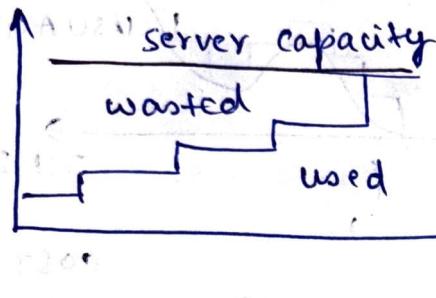
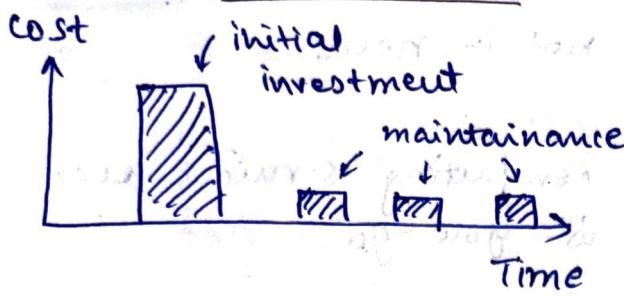


(CapEx)

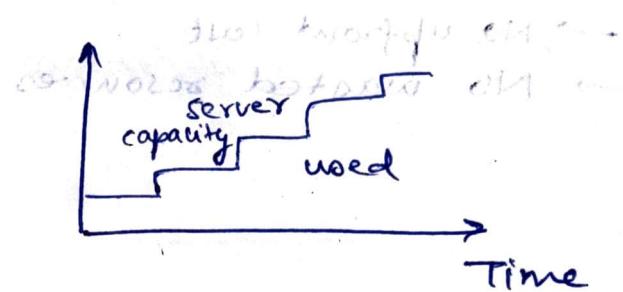
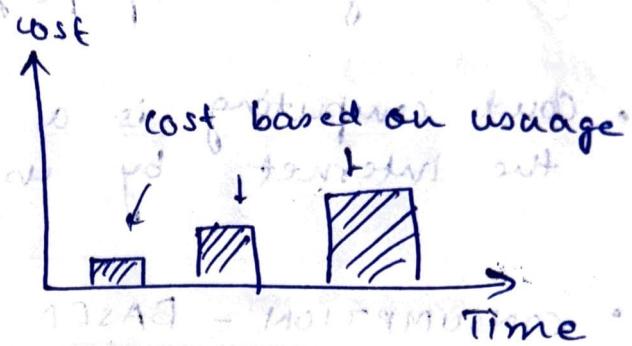
CAPITAL EXPENDITURE



[CapEx]

(OpEx) ①

OPERATIONAL EXPENDITURE



[OpEx]

upfront cost	Significant
ongoing cost	Low
Tax deduction	over time
Early Termination	No
Maintenance	significant
Value over time	Lowers

None

based on usage

* same year

Anytime

low

No change

Eg: repairing the parking lot, company vehicle.

Eg: Renting convention center, signing up for cloud.

- Cloud computing falls under OpEx because it operates on consumption-based Model.
↳ you don't pay for physical infra, electricity etc.

Q3: having your own datacenter infra in a big initial cost associated.

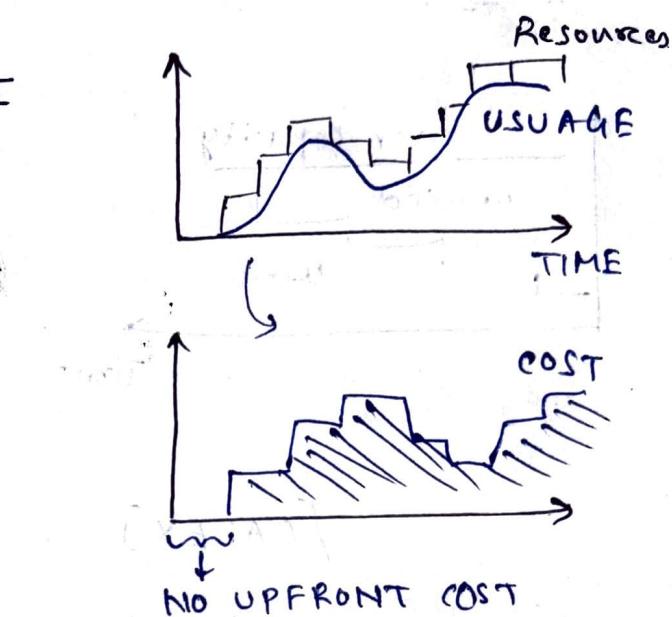
CONSUMPTION - BASED MODEL BENEFITS

- ① No upfront cost
- ② ability to pay for more resources when needed.
- ③ Ability to stop paying when not in need.

- Cloud computing is a delivery of computing services over the Internet by using pay-as-you-go.

CONSUMPTION - BASED MODEL

- NO upfront cost
- NO wasted resources



APPLICATION DATA Data, Apps] SOFTWARE

RUNTIME IIS, docker

MIDDLEWARE software

OS windows, linux

VIRTUALISATION multiple VM

SERVERS Memory, CPU, mother board

NETWORKING internet

STORAGE HDD, SSD

PLATFROM

ON-PREMISES INFRASTRUCTURE (SaaS)

- ON-PREMISES → you responsible for everything.
- ownership: cloud provider manages **NOTHING**
- You manage: everything
 - (i) infrastructure: networking, hardware, virtualisation
 - (ii) Platform: OS, middleware, runtime
 - (iii) Software: data & application
- IaaS (Infrastructure As A Service) → **most responsibility** in basis of model.
 - ownership: cloud provider manages infrastructure
 - You manage: platform
: software
 - use case:
 - ① migration of workload
 - ② Test and development
 - ③ Storage, backup and recovery
- PaaS (platform as a service)
 - ownership: cloud provider manages infrastructure & platform
 - You manage: software
 - use case:
 - ① development framework
 - ② Analytics & business Intelligence.
- SaaS (Software as a service)
 - ownership: cloud provider manages infrastructure & platform & software
 - You manage: Nothing
 - use case:
 - ① buying off-the-shelf Applications.
 - Eg: OneDrive

PUBLIC CLOUD

- Everything runs on cloud provider hardware
- No local hardware
- Some services share hardware with other customers.



ADVANTAGE

- ① No capEx
- ② High Availability & Agility
- ③ Pay - as - you - go.
- ④ No deep technical skills required

DISADVANTAGE

- ① security & compliance
- ② Ownership

③ IT skill & expertise required

PRIVATE CLOUD

- Everything runs on your own datacenter.
- self-service should be provided.



CLOUD SERVICE

ADVANTAGE

- ① can support any scenario
- ② control over security & compliance

DISADVANTAGE

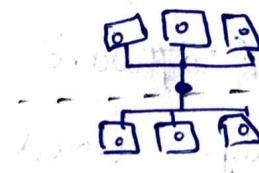
- ① Initial CapEx
- ② Limited Agility
- ③ IT skill & expertise required



CLOUD SERVICE

HYBRID CLOUD

- combine public & private cloud.
- Great flexibility.



ADVANTAGE

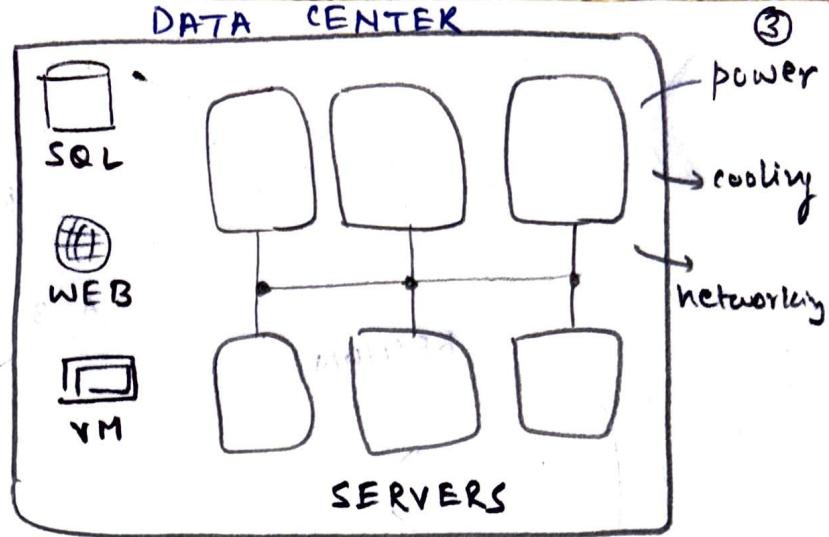
- ① great flexibility
- ② Utilize existing infra
- ③ Meeting Any security
- * ④ Run legacy apps in private cloud!

DISADVANTAGE

- ① can be expensive
- ② complicated to manage
- ③ IT skill mandatory

• DATA CENTER

- physical facility
- Hosting a group of networked servers.
- own powers, cooling & networking infra.



• AZURE INFRASTRUCTURE

→ independent cooling, power.

AVAILABILITY ZONE

- designed to protect from data center failure
- availability zone is no. of assigned to data center in a region
- if zone goes down others continue working.

ZONE SERVICE

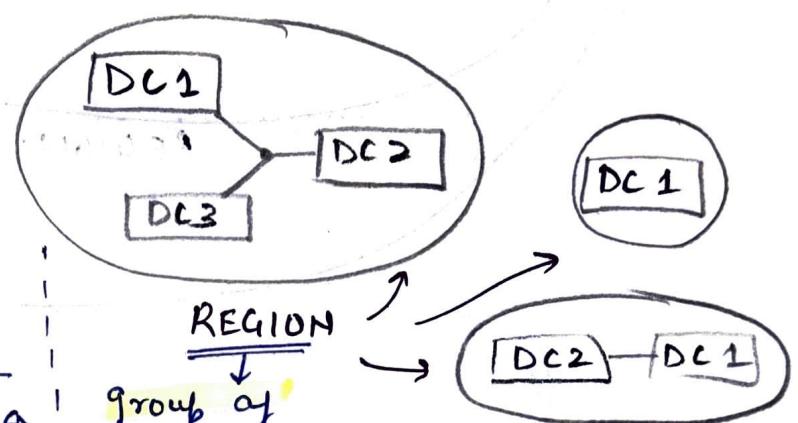
VM, Disk

allow their customers to choose which AZ their service be deployed

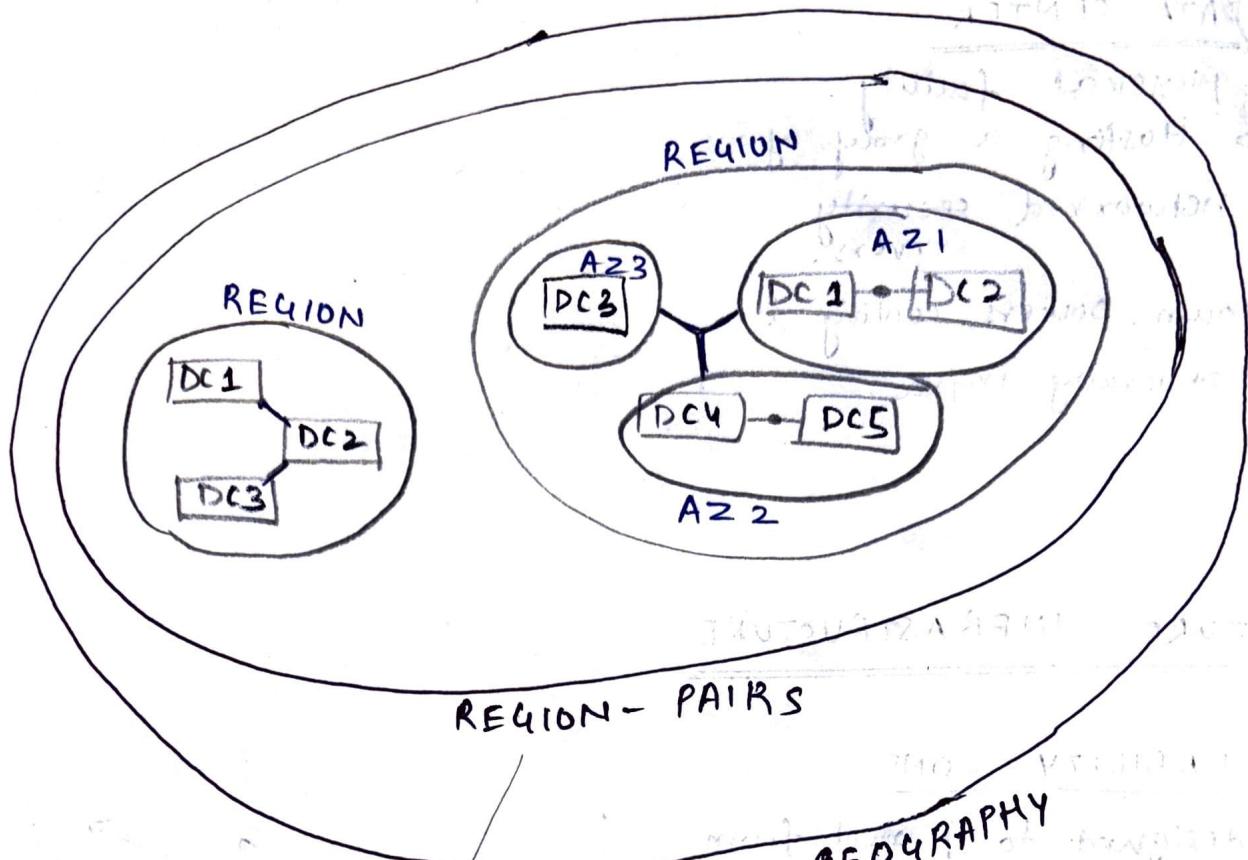
ZONE-REDUNDANT

SQL, Storage

- location of your service.
- some services are available only in certain regions



- Each region is paired with another region making it a region-pair
- Each pair resides within same geography
Except : Brazil South
- Region pair are static and cannot be chosen!



following protect
your Application from
region - wide disasters.

GEOGRAPHY

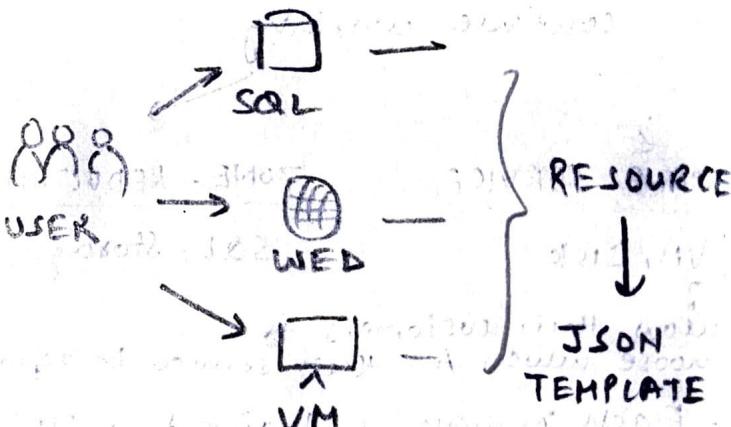
→ contains two or more regions.
Each region belong only to 1 geography.

RESOURCES

- objects used to manage service at azure
- Represent service lifecycle
- Saved as JSON definition.
- ★ it is a purchased service

RESOURCE GROUPS

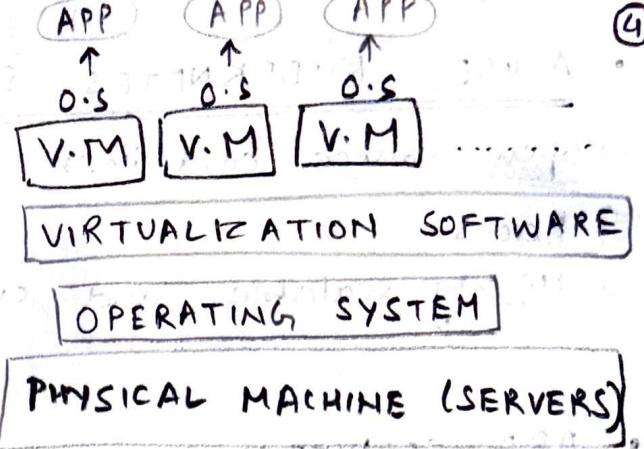
- Grouping of resources
- holds logically related resources
- each resource can only be in one group.
- resource group have location assigned.
- can't be nested.



NOTE : Azure Resource Manager : centralized management layer for managing all azure resour

• VIRTUALIZATION

- ⇒ allows organizations to turn a single physical computer or server into several V.M.
- ⇒ each running independently and potentially with different O.S.



• VIRTUAL MACHINES

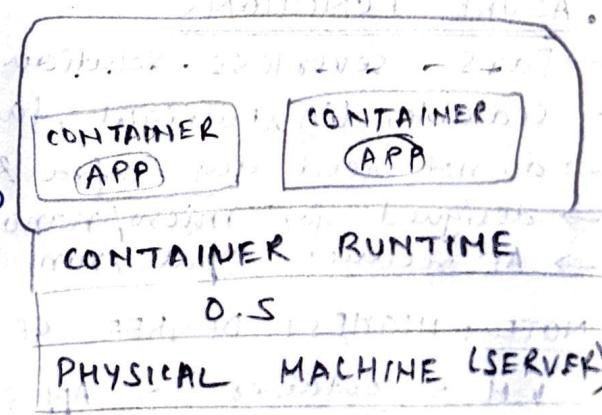
- IaaS
- Total control over the O.S. and software.
- Azure V.M gives you flexibility of virtualization without having to buy and maintain physical hardware that runs on the VM.
- but you still need to configure, update, and maintain.
- you can create or use an already created image to rapidly provision VM.
- custom software, custom requirements.

• AZURE V.M SCALE SETS

- IaaS [that can automatically scale up or down based on demand]
- set of identical V.M., load-balanced V.M.s.
- Built-in auto-scaling features
- Scale set allow you to centrally manage, configure and update a large no. of VMs in minute.
- scale set automatically deploys a load-balancer.

• CONTAINERS vs V.M

- use host's O.S.
- lightweight (no O.S.)
- respond quicker to demand changes



Eg: lego set which has every piece and after building you can place it anywhere.

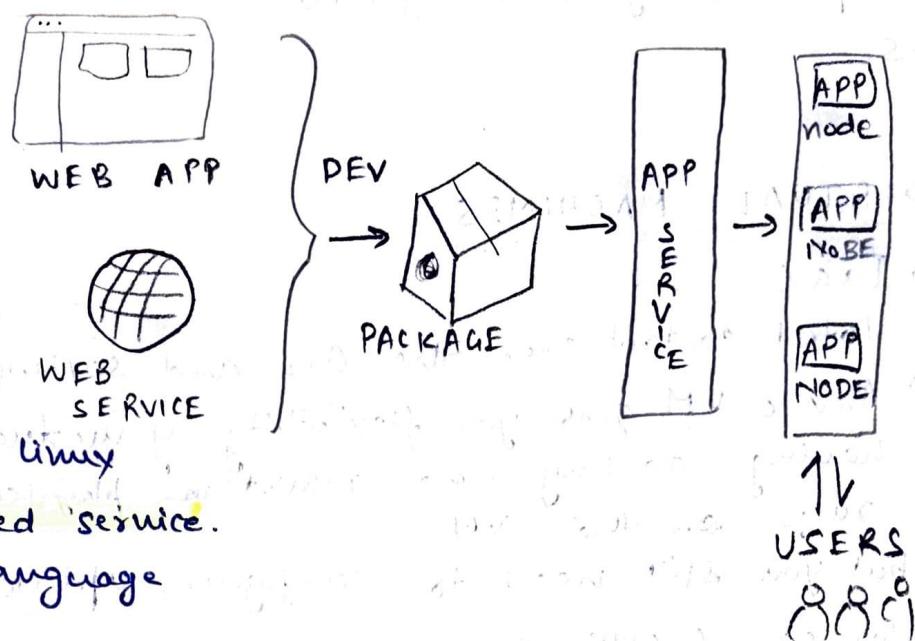
easy to deploy, manage and scale containerized

• AZURE KUBERNETES SERVICES (AKS) application using Kubernetes.

- open source container orchestration platform
- PaaS
- Highly scalable and customizable

• APP SERVICES

- PaaS
- enables you to build and host web pages.
- automatic scaling and high availability.
- support windows & Linux
- is an HTTP-based service.
- support multiple language



① Web Apps: includes full support for hosting web apps using ASP.NET, Python etc.

② API Apps: hosting a website.

- can build REST-based web APIs
- apps can be consumed from any client using HTTP or HTTPS-based client

③ Web Jobs: feature run a program or script. often used to run background tasks.

④ Mobile Apps: use mobile apps to quickly build a back end for iOS and Android Apps.

• AZURE FUNCTIONS

- PaaS, serverless solution
- scalable, lightweight, fast to execute
- do not need any Infra & O maintenance
- designed for micro/nano services
- AF receives input, run it's logic, provide output.

NOTE: HIGHEST DEGREE OF CONTROL TO LEAST

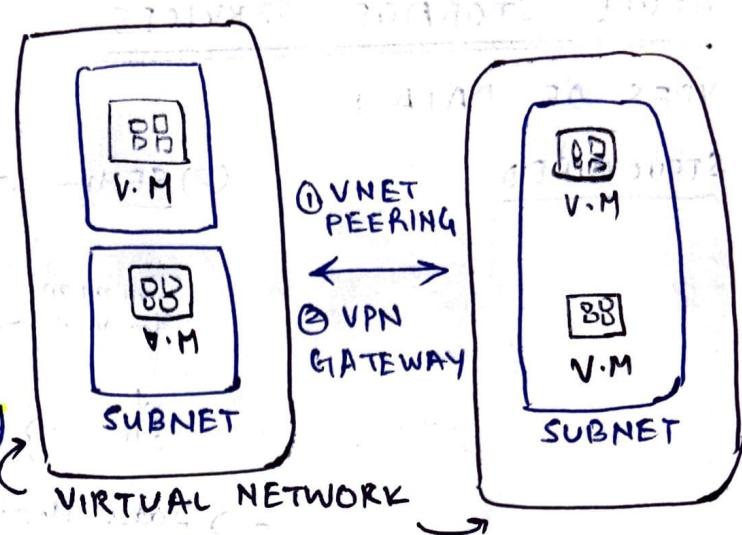
V.M > container instance > App services > Functions.

: VIRTUAL NETWORK

- Azure virtual network & subnets enables resources, such as VMs, web apps to communicate with each other.

→ scoped to single region.

→ VNet peering & VPN gateway allows cross communication.



- SUBNETS: used for -

i) address allocation

ii) NSG (network filtering / Network security Group)

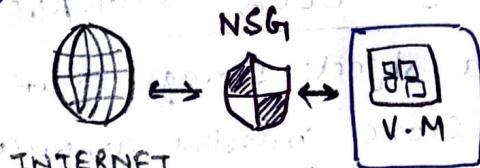
iii) ASG (Application security group)

→ cannot be nested

- VPN Gateway

→ connect on-premises to azure

traffic over public internet.



- Azure Load Balancer

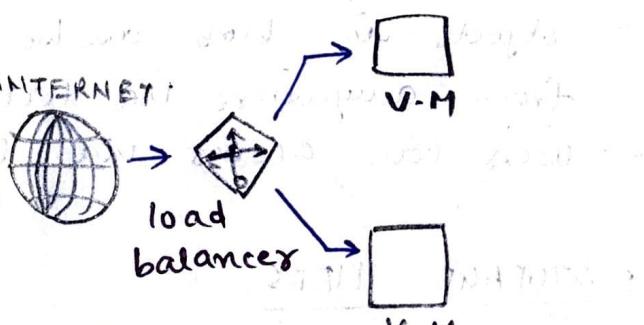
→ provide even traffic distribution

→ highly-availability & scalability

→ Both TCP (transmission control protocol)

(and UDP: user datagram protocol)

→ External & internal traffic

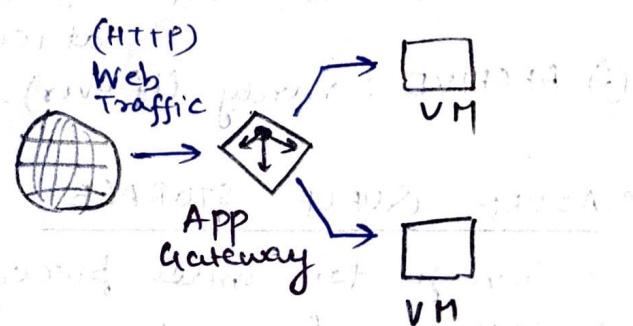


- Application Gateway

→ web traffic load balancer

→ web application firewall

→ SSL termination



- CONTENT DELIVERY NETWORK (CDN)

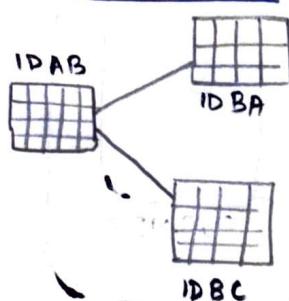
→ Global content caching and distribution to offload web-application and reduce latency

→ helps deliver web content to user more quickly and efficiently. by caching content.

AZURE STORAGE SERVICES

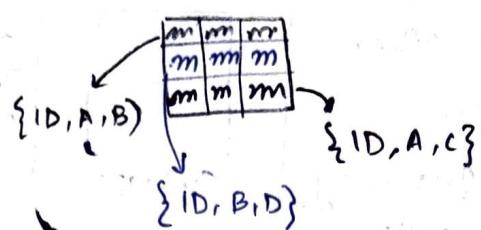
TYPES OF DATA :

(1) STRUCTURED



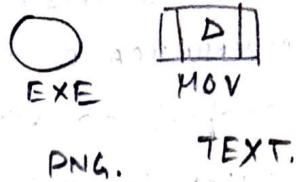
→ organised data in defined format, such as rows and columns

(2) SEMI-STRUCTURED



→ Data that doesn't fit into traditional tables but still has some structure.

(3) UNSTRUCTURED



→ data without pre-defined schema or format

AZURE BLOB STORAGE

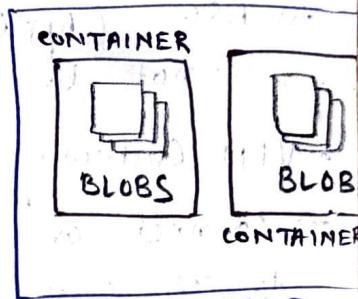
→ is an object storage solution for cloud.
→ can store massive amount of data such as text & binary.

PNG

EXE

TXT

UNSTRUCTURED



→ unstructured.
→ objects in blob can be accessed from anywhere via HTTP or HTTPS.
→ users can access via URL.

STORAGE TIERS

- ① HOT ACCESS TIER : frequently accessed data (Eg : Images)
- ② COOL ACCESS TIER : infrequently accessed data and stored at least for 30 days (Eg : invoices of user)
- ③ ARCHIVE : rarely (if ever) accessed data.

AZURE QUEUE STORAGE

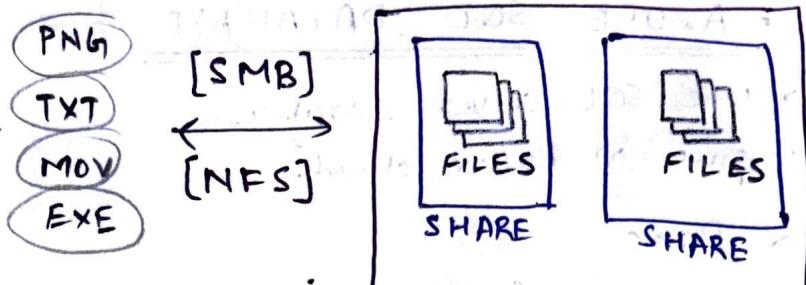
→ storage for small pieces of data [messages]
→ designed for scalable asynchronous processing. ↳ upto 64KB size

AZURE TABLE STORAGE

→ storage for unstructured data (NO SQL)

AZURE FILE STORAGE

- offers full managed file share in cloud that are accessible via SMB (standard servers message block) or NFS (network file system).



BENEFITS: ① You can seamlessly replace your on-premises file shares with Azure file shares.

↳ lift and shift scenarios.

• STORAGE ACCOUNT: Group of services include -

- Highly scalable.
- Highly durable.
- Cheapest per GB storage
- 1) blob storage
2) queue storage
3) table storage
4) file storage

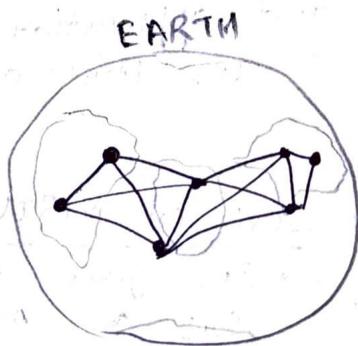
AZURE DISK STORAGE

- are block level storage volumes managed by Azure.
- different sizes, SSD, HDD, performances are available.
- disk can be unmanaged or managed.

AZURE DATABASE SERVICES

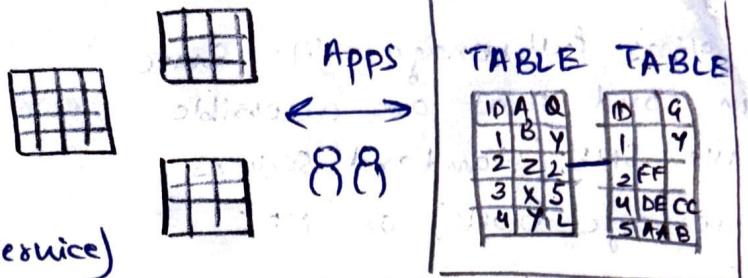
AZURE COSMO DB

- Globally distributed NoSQL data service
- semi-structured data
- schema-less
- Multiple APIs (SQL, MongoDB, table storage)
- super latency responses < 10ms



AZURE SQL DATABASE STRUCTURED

→ Use SQL Server database engine in Azure cloud.



→ PaaS

→ DBaaS (Database-as-a-service)

→ Structured data service defined using schema and rel.

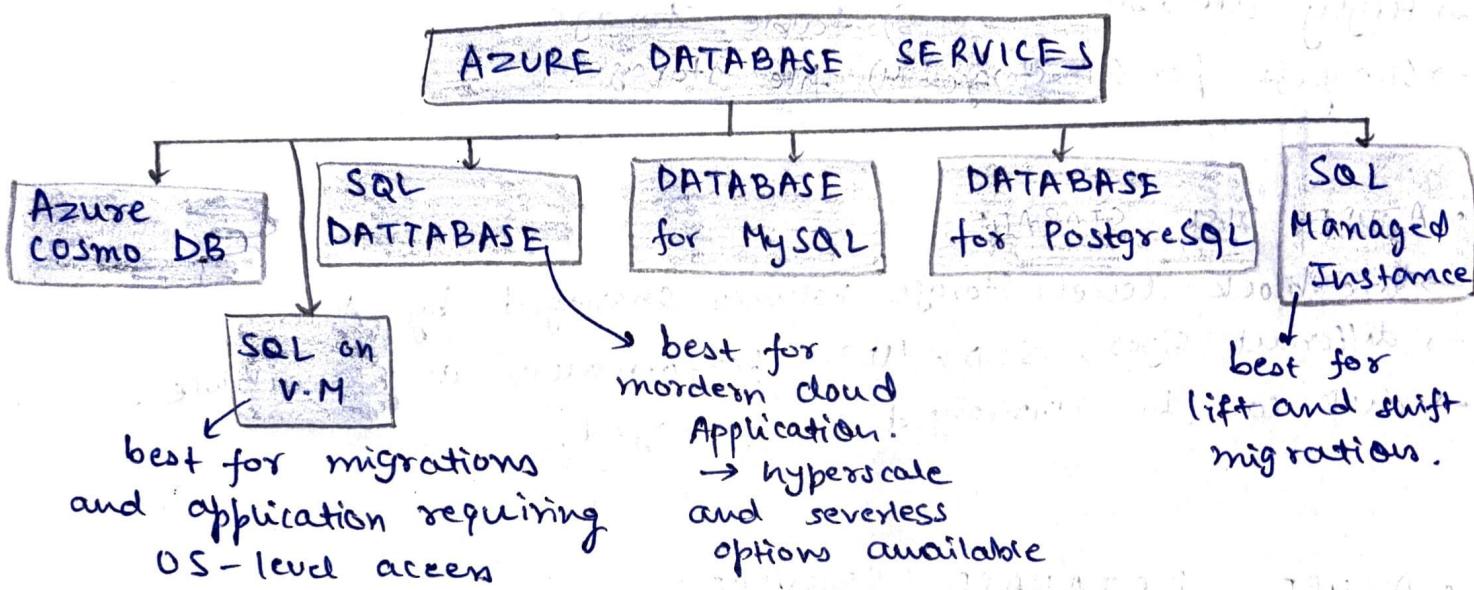
→ High performance, reliable, fully managed and secure.

Benefits : → cost saving

→ ↑ flexibility & scalability

→ pay-as-you-go

→ provide built-in disaster recovery capabilities.



SQL on VIRTUAL MACHINE (VM)

→ it's just a SQL server, so all SQL server skill transfer.

→ SQL on Azure is IaaS.

→ SQL Managed Instances & SQL Database

PaaS

- SQL Managed Instances / SQL Database FEATURES : 7
 - ① High availability, no need to worry about maintenance.
 - ② Automated backups are created.
 - ③ use Azure Read access (RA-GRS) to provide geo-redundancy.
 - ④ long term backup upto 10 yrs.
 - ⑤ Geo-replication creates readable replicas of your database.
 - ⑥ Scalability
 - ⑦ Azure Network security protect your data over internet.

NOTE : SQL Database and SQL Managed Instances are versionless.

• SQL MANAGED INSTANCES

→ like having your own private database server in cloud, without managing infra.

- PaaS
- This feature is ideal for customer who want to use instance-scoped feature and want to move to Azure without rearchitecting their Application.
- This include :
 - i) SQL server Agent
 - ii) Service broker
 - iii) CLR (common language runtime)
- allows you to access instance features, but you don't have to worry about, nor do you have access to OS or infra.

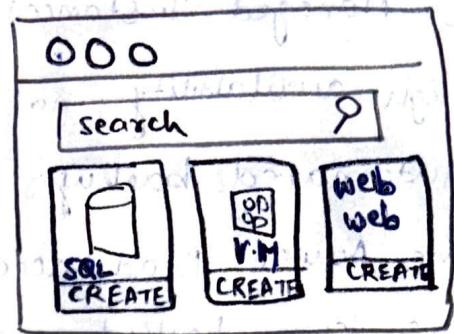
• SQL DATABASE

- PaaS
- abstract both OS and SQL server instances away from user.
- * → only deployment option that supports scenarios that require unlimited database storage (hyperscale) & auto scaling for unpredictable workload (serverless).
- * → It has highest availability. SLA.

Eg : AccuWeather.

AZURE MARKETPLACE

- Azure shop
- First & third party products
- IaaS, PaaS & SaaS



COMMERCIAL MARKETPLACE

Microsoft

APPSOURCE

AZURE

MARKETPLACE

→ Azux

- Azure
- Power BI
- Dynamic 365
- Microsoft 365

PaaS

Business user

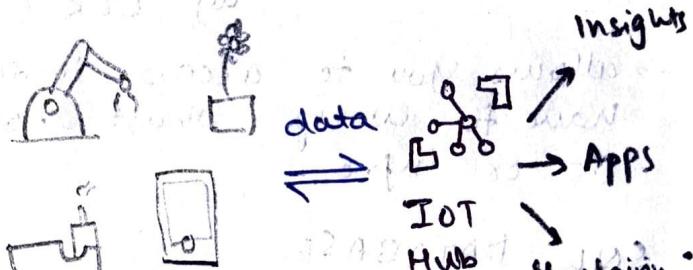
Developers and IP Pros

INTERNET OF THINGS (IOT)

⇒ is a network of internet connected devices (IoT devices) embedded in everyday objects enabling sending & receiving data such as setting & telemetry.

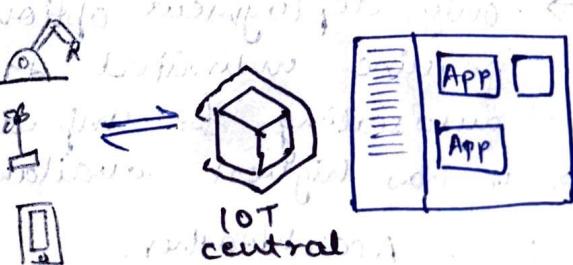
AZURE IOT HUB

- Managed service for bi-directional communication
- PaaS
- Highly secure, stable, reliable
- Integrates with IoT Azure service
- Multiple protocol (HTTPS, AMQP, MQTT)



AZURE IOT CENTRAL

- SaaS
- Industry-specific App template
- No deep knowledge required.
- It manages, monitors all the IoT devices.

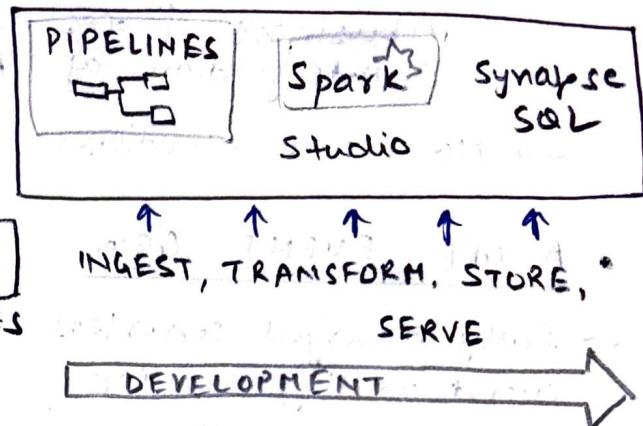


AZURE SPHERE

- Secure end-to-end IoT solution
- Certified chips (MCUs)
- Azure Sphere OS

AZURE SYNAPSE ANALYTICS

- PaaS
- Multiple components
 - i) Sparks
 - ii) Synapse SQL
 - iii) Synapse pipelines
- Studio



AZURE HD-INSIGHT

- flexible multi-purpose big data platform (PaaS)
- multiple technologies: Hadoop, Spark, Kafka etc.

AZURE MACHINE LEARNING

- creating, managing, and publishing ML model

→ PaaS

- Machine learning Workspace : top level resource
- Machine learning Studio : web portal for end-to-end dev.
- FEATURES : Notebooks - using python and R
 - : Automated ML -
 - : Designer
 - : Data & compute
 - : Pipeline

- Serverless Computing : cloud is a way to run code without managing servers. The cloud provider takes care of infra.

Eg : Azure Functions.
: Azure logic Apps.

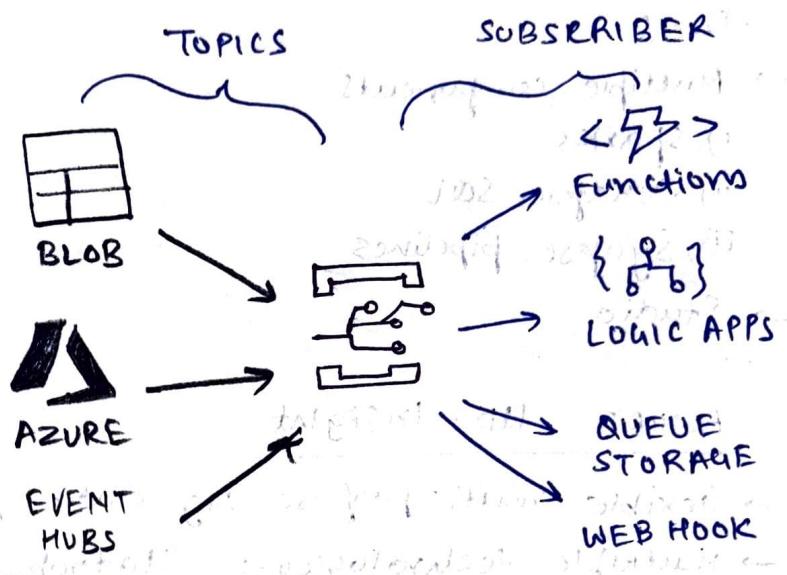
AZURE LOGIC APPS

- Serverless integration service (PaaS)
- 200+ connectors for popular services
- Designed for orchestration of:
 - i) business processes
 - ii) integration of App, data, and logic

→ No-code solution

AZURE EVENT GRID

- fully managed serverless event routing service
- publish-subscribe model
- support built-in events
- Eg: of serverless.



• DEVOPS : set of practices that combine both development (Dev) and operations (Ops).

AZURE DEVOPS :

- one stop shop for developers need to create and manage
- toolbox for developers that helps them to work together, manage code and automate the process.

AZURE SECURITY GROUPS

NSG [NETWORK SECURITY GROUPS]

- designed to filter traffic to (inbound) and from (outbound) Azure resources

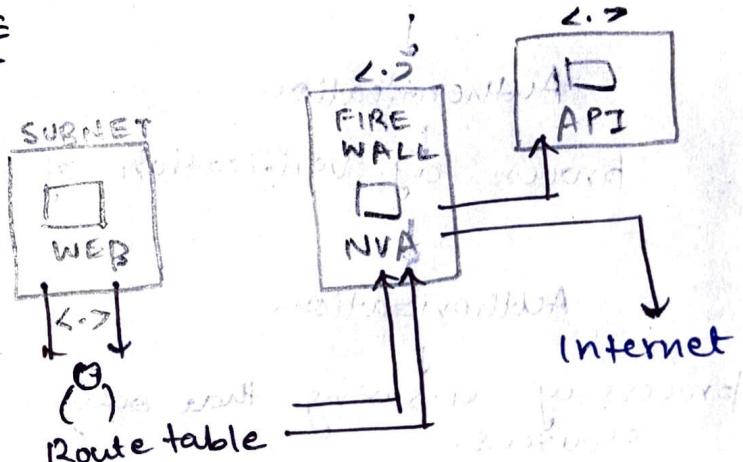
ASG [Application security Group]

- allow grouping of VM located in Azure network.
- designed to reduce the maintenance effort.

Routing : process of finding/selecting a path for a traffic in one or across multiple network.

USER - DEFINED ROUTE

- custom (user-defined, static) routes (UDRs)
- designed to override Azure default routing or add new route.
- Managed via Azure Route table resource.



AZURE FIREWALL → network security that monitor & control incoming & outgoing traffic.

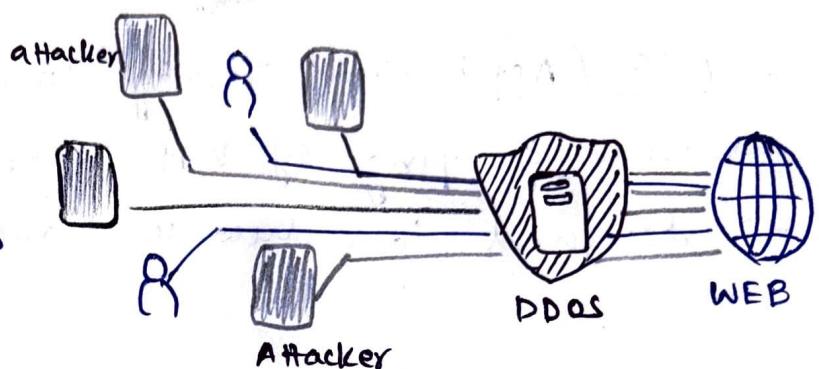
- cloud based (PaaS)
- high availability
- high scalable
- Inbound & outbound traffic filtering rule.
- Support for FQDN (fully qualified Domain Name)
- fully integrated with Azure Monitor for logging and analytics.

- DOS - Denial of Service
 - cyber attack with intent to cause temporary or indefinite disruption of service.

• DDoS PROTECTION {Distributed Denial of Service}

→ detect malicious traffic and blocks it while allowing legitimate users to connect.

→ prevent additional costs for auto-scaling



TWO TIERS:

- 1) Basic - automatically enable for Azure platform
- 2) Standard - Additional monitoring capabilities
 - use ML to Analyze traffic pattern for better Accuracy.

• AZURE IDENTITY SERVICE

A user with username & password

Authentication

process of verification of Identity

Authorization

process of ensuring that only authenticated Id get access to resources.

Access Management

• AZURE ACTIVE DIRECTORY

→ Identity & Access Management service in Azure.

→ used by many Microsoft cloud platform

→ Sync with on-premises AD

PPPS user

AZURE AD



Subscription,
V.M.,
Database,
Resource Group

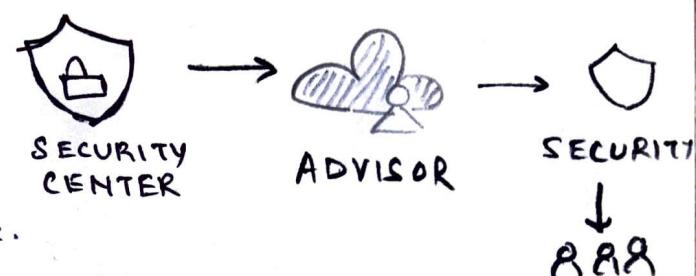
Skype,
Outlook,
Power BI,
Teams

- MULTI - FACTOR AUTHENTICATION

- process of presenting two or more pieces of evidence to prove Identity.
- like : knowledge factor, physical factor (fingerprint), location factor (GPS).

- AZURE SECURITY CENTER

- centralised infra & platform security management service
- Natively embedded in Azure.
- Integrated with Azure Advisor



- AZURE KEY VAULT

- managed service for securing sensitive information (PaaS).
- secure storage service for: key, secrets and certificates.
- Highly integrated with other Azure service.
- centralization.
- Access monitoring & logging.

- RESOURCE LOCKS

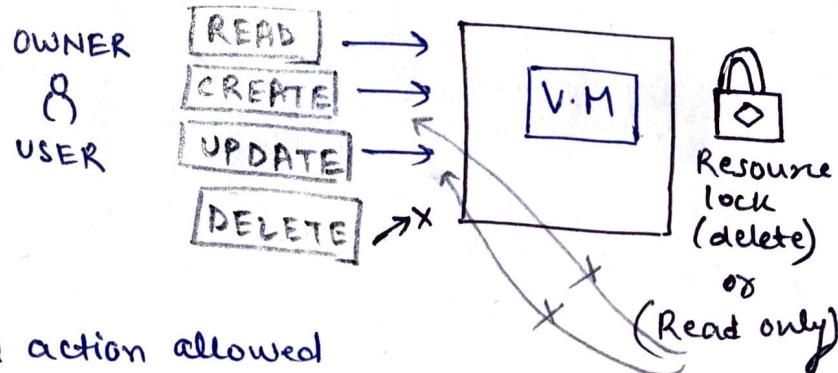
- designed to prevent accidentally deletion or modification.

→ TYPES OF LOCKS:

- Read only - only read action allowed
- Delete (can't delete).

→ Management Group can't be locked.

→ Only owner and User Access Administrator role can manage locks.



OpEx cost can be impacted by :

- ① Resource type
- ② consumption
- ③ Maintenance
- ④ Geography
- ⑤ Subscription type
- ⑥ Azure Marketplace.

Pricing calculator

- designed to give you estimated cost for provisioning resource
- you can get estimate for individual resource.
- info only.
- you won't get charged for any service you select.

TCO calculator (Total cost of ownership)

- designed to help you compare the cost for running an on-premises infra compared to Azure cloud infra.
- You don't need an Azure subscription to work with TCO calculator.

Cost Management

- ability to check Azure Resource costs,
- create alerts based on resource spend.
- create budget.

Cost Alert

- provide a single location to quickly check on all alert by cost Management.

TYPES OF ALERT

- ① Budget → where you set a spending limit for A.
- ② Credit → when your credit monetary commitments are consumed.
- ③ Department spending quota.

↳ when department spending reaches a fixed threshold of quota.

Azure policy

→ enables you to create, assign and manage policies that control your audit in resources.

Resource locks

→ designed to prevent accidentally deletion or modification.

Types of locks

- ① Read only - only read action allowed.
- ② Delete - can not delete.

→ only owner and user Access Administrator role can manage locks.

Service Trust Portal

portal that provide access to various content, tools, & other resources about Microsoft security, privacy & compliance practise.

Azure Advisor

→ evaluate your Azure resources and make recommendations to help improve

- ① reliability
- ② security and performance
- ③ operational excellence
- ④ reduce cost
- ⑤ performance.

→ designed to save your time on cloud.

Azure Service Health

→ helps to keep track of Azure resource both specifically deployed resource and overall status by Azure.

3 SERVICES :

- ① Azure Status : inform you of service outages in Azure.
: health view of Azure service across region
- ② Service health : focus on Azure service and region
- ③ Resource health : provide health info of individual cloud resource.

AZURE MONITOR

- platform collecting data of your resources
- Analysing data.
- visualising info.
- keeps an eye on everything running in Azure.

Azure Log Analytics

- tool within Azure Monitor
- allow you to write queries to search through this data.

Application Insights

- feature of Monitor
- helps you monitor the performance and usage of your web application.

AZURE ARC

- bridge that connects your on-premises server and other cloud environment to Microsoft Azure.
- allows you to manage and govern your resources.

AZURE RESOURCE MANAGER (ARM)

- provide a way to organise and manage your Azure resources.
- allow you to deploy, update and delete resource in coordinated manner.
- a tool that helps you manage all parts of Azure in organised way.

AZURE ARM TEMPLATES

- are JSON files that define infra and config for your Azure resources.

AZURE EXPRESS ROUTE

→ let you extend your on-premises network into the Microsoft cloud over a private connection.

benefits:

- ① connectivity across all regions in geopolitical region.
- ② Dynamic routing b/w your network and Microsoft via (BGP) border gateway protocol.

Office 365
Dynamic 365
Cosmo DB

Colocation at cloud exchange

refers to datacenter, office being physically colocated at a cloud exchange

AZURE DNS

hosting service for DNS domains.

NOTE: cannot use (DNS Azure) to buy a domain name.

AZURE ROLE BASED ACCESS - CLOUD (ABAC)

- ensure that people only have access to the resources they need to do their job, improving security and reducing risk of accidental change or data breaches.
- manage who have permission to do what in cloud
- it can be implemented using (ARM)

ZERO TRUST MODEL

- assumes the worst case scenario and **protect resources** with that expectation.
- security approach that assumes no one or nothing inside or outside can be automatically trusted.

DEFENSE IN-DEPTH

- protect info and prevent it from being stolen by those who aren't authorized.
- set of layers
- each layer provide protection and if breached, subsequent layer is already present.

DEFENDER FOR CLOUD

- monitoring tool
- for security posture management & threat protection.
- monitor your cloud, on-premises, hybrid, multi-cloud to provide guidance at strengthening security.

MICROSOFT ENTRA

(enables) organization to implement zero trust security strategy and create a Trust Fabric.

- ① Conditional Access is a tool that Microsoft Entra ID uses to allow or deny access to resources based on identity signals.