

## Shared responsibility model

By this model responsibilities are shared among cloud provider & consumer. Physical security, power, cooling and network connectivity are responsibility of cloud provider, whereas consumer is responsible for data & information stored in cloud. Consumer is also responsible for access security, meaning you only give access to those who need it.

IaaS gives most responsibility on consumer, cloud provider being responsible for basis of physical security, power & connectivity only. Whereas SaaS places most responsibility on cloud provider.

## Cloud models

They define the deployment type of cloud resources. These main cloud models are : private, public and hybrid

## Azure ARC

Azure Arc is set of technologies that helps manage your cloud environment. Azure Arc can help manage your cloud environment, whether its public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration or even a multi-cloud environment running on multiple cloud providers at once.

## Azure VMware Soln

> lets you run your VMware workloads in Azure with seamless integration & scalability

# Cloud Service types

Q2

## 1) IaaS

- most flexible category of cloud services
- cloud provider is responsible for maintaining hardware, network connectivity & physical security
- it is basically renting the hardware in cloud datacenter, but what you do with hardware is upto you.

### Scenarios :

1) Lift & shift migration : simply moving things running on-premises to running on IaaS infrastructure

2) Testing & development : since you can standup or shut down the different environments rapidly with an IaaS structure, u can use it for development & test on different environments.

## 2) PaaS

- With things of IaaS, cloud provider also maintains OS, middleware, development tools & business intelligence services that make up a cloud sdn.

### Scenarios :

1) Development framework : PaaS lets developers create apps using built-in software components.

2) Analytics or business intelligence : tools provided as a service with PaaS allows organizations to analyze & mine their data, finding insights & patterns & predicting outcomes to improve forecasting, product design decisions, investment returns & other business decisions

## 3) SaaS

- is most complete cloud service model from product perspective
- here you are essentially renting or using a fully developed application

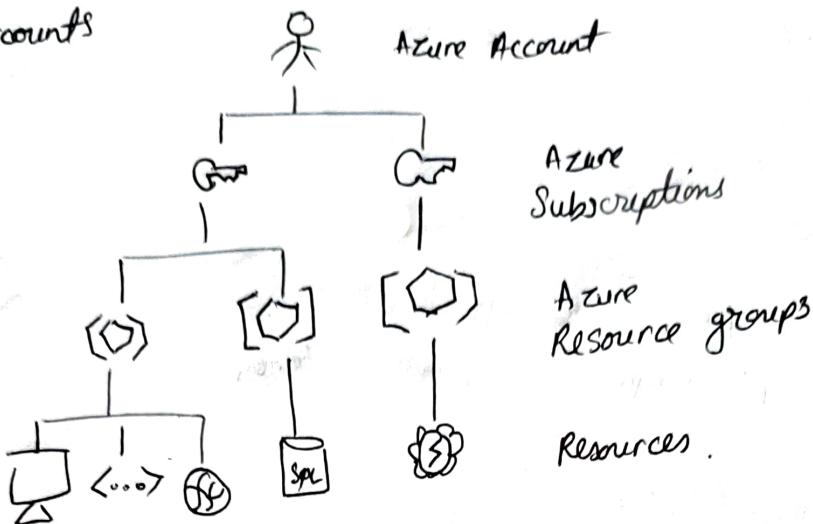
### Scenarios :

- 1) Email & messaging
- 2) Business productivity applications
- 3) Finance & expense tracking

# Azure Architecture & Services

(3)

## Azure accounts



### Azure free account

- > free access to popular azure products for 12 months
- > credit to use for first 30 days (\$200)
- > Access to more than 25 products that are always free.

### for student

- > free access to certain azure services for 12 months
- > credit \$100 for 12 months
- > free access to certain software developer tools

### Physical infrastructure

it starts with datacenters which are grouped into Azure Regions or Azure Availability Zones.

- Region : it is geographical areas on planet that atleast contains one datacenter
- Availability : Availability zones are physically separate datacenters within an azure zones region. Each availability zone is made of one or more datacenters equipped with independent power, cooling & networking. An availability zone is set up to be an isolation boundary. If one zone goes down, the other continues working. Availability zones are connected through high-speed private fiber-optic networks.

Region pairs : Most azure regions are paired with another region with same geography at 300 miles away. This approach allows for replication of resources across geography that helps reduce the likelihood of interruptions because of events like natural disasters.  
eg east us paired with west us.

## Azure management Infrastructure

Resource : It is basic building block of Azure. Anything you create, provision, deploy etc is a resource. VM, databases, cognitive services are some examples.

Resource group : Ans. Ans. Ans.

Azure Compute & networking services

3 compute options (Virtual Machines, containers and Azure functions)

### 1) Azure Virtual Machines

(note)

VMS provide IaaS in form of virtualized server & can be used in many ways. Just like physical computer, you can customize all of the software running on your VM. VM's are an ideal choice when you need.

- 1) Total control over the OS
- 2) Ability to run custom software
- 3) To use custom hosting configurations

> You can use already created image to rapidly provision VMS. An image is a template used to create a VM & may already include an OS and other software like development tools or web hosting environments. Images only for windows & Linux.

> Virtual machine scale sets : VM scale sets let you create & manage a group of identical load-balanced VMs. Scale sets allow you to centrally manage, configure and update large number of VMs in minute. Also no. of VM instances can automatically increase or decrease in response to demand.

> Virtual machine availability sets : They are another tool to help you build a more resilient, highly available env. They are designed to ensure that VMs stagger updates & have varied power & network connectivity, preventing you from losing all your VM's with single network or power failure.

### When to use VMS

- 1) During testing & development
- 2) When running applications in the cloud
- 3) When extending your datacenter to the cloud
- 4) During disaster recovery.

• Azure Virtual Desktop : desktop & application virtualization service that runs on cloud. Just a copy of your desktop on cloud.

- Azure Containers

↳ Azure Container Instances

- Azure Functions

Azure Functions is an event driven, serverless compute option that doesn't require maintaining VMs or containers. If you build an app using VMs or containers, those resources have to be "running" in order for your app to function. With Azure Functions, an event wakes the function, alleviating the need to keep resources provisioned when there are no events.

- Functions scale automatically based on demand, so good choice when demand is variable
- Functions runs your code when its triggered and automatically deallocated resources when fn is finished. So you're only charged for CPU time used while fn runs
- Functions are key component for serverless computing. They are also a general compute platform for running any type of code.
- Functions can be either stateless or stateful. When they are stateless (the default), they behave as if they are restarted every time they respond to event. When they are stateful (called Durable Fn's), a context is passed through the fn to track prior activity.

## # Application hosting options

1) can use VMs

2) Containers

3) Azure App Services

- Azure App service enables you to build & host web apps, background jobs, mobile - back-ends & RESTful APIs in programming language of your choice without managing infrastructure
- Offers automatic scaling & high availability
- Support windows & Linux
- enables automated deployments from Github, Azure Devops or any git repo to support continuous building model
- It is HTTP-based service for hosting

## Azure Virtual Networking

Azure Virtual networks & virtual subnets enables Azure resources such as VMs, databases to communicate with each other. Azure virtual networking supports both public & private endpoints to enable communication b/w external or internal resources with other internal resources.

> Azure Virtual networks provide following key networking capabilities:

- 1) Isolation & segmentation
- 2) Internet communications
- 3) Communication b/w Azure resources
- 4) Communication with on-premises resources
- 5) Route network traffic
- 6) Filter network traffic
- 7) Connect virtual networks.

• Peering : allows to connect two virtual networks.

## Azure Virtual Private Networks (VPN)

A VPN uses an encrypted tunnel within another network. VPNs are typically deployed to connect 2 or more trusted private networks to one another over an untrusted network (like public internet) and traffic is encrypted to prevent eavesdropping or other attacks.

## Azure Express Route

It lets you extend your on-premises networks into Microsoft cloud over a private connection. With ExpressRoute you can establish connections to Microsoft cloud services such as Azure or Microsoft 365. This allows you to connect offices, datacenters to microsoft cloud. Each location having its own ExpressRoute circuit.

## Used Dynamic Routing

> ExpressRoute uses BGP (Border Gateway protocol). BGP is used to exchange routes b/w on-premises networks & resources running in Azure.

## Azure DNS

By hosting your Domain in Azure, you can manage your DNS record using same credentials, APIs, tools & billing as your other Azure services.

# # Azure Storage

HOT : data accessed frequently

Cold storage tier : less frequently access

archive : rarely access data (like backups)

## # Azure Storage redundancy

Azure Storage always stores multiple copies of your data.

### 1) Local redundant storage

LRS replicates ur data 3 times within single data center in primary region

### 2) Zone redundant storage

for availability zone - enabled regions , ZRS replicate Azure data synchronously  
Across 3 Azure availability zones in primary region

### 3) Geo - Redundant storage

GRS copies your data synchronously 3 times within single physical location  
in primary region using LRS. It then copies your data asynchronously  
to a single physical location in secondary region (region pair) using LRS.

### 4) Geo - zone - redundant storage

Data in GZRS storage account is copied across 3 Azure availability  
zones in primary region (similar to ZRS) and is also replicated to  
secondary geographic region using LRS .

# By default, data in secondary region isn't available for read or write  
access until there's a failover to secondary region

## # Azure Storage services

If has following data services

1) Azure Blobs : A massively scalable object store for text & binary data  
Also includes storage for big data analytics

2) Azure Files : Managed file shares for cloud or on-premise deployments

3) Azure Queue : A messaging store for reliable messaging betn application components

4) Azure Disks : Block level storage volumes for Azure VMs.

Also Azure migration options

? Azure Migrate  
Azure Data Box

## # Azure file movement options

Include tools designed to help you move or interact with individual files or small file groups.

- > AzCopy
- > Azure Storage Explorer
- > Azure file Sync

### AzCopy

> it is command-line utility that you can use to copy blobs or files to or from your storage account.

### Azure Storage Explorer

> Azure Storage Explorer is stand-alone app that provides graphical interface to manage files & blobs in your Azure storage account.

### Azure File Sync

Azure File Sync is a tool that lets you centralize your file shares in Azure files and keep the flexibility, performance & compatibility of windows file server. It's almost like turning your windows file server into miniature content delivery network.

# basically, Azure file sync keeps files b/w on-premises windows servers & an azure cloud environment updated.  
It maintains bi-directional synchronization of files.

## ⑦ Azure Data migration options

way to get your data & information into Azure. Azure Support Both real-time migration of infrastructure, apps & data using Azure Migrate, as well as asynchronous migration of data using Azure Data Box.

### 1) Azure Migrate

It is service that helps you migrate from on-premises env. to cloud. Azure Migrate functions as a hub to help you manage the assessment and migration of your on-premise datacenter to ~~cloud~~ Azure.

### 2) Azure Data Box

## Describe core architecture components of Azure.

- Account, physical infrastructure
- Regions, Availability zones, Region Pairs, geography.

### Sovereign Regions

- > Sovereign regions are instances of Azure that are isolated from main instance of Azure.
- > You need to use sovereign region for compliance or legal purpose.

- eg
- 1) Azure gov. for US, These datacenters are operated by screened US personnel and include additional compliance certifications.
  - 2) Azure China : partnership with 21Vianet, whereby Microsoft doesn't directly maintain the datacenters.

- Resource & resource group, subscriptions, management grp.

### Azure Compute & networking Services

- 2.2
- VM, VM Scale set, VM availability set.
  - Azure Virtual desktop
    - Container (Azure support Docker)  
(VM are more flexible)
    - Azure functions
    - Azure App Service

### Azure virtual networks

VN enable you to link resources together in your on-premises environment and within your Azure subscription. There are 3 mechanism to do this:

- 1) Point-to-site virtual Private network: connects computer outside your organization back into your corporate network via encrypted VPN connection.
- 2) Site-to-site VPN: link your on-premises VPN device or gateway to Azure VPN gateway in VN. Devices in Azure can appear as being on local network. Connection is encrypted & works over internet.
- 3) Azure Express Route: provides dedicated private connectivity to Azure that doesn't travel over internet, greater bandwidth & security.

VN has Route table: which allow you to have defined rules on how to direct traffic. Can also use BGP (Border gateway protocol).

- VPN gateway, express Route.

# # Azure identity, access & security

## 1) Azure Directory (AD) services (SAAs)

AD is directory service that enables you to sign in & access both Microsoft cloud applications and cloud apps you develop.

Azure AD is cloud-based identity & access management service.

> Authentication      > Single sign-on      > Application management  
> Device management      > Multi-factor authentication.

Azure AD Connect :- it synchronizes

betw on-premises Active Directory & Azure AD.

user identities

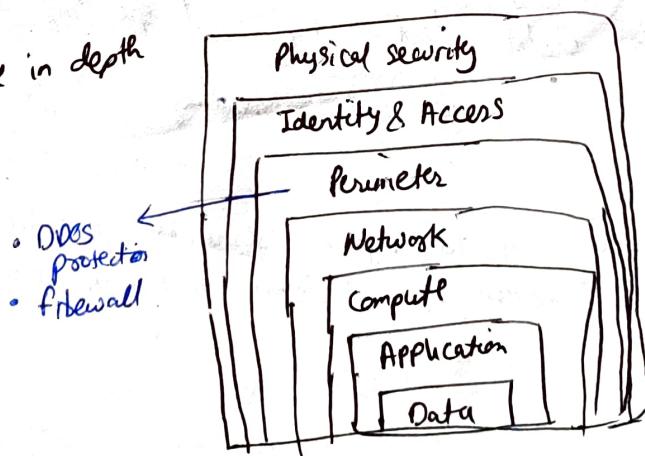
Azure Active Directory Domain services (Azure AD DS) : it is service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP) & Kerberos/NTLM authentication.

## 2) Azure Role-based access control (Azure RBAC)

Azure provides built-in roles that describe common access rules for cloud resources. You can define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all associated access permissions at application or data level.

Azure RBAC doesn't enforce access permission at application or data level.

Layers of defense in depth



Zero trust :- is a security model that assumes the worst case scenario & protects resources with that expectation.

# Azure Cost Management

(19)

CapEx vs OpEx

OpEx cost can be impacted by many factors:

- 1) Resource type
- 2) Consumption
- 3) Maintenance
- 4) Geography
- 5) Subscription type
- 6) Azure Marketplace

2 calculators for azure cost

1) Pricing calculator

2) Total cost of ownership (TCO)

Pricing calculator:

on cost of provisioned resources in Azure.

Pricing calculator focuses

TCO calculator: TCO calculator is designed to help you compare costs of running on-premises infrastructure compare to Azure Cloud.

## Azure Cost Management

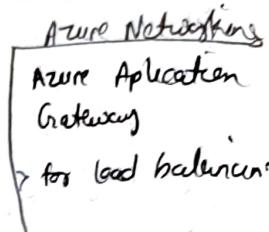
Cost management provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.

Cost analysis is subset of cost management that provide quick visuals for your Azure costs.

Cost alerts: provide a single location to quickly check on all of different alert types that may show up in Cost management service. Includes budget alerts, credit alerts, Department spending quota alert.

Budget: A budget is where you set a spending limit for Azure.

Tag: Resource tag are way to organize resources, just like resource group. Tags provide extra information, or metadata about your resources.



## Governance & compliance tools

- 1) Azure Blueprints :- lets you standardize cloud subscription or environment deployments. With Azure Blueprints you can define repeatable settings & policies that are applied <sup>whenever a</sup> new subscription is created.
- artifact : Each component in blueprint definition is known as artifact. Artifacts can also contain one or more parameters that you can configure.
- 2) Azure policy : Azure policy is a service in Azure that enables you to create, assign and manage policies that control or audit your resources. These policies enforce different rules across your resource configurations so that these configurations stay compliant with corporate standards.
- Azure Initiative : Azure Policy Initiative is a way of grouping related policies together. <sup>Policy</sup> Initiative definition contains all of the policy definitions to help track your compliance state for larger group.
- 3) resource lock : It prevents resources from being accidentally deleted or changed.
- 2 types of resource locks.
- 1) Delete : you can read & modify resource but can't delete
  - 2) ReadOnly : can only read, other actions are restricted.
- 4) Service Trust portal : This portal provides access to various content, tools & other resources about Microsoft security, privacy & compliance practices.

## Tools for managing & Deploying Azure resources

- Tools for managing environment
  - 1) Azure portal
  - 2) Azure Powershell
  - 3) Azure Command Line Interface (CLI)
- Azure portal : It is web-based, unified console that provides alternate to command-line tools, you can manage your Azure subscription by using graphical user interface, you can:
  - 1) Build, manage & monitor everything from simple web apps to complex cloud deployment
  - 2) Create custom dashboards for an organized view of resources
  - 3) Configure accessibility options for optimal experience

2) Azure cloud shell : Browser based shell tool that allows you create, configure & manage Azure resources

3) Azure powershell : It is a shell with which developers, DevOps and IT professionals can run commands called command-lets (cmdlets). These commands call Azure REST API to perform management tasks in Azure.

4) Azure CLI : Functionally equivalent to Azure Powershell with primary difference being syntax of commands. While Azure Powershell uses powershell command, Azure CLI uses Bash commands.

5) Azure Arc : Arc lets you extend your Azure compliance & monitoring to your hybrid & multi-cloud configurations.

Basically it also manages non-Azure resources, means manage resources hosted outside of Azure.

Azure resource manager (ARM) : It is the deployment & management service for Azure. It provides management layer that enables you to update, create and delete resources in your azure account.

- ARM template : With ARM you can manage your infrastructure through declarative templates rather than scripts. ARM template is JSON file that defines what you want to deploy in Azure.

Infrastructure as a code : It is a concept where you manage your infrastructure as line of code. Can use Azure cloud shell, CLI or powershell and also ARM template for this purpose.

## # Monitoring tools. ( $\geq$ 8 Pcs)

1) Azure Advisor : It evaluates your Azure resources & make recommendations to help improve reliability, security and performance, achieve operational excellence & reduce cost.

2) Azure Service Health : It helps you keep track of Azure resources, both your specifically deployed resources & overall status of Azure.

3) Azure monitor : It is a platform for collecting data on your resources, analyzing that data, visualizing the information and even acting on results. Azure monitor can monitor Azure resources, your on-premises resources, and even multi-cloud resources like VM hosted with different cloud provider.

• Azure insight : Tool of Azure monitor, that monitors your web applications

• Azure log Analytics : Run & write log queries on data collected by Azure monitor