maintaining security.
* NSG ***uses inbound and outbound rules to filter network traffic*** to and from Azure resources connected to Azure Virtual Networks.
* ***Azure Firewall*** provides network ***traffic filtering across multiple Azure subscriptions*** and VNets. Whereas, ***NSG is used for single Subscription***.

-- **VNet Subnets**: Group resources within VNet. Each kind of resource has distinct access requirements. Elastic Load Balancers that are publicly available are accessible through the internet (public resources). Databases and App Server instances should be inaccessible from the internet.

* Only apps running inside your VNet should be able to access them (private resources). How do you partition public and private resources inside a Virtual Network? - That is through Subnets.
* Organize and group resources on subnets. Separate public and private resources into distinct subnets.
* Resources in a public subnet can be accessed from internet.
* Resources in a private subnet cannot be accessed from internet, but resources in a public subnet can connect with resources in a private subnet.
* We can use ***network security groups*** to secure individual subnets.

-- **VNet Peering**:

* *Connect VNets from same or different regions* (Global VNet peering).
* Secure communication between VNets.
* Low Latency
* High bandwidth connections.
* Must not have CIDRs that overlap (OP address range).
* The network traffic between peered VNets remains ***private and secure***, ***traveling*** ***exclusively on the Microsoft backbone network***.
* This ensures that the communication between the resources ***does not traverse the public internet,*** enhancing security and privacy.
* *When you create a Virtual Network (VNet) with* ***multiple subnets*** *in Azure, by default, there are no network security group (NSG) rules or other restrictions preventing communication between VMs in different subnets within the same VNet. Therefore, VMs in* ***one subnet******can communicate with resources in******another subnet******by default****, as long as there are no explicit NSG rules or other configurations that block this traffic*.

-- **VPN (Virtual Private Network):**

* VPN is used to connect On-premises and Azure VNet. All transferred data is encrypted in a private tunnel as it crosses the internet.
* Site-to-Sit connection, Point-to-Site connection, Multi-Site connection and Network-to-Network connection.
* VNet1 >> VPN Gateway >> Tunnel << VPN Gateway << VNet2.
* VPN Gateway needs to be installed at the VNet to connect with Tunnel on both sides. Two ways to connect two VNets – VNet (Network) Peering and VPN Gateway Tunnel.
* VPN Gateway provides low bandwidth connection and hence due to this VNet Peering used mostly.

-- **Application Gateway**:

* *Load Balancer uses IP address/port to distribute traffic. But how to distribute with other parameters - like I want any image will go to the Image VM for image processing and any Video will go to the Video VM for video processing*?? Application Gateway provides HTTP based load balancing.
* Routing rules based on HTTP request parameters - URI path (web address), Host headers (request data).
* Provides auto-scaling, end-to-end encryption, zone redundancy and multi-site hosting.

-- **CDN (Content Delivery Network):** Edge location, Datacenter location and Network.

* To reduce latency, CDNs cache content on edge servers near end users.
* Reducing traffic to the original server. This is also called as POP (Point of Presence).

-- **ExpressRoute**: Fast, reliable, and *private connection to Azure with On-Premises*.

* With ***VPN Gateway*** - Data travel over the Internet, Data is Encrypted, Slow connection, High Latency and use for light traffic. So, ***Express Route*** - Use a private, dedicated connection, Data do not go over the public Internet, Data is not Encrypted, Low Latency, Faster connection, and use for High traffic (peta bytes, Giga bytes, Tera Bytes).
* The setup and configuration for ExpressRoute is more complex, and will require collaboration with the connectivity provider, there are connectivity provider companies in the market which help in this.
* Uses - Large-scale, mission-critical workloads requiring scalability and resilience are suitable for this architecture.

-- **Azure DNS (Domain Name System):** It has name and IP address mapped. Domains can be hosted in Azure DNS for record management. Billing = no of DNS Zone + no of DNS queries received.

-- **Azure Service Endpoints**: Provides secure and direct connectivity to Azure services. Use optimized route over the Azure backbone network. You can access Azure service to only your VNets. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet. Server needs to install Azure Storage Explorer. We can restrict connection with the VM so that other devices could not access.

-- **Private Endpoints**: A network interface that uses a private IP address from your virtual network.

* This network interface connects you privately and securely to a service that's powered by Azure Private Link.
* **Service Endpoint** will continue to be a publicly routable IP address. Private Endpoint is a private IP in the address space of the virtual network where the private endpoint is configured. Both are used to connect Azure services.
* Private Link has a built-in data protection system, but Service Endpoint - for exfiltration protection, traffic must pass through an NVA/Firewall. Both are not available for all resources/services.

-- **Azure Private Link:**

* Allows companies to ***securely connect their Azure PaaS services to their Virtual Network (VNet)*** using private endpoints.
* This ***ensures*** that the data flow between services like Azure Storage, Azure Cosmos DB, and Azure SQL Database and the VNet is ***isolated*** from the public internet, ***enhancing security and privacy***.

-- **VPN Gateway**: A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed to a dedicated subnet of a virtual network. You can use them to connect on-premises datacenters to virtual networks through a *Site-to-Site (S2S) VPN connection*.

-- **Site-to-Site VPN** connection is used to establish a secure, encrypted connection between an ***on-premises VPN device or gateway and an Azure VPN gateway*** in a virtual network ***over the internet***. This type of VPN connection allows for secure communication between the on-premises network and the Azure virtual network.

* ***ExpressRoute*** also connects the same with secure and encrypted but this is dedicated and ***not exposed to internet***.

3. Describe Azure storage services -------------------------------------------------

**-- Storage Service**: Table, Queue, File, Blob (Containers), Disk. These all services are kept under Azure Storage Account. Features - Durable and HA, Redundancy across datacenters or regions, Secure - by default all data encrypted, Scalable-massively scalable, Managed, Accessible from anywhere in the world over HTTP(S).

-- **Premium storage accounts** in Azure ***support multiple types of storage***, including Blob Storage, Data Lake Storage, Premium file shares, and Premium page blobs.

-- **Azure Storage Explorer –**

* Allows users to ***manage files and blobs*** in Azure Storage using a ***graphical interface.***
* Compatible with Windows, macOS, and Linux operating systems.

-- **Blobs (Binary Large Objects):** *Text and binary data*.

* Any type or format - Text, Images, audio, video, excel, backup files.
* Use cases - ***Shared access, video and audio streaming, analysis (data lake), log file***.
* Flat structure - account --> Container --> Blob, here a container cannot be created inside the container and blob cannot be created inside the blob. Within container, you can only upload files, there's no option to create container etc.
* Provides a unique namespace - http://mystorageaccount.blob.core.windows.net. Three types.

1. **Block blobs** - large objects like media files or image files for websites.
2. **Append Blobs** - Optimized for append operations like Logs. When you modify an append blob, blocks are added to the end of the blob only. Updating or deleting of existing blocks is not supported.
3. **Page Blobs** - Optimized for random read and write operations. Provide durable disks for Azure Virtual Machines (Azure VMs).

* Azure Blob Storage ***allows users to change the access tiers of an object at any point in time***. This flexibility enables users to optimize storage costs and performance based on their current needs.

-- **File Storage**: ***Managed files shares*** (SMB Protocol).

* *This Storage is shared with multiple VMs*. Hence this is a common storage for VMs.
* This is managed service, we don't need to maintain anything. It Enables you to create files shares in the cloud, and access these file shares from anywhere with an internet connection.
* Mounted concurrently by cloud or on-premises deployments.
* Accessible from Windows, Linux, and mac OS clients. Accessible ***Server Message Block (SMB) protocol*** or ***Network File System (NFS) protocol***. Azure Files ensures the data is encrypted at rest, and the SMB protocol ensures the data is encrypted in transit.
* Use Cases - Replace or supplement on-premises file servers, Share application settings, Dev/Test/Debug. Benefits - *Shared access, Fully managed, Resiliency* as you don't have to deal with local power and network issues.
* Azure Files offers *fully managed file shares in the cloud with shares* that are accessible by using *Server Message Block (SMB) protocol*. Mounting Azure file shares is just like connecting to shares on a local network.

-- **Queue Storage**: Messaging. ***Stores large numbers of messages***. Access messages via authenticated calls using HTTP or HTTPS. May contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously. It works as a buffer storage where messages are dequeened.

-- **Table Storage**: NoSQL store. Also Cosmos DB. NoSQL key-value Storage. Items are referred to as rows, and fields are known as columns. Semi-structured db. All rows in a table must have a key. No concept of relationships, stored procedures, secondary indexes, or foreign keys. Data will usually be denormalized. To help ensure fast access, Azure Table Storage splits a table into partitions. Support very large volume of Data. Uses - Event logging and performance monitoring data.

-- **Disk Storage**: The storage which are linked with the VM for OS, or any data. High-performance, highly durable block storage for Azure VMs. While creating VM, one Disk is by default attached for OS. You can create and attach new/existing disk with the VMs.

-- **Storage Data Redundancy**: (Region 🡪 Availability Zone 🡪 Datacenter)

* Protect your data from hardware **failures**, network or power outage, and natural disasters. There are four types of it.

1. **Locally redundant storage (LRS) (**Datacenter**)** - Three synchronous copies in same data center, in case of ***single datacenter goes down***.
2. **Zone-redundant storage (ZRS) (**Availability Zones in a Single Region**)** - Three synchronous copies in three availability zones (AZs), in case the ***complete Availability Zone is failure/down***.
3. **Geo-redundant storage (GRS) (**Secondary Region**)** - LRS + Asynchronous copy to secondary region (three more copies using LRS), Read only access - in case of the whole Region goes down.
4. **Geo-zone-redundant storage (GZRS) (**More Copies**)** - ZRS + Asynchronous copy to secondary region (three more copies using LRS) - Read only access. With GRS or GZRS, the data in the secondary region isn't available for read or write access unless there is a failover to the secondary region.

* Zone-Redundant Storage (ZRS) *replicates data across multiple availability zones within a single region*.
* Geo-Redundant Storage (GRS) *replicates data to a secondary region*.
* Read-Access Geo-Redundant Storage (RA-GRS) *replicates data to a secondary region and provides read access to the data in the secondary region*.
* Locally Redundant Storage (LRS) *replicates data within a single data center in a region.*
* *Every Azure region has multiple datacenters*.

-- **Storage Access Tiers**: Data stored in the cloud can be different based on how it's generated, processed, and accessed over its lifetime. Blob access tiers - Hot, Cool, Archive. Tier can be changed later also using Change tier option however, you can change one file at a time, you cannot change the tier for all/some files at a time - means one-by-one.

* **Hot** - Frequently accessed data, ***low latency, higher access cost***.
* **Cool** - Infrequent accessed data like invoices for customers. ***High latency, lower cost***, stored for at least 30 days.
* **Archive** - Rarely accessed data like long-term backups. ***Highest access times and access cost***, Latency in hours, stored for at least 180 days. Use Case - Business policy mandated Data Archiving, long term retention like healthcare data. The ***Archive storage tier*** ***stores data offline*** and offers the lowest storage costs, but also the highest costs to rehydrate and access data. The ***Hot storage*** tier is optimized for storing data that is accessed frequently.
* ***Hot, cool and cold*** access tiers can be set at the ***account level*** in Azure Blob Storage. However, the ***archive access tier is not available at the account level***.

-- **Azure Databricks –**

* A fast, easy and collaborative ***Apache Spark-based big data analytics service***.
* Seamlessly integrate with open source libraries, Spin up clusters and build quickly in a fully managed Apache Spark environment with the global scale and availability of Azure.

5. Azure DevOps CI/CD Pipeline ---------------------------------------

Create Pipeline –

Pipelines 🡪 New Pipeline 🡪

1. Pipelines
2. New Pipeline
3. Use the classic editor (if you go for yaml file, you need to create yaml code)
4. Select source then Team then repository select branch
5. Empty job or Pre-defined template(featured) so select .Net core/Framework
6. It will list down all Job we want (Build, Restore,Test, Publish)
7. Name of Pipelin, agent pool(hosted or private VM), agent specification(required to run pipleline)
8. Set, Save and Queue.

**Assessments ------------------------------------------------------------**

1. **Resource location and usage** - Which two factors affect Azure costs? Each correct answer presents a complete solution? Usage meters, such as CPU time, disk size, and write operations, are used to calculate your bill for an Azure resource. Deleting or deallocating a resource means that you will no longer be billed for it. Different regions can have different associated prices. Resources cost the same no matter the time of day or the day of the week.
2. **Azure Cost Management** -- Azure Cost Management allows you to ***create and manage cost and usage budgets*** by monitoring resource demand trends, consumption rates, and cost patterns. It also allows you to ***use historical data to generate reports and forecast future usage and expenditures***.
3. **Deallocation of VMs** - You have an Azure virtual machine that is accessed only between 9:00 and 17:00 each day. What should you do to minimize costs but preserve the associated hard disks and data? -- If you have virtual machine workloads that are used only during certain periods, but you run them every hour of every day, then you are wasting money. These virtual machines are great candidates to ***deallocate when not in use and start back when required to save compute costs*** while the virtual machines are deallocated.
4. **Resource Tags** - Resource tags can be used to group billing data and ***categorize costs by runtime environment***, such as billing usage for virtual machines running in a production environment.

* You can apply tags to your Azure resources, resource groups, and subscriptions but ***not to management groups***.
* Tags are stored as plain text. *Do not add sensitive values to tags*.
* Resources ***don't inherit the tags*** you apply to a resource group or a subscription.
* Different organizations, use the tags to group usage by cost center.
* ***Categorize costs by department***, such as human resources, marketing, or finance, or by environment, such as test or production.
* Resource tags are used to ***locate and act on resources associated with specific workloads, environments, business units, and owners***.
* In Azure, *you can assign* ***multiple tags to a single Azure resource***.

**Resource Group** – Resource Group is the *logical container* used to combine and organize Azure resources. Resources are combined into resource groups, which act as a logical container into which Azure resources like web apps, databases, and storage accounts, are deployed and managed.

**Region Pair** - In a region pair, a region is paired with another region in the same Geography. *Each Azure region is always paired with another region within the same geography, such as US, Europe, or Asia, at least 300 miles away*. Region pairs allow the replication of Azure *resources across geographies* to help ensure that a secondary region is available in case of any disaster at the primary region.

**Subscriptions** – (MG 🡪 Subscription 🡪 Resource Groups 🡪 Resources)

* For which resource does Azure generate separate billing reports and invoices by default? Azure *generates separate billing reports and invoices for each subscription* so that you can organize and manage costs.
* ***Resource groups can be used to group costs***, but you will not receive a separate invoice for each resource group.
* ***Management groups*** are used to efficiently manage access, policies, and compliance for subscriptions.
* You can set up billing profiles to roll up subscriptions into invoice sections, but this requires customization.
* ***Two subscriptions* cannot *be merged into one***. Each subscription is a separate billing entity with its own resources, permissions, and configurations. It is not possible to combine two subscriptions into a single entity.
* You can ***move resources from one subscription to another***.
* You can ***transfer the ownership of a subscription to another account*** if you have the necessary permissions.
* You can ***convert a Free Trial subscription to a Pay as you go subscription***, and the resources in the subscription will continue to function ***without any issues***.

**Availability Zones** - Which Azure resources can make use of availability zones?

* Availability zones are primarily for *virtual machines, managed disks, load balancers, and SQL databases*.
* Availability Zones are physically separate datacenters within an Azure region.
* Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

1. **Azure Reservations** - Minimize the costs of the virtual machines without reducing the functionality of the virtual machines? -- Azure Reservations offers discounted prices on certain Azure services. Azure Reservations can save you up to 72 percent compared to pay-as-you-go prices. To receive a discount, you can reserve services and resources by paying in advance. Spending limits can suspend a subscription when the spend limit is reached.
2. **Resource lock** –

* What can be applied to a resource to ***prevent accidental deletion***? -- A resource lock prevents resources from being ***accidentally deleted or changed***.
* ***Multiple locks can be set on a single resource*** to provide different levels of protection and control.
* A resource lock will meet both requirements - ***change and deletion***.

1. **Azure Policy** - What can you use to restrict the deployment of a virtual machine to a ***specific location***?

* Azure Policy can help to create a policy for allowed regions, which enables you to restrict the deployment of virtual machines to a specific location.
* What can you use to ensure that a development team can only create virtual machines of a ***certain size***? ***Azure Policy*** enables you to define both ***individual policies and groups*** ***of related policies called initiatives***.
* Azure Policy evaluates your resources and highlights resources that are not compliant with the policies you created.
* Azure Policy can also prevent noncompliant resources from being created.
* Azure Policy is a service in Azure that *enables you to create, assign, and manage policies that control or audit resources*.

1. **Azure Policy v/s Azure Management Group:**

* ***Azure Management Groups*** *provide centralized management for access, policy, and compliance across multiple* ***subscriptions***.
* ***Azure Policy*** helps enforce governance at ***a resource level***, it does *not provide centralized management for access, policy, and compliance across multiple subscriptions.*

1. **Azure role-based access control (RBAC)** - What can you use to allow a user to manage all the resources in a resource group?

* Azure RBAC allows you to assign a set of permissions to a ***user*** or ***group***.
* An Azure RBAC role is applied to a ***scope***, which is a resource or set of resources that the access applies to.

1. **Azure Key Vault** –

* Key Vault is a centralized cloud service for ***storing an application secrets in a single, central location***.
* Securely stores and manages sensitive information such as ***keys***, ***secrets***, and ***certificates***.

1. **Microsoft Purview –**

* Microsoft Purview is a ***comprehensive suite of data governance, risk, and compliance tools***.
* A ***unified view*** into data across on-premises, multi-cloud, and software-as-a-service environments.
* It helps ***enterprises gain insights*** and manage their data more effectively by offering ***data discovery, data classification, data lineage, and data cataloging*** capabilities.
* ***Microsoft Purview*** – for governance, risk and compliance tools. ***Azure*** ***Management Groups*** for subscriptions, and ***Azure Policy*** for individual resource level.

1. **Azure Resource Manager (ARM) templates** - What can you use to define the resources you want to provision in a declarative ***JSON format***? By using ARM templates, you can describe the resources you want to use in a declarative JSON format.

What can you use to create resources in Azure and includes a validation step to ensure all resources are created in a specific order based on dependencies, in parallel and idempotent? ***ARM templates*** define an application's infrastructure requirements for a repeatable deployment that is done in a consistent manner. A validation step ensures that all resources can be created in the proper order based on dependencies, in parallel and idempotent.

1. **Azure Advisor** -

* Makes ***recommendations*** to *help improve reliability, security, and performance, achieve operational excellence, and reduce costs*.
* You need to be notified when there are new recommendations for reducing Azure costs. ***Azure Advisor*** evaluates Azure resources and makes ***recommendations*** to help improve reliability, security, and performance, and reduce costs.
* The recommendations are divided into five categories:
* **Reliability**
* **Security**
* **Performance**
* **Operational Excellence**
* **Cost**

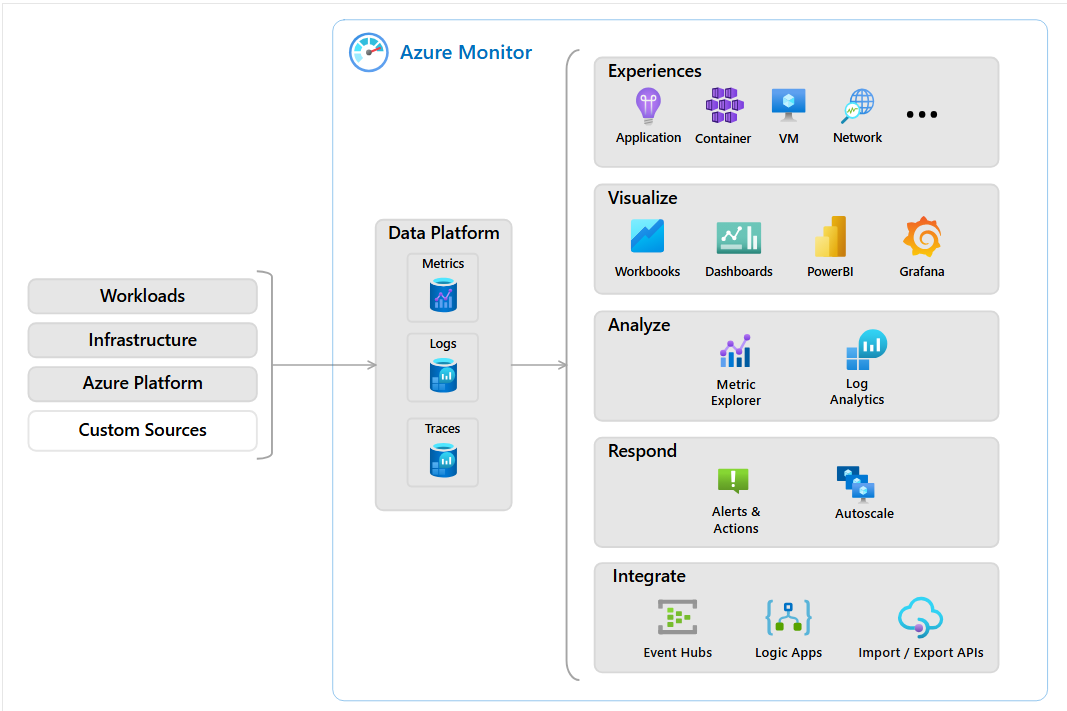
**Azure Service Health** - You need to review the root cause analysis (RCA) report for a service outage that occurred last week. Where should you look for the report?

* After an outage, ***Service Health*** provides official incident reports called ***Root Cause Analysis (RCA),*** which you can share with stakeholders.
* What can you use to get notification about an outage in a ***specific Azure region***? ***Service*** ***Health*** notifies you of ***Azure-related service issues***, such as region-wide downtime.
* What can you use to find information about ***planned maintenance*** *for Azure services that are critical to your organization*? You can drill down to the affected services, regions, and details to showhow an event will affect you and what you must do.
* Most of these events occur without any impact to you and will not be shown. In a rare case that a reboot is required, Service Health allows you to choose when to perform the maintenance to minimize the downtime
* Azure service health does this by combining three different Azure services:
* **Azure Status - Azure status informs you of *service outages* in Azure on the Azure Status page. It’s a good *reference* for incidents with *widespread impact*. It *provides a comprehensive view of health and status of Azure services across all regions*.**
* **Service Health - This is the best place to look for service *impacting communications about outages, planned maintenance activities, and other health advisories* because the authenticated Service Health experience knows which services and resources you currently use.**
* **Resource Health - It provides information about the health of your *individual cloud resources*, such as a *specific* virtual machine instance. *Specific application is impacted*.**

**Azure Health Advisory** - What should you proactively review and act on to avoid service interruptions, such as service retirements and breaking changes? Health advisories are issues that require that you take proactive action to avoid service interruptions, such as service retirements and breaking changes. Service issues are problems such as outages that require immediate actions.

**Azure Monitor** –

* You need to create a custom solution that uses thresholds to ***trigger*** ***autoscaling*** functionality to scale an app up or down to meet user demand.
* Azure Monitor is a ***comprehensive platform*** that collects metric and logging data, such as CPU percentages from ***different environments***. The data can be used to ***trigger autoscaling***.
* Which Azure service can generate an ***alert*** if virtual machine utilization is ***over 80%*** for five minutes? Azure Monitor is a platform for ***collecting***, ***analyzing***, ***visualizing***, and ***alerting*** based on metrics.
* Azure Monitor can ***log data*** from an entire Azure and on-premises environment.
* ***Container Insights*** is a feature of Azure Monitor that ***provides monitoring and performance insights for containerized applications*** running on Azure Kubernetes Service (AKS) or Azure Container Instances.



* ***Log Analytics*** is a feature of Azure Monitor that *collects and analyzes log and performance data from various Azure resources and on-premises environments*.
* Features of Azure Monitor-

1. Container Insights
2. Log Analytics
3. Creating Alerts

* ***Azure Application Insights*** – a part of Azure Monitor, *automatically detect performance anomalies*. *Visually analyze telemetry data* by *integrating with visual studio*.
* ***Azure Activity Logs*** is a feature of Azure Monitor, track activity logs like – *who, what and when done something with the resources, who accessed which resources and when*.
* N.B: ***Analyzing Costs*** is ***not the features of Azure Monitor***.

1. **Consumption-based Model** - What are two characteristics of a consumption-based model? In a consumption-based model, you do not pay for anything until you start using resources, and you only pay for what you use. If you stop using a resource, you stop paying for it. High expenditures are usually associated with the purchase of the physical infrastructure, which is not needed in a consumption-based model.

* No upfront costs
* The ability to stop paying for resources that are no longer used.

1. **Capital Expenditure and Operational Expenditure**- refers to upfront costs incurred one time, such as hardware purchases. Capital expenditures are one-time expenses that can be deducted over time. Operational expenditures are billed as you use services and a do not have upfront costs.
2. **Disaster Recovery Plans** - What are cloud-based backup services, data replication, and geo-distribution features of? Disaster recovery uses services, such as ***cloud-based backup***, ***data replication, and geo-distribution***, to keep data and code safe in the event of a disaster.
3. **Elasticity** refers to the ability to *scale resources as needed*, such as during business hours, to ensure that an application can keep up with demand, and then reducing the available resources during off-peak hours. Means *automatically scaling an application* to ensure that the application has the resources needed to meet customer demands.

**Agility** refers to the ability to *deploy new applications and services qui*ckly.

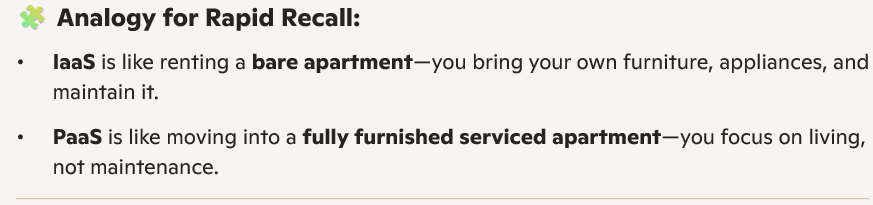
**High availability** refers to the ability to *ensure that a service or application remains available in the event of a failure*.

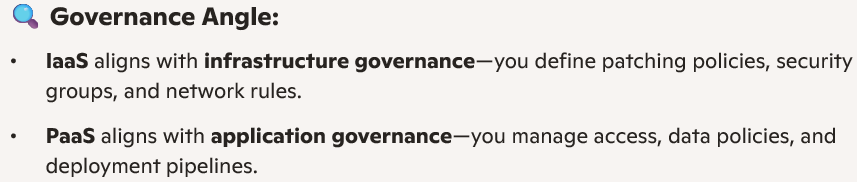
**Geo-distribution** makes a service or application available in multiple geographic locations that are typically close to your users. In cloud computing, ***Geo-location*** allows you to *deploy applications to regional datacenters around the world*. You can deploy apps and data to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region. This is referred to as ***geo-distribution***.

**Predictability** ensuring that *performance and costs remain consistent over time*. *Forecasting and managing resources to maintain a stable* and predictable environment, which is essential for *budgeting and planning purposes*.

1. **IaaS, PaaS and SaaS** –

* ***IaaS*** is the most flexible category of cloud services. It aims to give you *complete control over the hardware that runs applications*. *IaaS is the closest service model to managing physical servers*.
* **PaaS** - Users do ***not control the operating system and do not configure*** the underlying servers in ***PaaS***. You need to focus on application development ***rather than configuration and management of servers***. *With PaaS, users can focus on application development because the cloud provider handles all the platform management*.
* ***IaaS*** consists of virtual machines and networking provided by the cloud provider. The customer is responsible for the OS and applications.
* *The cloud provider is responsible for the OS in PaaS and SaaS.*
* *PaaS and IaaS use a consumption-based model, so you only pay for what you use.*
* **SaaS** - With ***SaaS***, you are using as-is software hosted in the cloud, instead of creating a platform to host a software yourself. Which type of cloud service model is typically licensed through a monthly or annual subscription? SaaS is software that is centrally hosted and managed for you and your users or customers. Usually, one version of the application is used for all customers, and it is licensed through a *monthly or annual* *subscription*. SaaS allows you to pay to use an existing application on hardware managed by a third party. You supply data and configure access. *In SaaS, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications*.
* Customers are only responsible for storage in a ***private cloud***. Customers are responsible for virtual machines and runtime in ***IaaS*** and the ***private cloud***.





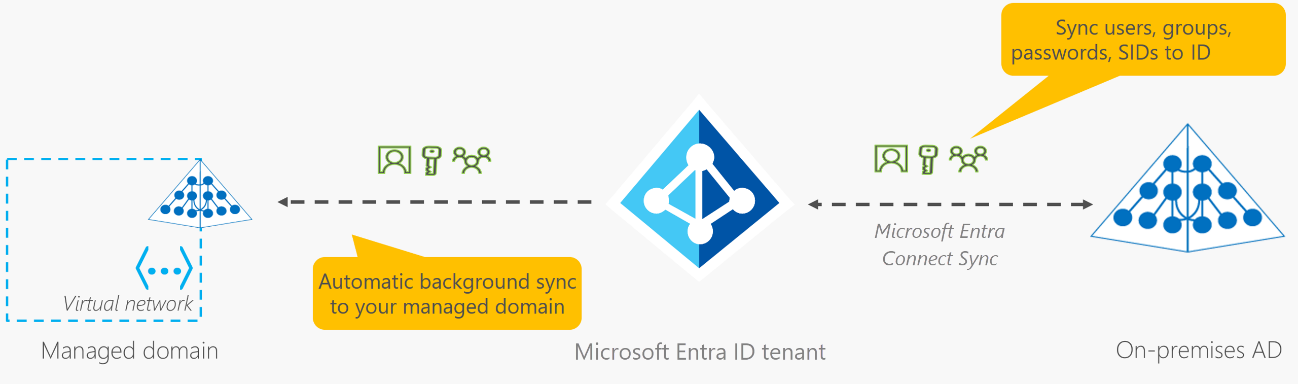
1. **Azure Virtual Desktop** – Azure Virtual Desktop is a desktop and application virtualization service that runs in the cloud. It enables your users to use a cloud-hosted version of Windows from any location. *Azure Virtual Desktop works across devices such as Windows, Mac, iOS, Android, and Linux*. It works with apps that you can use to access Remote Desktops and apps. You can also use most modern browsers to access Azure Virtual Desktop-hosted experiences.
2. **Azure Kubernetes Service (AKS)** - What are two services that allow you to run applications in containers? *Containers* are a virtualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. Unlike virtual machines, you do not manage the operating system for a container.

* Containers
* Azure Container Instances
* Azure Kubernetes Service (AKS)

1. **Single-Sign In (SSO)** - What enables a user to sign in one time and use that credential to access multiple resources and applications from different providers? SSO enables a user to sign in ***one time and use that credential to access multiple resources and applications from different providers***.

**Microsoft Entra ID** - Microsoft Entra supports the registration of devices.

* Microsoft Entra ID provides services such as: ***Authentication*, *Single sign-on (SSO)***, ***Application management, Device management, IAM*.**
* Along with accounts for individual people, Microsoft Entra ID supports the registration of devices.
* It also includes providing functionality such as *self-service password reset*, *multifactor authentication*, a *custom list of banned passwords*, and *smart lockout services*.
* Applications, services, and VMs in Azure that connect to the managed domain can then use common Microsoft Entra Domain Services features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.
* ***Identity and Access***: Managing user identities and controlling access to resources.
* ***Configure B2B collaboration in Microsoft Entra ID to provide external partners with access to your organization’s resources without requiring them to have accounts in your Entra ID tenant***.



**Defense in Depth** - A defense in depth strategy *uses a series of mechanisms to slow the advancement of an attack* that aims to gain unauthorized access to data. The principle of least privilege means restricting access to information to only the level that users need to perform their work.

**DDoS attack** - A **DDoS attack** attempts to overwhelm and exhaust an application's resources.

**The perimeter layer** - The perimeter layer is about protecting an organization's resources from network-based attacks.

**Microsoft Defender for Cloud** –

* Continually ***compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks***.
* Used to ***evaluate whether your company’s Azure environment meets regulatory requirements***.
* It can be used for ***just-in-time (JIT) access*** to protect your Azure VMs from unauthorized network access. Many times firewalls contain allow rules that leave your VMs vulnerable to attack. JIT lets you allow access to your VMs only when the access is needed and for the period of time needed.

**Conditional Access** - Conditional Access allows administrators *to control, allow, or deny access to resources based on certain signals*. You can require that access to certain applications only be allowed if the users are using an approved client application.

* What can you use to ensure that users authenticate by using multi-factor authentication (MFA) when they attempt to sign in from a specific location? - *Conditional Access can use signals to determine information about authentication attempts, and then determine whether to block access or require additional verifications, such as MFA*.
* Assignments (***Who, What, Where***) Target specific users, groups, roles, or guests.
* ***Locations***: Trusted or risky geographic locations.
* Access Controls (Then What).
* Conditional Access is a tool that ***Microsoft Edntra*** uses to allow or deny access to resources based on identity signals.

**Multi-Factor Authentication (MFA)** –

* MFA is a process whereby a user is prompted during the sign-in process for an additional form of identification. Examples include a code on their mobile phone or a fingerprint scan.
* What Microsoft Entra feature can you use to configure security authentication that requires users to use their mobile phone to sign in? MFA is the concept of requiring something more than only a password to sign in to an application.
* You can use the mobile phone to receive a phone call, text, or a code to get authenticated.

**Azure Security Center -**

* Providing ***unified security management*** and ***advanced*** threat protection across hybrid cloud workloads.
* Offers ***security recommendations*** and threat protection.

**Azure Information Protection** –

* Allows you to ***classify, label, and protect documents and emails*** by applying encryption and access policies.
* ***Automatically add a watermark to Microsoft word documents that contain sensitive data like credit card information***.

**N.B:-**

Key Vault - Application Security Layer

Microsoft Entra ID - Identity and Access Layer

1. **Microsoft Sentinel –**

* A cloud-native ***SIEM (Security Information and Event Management)*** service
* ***Collect and analyze log security events*** from various security services within an enterprise environment.
* It ***provides advanced threat detection, investigation, and response capabilities*** to help identify potential threats and provide comprehensive threat intelligence.
* **Playbooks** in Microsoft Sentinel allow for the ***automation and orchestration of response actions*** to enhance incident management and streamline security workflows. By creating and customizing playbooks, security teams can ***automate repetitive tasks, respond to incidents faster, and ensure consistent and effective incident response processes***.

1. **Total Cost of Ownership (TCO) Calculator** - The TCO Calculator helps you estimate the cost savings over time of operating a solution in Azure ***compared*** to operating in an on-premises datacenter.

**The Azure Pricing Calculator** - The Azure Pricing calculator allows you *to estimate and configure according to your specific requirements*. You will then receive a *consolidated estimated* price and a detailed breakdown of the costs associated with each resource you added to your solution.

**Azure Cost Management** – Ability to quickly check Azure resource ***costs, create alerts based on resource spend, and create budgets*** that can be used to automate management of resources.

* Cost analysis is a subset of Cost Management that provides a quick visual for your Azure costs.
* Variety of different ways, including by billing cycle, region, resource.
* The ***three types of alerts*** that may show up are:
  + Budget alerts
  + Credit alerts
  + Department spending quota alerts.
* Provides tools and features to ***control and optimize cloud spending*** in Azure.
* It allows users to ***set budgets, monitor usage, create cost alerts, and analyze spending patterns to prevent overspending*** on Azure resources.

**N.B:-**

**Azure Pricing Calculator -** *Estimate* the cost of Azure services.

**Total Cost of Ownership (TCO) Calculator -** *Compare* the costs.

**Azure Advisor -** *Recommends* to optimize cost, performance, security, and high availability.

**Azure Cost Management -** Set budgets, monitor resource usage, and create cost alerts to *prevent* *overspending*.

1. **Azure Portal** - The Azure portal provides a GUI to view all the services you are using, create new services, configure your services, and view reports.

* Create new resources.
* Create Microsoft Entra user.
* The Azure portal can run on devices that have the ***Android operating system*** installed. The browser can be any type, such as Internet Explorer 11, Chrome, Firefox, or Safari (all the latest versions). When you visit the portal, you will see Cloud Shell. Users can then access Bash and PowerShell from within Cloud Shell. You can use Bash and PowerShell to create Azure virtual machines.
* To run on Android, it needs - the *Azure portal* and *PowerShell in Azure Cloud Shell*.

**Azure Arc** - Azure Arc enables you to *manage, govern*, and secure infrastructure and applications across *on-premises, multi-cloud, and edge environments* — as if they were native Azure resources.

* ***RBAC*** & ***Tags***: Apply role-based access and metadata across environments.
* ***Policy Enforcement***: Enforce compliance, security baselines, and cost controls.
* ***GitOps*** for Kubernetes: Declarative config management via Git repositories.
* Hybrid cloud governance.

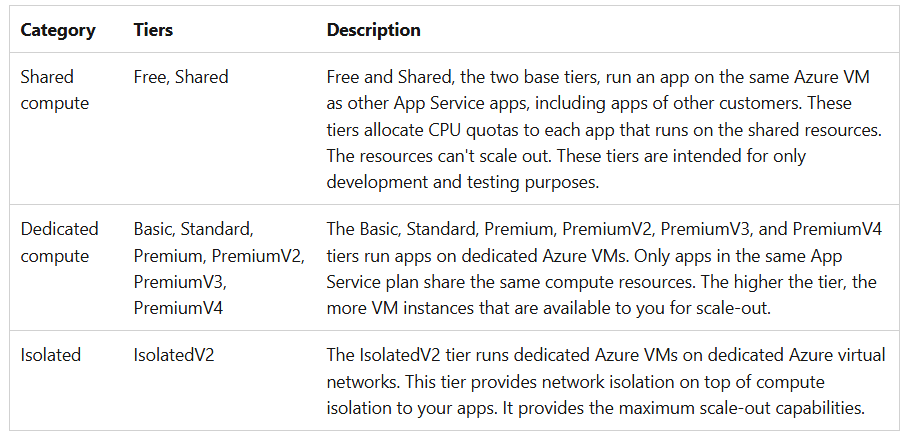
1. **Read-only geo-redundant storage –**

* Data must be stored on multiple nodes.
* Data must be stored on nodes in ***separate geographic locations***.
* Data can be read from both the ***secondary location*** as well as from the primary location.

1. **Support plans –**

* ***Basic support*** - access to billing and subscription management support.
* ***Professional Direct support*** - advisory services. More expensive.
* ***Standard support*** - assessment of an Azure environment’s design, architecture guidance. Cheaper than Professional direct support.

1. **Web Tiers Plans –**



* Basic – does not provide Custom Domain and Load Balancer features. It supports upto ***10 GB Storage***.
* Standard – Custom Domain, Load Balancer.
* Free and Shared – Only upto ***1 GB Storage***.

1. **Expenditure Models – 3**

* ***Pay-as-you-go (OpEx)*** = Pay for what you use, scale up/down anytime.
* ***Reserved Instances*** = Commit for 1 or 3 years for a discount.
* ***Spot Pricing*** = unused capacity at discount.
* In Azure, *when you provision virtual machines, you are* ***charged*** *for the allocated resources* ***such as storage and networking, associated with the virtual machine***, *regardless of whether the virtual machines are running or stopped*. ***Stopping a virtual machine only stops the compute resources but does not stop the billing for the resources allocated to the VM***. While stopping a Virtual Machine (VM) in Azure *may save costs on compute resources*, *charges may still apply for storage resources*, such as disks.

1. **Azure AD (using Azure AD Connect** - By ***syncing*** all ***on-premises AD user accounts*** to Azure AD (using Azure AD Connect), users can continue using the same usernames and passwords to access cloud resources.
2. **Azure API Management –**

* Azure API Management is a service to publish, secure, and manage APIs.
* It is ***not a tool for automating the creation or deployment*** of Azure resources like virtual machines, storage accounts, or networks.

1. **Management Groups -** Organize and manage Azure resources at scale.

* They don't directly create resources themselves.
* ***Not automatic***, like ARM templates, Azure Policy, or Infrastructure as Code (IaC) tools.

1. **Availability Zones** – How many Zones are required for availability. ***This is same as a single*** ***Zone***.
2. **Azure Front Door:**

* Azure Front Door is a content delivery network (***CDN***) service.
* Helps with geo-distribution by delivering content to users ***based on their geographic location.***
* It ensures that content is served ***with low latency and high performance*** by ***routing user requests to the nearest available backend server***.

1. **SLA** – guaranteed:

* Availability.
* Uptime
* SLA quality ***does not depends on multiple subscriptions***. But we can improve by adding redundant service to the application.

1. **Data Migration: (**data box **<** data box disk **<** data box heavy**)**
2. **Data Box:** It is a physical device used for ***offline data transfer to Azure***. Data Box is more suitable for ***smaller data*** migration tasks.
3. **Data Box Disk:**  It is more suitable for ***migrating*** data in the ***terabyte*** range ***rather than petabytes***, making it less efficient for the migration of 1 PB of data.
4. **Data Box Heavy:** It is specifically designed for ***large-scale data migration*** scenarios, such as ***migrating 1 PB of data*** from on-premises environments to Azure. It provides the necessary capacity and capabilities to ***handle massive data volumes efficiently,*** making it the ***ideal choice for offline migration*** of substantial amounts of data.
5. **Azure Government** - It is an Azure environment ***specifically*** built to meet compliance and security requirements for US government.
6. **Azure Hybrid Benefits** – A ***licensing benefit*** that helps you to ***significantly reduce the costs of running your workloads in the cloud***. It works by letting you use your on-premises ***Software Assurance*** enabled Windows Server and SQL Server licenses on Azure.
7. **Trust Center** –

* Provides information about the Azure Compliance offering.
* Provide details of regulatory standards and regulations.
* Provide ***details of Security, privacy, Compliances, policies and practices of Microsoft***.
* ***Microsoft Purview*** provides all these ***in-depth for Products***. Whereas, ***Trust Center provides customer-centric just posture***.

1. **Private Preview** –

* The feature is ***being Beta tested by Azure customers with Enterprise subscriptions***.
* All Azure services in Private preview ***can be accessed by using Azure Portal***.

1. **Azure Repos –**

* A set of ***version control tools***.
* Used to manage codes.
* Two types of version control – Git and TFS.