Cloud Computing: it is a delivery of computing resources over the internet, enabling faster innovation, flexible resources, and economies of scale.

Cloud service providers offers:

- computer power
- Storage
- Applications
- Networking
- Analytics

Deployment models in cloud computing:

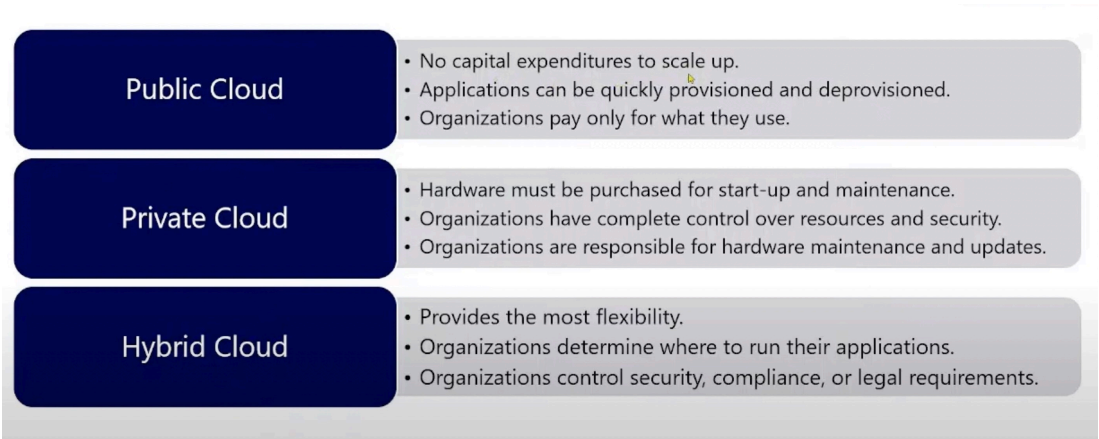
- private cloud - organizations is responsible for creating a cloud environment and data center
  - organizations is responsible for operating the services they provide
  - does not provide access outside the organization

- Public cloud - owned by cloud services or hosting provider
  - provides resources and services to multiple organizations and users
  - accessed via secure network connection (typically over internet)

  Eg: AWS, AZURE, GCP

- hybrid cloud - combines public and private cloud to allow applications to run in the most appropriate location.

Cloud model comparison



Points to remember:

Capital expenditure vs operational expenditure

CapEx: the up-front spending of money on physical infrastructure
- costs from CapEx have a value that reduces over time

OpEx: spend on products and services as needed, pay-as-you-go
- get billed immediately

Blind view:

Public cloud — OpEx

Private cloud — CapEx

→ in most of the cases

Cloud benefits

- high availability - can be deployed in multiple data centers (low chance of website going down)
- Reliability - as deployed in multiple data centers, reliability can be achieved (replication)
- Security - most of the time cloud is more secure compared to on premises
- Manageability - cloud service providers provide different ways to manage our resources
- Scalability - scaling of resources is the major advantage of cloud (scale according to needs)
- Governance - cloud runs on certain rules. So chance of mis communication is very low
- Predictability - can predict the cost of the service before we use them

Cloud service models:

IaaS - Infrastructure as a service
PaaS - platform as a service
SaaS - software as a service

IaaS

- delivers compute infrastructure, typically a platform virtualization environment as a service.
- cloud providers build data centers, managing power, scale, hardware, networking, storage, distributed systems, etc.
- Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as fully outsourced.

General users: — who wants to migrate legacy applications to the cloud environment

Eg: AWS EC2, Azure VM, GCP compute engine.

when to use IaaS?

↳ legacy applications (say: Bank of America)

↳ want to move to cloud

↳ Then they just use infrastructure

(as they already have everything built say, code, environment etc)

PaaS

- provides environment for building, testing, and deploying software applications; without focusing on managing underlying infrastructure.

Eg: AWS Elastic Beanstalk, Azure App Service, Google App Engine`

when to use PaaS?

Say I want to deploy a web browser

↓

I build application (out side cloud)

↓ Now

I need web server, vm's, OS to host application

↳ All this can be taken care by the cloud provider in PaaS model.

SaaS

- Users connect to and cloud-based apps over the internet, for example: Gmail, Office365..

Note:

1. SaaS is a software delivery methodology that provides licensed multi-tenant access to software and its functions remotely as a web-based service.

hosted in cloud providers data center (say AWS) by the third party (say BofA) and given access to many people (BofA users).

Single-tenant access → Hosted in cloud providers data center (sayAWS) by third party (say MAC international) and has access to only MAC international employees.

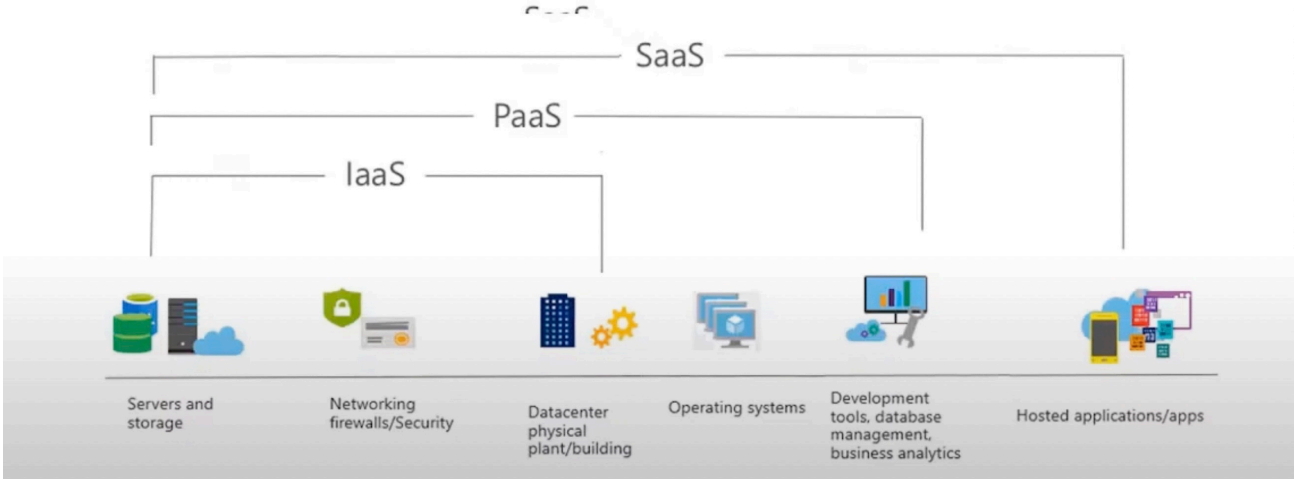
who use what services?

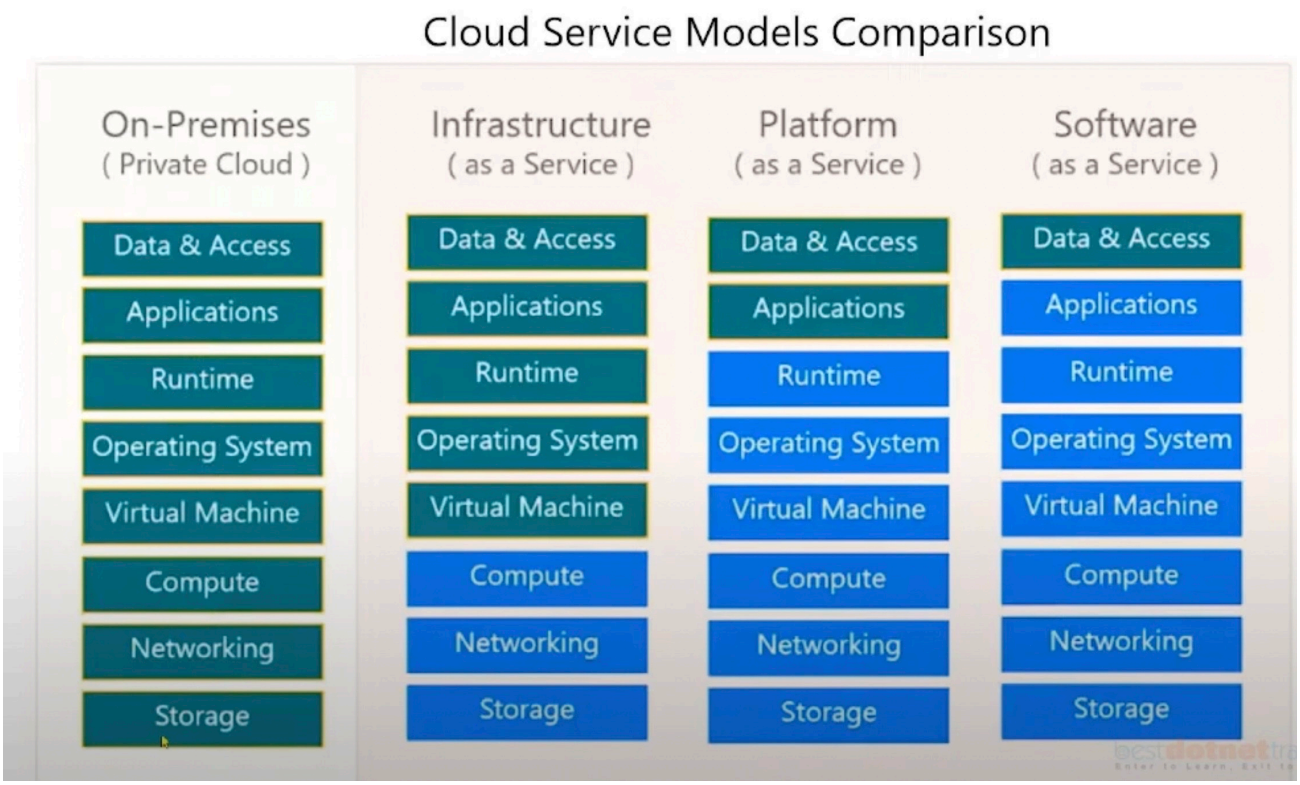
saas – End users

paas – Application developers

Iaas – Infrastructure & network architects

Comparison of models:





AZURE

Azure architectural components

- azure regions, region pairs, and sovereign regions
- Availability zones
- Azure data centers
- Azure resources and resource groups
- Subscriptions
- Management groups
- Hierarchy of resource groups, subscriptions, and management groups

Note: sovereign regions — these data centers are build for government (common users does not have access to these data centers)

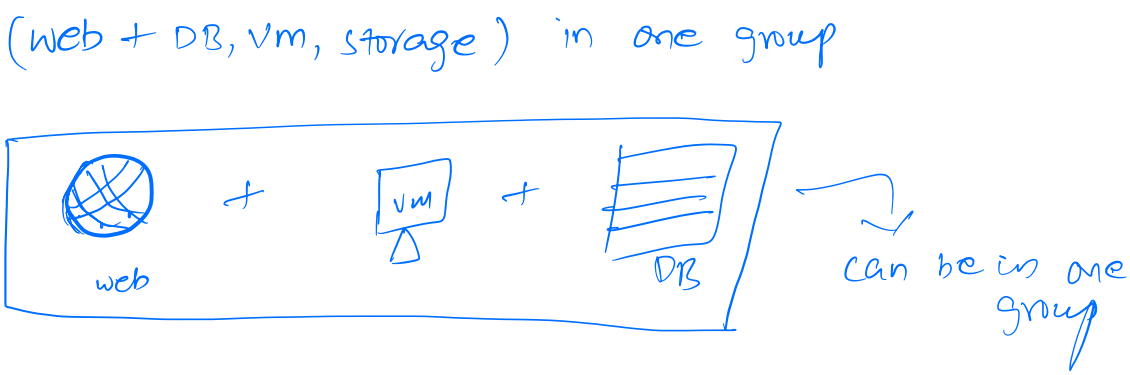
Azure resources:

- Virtual machines
- Storage accounts
- Virtual networks
- App services
- SQL databases
- Functions

Resource group: a resource group is a logical container to manage and aggregate resources in a single unit

- resources can exist in only one resource group
- Resources can exist indifferent regions
- Resources can be moves to different resource groups
- Applications can utilize multiple resource groups

Eg:

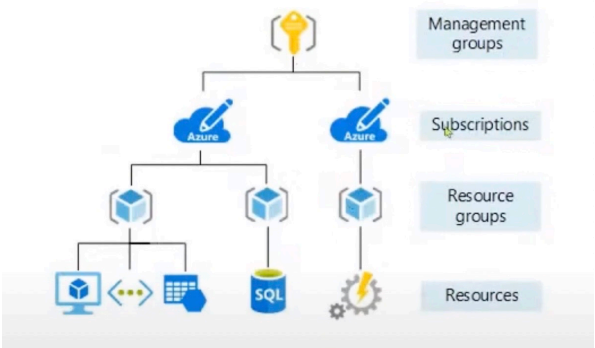


Azure subscription: an azure subscription provides you with authenticated and authorized access to azure accounts.

- can act as **billing boundary** and **access control boundary**

Subscriptions can be different for **Development, testing** and **production —** each one access is given to corresponding users (not everything to all users)

Management Groups: Management groups can include multiple azure subscriptions. The hierarchy is given below



Note:

- 10,000 management groups can be supported in a single directory
- A management group tree can support up to six levels of depth

Creating Virtual Machine

First create a resource group and follow the options we have in the azure console

Some options to remember while creating VM

- Select inbound ports - Various option and their port numbers

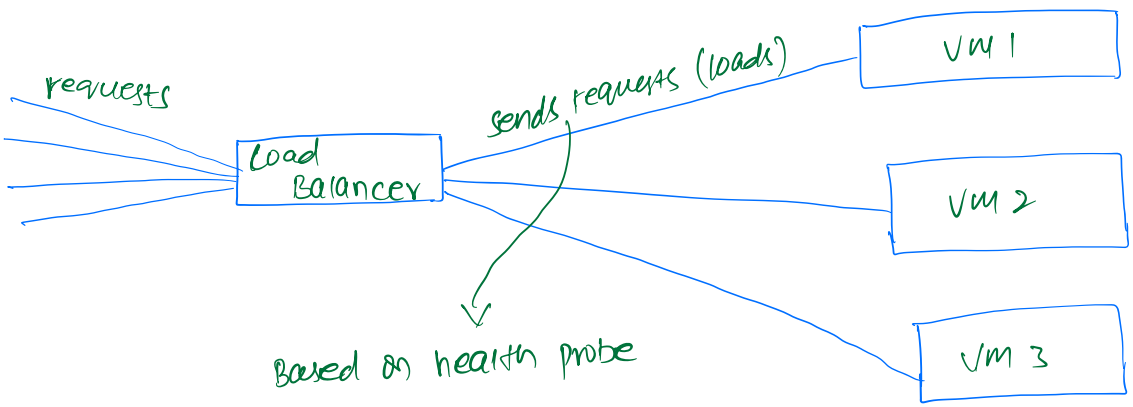
HTTP	-	80
HTTPS	-	443
SSH	-	22
RDP	-	3389

- Actually we have to create a virtual network before creating virtual machine, but here, the virtual network is automatically created while creating VM.
- after successfully creating VM, we can connect to that VM using our desktop remotely and can perform operations on the VM which is in server (Azure DC).
- we also have the option to shutdown virtual machine temporarily and save cost.

Load Balancer

In azure console search for load balancers - click on create - follow steps - created

- after successful creation of load balancers, we have to navigate to load balancers tab and select options **Backend Pools** - to add virtual machine.
- Load balancer is a separate service used to maintain the load of virtual machines.



Health probe: it is a scale which is used to measure the health of virtual machine, if VM is weak then load balancer diverts that load to another VM.

- load balancer is in existence at transportation layer of OSI model (max uses TCP protocol)

How many virtual machines a basic load balancer can handle?

- Basic load balancer can handle 100 instances but standard tier can handle up to 1000 instances (matching a virtual machine scale set)

Does load balancer has separate IP address?

- Yes, load balancer has separate IP address and we have to request the application with the load balancer IP address not with the IP address of the virtual machine (web server).

↳ means we have to map the domain name with load balancer IP address not with the web server IP address

Container services: containers are a virtualization environment where you do not manage an operating system

Docker: docker is very popular container tool.

Work flow of container services (or docker tool)

Developers develop the dockers images

These docker images are uploaded into a repository — docker themselves provides a repository called as docker hub and Microsoft also provides a repository in azure called as docker container registry

Once the images are uploaded, then by selecting one of the images we can create a container instance.

Azure container instance is a light weight virtual machine

Note: if you have only one container in your application, then you can directly make use of azure container instance services.

If your company is using micro services architecture then you have to deploy each micro service in one separate container. one application can contain many micro services so, there will be many containers

To manage all those micro services right from their instantiation to the complete life cycle management

To do the above mentioned job, we need some orchestration services. For this azure two kinds of services as following

- **Azure kubernetes services** - very popular
- **Azure service fabric**

Azure Data Categories: in azure data is divided into three categories as following

1. Structured data
2. Semi-structured data
3. Unstructured data

	Schema	Data relationships	Examples
Structured data	Adheres to a schema, with the same data fields or properties.	Storable in relational database tables, with rows and columns.	Sensor data and financial data.
Semi-structured data	Has an ad hoc schema with less organized fields and properties.	Non-relational or NoSQL data, not storable in tables, rows and column.	Books, blogs, JSON, XML, HTML documents.
Unstructured data	Has no designated schema or data structure.	Non-relational or blob data, with no restrictions on the kinds of data blobs contain.	PDFs, JPGs, videos.

Azure Storage Services: storage services are available in azure are following

- Azure Blobs: A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
- Azure Files: Managed file shares for cloud or on-premises deployments.
- Azure Elastic SAN (preview): A fully integrated solution that simplifies deploying, scaling, managing, and configuring a SAN in Azure.
- Azure Queues: A messaging store for reliable messaging between application components.
- Azure Tables: A NoSQL store for schemaless storage of structured data.
- Azure Disks: Block-level storage volumes for Azure VMs.

When to use which storage

Azure files: offers fully managed cloud file shares that you can access from anywhere via the industry standard
Azure Blob: allows unstructured data to be stored and accessed at a massive scale in block blobs
Azure Elastic SAN: it is a fully integrated solution that simplifies deploying, scaling, managing, and configuring a SAN, while also offering built-in cloud capabilities like high availability.
Azure Disks: allows data to be persistently stores and accessed from an attached virtual hard disk
Azure Queues: allows for asynchronous message queuing between application components.
Azure Tables: allows you to store structured NoSQL data in the cloud, providing as key store with schema-less design.

Note: there is another special storage service available which is Azure NetApp Files -> which offers a fully managed, highly available, enterprise-grade NAS service that can handle the most demanding, high-performance, low latency workloads requiring advanced data management capabilities.

Azure database services: the following are the azure database services

- Azure Cosmos DB
- Azure SQL Database
- Azure database migration

Azure cosmos DB: it is globally distributed database service -> data is replicated among various service globally

↳ highly scalable service
↳ extraordinary throughput
↳ useful to deal with huge volume of data

Note: the basic advantage of NoSQL is three V's —-> volume, velocity, and variety.

Azure SQL database: it is a relational database as a service (DaaS)

Azure Database Migration: it is a fully managed service designed to enable seamless migrations from multiple database sources to azure data platforms with minimal downtime.

↳ migrating on premise data to Azure database

Azure Marketplace: it is platform where one can develop an application and make available for others to use that applications on subscription basis.

↳ provides variety of services

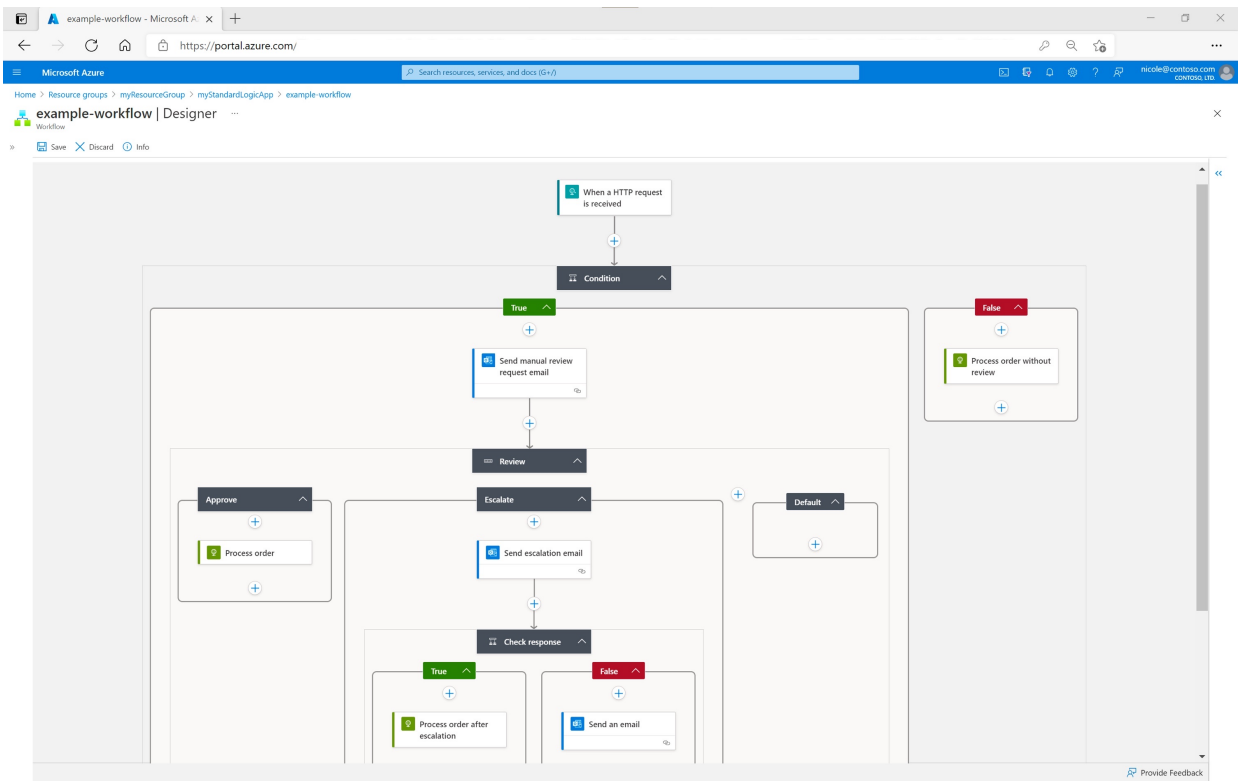
ServerLess Computing: this service doesn't mean completely serverless, but server side of work can be taken care by the cloud provider.

- Azure functions
- Azure logic apps
- Azure event grid

Azure Functions: Azure Functions is a serverLess solution that allows you to write less code, maintain less infrastructure, and save on costs. Instead of worrying about deploying and maintaining servers, the cloud infrastructure provides all the up-to-date resources needed to keep your applications running.

Azure Logic Apps: it is a cloud platform where you can create and run automated workflows with little to no code. By using the visual designer and selecting from prebuilt operations, you can quickly build a workflow that integrates and manages your apps, data, services, and systems.

Note: following is the example of work done in logic apps



Azure Event Grid: Event Grid is a highly scalable, serverLess event broker that you can use to integrate applications using events. Events are delivered by Event Grid to subscriber destinations such as applications, Azure services, or any endpoint to which Event Grid has network access. The source of those events can be other applications, SaaS services and Azure services.

Azure APP Service: 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.

- Multiple languages and frameworks
- Global scale with high availability
- Security and compliance
- Visual studio integration

Azure management tools: the following are some azure management tools
- Azure portal
- Azure power shell and Azure Command-Line Interface (CLI)
- Azure cloud shell

- Azure mobile app
- Azure REST API

Azure Advisor: analyzes your deployed azure resources and recommends ways to improve —> following

- availability
- security
- Performance
- Cost
- Operational excellence

Azure core solutions

Azure internet of things: in azure IoT mainly there are following services

Azure IoT Hub: it is a managed service hosted in the cloud that acts as a central message hub for bi-directional communication between IoT applications and the devices it manages

Acts as a middle man between software application and the IoT sensors (devices)

in a way that

IoT hubs gets data from IoT sensors and software applications can fetch that data and process it and shows it the end user

And also, if end user sends any instruction, then such instruction will be forwarded to the IoT devices by the IoT hub.

Azure IoT central: it is a fully managed global IoT SaaS solution that makes it easy to connect, monitor, and manage IoT assets at scale

Big data and analytics

In azure the following services are available majorly

Azure synapse analytics - a cloud based enterprise data warehouse

Azure HDInsight - a fully managed, open-source analytics service for enterprises

Azure DataBricks - Apache Spark based analytical service.

Artificial intelligence and machine learning

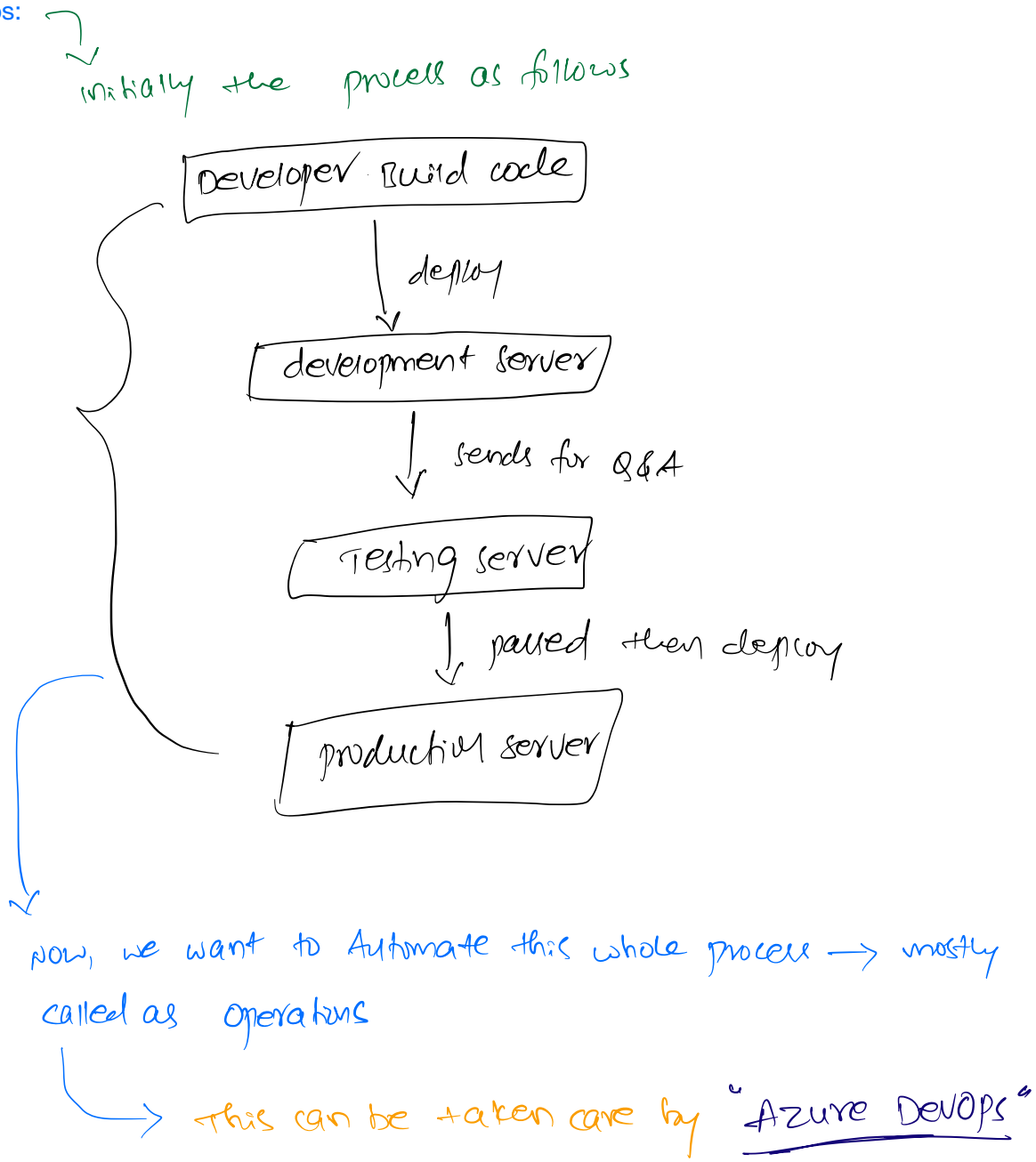
Azure Machine Learning - it is a cloud based service to build, train, and deploy machine learning models

Cognitive Services: quickly enables apps to see, hear, speak, understand, and interpret a users needs. (Alexa, HomePod)

Azure Bot Service: develop intelligent, enterprise-grade bots (eg., smart chats)

DevOps and GitHub:

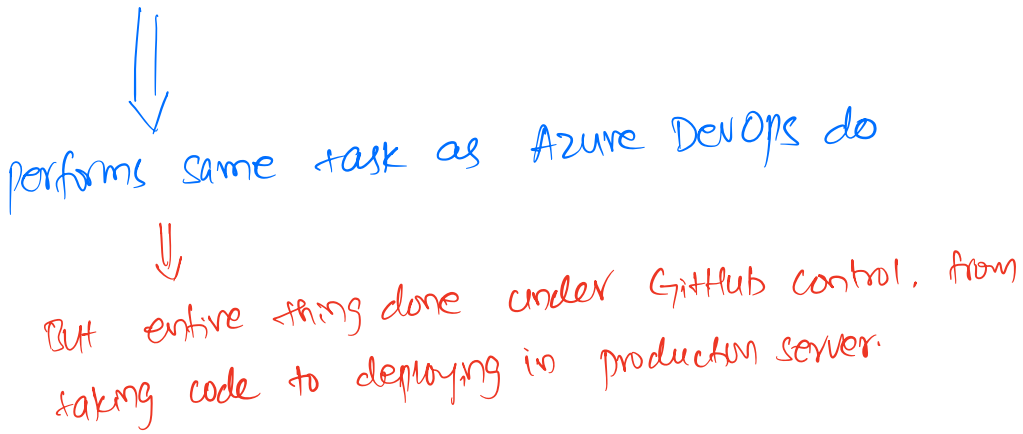
Azure DevOps:



Note: the above shown is just a task, azure can do lot of things that DevOps engineers do

GitHub: it is an version control system and it can be done in azure now.

GitHub Actions for Azure: automates software workflow to build, test, and deploy from writing GitHub.



Azure DevTest Labs: quickly create environments in azure while minimizing waste and controlling cost.

Azure Management Tools:

- Azure portal, azure PowerShell, Azure CLI, cloud Shell, and Azure Mobile App.
- Azure Advisor
- Azure Resource Manager (ARM) templates
- Azure Monitor
- Azure Service Health

Azure Advisor: analyzes deployed azure resources and makes recommendations on the best practices to optimize azure deployments ——> purpose ——> we may have large number of virtual machines, we can't go through each VM to look after it, So Azure provided Azure Advisor service to look after of them and make some recommendations. (We can say it can generates reports on VM's). It can advise following

- Availability
- security
- Performance
- Cost
- Operational excellence

Azure Monitor: it maximizes the availability and performance of applications and services by collecting, Analyzing, and acting telemetry from cloud and on-premises environments. It can do following tasks

- application insights
- Log analytics
- Smart alerts
- Automation actions
- Customized dashboards

E.g., if RAM is used 80% then it will send an notification that RAM is almost near to deadline. So, we have to act accordingly

Azure Service Health: it provides a personalized view of the health of azure services and the regions being used.

- Communication regarding outages
- Planned maintenance
- Other health advisories

Azure Resource Manager (ARM): ARM templates are a form of infrastructure as code, a concept where you define the infrastructure that needs to be deployed. ARM templates use declarative syntax, meaning you define the resources for Azure to deploy without specifying how the resources are created.

Security:

Azure security features
- Security center and resource hygiene
- Key vault and dedicated hosts

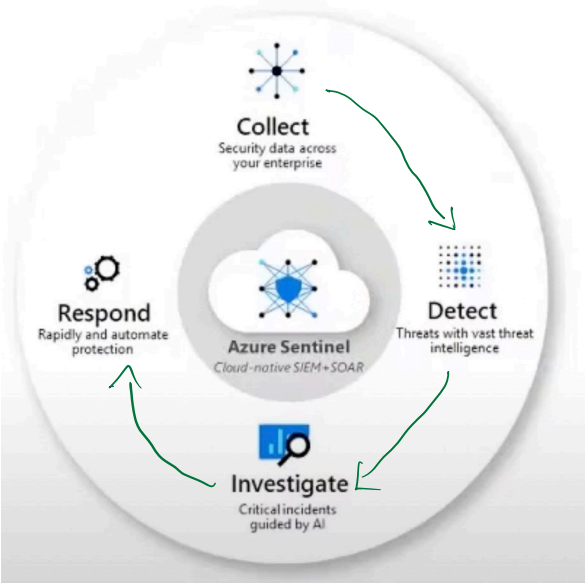
Azure network security
- Defense in depth
- Network security groups and firewalls
- DDoS protection

Security tools and features
- Azure security center, including policy compliance, security alerts, secure score, and resource hygiene
- Azure sentinel
- Key vault
- Azure dedicated hosts

Azure Security Center: it is a monitoring service that provides threat protection across both Azure and on-premises data centers
- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports (I.e., opening ports for limited time whenever is needed)

Azure Sentinel: it is a security information management and security automated response solution that provides security analytics and threat intelligence across an enterprise

It follows a chain as shown in the following diagram



Azure Key Vault: it stores application secrets in a centralized cloud location in order to securely control access permissions and access logging. (Like bank locker)

- Secrets management
- Key management
- Certificate management
- Storing secrets protected by hardware security modules (HSMs)

Azure dedicated host: provides physical servers that host one or more azure virtual machines that is dedicated to a single organizations workload

Benefits

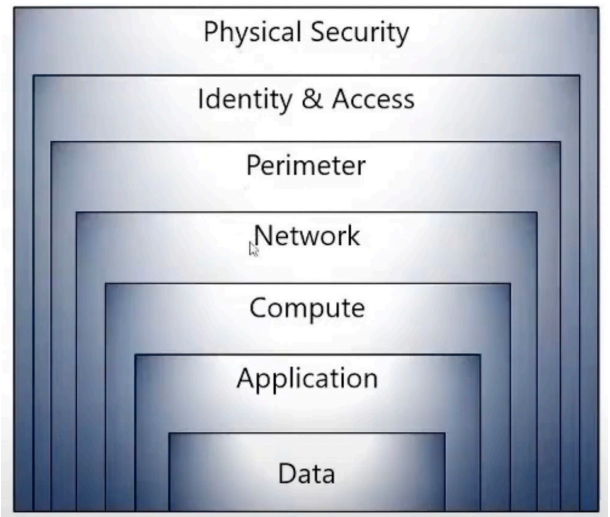
- Hardware isolation at the server level
- Control over maintenance event timing
- Aligned with azure hybrid use benefits

Secure network connectivity:

- Defense in depth
- Network security groups
- Azure firewall
- Azure DDoS protection

Defense in depth: generally in providing security, a layered approach is followed for securing computer systems.

- provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers



Shared security model:

Certain things we have to manage and certain things will be managed by Azure like shown in the diagram

Responsibility	On-Premises	IaaS	PaaS	SaaS
Data governance and Rights Management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account and access management	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network controls	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Customer	Microsoft	Microsoft
Physical hosts	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacenter	Customer	Microsoft	Microsoft	Microsoft

Network security groups: it is used to set inBound and outBound rules to filter by source and destination IP address, port, and protocol. (I.e., deals with IP address, port, and protocol)

What can be done?

- Add multiple rules, as needed, within subscription limits.
- Azure applies default, baseline security rules to new NSGs
- Override default rules with new, higher priority rules

Now, NSGs work on IP address, what if I want to deal with domain name

Azure Firewall: it is a stateful, managed firewall as a service (FaaS) that grants/denies server access based on originating IP address (with domain name), in order to protect network resources

Then it do same job as NSGs and additionally it maintains logs for every activity too.

Azure distributed denial of service (DDoS) protection:

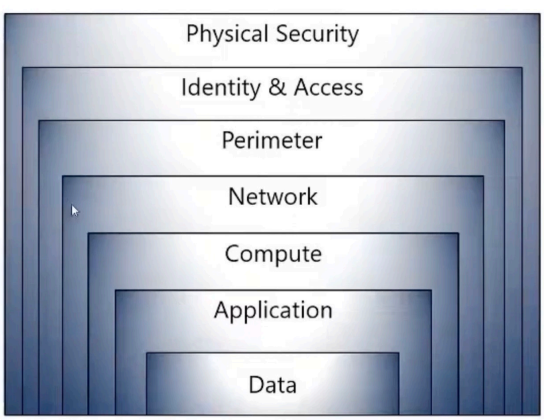
DDoS attacks overwhelm and exhaust network resources, making apps slow or unresponsive.

- Sanitizes unwanted network traffic before it impacts service availability.
- Basic service tier is automatically enabled in Azure.
- Standard service tier adds mitigation capabilities that are tuned to protect Azure Virtual Network resources.

Defense in Depth Reviewed

Combining network security solutions

- **NSGs** with **Azure Firewall** to achieve defense in depth.
- **Perimeter layer** protects your network boundaries with Azure DDoS Protection and Azure Firewall.
- **Networking layer** only permits traffic to pass between networked resources with Network Security Group (NSG) inbound and outbound rules.



Azure identity, governance, privacy, and compliance

Azure identity services
- Authentication VS authorization
- azure AD, MFA, SSO and conditional Access

Azure governance features
- RBAC
- Resource locks and tags
- Policy, blue prints, and CAF

Azure privacy and compliance
- Privacy statement and online service terms
- Trust center and compliance documentation
- Azure sovereign regions

Authentication VS Authorization

Authentication
- Identifies the person or service seeking access to a resource.
- Requests legitimate access credentials.
- Basis for creating secure identity and access control principles.

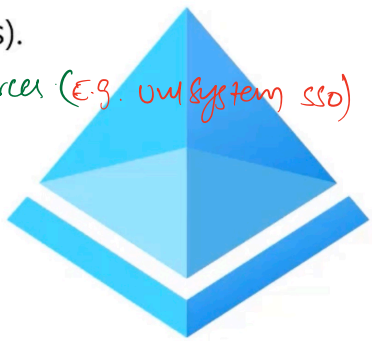
Authorization
- Determines an authenticated person's or service's level of access.
- Defines which data they can access, and what they can do with it.

Now, who will take care of this authentication and authorization

Let's dive into Azure Active directory

Azure Active Directory (AAD) is Microsoft Azure's cloud-based identity and access management service.

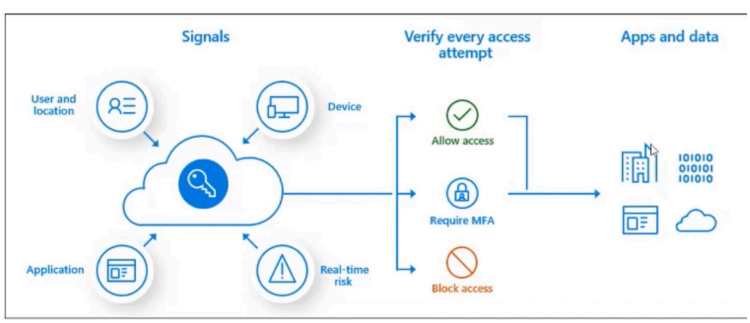
- Authentication (employees sign-in to access resources).
- Single sign-on (SSO). — login one time & use all resources (E.g. UM system SSO)
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.



Conditional Access: Multi factor authentication can be done with the help of conditional access as shown below

Conditional Access is used by Azure Active Directory to bring signals together, to make decisions, and enforce organizational policies.

- User or Group Membership
- IP Location
- Device
- Application
- Risk Detection



MFA can be done if any doubts regarding above shown factors

E.g. If user logins from USA & his account is from India (very unique activity). So, it asks for MFA

⇓

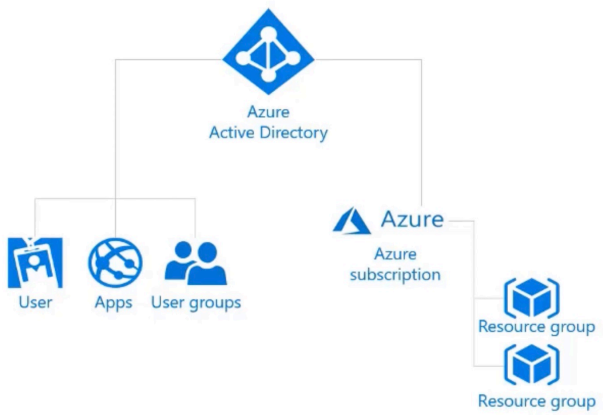
This scenario can be done on IP location

⇓

like this every factor has its own scenario

Azure Governance Methodologies:

Role based access control:



- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

Note: if access to granted to the resource group, then the permission will be granted to all users in the resource group

If access to granted to the management group, then permission we be granted to all users, applications, and what ever is under the management group

Note: the hierarchy is written in the above pages (resources-resource groups-subscriptions-management groups)

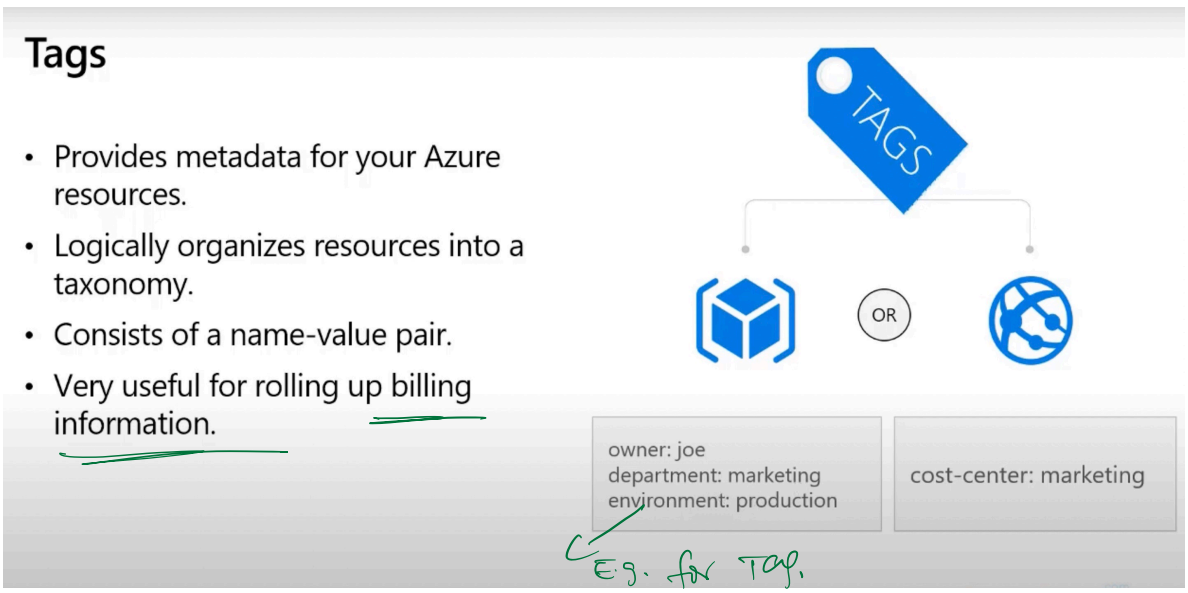
Resource Lock:

- Protect your Azure resources from accidental deletion or modification.
- Manage locks at subscription, resource group, or individual resource levels within Azure Portal.

Lock Types	Read	Update	Delete
CanNotDelete	Yes	Yes	No
ReadOnly	Yes	No	No

Note: in ReadOnly lock doesn't allow us to do anything other than read, however CanNotDelete lock allow us to do updates but not deletion.

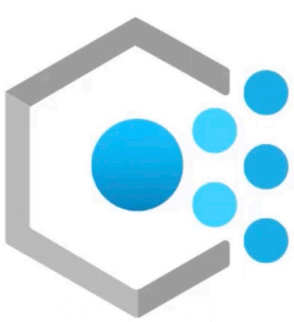
Tags:



Azure Policy:

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Provides governance and resource consistency with regulatory compliance, security, cost, and management.

- Evaluates and identifies Azure resources that do not comply with your policies.
- Provides built-in policy and initiative definitions, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.



↳ Policies can be set at any level (i.e. subscription level, resource level, etc)

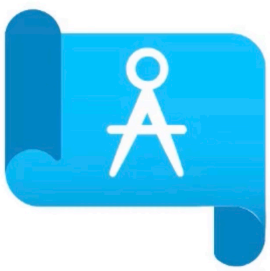
Note: kind of policies (Example): If I set a policy that a VM can't be created in location other than India, then VM Should not be created outside India

- Policy can be implemented on anything (if provided in azure)

Azure Blueprints:

Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments. Development teams can quickly build trust through organizational compliance with a set of built-in components (such as networking) in order to speed up development and delivery.

- Role Assignments
- Policy Assignments
- Azure Resource Manager Templates
- Resource Groups

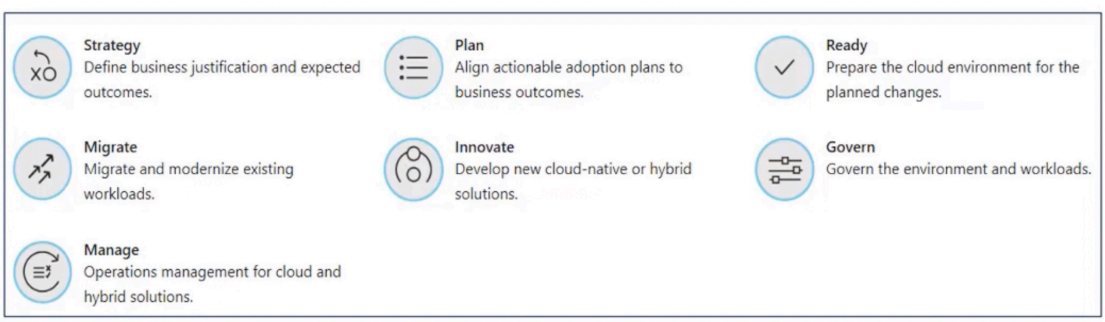


All this are assigned by default with the help of Blue prints

E.g., if in a blueprint a set of policies are assigned for an VM, then no need to assign new policies when VM is created. Similarly Blueprints can assign roles, ARM templates, and resource groups

Cloud adoption framework:

Cloud Adoption Framework



- The One Microsoft approach to cloud adoption in Azure.
- Best practices from Microsoft employees, partners, and customers.
- Tools, guidance, and narratives for strategies and outcomes.

Privacy, compliance, and data protection:

Security, Privacy, and Compliance

Security: Secure by design. With built in intelligent security, Microsoft helps to protect against known and unknown cyberthreats, using automation and artificial intelligence.

Privacy: We are committed to ensuring the privacy of organizations through our contractual agreements, and by providing user control and transparency.

↳ microsoft can't use our data.

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

↓

compliance terms & requirements

Compliance Terms and Requirements

Microsoft provides the most comprehensive set of compliance offerings (including certifications and attestations) of any cloud service provider. Some compliance offerings include.

CJIS Criminal Justice Information Services	**HIPAA** Health Insurance Portability and Accountability Act
CSA STAR Certification	**ISO/IEC 27018**
EU Model Clauses	**NIST** National Institute of Standards and Technology

↳ for all this security, Microsoft issues "microsoft privacy statement"

↓

Microsoft Privacy statement: it provides honesty and openness about how Microsoft handles the user data collected from its products and services.

The privacy statement explains
- What data Microsoft processes
- How Microsoft processes it
- What purposes the data is used for

Note: explore various compliances in Microsoft website

Azure Sovereign Regions (US government services)

Meets the security and compliance needs of US federal agencies, state and local governments, and their solution providers.

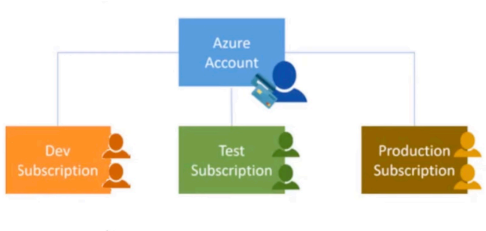
Azure Government:
- Separate instance of Azure.
- Physically isolated from non-US government deployments.
- Accessible only to screened, authorized personnel.

Examples of compliant standards : FedRAMP, NIST 800.171 (DIB), ITAR, IRS 1075, DoD L2, L4 & L5, and CJIS.

Note: in the same way as shown above, Microsoft provides compliances to different countries governments (e.g. China, Germany)

Review Microsoft azure and support

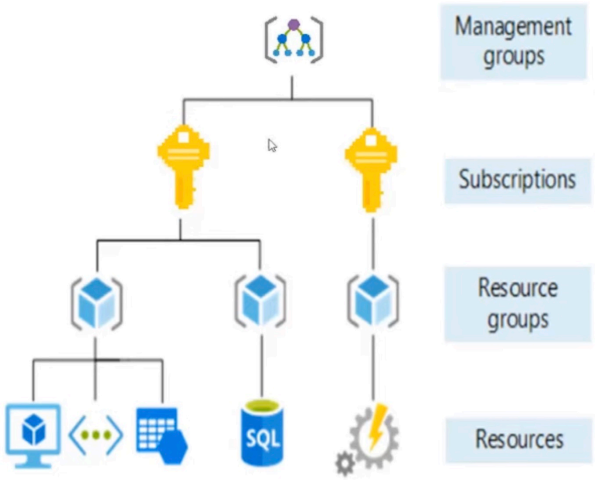
Azure subscriptions



An Azure subscription provides you with authenticated and authorized access to Azure accounts.
Subscriptions can provide billing and access control boundaries.
An account can have one subscription or multiple subscriptions.

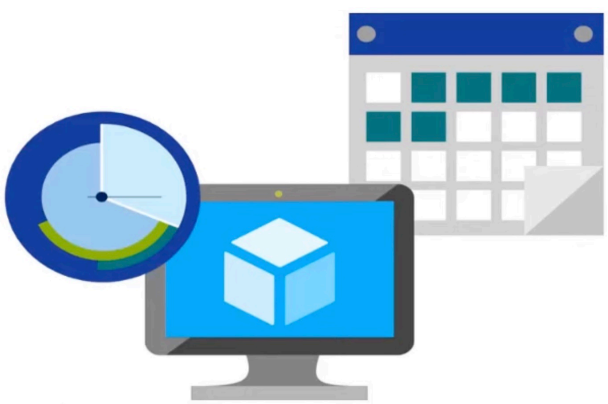
Management Groups:

- Management groups can include multiple Azure subscriptions.
- Subscriptions inherit conditions applied to the management group.
- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth.



Factors affecting costs:

Explore Factors affecting costs



There are three primary factors affecting costs:

Resource Type	Services	Location
Costs are resource-specific, so the usage that a meter tracks and the number of meters associated with a resource depend on the resource type.	Azure usage rates and billing periods can differ between Enterprise, Web Direct, and CSP customers.	The Azure infrastructure is globally distributed, and usage costs might vary between locations that offer Azure products, services, and resources.

Identify Zones for Billing Purposes

Bandwidth - data moving in and out of Azure datacenters. Some inbound data transfers are free, such as data going into Azure datacenters. For outbound data transfers—such as data going out of Azure datacenters—pricing is based on Zones.

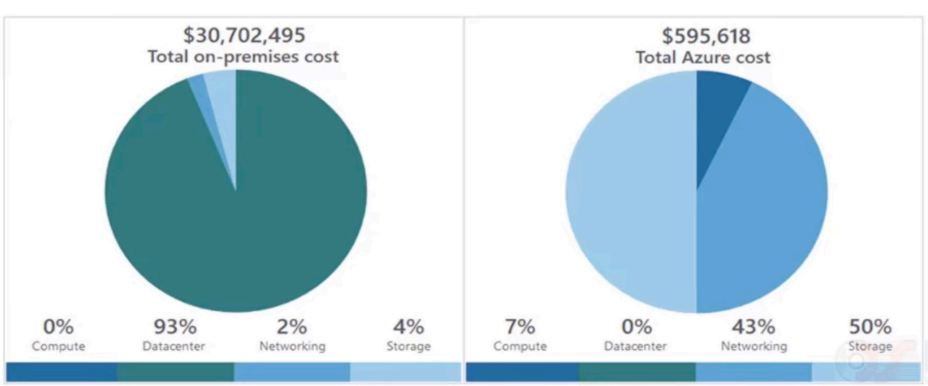
Zone 1	West US, East US, West Europe, and others
Zone 2	Australia Central, Japan West, Central India and others.
Zone 3	Brazil South only.
DE Zone 1	Includes Germany Central and Germany Northeast.

Azure Pricing calculator: Provides a detailed estimate of the costs associated with your infrastructure configuration

Note: there is a TCO calculator which differentiate your on-premises cost and Azure cost (shown u=in following figure)

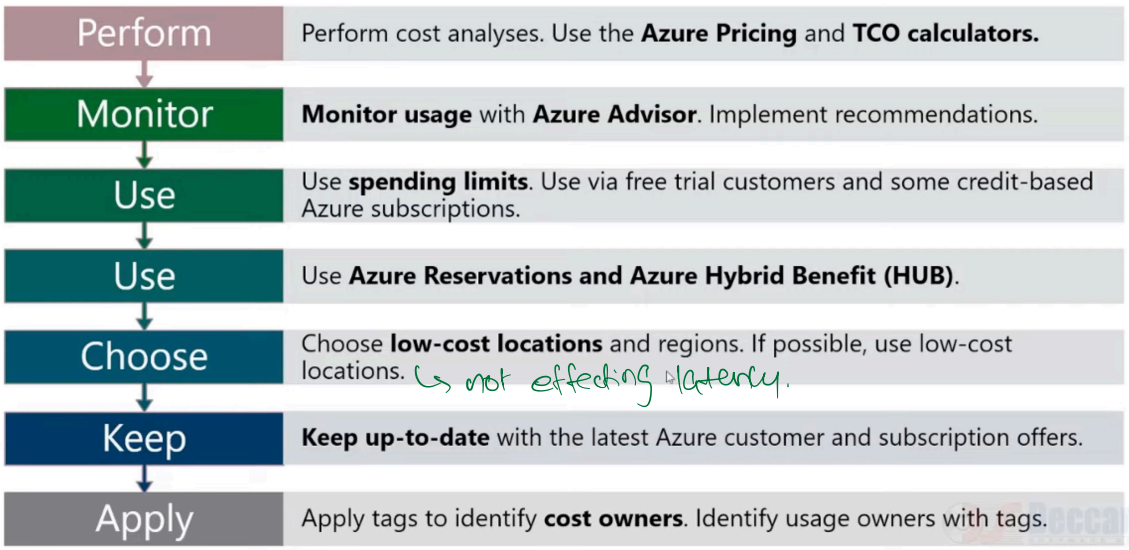
Explore Total cost of ownership (TCO) calculator

A tool to estimate cost savings you can realize by migrating to Azure.
A report compares the costs of on-premises infrastructures with the costs of using Azure products and services in the cloud.



Minimizing cost:

Explore Minimizing costs



Azure Support plans:

Explore Support plan options

Every Azure subscription includes free access to billing and subscription support, Azure products and services documentation, online self-help documentation, white papers, and community support forums.

	Basic	Developer	Standard	Professional Direct
Scope	Available to all Microsoft Azure accounts	Trial and non-production environments	Production workload environments	Business-critical dependence
Technical Support		Business hours access to Support Engineers via email	24x7 access to Support Engineers via email and phone	24x7 access to Support Engineers via email and phone

Other support options

- Microsoft Developer Network (MSDN) Azure Forums
- Stack Overflow

- Microsoft Azure general feedback
- Server Fault
- @AzureSupport (twitter)

Note: there is also a service called "Knowledge Center" where already questions posted and answers given —> we can search our issue here.

Service level Agreements:

SLAs document the specific terms that define Azure performance standards.

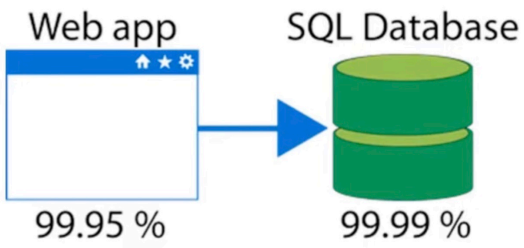
- SLAs define Microsoft's commitment to an Azure service or product.
- Individual SLAs are available for each Azure product and service.
- SLAs also define what happens if a service or product fails to meet the designated availability commitments.

SLA	Downtime per month	Downtime per year
99.9%	43.2 minutes	8.76 hours
99.95	21.6 minutes	4.38 hours
99.99	4.32 minutes	52.56 minutes

- Performance targets are expressed as uptime and connectivity guarantees.
- Performance-targets range from 99.9% (three nines) to 99.99% (four nines).
- If a service fails to meet the guarantees, a percentage of the monthly service fees can be credited to you.

Define Composite SLAs

If the App Service has a 99.95% SLA, and the Azure SQL Database has a 99.99% SLA, what is the composite SLA for your application?



Composite SLA

.9995 * .9999
= 99.94%

- Notice the composite SLA is lower than the individual SLAs.
- Improve the SLA by creating independent fallback paths.

Customers should determine what SLA is needed for their application:

- Know your workload requirements and usage patterns.
- Design for resiliency and availability.
- Establish availability metrics — mean time to recovery (MTTR) and mean time between failures (MTBF).
- Establish recovery metrics — recovery time objective and recovery point objective (RPO).
- Implement resiliency strategies.
- Build in availability requirements.