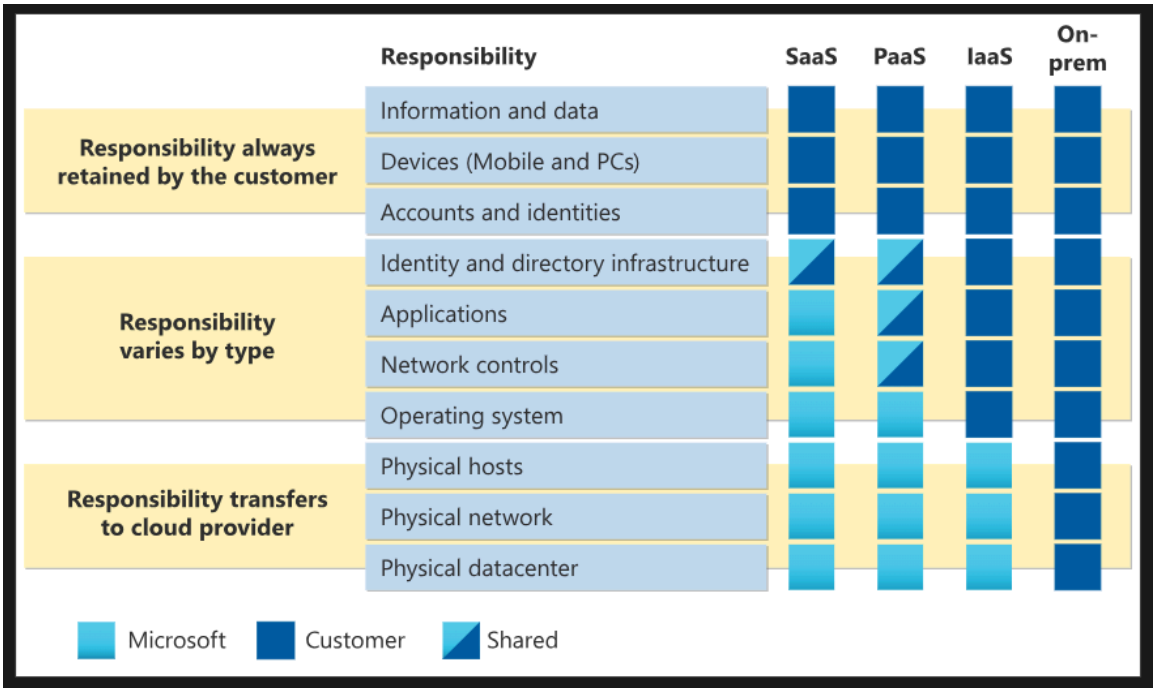
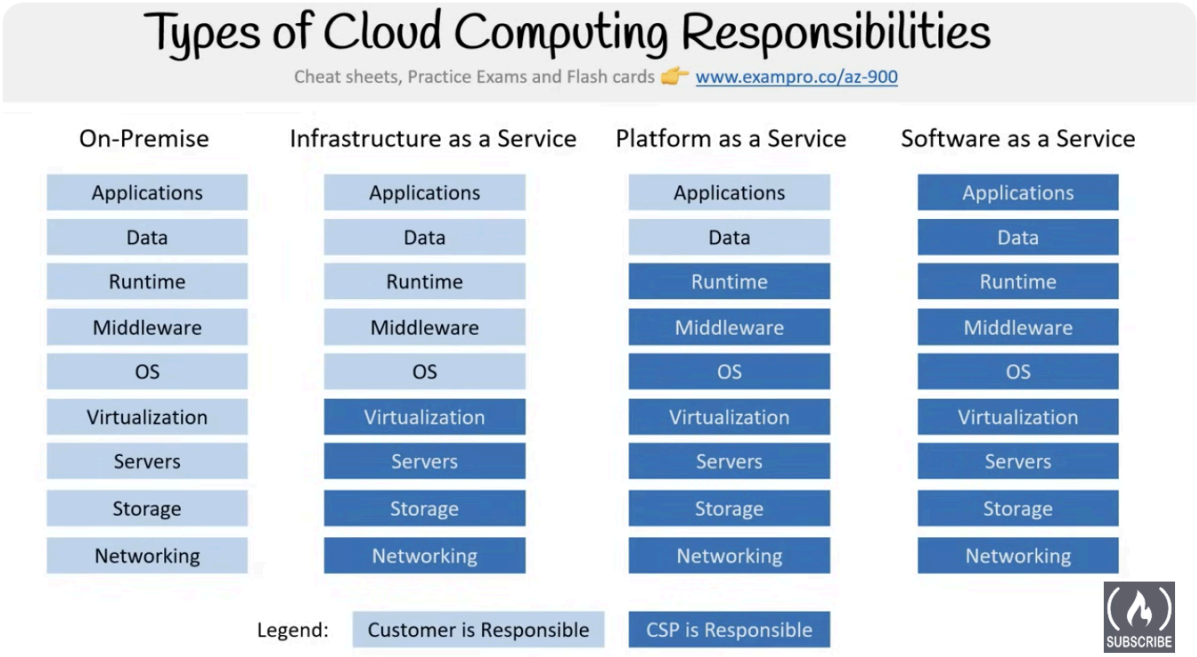
Cloud Concepts

- Cloud Computing is the practice of using network of remote servers hosted on the internet to store, manage and process data instead of a local sever or pc OR the delivery of computing services over the internet by using a pay-as-you-go pricing model. You typically pay only for the cloud services you use
- Cloud Providers basic services are: compute power (processing volume) & storage (volume of data like hard drive)
- Evolution of computing: Dedicated server → Virtual Machines (VM) → Containers (software name - docker deamon) → Functions (managed VMs running managed containers, also known as serverless compute. The most cost-effective)
- Dedicated server: one physical machine for a single business, Virtual Private Server (VPS): one physical machine for a single business virtualized into sub-machine, Shared hosting: one physical machine shared by hundred of businesses, Cloud Hosting: Multiple physical machine that act as one system, broken down into multiple cloud services
- Common Cloud Services for IaaS (Compute, Storage, Networking, Databases)
- Azure: Microsft Cloud Provider Service
- Benefits: PAYG, Go global, Secure by default, Reliability, Scalability, Elasticity, Current (always upgraded)
- Types of Cloud Computing: SaaS (for customers, scenarios: Email & Messaging, Business Productivity Applications, Finance & Expense Tracking), PaaS (for developers, scenarios: Development framework, Analytics/business intelligence), IaaS (for admins, scenarios: Lift-and-Shift Migration, Testing & Development)
- Cloud Computing Responsibilities: ***IaaS places the most responsibility on the consumer,*** with the cloud provider being responsible for the basics of physical security, power, and connectivity. On the other end of the spectrum, SaaS places most of the responsibility with the cloud provider. ***PaaS*** (Azure Storage accounts and Azure App Service), being a middle ground between IaaS and ***SaaS (MS 365) can automatically scale without any manual intervention,*** rests somewhere in the middle and evenly distributes responsibility between the cloud provider and the consumer.





- Azure Deployment Models: Public Cloud, Private Cloud/On-Premise (Openstack), Hybrid, Cross-Cloud (Multiple cloud providers aka multi-cloud, hybrid-cloud)

Public cloud	Private cloud	Hybrid cloud
No capital expenditures to scale up	Organizations have complete control over resources and security	Provides the most flexibility
Applications can be quickly provisioned and deprovisioned	Data is not collocated with other organizations' data	Organizations determine where to run their applications
Organizations pay only for what they use	Hardware must be purchased for startup and maintenance	Organizations control security, compliance, or legal requirements
Organizations don't have complete control over resources and security	Organizations are responsible for hardware maintenance and updates	

- Azure Arc: Set of technologies that helps manage cloud environment whether public, private, hybrid or multi-cloud
- Azure VMware Solution: Want to migrate from private cloud to a public or hybrid cloud? Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability

Azure's Deployment Models

Cheat sheets, Practice Exams and Flash cards 👉 www.exampro.co/az-900

	Cost	Security	Level of Configuration	Technical Knowledge
Public Cloud	👍 Most cost-effective	👍 Security Controls by Default 👎 Might not meet security requirements	👎 Limited based on what the Cloud Service Provider exposes to you.	👍 You don't need in-depth knowledge of underlying infrastructure
Private Cloud	👎 Most expensive	👎 no guarantee its secure 👍 can meet any security compliance requirement if you put in the work.	👍 You can configure the infrastructure however you like.	👎 You need to know in-depth how to configure all levels of your infrastructure
Hybrid	👍👎 Could be more cost-effective based on what you offload to the cloud.	👎 you now have to secure your connection to the cloud 👍 can meet all security requirements	👍 You get the best of both worlds.	👎 You need to know in-depth how to configure all levels of your infrastructure and know the CSPs services.

SUBSCRIBE

- Solution architect: Architecting technical solutions using multiple system via researching, documentation and experimentation while Cloud architect: Architecting technical solutions using cloud srevices. Business requirements to consider are availability, scalability, elasticity, fault tolerance, and disaster recovery while Business factors are security and cost

Benefits of Cloud

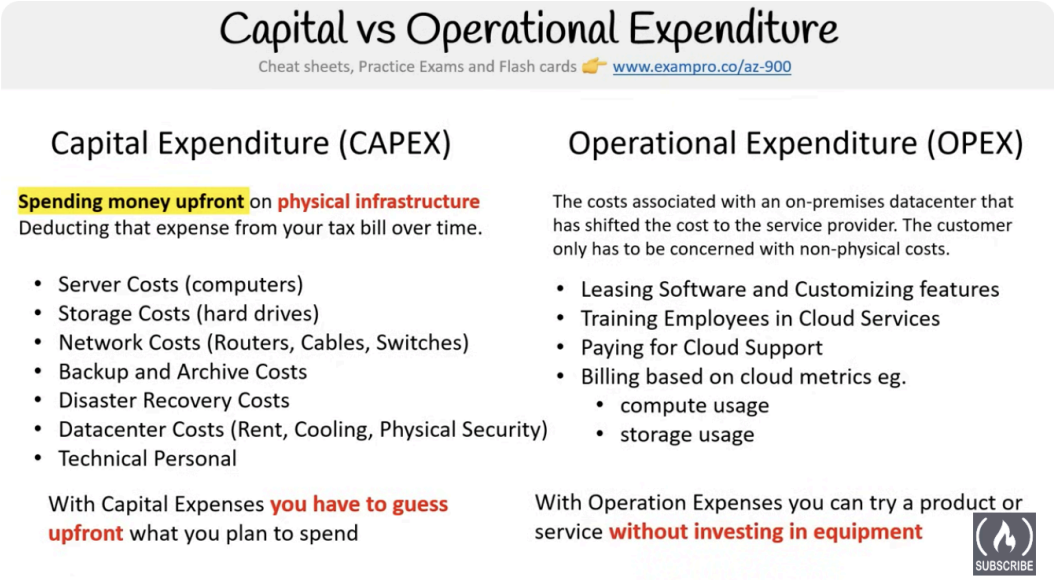
- Availability (Uptime): Means that cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong. Azure load balancer allows to evenly distribute traffic to multiple servers in one or more datacenter. Different services have different SLAs, sometimes different tiers of the same service will offer different SLAs, which can increase or decrease the promised availability.
- Agility means that you can deploy and configure cloud-based resources quickly as app requirements change.
- Scalability: Vertical scaling (scaling up) is focused on increasing or decreasing the capabilities of resources e.g., adding more memory (CPU/RAM) to one server while horizontal severe (scaling out) is adding or subtracting the number of resources.e.g, adding more servers, VMs, containers
- Elasticity: Autoscaling. Increase or decrease capacity based on demand, traffic, or computing power. Mostly associated with horizontal scaling as vertical scaling is difficult for traditional architecture. Azure VM scale sets or SQL severe stretch database are tools used.
- Reliability: Ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework.
- Predictability: Performance predictability (Autoscaling, load balancing, and high availability) or cost predictability (predicting or forecasting the cost of the cloud spend using TCO).
- Fault tolerance: no singlepoint of failure by using failovers (shift traffic to a redundant/secondary system in case the primary system fails) e.g., ***Azure Traffic Manager (DNS based traffic balancer)***
- Durability: Recover from disaster & prevent loss of data.

Management & Governance

Cost Management

- TCO (***Understand & compare*** cost savings of operating solution on Azure compared to on-premises), Pricing Calculator (***Determine & Estimate Azure services*** that fit budget), Azure Advisor (Monitor actual costs, Recommendation & Optimization) are tools to helps understand costs & savings when moving to the cloud
- Total Cost of Ownership (TCO) - 75% when you move from on-premises to azure
- Cost Management: Cost Alerts (Budget alerts, Credits alerts (Works for Enterprise Agreement), Department spending quota alerts (Works for Enterprise Agreement (EA), can be configured in EA portal) AND Budgets
- Tags are used to organize related resources & place them in their own subscriptions. It is useful for: Resource Management, Cost Management & Optimization, Operations Management, Security, Governance & Regulatory Compliance, Workload Optimization & Automation.

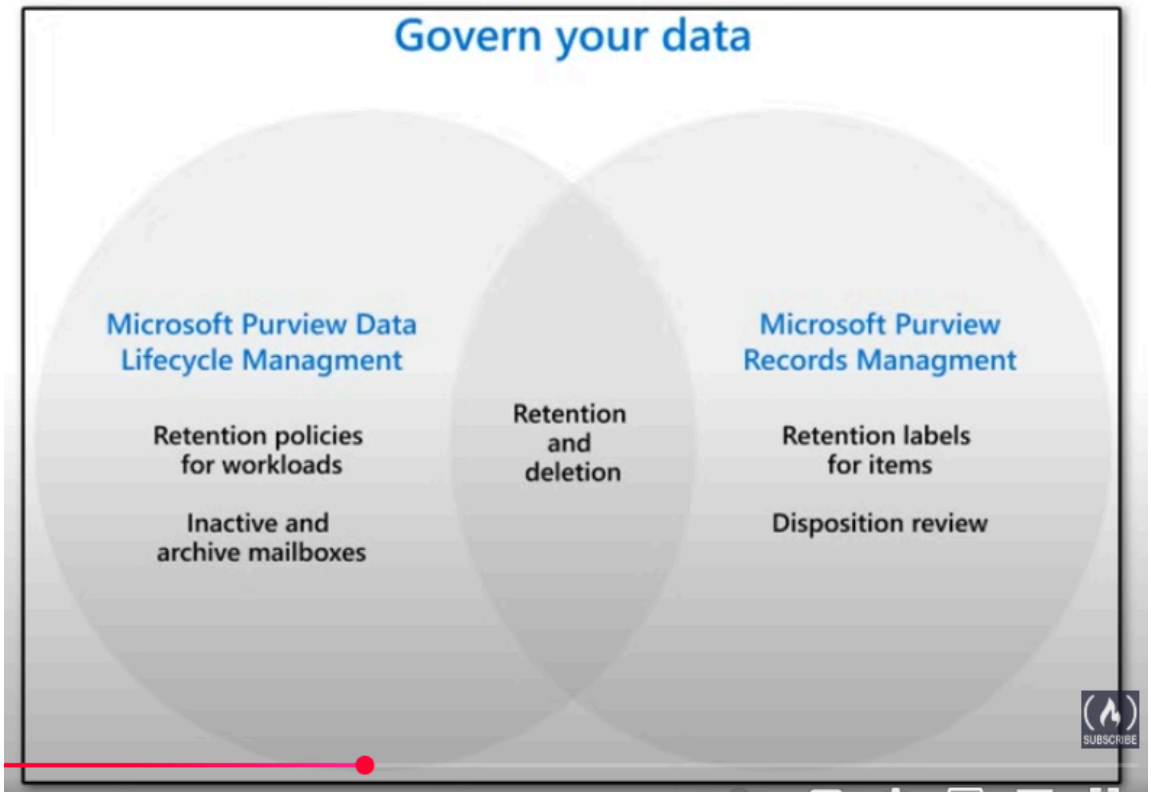
- Azure Reservations can be used to minimize the costs of VMs without reducing the functionality of the VMs. You commit to a one-year or three-year term plan. However, you have the option to pay your Azure reservations monthly instead of an upfront payment, allowing you to spread out the cost.
- Cloud computing operates on a consumption-based model (OpEx). OpEx costs depends on Resource type, Consumption, Maintenance, Geography, Subscription type, Azure Marketplace
- Capital expenditure (CapEx) - physical infrastructure costs, Operational Expenditure (OpEx) - non-physical costs



Governance & Compliance

- Microsoft Purview Information Protection: Collection features within MS purview to help discover, classify & protect sensitive info wherever it lives/travels. Know your data (sensitive info types, trainable classifiers, data classification), Protect your data(sensitivity labels, double key encryption, microsoft defender for cloud etc), Govern your data, Prevent data loss.
- MS Purview areas: Risk & Compliance, Unified Data Governance
- Microsoft Purview Data Loss Prevention (DLP):
- Microsoft Purview Data Lifecycle Management (formerly MS Information Governance): Collection of features to govern data for compliance or regulatory
- Microsoft Purview Records Management: Manage high-value items for business/legal/regulatory record-keeping requirements

Data Catalog — This enables data discovery.
Data Sharing — This shares data within and between organizations.
Data Estate Insights — This accesses data estate health.
Data Policy — This governs access to data.



- Azure Policies: Enforce organization standards & assess compliance at-scale both at individual and group level. Policies don't restrict access, they only observe for compliance. Components are: Policy Definitions, Policy Assignment, Policy Parameters, Initiative Definitions
- Resource Locks: Lock subscription, resource group or resource to prevent other users from accidentally deleting or modifying said resources. CanNotDelete or ReadOnly modes)
- Resource Group: A container that holds related resources for an Azure solution. A resource group's permission will be inherited by the resources inside it. Resources can connect to other resources located in another resource group.
- Microsoft Service Trust Portal is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices. Needs MS Entra account/authenticated user with your Microsoft cloud services account to be able to access some of the resources on the Service Trust Portal.
- Azure Blueprints: Enable quick creation of governed subscriptions (process/expectations of how the subscription should be set up). Blueprints can be used based on common artifacts.

Managing & Deploying Azure Resources

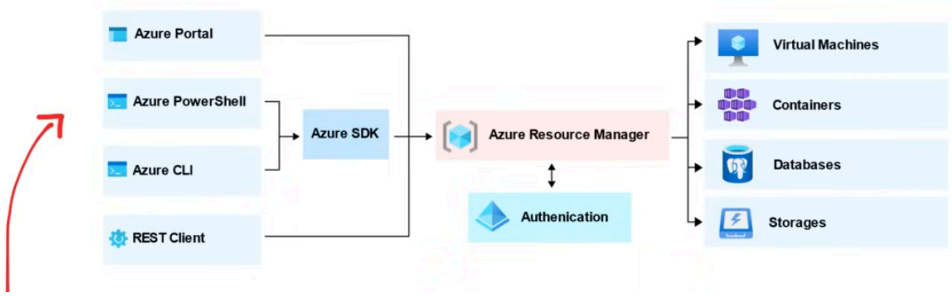
Azure Management Tools

- ARM Template are stored locally or in source control while Azure Blueprints is the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) & supports improved tracking and auditing of deployments
- Azure Portal: Web-based graphic unified console that provides alternative to command-line tools. Azure subscriptions can be managed from Portal
- Azure Preview Portal: Utilize new features that are in preview, beta or pre-release
- Azure Arc is a control pane that can manage compute resources (Servers, Kubernetes Clusters, Azure Data Services, SQL Server, VM Preview) across cloud providers, on-premises and at the edge. Arc lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.
- Azure Cloud Shell: Interactive, authenticated, ***browser-accessible shell*** for creating, configuring, managing Azure resources. It provides flexibility of choosing shell experience of choice (Azure PowerShell or Azure CLI)
- PowerShell: Task automation & configuration management framework. Command Line Shell & scripting language
- Azure PowerShell: Set of cmdlets for managing Azure resources directly from the PowerShell command line. The commands call the Azure REST API to perform management tasks in Azure
- Azure CLI: CLI processes commands to a computer program in the form of lines of text. Azure CLI uses bash commands and can be installed on Windows, Mac or Linux. Azure CLI commands can be used to create, update, delete, view & mange Azure resources.
- Visual Studio Code: Free source-code editor made my MS for Windows, Linux & MacOS

Azure Resource Manager (ARM)

- ARM is a service that allows you to manage Azure resources
- It is a collection of service that makes up management layer that allows: Create, update, delete resources; Apply management feature, Writing IaC.
- Features that make up ARM layer are: Subscriptions (grant access to Azure services based on billing & support agreement), Management Groups (logical grouping of multiple subscriptions), Resource Groups (logical grouping of multiple resources in a subscription), Resource Providers, Azure Blueprints, Resource Tags, Acces Control (IAM), RBAC, Azure Policies, & ARM Templates
- Gatekeeper that allows flow of requests and decides whether the request can be performed on a resource
- Scoping: Boundary of control for Azure resources and a way of governing by logical grouping & applying restrictions

- Bicep is a language that uses declarative syntax to deploy Azure resources. A Bicep file defines the infrastructure and configuration. Then, ARM deploys that environment based on your Bicep file. While similar to an ARM template, which is written in JSON, Bicep files tend to use a simpler, more concise style.
- Azure IaC examples: ARM Templates, Bicep, Terraform
- ARM Templates: IaC. Process of managing and provisioning computer data centers (e.g, Azure) through machine-readable definition files (e.g. JSON files) rather than physical hardware configuration or interactive configuration tools. ***It can be declarative or imperative***. They are ***JSON files*** that define Azure resources that you want to provision & Azure services that you want to configure. They can be ***exported.***



With ARM templates you can:

- **ARM templates** are declarative. (you get exactly what you define)
- stand up, tear down or share entire architectures in minutes
- Reduce configuration mistakes
- Establish an architecture baseline for compliance
- **Modularity** Break up your architecture in multiple files and reuse them
- **Extensibility** Add PowerShell and Bash scripts to your templates
- **Testing** You can use the ARM template tool kit (arm-ttk)
- **Preview Changes** Before you create infrastructure via template, see what it will create
- **Built-In Validation** Will only deploy your template if it passes
- **Tracked Deployments** Keep track of changes to architecture over time
- **Policy as Code** Apply Azure policies to ensure you remain compliant
- **Microsoft Blueprints** (establishes relationship between resource and the template)
- **CI/CD integration**
- **Exportable Code** (exporting the current state of a resource groups and resources)
- **Authoring Tools** Visual Studio Code has advanced features for authoring ARM templates

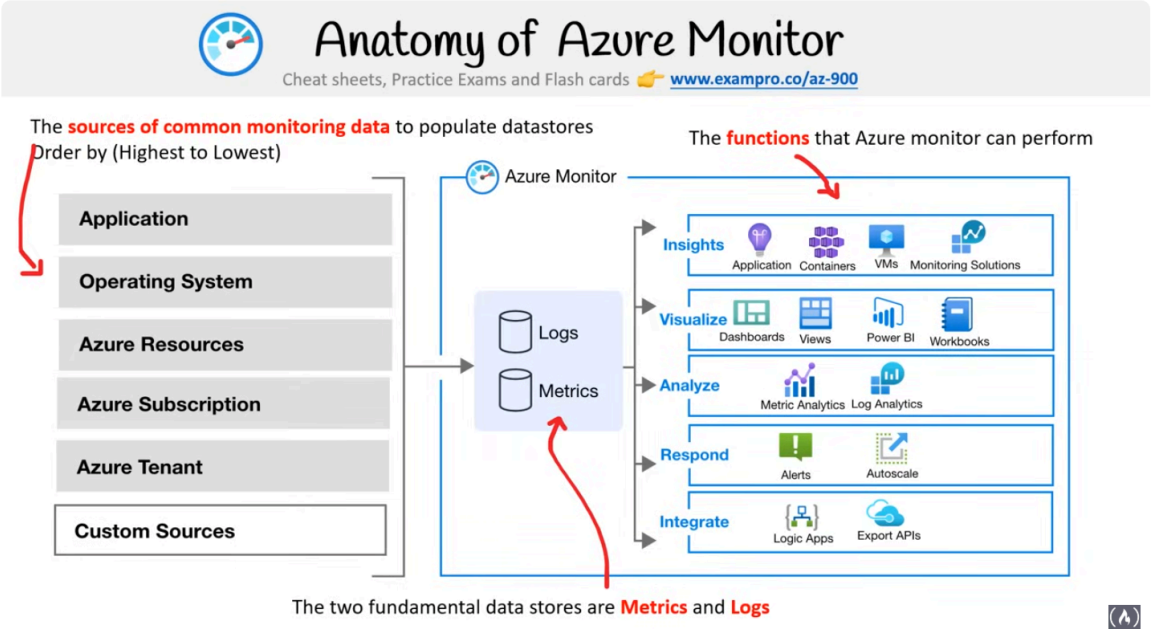
- Management of resources in the cloud can be done through: Web portal, Command Line Interface (CLI), APIs, PowerShell

Monitoring Tools

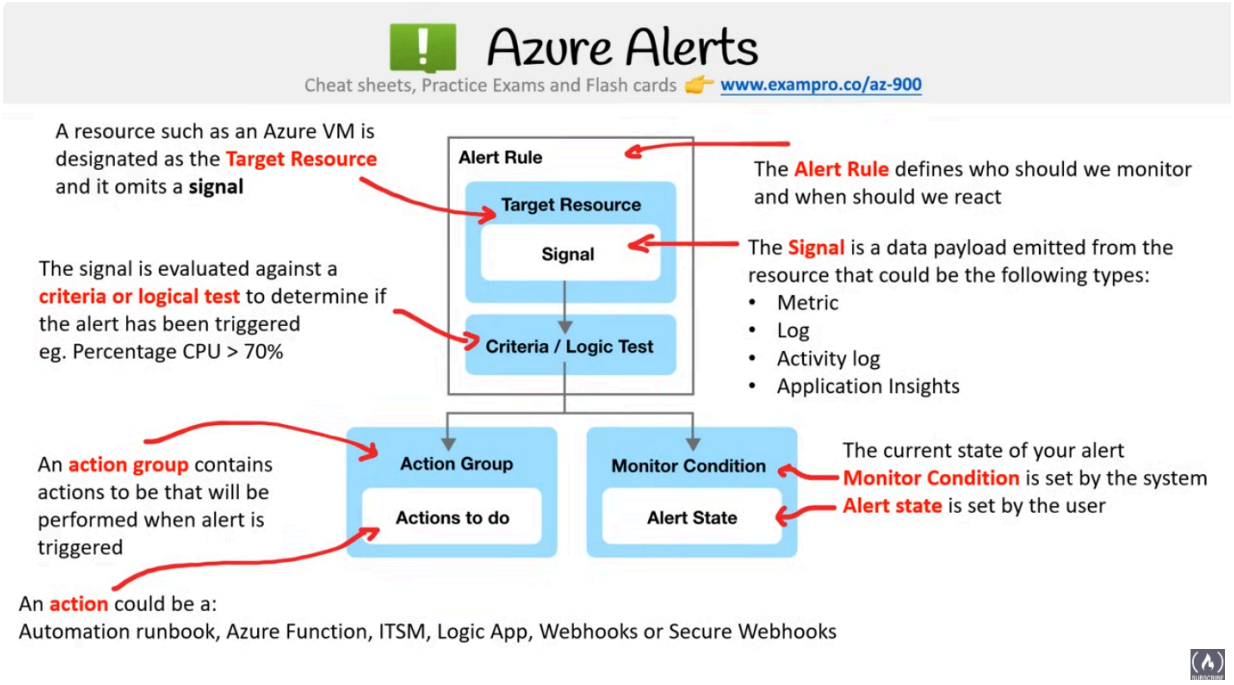
- ***Azure Advisor***: Personalized cloud consultant that helps follow best practices to optimize Azure deployments. It ***evaluates your Azure resources & recommends*** based on: Reliability/High availability, Security, Performance, Cost, Operational Excellence. The recommendations are available via the Azure portal and the API, and you can set up notifications to alert you to new recommendations. ***Analyzes your***

resource configuration and usage telemetry and then recommends solutions that can help you improve the cost-effectiveness, performance, reliability, and security of your Azure resources

- **Azure Monitor**: Comprehensive solution for collecting, analyzing & acting on **telemetry** from on-premises and cloud environments into ***centralized repository***. Create dashboards, smart alerts, automated actions & log monitoring. Many Azure services are by default already sending telemetry data to Azure Monitor. Use Cases: Generate an alert if virtual machine utilization is over 80% for five minutes, Create a custom solution that uses thresholds to trigger autoscaling functionality to scale an app up or down to meet user demand
- Pillars Of Observability: Needs metrics (number measured over time), logs (text files where each line contains event data that happened at a certain time) & traces (history of request that travels through multiple apps/services that pin-point performance or failure)
- Anatomy of Azure Monitor



- Log Analytics: Tool used to edit & run log queries with data in Azure Monitor Logs. Uses query language called KQL
- Log Analytics Workspaces: Unique environment for Azure Monitor Log data. Each workspace has is own data repo & configuration while data sources & solutions are configured to store their data in a particular workspace
- Azure Alerts: Types are: Metric, Log & Activity Log. It comprises of Alert Rule, Signal,



- Application Insights: ***Application Performance Management (APM) service for developers and DevOps professionals***. Sub-service of Azure monitor. Use cases of Application Insights are: Detect performance anomalies, Analytics tools to diagnose and understand how users use apps, Works for apps on a for NET, Node.js, Java, and Python hosted on-premises, hybrid, or any public cloud, Integrates with your DevOps process, Monitor and analyze telemetry from mobile apps by integrating with Visual Studio App Center. You need to instrument your app (***enable SDK***) to be able to use it.

What does Application Insights Monitor?

- Request rates, response times, and failure rates
- Dependency rates, response times, and failure rates
- Exceptions
- Page views and load performance
- AJAX calls
- User and session counts
- Performance counters
- Host diagnostics
- Diagnostic trace logs
- Custom events and metrics

Where do I see my telemetry?

- Smart detection and manual alerts
- Application map
- Profiler
- Usage Analysis
- Diagnostic search for instance data
- Metrics Explorer for aggerated data
- Dashboards
- Live Metrics Stream
- Analytics
- Visual Studio
- Snapshot debugger
- Power BI
- REST API
- Continuous Export

- Application Performance Management (APM): Monitoring & management of performance & availability of software apps. It strives to detect & diagnose complex application performance problems to maintain an expected level of service.

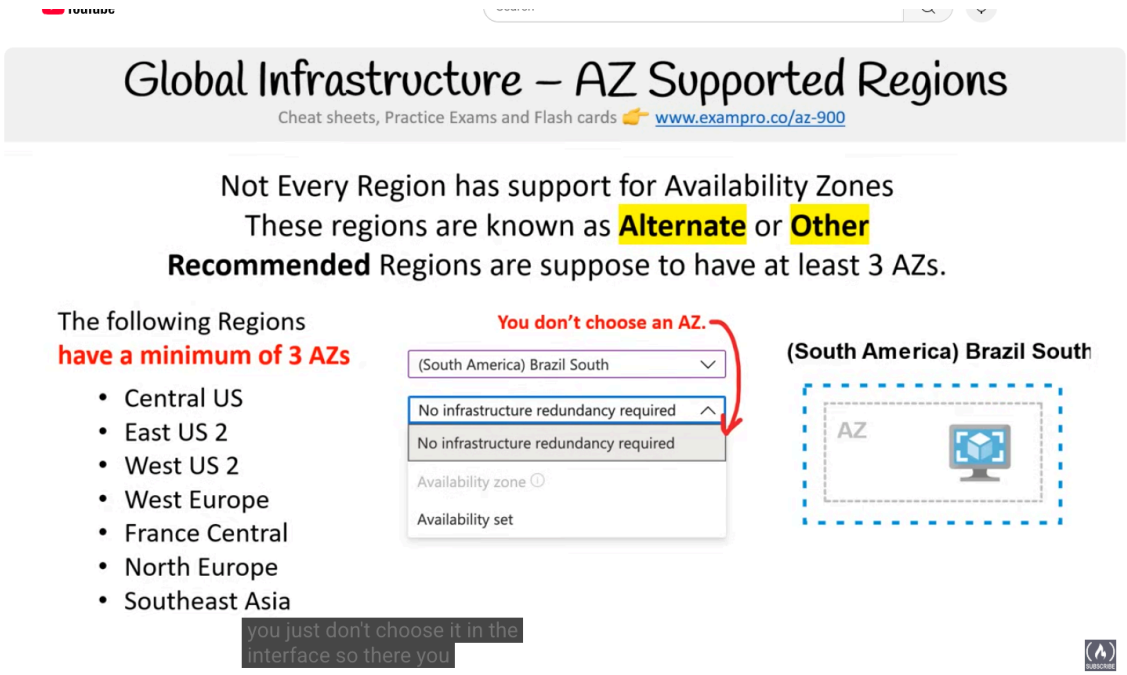
Azure Service Health

- Info about current and upcoming issue e.g., service impacting events, planned maintenance and other changes that may affect availability
- Azure Status informs about service outages and the health of all the Azure resources that you're using and other Azure services across all Azure regions.
- Azure service health shows planned maintenance, personalized view of health of Azure Service and regions you're using and links to support if a workload you're running is impacted by an event. Review the root cause analysis (RCA)
- Azure resource health shows info about the health of your individual cloud resources

Azure Architecture & Services

Architectural Components

- Physical Infrastucture are Datacenters while Management Infrastucture includes Azure resources and resource groups, subscriptions, and accounts.
- Resources → Resource Group → Subscription → Management Groups
- Subscriptions are unit of management, billing and scale. Subscription boundaries are: Billing Boundary & Access Control Boundary. They can further be separated into: Environment, Organizational structures, Billing
- Management Group: manage access, policies, and compliance for subscriptions
- AZs: Physically separate datacenters within an Azure region. One or more datacenters. Combination of fault domain (logical grouping of hardware to avoid single point of failure within an AZ) and update domain (ensure resources don't go offline). Set up with isolated boundary.
- Azure services that support AZs fall into three categories: Zonal services, Zone-redundant services & Non-regional services:Datacenter: Building that contains hundreds of thousands of computers.
- Region: Grouping of multiple datacenters or AZs, mostly 3 AZs close enough to provide low latency. Specialized regions are for compliance/legal reasons
- Region Pair: When Azure regions appeared with another region within the same geography at least 300 miles away, this allows for the replication of resources across a geography to reduce events like natural disasters, civil unrest, power outages etc. E.g: West US paired with East US, South-East Asia paired with East Asia. Some azure services rely on paired regions for disaster recovery



- Sovereign Regions: Isolated from the main instance of Azure, may be used for compliance or legal purposes. Examples: US DoD Central, US Gov Virginia, US Gov Iowa, China East, China North
- Geography: Market of 2/more regions that preserves data residency and compliance boundaries; US, Canada, Brazil, Mexico Azure govt (US). Not all services are available in all regions. 58 regions, 140 countries.
- A zone is a geographical grouping of Azure regions for billing purposes.
- Azure cloud services are categorized into three:

General availability (GA) is when a service is considered ready to be used publicly by everyone.

Azure Cloud services are grouped into **three** categories.
Their category determines when cloud services become available:

1. **Foundational.** When GA, immediately or in 12 months in Recommended and Alternate Regions
2. **Mainstream** When GA immediately or in 12 months in Recommended Regions
   May become available in Alternate Regions based on customer demand
3. **Specialized.** Available in Recommended or Alternate Region based on customer demand.

- Availability set is logical grouping used in Azure to ensure VMs placed in the availability set are different fault/update domain to avoid downtime. Each VM in Availability set are assigned fault domain & update domain
- Container Instances: docker as a service, stateless by default
- Azure Kubernetes Service (AKS): Kubernetes as a service, containerized apps
- Azure Service fabric: Tier-1 Enterprise containers as a service

- Azure Functions: Event-driven, serverless compute. Runs code without the need of provisioning and managing a server.
- Azure Batch: Plan, schedules & execute batch computer workloads across running 100+ jobs in parallel. It uses spot VMs to save money

Compute & Networking Services

VMs

- VMs are the most common type of compute, IaaS, highly configurable server (choose storage disks/compute, size/memory, storage). 20 VMs per region, ***billed per second***. N.B: Azure doesn't support VHDX format, only fixed VHD
- Azure VM scale sets helps automatically increase or decrease VM capacity
- VM can be grouped into: Update Domain, Fault Domain
- Load balancer (e,g., application gateway for HTTP/HTTPS and Azure load balancer for TCP/UDP) can be associated with sacle sets coz it distribute VMs cross multiple AZ and allow for more robust health checks. Public Load Balancers are used to load balance Internet traffic to your VMs.
- Scaling policy determine when VM should be added/removed (scale in/out) to meet capacity requirements. **Scale-in policy** (default, newest VM, oldest VM) determines what VM is removed (d) to decrease the capacity of the Scale Set while **update policy** (automatic, default, rolling) determine how VM instances are brought up-to-date with the latest scale set model
- Health monitoring determine if server is healthy or unhealthy. Modes are application health extension (ping) & load balancer probe (needs to have a load balancer attached to the VM). Automatic repair policy is advised to be turned on
- **Azure Virtual Deskto**p is a desktop & app virtualization service that runs on the cloud. Enables ***secure & remote work*** on any device, reduce cost of licensing & infrastructure, protect against outages, keep application & user data **secure using MS Entra ID, RBAC, MFA**. It is the only Windows client-based operating system that enables multiple concurrent users on a single VM
- The Custom Script Extension is an easy way to download and run scripts on your Azure VMs

Azure App Service

- PaaS. Can host Web Apps, API Apps, WebJobs, Mobile Apps. Supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python
- It offers automatic scaling and high availability. App Service supports Windows and Linux. It enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.
- HTTP-based service, takes care of underlying infrastructure

- Cannot be stopped. Pay based on an Azure App Service Plan (Shared Tier - 2 types which are Free (10 apps on an instance, compute quota of 60 mins in a day) & Shared Tier (100 apps on an instance, compute quota of 240 mins in a day), Dedicated Tier (Basic, Standard, Premium, PremiumV2 & Premium V3) and Isolated Tier).
- You choose Runtime (programming languages, libraries and framework).
- Azure App Servive allows you to define Custom container which is used for different runtime/bundle in a package/software.
- Deployment slot allow creatine of different environment of web app associated to a different hostname (Swap environment - blue-green deploy).
- App Service environment (ASE) is an Azure App Service feature that provides fully isolated & dedicated environment for securely running app service apps at high scale, pricing Tier is Isolated Tier. Deployment types are External ASE (exposes ASE-hosted app on an internet-accessible IP address) & ILB ASE (exposes ASE-hosted app on IP address inside your VNet, internal endpoint is Internal Load Balancer (ILB))

Azure Container

- Containers = Virtualization Environment
- Package, scale, deploy & manage cloud applications. Can be used to split solutions into smaller, independent pieces e.g., split a website into a container hosting your front end, another hosting your back end, and a third for storage
- VM virtualize the hardware while containers virtualize the operating system. Decision to choose depends on flexibility need. If you need to completely control the environment then you should choose a VM, Otherwise, container would be the better choice because of the portability, performance characteristics and management capabilities
- Launch containers without worrying about underlying VMs.
- Container Instances: PaaS, Fully managed ***docker*** as a service, stateless by default, containerized apps
- Container groups are collection of containers that gets scheduled onn the same host machine and similar to Kubernetes pod. The container in the group share lifecycle, resources, local network and storage volumes. Ways to deploy are Resouce Manager Template (ARM Template) & YAML file
- Container restart policyspeciifies what a container should do when their process is complete. They are ‘Always’, ‘Never’, & ‘OnFailure’
- Env Var allow passing configuration details to containers. Can be set through azure Portal, CLI or PowerShell
- Persistent Storage: mount external volume
- Azure Kubernetes Service (AKS): Kubernetes as a service, containerized apps, container orchestration service (manages lifecycle of containers)

Hence, these are the correct descriptions for the following Azure Compute services:

– Azure Container Instances – Microservice architecture.

– Azure Virtual Machines – Total control over the operating system.

– Azure App Service – Allows you to build and host web apps without managing infrastructure.

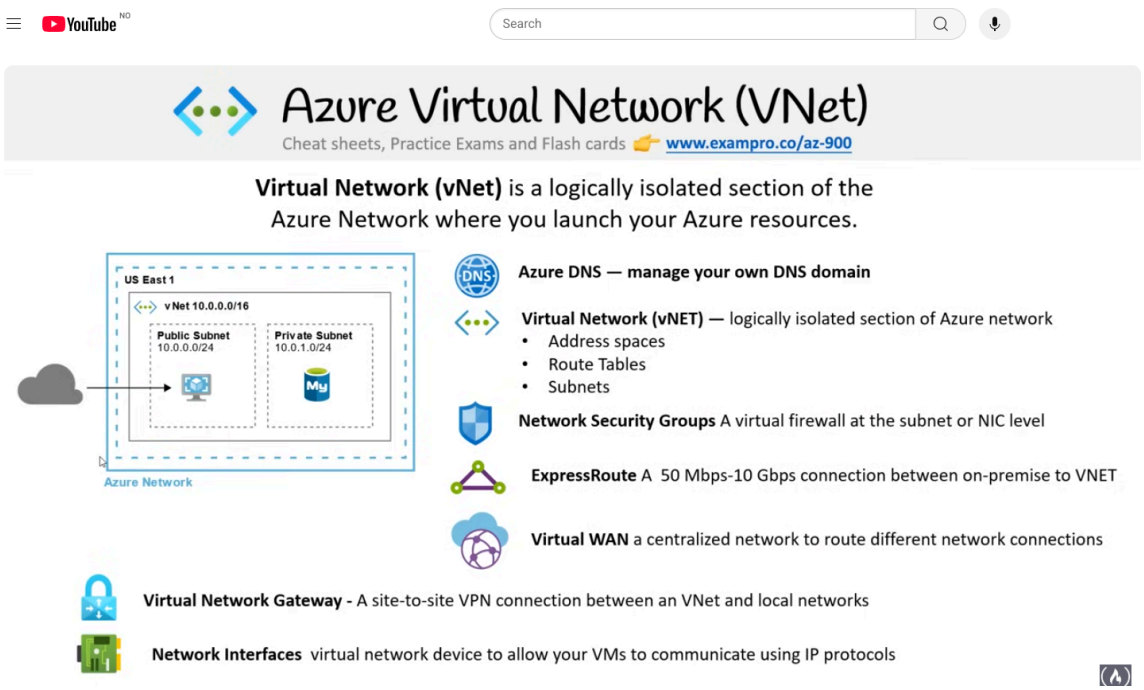
– Azure Functions – Serverless offering that doesn't require maintaining virtual machines or containers.

Serverless Services

- Serverless is when underlying servers, infrastructure and OS is taken care of by cloud service provider. Highly available, scalable & cost effective
- **Event-Driven Scale**: Serverless function that can be triggered or trigger other events allowing you to compose complex apps, **Abstraction of Servers**: Servers are abstracted away, code is described as functions which can be running on different compute instances, **Micro-billing**: Serverless compute could run for a fraction of a second. Billing into micro-seconds will save money
- Azure Functions: Event-driven, serverless compute option that doesn't require maintaining virtual machines or containers. Run smalls mounts of code as serverless functions in fav language and not worry about underlying server/infrastructure. Can be stateless (default) or stateful (Durable Functions)
- Blog Storage: Serverless object storage. Just upload files without thinking of underlying systems or resizing
- Logic Apps: Build serverless workflows composed of Azure Functions. Build a state machine for serverless compute
- Event Grid: Uses Pub/Sub messaging system to allow you react to events & trigger other Azure cloud services like Azure Functions

Azure Virtual Network (VNet)

- Logically isolated section of azure network where Azure resources are launched



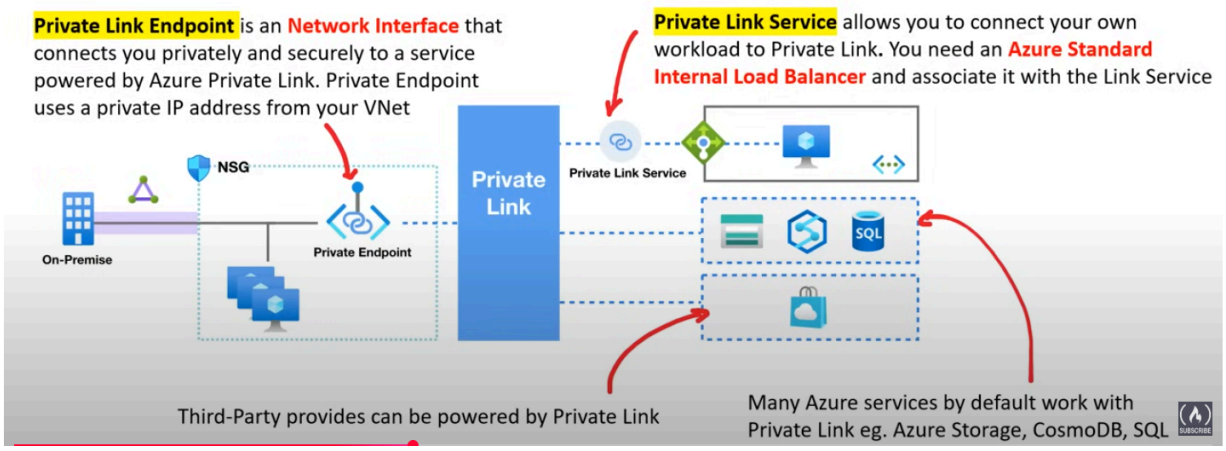
- VNet peering is when you connect multiple VNet to act as one network. Types are Regional & Global

Virtual Networking

- Network Interface is a Software or hardware interface between two pieces of equipment or protocol layers in a computer network while Network Interface Controller (NIC) is a computer hardware component that connects a computer to a computer network. Also known as: network interface card, network adapter, LAN adapter, physical network interface
- Azure Network Interfaces are attached to Azure VM instance. Without an NIC, An Azure VM instance would have no way to communicate. An Azure VM instance has to have an NIC and can have multiple NICs.
- Subnets: Logical division of access space. It needs route table & Network Security Group (NSG). Types are Public & Private (private has to be configured by enabling Internet Getway (IG))
- DNS is responsible for translating service name to IP address while Azure DNS is used for hosting service for DNS domain that provides name resolution by using Microsoft Azure infrastructure. You can't use Azure DNS to buy domain name
- VPN allows send & receive data across shared or public network. **Point-to-site VPN** connections are for individual networks to virtual networks and/or from a computer outside your organization back into your corporate network (e.g., the client computer initiates an encrypted VPN connection to connect to the Azure virtual network). **Site-to-site VPN** link your **on-premises VPN device or gateway to the Azure VPN gateway in a virtual network,** VPN connection, works over IPSec and connects on-premises to Azure virtual network. Requires VPN device located on-premises, Works

over public internet. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet. **Network-to-network VPN** connect virtual network to other virtual networks

- Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.
- **In Route-based gateways**, IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets. ***Use a route-based VPN gateway for: Connections between virtual networks, Point-to-site connections, Multisite connections, Coexistence with an Azure ExpressRoute gateway***
- **Azure Express Route** creates private connection (not over internet) between Azure datacenters & infrastructure on your ***premises*** or in a colocation environment to MS Office, Dynamic 365 & Azure Compute, Cloud services. Not a VPN connection but connect on-premises to Azure network through connectivity provider. Doesn't pass through public internet. Connectivity can be from an: **any-to-any (IP VPN) network, a point-to-point Ethernet network, CloudExchange colocation, Directly from ExpressRoute sites. Benefits of ExpressRoute are: Global Connectivity, Dynamic Routing via Border Gateway Protocol, Built-in redundancy in every peering location**
- ***ExpressRoute connections and Azure VPN Gateway are two services that you can use to connect an on-premises network to Azure.***
- Service endpoints are used to expose Azure services to a virtual network, providing communication between the two. Works for only azure services. Provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks.
- Network Security Group (NSGs) allow you to configure inbound and outbound rules for virtual networks and virtual machines.
- Azure Private Links allows you to establish secure connections between Azure resources so traffic remains within the Azure Network. Private Link Endpoint & Private Link Service



- Network security groups (can contain multiple inbound and outbound security rules) and network virtual appliances (specialized VMs that can be compared to a hardened network appliance) are used to filter network traffic between subnets. Subnet and Network interface can be attached to NSGs

Cloud-Native Networking Services

- Azure DNS: Based on Azure Resource Manager, Hosting service, Provide ultra-fast DNS response and ultra-fast domain availabilty. Benefits: Reliability and performance, Security, Ease of Use, Customizable virtual networks, Alias records
- Azure Virtual Network (VNet): Logical isolated section of Azure network for customers to launch Azure resources in.
- Azure Load Balancer: OSI Level 4 (transport) load balancer/regional balancer
- Azure Application Gateway: OSI Level 7 HTTP load balancer/regional balancer, can apply a WAF
- Traffic Manager: DNS based global traffic routing
- Network Security Groups: Virtual firewall at subnet level. CANNOT be attached to a virtual network or network interface
- Azure Firewall: Managed, cloud-based network security service that protects your Azure Virtual Network resources. ***Uses a static public IP address*** for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. Fully stateful firewall-as-a-service that allows you to centrally create, enforce, and log application and network connectivity policies across subscriptions and Azure virtual networks.

Azure Network Security Group	Filter network traffic to and from Azure resources in an Azure virtual network.
Azure VPN gateway	Connects your on-premises network to Azure virtual network.
Azure Application Gateway	Distribute traffic to your web applications.
Azure Virtual Network (VNet)	It is a logical isolation of the Azure cloud dedicated to your subscription.

Storage Services

- Azure Blob Storage: ***Object Serverless Storage for text and binary data. PAYG***
- Azure Disk Storage: ***Block-level storage volumes for Azure VMs. Disks for VM. Virtual volume. SSD/HDD***
- Azure File Storage: ***Fully-managed. File Shared volume that can be accessed and managed like a file server accessible by using Server Message Block (SMB) protocol. For cloud or on-premises deployments.***
- Azure Queue Storage: ***Messaging queue. Data store for queueing and delivering messages between apps component for cloud, desktop, on-premises or mobile devices. NoSQL.***
- Azure Table Storage: ***Wide-column NoSQL Database for key value pairs. For no schema, structured, non-relational data.***
- Azure Data Box: ***Rugged briefcase*** computer & storage designedto move terrabyte/petabytes of data
- Azure Archive Storage: Long-term cold storage Cheapest storage option
- Azure DataLink Storage: Centralized repo that allows structured and unstructured data
- Core storage services are Azure Blob, Azure Files, Azure Queues, Azure Tables, Azure Disks (Block-level storage volume for Azure VMs)
- Azure File Sync: Centralize & automatically updates your file shares in Azure Files/Cache Azure files shares on an on-premises Windows server or cloud VM. Uses protocols like SMB & NFS

Hence, these are the correct descriptions for the following Azure Compute services:

– Azure Container Instances – Microservice architecture.

– Azure Virtual Machines – Total control over the operating system.

– Azure App Service – Allows you to build and host web apps without managing infrastructure.

– Azure Functions – Serverless offering that doesn't require maintaining virtual machines or containers.

Storage Accounts

- Azure Storage Accounts provides ***unique namespace a***nd contains all azure storage data objects like blobs, files, queues, tables and disks. ***Billed monthly***
- Types are: ***Standard (General-purpose v1, General-purpose v2), BlobStorage (Premium Page Blobs), BlockBlobStorage (Premium Block Blobs), FileStorage (Premium File Shares)***. Storage accounts types vary with different features like: ***Supported services, Performance Tiers, Access Tiers, Replication and Deployment model.***

Type	Supported services	Redundancy Options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs	Blob Storage (including Data Lake Storage)	LRS, ZRS	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency.
Premium file shares	Azure Files	LRS, ZRS	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	LRS	Premium storage account type for page blobs only.

Type	Service	Performance Tiers	Access Tiers	Replication	Deployment Models
General-purpose V2	Blob, File, Queue, Table, Disk, Data Lake Gen 2	Standard, Premium	Hot, Cool, Archive	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Resource Manager
General-purpose V1	Blob, File, Queue, Table, Disk	Standard, Premium	N/A	LRS, GRS, RA-GRS	Resource Manager **Classic**
BlockBlobStorage	Blob (block, append)	Premium	N/A	LRS, ZRS	Resource Manager
FileStorage	File	Premium	N/A	LRS, ZRS	Resource Manager
BlobStorage	Blob (Block, append)	Standard	Hot, Cool, Archive	LRS, GRS, RA-GRS	Resource Manager

- Performance Tier for blob are standard & premium. Blob Storage Access Tier are ***Cool*** (infrequently accessed data, short-term backup, at least 30 days, Lower storage cost & higher access cost), ***Cold*** (infrequently accessed data, short-term backup, at least 90 days, Lower storage cost & higher access cost), ***Hot*** (frequently accessed data, Highest storage cost & lowest access cost), ***Archive*** (rarely accessed & stored for at least 180 days, Lowest storage cost & highest access cost)
- When a blob is uploaded or moved to another tier, it is charged at the new tier's rate immediately upon tier change.

Azure Blobs

- Object store for storing massive amounts of unstructured data. Can store binary or text data. Support big data analytics
- Components are domain, containers, data being stored (blobs)
- Types are ***block blobs*** (for binary data, managed individually), ***append blobs*** (for append operations, logging data from VM), ***page blobs*** (store random access files up to 8TB, store virtual HD files & serve as disks for Azure VM)

AZ Copy

- Copy blob/files to/from storage account. Upload files, Download files, Copy files between storage accounts, and even synchronize files. Can work with other cloud providers
- Command Line Utility
- Level of authorization are: Storage Blob Data Reader for download while Storage Blob Data Contributor & Storage Blob Data Owner to upload
- Gain access through Azure Active Directory (AD) & Shared Access Signature (SAS)
- Copy command is used to upload & download

Azure Storage Explorer

- Standalone app that provides graphical interface that makes it easy to work with Azure Storage Data and cloud storage services
- Can create blob containers, upload files and create snapshots of disks etc

- ***Azure Resource Explorer is primarily used to view the available Azure Resource Management APIs and make actual API calls directly to your own Azure subscriptions.***

Azure Files

- Fully managed file share in cloud
- Centralized server for storage that allows multiple connections
- One big shared drive for everyone in the VM
- Network protocol is used to connect to the file share (mounting)
- Azure Files offers fully managed file shares in the cloud that are accessible via industry-standard SMB and NFS protocols.
- Use cases are: can replace or supplement on-premises file server, left & shift on-premises storage to cloud via classic lift (where both the application and its data are moved to Azure) or hybrid lift (where the application data is moved to Azure Files, and the application continues to run on-premises), simplify cloud development (shared application settings, diagnostic share and dev/test/debug), containerization
- Advantages are: Shared Access, Fully Managed, Scripting & Tooling, Resiliency, Familiar Programmability

Replication & Data Redundancy

- Replication data redundancy is replication type of storage account that creates multiple copy of data to protect it. Types are: Primary Region redundancy, Secondary Region redundancy and Secondary Region redundancy with Read Access. The greater the level of redundancy, the more expensive the cost of replication.
- Data are replicated 3 times in the primary region***.***
- ***Options are:***
    - ***Locally Redundant Storage (LRS)*** (which is cheapest option, 11 9s) replicates data 3 times within a single data center ***in Primary regions***
    - ***Zone Redundant Storage (ZRS)*** (12 9s) replicates data across 3 AZs in ***Primary regions***
    - ***Geo Redundant Storage*** (16 9s, copies data synchronously 3 times to primary region and asynchronously to a single region in secondary region) N:B: ***Replication to secondary regions in case of primary region disaster.***
    - ***Geo-Zone-Redundant Storage*** (16 9s, copies data synchronously to 3 AZs in primary region and asynchronously to secondary region) N:B: ***Replication to secondary regions in case of primary region disaster***
    - ***Read-access Geo Redundant Storage*** (16 9s, copies data synchronously to primary region and synchronously to secondary region). N:B: In this case,read access is enabledto the secondary region, your data is always available, even when the primary region is running optimally.
    - ***Read-access Geo-Zone Redundant Storage*** (16 9s, copies data synchronously across 3 AZs in primary region and asynchronously to secondary region). N:B: In

this case,read access is enabledto the secondary region, your data is always available, even when the primary region is running optimally.

Data Migration

Azure Migrate

- Streamlined service for migration from an on-premises environment to the cloud, modernization and optimization on Azure
- Easily integrates with third party tools form independent software vendors
- It features tools like “Azure Migrate: Discover & Access” and “Migration and Modernization”
- It offers unified migration platform, diverse tool set for migration and modernization
- Assess, migrate and modernize in Azure migrate Hub
- Databases, web apps, virtual desktop and data transfer
- Integrated tools are ***“Azure Migrate: Discover & Access”, “Azure Migrate: Server Migration”, “Azure Database Migration Service”, “Data Migration Assistant”, “Azure AppService Migration Assistant”, “Azure Databox” and “Migration and Modernization”***

Azure Databox

- Physical device. Inexpensive way of sending terabytes (80TB) of data in and out of Azure
- Use cases are: Importing data (One time migrations, initial bulk transfers, periodic uploads) and Exporting data (Disaster recovery, security requirements and migration)

Azure identity, access, and security

Microsoft Entra ID (Formerly Azure Active Directory (Azure AD))

- Cloud-based Identity and Access Management (IAM) service used to manage users, sign-ins and access
- Provides security tokens that you can use for the authentication flow of your cloud-based applications
- Can be used to implement ***single sign-ons & authentication***
- Editions are: free, Office 365 apps, Premium 1, Premium 2
- Cannot create custom access control with Free and Office 365 apps edition
- Use cases are: Authorize & authenticate to multiple sources to on-premises AD, web app, to Office 365 or Azure Microsoft
- Domain is an area of network organized by single authentication DB. Entra ID domain is a logical grouping of Entra ID objects on a network

- Domain Controller is a server that authenticate user identities & authorizes their access to resources
- Domain Computer is a computer registered with a central authentication DB. It would be an Entra ID object
- Entra ID Object is a basic element of Entra ID e.g., Users, Groups, Printers, Computers & Shared Folders
- Group Policy Object is a virtual collection of policy settings. It contains what Entra ID objects has access to
- Organization Units is a subdivision within Entra ID into which you can place objects like users, groups etc
- Directory Service (e.g Entra ID Domain Services) provides the methods for storing directory data & making the data available to network users & administrators. It runs on a Domain Controller
- ***Microsoft Entra ID Domain Services*** provides managed domain services like domain joins, group policies, Lightweight directory access protocol (LDAP) & Kerberos/NLTM authentication. You get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.
- ***Microsoft Defender for Identity: Monitor the domain controller traffic and detect security threats using a sensor***

Single Sign-on (SSO)

- A feature that allows user to authenticate once with Entra ID & then access multiple applications & services without having to authenticate again. Entra ID creates a security token that can be used to access other resources within the same organization.
- SSO supports cloud-based applications, uses (Microsoft 365, Salesforce & Dropbox), on-premises applications (SharePoint & SAP) and custom-built applications (SAML, OpenID Connect & OAuth).
- Choosing SSO depends on how the app is configured for authentication.
- Cloud-based applications can use SAML, OpenID Connect, OAuth, password-based or linked for SSO which can also be disabled while on-premises applications can use password-based, Integrated Windows Authentication, header-based or linked for SSO. On-premises choices only work when apps are configured for Application Proxy
- SSO Protocols supported in Azure are: OpenID Connect & OAuth (authentication & authorization of users in a secure & standardized manner), SAML (authentication & authorization data between an identity provide & a service provider), password-based authentication, Linked authentication, Integrated Windows authentication, Header based authentication (token)

External Identities (Microsoft Entra External ID)

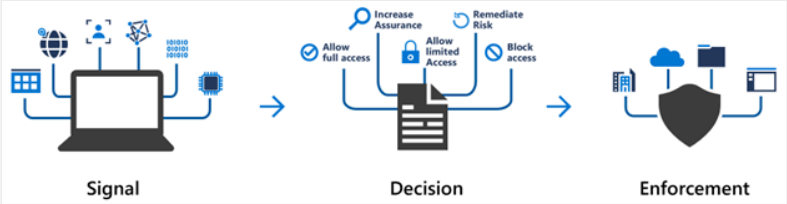
- Allow people outside your organization to access your apps & resources while letting them sign in using any identity they prefer
- Capabilities are: Business-to-business collaboration, B2B Direct Connect, Microsoft Azure Active Directory business to customer (B2C)

- ***May be similar to SSO***

Conditional Access

- Tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. Granular MFA access. Can vary the credentials needed to log in based on signals
- Provides an extra player of security before allowing authenticated users access data or other assets by collecting signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

The following diagram illustrates this flow:



Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

- Usually implemented via Conditional Access policies which are sets of rules that specify the conditions under which sign-ins are evaluated and allowed
- Conditional Access policy enables MFA enforcement based on group membership
- Conditional Access policiies analyzes signals (metadata associated with identity e.g., User/group membership, IP location, Device, Application, Real-time sign-in risk detection, Cloud apps, user risk) and verifies every attempt via access Controls
- Use Cases: ***Require MFA***, Require access to services only through approved client applications, Require users to access your application ***only from managed devices***, Block access for untrusted sources or unknown locations

Common Decisions

- Defines the access controls that decide what level of access based on signal info.
- Decisions are: block access, grant access
- Can be used with MS 365 Business Premium, MS 365 E3 & E5, Entra ID P1 & P2

Active Directory Vs Microsoft Entra ID

- Active Directory manages multiple **on-premises** infrastructure components and systems using a single identity per user while MS Entra ID takes this approach to next level by providing organizations with an Identity as a Service (IDaaS) solutions for all apps across **cloud** & on-premises

Passwordless Authentication

- E.g: Windows Hello for Business (tied to user's PC), Microsoft Authenticator app (employee's phone), Fast Identity Online (FIDO2) security keys (an external security key or a platform key built into a device, are typically USB devices, but could also use Bluetooth or NFC)

Role Based Access Controls (RBAC)

- Azure RBAC helps ***manage who has access to Azure resources***, what they can do with the resources & area they have access to
- Role assignments control access to resources and consists of ***security principal*** (identity requesting access to Azure resource, can be a user, group, or service principal, managed identity), ***role definition*** (collection of permissions. It lists the operations that can be performed such as read, write or delete. It can be high-level e.g., owner or specific e.g., virtual machine reader) and ***scope*** (set of resources that access for role assignments applies to. It access controls at the ***management, subscription, single resource or resource group level***)
- Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager.
- Azure RBAC doesn't enforce access permissions at the application or data level.
- Four fundamental Azure roles (owner, contributor, reader and User Access Administrator) & 70 built in roles

Microsoft defender for cloud

- Microsoft defender for cloud provides advanced protection for your Azure & on.-premises workloads by monitoring your cloud, on-premises, hybrid, and multicloud environments to provide guidance and notifications aimed at strengthening your security posture.
- ***When necessary, Defender for Cloud can automatically deploy a Log Analytics agent to gather security-related data. For Azure machines, deployment is handled directly. For hybrid and multicloud environments, Microsoft Defender plans are extended to non-Azure machines with the help of Azure Arc. Cloud security posture management (CSPM) features are extended to multicloud machines without the need for any agents.***
- Defender for Cloud helps detect threats across: Azure PaaS services, Azure Data Services, Networks. It can also defend hybrid resources, resources on other clouds. Use just-in-time ***(JIT) VM*** access

- Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises: ***Continuously assess*** (Know your security posture. Identify and track vulnerabilities), ***Secure*** (Harden resources and services with Azure Security Benchmark), ***Defend*** (Detect and resolve threats to resources, workloads, and services)
- Coverage allows to see resources types in subscription & eligible for protection by azure Defender
- **Defend**: Security alerts describe details of affected resources, suggested remediation steps, and in some cases an option to trigger a logic app in response
- Insights is rolling pane of news that give suggested reading, and high priority alerts gives Security Center's insights into pressing security matters that are relevant to you and your subscription

Azure Defender has **many plans** for specific Azure resources:

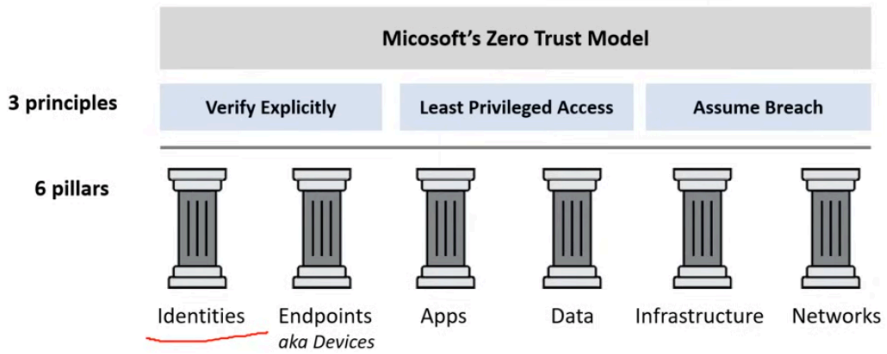
- Azure Defender for servers
- Azure Defender for App Service
- Azure Defender for Storage
- Azure Defender for SQL
- Azure Defender for Kubernetes
- Azure Defender for container registries
- Azure Defender for Key Vault
- Azure Defender for Resource Manager
- Azure Defender for DNS
- Azure Defender for open-source relational databases

When you turn on Azure Defender **all plans are activated**

- Network map provides a graphical view with security overlays giving recommendations & insights for hardening network resources
- Hybrid Cloud Protection: Azure Defender can protect VM in other cloud providers like AWS & Google Cloud Platform (GCP) via Azure Arc
- Azure Arc is a control pane that can manage compute resources (Servers, Kubernetes Clusters, Azure Data Services, SQL Server, VM Preview) across cloud providers, on-premises and at the edge. Arc lets you extend your Azure compliance and monitoring to your hybrid and multi-cloud configurations. Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.
- Azure Security Center: Unified infrastructure management security system that strengthen security posture of data centers and provides advanced threat priotection across hybrid workloads in cloud
- Key Vault: Safeguard cryptographic keys & other secrets used by cloud apps & services. Secrets management, key management, certificate management & Hardware Security Module (HSM) (Piece of hardware designed to store encryption keys, FIP 140-2 compliant for multi-tenant & FIP 140-3 compliant for single-tenant)
- Azure Distributed Denial of Service (DDoS) Protection: Types are Volumetric attacks, protocol attacks and application layer attacks (WAF as protection). Tiers are: DDoS Protection Basic, DDoS Protection Standard
- ***Management Groups: Managing multiple subscriptions*** into a hierarchical structure

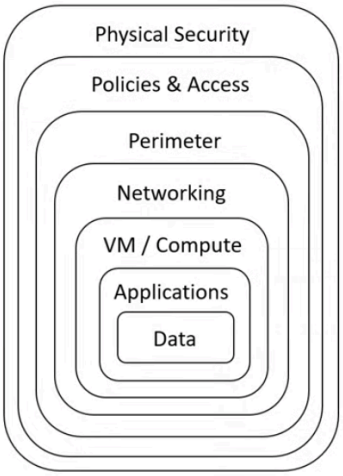
Zero-Trust Methodologies

- Operates on “Use least privilege access, Assume breach, Verify everything explicitly”



Layers of Defense

- Series of mechanisms to slow the advancement of an attack that aims to gain unauthorized access to data



The 7 Layers of Security

1. Data
access to business and customer data, and encryption to protect data.
2. Application
applications are secure and free of security vulnerabilities.
3. Compute
Access to virtual machines (ports, on-premise, cloud)
4. Network
limit communication between resources using segmentation and access controls.
5. Perimeter
distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
6. Identity and access
controlling access to infrastructure and change control.
7. Physical
limiting access to a datacenter to only authorized personnel.