terraform console — terminal command that can be used interactively to get info about the current terraform state

* resource\_type.resource\_name
  + IE aws\_s3\_bucket.my\_s3\_bucket
* resource\_type.resource\_name[0]
* var.resource\_name
* concat(var.resource\_name, “string\_value”)
* contains(var.resource\_name, “string\_value”)
* map of string
  + keys(var.resourse\_name) or values(var.resource\_name) or lookup(var.resource\_name,”string”

terraform apple -refresh=false

terraform apply -target resource\_type.resource.name — updates specific resource

terraform.tfstate

* .tfstate: stores current infra layout
* .tfstate.backup: stores the prior changes
* maps of terraform objects to the objects in the cloud
* acts as a cache to get environment footprint for better perfromance
* metadata

separate projects/folders/modules to manage the resources for the particular environment

collection functions

map of string {} uses a key:value pair. IE name:country

for\_each = var.resource\_name

name = each.key

tags = { country:each.value }

<https://www.youtube.com/watch?v=VaMdHKJQ15c&list=PLlVtbbG169nED0_vMEniWBQjSoxTsBYS3&index=2>

<https://www.youtube.com/watch?v=l7K1LPAgL5I>

<https://www.youtube.com/watch?v=8n-kWJetQRk> —---working. mOST INFOR IS from here

Azure functions, Azure Event Grid, azure app service, CDN, Azure DataBrinks, Azure Front door, azure policy, azure blueprint, Azure monitoring

Public cloud/multi tenant – infrastructure provided by cloud provider

* 
* Agility, reliability, availability, scalability, elasticity, security
* OpEx- pay as you go

Private cloud/single tenant – dedicated to a single company. On-prem

* 
* Legacy support, 100% control, compliance
* capEx spend money upfront

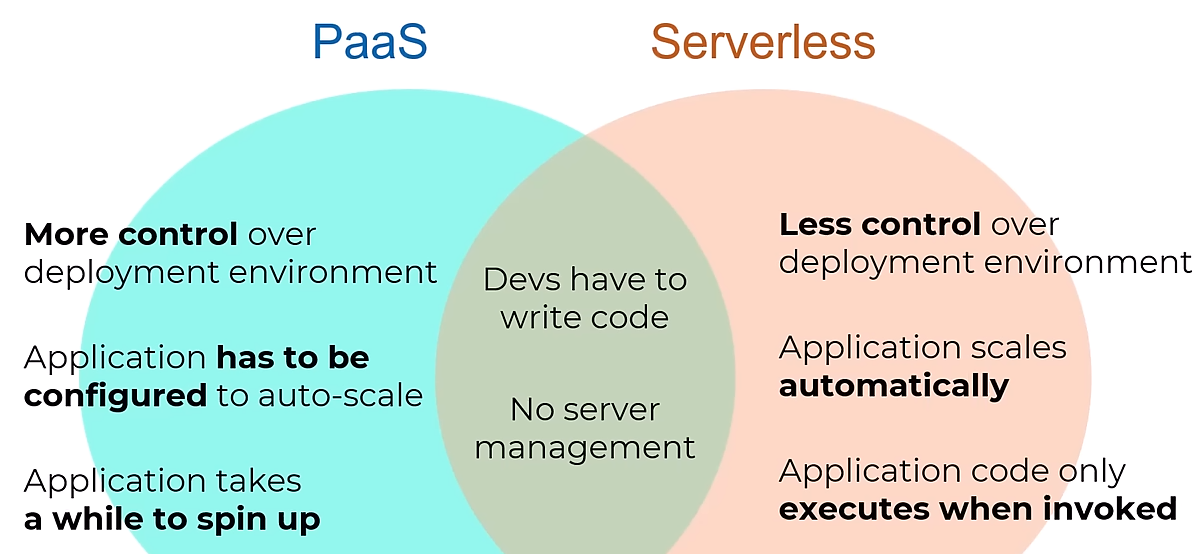
Hybrid cloud

* 
* Flexibility

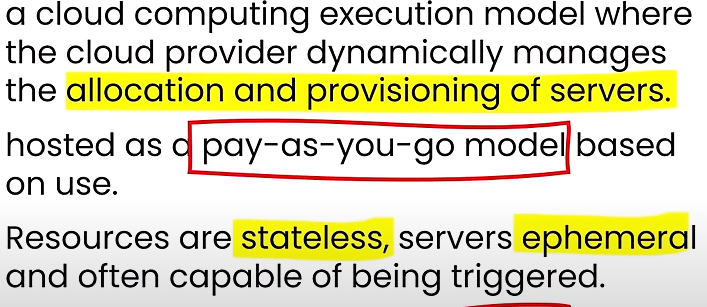
Compute at lower cost than on-prem

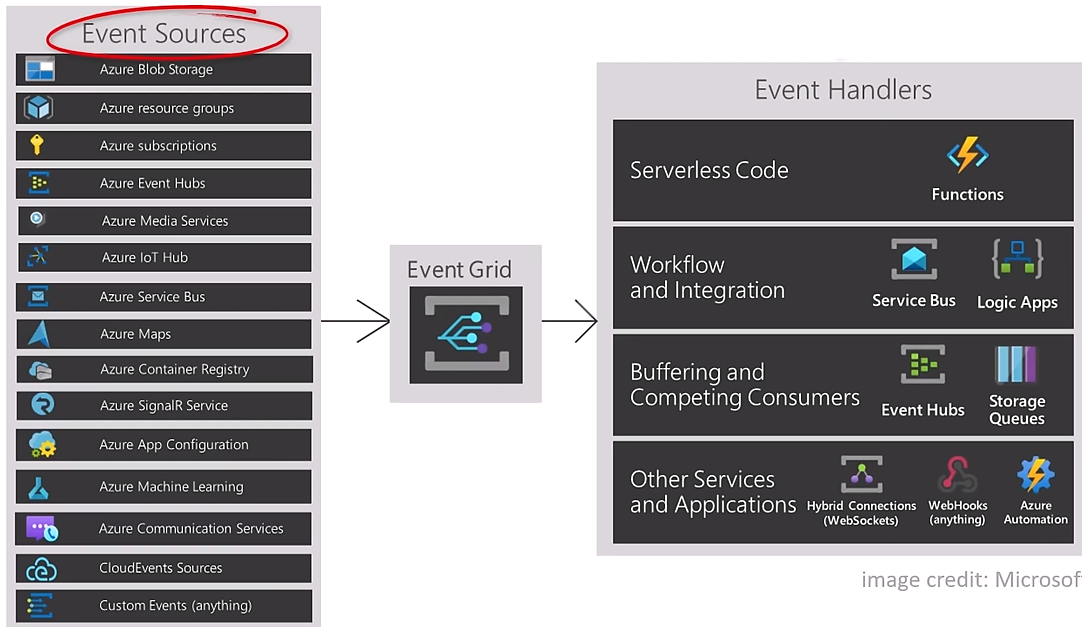
Fixes price model: provision resources and you pay for them whether you use them or not. Predictable cost

offers over 55 free services



Serverless:

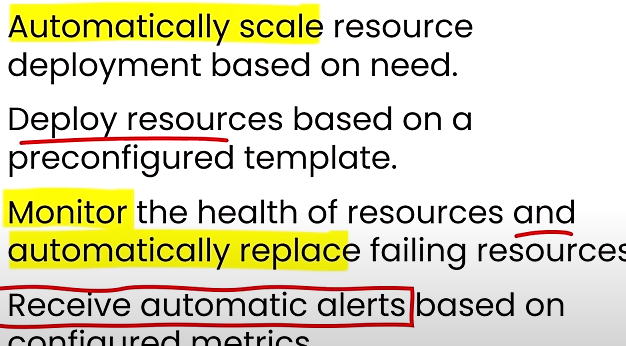


* **Azure Functions**(PaaS): serverless compute service that enables users to run event-triggered code without having to provision or manage infrastructure. As a trigger-based service, it runs a script or piece of code in response to a variety of events
  + event driven compute on demand experience that extends the existing azure app platform with capabilities to implement code **triggered by events** occurring in Azure as well as on prem. Billed per execution, cheap
* **Logic apps**: helps schedule, automate, and orchestrate tasks, business process, and **workflows** pre-built connectors. Like 365 and ServiceNow,Adobe, etc. Power Automate(Azure Flow)
* **Event grid(PaaS)**: enables for easily managed events across many different azure servers and apps. Once subscription is created, it’ll **push** events to the configuration destination. Pub-sub model. Pay per use
  + 
* Container apps, kubernetes, Cosmos DB

What makes an application unavailable

* Network issue, application failure, system outage (VM), a power outage, a problem with a reliant system like a database

Cloud benefits

* Availability
  + Infra, apps, and services
  + HA(service-level failure) is typically considered to be 99% or above
* Scalability ability to handle more work load
  + Vertical – increase compute power(memory, CPU, space, disk)
  + Horizontal – build more of the same infrastructure.
  + Scale in and scale out
* Elasticity – ability to grow and shrink automatically based on app demand
* Fault tolerance (maintain availability when a fault happens. Components failures
  + Fault is a failure.
* Agility speed and ease of allocating and deallocation resources
* Security and governance
  + Security: restrict access to your resources to only those you allow
    - DATA, app, infrastructure
  + Governance refers to how your org does business. the level of access someone has, what they can do with that access, and how they can do it.
    - Guardrails that ensure we’re as secure, consistent, and efficient as possible. Auditing and reporting
    - Azure Policy
  + Cloud adoption framework: guidance designed to help you create and implement the business and technology strategies to succeed in Azure. Five disciplines of cloud governance
  + Security is better in the cloud
* Reliability ability to recover from failures and continue to function
  + Resiliency aims to return an app to a fully functioning state after a failure occurs
  + Availability to provide consistent access to your app
  + auto-scaling
* Predictability the level of service and performance and the associated cost are known in advance. Predictable cost and performance
* Manageability
  + What
    - 
  + How
    - 
  + management of the cloud
    - templates, automation,scaling, self-healing, monitoring and alerts
  + management in the cloud
    - web portal, command line, APIs, PowerShell

Most control to least control

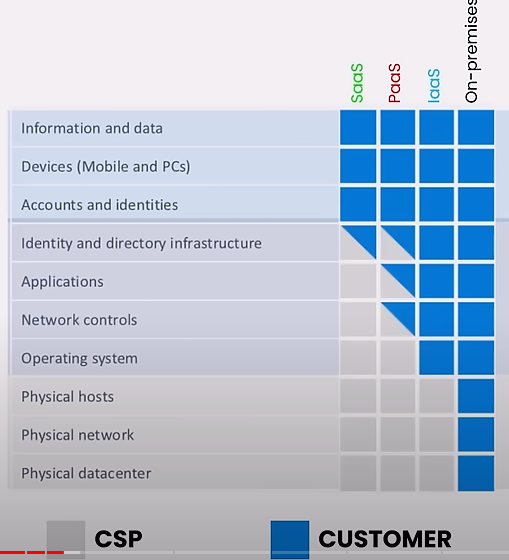
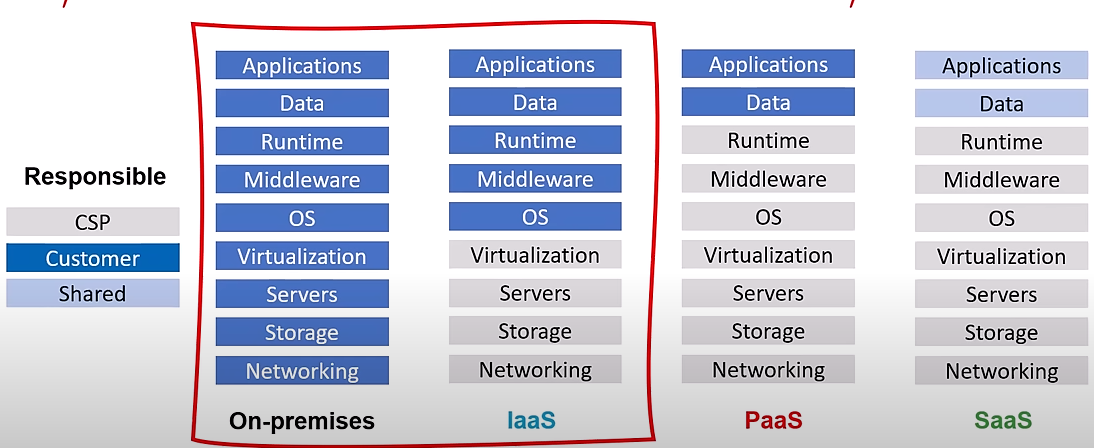
* VM>container>Azure function>Azure App service

Azure DDOS

* INCLUDES LOGGING, ALERTING AND TELEMETRY

Cloud computing delivery of computing services over the internet

Service type

* IaaS(AzureVM)(private)(EC2,GCP compute engine)
  + Cost based on consumption. User has most level of control and responsibility
  + Infrastructure is provided by the cloud provider
  + Test and Dev deployments, DR scenario
  + SQL server
  + Azure storage, Azure network
* PaaS(Azure App service(fully managed platform for creating web applications))(hybrid)
  + Infrastructure, OS,runtime,middleware provide by the cloud provider
  + Offer turn-key features, Reduces management burden
  + SQL server Managed instance,Azure SQL database, API management, Azure app service, Azure functions, Azure Container Apps
  + When to use
    - Development framework, build and customize cloud-based apps, builtin software components. complete Dev and deployment envir in cloud
    - Simplifies Analytics/business intelligence and improves business outcomes
    - Networking (Azure front door, LB, FIREWALL)
* SaaS(m365, OneDrive,ServiceNow)(public)
  + Infrastructure, OS, software provide by the cloud provider
  + Often accessible via a web, User has the least responsibility
  + **Customers just configures features**
  + Enables companies to securely and reliably outsource a variety of functions so they can focus on making money and innovation
*  

Azure Front Door is Microsoft’s modern cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications’ static and dynamic web content across the globe.

* delivers your content using Microsoft’s global edge network with hundreds of global and local points of presence (PoPs) distributed around the world close to both your enterprise and consumer end users

Core architecture and services

* **Azure geography** a discrete market containing 2 or more regions that preserve data residency and compliance boundaries .NA, EUROPE, CHINA, AFRICA, SOUTH AMERICA
* **Region** – a geographical location comprised of data centers connected through a low-latency network
* **Region pairs**: Paired for HA, connected over low latency networks within geography. See MS doc. Usually are at least 300 miles apart, DR purposes
* **Sovereign regions** are isolated from the rest of Azure. Microsoft doesn't necessarily manage them, and they can be restricted to certain types of customers. China, US gov
* **Availability Zones:** Comprising 1 or more datacenters, physically separate locations within each Azure region that are tolerant to local failures. Provides 99.99% SLA uptime. each zone includes datacenters with independent power, cooling, and networking that combines update and fault domains to **protect against datacenter/single point failures**. not every region has a availability zone
  + zonal services: users choose a specific AZ to deploy service to
  + zone redundant service
  + Always available services
* **Azure datacenter**: physical builds that contain thousands of servers and other hw to provide cloud computing. Organized into regions

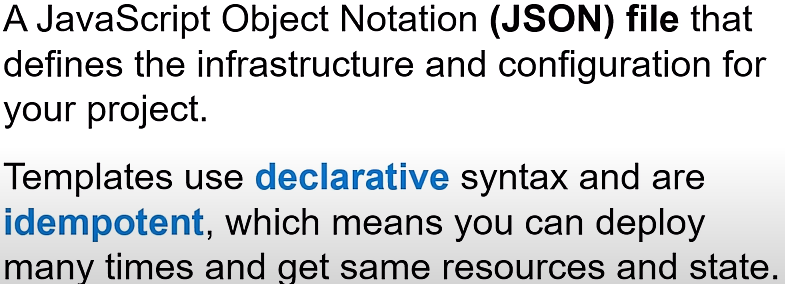
5 PILLARS:

* Operational excellence, security, reliability, performance efficiency, cost optimization(Azure Advisor)

**Azure Resource Manager** is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

* provides a management layer that enables you to create, update, and delete resources in azure

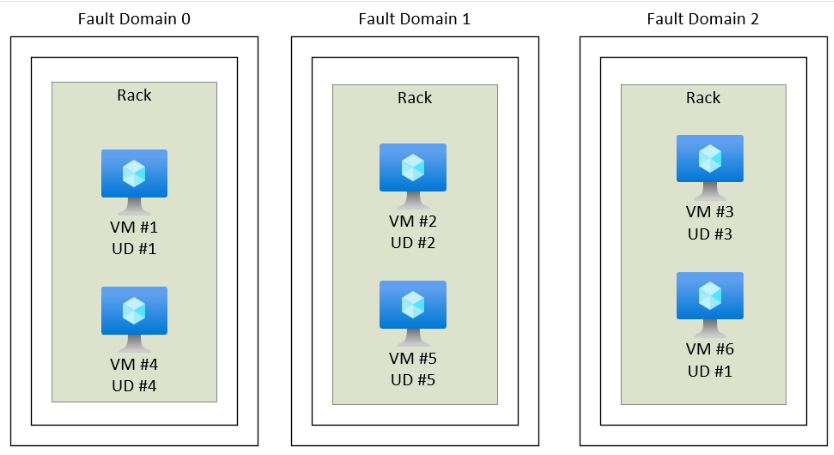
ARM template: declarative(define what you want. idempotent(can be deployed many times)

* 

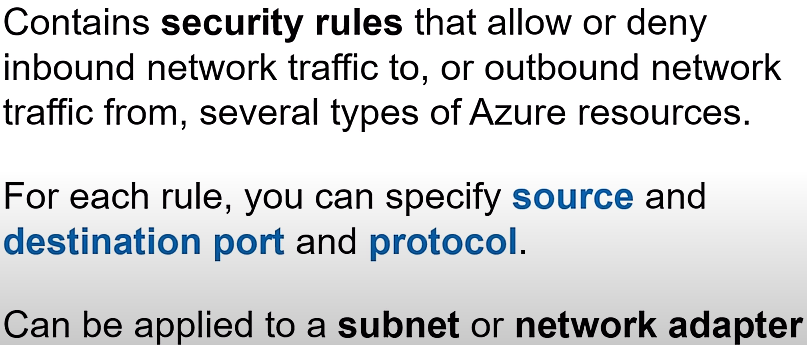
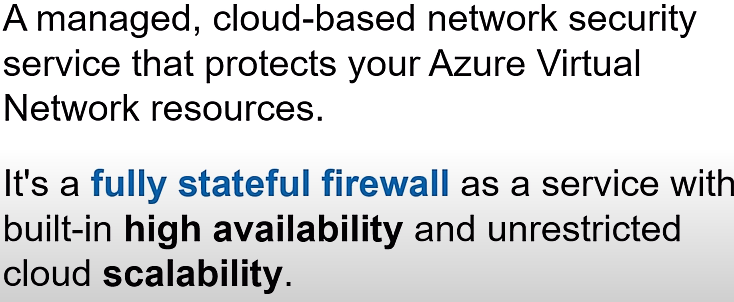
Account structuring

* Management>subscription>resource group>resource
* Management: Provides a level of scope above subscriptions. A management group tree can support up to six levels of depth. 10,000 management groups can be supported in a single directory. Top level is root. Can hold multiple subscriptions
  + An aggregate policy and initiative assignments via azure policy
* Subscription: billing boundary for resources. Logical container used to provision resources in Azure. Can be used to isolate resources between departments, projects, etc
  + Azure Blueprints: is a template that allows for creation of new subscriptions that already has policies, roles, RGs and ARM templates.
* Resource group: container that holds related resources for an azure solution. Share a common lifecycle(vm,network adapter,network interface,NSG,storage disk,public IP address)
* Resource: entity managed by azure

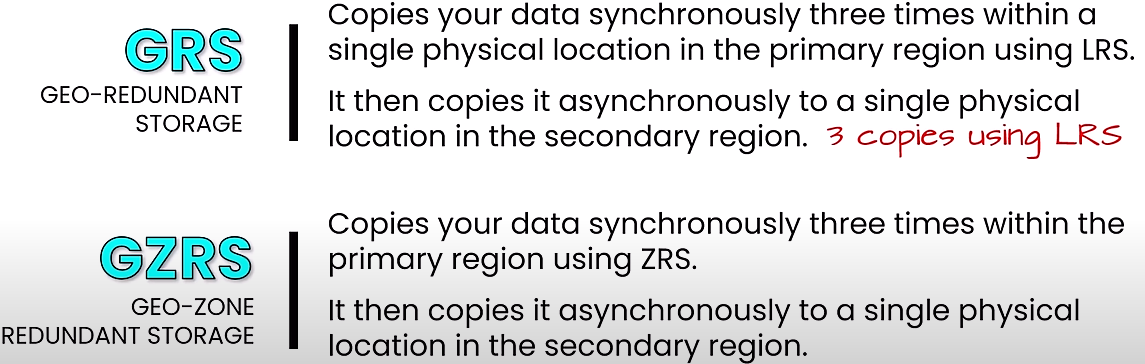
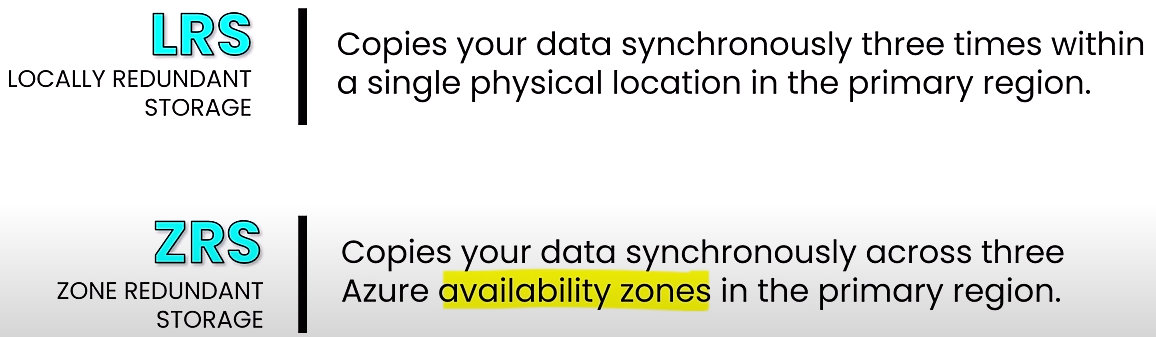
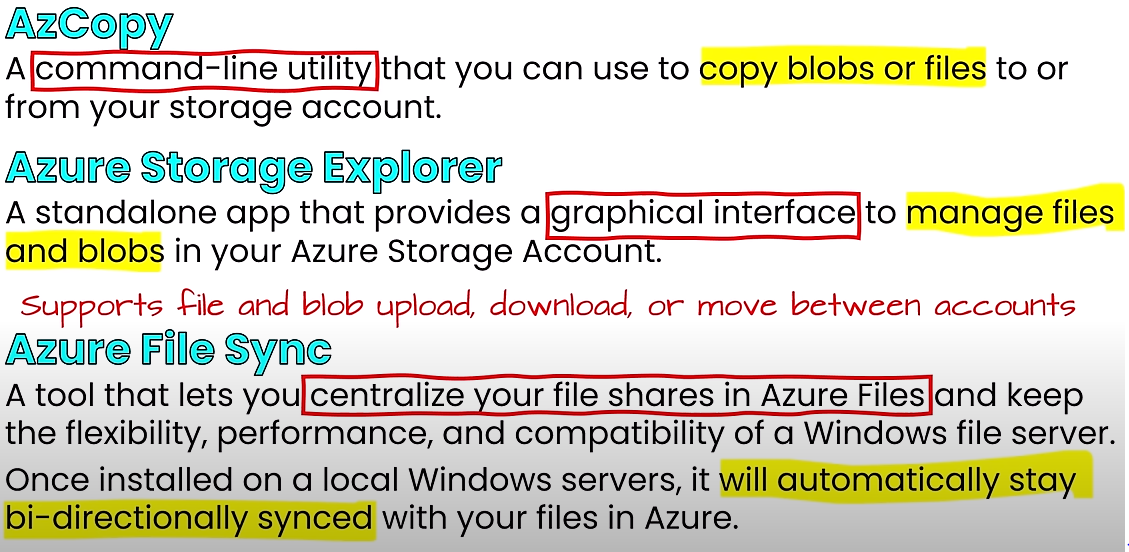
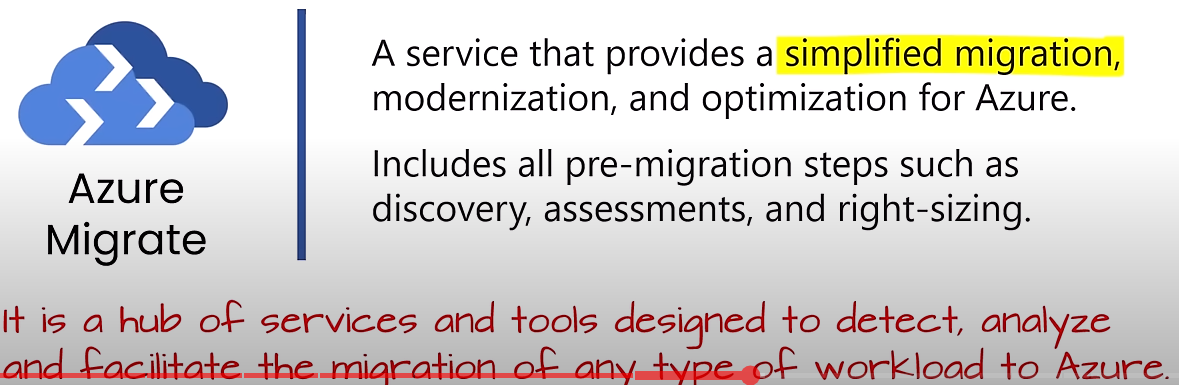
Compute types

* VMs
  + Compute on-demand w/o need for hw purpose
  + VM scale set and availability sets
    - 
    - Availability sets
      * Update domains allows Azure to perform incremental or rolling upgrades across a deployment. During planned maint only 1 domain is rebooted at a time
      * Fault domains are a group of VMs that share a common set of hardware/switches, that share a single point of failure. VMs in an availability set are placed in at least 2 fault domains
      * 
  + Requirements: (vm,vnet,network interface,NSG,storage disk,public IP address)
* **AKS(Azure kubernetes service):** hosted k8s service where azure handles critical tasks like health monitoring and maintenance for the customer. You pay for only the agent nodes within the cluster not the master. Enterprise, can get complicated
* **Azure container instance(ACI):** runs docker containers on-demand in a managed, serverless Azure environment. isolated containers w/o orchestration. Easier to utilize, manage,deploy
* Azure container apps is a serverless platform that allows you to maintain less infrastructure and save costs while running containerized applications. provides all the up-to-date server resources required to keep your applications stable and secure.
* **Azure virtual desktop:** desktop and app virtualization service that runs in MS Azure
* **Azure App service:** HTTP based service for hosting web apps, REST APIs, and mobile back ends
  + Web apps, API apps, web jobs(run a program on a trigger), mobile apps
  + upload code and config files to Azure and it runs your code w/o you needing to manage underlining hw. includes CI/CD,containers, staging/dev environments

Network

* Virtual network(VNET) logical representation of network in azure. Containers 1 or more subnets
  + LOGICAL isolations. Decidcate cloud only network
  + can be Used to securely extend your data center(site-to site VPN- goes over the internet)
  + VMs in different vnets cannot comm by default
* Virtual subnet
  + segments address space of a VNET to create sub-networks. Resources can be deployed to a specific subnet(segmentation)
  + vms in different subnets within a vnet can communicate by default
* VPN Gateway (Azure virtual network gateway)
  + a virtual network gateway that sends encrypted traffic between an Azure vnet and an on-prem location over the internet
* VNET Peering
  + enables connection between 2 or more vnets.
* ExpressRoute
  + extends on=prem networks into Azure over a private connection with the help of a connectivity provider. **TRAFFIC DOESN’T CROSS OVER THE INTERNET**
    - **more secure, less latency**
* Azure DNS: hosting service for DNS. internal and external DNS provider
* endpoint
  + private: grants access to a specific instance of a PaaS service in your VNET on a private IP address. Enables access from on-prem w/o public endpoint
  + service(public) provides a way to lock down access to all instances of a PaaS service to a VNET. Accessible from public internet
* defense in depth: layer approach that doesn’t relay on 1 method to protect your environment
  + data- virtual network endpoint
  + application: API management
  + compute: RDP access & windows updates
  + network: NSG, subnet usage,deny by default
  + perimeter: DDoS, firewalls
  + Identity & access: Entra ID
  + physical: door locks and key cards
* NSG
  + attached to a subnet is common implementation
  + between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers
* Azure Firewall (traffic filter)
  + 
* Azure DDoS: protects against Distributed denial of Service

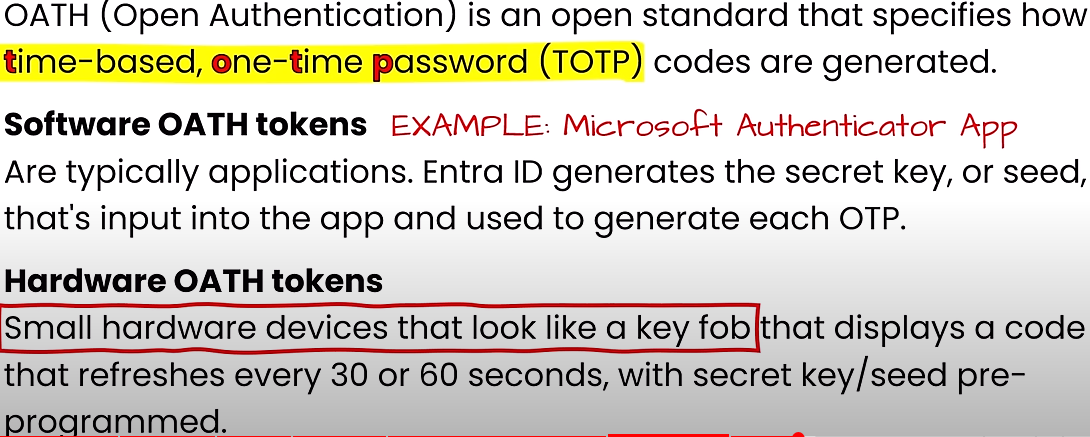
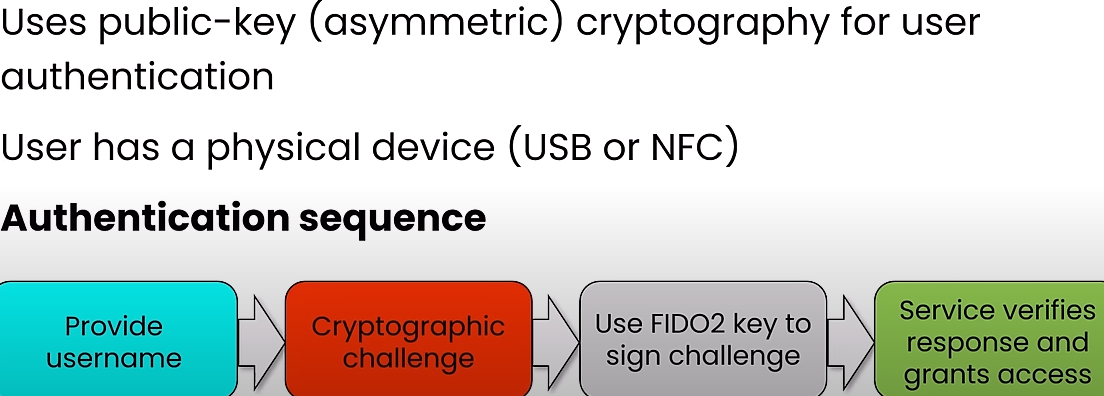
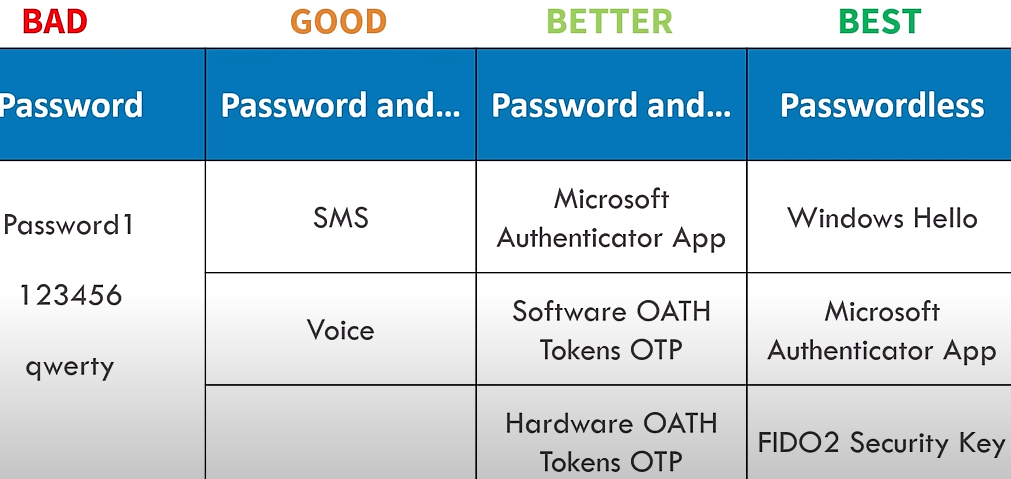
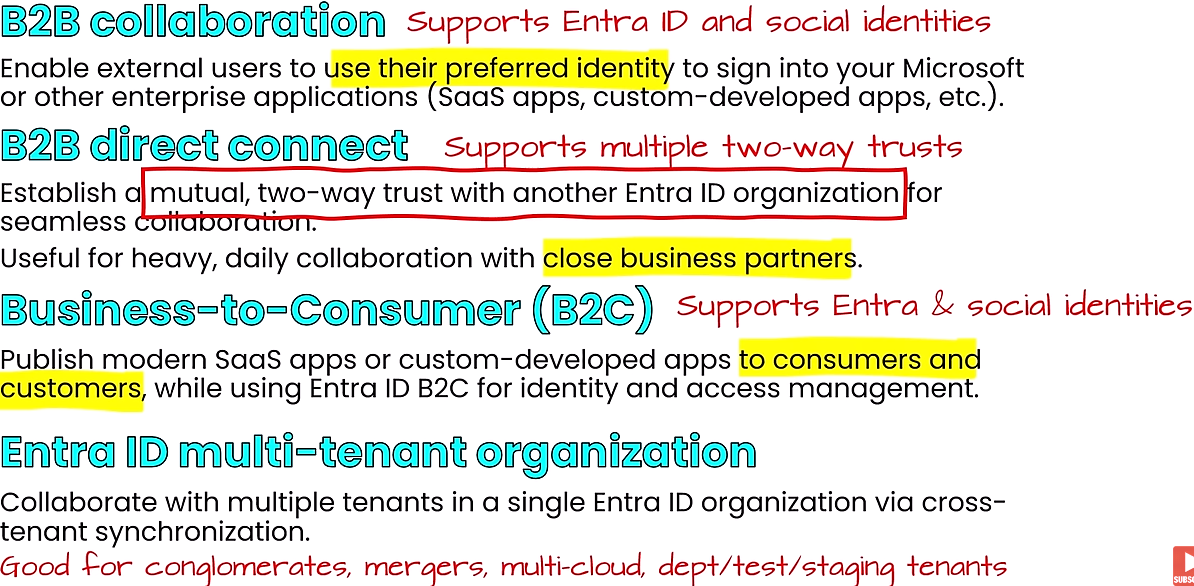
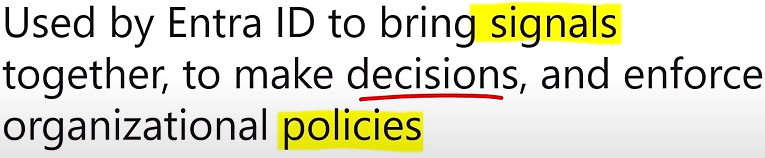
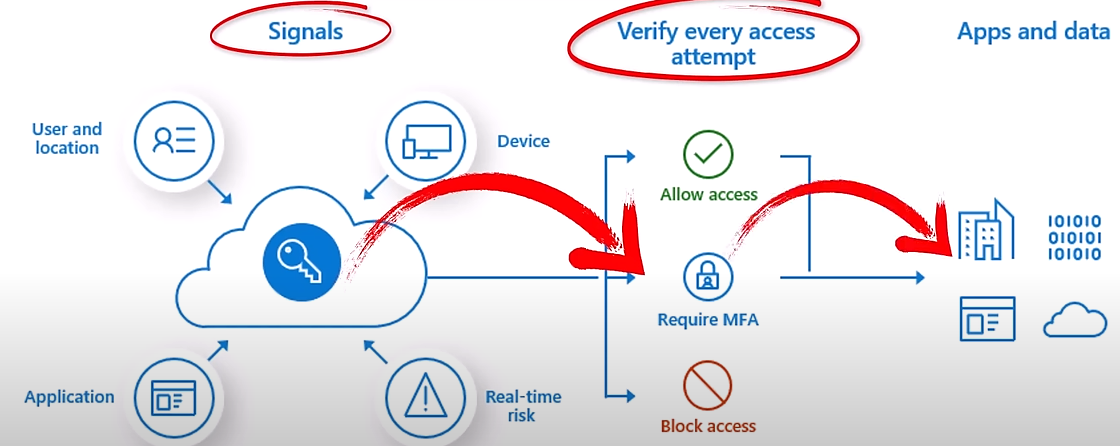
Storage

* Azure blob:- stores unstructured data, cannot be contains in a row/column model. images, files, etc. Azure blob: a massively scalable object store for text and binary data. Blob storage for unstructured data. Backup archiving, DR testing
  + <http://mystorage.blob.core.windows.net>
  + Static website: https://<storage-account>.web.core.windows.net
* Azure Files/file shares: managed file shares for cloud or on-prem deployments. Uses SMB protocol. fully managed. Lift and shift migration. add DR(redundancy, failover, recovery)
  + <http://mystorage.file.core.windows.net>
    - Azure File Sync enables you to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of a Windows file server. has the ability to transform Windows Server into a quick cache of your Azure file share. Protocols SMB, NFS, and FTPS
* Azure Tables: key/attribute option for structured non-relational data. Non-SQL data. A NoSql store for schema less storage of structured data
  + <http://mystorage.table.core.windows.net>
* Azure queues: a messaging store for reliable messaging between application components. 64 kb per file. HTTPS/HTTP calls for authentication
  + <http://mystorage.queue.core.windows.net>
* Azure disk storage
  + azure managed disks are block-level storage volumes that are managed by Azure and used with Azure VMs
* Storage redundancy
  + Lrs 11 9s
  + Zrs 12 9
  + Grs 16 9s
  + Gzrs 16 9s
  + 
* Storage access tier storecs blob object
  + Hot- higher to store, cheapest to access. online tier
  + Cool – 30 days. online tier
  + Cold – 90 days. online tier
  + Archive – 180 days storage. Up to 15 hours to retrieve. cheapest to store, highest to access. offline, flexible latency requirements
* Azure Storage Explorer is a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. GUI interface, can be downloaded
* Azcopy: azcopy copy *SOURCE DESTINATION*. can be downloaded to Windows, macOS, and Linux
  + can work across subscription with SAS keys
* Azure file sync: hybrid option, cloud tiering(most access on-prem and everything else in cloud). Allows users to move/sync files between on-prem and in the cloud.
  + Azure File Sync enables you to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of a Windows file server. has the ability to transform Windows Server into a quick cache of your Azure file share. Protocols SMB, NFS, and FTPS
  + 
* Azure migrate
  + 
* Azure data box
  + a solution that lets you send TBs of data into and out of Azure in a quick, cheap and reliable way. customers are shipped proprietary data box storage devices. larger than 40 TB when users have slow or not network connectivity

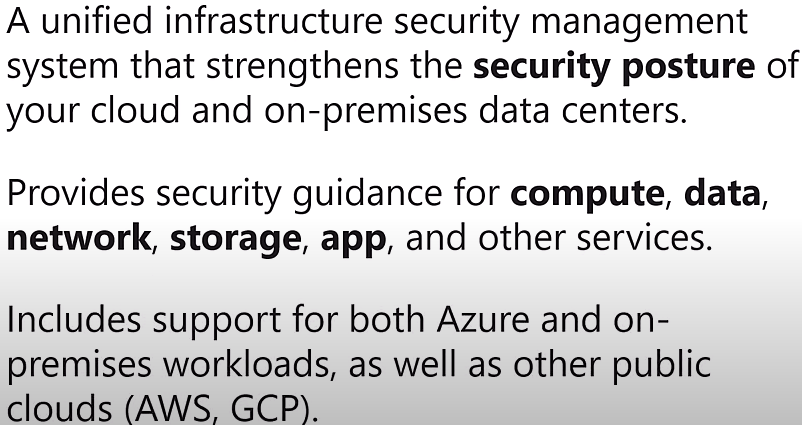
Identity an Entra ID (https://entra.microsoft.com/)

* Authentication (AuthN)- who are you. identity
* Authorization(AuthZ) - can you do it. access
* Entra ID can be used to grant access to internal and external resources(SaaS)
* Groups
  + Security and Microsoft 365
  + membership type: assigned and dynamic

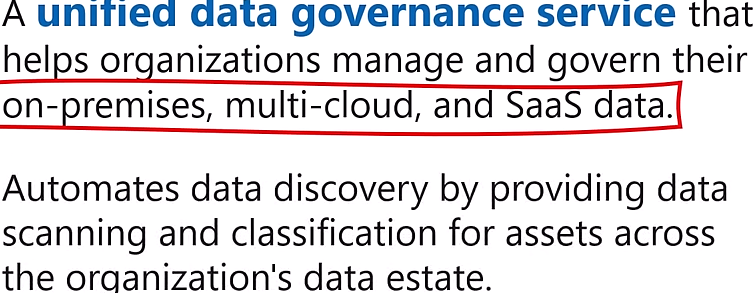
Authentication method

* SSO: modern authentication
* MFA: something you know, something you have, something you are
  + SMS is weak and is not recommended
  + Authenticator app can be used as a primary form of authentication to sign into any entra id account. can alos be used as an additional verification option during SSPR(pwd reset)
  + OATH(open authentication)
    - 
  + passwordless: Windows Hello, MS Authenticator App, FIDO2 security key. **concerned highly secure and convenient** 
    - FIDO2
    - Windows Hello
  + 
* B2B and B2C
  + 
* Conditional access(location, device,device platform), p1 and higher plan
  + 
  + 
* RBAC manages:
  + who has access, what they can do, what resources they have access to
  + built on Azure resource manager
  + Authz
  + roles
    - reader
    - owner: can assign share permissions and has access to everything
    - contributor: has all permissions/access but cannot grant others permissions
* Zero trust- security based on identity, must prove everything. trust must be earned.
  + **verify explicitly**
  + **use least privilege access**
  + **assume breach**. segment access to minimize blast radius. blocking subnets. ended to end encryption
  + a layered approach to security. App security>device>network>perimeter>IAM>physical

Defender for cloud

* 
* free and standard tier, generates a security score and recommendations

Governance and management

* **cost impact**
  + resource types, ,services, locations, ingress and egress traffic
* **reducing costs**
  + **reserved instances**(VM) can save up tp 72% over pay as go. 1 and 3 yr commitments
  + **reserved capacity** savings on Azure sql Database, azure cosmosDB, Azure Synapse Analytics and azure cache for redis. Predicted and variable workloads
  + **hybrid use benefit**: license benefit that allows you to use an on-prem software assurance enabled windows server and sql server license on Azure
  + **spot pricing-** access unused azure compute capacity at deep discounts.NON mission critical workloads. ONLY VMs
  + **pricing calculator-** interactive to estimate service pricing. before you deploy(**planning**)
  + **TCO(total cost ownership)**: can be used to estimate cost saving by migrating workload to cloud from on-prem. detailed breakdown. **planning**
  + **Azure cost management:** site of tools provided by MS that helps you analyze, manage, and optimize costs of workloads. resources already deployed in cloud
* Tags: key/value pair to locally azure resources
* scope: is the set of resources that access/policy applies to
* MS Purview: DATA GOVERNANCE/SECURITY
  + 
  + used to manage and restrict access to important data
* Azure policy - definition of the conditions which you want to control/govern
  + initiative: collection of azure policy definitions that are grouped together towards a specific goal
* Azure Blueprint: a container for composing sets of standards, patterns, and requirements for implementation of azure cloud services, security, and design
  + **Azure Blueprints: is a template that allows for creation of new subscriptions that already has policies, roles, RGs and ARM templates.**

**Resource locks** overrides any permissions. prevent accidental deletion. Incase added to a storage account, user can still add data to storage

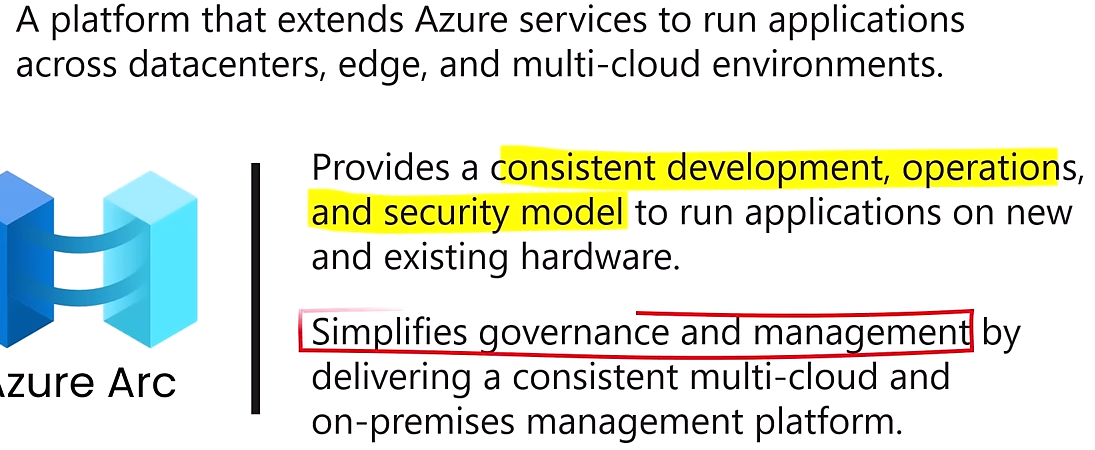
* types
  + Read Only – resources can’t be modified or deleted but can still be read.
  + Can Not Delete – resource can be modified and read but not deleted, by anyone
* can be applied to a VM, subscription, and resource group

Interact with Azure

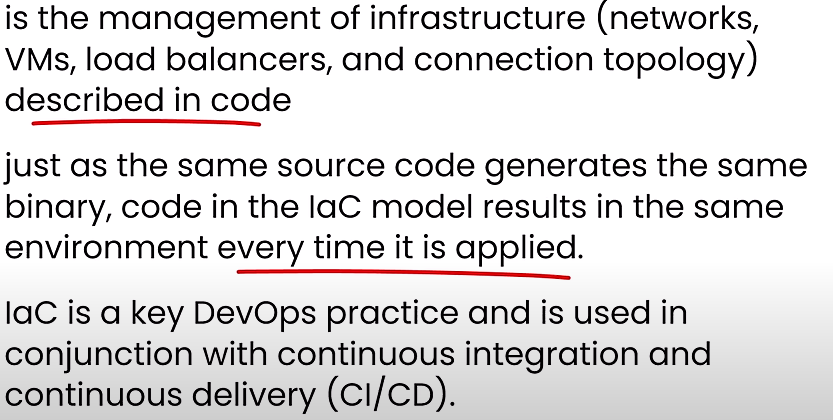
* Azure portal- web base UI
* Azure powershell: set of cmdlets for managing azure resources from a powershell command line
* Azure CLI: set of commands used to create & manage azure resources
* Azure cloud shell interactive browser shell for managing resources. Bash and powershell options
* Azure mobile: iOS/andriod. used to manage, track health/status & troubleshoot azure resources

Service Trust portal: MS public site for publishing audit reports and other compliance related info associated with microsoft’s cloud services

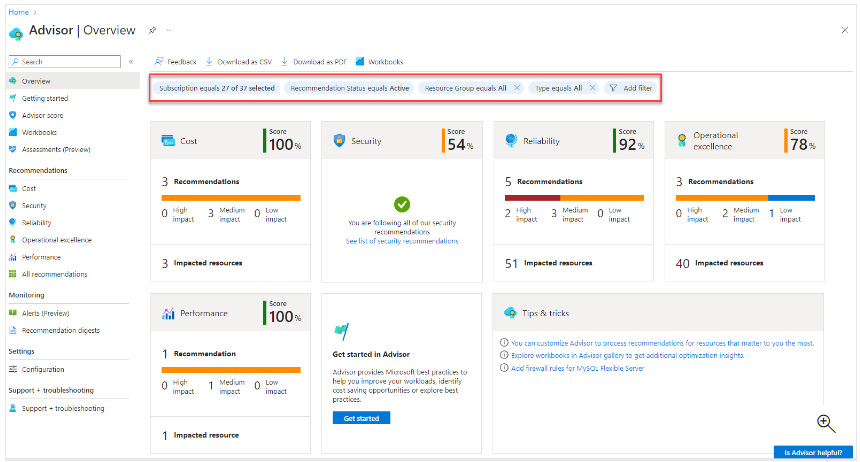
Azure Arc

* can manage Linux, windows, and K8s deployments in cloud(AWS,AZURE,GPC and on-prem)
* manages on-prem and cloud deployments
* 

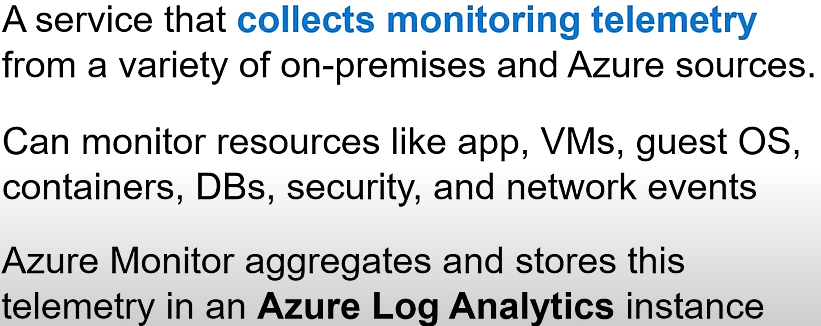
IaC: used with CI\CD

* 

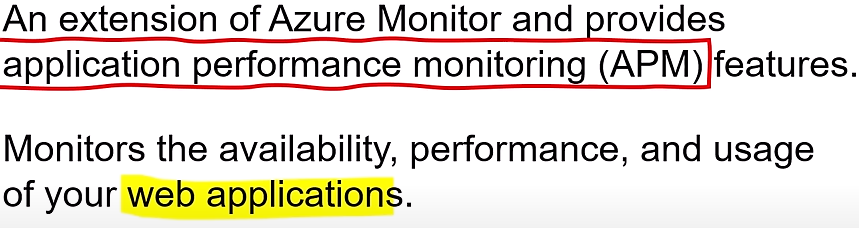
Azure advisor

* 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.
* Operational excellence, security, reliability, performance efficiency, cost optimization
* 
* 

Azure monitor

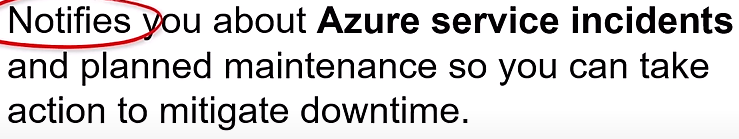
* 
* used to centrally collect,store and act on events
* Azure monitor Alert
  + 
  + view alerts in the portal, send notifications, or initiate automated responses(Azure functions or Azure automation runbooks)
* utlizies KQL

**Application insights** enables proactive understanding of app performance and reactive review of app execution to determine root cause

* 
* used to monitor health and performance of microservice apps running on AKS

Container insights, VM insights, Network insights

Azure service Health

* 
* monitors Azure’s core infrastructure

Azure log analytics: tool in the Azure portal that's used to edit and run log queries against data in the Azure Monitor Logs store. **Used to correlate events from multiple azure resources in a single repo**

* backend database for azure monitor
* KQL

Event Hubs is a fully managed, real-time data ingestion service that’s simple, trusted, and scalable. Stream millions of events per second from any source to build dynamic data pipelines and immediately respond to business challenges.

Azure Sentinel, renamed to Microsoft Sentinel, is a cloud native security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solution that runs in the Azure cloud

Microsoft Entra ID Protection (Azure identity protection)

* uses advanced machine learning to identify sign-in risks and unusual user behavior to block, challenge, limit, or allow access

CIAM is an industry recognized category that covers solutions that manage identity, authentication, and authorization for external identity use cases (partners, customers, and citizens). Common functionality includes self-service capabilities, adaptive access, single sign-on (SSO), and bring your own identity (BYOI)

2:15:03

VM scale set

- Provides a LB opportunity to automatically scale resources

VM availability set

- Default domain group based on network switch

App services

- Fully managed platform to build deploy

Azure data box

Azcopy

Azure storage explorer

Azure file sync – installed on-prem and connect to the cloud

Entra ID

- Authentication, SSO, application management, B2B, device management

- Entra domain services

- External

o B2C – separate service

- Conditional access used to make decisions and enforce org policies. Based on goruip memberships, ip address, device , etc

RBAC