AZURE

Cloud Computing - Delivery of computing services over the internet. Traditional services like compute, storage, network, databases as well as IOT, ML, AI too. You don't have to wait to build a new data-centre you can just use cloud

Responsibility of Customer -
- Information & data stored in cloud
- Devices that are allowed to connect to your cloud
- Accounts & identities of people services within your org.

Responsibility of Cloud -
- Physical Data Centre
- Physical Network
- Physical hosts

Service models - (IaaS) (PaaS) (SaaS)
- OS
- Network control
- Apps
- Identity & Infrastructure

} Service model's responsibility

Cloud Models -

Public Cloud - No expenses to scale up
apps can be provisioned & deprovisioned
pay only for what you use
you don't have complete control over resources & security

Private Cloud - Org has complete control over security & resources.
Org are responsible for hardware maintainence & updates
Data is not collected with other orgs data
Hardware must be purchased for startup & maintainence.

Hybrid Cloud - Provides most flexibility
Orgs decide where to run apps
Orgs control security, governance & resources.

Multicloud - You use multiple public cloud providers.
Using different features from different cloud providers
Manage security, resources in both cloud.

Azure Arc - Helps to manage cloud environment whether pubic or private in datacenter, hybrid or multi-cloud environment running on multiple cloud providers at once.

Azure VMware Solution - Already established in a private cloud with VMware. Azure lets you run workloads with integration & Scalability.

Consumption Models -

CapEx - Capital Expenditure
OpEx - Operational Expenditure

CapEx - Owning, one time payment, upfront to purchase resources. Ex - Buying a vehicle

OpEx - Renting, spending money overtime. Ex - Renting vehicle

Cloud computing falls under Op Ex.

Pay as you go pricing model.

- Plan & mange your operating cost
- Run infra more efficiently
- Scale your business

→ High Availablity (uptime) & Scalability - (abiliby to handle demand)

SLA - service level agreement

Agreement between service provider & custom-er about service.

Ex - Microsoft Azure & Org.

SLAs also used between IT department & customers/clients of that business

Azure SLA = % representation.

Services that are always available uptime

then you should represent 100%. However, 100% uptime is difficult due to upgrades & maintainence so they are available 99%, 99.9, 99.95, 99.99% time available.

Credit & Downtime is also present

Difference between 99% & 99.9% available

99% available means 1.68 hr downtime per week or 7.2 hrs downtime per month.

99.9% available means service was 10 mins down per week or 43.2 mins per month.

Each Azure service has its own SLA.

Highly available services ~~have~~ comes with extra cost.

→ Scalability - Adjusting resources to meet demand during peaktime. Demand drops remove services

Scalability

Horizontal Vertical

Vertical Scaling - While developing an app you could vertically add CPUs RAMs to your virtual machine. If you overspecified your needs then you can scale down by lowering CPUs RAMs

Horizontal Scaling - If there was a peak demand then you could scale out services automatically or manually. Adding containers, virtual machine to scale out. If demand drops deployed resources could scale in manually or automatically.

→ Reliability - Reliability is the ability to recover from failures & perform. Azure is decentralized i.e. you can configure resources in different regions around globe. If one region has disaster you can shift resources to another region. Sometimes your cloud environment itself automatically shifts to other regions without your action.

→ Predictability – Performance or Cost predictability (3)

D.Y. PATIL DEEMED TO BE UNIVERSITY RAMRAO ADIK INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Performance Predictability – Focuses on predicting resources that will create a positive change for your customers. Autoscaling, Loadbalancing & high availability are some of cloud concepts that come under performance predictability.

Cost Predictability – Focused on predicting cost of cloud spend. With Azure, track & monitor resources also apply data analytics to find patterns to plan better resource deployments. (TCO) Total Cost of Ownership. Pricing Calculator.

→ Durability – How well data is protected from loss or corruption.

→ Governance & Security – ~~With whether you are using~~ Cloud features support governance & compliance. 'Set templates' helps you ensure that all deployed resources meet corporate standards & government regulatory requirements. Upate all your deployed resources to new standards as standards change. Cloud based auditing flag any resource that's out of compliance ~~stand~~ with your corporate standards.

Security – If you need max. control of security go with Iaas but you have to manage os, maintainence & software patches. If you want patches & maintainence to be taken care of automatically go with Paas.

→ Manageability –

Management of Cloud —

— Scale resources deployments in need automatically
— Deploy resources on preconfigured template, removing manual configuration.
— Monitor health of resources & replace failing resources.
— Receive automatic alerts ~~about~~ based on configured metrics, so you're aware of performance in real time.

Management in Cloud —

How you can manage resources

— APIs — Web portal
— Powershell — CLI

→ IAAS — Infrastructure as a Service

IaaS is most flexible category of cloud services as it provides you with maximum amt. of control. Cloud provider is responsible for maintaining hardware physical security, network connectivity. You're responsible for everything OS installation, configuration & maintainance, network configuration, databases etc. Basically renting hardware from cloud datacenter & what you do with that hardware is upto you.

Shared responsibility Model — IAAS places largest share responsibility with you.

Scenarios — Lift & Shift migration — Youre standing on similar resources ~~of~~ ~~cloud~~ cloud to on prem & then moving from on prem to IaaS infra.

Testing & Development – You have established configuration for development & test environments that you need to rapidly replicate. You can stand up or shut down environments rapidly with an IaaS infra while maintaining complete control.

→ PAAS – PaaS is middle between IaaS and SaaS. The cloud provider maintains OS, patches, updates, maintainence, physical security, etc You don't have to worry about it.

⇒ PaaS is suited to provide a complete development environment without headache to maintain all infra.

Scenarios – Development Framework – PaaS provides devs with scalability, high availability & multitenant capability reducing amount of coding devs must do. Devs can build custom cloud solns. on PaaS.

⇒ Analytics & Business Intelligence – Tools provide as a service with PaaS allow orgs to analyze & mine data, find insights patterns & predicting outcomes to improve forecasting, product design, investment return & other business decision.

→ SaaS – Renting or using fully developed app. Email, financial software, messaging software & connectivity software are common ex of SaaS Requires least amount of technical knowledge & least flexible

Least responsibility with user & most responsibi
-lity with cloud provider. In SaaS you are respo
-nsible for data to put in software, users having
access & devices to connect to software.

Scenarios - Email & Messaging
- Finance & expense tracking
- Business productivity apps.

⇒ Physical Infra -

Datacenters like large corporate datacenters.
Facilities with resources arranged in racks with dedic
-ted power, cooling & networking infra.
Datacenters are grouped into Azure Regions &
Availability Zones.

Regions - Geographical area that contains atleast 2
potentially more datacenters networked together with
a low latency network. Azure intelligently controls
resources within each region to ensure workloads are
appropriately balanced. Some services or VM
features are only available in certain regions
such as VM sizes or storage types. Some servic
don't require particular region such as Azure service
directory, Traffic Manger, DNS.

Availability zones - There are more than 1 availability or atleast 1
zones in every region. Each availability zones is made
up of one or more datacenters equipped with power, cooli
-ng & networking. Availability zone is set up to be an

an isolation boundary. High speed, private fib(9)-re opti-c networks. one goes down other continues working.

You have to pay colocate compute, storage networking within an availability zone & replicate in other availability zones. There could be a cost to duplicate your services & transfer data between availability zones. Availability zones are primarily for VMs manged disks, load balancers & SQL databases.

- Zonal Services - Pin resource to specific zones (VMs, IP addresses)
- Zone redundant services - platform replicates automatically across zones. (zone-redundant storage & SQL databases)
- Non regional services - services that are always available from Azure geographies & are resilient to zone wide outages or region wide outages.

Regional Pairs - Two regions are paired (Ex- East US & East US2). This allows replication of resources across geograph & reduces likelihood of interruptions because events such as natural disasters, civil unrest, power outages, physical network outages that affect an entire region. If a region pair was affected by a natural disaster, services automatically fallover other region. Not all azure services automatically fail back to its region pair. In these scenarios recovery & replication must be configured by customer.

Advantages - • If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure atleast one is restored as quickly as possible for apps hosted in that region.

- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime & risk of app outage.
- Data continues to reside within same geography as its pair for tax & law enforcement jurisdiction purposes.

In one direction pairing, primary region doesn't provide backup for secondary region. West India's secondary region is South India & South India doesn't rely on West India.

→ Sovereign Regions - Azure has sovereign regions. Sovereign Regions are instances of Azure that are located isolated from main instance of Azure. Sovereign regions are mostly for compliance & legal purposes.

Ex- US DoD central, US Gov Virginia - These are physical logical network isolated instances of Azure for US government agencies & partners. These datacentres operated by US personnel & includes additional compliance certs.

China East, China North - Unique partnership between Microsoft & 21Vianet whereby Microsoft doesn't directly maintain datacentres.

→ AZURE MANAGEMENT INFRASTRUCTURE

- What is a resource?

Ans - Building block of Azure. Anything you create, provision & deploy etc. is a resource.

Ex - VMs, virtual networks, databases, cognitive services etc. all considered resources within Azure. Resource groups are simply grouping of resources. When you create a resource, you're required to place it into a resource group. While a resource group can contain many resources, a single resource can only be in one resource group. Some resources maybe moved between resource group, but, when you move resource to a new group, it will no longer be associated with former group. You can't put one resource group into another resource group. When you apply action to a resource group it applies to all resources in resource group. When you grant or deny access to a resource group it applies to all resources in that group. If you delete a resource group, all resources will be deleted. Ex - temp dev environment, grouping all resources together means you can deprovision all of associated resources at once by deleting resource group.

→ Azure Subscriptions - Subscriptions allow you to logically organize your resource groups & facilitate billing. Using Azure requires an Azure subscription. A subscription provides you with authenticated & authorized access to Azure products & services. Azure subscription links to an Azure account which is an identity in Azure Active Directory or in a directory that Azure AD trusts.

In a multi-subscription account you can use subscriptions for different types of billing requirements. Azure generates separate billing reports & invoices for each subscription so that you can organize & manage costs.

2 types of subscription boundaries -

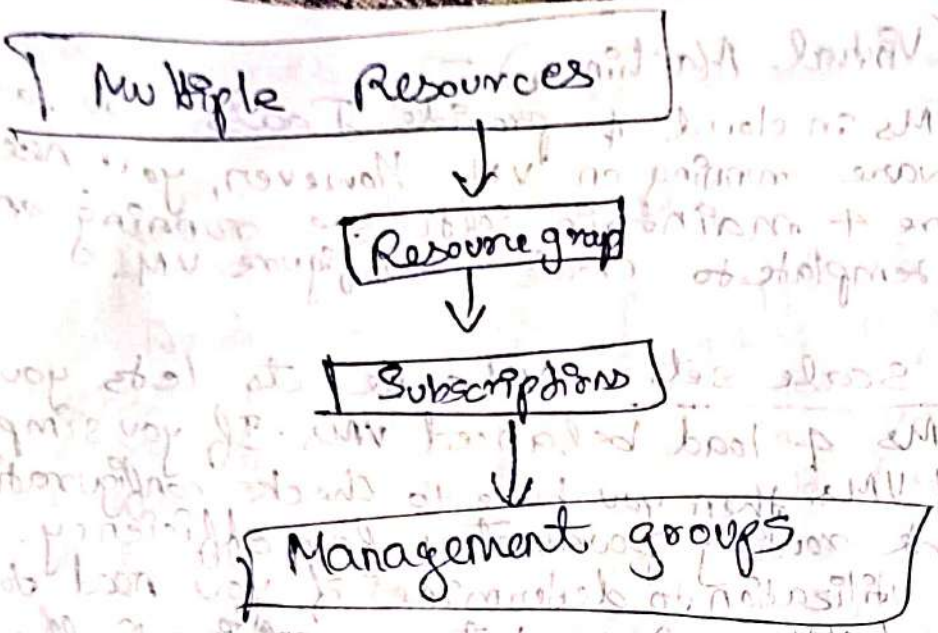
- Billing Boundary - This subscription type determines how Azure account is billed for using Azure. You can create multiple subscriptions for different type of billing requirements. Azure generates separate billing reports & invoices for each subscription so that you can organize & manage costs.
- Access control boundary - Azure applies access management policies at subscription level & you can create separate subscriptions to reflect different org. structure. Ex - Within a business you have separate different departments to which you apply distinct Azure subscription policies.

→ Create Azure subscriptions -

→ Environments - You can choose to create subscriptions to set up separate environments for development & testing security or isolate data.

→ Organisational structures - Subscriptions to reflect different organizational structures. Ex - Limiting one team to lower cost resources while allowing IT dept. full range. This allows you to access resources that users provision within each subscription.

→ Billing - Subscriptions for billing purposes. To track & manage costs. One subs. for production workloads, another for dev & testing workloads.



If you have many subscriptions, you might need a way to efficiently manage access, policies & compliance for those subscriptions. Azure management groups provide scope above subscriptions. You organize subscriptions into containers called management groups & apply governance conditions to the management groups. All subscription within management group automatically inherit conditions from management groups & management groups can be nested.

Facts -
- 10,000 management groups can be supported in a single directory.
- A management group tree can support upto 6 levels of depth. Limit doesn't include root level or subscription level.
- Each management group & subscription group can support only 1 parent.

Azure VMs (Virtual Machines) –

Can create VMs in cloud & provide IaaS. You can cus
-tomize all of software running on VM. However, you need to
update, configure & maintain software running on you
VM. You can use a template to create & configure VM.

Virtual Machine scale sets – VM scale sets lets you ma
-ge identical VMs & load balanced VMs. If you simply
created a lot of VMs then you have to check configuration
& setup network routing parameters for efficiency. You
have to monitor utilization to determine if you need to in
or decrease no. of VMs. Azure lets you automatically
configure, scale, update large no. of VMs centrally in min
Scale sets also deploy load balancer automatically so that
resources are being used efficiently.

Ex. of When to use VMs –

– Testing & Development – VMs provide an easy way to create
different OS & app configs. Test & dev teams can
then delete when they don't need them.

– Disaster recovery – As some apps running on cloud &
on premises, you can get significant cost savings by using
an IaaS approach. If datacenter fails, you can create
VMs & then shut them down when datacenter becomes
operational again.

– Running apps in cloud – When demand strikes you can
setup & start VMs quickly & remove when demand
goes.

– Extending datacenter to cloud – You can run apps on azure
instead of running locally. This makes it easier & less expe
-nsive to deploy on Azure.

VM Resources - size, storage disks, Networking.

→ Azure Virtual Desktop -

Azure Virtual Desktop 4 application virtualization service that runs on cloud. It enables you to use a cloud hosted version of Windows from any location. Azure Virtual Desktop works across devices 4 operating systems, works with apps that you can use to access remote desktops or most modern browsers. Azure Virtual Desktop has centralized security management for users desktops with Azure Active Directory. Enabling multifactor auth also secure data by assigning rolebased access controls. The actual desktop 4 apps are running in cloud so no data is left on personal device, single 4 multisession environments.

→ Containers - Containers are a virtualization environment, Much like running multiple VMs on single host. Containers are light weight, scaled out 4 stopped dynamically. With containers you can reach the demand 4 restart after hardware interruptions.

Difference between VMs 4 Containers -

- VMs → Runs app in isolation or with other apps. Has a separate layer for CPU, processor 4 OS. VMs can only Virtualizes hardware run 1 OS at a time. If multiple apps require diff. complete OS then we need multiple VMs. So tasks like control starting an app or taking snapshot requires time.
- Containers - Lighter weight, bundles app 4 its dependencies 4 deploys on host. The host extracts dependencies 4 requirements 4 lets containers run side by side. Virtualizes OS. Portability Performance 4 manageability.

⇒ Azure Container Instances lets you run your containers fastly & simply by adding containers (containing code).

Containers are used to create solns. using microservice architecture. You can host frontend, backend & storage in diff. containers & scale update independently. Suppose backend ~~container~~ website reached its capacity ~~then~~ & frontend & storage are not being stressed. You can scale backend separately without frontend or storage.

⇒ AZURE FUNCTIONS - If you deploy your app on VM or containers on host then it needs to be "running" for your app to work. But in azure functions, an event wakes the function to do its job. alleviating need of keep resources provisioned when there are no events.

⇒ Serverless - Handling the ~~server~~ app development process while server stuff is being handled by cloud.

Benefits -
- No infra. management
- Scalability
- Only pay for what you use

Just upload code & management of infra., scalability & is handled with pay for what you use model.
Azure functions runs your code when its triggered & deallocates resources when its finished. Functions can be stateless or stateful. If stateless then they behave as if they're restarted everytime they respond to an event. When they're stateful (Durable functions) context is passed through function to track prior activity.

→ Hosting

When you want to host your app you might choose VMs or containers respective of their strengths & weaknesses. However you have one more option - Azure App Service.

Azure App Service lets you host web apps, mobile backend & RESTful APIs in programming language of your choice without managing infra. Offers automatic scaling & high availability. Supports Windows & Linux. Automated deployments, Azure DevOps, GitHub.

⇒ Infra decisions during hosting -
- Sites can be scaled during demand spike.
- Endpoints can be secured.
- Deployment & management are integrated into platform.
- Load balancing & traffic manager provide high availability.

→ AZURE VIRTUAL NETWORKING -

Azure virtual networks let you communicate with users ~~from app~~ over internet also communicate with client computers on on-premises staff. Azure virtual network also allows public/private endpoints to communicate between internal or external resources.

- Public endpoints have public IP address & can be accessed from anywhere in the world.
- Private endpoints exist within a virtual network & have a private IP address from within address space of that network.

→ Isolation & Segmentation - Creating an isolated virtual network. you define private IP address using public or private IP address range. IP range only exists within virtual network & isn't internet routable. Divide IP address space into subnets.

→ Internet Communication -

Communication between Azure Resources -

- Virtual networks can connect not only VMs but other Azure resources, such as App Service Environment for Power Apps, Azure Kubernetes Service, etc.
- Service endpoints can connect to Azure resource types such as Azure SQL databases & storage accounts.

Communication with on-premises resources -

You can link local & cloud environments & create network with your Azure subscriptions.

- Point to site virtual private network connections are from a computer outside your org. back into your corporate network. Client initiates encrypted VPN connection to connect to Azure virtual network.
- Site to site virtual private network links your onprem VPN device gateway to Azure VPN gateway. Connection is encrypted & works over internet.
- Azure ExpressRoute - provides dedicated connectivity to Azure without travelling over the internet. Useful for higher levels of security & greater bandwidth.

→ Route Network Traffic -

- Route tables allow you to define rules about how traffic should be directed. Custom route tables that controls how packets are routed between subnets.

- Border Gateway Protocol (BGP) works with Azure VPN gateways. Azure Route Server, Azure ExpressRoute to propogate on premise BGP to Azure virtual net

→ Filter Network Traffic –

- Network Security groups are Azure resources that contain multiple inbound & outbound security rules. You can define these rules to allow or block traffic from specific port, IP address & protocol.
- Network virtual appliance carries out particular network function, such as running firewall or performing WAN optimization.

→ Connect Virtual Networks – Virtual Network Peering Allowing 2 virtual networks to connect privately & communicating through Microsoft backbone network, never entering public internet. Can be in 2 separate regions & globally interconnected. User define routes (UDR) allow to create table between subnets in a virtual network or between virtual networks. Greater control over network traffic flow.

→ AZURE VIRTUAL PRIVATE NETWORKS

All data is encrypted inside a private tunnel as it crosses the internet. Azure VPN Gateway are deployed ~~on~~ in a dedicated subnet of virtual network. You can deploy only 1 VPN gateway in each virtual network. You can use one gateway to connect various locations which include other virtual networks or on premises datacentres. When you deploy VPN gateway you specify a VPN type: policy based or route based.

Main diff. is how traffic to be encrypted is specified. In both VPN gateways preshared keys are only way for auth.

Policy based VPN - ~~Static~~ IP addr. of packets that should be encrypted through each tunnel. Checks data packet against set of IP addresses to choose tunnel where packet is going to be sent through.

Route based gateways - IPSec tunnels are modeled as network interface or virtual tunnel interface. IP routing decides which tunnel to use for every packet. Route based VPNs are preffered for onpremise devices.

Active/Standy - If any planned maintainence or unplanned disruption occurs to active instance, automatically standby instance assumes responsibility without user intervention.

Active/active - You assign unique public IP addr. to each instance & create separate tunnels from onpremise to each IP add.

ExpressRoute failover - ~~They~~ Have resiliency built in & aren't immune to physical problems that affect cables delivering connectivity. In cases of outage of ExpressRoute you can provision VPN gateway that uses Internet as an alternative method of connectivity.

Zone redundant gateways

ExpressRoute benefits -

- Connectivity to Microsoft across all region in geopolitical region.
- Global connectivity to Microsoft across all regions with ExpressRoute Global Reach.
- Dynamic routing between your network & Microsoft via Border Gateway Protocal.
- Built in redundancy in every peering location for higher reliability.

Global connectivity - You can enable ExpressRoute Global Reach to exchange data across your on premises by connecting ExpressRoute circuits & delivering data via Microsoft network.

Dynamic Routing - ExpressRout uses BGP. Connection between Microsoft Azure services & onpremise network.

Connectivity Models - Cloud exchange
- ~~ExpressRoute~~ Colocation
- Point to Point Ethernet connection
- Any to any connection
- Directly from ExpressRoute sites.

~~Ex~~ Cloudexchange colocation - Colocation refers to your datacenter, office colocated at cloudexchange like ISP. If yes you can request a virtual cross connect to ~~M~~ Azure.

Point to Point - Using a point to point connection to connect to Azure.

Any to any - You can integrate WAN with Azure by connecting offices & datacenters.

Directly from ExpressRoute sides - Connect to Azure at peering location distribute across world.

→ AZURE DNS

- Reliability & Performance
- Security
- Ease of use
- Alias records
- Customizable Virtual networks

Reliability & Performance - Hosted on Azure's global DNS network & made sure that each DNS query is answered by closest available DNS server & uses anycast networking.

Ease of Use - Azure DNS can manage DNS records for Azure services & provide DNS for external resources as well. Automated DNS management can integrate with service by using SDKs & REST APIs

Customizable - Azure DNS also supports private DNS domains - DNS. Allows to use own domains on private virtual networks.

Alias - Use an alias record set to refer an Azure resource such as an Azure public IP address. If IP add. of underlying resource changes, alias record set seamlessly updates itself during DNS resolution.

⇒ STORAGE -

→ Blob storage - To store massive amounts of unstructured data such as text or binary. Ideal for storing images or documents serving browser directly, streaming video audio

→ Azure File storage - To store files & shares are accessible

→ Disk storage - Used for VMs to store data on disks. Solid & conventional hard drives.

⇒ Table storage - Nosql data storage for key value pairs. Storing petabytes of semistructured data to keep cost down.

→ Queue storage - Asyn messaging storage & serving components

3 Azure storage tiers -
Hot, Cool, Archive.

Hot storage - Data that can be accessed frequently such as images for website.

Cool storage - Infrequently accessed data & stored for 30 days such as customer invoices.

Archive storage - Data that is barely accessed such as longterm backups & stored for 180 days.

When creating a storage account we have to create storage account type. This account type determines services & redundancy options & has impact on use cases.

List of redundancy options-

- Locally redundant storage (LRS)
- Geo redundant storage (GRS)
- Read-access geo redundant storage (RA-GRS)
- zone Redundant storage (ZRS)
- Geo-zone-redundant storage (GZRS)
- Read Access Geo Zone redundant storage (RA-ZRS)

1) Standard General Purpose [Blob storage (data lake), queue, Table & Azure files] Recommended for most scenarios

2) Premium block blobs [Blob storage (data lake)] Recommended for most scenarios with high transaction rate or smaller objects & require low storage latency

3) Premium file shares [Azure files] Recommended for enterprise or high performance scale apps.

4) Premium page blobs [Page blobs only] Premium storage account for page blobs only.

Every Azure storage account has a unique-in-name. Both account name & Azure Storage service endpoint form endpoint for your storage account.

Storage account names must be 3 or 24 characters in length & may contain no.s or lowercase letters only. No 2 storage account can have same name.

Ex- Blob storage - https://<storage account name>.blob.core.windows.net

Azure files - https://<storage account name>.files.core.windows.net

Table Storage - https://<storage account name>.files.core.windows.net

→ Azure storage always copies data so that its protected (11) from hardware failures, power outages & natural disasters.

Factor for redundancy options -

- How your data is replicated in primary region.
- Whether your data is replicated to second region i.e. distant to primary region to protect against natural disasters.
- Whether your app needs read access to replicated data in secondary region if primary region is unavailable.

→ REDUNDACY IN PRIMARY REGION -

Replicate 3 in primary region.

LRS & ZRS

Locally Redundant storage (LRS) - Replicates data 3 times within single data center in primary region & provides 11 nines of durability over given year (99.999999999%). Lowest cost & least durability. Protects data against server rack or drive failures. If disaster occurs then its unrecoverable & lost.

Zone Redundant Storage (ZRS) - Replicates data across all availability zones in primary region. Durability of 12 nines over year. If one zone goes down Microsoft performs updates to the zone & if your app tries access before updates are done then it may lead to problem. Read & write access to all availability zones.

→ REDUNDANCY IN SECONDARY REGION - You can choose to copy data into secondary region i.e. 100s of miles away. If data is copied to secondary region then its durable & if disaster occurs in primary region then data is still protected. 2 options.

Geo redundant storage (GRS)

Geo zone redundant storage (GZRS)

By default, read write isn't present in secondary region. If primary region goes down & failover happens to secondary region & then after failover secondary region becomes primary region then you can read & write data. Because data is copied asynchronously the interval between most recent write in primary region & last write in secondary region is known as RPO (recovery point objective). RPO indicates point in time in which data can be recovered. Azure storage typically has an RPO of less than 15 mins & there's no SLA on how long it takes to replicate data to secondary region.

Geo Redundant Storage - Copies data synchronously 3 times in primary region at single location using LRS then copies data asyn to single location in secondary region using LRS. Durability of 16 nines 99.99999999999999%.

Geo Zone Redundant Storage - Copies data to all availability zones in primary region & then copies the data async using LRS to a single location in secondary zone. 16 nines of durability.

However, data in secondary region is only available to read if failover from primary to secondary region. However, if you enable read access to secondary region, your data is always available even when primary region is running optimally. For read access to secondary region, enable (RA-GRS) Read Access Geo Redundant storage or (RA-GZRS) Read Access Geo zone Redundant storage.

→ AZURE STORAGE SERVICES -

Azure Blobs, Azure Files, Azure Queues, Azure Disks

Benefits of Azure storage - Durable & highly available, Secure, Scalable, Accessible, Managed.

→ Blob Storage - Massive amounts of all types of unstructured data. Serving images, documents from browser, storing files for distributed access, Streaming audio & video, backup restore storing data for analysis by an on premise or Azure hosted service. Accessed using HTTP or HTTPS. Only hot & cool access tiers are set at account level. Archive -ve access isn't available at account level. Hot cool & archive can be set at blob level during or after upload. For data in cool access tier, lower SLA & high costs is there as compared to hot data. Archive storage has lowest cost to store but high cost access & update.

→ Azure files - Manages files on cloud via (SMB) Server Message Block or (NFS) Network File System. SMB files accessible from Windows, Linux & MacOS. NFS files accessible from Linux, MacOS. SMB file can be cached on Window Servers with Azure file sync for fast access near where data is used.

Benefits - Fully Manged (files can be created without need to manage hardware or OS).
Shared Access (supports SMB & NFS industry standards).
You can replace on premise file shares with Azure file shares).
Scripting & tooling (Powershell cmdlets can be used to create mount manage Azure file shares as part of administration of Azure apps).
Resiliency (Azure files are available. Resiliency means you don't have to wake up every night to deal with local power outages or network issues).

Familiar programmability & Devs can access files via APIs, I/O)

→ Queue Storage – Used for storing messages. Size of upto 64 KB
Used to create backlog of work to process synchronously.

→ Disk Storage – Disk storage are block level storage volu
i.e. for Azure VMs. Same as physical disk but virtualized.

→ AZURE DATA MIGRATION OPTIONS

→ AZURE MIGRATE – Azure Migrate help you migrate from an onpremises environment to the cloud. Functions as a hub to manage assesment & migration of your on premise datacente to Azure.

- Unified Migration Platform – Single portal to start, run & track your migration to Azure.
- Range of tools – Azure migrate tools include:
  Azure Migrate: Discovery & assesment
  Azure Migrate: Server Migration
  Also integrates with other Azure services.

Integrated tools:

1) Azure Migrate: Discovery & Assesment ⟹ Discover & asses onpr mise servers running on VMWare, Hyper-V, & physical server in preparation for migration to Azure.
2) Azure Migrate: Server Migration ⟹ Migrate VMWare VMs, Hyper-V VMs physical servers & public cloud VMs to Azure.
3) Web App Migration Assistant – Azure App Service Migratio Assistant is a tool to asses onpremise websites for migration to Azure App Service.
4) Azure Data Box to move large amounts of offline data to Azure.

5) Azure Database Migration Service - Migrate on premises databases to Azure VMs running SQL Server, Azure SQL Database, SQL Managed Instance.

6) Data Migration Assistant - Pinpoints potential problems blocking migration. Identifies unsupported features, new features that can benefit your migration.

→ AZURE DATABOX - Physical migration service that helps transfer large amts of data in a quick, inexpensive, unreliable way. The data transfer occurs by shipping you a proprietary Data Box storage that has max storage of 80TB. The Data Box is transferred to & from your datacenter via regional carrier. Order Data Box via Azure portal. Once received set it up by local UI & connect to your network. Once finished transferring data simply return Data Box. If you are transferring to Azure Microsoft does it automatically once data box is received. This can be done once, periodically or initial bulk transfer.

Scenarios to import data to Azure -

Onetime migration - Large amt of on premise data moved to Azure.
Moving media library from offline tapes to Azure.
Migrating VM farm, SQL server & apps to Azure.
Moving historical data to Azure for analysis.
Initial Bulk Transfer
Periodic uploads - Large amts of data generated periodically needs to be moved to Azure.

Scenarios where to export data from Azure -

Disaster Recovery - During disasters, Microsoft ships data box with data to store data to on premise.

Security requirements – when you have to export data due to Government or security requirements.

Migrate back to another cloud provider or onpremises

→ AZURE FILE MOVEMENT OPTIONS –

AzCopy - Commandline utility that you can use to copy blob files to or from your storage account. Helps you upload, download, copy files between storage accounts & synchronize files. AzCopy can be used with other cloud providers to help move files back & forth. One direction synchronization.

Azure Storage Explorer - Provides GUI to manage blobs ~~and~~ files in your storage account. Works on Mac, Windows & Linux & in backend uses AzCopy for tasks. Download, upload, move between storage accounts.

Azure File Sync - Lets you centralize files on Azure files & keep flexibility, performance & compatibility of Windows file server. Bidirectional synced files on Azure with your

Configure cloudtiering so that you can access most frequently files & replicate while infrequently accessed files are kept in cloud.

Have many caches across world.

Replace failed local server by installing Azure file Sync on new server.

Use any protocols like NFS, SMB, FTPS.

→ AZURE DIRECTORY SERVICES

→ Azure Active Directory (Azure AD) is a directory service that enables you to sign in & access your cloud apps as well as Microsoft's cloud apps. Azure AD can also help you maintain your ~~Azure~~ Active Directory dydy. For onpremises, Active Directory is used & for Azure Azure AD is used. When you secure your onpremises with Active Directory it doesn't monitor sign in attemp -ts when you connect Active Directory to Azure AD then it helps you detect sus. signin attempts.

→ Who uses Azure AD?

App devs – Enabling app to work with users credential
IT admins – To control access to apps & resources
Users ie, online service subscription – MS 365, MSoffi -ce.

Azure AD use cases / features –

Auth – verifying identity to access apps & resources. 2FA list of banned passwords, etc.

→ Single Sign on (SSO) – Remember only one username password to access multiple apps. A single identity is tied to a user. As users change roles & leave orgs, access modifications are tied to identity.

App management – Manage cloud & onpremise apps using Azure AD. App proxy, SSO etc.

Device management – Azure AD for registration of devices Device based conditional access policies to restrict attempts to only those coming from known devices.

Can I connect Azure AD with Active Directory on premise?

Yes using Azure AD connect which syncs all the identities as well as features like SSO, 2FA etc under both onpremise & Azure AD.

→ AZURE ACTIVE DIRECTORY DOMAIN SERVICES (Azure AD DS)

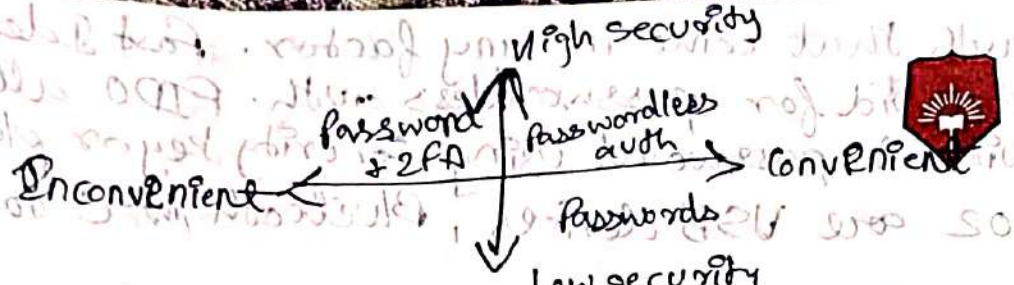
Azure Active Directory Domain provides managed domain services like domain group, group policy, NTLM & lightweight directory access protocol. You can get benefit of domain services without need to deploy, manage & patch domain controllers in the cloud. You can lift & shift on premise legacy apps to cloud & apps that don't have modern auth.

Azure AD DS integrates with Azure AD tenant & lets you sign into services & apps connected to domain using their existing credentials. You can also use existing groups & user accounts to secure access to resources.

→ How Azure AD Domain Service work?

Create an Azure AD DS domain & you define unique namespace. Namespace is the domain name. 2 Windows server domain controllers are deployed to selected Azure region. ~~You don't have to~~ known as replica set. You don't have to manage configure or update these's domain controller

Synchronization - Managed domain is setup for IDirectory transfer from Azure AD to Azure AD DS. You can create resources on managed domain but they aren't synchronized to Azure AD. In a hybrid environment with onpremise AD DS environment Azure AD connect syncs to Azure AD which syncs to manage domain.



→ (SSO) Single Sign On – Enables users to sign in once & use that credentials to access multiple apps & resources. All apps & resources should trust initial authenticator. When we have more identities & more users it becomes difficult to manage everything & if user leaves org then disabling accounts etc becomes challenge -ng. With SSO, you need to remember only one username & password. Access of SSO is tied to identity & if user leaves org its still tied to an identity & not user.

→ Multifactor (MFA) – MFA is a process of prompting user with other form of auth (extra auth). Helps in situations when passwo -rd was compromised but MFA wasn't. Ex- OTP of github MFA requires 2 or more ~~3de~~ elements to fully authenticate Categories of elements –
– Something user knows – challenging question
– Something user has – code sent to user's phone
– Something user is – fingerprint, face scan

MFA increases identity security by limiting impact of creden -tial exposure. An attacker who has username, password cannot access because of MFA like OTP, Fingerprint.

→ Windows Hello for business – Ideal for workers having their own PC as ~~id~~ credentials are tied to PC & has SSO & Public Key Infras. Integration for accessing onpremise & cloud.

→ Microsoft Authenticator – An iOS, android app.

→ FIDO2 security keys – Latest standard that incorporates WebAuth standards. Promotes reduction of password usage. FIDO2 security keys are ~~phis~~ unphishable passw

-ordless auth that come in any factor. Fast Identity online (FIDO) standrid for passwordless auth. FIDO allows users to sign in without password using security key or platform. These FIDO2 are USB devices, Bluetooth NFC too.

→ Passwordless Auth – Passwords are replaced by something -ng you are, you know, you have. Ex-Thumb. Fingerprint is something you have & you can sign in without password with that something. Microsoft global Azure & Azure Government offer passwordless auth with Azure Active Directory.
- Windows Hello for Business
- Microsoft Authenticator App
- FIDO2 security keys

→ AZURE EXTERNAL IDENTITIES –

External identity is a person, device, service, etc. i.e. outside your org. If you want to collab with distributors, suppliers, vendors you can share resources & how external users can access external orgs. If you are a dev, then manage customer identity experience. Users externally can bring professional or casual identities.

B2B collab – Collab with external users by letting them use their preferred identity to sign in your Microsoft apps. B2B collab users are represented in your directory as guest users.

B2B direct connect – Establish 2 way trust with another Azure AD org for seamless collab. B2B direct connect lets external users access your resources within home instance of Teams shared channels. They aren't represented in your directory but visible within teams shared channel & monitored using Team admin center reports.

→ B2C - Publish Saas apps to customers while using Azure AD B2C for identity & access management. Collab with other orgs possible by enabling Azure AD B2B feature. Make sure that guest users have appropriate access.

→ AZURE CONDITIONAL ACCESS -

Conditional access is a tool that Azure AD uses to allow or deny access to resources based on identity signals. Signals include who user is, where user is, what device user is requesting access from.

- Protect orgs assets
- Make users productive, whenever wherever

During sign in, Conditional Access collects signals from user, make decisions based on signals & then enforces decision by allowing or denying access request.

Uses of conditional Access -

→ Require MFA to access apps depending on requesters role, location, network.

→ Require access to resources only through approved client apps.

→ Requires access only from managed device

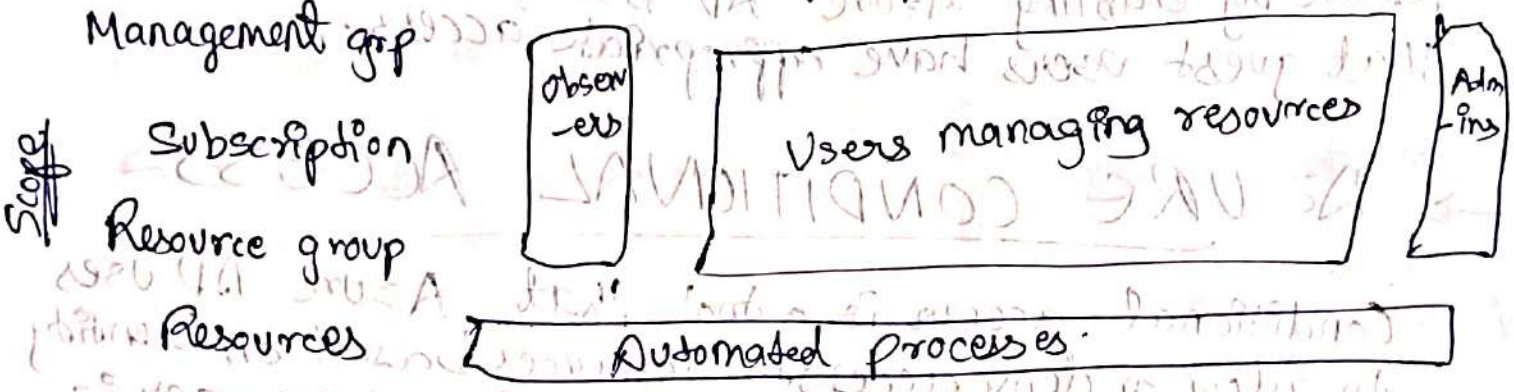
→ Block access from untrusted sources.

→ AZURE ROLE BASED ACCESS CONTROL -

Azure provides built in access to resources for particular role. You can define your own roles. Each role has a set of access permission related to that role. Individuals groups can have access to one or more roles & more accessibility of resources.

Role

Reader | Resource specific | Custom | Contributor | Owner



Azure RBAC (Role Based Access) is hierarchical parent permissions are inherited by children

Azure RBAC allows you to perform actions for your role. If you have one role to read access to resources & other to write access to same resources then you have both read & write access.

→ ZERO TRUST MODEL - Zero Trust assumes worst case scenario & protects resources with that expectations.

Principles of Zero Trust Model -

Verify explicitly - Always authenticate & authorize based on all data points.

Use least privilege access - Limit user access with Just-in-Time & Just Enough Access, data protection.

Assume Breach - Drive threat detection, analytics to get visibility, verify end to end encryption, improve defense.

Modern approach.

→ Defense in depth – Protect info. 4 prevent from being stolen by those who aren't authorized to access it.

Physical Security
Identity 4 Access
Perimeter
Network
Compute
App
Data

Physical Security – Physically securing access to building 4
⇒ securing computer hardware within data center.

Identity 4 Access – Ensuring identities are secure 4 access is granted to what's needed 4 changes are logged.
Use SSO. Audit event 4 changes. Control access to infra 4 change control.

Perimeter – Network perimeter protects from network based attacks against your resources, eliminating impact 4 alerting when they happen. Use DDOS protection to filter large scale attacks before they affect. Use perimeter firewalls to identify 4 alert malicious attacks.

Network – Limiting network connectivity to only resources that are required. Deny by default. Limit communication between resources. Implement secure connectivity to onprem networks. Restrict inbound 4 limit outbound internet access.

Compute – Make sure that compute resources are secure to control in place to minimize security issues.
Secure access to virtual machines.
Endpoint protection on devices.

App - Integrating security into app development cycle. Apps are secure bydefault : Store app secrets in secure medi
-m. Make security a design requirement of app.

Data - Stored in SaaS, cloud storage, disk, database

→ MICROSOFT DEFENDER FOR CLOUD -

Security tool that monitors cloud, hybrid, multicloud, onpr -emise environments & gives guidance about security of services. Defender is Azure built in. So for Azure you do other cloud & onpremise, Defender plans are there & there are Cloud security posture management (CSPM) features.

We can detect errors across -
Azure PaaS Services, Data Services & Networks.

Networks - Limit exposure to bruteforce attacks. By reducing access to VM ports using just in time VM access, harden network using unnecessary access.

Suppose, you have your app on Azure as well as Aws.
- Defender helps you container threat detection & a an ce defenses to your Amazon EKS Linux clusters also. Linux EC2 & windows instances.

→ ASSESS, SECURE, DEFEND -

→ Asses - Identify & track vulnerabilities. Defender provides solns for your VMs, registers, SQL servers. automatic integration of Defender for servers. With this you'll have regular vulnerability scans for infra., data & compute.

→ Secure – You can set security policies & run on whole tenant, subscriptions & management groups.
Defender checks if new resources added follow security policies. Azure security Benchmark provides guidelines for security & compliance best practises. Adds score value This score is like health of security.

→ Defend – Defender ~~pro~~ provides advance threat protection features & security alerts.

Security alert –
- Describe details of ~~se~~ affected resources
- Suggest remediation steps
- Provides option to trigger logic app in response.

fusion kill chain analysis
cyber kill chain analysis

APP SERVICE PLANS

Free:	Shared	Basic	Standard	Premium	Isolated
Free	Environment for dev/test	Dedicated environment for dev/test	Production workloads	Enhanced performance & scale	High performance, security & isolation
10 apps	100 apps	Unlimited	Unlimited	Unlimited	Unlimited
1 GB disk space	1 GB disk space	10 GB disk space	50 GB disk space	250 GB disk space	1 TB disk space
0 maximum instances	0 maximum instances	3 maximum instances	10 maximum instances	30 maximum instances	100 maximum instances
No custom domain	Custom Domain supported	Custom domain supported	Custom domain supported	Custom domain supported	Custom domain supported
No auto scale	No auto scale	No auto scale	Autoscale	Autoscale	Autoscale
Shared compute	Shared compute	Dedicated compute	Dedicated compute	Dedicated compute	Dedicated compute
Private Endpoints not supported	Private Endpoints not supported	Private Endpoints Supported	Private Endpoints supported	Private Endpoints supported	Private endpoints supported

COST MANAGEMENT AZURE

TCO & Pricing Calculator.

OpEx - Renting out infra. for what you need

- Resource Type
- Consumption
- Maintainence
- Geography
- Subscription
- Azure marketplace

⇒ Resource Type - Type, setting, region will impact resources Azure creates metered instance for that resource. Meter tracks everything about resource.

Ex - Blobs - type, performance, access, region, redundancy

VMs - Network interface, storage, license for OS etc

⇒ Consumption - Pay as you go is consistent theme for cloud payment model. But you can use set of resources in each cycle & get discount on those reserved resources. If you have reserved resources & if you see sudden urge then only pay for additional resources usage.

⇒ Maintainence - If you configure VM other resources are also configured. If you deconfigure VM other resources do not get deconfigured so keep an eye on resources.

→ PRICING & TOTAL COST OF OWNERSHIP CALCULATORS

→ Pricing Calculator - Designed to give you estimated cost for provisioning resources in Azure such as compute, storage, redundancy, network.

→ TCO (Total Cost Ownership) - Compare cost for running on premise infra. compared to cloud infra. You enter data of storage, compute, network, etc for cloud infra. In on premise add configurations, IT labour costs & gives an estimation of cost difference.

→ AZURE COST MANAGEMENT -

Cost management provides ability to check Azure cost, creat alerts based on resource spend & create budgets that can be used to automate management of resources. Cost analysis is a subset of Cost management that provides visual view for your costs.

Cost alerts - Check all alerts in Cost Management service.
- → Budget alerts
- → Credit alerts
- → Dept. spending quota alerts

→ Budget Alerts → Notify when spending based on usage reaches exceeds amount defined in alert condition of budget. Budget alerts support both cost based usage based. Alert mail is also sent to people in alert recepients list of budget.

→ Credit Alerts → Credit alerts are done when credit balance is down. Generated at 90% & 100% of your Azure Credit balance

D Y PATIL DEEMED TO BE UNIVERSITY — RAMRAO ADIK — INSTITUTE OF TECHNOLOGY NAVI MUMBAI

Ramrao Adik Institute of Technology

Department of _____

LIST OF EXPERIMENT

Serial No.	TITLE	Page	Date	Signature
→	Department Spending quota alerts when dept. spending reaches fixed quota 50% or 75% Threshold met == cost alert generated			
→	Tags — A way to organize resources. Tags provide extra info. or metadata about resources.			

Resource Management – Tags enable you to act on resources with specific workloads.

Cost management & optimization – Tags enable you to group resources so that you can track budgets, forecast estimated cost

Operations Management – Tags enable you to group resources as per their critical availability in business & lets you form SLAs (uptime guarantee between you & your users)

Security – Tags enable you to classify data as per security level public or confidential.

Governance & regulatory compliance – Tags enable you to identify resources that align with governance or regulatory compliance requirements.

Workload optimization & automation – Tags help you visualize all resources that participate in complex deployments.

Create tags using Powershell, portal, API also tags don't get inherited they are only at one level. You can create tags by setting rules on resources etc.

AZURE BLUEPRINTS - Azure Blueprints lets you apply same settings & policies to every new subscription created. You can setup new test/dev environment with security & compliance settings already configured.

Artifact - Each component in blueprint definition is artifact. Ex- Deploy threat detection on SQL server which requires no additional configurations. It is possible for artifacts to have no parameters as well as one or more parameters.
Artifacts can include things such as -
- Role assignments
- Policy assignments
- Resource groups
- Azure resource manager templates

Azure Blueprints are versionable, allowing you to configure initially & then ~~as~~ update later on.

Blueprint definition - What should be deployed
Blueprint assignment - What was deployed

AZURE POLICY - Lets you enable to create, assign & manage policies that control or audit your resources

Azure policy lets you define individual policy as well as group of related policies, known as initiatives. Evaluates your resources highlights your resources that aren't compliant to your policies. You can set policies on each level (resource, resource group, subscription). Azure policies are inherited. Azure policy comes in with built in policy & initiatives.
Ex - If all resources in a resource group should be tagged with a name then Azure policy evaluates all resources & if some resource doesn't have tag name it applies to it but if you don't want that resource to be tagged you can flag that resource as exception.

Azure policy initiatives - Grouping of related policies together. Azure policy includes initiative name such as Enable Monitoring in Azure Security Centre. Its goal is to monitor all security recommendations for all Azure resource types in Azure Security Centre.

Enable Monitoring Initiative contains 3 policies -

- Monitor unencrypted SQL database in Security Center
- Monitor OS vulnerabilities in Security Center
- Monitor missing Endpoint Protection in Security Center

→ PURPOSE OF RESOURCE LOCKS -

A resource lock prevents resources from being accidentally deleted. Some people with access might delete critical cloud resources so it prevents. Inheritance & application of resource locks at each level (subscription, resource grp. etc)

Types of resource locks -

- Delete - Users can read & modify a resource but they can't delete resources.
- ReadOnly - Users can read resource but cannot modify or delete it.

If you want to change locked resource. You must first remove lock & then change.

→ SERVICE TRUST PORTAL -

Service Trust Portal is a portal that provides acces to various content, tools, & other resources about security, privacy & compliance practices.

Get notified ... ok

D Y PATIL
RAMRAO ADIK INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

AZURE RESOURCE MANAGER - ARM

Lets you manage resources in cloud.

ARM benefits - Manage infra through templates rather than script. ARM template is a JSON file that define what you want to deploy.

Deploy manage, monitor all resources as a grp.
Redeploy resources through development cycle.
Define dependencies between resources.
Apply access control to all services.
Apply tags to resources.
Clarify orgs billing.

ARM templates - IaaS is a concept where you manage IaaS by lines of code. ARM templates are another ex. of IaaS. Templates are already json data you just have to edit it as per your need.

Benefits of ARM templates -

Declarative syntax - Just put requirements without writing actual commands.

Repeatable results - Repeatedly deploy infra through dev cycle.

Orchestration - Deploy template through 1 command & deploy everything parallely.

Modular files - Break into smaller subtemplates also nest templates.

Extensibility - you can add Powershell, bash to your templ -ates. Script can be stored in other source & referrenced in template.

→ AZURE ADVISOR - Azure Advisor evalu -tes your resources & makes recommendations to help improve, security, reliability & performance & reduce costs. You can set advisor for specific subscrip -ons, resource groups, etc.

→ AZURE SERVICE HEALTH - Provides overall status of azure & specific deployments on Azure

Azure Status - Picture of status of Azure globally. Informs about service outages in Azure.

Service Health - Narrower view of Azure. focuses on services, regions, etc. It kows which resources, services you currently use.

Resource Health - Tailored view of actual Azure resources. Health of individual cloud resour -ces.

→ AZURE MONITOR - Help you collect data, analyze, visualize & act on results. Monitor resources on multicloud also.

Azure Log Analytics – Tool in portal to write simple & complex queries. Ex – Simple query – to gather data from resources & complex query is performing statistical analysis.

Azure Monitor Alerts – Automated way to stay informed when Azure Monitor detects threshold being crossed. Alert conditions, notification actions. Ex – you could set a alert when CPU of VM is used 80%.

Application Insights – Monitors your web apps & capable of monitoring apps on on premise, Azure or in different environment!!

You can use to monitor –
→ Request rate, response time, failure rate
→ Page view load performance
→ AJAX calls
→ User session counts
→ Performance counters on diff. OS.

You can periodically monitor apps using App Insights.

2 or more VMs in 2 or more availability zones
→ 99.99%

2 or more VMs in same availability zone → 99.95%

Azure Key Vault → stores only server, apps secrets
Doesn't store Azure AD related secrets
Also stores administrative credentials
Generates new secret after every use.

Authentication → Azure AD RBAC → Authorization

1) Organization that defines international standards across all industries
→ ISO (International Organization for Standardization)

2) Organization defines standards used by Azure Government
→ NIST (National Institute of Standards & Technology)

3) European policy regulates data privacy & protection
→ GDPR (General Data Protection Regulation)

ExpressRoute operates at OSI layer 3.

→ VMs deployed. Now if single data center fails how to make sure that services are upp & running?
Ans → Depby VMs to 2 or more availability zones or regions.
✗ Not to deploy to scale set or 2 or more scale sets.

Azure DDoS protection operates at Network layer (layer 3,4) & application layer (layer 7)

Azure Policies provides orgs with ability to manage compliance of azure resources across multiple subscriptions.

Cassandra → NoSQL, key-value pair.

ExpressRoute helps extend on premise to azure over private connection with help of a connectivity provider

Get notified with Azure Service Health when Microsoft plans to update maintain resources affecting your subscription.

Azure Devops ⇒ CI/CD & store code in git repo.

Connection between on premise VPN device to an Azure VPN gateway through encrypted tunnel over internet.

Ans ⇒ Site to Site VPN.

Individual client for virtual network

Ans ⇒ Point to Site VPN.

Azure AD, Traffic Manager, DNS doesn't require to select particular region

Retrive security tokens from Azure Active Directory

Compliance manager can be accessed from Microsoft Purview compliance portal

Logic apps execute workflows with predefined logic blocks without coding

Azure Batch lets you scale upto 1000s of virtual machines for high computing large scale parallel jobs

Local Network Gateway is object in Azure that represents your onpremise VPN device. A virtual network gateway is VPN object at Azure end of VPN. Connection between them brings up the VPN. (Site to Site)

Azure Advisor provides recommendations on VMs & network settings for VMs.

Microsoft Intune → SaaS

Authorization – Grant access to a legitimate user

Authentication – Who wants to access

→ Enable Just In Time VM access using Azure Security Centre.
Azure JIT locks down inbound traffic to VM. Reduces attacks & connect VM.

→ Monitor Threats using sensors – Azure Advanced Threat Protection
Enforce MFA via Azure Active Directory Identity protection.

→ Downloading of Regulatory Compliance Report → Microsoft Defender for Cloud

Formula for calculating uptime percentage –

$$\frac{\text{Maximum Available minutes} - \text{Downtime in minutes}}{\text{Maximum Available minutes}} \times 100$$

Data ingress (filling in Azure) → free
Data egress (leaving Azure) → charged

VM stopped deallocated/dismounted/unloaded → No charge
VM stopped allocated/mounted/loaded → Charged

Billing/Global administrator can transfer subscription ownership.
Spending limit is fixed & can't be increased or decreased - true
You can remove spending limit.

→ Use DDoS protection in combination with Web app firewall for protection on both at the Network & Application layer.

Increase uptime SLA by – redundant services, adding resources to multiple regions.
Minimum all SLA → 99.9%. Subscriptions don't affect SLA.

Automate response to threats detected by Azure Sentinel?
→ ARs → Azure Monitor Workbooks

Encrypt VM2 → Azure Key Vault

Enterprise messaging soln. integrated → Service Bus

Synapse Analytics SQL architecture → Scalability

IOT Hub ⇒ To monitor control millions of IOT assets.

IOT Edge → Analyse data on end user devices.

IOT Central → Provides application platform as a service (PaaS) that makes it easy to connect monitor & manage IoT assets at scale.

Azure Time Series Insights → Fully managed analytics, storage, visualization service simple to explore analyze billions of IoT events. Gives global view of your data.

Management group tree → 6 levels of depth

Additional resources for VM → NIC Card, Azure Virtual Network

Azure storage capacity limits → Account level

Express Route → 3rd OSI layer

CosMos DB → 1) API selection determines account type
2) Encryption for data at rest is enabled by default.

2 keys available in properties blade for Azure Cognitive Services.
1) Why are these keys available.
2) Key safekeeping

Azure Sentinel → Study

⇒ Which service enables you to achieve those goals is the secure score → Microsoft Defender for cloud

Azure firewall → stateful, scalable

Microsoft Defender ⇒ Cloud's JIT access to protect from Azure VMs from unauthorized access.

Cross Origin Resource Sharing (CORS) is a mechanism that allows domains to give each other permissions for accessing each other's resources.

Microsoft Authenticator provides a user friendly MultiFac -tor Authentication that works with both Microsoft, Azure AD & Microsoft accounts & includes support for wearables & fingerprint-based approval

Basic	Developer	Standard	Professional Direct
Include for all Azure customers	Trial non production workloads	Production workloads	Business critical dependencies.
Billing & subscription management support.	Billing & subscription management support.	Billing & subscription management support.	Billing & subscription management support
Ability to submit as many support tickets as you need.	Ability to submit as many support tickets as you need.	Ability to submit as many support tickets as you need.	Ability to submit as many support tickets as you need.
NO 24/7 support after request submitted.	only support is provided during business hours		
NO architectural support.	General Guidance	General guidance	From a pool of Proactive delivery mangers