Very high level view, how all connected in Azure : <https://www.youtube.com/watch?v=t1nB1RYihJg>

**Section 1 - Session 1**

**Availability** - if one machine got down you can use backup immediately and connect and get data. *Availability* refers to the time that a system is functional and working. Maximizing availability requires implementing measures to prevent possible service failures.

**Scalability** - you can add and remove resource, but you have to manually

You may have heard the terms scaling up(vertical scaling) and scaling out(horizontal Scaling).

Scaling up, or vertical scaling means to increase the memory, storage, or compute power on an existing virtual machine. For example, you can add additional memory to a web or database server to make it run faster.

Scaling out, or horizontal scaling means to add extra virtual machines to power your application. For example, you might create many virtual machines configured in exactly the same way and use a load balancer to distribute work across them.

**Elasticity** - resource added / removed automatically as per work load

**Agility**

* how fast it reacts, i.e. resource get added/removed as per requirement
* agility is the ability to rapidly change an IT infrastructure to adapt to the evolving needs of the business.

**Fault tolerance** - if some hardware gets faulted you can easily shift to other backup server

**Security** - compliance, privacy, governance, access control

**Disaster recovery** - if datacentres go down you can immediately start your service from other datacentres located in some other region or zone

**Global reach** - you can reach customer around the globe as cloud server located around glob

Less technical skill and less maintenance = Increased productivity, as no need to buy physical machine, patch them, cool them and don’t have hire expensive it staff to maintain it

**Pay as You got** - consumption base model = you pay for services, compute power, storage you are using

**Economies of Scale** = is the ability to reduce costs and gain efficiency when operating at a larger scale in comparison to operating at a smaller scale

**Capital Expenditure(capex) vs Operational Expenditure(opex)** (consumption base model), useful when all due diligence done and one can predict things/resource required easily

**capex**= upfront cost buying hardware for new business application and maintaining it

* Server costs
* Storage costs
* Network costs
* Technical staff cost
* Datacentre cost

**OpEx** is particularly appealing if the demand fluctuates or is unknown. Cloud services are often said to be agile. **cloud provider takes care of hardware and maintenance, very useful and growth where demand is unpredictable**

* + Leasing software and customized feature
  + Scaling charges based on usage/demand instead of fixed hardware or capacity
  + Billing at the user or organization level
  + OpEx is particularly appealing if the demand fluctuates or is unknown

**Consumption-based models**

* pay as per use
* allow for better cost prediction

**kinds of services you'll find on Azure:**

* + Compute services such as VMs and containers that can run your applications
  + Database services that provide both relational and NoSQL choices
  + Identity services that help you authenticate and protect your users
  + Networking services that connect your datacentre to the cloud, provide high availability or host your DNS domain
  + Storage solutions that can accommodate massive amounts of both structured and unstructured data
  + AI and machine-learning services can analyse data, text, images, comprehend speech, and make predictions using data — changing the world of agriculture, healthcare, and much more.
  + DevOps
  + IOT

**Cloud deployment models**

Public cloud (azure, google are public cloud),

Advantages:

* + No CapEx. You don’t have to buy a new server in order to scale.
  + Agility. Applications can be made accessible quickly, and be provisioned whenever needed.
  + Consumption-based model. Organizations pay only for what they use, and operate under an OpEx model.
  + Maintenance. Organizations have no responsibility for hardware maintenance or updates.
  + Skills. No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.

Disadvantages:

* + Security. There may be specific security requirements that cannot be met by using public cloud.
  + Compliance. There may be government policies, industry standards, or legal requirements which public clouds cannot meet.
  + Ownership. Organizations don't own the hardware or services and cannot manage them as they may wish.
  + Specific scenarios. If organizations have a unique business requirement, such as having to maintain a legacy application, it may be hard to meet that requirement with public cloud services.

private cloud (Expensive-Azure stack ex. Government, financial institution)

- Azure stack help to achieve this

Advantages:

* + Control. Organizations have complete control over the resources.
  + Security. Organizations have complete control over security.
  + Compliance. If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.
  + Specific scenarios. If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.

Disadvantages:

* + -Upfront CapEx. Hardware must be purchased for start-up and maintenance.
  + -Agility. Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.
  + -Maintenance. Organizations have the responsibility for hardware maintenance and updates.
  + -Skills. Private clouds require in-house IT skills and expertise that may be hard to get or be costly.

Hybrid cloud (public + private cloud)

-Azure stack edge can help for this

Advantages:

* + Flexibility. The most flexible scenario: with a hybrid cloud setup, an organization can decide to run their applications either in a private cloud or in a public cloud.
  + Costs. Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.
  + Control. Organizations can still access resources over which they have total control.
  + Security. Organizations can still access resources for which they are responsible for security.
  + Compliance. Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.
  + Specific scenarios. Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications. In this case, they can keep the old system running locally, and connect it to the public cloud for authorization or storage. Additionally, they could host a website in the public cloud, and link it to a highly secure database hosted in their private cloud.

Disadvantages:

* + Upfront CapEx. Upfront CapEx is still required before organizations can leverage a private cloud.
  + Costs. Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.
  + Skills. Deep technical skills are still required to be able to set up a private cloud.
  + Ease of management. Organizations need to ensure there are clear guidelines to avoid confusion, complications or misuse.

Iaas = you have more control but comprise on scalability, availability

* + IaaS is useful for managing unpredictable demand and steadily growing storage needs
  + simplify the planning and management of backup and recovery systems.
  + shared responsibility model

Commonly used for

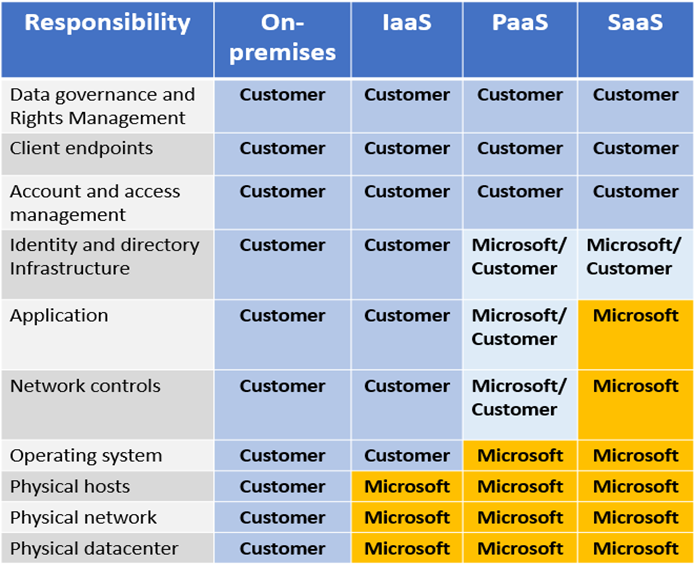
* + - -Migrating workloads
    - -Test and development
    - -Storage, backup, and recovery

Paas = could provider have more control, scalability, availability is high compare to iaas

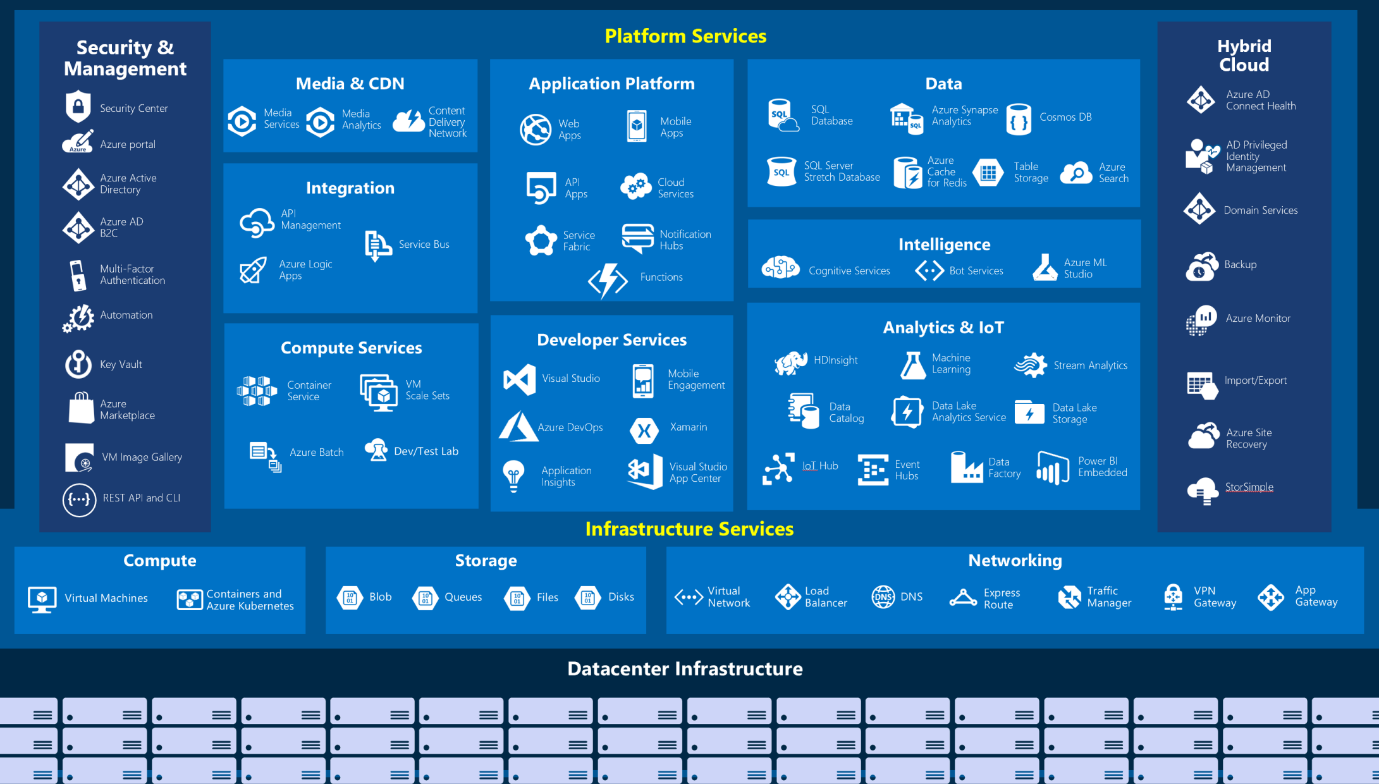
* + -provides an environment for building, testing, and deploying software applications.
  + -example, when deploying a web application using PaaS, you don't have to install an operating system, web server, or even system updates.
  + -commonly used in
    - -Development framework
    - -Analytics or business intelligence = Tools provided as a service with PaaS allow organizations to analyse and mine their data.

Saas = you have no control, it finished application ex. Gmail, google docs, only limitation here it cannot be customized

But you are responsible for configuring saas solution.

****

<https://docs.microsoft.com/en-us/learn/modules/principles-cloud-computing/5-types-of-cloud-services>



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Section 2 - Session 1**

Availability sets (maintenance domain & fault domain) >> availability Zones (disaster recovery) >> region (organized zones) >> geographic

Region - A region is a geographical area on the planet containing at least one, but potentially multiple datacentres that are in close proximity and networked together with a low-latency network.

* + Azure has more global regions than any other cloud provider.
  + Regions provide customers the flexibility and scale needed to bring applications closer to their users.
  + Regions preserve data residency and offer comprehensive compliance and resiliency options for customers.
  + For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be deployed.
  + not every product (service) is available in all region
  + **some global Azure services that do not require you to select a particular region, such as Microsoft Azure Active Directory, Microsoft Azure Traffic Manager, and Azure DNS.**
  + Minimum 3 zone in one region
  + Datacentres organized by region

**Region Pairs**

* It's possible that a large enough disaster could cause an outage large enough to affect even two datacentres. That's why Azure creates region pairs
* **Azure Geo-Redundant Storage (GRS)** replicates data to a secondary region automatically, ensuring that data is durable even in the event that the primary region isn't recoverable.

**Note that not all Azure services automatically replicate data, nor do all Azure services automatically fall-back from a failed region to its pair. In such cases, recovery and replication must be configured by the customer.**

Geographies

* + it has two or more regions under it
  + Apac, Europe, Americas, Africa and middle east
  + This division has several benefits.
    - Geographies allow customers with "specific data residency and compliance needs" to keep their data and applications close.
    - Geographies ensure that data residency, sovereignty, compliance, and resiliency requirements are honoured within geographical boundaries.
    - Geographies are fault-tolerant to withstand complete region failure through their connection to dedicated high-capacity networking infrastructure.

Availability Options

* Single Premium VM - SLA 99.9
* Availability Set - SLA 99.95 - are a way for you to ensure your application remains online if a high-impact maintenance event is required, or if a hardware failure occurs.
  + Update domains - it is logical section of the datacentre. When a maintenance event occurs (such as a performance update or critical security patch applied to the host), the update is sequenced through update domains
  + Fault domains- Fault domains provide for the physical separation of your workload across different hardware in the datacentre.
    - This includes power, cooling, and network hardware that supports the physical servers located in server racks.
    - In the event the hardware that supports a server rack becomes unavailable, only that rack of servers would be affected by the outage.

Availability Zone - SLA 99.99 - are physically separate locations within an Azure region that use availability sets to provide additional fault tolerance.

* You can use "Availability Zones to run mission-critical applications and build high-availability" into your application architecture by co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones.
* Availability Zones are primarily for "VMs, managed disks, load balancers, and SQL databases". Azure services that support Availability Zones fall into two categories:
  + Zonal services – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses)
  + Zone-redundant services – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).
  + Multi region - data residency maintained

**Azure Resource manager** (https://resources.azure.com/) - underlying engine (api of azure) - is a management layer in which resource groups and all the resources within it are created, configured, managed, and deleted.

It provides a consistent management layer which allows you automate the deployment and configuration of resources

using different automation and scripting tools, such as following tools can user ARM (Azure Resource manager) api to interact with azure

* + Microsoft Azure PowerShell,
  + Azure Command-Line Interface (Azure CLI),
  + Azure portal,
  + REST API,
  + client SDKs.

Azure Resource Manager, you can:

* Deploy Application resources
* Organize resources
* Control access and resources.
* You manage permissions by defining roles, adding users or groups to the roles, and applying policies at resource group level.

Examples of elements you may wish to control are: enforcing naming convention on resources, limiting which types and instances of resources can be deployed, or limiting which regions can host a type of resource.

<https://docs.microsoft.com/en-us/learn/modules/discuss-core-azure-architectural-components/9-explore-azure-resource-manager>



**Resource group**

folder, to manage resource - You can think of your resource group as a container that allows you to aggregate and manage all the resources required for your application in a single manageable unit

"You can manage and apply the following resources at resource group level:

* + Metering and billing
  + Policies
  + Monitoring and alerts
  + Quotas
  + Access control"

Resource groups can be created by using the following methods:

* + Azure portal
  + Azure PowerShell
  + Azure CLI
  + Templates
  + Azure SDKs (like .NET, Java)
  + REST API

NetworkWatcherRG. You can ignore this resource group, it's created automatically to enable Network Watcher in Azure virtual networks.

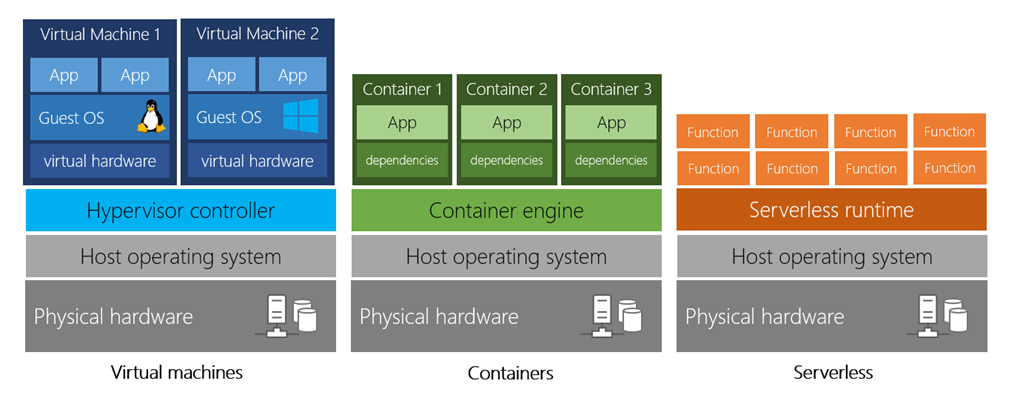
There are a few factors that can play into the strategy you use to organize resources: authorization, resource life cycle, and billing.

https://docs.microsoft.com/en-us/learn/modules/discuss-core-azure-architectural-components/8-explore-resource-groups

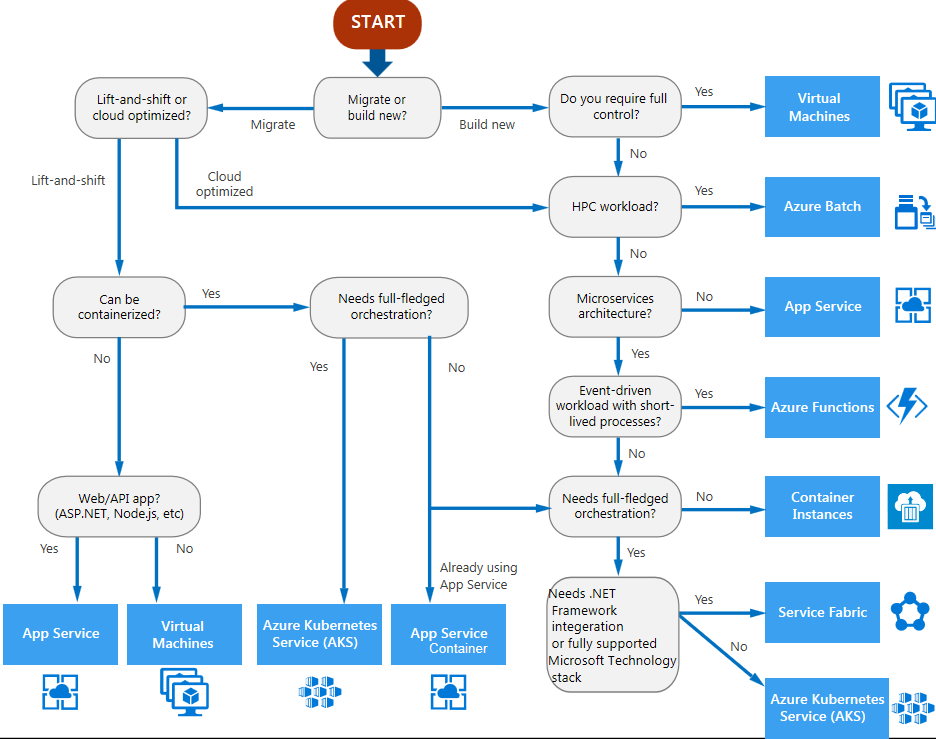
**Azure compute Services**

It provides computing resources such as disks, processors, memory, networking and operating systems.

* Virtual machines
* Virtual machine scale sets
  + Azure Insights Autoscale, autoscale virtual machines
  + help to achieve high availability and scalability when needed
* App services (Paas)
  + you can quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform.
* Functions (Server less architecture)
  + ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure
* Windows virtual desktop
  + check WVD image
  + allows to connect with you azure desktop/vm via browser
  + so allows to connect from any where
  + this is because of codivid and to support Work from home
* Virtual Machine
* Overview page - shows details of VM like operating system, ram
* you can increase size of ram , storage of vm via this
* Access Control - where you can set access control
* click on Connect
* RDP - remote desktop protocol for windows
* SSH - Secutre shell protocol for linux
* --Just in time access policy for security where you get time limited window to access machine
* Container = ex. docker - Pass (Server less architecture)
  + it’s not depend on operating system and allows to run multiple container (which contain application) on one machine
  + Containers are a virtualization environment.
  + Containers reference the operating system of the host environment that runs the container.
  + Unlike virtual machines you do not manage the operating system.
  + Containers are lightweight and are designed to be created, scaled out, and stopped dynamically.
  + Containers allows you to respond to changes on demand and quickly restart in case of a crash or hardware interruption.
  + Azure supports Docker containers.
  + we create, configure, and deploy a Docker container by using Azure Container Instances (ACI)
* VM vs Container
  + VM= virtualize hardware, if provide full control over Os and environment
  + Container = virtualize Operating system, it good for portable application and performance and can scale out easily, managed by container orchestrator
* Azure container registry
  + registry for container
* Azure Container Instances
  + fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services
  + It is a PaaS offering that allows you to upload your containers, which it will run for you.
* Azure Kubernetes Service (AKS) - is a complete orchestration service
  + to manage containers, automating, managing, and interacting with a large number of containers



<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/compute-decision-tree>



* Azure network services
  + Azure Network is software define networking.
  + Azure Virtual Network - enables many types of Azure resources such as Azure VMs to securely communicate with each other, the internet, and on-premises networks.
    - is scoped to a single region;
    - however, multiple virtual networks from different regions can be connected using virtual network peering.
  + VPN Subnet - Each VPN network consists of one or more useful IP range partitions called subnets.
  + Azure Load Balancer - can provide scale for your applications and create high availability for your services. 99.99%
  + Virtual Private Network (VPN) gateway - is a specific type of virtual network gateway that is used to send encrypted traffic between an Azure Virtual Network and an on-premises location over the public internet.

Azure Application Gateway - is a web traffic load balancer that enables you to manage traffic to your web applications

* + Content Delivery Network - is a distributed network of servers that can efficiently deliver web content to users.

Hybrid networking - <https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/vpn>

Azure stack = is portal version of azure public cloud but for local infrastructure, All services >> select App Services, allows to access azure services (IAAS,Paas,Saas) like azure service from local way i.e. private cloud way, you can link it with your on-premise network or with azure network

**VM-->Networking**

Virtual network --> created for you where you can put all related vm call VNET

https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/windows-vm

**NIC** - Network interface

* + this basically hardware but on cloud its software that allows to connect
  + Private IP address allow to connect with in Virtual network i.e VNET
  + Public IP address allows to connect outside
  + this means that you are exposing your VM outside i.e. public network where attack can happen
  + this means that you are exposing your VM outside i.e. public network where attack can happen

How to connect Azure VPN with On-premise Network

1. Point to Site VPN allows to connect single or private machine to Azure VPN via Gateway subnet.
2. VPN gateway in azure allow to connect on-premise network over public internet and encrypted communication, this is example of Site to site connection.
3. Express Route allows to connect on-premise network to azure network, this is dedicated and private connection not going via public internet.
4. Microsoft Peering allows to connect with Azure PAAS service.
5. Private end point is IP address of Pass Service with in VPN

**Load balancer VS Application Gateway**

* Load balancer- can use to balance load for any kind of traffic (its not specific to web), between any kind of resources i.e. vm, servers

- less expensive

- less complex

* Application gateway - can use to balance load for web application only i.e. web traffic, have Web application firewall
  + firewall,
  + traffic routing
  + terminating ssl & tsl connection give web server more cpu power

**Bastion**

[Azure Bastion](https://docs.microsoft.com/en-us/azure/bastion/) allows you to log into VMs in the virtual network through SSH or remote desktop protocol (RDP) without exposing the VMs directly to the internet. If you lose connectivity through the VPN, you can still use Bastion to manage the VMs in the virtual network.

**Load balancer that is not bound to region, help to distribute traffic**

**Traffic Manager**

**Front Load**

* Azure data categories
  + Structured data = Relational data
  + Semi-structured data = NoSQL data
  + Unstructured data = document, images, files
* Azure Storage -IAAS

Azure data storage provides data backup, load balancing, disaster recovery, and data replication as services to ensure data safety and high availability.

Redundancy : <https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

Tool- Storage explorer can be download and install on windows, allows to upload and download store data

service that you can use to store files, messages, tables, and other types of information

* Disk storage = VM disk storage
* Disk storage allows data to be persistently stored and accessed from an attached virtual hard disk.
* Disk encryption done via programmatically by Azure cli or PowerShell, it cannot be done via portal
* Typical scenarios for using disk storage are if you want to lift and shift applications that read and write data to persistent disks, or if you are storing data that is not required to be accessed from outside the virtual machine to which the disk is attached.

Type of disks - Storage types

* + - * HDD - for low important and in frequent access
      * Standard HDD - for entry level production
      * Premium HDD - enterprise production
      * Ultra Disk - for low latency
* Containers (Blobs)
  + Blob storage is optimized for storing massive amounts of unstructured data, such as text or binary data.
  + blob can allow to store data of vm, image, files, Streaming video and audio
  + for backup and restore, disaster recovery, and archiving
  + for analysis by an on-premises or Azure-hosted service
* Files
  + Files enables you to set up highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol.
  + Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analysed later
* Queues
  + is used to store and retrieve messages. Queue messages can be up to 64 KB in size, and a queue can contain millions of messages.
  + for messages, to send data from and to components i.e. microservices developed by developers
* Tables
  + are ideal for storing structured, non-relational data.
  + Tables and Queues mostly used by developers
* Storage Account
  + Storage tiers
    - Hot = frequent access data = Allow to read at low cost but, high charge for space occupied
    - Cool = infrequent access data (30 day) = less charges for store but high charges for read
    - Achieve = Rarely used data = data stored in archive need to rehydrate, and rehydrate operation is chargeable
      * after rehydrate put it in cool or hot tier

Storage account => to store data or bucket to store your stuff

-name of storage account is unique accross all azure storage accounts.

\* Creat Storage Account

--Replication = how many copy of storage account needed

--Access - hot means not archive, frequently accessed

\* after create

--Settings --> deployment --> activity log - shows deployment done what time and by who

**Azure Database Services- offered as paas**

https://azure.microsoft.com/en-us/product-categories/databases/

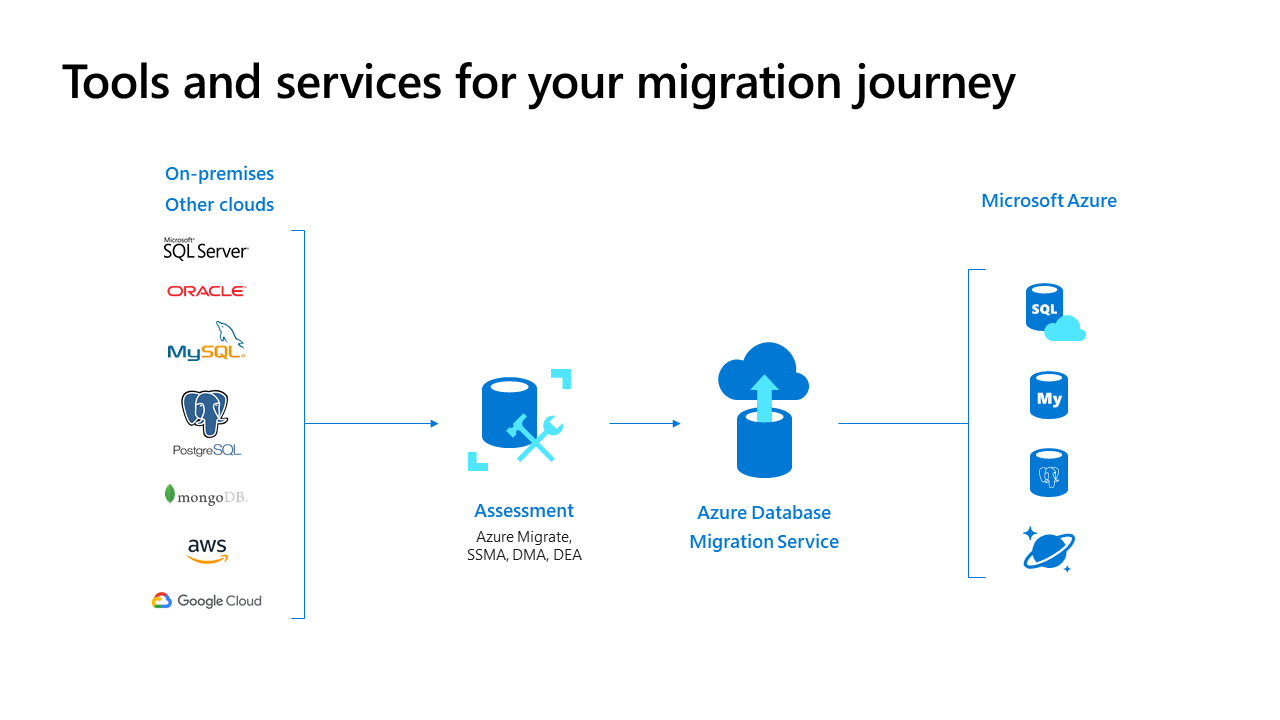
* Databases -- Paas -- All services blade >> SQL databases
* Azure SQL Server Managed instance - provide more control over underlying virtual machine
* Azure MySql, MariaDb, PostgreSql
* Azure Cosmos DB (PAAS)- supports schema-less data, globally distributed database service that enables you to elastically and independently scale throughput and storage across any number of Azure's geographic regions

**Azure SQL Database (Pass - DAAS)** - based on the latest stable version of Microsoft SQL Server database engine. Sla 99.995%

* Create Database Service to host Database
* you have to specify compute --> i.e. memory and ram
* Support vertical scaling
* geo-replication supported
* Security
  + Advance data security supported -
  + to remain in compliance by putting classification i.e by label
  + vulnerability assessment to remediate
* https://docs.microsoft.com/en-us/learn/modules/define-core-azure-services-products/13-walkthrough-create-sql-database

**Azure Database Migration** - fully managed service designed to enable seamless migrations from multiple database sources to Azure data platforms with minimal downtime

"Microsoft Data Migration Assistant" to generate assessment reports that provide recommendations to help guide you through required changes prior to performing a migration



**Non SQL db = Azure Cosmos DB main product**

* support 5 non sql db models
* document based model allows to write structure query

**Azure Marketplace**

* Microsoft application i.e. vm images
* third party application + Microsoft application
* service on Azure that helps connect end users with Microsoft partners, independent software vendors (ISVs), and start-ups that are offering their solutions and services, which are optimized to run on Azure.
* Azure Marketplace allows customers—mostly IT professionals and cloud developers—to find, try, purchase, and provision applications and services from hundreds of leading service providers, all certified to run on Azure.
* **Third party market product installed by you in azure are found in subscription**.

**Internet of Things**

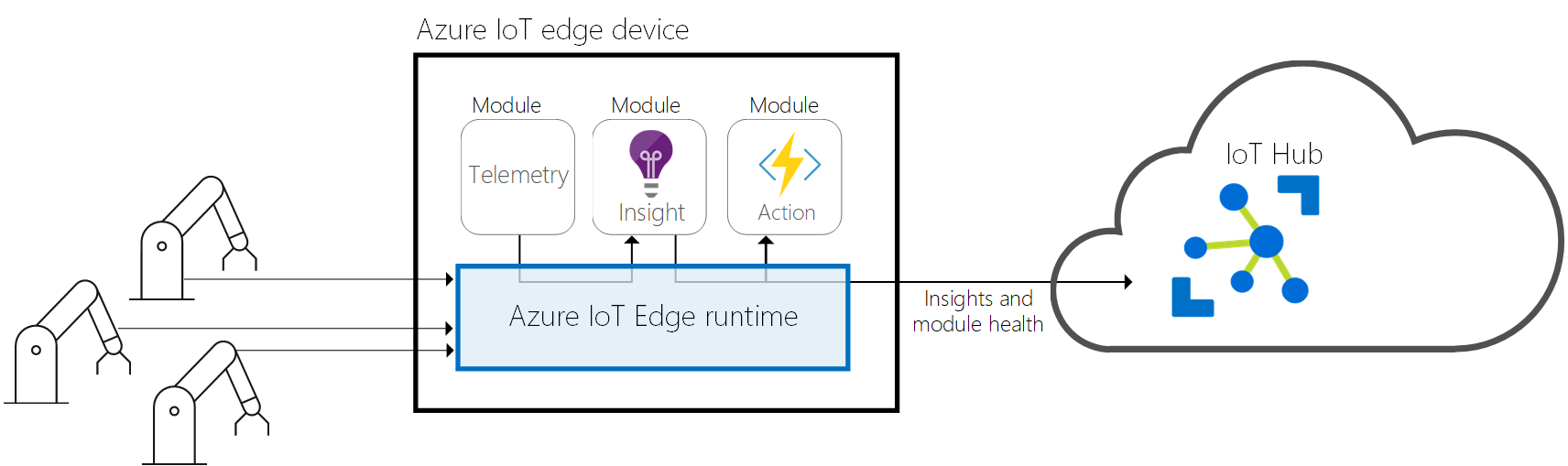
is the ability for devices to collect and then relay information for data analysis.

* IoT Central
  + software as a service (SaaS) solution that makes it easy to connect, monitor, and manage your IoT assets at scale
* Azure IoT Hub = All services >> select IoT Hub
  + aged service hosted in the cloud that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages.
  + messaging patterns such as device-to-cloud telemetry, file upload from devices, and request-reply methods
* Azure IOT Edge device -https://docs.microsoft.com/en-us/azure/iot-edge/about-iot-edge
  + is act as bridge between IOT device and Azure IOT hub
  + is receives data from IOT device and do operation on it and only pass relevant data to Azure IOT hub
* Azure Sphere
  + IOT device standardization as right now there is no standardization exists in IOT devices developed by different vendors

https://docs.microsoft.com/en-us/learn/modules/identify-azure-solutions/2-define-internet-of-things

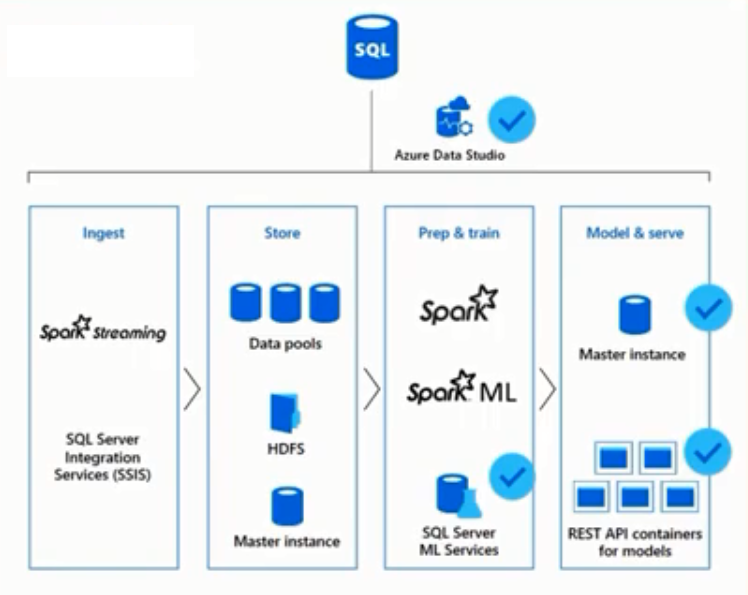
imp - https://azure.microsoft.com/en-us/overview/iot/product-selector/

<https://azure.microsoft.com/en-us/product-categories/iot/>



**Big data and analytics = 3V model = volume, velocity & variety**

-we talk about big data; we're referring to large volumes of data. Data from weather systems, communications systems, imaging platforms, and many other scenarios generate large amounts of data.



* Azure Synapse Analytics
* (formerly Azure SQL Data Warehouse + Apache spark for analytics) is a limitless analytics service that brings together enterprise data warehousing and big data analytics.
* Known data structures
* support horizontal scaling
* Store relational data
* OLAP database
* Azure HDInsight = Azure hosted Apache hadoop
* is a fully managed, open-source analytics service for enterprises.
* allows you run popular open-source frameworks and create cluster types such as Apache Spark, Apache Hadoop, Apache Kafka, Apache HBase, Apache Storm,
* Support Machine Learning Services
* Support ETL
* Support IOT
* Support Dataware housing
* This is costly solution as it keep running and reserve resource
* Azure Data Lake Analytics
  + is an on-demand analytics job service that simplifies big data.
  + Work on unknown data, structure
  + Instead of deploying, configuring, and tuning hardware, you write queries to transform your data and extract valuable insights
  + Charges occur when you run query so it like on demand service
* Azure Databricks = Azure cloud hosted Databricks
  + Databricks is third party product
  + Databricks= cloud hosted Apache spark
  + latest where big data analytics going
  + done work in memory
  + gen 2

R, Scala and python are language for big data

<https://docs.microsoft.com/en-us/learn/modules/identify-azure-solutions/4-explore-big-data-analytics>

**Azure Artificial Intelligence** -https://docs.microsoft.com/en-us/azure/machine-learning/overview-what-is-azure-ml

* the core of it is Machine Learning.
* Machine Learning is a data science technique that allows computers to use existing data to forecast future behaviours, outcomes, and trends.
* Using machine learning, computers learn without being explicitly programmed.
  + Azure Cognitive Services
    - are a collection of domain-specific pre-trained AI models that can be customized with your data
      * vision
      * speech
      * face
      * search
      * language
      * knowledge
* Azure Machine Learning Service = Azure Machine Learning
  + prediction and classification based on data and model developed i.e. algorithm
  + provides a cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models.
  + can auto-generate a model and auto-tune it for you.
  + pipelines and graphical designer
* Azure Bot
  + Application with human-like interaction, human like component
  + example: chat bot application
  + example : siri, google, alexa

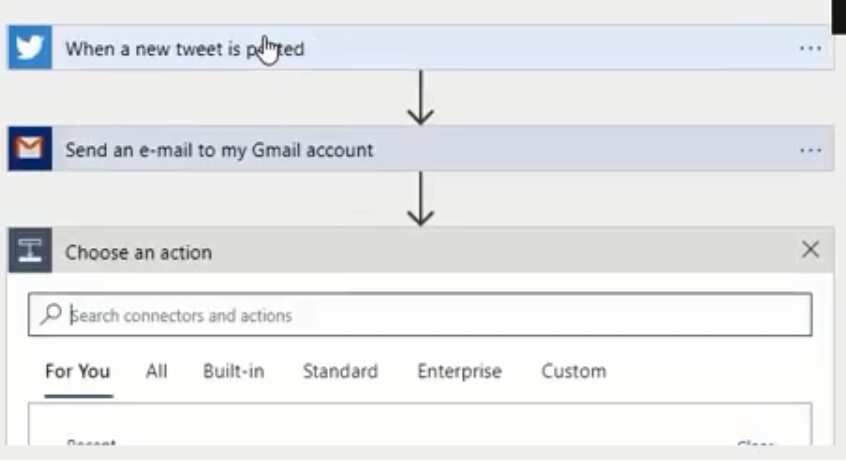
https://docs.microsoft.com/en-us/azure/bot-service/bot-service-overview-introduction?view=azure-bot-service-4.0

**Azure Databricks**

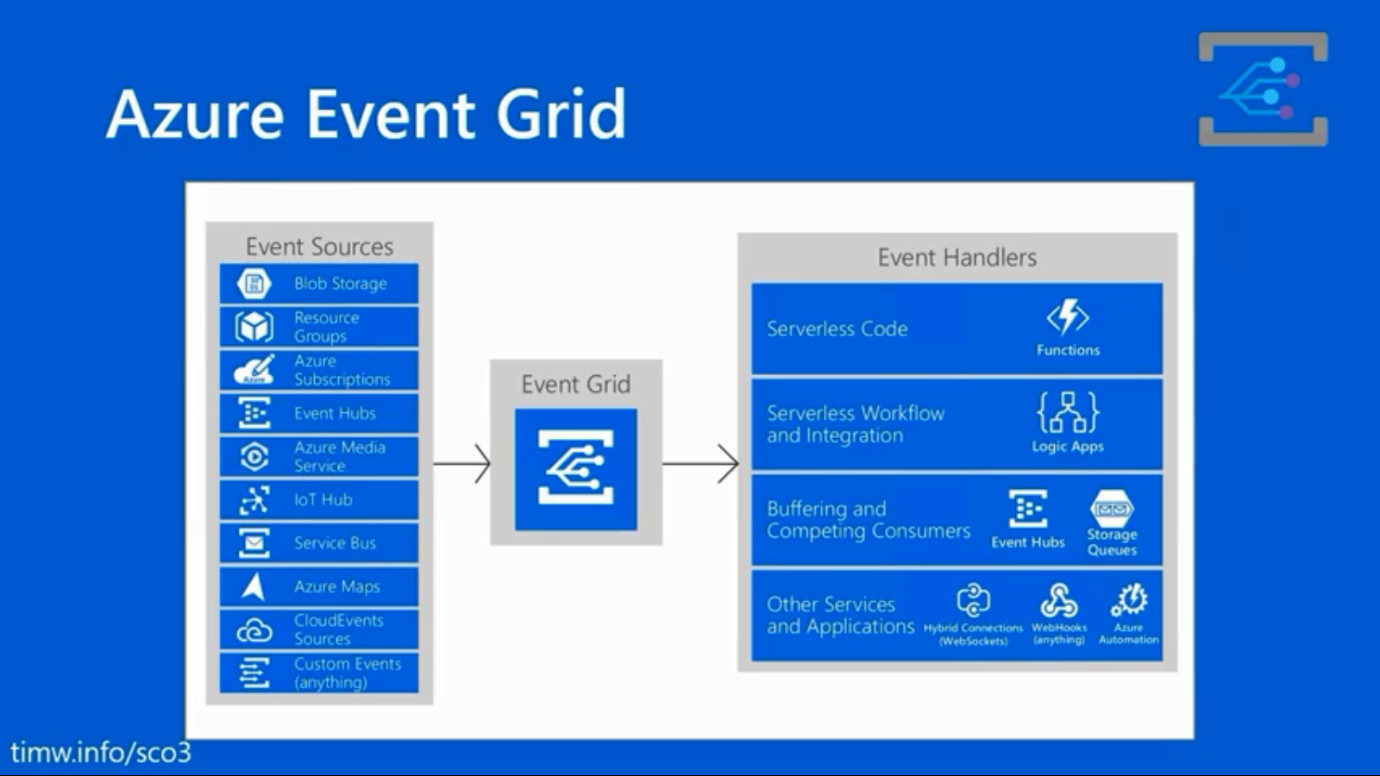
https://docs.microsoft.com/en-us/learn/modules/identify-azure-solutions/5-explore-artificial-intelligence

**Serverless computing**

* it take and runs your code and hide all other details under it , check the image
* cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment
* You configure your serverless apps to respond to events. An event could be a REST endpoint, a periodic timer, or even a message received from another Azure service. The serverless app runs only when it's triggered by an event.
  + Azure Functions = All services >> select Function ApP
    - need development skills
    - are ideal when you're only concerned with the code running your service and not the underlying platform or infrastructure.
    - Azure Functions are commonly used when you need to perform work in response to an event—often via a REST request, timer, or message from another Azure service—and when that work can be completed quickly, within seconds or less
    - scale automatically, and charges accrue only when a function is triggered, so they're a solid choice when demand is variable.
    - are stateless; they behave as if they're restarted every time they respond to an event. This is ideal for processing incoming data. And if state is required, they can be connected to an Azure storage service.
    - C#, java, javascript , powershell, python
  + Azure Logic Apps = for integration solution
    - helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations.
    - help to design and build scalable solutions—whether in the cloud, on premises, or both—for app integration, data integration, system integration, enterprise application integration (EAI), and business-to-business (B2B) integration.
    - web-based designer and can execute logic triggered by Azure services without writing any code.
    - -include services such as Salesforce, SAP, Oracle DB, and file shares.



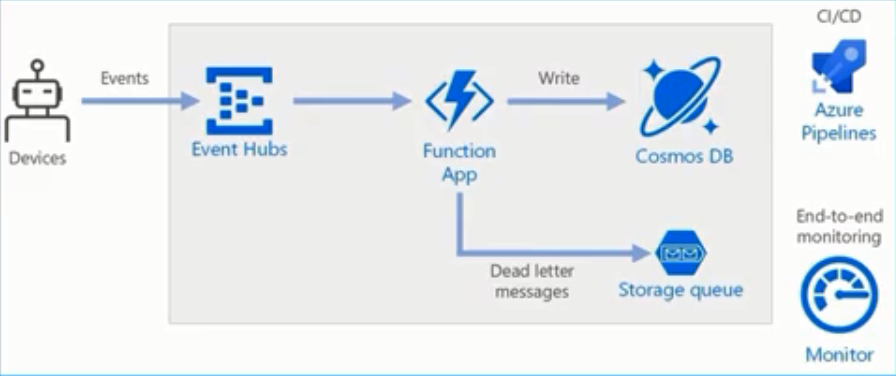
* + Azure Event Grid
    - allows you to easily build applications with event-based architectures.
    - topic based
    - reactive programming based
    - check image



**Azure event hub**

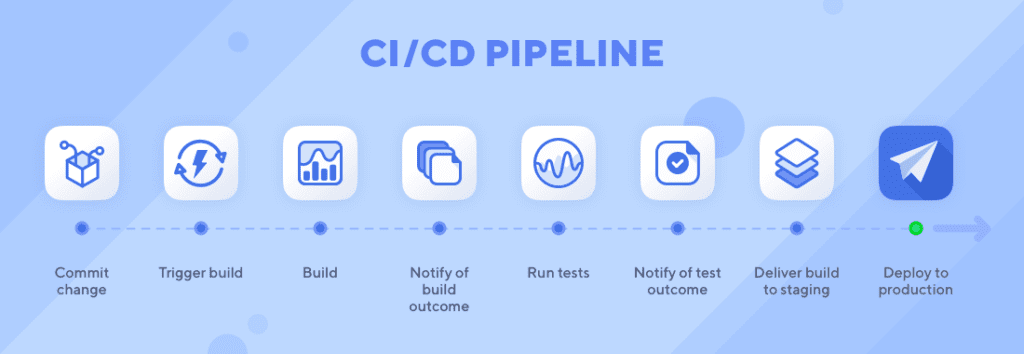
**Azure even grid vs Azure event hub**

* + basic difference is data, that process by this services
  + event hub receives telemetry (collection of measurement) ex. data from IOT devices basically tsunami of messages from that yours subscribe to few of them other side
  + event grid receives data based on topic subscription done by end service, application or resource



**Azure DevOps**

allows you to create, build, and release pipelines that provide continuous integration, delivery, and deployment for your applications.



* Azure DevOps Services
  + provides development collaboration tools including high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing.
* Azure Lab Services or Azure DevTest labs
  + <https://docs.microsoft.com/en-us/azure/devtest-labs/devtest-lab-overview>
  + service that helps developers and testers quickly create environments in Azure, while minimizing waste and controlling cost.
  + It saves time of administrator and dev both as admin don’t have to create machine every time dev request machine and dev can easily claim machine already present in dev/test lab without any delay
  + It provides way to create pre-configured machines i.e. machine get created based on some automation and saved images & new tools get added easily so dev doesn’t have to worry about creating machine from the Scrach
  + It also helps to control save cost by putting policies and governance like size of vm

**Azure App Service = All services >> App Services**

* quickly and easily build web and mobile apps for any platform or device. Azure App Service enables you to build and host web apps, mobile back ends, and RESTful APIs in the programming language of your choice without managing infrastructure.
* is actually a collection of four services, all of which are built to help you host and run web applications. The four services (Web Apps, Mobile Apps, API Apps, and Logic Apps) look different, but in the end they all operate in similar ways.

Supports

* Multiple languages and frameworks.
* DevOps optimization.
* Global scale with high availability
* Connections to SaaS platforms and on-premises data
* Security and compliance
* Application templates
* Visual Studio integration
* API and mobile features
* Serverless code
  + Server less deployment -- allows to deploy code

**Azure Management tools**

tools available for the command line, language-specific Software Development Kits (SDKs), developer tools, tools for migration, and many others.

* Azure portal
  + is a public website that you can access with any web browser.
  + After you sign in with your Azure account, you can create, manage, and monitor any available Azure services.
  + You can identify a service you're looking for, get links for help on a topic, and deploy, manage, and delete resources.
  + It also guides you through complex administrative tasks using wizards and tooltips.
  + -"does not provide any way to automate repetitive tasks"
* Azure PowerShell
  + is a module that you add to Windows PowerShell or PowerShell Core that enables you to connect to your Azure subscription and manage resources.
* Azure Command Line Interface (CLI)
  + is a cross-platform command-line program that connects to Azure and executes administrative commands on Azure resources.
* Azure Cloud Shell
  + is a browser-based scripting environment in your portal.
  + it allows you to choose either PowerShell or Command line interface to intrect with azure services
* Azure Mobile App
  + not all features of azure feature
  + -allows you to access, manage, and monitor all your Azure accounts and resources from your iOS or Android phone or tablet.
  + Use the Azure Cloud Shell to run saved scripts or perform unplanned administrative tasks
* Azure REST API
  + are service endpoints that support sets of HTTP operations (methods), which provide create, retrieve, update, or delete access to the service's resources.
* Azure SDK
  + available for all language
  + retry and error correction
  + under the hood gives call to rest api
* Azure portal app
  + desktop application
  + this is for windows machines only

Create a Virtual Machine with a Template

-In a browser, access the Azure quickstart Templates gallery . In the gallery, you will find a number of popular and recently updated templates. These templates automate deployment of Azure resources, including installation of popular software packages.

-Deploy Azure resources through the Azure Resource Manager with community contributed templates to get more done. Deploy, learn, fork and contribute back.

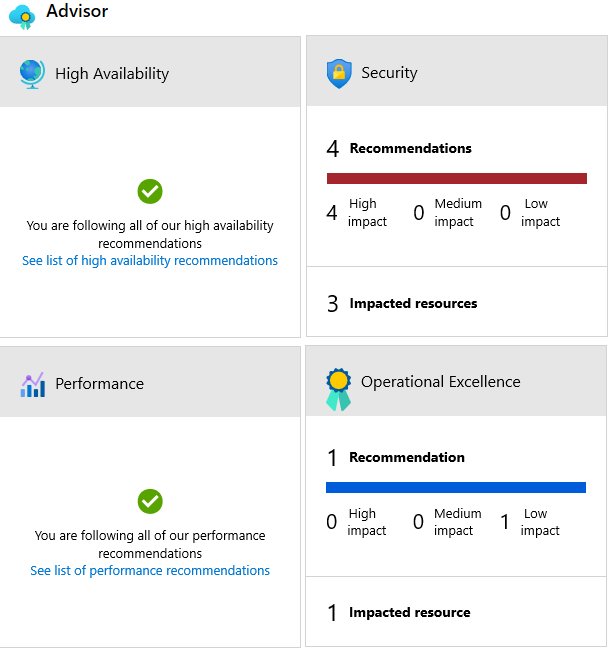
<https://docs.microsoft.com/en-us/learn/modules/differentiate-azure-management-tools/4-template>

**Azure advisor = All services >> select Advisor.**

* free service built into Azure that provides recommendations on high availability, security, performance, and cost.
* can help to set alert
* provide remediation i.e. repair suggestions

Azure naming convection - search on google give you guidelines

Geo redundancy = allows to replicate db multiple location



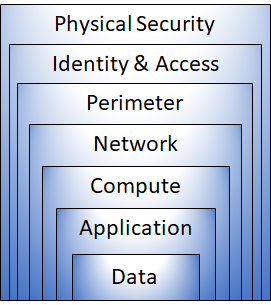
**Section 3 - Security, Privacy, Compliance and Trust with Azure**

**Security** - is still a shared responsibility.

* How much of that responsibility falls on us depends on which model we use with Azure.
* We use the defence in depth rings as a guideline for considering what protections are adequate for our data and environments.

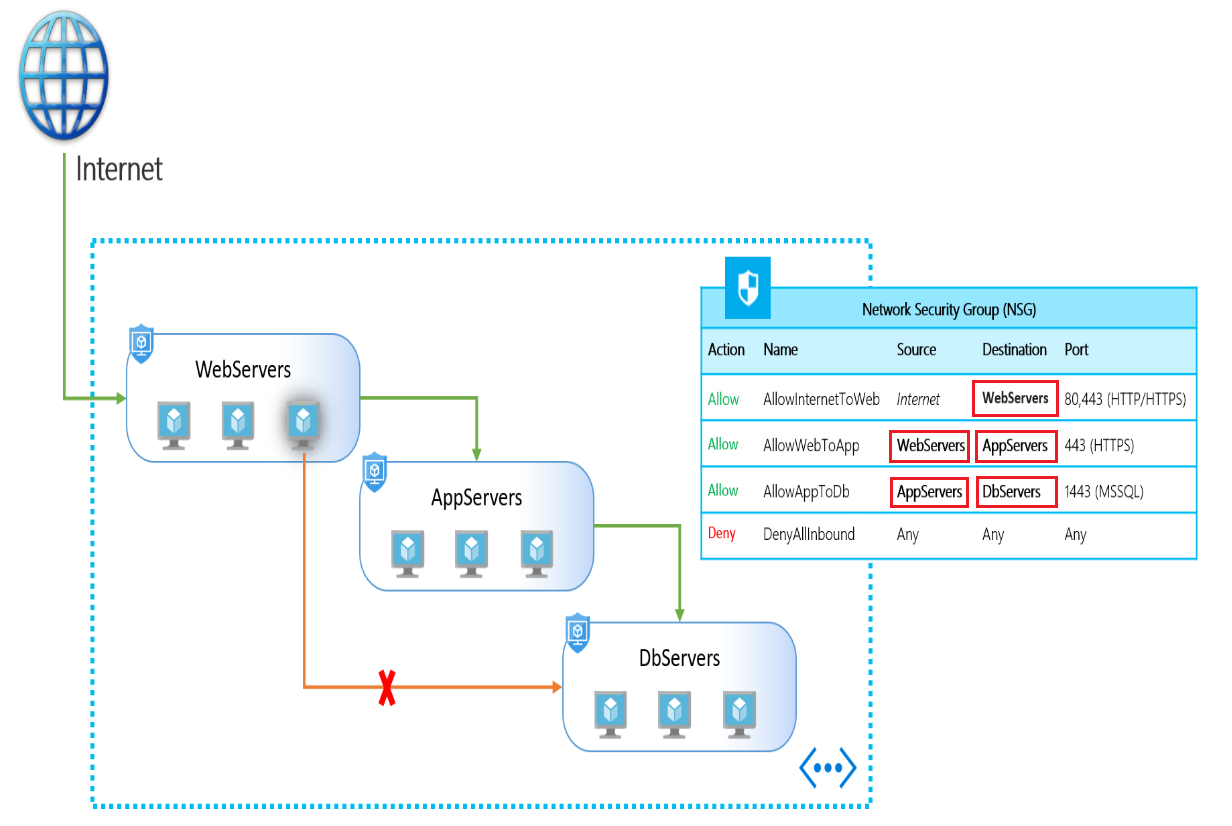
**Defence in depth**

* is a strategy that employs a series of mechanisms to slow the advance of an attack aimed at acquiring unauthorized access to data.
* The common principles used to define a security posture are confidentiality, integrity, and availability, known collectively as CIA
* <https://docs.microsoft.com/en-us/learn/paths/azure-well-architected-framework/>
* Video: <https://azure.microsoft.com/en-us/resources/videos/defense-in-depth-security-in-azure/>



**below can be configure or take action to protect**

* Physical security = not in consumer hand i.e not in our our hand , is the first line of defense to protect computing hardware in the datacenter.
  + Physical building security and controlling access to computing hardware within the data center is the first line of defense.
* Identity & Access = (Authentication and Authorization) controls access to infrastructure and change control.
  + -Control access to infrastructure and change control.
  + -Use single sign-on and multi-factor authentication.
  + -Audit events and changes.
* Perimeter= VPN == product use Azure firewall, DDOs, layer uses distributed denial-of-service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
  + Use distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for end users.
  + Use perimeter firewalls to identify and alert on malicious attacks against your network.
* Network = product use NSG, layer limits communication between resources through segmentation and access controls.
  + Limit communication between resources.
  + Deny by default.
  + Restrict inbound internet access and limit outbound, where appropriate.
  + Implement secure connectivity to on-premises networks.



* Compute = VM, layer secures access to virtual machines.
  + Secure access to virtual machines.
  + Implement endpoint protection and keep systems patched and current.
* Application - layer ensures applications are secure and free of vulnerabilities.
  + Store sensitive application secrets in a secure storage medium.
  + Make security a design requirement for all application development.
* Data
  + It's the responsibility of those storing and controlling access to data to ensure that it's properly secured.
  + Often, there are regulatory requirements that dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.
* CIA = confidentiality, integrity, and availability
  + Confidentiality - The Principle of least privilege restricts access to information only to individuals explicitly granted access. This information includes protection of user passwords, remote access certificates, and email content.
  + Integrity - The prevention of unauthorized changes to information at rest or in transit. A common approach used in data transmission is for the sender to create a unique fingerprint of the data using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The data's hash is recalculated and compared to the original by the receiver to ensure the data wasn't lost or modified in transit.
  + Availability - Ensure services are available to authorized users. Denial of service attacks are a prevalent cause of loss of availability to users.

**Define shared security**

**Azure Firewall** - is a managed, cloud-based, network security service that protects your Azure Virtual Network resources , Faas - Firewall as a service

<https://www.youtube.com/watch?v=E_5YP85kuI0&list=PLYGZ9Q0oTOHfsI-3IAhvyc09ssPDfoePv&index=30>

https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity/4-explore-azure-firewall

* A Firewall is a service that grants server access based on the "originating IP address" of each request.
* Firewall rules also include "specific network protocol and port information".
* **You can "create, enforce, and log", "application and network connectivity policies across subscriptions, and virtual networks, centrally".**
* You create firewall rules that specify ranges of IP addresses.
* Only clients from these "granted IP addresses" will be allowed to access the server.
* Firewall rules also include specific network protocol and port information.
* statefull - means if rule is created for traffic coming in from certain ip address there is no need to create rule for traffic going out,
* it keeps track of traffic coming in
* it screens traffic very deeply to make it more secure
* Azure Firewall provides many features, including:
  + Built-in high availability.
  + Unrestricted cloud scalability.
  + Inbound and outbound filtering rules.
  + Azure Monitor logging.
* create NAT rules, Network rules and Application rules
* **Common usage scenarios**
  + You typically deploy Azure Firewall on a central virtual network to control general network access. **With Azure Firewall you can configure:**
    - Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
    - Network rules that define source address, protocol, destination port, and destination address.

Azure Application Gateway also provides a firewall, called the Web Application Firewall (WAF).

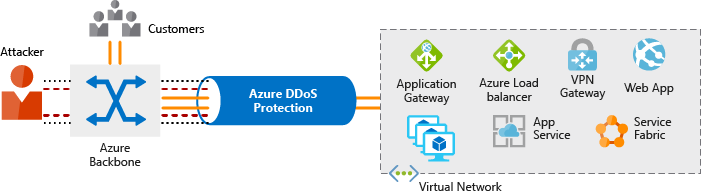
WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities.

**Azure Distributed Denial of Service protection**

* service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.
* no configuration required

**Distributed Denial of Service (DDoS)** - attacks attempt to overwhelm and exhaust an application’s resources, making the application slow or unresponsive to legitimate users.

* DDoS attacks can be targeted at any endpoint that is publicly reachable through the internet. Thus, any resource exposed to the internet, such as a website, is potentially at risk from a DDoS attack.



**Azure DDoS Protection provides the following service tiers:**

* Basic = The Basic service tier is automatically enabled as part of the Azure platform
  + Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defences that Microsoft’s online services use
  + public ip address protection but no telemetry, you don’t know what happen
* Standard = Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms.
  + Policies are applied to public IP addresses which are associated with resources deployed in virtual networks, such as Azure Load Balancer and Application Gate
  + here you can get notifications of attack on your resources with help of machine learning
  + you get telemetry data log, metrics & monitoring
  + it covers all resources where basic cover only public ip address
  + to costly

DDoS standard protection can mitigate the following types of attacks:

* Volumetric attacks. The attack's goal is to flood the network layer with a substantial amount of seemingly legitimate traffic.
* Protocol attacks. These attacks render a target inaccessible, by exploiting a weakness in the layer 3 and layer 4 protocol stack.
* Resource (application) layer attacks. These attacks target web application packets to disrupt the transmission of data between hosts.

Distributed Denial of Service – DDOS

* to protect azure resource having public ip address , so it not get attacked and get out of service
* provide basic protection which is default and premium

**Network Security Groups** - set rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol

(NSG) Network Security Group Firewall- this provide basic security to create access rules

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You cannot remove the default rules, but you can override them by creating new rules with higher priorities.

* + firewall but work in network only
  + its software
  + Usage: stop denial of service(dos) attack and brute-force attack based
  + NSG you can define rules based on below
    - source and destination ip address
    - source and destination port number
    - protocol
  + apply at machine level or at Subnet level (VPN subnet)
  + create problem when applied machine level and subnet level
  + stateful packet firewall

https://docs.microsoft.com/en-us/azure/virtual-network/security-overview

**Application Security Groups**

* allowing you to group virtual machines and define network security policies based on those group
  + An Application Security Group enables you to group servers with similar port filtering requirements, and group together servers with similar functions, such as web servers.

-example, we have ASGs defined for Web Servers, App Servers, and DB Servers

Choose Azure network security solutions

* Perimeter= VPN == product use Azure firewall, DDOs,
* Network = product use NSG

Combine services

* Network security groups and Azure Firewall
* Network security groups provide distributed network layer traffic filtering to limit traffic to resources within virtual networks in each subscription.
* Azure Firewall is a fully stateful, centralized network firewall-as-a-service, which provides network and application-level protection across different subscriptions and virtual networks

**Application Gateway WAF and Azure Firewall**

* WAF is a feature of Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities.
* Azure Firewall provides inbound protection for non-HTTP/S protocols (for example, RDP, SSH, FTP), outbound network-level protection for all ports and protocols, and application-level protection for outbound HTTP/S

**Identity and access**

* involves network perimeters, firewalls, and physical access controls.
* Identity has become the new primary security boundary

Two fundamental concepts that need to be understood when talking about identity and access are

* Authentication = act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control use. It establishes if they are who they say they are.
* Authorization = what level of access an authenticated person or service has

Identity can be

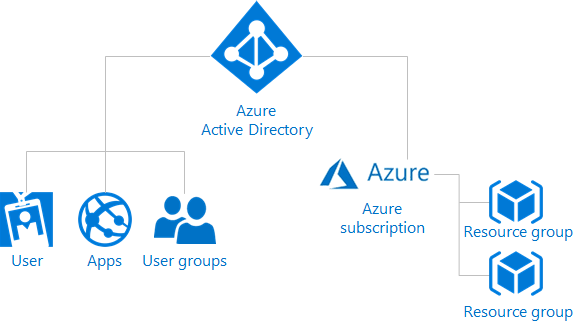
* + - user
    - service principle i.e. for applications

**Azure Active Directory** (<https://www.youtube.com/watch?v=mSxS0DW7fOs&list=PLYGZ9Q0oTOHfsI-3IAhvyc09ssPDfoePv&index=33>)

<https://www.youtube.com/watch?v=EUVKEhiHYG0-> 29 min onwards

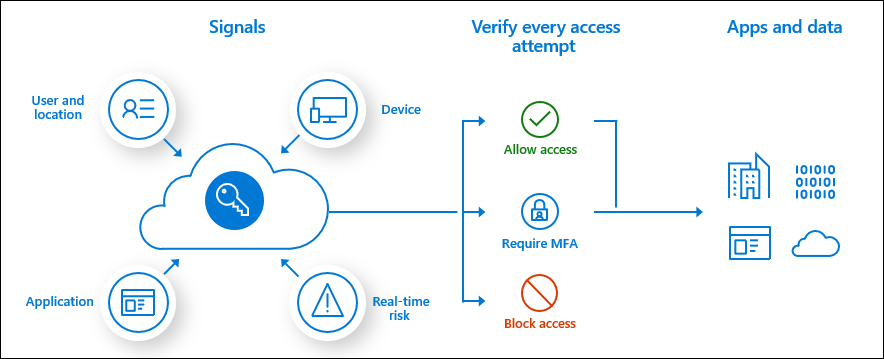
* is a Microsoft cloud-based identity and access management service. Azure AD helps employees of an organization sign in and access resources
* External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.
* Internal resources might include apps on your corporate network and intranet, along with any cloud apps developed by your own organization.
* Multi-tenant - multiple azure directory under on subscription
* single ad tenant id coming from other AD or outside AD
* **Azure Ad connect - to sync account with your local domain**
* Company branding - set your log and details of your company
* Groups help to simplify resource access and license distribution.

Azure AD group - Azure Directory - have dynamic group where user get assigned based on rules



**Azure AD provides services**

* Authentication
  + Authenticate service or person
* Providing functionality such as
  + self-service password reset,
  + multi-factor authentication (MFA),
  + a custom banned password list, and
  + smart lockout services.
  + Single sign-on (SSO)
    - Enables users to remember only one ID and one password to access multiple applications.
    - A single identity is tied to a user, simplifying the security model.
    - As users change roles or leave an organization, access modifications are tied to that identity, greatly reducing the effort needed to change or disable accounts.
  + Application management
    - manage your cloud and on-premises apps using Azure AD Application Proxy, single sign-on, the My apps portal (also referred to as Access panel), and SaaS apps.
  + Business to business
    - help to manage you azure users i.e. employees
    - Manage your guest users and external partners while maintaining control over your own corporate data
  + Business-to-customer
    - this helps to manage user of your application i.e. not azure users but user of application your developed
    - Customize and control how users sign up, sign in, and manage their profiles when using your apps with services.
  + Device management
    - this about connecting via person devices or on premises devices
    - Manage how your cloud or on-premises devices access your corporate data
  + Domain Services
    - it for decommission on premise AD
  + Conditional access



* + Identity protection – p2 licence required this is about sign in and identity of user.
* Azure AD intended or used by
  + IT administrators
  + App developers
  + Microsoft 365, Microsoft Office 365, Azure, or Microsoft Dynamics CRM Online subscribers
* **Dynamic groups in AD get created based on condition or lets based on rule setup in AD.**

At Active directory level Azure admin can assigned licence to user for using azure application like office 365 licence allow to user office 365

here: myapp.microsoft.com

**Resources role**

owner - at manage group level

**Azure AD roles**

* Global Administrator
* User
* custom role

Global administrator- highest role in AD different from Resource role

Azure AD for single sign-on you'll also have the ability to combine multiple data sources into an intelligent security graph.

This security graph enables the ability to provide threat analysis and real-time identity protection to all accounts in Azure AD, including accounts that are synchronized from your on-premises AD.

By using a centralized identity provider, you'll have centralized the security controls, reporting, alerting, and administration of your identity infrastructure.

**Azure Multi-Factor Authentication**

* Global Administrator role is need to set this up
* it will ask your other details apart form your password like security question, text code sent on mobile phone, biometric property, such as a fingerprint or face scan
* additional security for your identities by requiring two or more elements for full authentication.

Multi-factor authentication (MFA) comes as part of the following Azure service offerings

* Azure Active Directory premium licenses
* Multi-factor authentication for Office 365
* Azure Active Directory global administrators

**Azure AD Conditional Access - premium**

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview

* to add AD user
* when use login to azure it will verified against conditional access policies set if rule matches login allowed or not allowed
* example. what is ip address
  + what device ex. mobile or computer
  + location of user
  + application trying to access

**Security tools and features**

concepts for protecting your infrastructure and data when you work in the cloud.

This module will help you understand the core security tools available to support you.

**Azure Security Centre**

* is a monitoring service that provides threat protection across all of your services both in Azure, and on-premise
* centralizes much of the help Azure has to offer.
* It provides a single dashboard, with a view into many of your services, and helps make sure you are following best practices.
* Continuously updated machine learning algorithms help identify whether the latest threats are aimed at your resources.
* And, it helps your organization mitigate threats.

Security Centre gives you defence in depth with its ability to both detect and help protect against threats.

Using machine learning to process trillions of signals across Microsoft services and systems, Security Centre alerts you of threats to your environments, such as remote desktop protocol (RDP) brute-force attacks and SQL injections.

* And it provides actionable recommendations for mitigating these threats.
* support hybrid cloud – for start subscription
* Secure score -
* it for all subscription i.e. environment
* based on resources, and how resource setup done
* high score lower security threats
* Security policy
  + integrate with azure policy
* Security alerts
* **"Regulatory compliance dashboard and reports"**
* Provide security recommendations based on your configurations, resources, and networks.
* Monitor security settings across on-premises and cloud workloads, and automatically apply required security to new services as they come online.
* Continuously monitor all your services and perform automatic security assessments to identify potential vulnerabilities before they can be exploited.
* **Use machine learning to detect and block malware from being installed on your virtual machines and services. You can also define a list of allowed applications to ensure that only the apps you validate can execute.**
* Analyse and identify potential inbound attacks and help to investigate threats and any post-breach activity that might have occurred.
* **Provide just-in-time access control for ports**, reducing your attack surface by ensuring the network only allows traffic that you require.
* The Security Centre blade from the Azure portal includes the ‘regulatory compliance dashboard’.
* **The regulatory compliance dashboard provides insight into your compliance posture for a set of supported standards and regulations, based on continuous assessments of your Azure environment.**

Two types

* Free = limited to assessments and recommendations of Azure resources only
* Standard = full suite of security-related services including continuous monitoring, threat detection, just-in-time access control for ports, and more.

you will get it for free for 30 day then it require upgrade to standard.

To upgrade a subscription, you must be assigned the role of

* Subscription Owner,
* Subscription Contributor, or
* Security Admin.

-Example 1 - Use Security Centre for an incident response



-Example 2 - Use Security Centre recommendations to enhance security

A security policy

* defines the set of controls that are recommended for resources within that specified subscription or resource group.
* In Security Centre, you define policies according to your company's security requirements.

https://docs.microsoft.com/en-us/learn/modules/review-security-tools-features/3-walkthrough-azure-security-center-usage-scenario

**Azure sentinal used by info sec professional**

* SIEM(security information event management) and SOAR(security orchestration automated response) product
* One stop shop for Security alert detection
* in azure environment and also in outside azure environment
* proactive threat hunting
* threat response
* can remediate outside azure via playbooks
* have connector to connect with third party products and other cloud service
* support jupyter not book and kusto query language
* it is extension to security center
* it includes monitoring security for hybrid cloud + third party vendor products
* full time security professional
* integrate with other vendor product

**Key Vault = All services blade >> select Key vaults**

is a centralized cloud service for storing your applications' secrets.

where to use

* Secrets management - store and tightly control access to tokens, passwords, certificates, Application Programming Interface (API) keys, and other secrets.
* Key management - Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys used to encrypt your data.
* Certificate management - provision, manage, and deploy your public and private Secure Sockets Layer/ Transport Layer Security (SSL/ TLS) certificates
* Store secrets backed by hardware security modules (this paid service for free software based approach used) - protected either by software, or by FIPS 140-2 Level 2 validated HSMs
* It integrates with azure resources easily
* It allows programmatically getting value without exposing

Use Case:

* use password in resource template i.e. vm template
* VM disk encryption
* Application secretes

**HSM** – hardware security module available with **premium** key-Vault version and that make use of hardware, it’s for very long key value

Lower cost key vault uses software to generate value , for encription

Key-Vault

it used to store password i.e. secrete data in it , and retrieve that without exposing password help in authenticate and authorization.

developer rather than putting key in program make use of key vault to store key and use it programmatically to authenticate user.

This helps to authenticate user programmatically by using key value.

integration of key-vault for authentication with program is not possible with portal but powershell and azure CLI can be used for this.

**Azure Information Protection (AIP)**

is a cloud-based solution that helps organizations classify and (optionally) protect its documents and emails by applying labels.

* does content scanning based on rules and apply label/classification to document required premium feature and separate licence required for this
* you need to create or use existing label and policy

**Azure Advanced Threat Protection (ATP)**

is a cloud-based security solution that identifies, detects, and helps you investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

is a cloud-based security solution that "**leverages your on-premises Active Directory signals**" to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

Components

* Azure Advanced Threat Protection (ATP) portal
  + you can monitor and respond to suspicious activity
  + portal to monitor, manage, and investigate threats in your network environment.
* Azure Advanced Threat Protection (ATP) sensor
  + installed directly on your domain controllers
  + without requiring a dedicated server or configuring port mirroring
* Azure Advanced Threat Protection (ATP) cloud service
  + runs on Azure infrastructure and is currently deployed in the United States, Europe, and Asia is connected to Microsoft's intelligent security graph

How to purchase

* Azure Advanced Threat Protection is available as part of the Enterprise Mobility + Security 5 suite (EMS E5), and as a standalone license.

Use-case:

* + - to prevent kill chain cyber-attack on your local active directory
    - data theft and data protection
    - basically protect against attack on local AD directory theft
    - it installs sensor for detecting threat
    - cloud app security portal license is required to use this

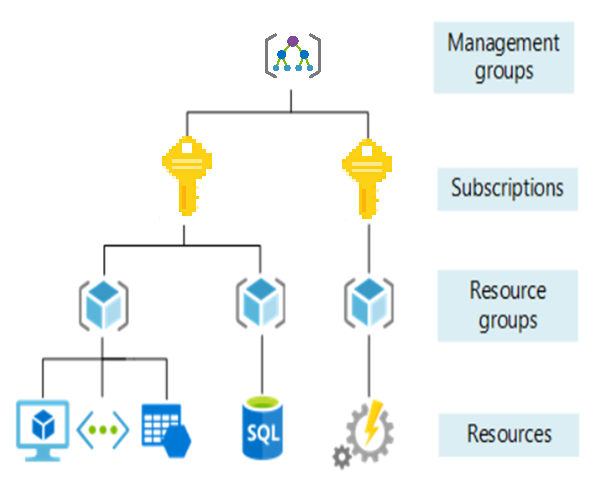
**Azure governance methodologies**

Good IT governance involves planning your initiatives and setting priorities on a strategic level to help manage and prevent issues

You need good governance when:

* You have multiple engineering teams working in Azure
* You have multiple subscriptions in your tenant
* You have regulatory requirements that must be enforced
* You want to ensure standards are followed for all IT allocated resources

In addition to providing IT standards, you need to be able to monitor your resources to make sure they are responsive and performing properly , following is image of how governance control flow in azure



**Azure Policy**

* is a service in Azure that you use to create, assign, and, manage policies
* policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements (SLAs
* can also integrate with Azure DevOps
* automatically remediate resources and configurations that are deemed non-compliant, thus ensuring the integrity of the state of the resources.
* comes with a number of built-in policy and initiative definitions that you can use, under categories such as
  + Storage,
  + Networking,
  + Compute,
  + Security Center, and
  + Monitoring.
* Example:
* applying specific tag on resource
* applying specific location on resource
* VM should of given size only
* enable diagnose on resource
* compliance, organization policy, budget
* can create policy (modify or dployifnotexists) to remediate when policy fails define in, for this MSI(manage service identity) id required as it related security who can deploy or modify resource

**Policy definition**

* A policy definition expresses what to evaluate and what action to take
* Every policy definition has conditions under which it is enforced. And, it has an accompanying effect that takes place if the conditions are met.
* Example policy definitions:
  + Allowed storage account SKUs - This policy definition has a set of conditions/rules that determine whether a storage account that is being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that do not adhere to the set of defined SKU sizes.
  + Allowed resource type - This policy definition has a set of conditions/rules to specify the resource types that your organization can deploy. Its effect is to deny all resources that are not part of the defined list.
  + Allowed locations - This policy enables you to restrict the locations that your organization can specify when deploying resources. Its effect is used to enforce your geographic compliance requirements.
  + Allowed Virtual Machine SKUs - This policy enables you to specify a set of VM SKUs that your organization can deploy.

Policy evaluation results

* When a condition is evaluated against your existing resources it is marked compliant or non-compliant.
  + You can review the non-compliant policy results and take any action that is needed.
* Policy evaluation happens about once an hour, which means that if you make changes to your policy definition and create a policy assignment then it will be re-evaluated over your resources within the hour.

**Policy initiatives = Home >> Policy - Definitions >> Authoring >> Assignment**

* An initiative definition is a set of policy definitions to help track your compliance state for a larger goal
  + Example, create Policy initiative named Enable Monitoring in Azure Security Center, with a goal to monitor all the available security recommendations in your Azure Security Center.
  + Under this initiative, you would have the following policy definitions:
  + Monitor unencrypted SQL Database in Security Center – For monitoring unencrypted SQL databases and servers.
  + Monitor OS vulnerabilities in Security Center – For monitoring servers that do not satisfy the configured baseline.
  + Monitor missing Endpoint Protection in Security Center – For monitoring servers without an installed endpoint protection agent.

https://docs.microsoft.com/en-us/learn/modules/describe-azure-governance-methodologie/4-define-policy-initiatives

Create a policy assignment = All services blade >> search for and select Policy >> under the Authoring >> section click Definitions

**Role-Based Access Control (RBAC)**

* RBAC, segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.
* Instead of giving everybody unrestricted permissions in your Azure subscription or resources, allow only certain actions at a scope level.
* When planning your access control strategy, grant users the lowest privilege level that they need to do their work.
* RBAC uses an allow model.
  + This means that when you are assigned a role, RBAC allows you to perform certain actions, such as read, write, or delete.
  + Therefore, if one role assignment grants you read permissions to a resource group, and a different role assignment grants you write permissions to the same resource group, you will have write permissions on that resource group.

**Usage scenarios**

* + Examples of when you might use RBAC include when you want to: Allow one user to manage VMs in a subscription, and another user to manage virtual networks.
  + Allow a database administrator (DBA) group to manage SQL databases in a subscription.
  + Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.
  + Allow an application to access all resources in a resource group.

Resource Group >> choose resource >> Access Control (IAM)

Doing access control at resource group role, it saves time and access given cascade to resources

Roles

* Owner = can do anything
* Contributor = can do anything except modifying access
* Reader = can only read
* Azure Service specific roles

**Resource Lock = management locks**

* help you prevent accidental deletion or modification of your Azure resources i.e. to avoid accidental delete or modification
* Resource locks apply regardless of RBAC permissions. Even if you are an owner of the resource, you must still remove the lock before you'll actually be able to perform the blocked activity.
* its not strong authorization like acccess control additional layer of security senity check to avoid human error
* need Owner or User Access Administrator needed to delete resource create/lock
* Two types of lock
  + - Delete
    - Read-Only

Resource Group >> resoucename-settings >> Locks

Resource Group >> resoucename >> Resoruce -- settings >> Locks

**Azure Blueprints**

* enable cloud architects to define a repeatable set of Azure resources that implement and adhere to an organization's standards, patterns, and requirements.
* Azure Blueprint, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.
* Maintaining relationships, in this way, improves auditing and tracking capabilities
* Azure Blueprint is a declarative way to orchestrate the deployment of various resource templates and other artifacts, such as:
  + Role assignments
  + Policy assignments
  + Azure Resource Manager templates
  + Azure Resource Manager Templates deploy resources; they have no active relationship with the deployed resources
  + Resource groups
  + Locking - no one can delete resource protected by blueprint
* Version - it has version

**Subscription governance**

There are mainly three aspects to consider in relation to creating and managing subscriptions:

* Billing,
  + Reports can be generated by subscriptions
  + a possible scenario is to create subscriptions by department or project
* Access Control, and
  + A subscription is a deployment boundary for Azure resources and every subscription is associated with an Azure AD
  + customers have separate subscriptions for Development and Production, each one is isolated from each other from a resource perspective and managed using RBAC.
* Subscription limits.
  + Subscriptions are also bound to some hard limitations.
  + For example, the maximum number of Express Route circuits per subscription is 10.

**Monitoring and Reporting**

For checking resource deployed in azure are healthy, working fine, performance of them and utilization of them.

**Explore Tags**

* Policy can be get created for Naming convention of Tags
* Example of tags. Department = "IT" or Environment = "Production"
* After you apply tags, you can retrieve all the resources in your subscription with that tag name and value.
* Tags enable you to retrieve related resources from different resource groups.
* This approach is helpful when you need to organize resources for billing or management.
* It's also common for tags to be used in automation. If you want to automate the shutdown and start-up of virtual machines in development environments during off-hours to save costs, you can use tags to assist in this automation.
* Tagging resources can also help in monitoring to track down impacted resources. Monitoring systems could include tag data with alerts, giving you the ability to know exactly who is impacted.

**limitations**

* **Not all resource types support tags.**
* Each resource or resource group can have a maximum of 50 tag name/value pairs. Currently, storage accounts only support 15 tags
* more can be applied via json string
* The tag name is limited to 512 characters, and the tag value is limited to 256 characters
* Virtual Machines and Virtual Machine Scale Sets are limited to a total of 2048 characters for all tag names and values.

**Tags applied to the resource group are not inherited by the resources in that resource group.**

**Texonomic Tags= Tags**

specially related to cost accounting

https://www.youtube.com/watch?v=uENWoZyuKhQ&list=PLYGZ9Q0oTOHfsI-3IAhvyc09ssPDfoePv&index=38

**Azure Monitor**

* **maximizes the availability and performance of your applications by delivering a comprehensive solution for collecting, analysing, and acting on telemetry from your cloud and on-premises environment**
* helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on
* Azure Monitor can collect data from a variety of source
  + Application monitoring data: Data about the performance and functionality of the code you have written
  + Guest OS monitoring data
  + Azure resource monitoring data: Data about the operation of an Azure resource
  + Azure subscription monitoring data: Data about the operation and management of an Azure subscription
  + Azure tenant monitoring data: Data about the operation of tenant-level Azure services, such as Azure Active Directory
* Workbook - combines logs and metrics data in single view
  + Activity Logs - record when resources are created or modified.
  + Metrics - tell you how the resource is performing and the resources that it's consuming.
  + Logs - persist metrics measurement, other azure diagnostic data query language to get data and generate reports and can help to set alert

**Enabling diagnostics**

* extend the data you're collecting into the actual operation of the resources by enabling diagnostics and adding an agent to compute resources.
* Under the resource settings you can enable Diagnostics
  + Enable guest-level monitoring
  + Performance counters: collect performance data
  + Event Logs: enable various event logs
  + Crash Dumps: enable or disable
  + Sinks: send your diagnostic data to other services for more analysis
  + Agent: configure agent settings

**Azure service health**

* Personalized alerts and guidance for Azure service issues
* Azure Service Health notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime.
* Configure customizable cloud alerts and use your personalized dashboard to analyse health issues, monitor the impact to your cloud resources, get guidance and support, and share details and updates.
* It can notify you, help you understand the impact of issues, and keep you updated as the issue is resolved.

Azure Service Health is composed of the following:

* Azure Status provides a global view of the health state of Azure services-https://status.azure.com/en-us/status
* Service Health provides you with a customizable dashboard that tracks the "state of your Azure services" in the regions where you use them
  + you can use the Service Health dashboard to create and manage service Health alerts, which notify you whenever there are service issues that affect you
* Resource Health helps you diagnose and obtain support when an Azure service issue affects your resources.
  + In contrast to Azure Status, which informs you about service problems that affect a broad set of Azure customers,
  + Resource Health gives you a personalized dashboard of your resources' health.
  + Resource Health shows you times, in the past, when your resources were unavailable because of Azure service problems.
  + It's then easier for you to understand if an SLA was violated.
  + Resource Health gives you a personalized dashboard of your resources' health

**Monitor applications and services**

* Data monitoring is only useful if it improves your visibility of the operations in your computing environment.
* Azure Monitor includes several features and tools that provide valuable insights into your applications, and the other resources they may depend on.
* Azure Monitor - features can be organized into four categories, these categories are:
  + Analyze,
  + Application Insights = is a service that monitors the availability, performance, and usage of your web applications
    - uses powerful data analysis platform in Log Analytics to provide you with deeper insights into your application's operations
    - Azure Monitor for containers = is a service that is designed to monitor the performance of container workloads, which are deployed to managed Kubernetes clusters hosted on Azure Kubernetes Service (AKS
    - Azure Monitor for VMs =is a service that monitors your Azure VMs at scale, by analyzing the performance and health of your Windows and Linux VMs
  + Respond,
    - effective monitoring solution must respond proactively to any critical conditions that are identified within the data it collects.

for example, sending a text or email to an administrator who is responsible for investigating an issue

* + - Autoscale
    - Azure Monitor uses Autoscale to ensure that you have the right amount of resources running to manage the load on your application effectively.
    - Autoscale enables you to create rules that use metrics, collected by Azure Monitor, to determine when to automatically add resources to handle increases in load when to reduce resource resource automatically
  + Alerts
    - Azure Monitor proactively notifies you of critical conditions using Alerts and can potentially attempt to take corrective actions.
  + Visualize and
    - Visualizations, such as charts and tables, are effective tools for summarizing monitoring data and for presenting data to different audiences.
    - Azure Monitor has its own features for visualizing monitoring data
    - Other tools
      * Dashboards
      * Views
      * Power BI
  + Integrate.
    - integrate Azure Monitor with other systems, and build customized solutions that use your monitoring data

**Examine privacy, compliance, and data protection standards**

**Security** = Learn about how we are creating a safer world for digital transformation.

**Privacy** = We believe in the timeless value of privacy and preserve the ability for customers to control their data.

**Compliance** = We respect local laws and regulations and provide comprehensive coverage of compliance offerings.

**Compliance terms and Requirements**

When selecting a cloud provider to host your solutions, you should understand how that provider can help you comply with regulations and standards

Some questions

* How compliant is the cloud provider when it comes to handling sensitive data?
* How compliant are the services offered by the cloud provider?
* How can I deploy my own cloud-based solutions to scenarios that have accreditation or compliance requirements?
* Type of compliance
  + Global
  + Us Government
  + Industry
  + Regional

**Microsoft privacy statement**

explains what personal data Microsoft processes, how Microsoft processes it, and for what purposes.

**Trust centre** - https://www.microsoft.com/en-us/trust-center

is a website resource containing information and details about how Microsoft implements and support

* security,
* privacy,
* compliance,
* and transparency

in all Microsoft cloud products and services.

find following in >> microsoft trust center

Which complince prgram azure certified ?

where is policy about how microsoft teats your data ?

https://docs.microsoft.com/en-us/learn/modules/privacy-compliance-data-protection-standards/4-explore-trust-center

**Service trust portal**

* hosts the Compliance Manager service, and is the Microsoft public site for publishing audit reports and other compliance-related information relevant to Microsoft’s cloud services.
* Service Trust Portal users can download audit reports produced by external auditors and gain insight from Microsoft-authored reports that provide details on how Microsoft builds and operates its cloud services.
* provide audit reports
* **complice manager** tool interactive tool, you can load complice program you need to audit here you can document your servcie met with given certification or not
* Service Trust Portal (STP) also includes information about how Microsoft online services can help your organization maintain and track compliance with standards
  + ISO
  + SOC
  + NIST
  + FedRAMP

https://servicetrust.microsoft.com/

https://docs.microsoft.com/en-us/learn/modules/privacy-compliance-data-protection-standards/6-explore-compliance-manager

**Compliance Manager** - is a dashboard that provides a summary of your data protection and compliance stature, and recommendations to improve data protection and compliance.

The Customer Actions provided in Compliance Manager are recommendations only;

* it is up to each organization to evaluate the effectiveness of these recommendations in their respective regulatory environment prior to implementation.
* Recommendations found in Compliance Manager should not be interpreted as a guarantee of compliance.

**Identify Azure Government services**

-https://www.youtube.com/watch?v=W6WFwHElS4U&list=PLYGZ9Q0oTOHfsI-3IAhvyc09ssPDfoePv&index=50

* is a separate instance of the Microsoft Azure service.
* It addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers.
* **Azure Government offers physical isolation from non-US government** deployments and provides screened US personnel.
* **Azure Government uses physically isolated datacentres and networks** (located only in the US).
* **Identify Azure China 21Vianet**
  + is operated by 21Vianet is a physically separated instance of cloud services located in China,
  + independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Centre Co., Ltd.

**Section 4**

**Microsoft Azure pricing, service level agreements, and lifecycles**

**Azure subscriptions = payment method to Microsoft**

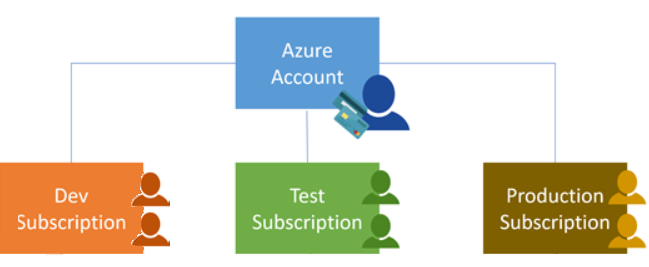
* Azure subscription which provides you with authenticated and authorized access to Azure products and services and allows you to provision resources.
* An Azure subscription is a logical unit of Azure services that links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that an Azure AD trusts
* account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies
* Azure subscriptions define boundaries around Azure products, services, and resources

There are two types of subscription boundaries

* + Billing boundary
  + Access control boundary

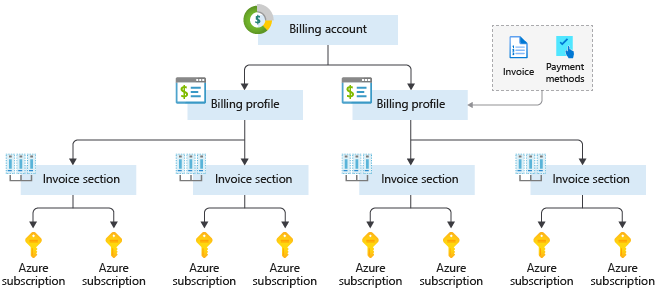
Create additional Azure subscriptions

* You might want to create additional subscriptions for resource or billing management purposes.
  + Environments
  + Organizational structures
  + Billing
  + Subscription limits



Customize billing to meet your needs

* For multiple subscriptions, you can organize them into invoice sections.
* Each invoice section is a line item on the invoice that shows the charges incurred that month.
* Depending on your needs, you can set up multiple invoices within the same billing account.
* To do this, create additional billing profiles.
* Each billing profile has its own monthly invoice and payment method.



Change subscription

https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/switch-azure-offer

Explore subscriptions offers

* https://azure.microsoft.com/en-us/support/legal/offer-details/
* There are several different options to purchase Azure from free to enterprise agreements.
* Azure offers free and paid subscription options to suit different needs and requirements
  + A free account
  + Pay-As-You-Go
  + Member offers
  + pre-pay = Enterprise Agreements, in this you get discount, detail control over cost if you are going to stay for long
    - you get discount for using azure
    - you get personalized portal for you EA subscription for detail cost tracking
  + Credit = you will get credit if you are mvp or trainer of microsoft , if you have msdn subscript or you are partner

Find azure credit offer in your region

* https://azure.microsoft.com/en-us/regions/offers/
* BizSpark - offer for start up business
* DreamSpark - offer for students

**Explore management groups**

* "Tent root" scope come at top of management group, it is associated with AD
* The organizing structure for resources in Azure has four levels
* management groups,
  + containers that help you manage access, policy, and compliance for multiple subscriptions.
  + All subscriptions in a management group automatically inherit the conditions applied to the management group
* subscriptions,
* resource groups, and
* resources

**Review planning and managing Azure costs**

Estimating costs and managing yours spend are crucial skills you will want when moving into the cloud

**Purchase Azure products and services**

* There are three main customer types on which the available purchasing options for Azure products and services is contingent
  + Enterprise
    - for enterprises
    - pay annually
    - get huge discount
  + Web direct
    - pay monthly via website
    - pay public prices
  + Cloud Solution Provider
    - Microsoft partner companies that a customer hires to build solutions on top of Azure
    - Payment and billing for Azure usage occurs through the customer's CSP
    - help with architects and implementation and trouble shooting
* The key takeaway is that resources are always charged based on usage.
* At the end of each monthly billing cycle, the usage values will be charged to your payment method and the meters are reset.

**Explore factors affecting costs**

* When you provision an Azure resource, Azure creates one or more meter instances for that resource
* meters track the resources' usage, and each meter generates a usage record that is used to calculate your bill
* Example, a single virtual machine that you provision in Azure might have the following meters tracking its usage:
  + Compute Hours
  + IP Address Hours
  + Data Transfer In
  + Data Transfer Out
  + Standard Managed Disk
  + Standard Managed Disk Operations
  + Standard IO-Disk
  + Standard IO-Block Blob Read
  + Standard IO-Block Blob Write
  + Standard IO-Block Blob Delete
* Main factors that affect Azure costs, including
  + resource type,
    - so the usage that a meter tracks and the number of meters associated with a resource depend on the resource type
  + services, and
    - Azure usage rates and billing periods can differ between Enterprise, Web Direct, and Cloud Solution Provider (CSP) customers
  + the user's location

**Identify zones for billing purposes**

* Billing zones help determine the cost of services you are using.
* Bandwidth refers to data moving in and out of Azure datacenters.
  + Some inbound data transfers, such as data going into Azure datacenters, are free.
  + For outbound data transfers, such as data going out of Azure datacenters, data transfer pricing is based on Zones.
* A Zone is a geographical grouping of Azure Regions for billing purposes
  + Zone 1 – West US, East US, Canada West, West Europe, France Central and others
  + Zone 2 – Australia Central, Japan West, Central India, Korea South and others
  + Zone 3 - Brazil South
  + DE Zone 1 - Germany Central, Germany Northeast
* in bound data trasfer in azure = ingress = ex. uploading data= there is no charge for this
* out bound data transfer out of azure= outgress = ex. downloading data = there is changes for this

**Explore the Pricing Calculator**

* is a tool that helps you estimate the cost of Azure products.
* <https://azure.microsoft.com/en-us/pricing/calculator/>
* The options that you can configure in the Pricing Calculator vary between products, but basic configuration options include
  + Region
  + Tier = sets the type of tier you wish to allocate to a selected resource, such as Free Tier, Basic Tier, etc.
  + Billing Options =Highlights the billing options available to different types of customer and subscriptions for a chosen product.
  + Support Options = Allows you to pick from included or paid support pricing options for a selected product.
  + Programs and Offers = price offerings according to your customer or subscription type
  + Azure Dev/Test Pricing = product you choose

**Explore Total Cost of Ownership Calculator**

is a tool that you use to estimate cost savings you can realize by migrating to Azure.

* Step 1: Define your workloads
  + Servers
  + Databases
  + Storage
  + Networking
* Step 2: Adjust assumptions
  + The assumption values you can adjust include
    - storage costs,
    - IT labor costs,
    - hardware costs,
    - software costs,
    - electricity costs,
    - virtualization costs,
    - datacenter costs,
    - networking costs, and
    - database costs
* Step 3: View the report
  + Generate report
  + The report allows you to compare the costs of your on-premises infrastructure with the costs using Azure products and services to host your infrastructure in the cloud.

**Explore minimizing costs**

The following best practice guidelines can help minimize your Azure costsPerform cost analyses

* Plan your Azure solution wisely. Carefully consider the products, services, and resources you need, and read the relevant documentation to understand how each of your choices are metered and billed.
  + user Price Calculator and TCO = total cost of ownership
* Monitor usage with Azure Advisor
  + The Azure Advisor feature identifies unused or under-utilized resources, and you can implement its recommendations by removing unused resources and configuring your resources to match your actual demand.
* Use spending limits
  + Free trial customers and some credit-based Azure subscriptions can use the Spending Limits feature.
  + Azure provides the Spending Limits feature to help prevent you from exhausting the credit on your account within each billing period.
  + If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.
* Use Azure Reservations
  + offer discounted prices on certain Azure products and resources.
  + To get a discount, you reserve products and resources by paying in advance.
  + You can pre-pay for one year or three years of use of Virtual Machines, SQL Database Compute Capacity, Azure Cosmos Database Throughput, and other Azure resources.
  + Azure Reservations are only available to Enterprise or CSP customers and for Pay-As-You-Go subscriptions
* Choose low-cost locations and regions
  + if possible, you should use them in those locations and regions where they cost less.
* Research available cost-saving offers
* Keep up-to-date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.
* Apply tags to identify cost owners
  + Tags help you manage costs associated with the different groups of Azure products and resources.
  + You can apply tags to groups of Azure products and resources to organize billing data.

**Define Azure Cost Management**

is an Azure product that provides a set of tools for monitoring, allocating, and optimizing your Azure costs.

main features of the Azure Cost Management toolset include:

* Reporting. Generate reports using historical data to forecast future usage and expenditure.
* Data enrichment. Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.
* Budgets. Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.
* Alerting. Get alerts based on your cost and usage budgets.
* Recommendations. Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.
* Price. Free to Azure customers
* Billing scope
  + RBAC
* Get all invoices
* Get all payments
* Track cost

**Explore Azure service level agreements (SLAs)** = SLA is all about how much uptime your solution will have based on services you define it not availability.

* In your on-premises datacentre, you knew how reliable the hardware was, as you controlled everything.
* And you knew exactly how long it would take to replace hardware if a problem occurred.
* Let's take a look at Service Level Agreements (SLAs) in order to give you peace-of-mind.

Microsoft maintains its commitment to providing customers with high-quality products and services by adhering to comprehensive operational policies, standards, and practices

* SLAs describe Microsoft's commitment to providing Azure customers with certain performance standards.
* There are SLAs for individual Azure products and services.
* SLAs also specify what happens if a service or product fails to perform to a governing SLA's specification.
* A SLA defines performance targets for an Azure product or service
  + **performance targets for some Azure services are expressed in terms of uptime or connectivity rates**

Monthly Uptime Percentage is represented by the following formula:

* Monthly Uptime % = (Maximum Available Minutes – Downtime) / Maximum Available Minutes X 100

SLA downtime estimates -https://docs.microsoft.com/en-us/learn/modules/explore-azure-service-level-agreements/3-explore-slas-for-azure-products-services

**Service Credits**

* describe how Microsoft will respond if an Azure product or service fails to perform to its governing SLA's specification
* how Microsoft respond if fail to meet SLA
* example, customers may have a discount applied to their Azure bill, as compensation for an under-performing Azure product or service.

Note:

* Azure does not provide SLAs for many services under the Free or Shared tiers.
* Also, free products such as Azure Advisor do not typically have a SLA.

**Define composite SLA**

* When combining SLAs across different service offerings, the resultant SLA is a called a Composite SLA.
* The resulting composite SLA can provide higher or lower uptime values, depending on your application architecture.

Ex.

Consider an App Service web app that writes to Azure SQL Database.

At the time of this writing, these Azure services have the following SLAs:

App Service Web Apps is 99.95 percent.

SQL Database is 99.99 percent.

99.95 percent × 99.99 percent = approx 99.94 percent

* + This means the combined value is lower than the individual SLA values, meaning higher probability of failure.
  + you can improve the composite SLA by creating independent fallback paths.
  + For example, if SQL Database is unavailable, you can put transactions into a Queue for processing at a later time.
  + However, it fails if both the SQL Database and the Queue fail simultaneously.
  + If the expected percentage of time for a simultaneous failure is 0.0001 × 0.001, i.e. (1.0 - 0.9999) x (1.0 - 0.999), the composite SLA for this combined path would be:

Database \*OR\* Queue = 1.0 − (0.0001 × 0.001) = 99.99999 percent

Web app \*AND\* (Database \*OR\* Queue) = 99.95 percent × 99.99999 percent = ~ 99.95 percent

However, there are tradeoffs to using this approach such as, the application logic is more complex, you are paying for the queue, and there may be data-consistency issues which you need to consider.https://docs.microsoft.com/en-us/learn/modules/explore-azure-service-level-agreements/4-define-composite-sla

**Define application SLA**

* Azure customers can use SLAs to evaluate how their Azure solutions meet their business requirements and the needs of their clients and users.
* By creating your own SLAs, you can set performance targets to suit your specific Azure application.
* When creating an Application SLA consider the following:
  + Identify workloads - is a distinct capability or task that is logically separated from other tasks, in terms of business logic and data storage requirements
  + Plan for usage patterns - Identify differences in requirements during critical and non-critical periods.
  + Establish availability metrics — mean time to recovery (MTTR) and mean time between failures (MTBF). MTTR is the average time it takes to restore a component after a failure.
  + Establish recovery metrics -recovery time objective and recovery point objective (RPO). RTO is the maximum acceptable time an application can be unavailable after an incident.
  + Implement resiliency strategies - Resiliency is the ability of a system to recover from failures and continue to function

High availability and disaster recovery are two crucial components of resiliency

Build availability requirements into your design - Availability is the proportion of time your system is functional and working

**Cost and complexity vs. high availability**

* as you increase availability, you also increase the cost and complexity of your solution
* The risk of potential downtime is cumulative across various SLA levels, which means that complex solutions can face greater availability challenges.
* Considerations for defining application SLAs
  + If your application SLA defines four 9's (99.99%) performance targets, recovering from failures by manual intervention may not be enough to fulfil your SLA.

**Examine service lifecycle in Azure**

Azure services have a lifecycle.

* Azure services start in the development phase.
* Next they are released to preview, to inform you new features are coming.
* Then the services release to public testing, so you can experiment with them.
* Finally, the service becomes available to everyone.

Services Lifecycle in Azure is the name of this release cycle.

**Define public and private preview features**

* Azure Previews, you can test pre-release features, products, services, software, and even regions.
* Previews allow users early access to functionality.
* users providing feedback on the preview features helps Microsoft improve the Azure service.
* two categories of preview
  + Preview feature - An Azure feature is available to certain Azure customers for evaluation purposes.
  + Public preview - An Azure feature is available to all Azure customers for evaluation purposes.

Azure Preview Terms and Conditions

* Azure feature previews are available with their own terms and conditions
* Some previews aren't covered by customer support

**Access preview features**

You can view preview services by doing the following

* Sign into the Azure portal
* Click Create a resource
* Type preview in the search box and press Enter
* A list of services is returned and displayed for you to browse through

You may choose to use an Azure preview service in production.

Remember, the preview feature or functionality may not yet be ready for production deployments.

Make sure you're aware of any limitations around its use before deploying to production.

**Access Azure Portal Preview**

- https://preview.portal.azure.com

-Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.

-Provide feedback

-Azure customers can provide feedback on the preview features they've tested by sending a smile in the portal.

-Or customers can post ideas and suggestions on the Azure portal feedback forum.

**Discuss general availability**

* Once a feature is evaluated and tested successfully, it may release to customers as part of Azure
* feature released to all Azure customers typically goes to General Availability or GA.

**Monitor service and feature updates**

* Azure updates page for information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements.
* <https://azure.microsoft.com/en-us/updates/>
* From the Azure updates page, you can:
  + View details about all Azure updates.
  + See which updates are in general availability, Preview, or Development.
  + Browse updates by product category or update type, by using the provided dropdown lists.
  + Search for updates by keyword by entering search terms into a text-entry field.
  + Subscribe to get Azure update notifications by RSS.
  + Access the Microsoft Connect page to read Azure product news and announcements.

**Industry compliance (GDPR,ISO,NIST)**

-https://www.youtube.com/watch?v=EFT3e2YMaZ4&list=PLYGZ9Q0oTOHfsI-3IAhvyc09ssPDfoePv&index=52

-voluntary or in-voluntary/mandatory (region, industry like health, finance, government, education) certification program

GDPR- General data protection Act, company hold EU citizen data or operate/Business in EU need this certification

ISO

NIST - mandatory in US if you are doing business with government

**Support plan** :-https://azure.microsoft.com/en-in/support/plans/

Basic - for all customer

Develoer - non production trial

Standard - production workload

Premium Direct - Business critical product or solution

**Free account** for 200hr for 30 days - full/ all azure services , but you get some services you get for 12 months and some services are always free Ex. aure functions under 1M/10,00,000 request, simple website for free

its not for doing production work , it helps you to evalute service you can use in paid subscription

you need microsoft acccount for creating subscription

you have to provide card details, but it dont charge till you upgrade

**Azure preview term portal**

https://azure.microsoft.com/en-in/support/legal/preview-supplemental-terms/

**Azure support plan**

--free account basic support

--based on payment you get other support

-- remember names of plan and difference between them for exam

-- support plan is not related Azure Active directory i.e. authorization

Support plan can be found in

Azure Active Directory >> (separate roles for support plan) Roles and Administrators >> create role based on function it can perform and assigned to azure users

**To file support ticket**

Help + Support (Blade) >> new support request

Help + Support (Blade) >> Service health = with help of AI/Machine learning it gives view of what issue affecting resource

**Azure Knowledge center**

-- it provide help , it basically question and answer portal

**Azure update portal**

--here you find product available and state of product

**Azure charts**

Portal to get more details