

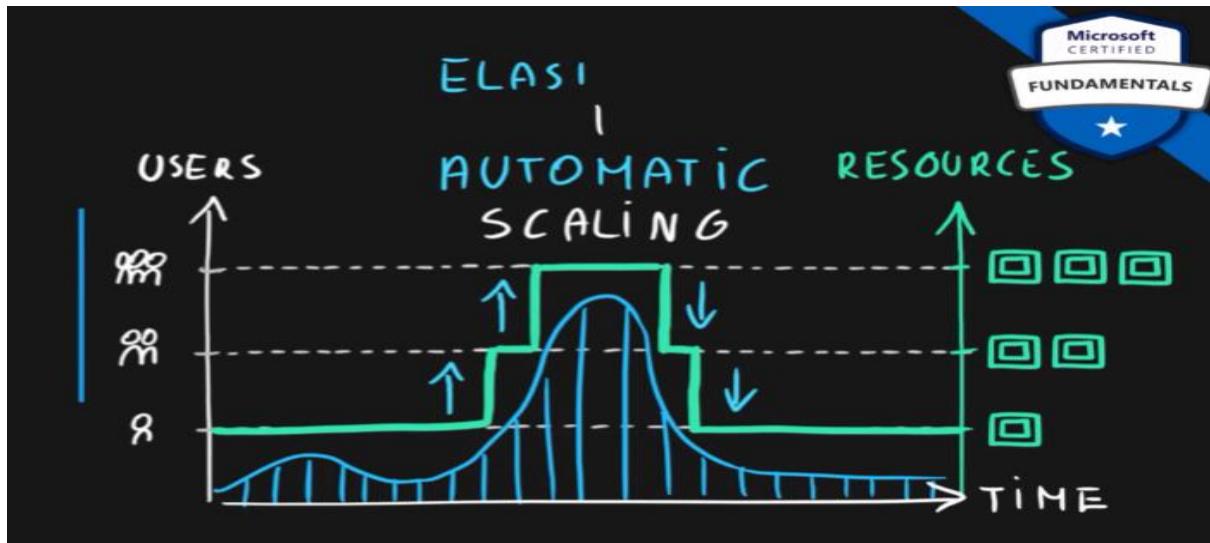
Scalability is the ability to scale

Scaling is a process of

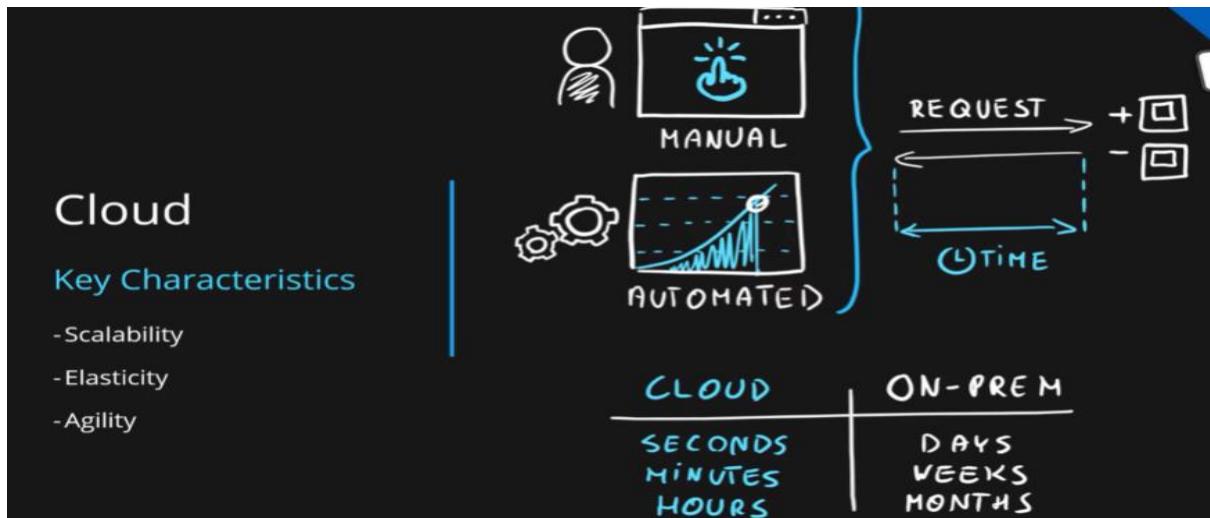
- allocating (adding) or
- deallocating (removing)

resources

Elasticity:- The ability of the system to scale dynamically.



Agility: - it is the ability to allocate & deallocate resources quickly.

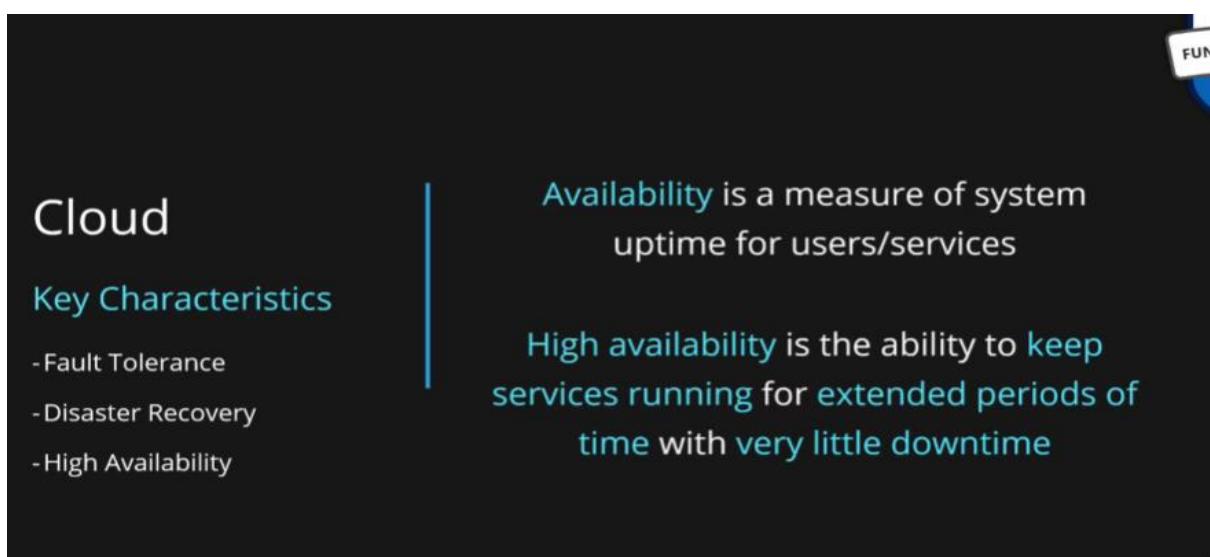
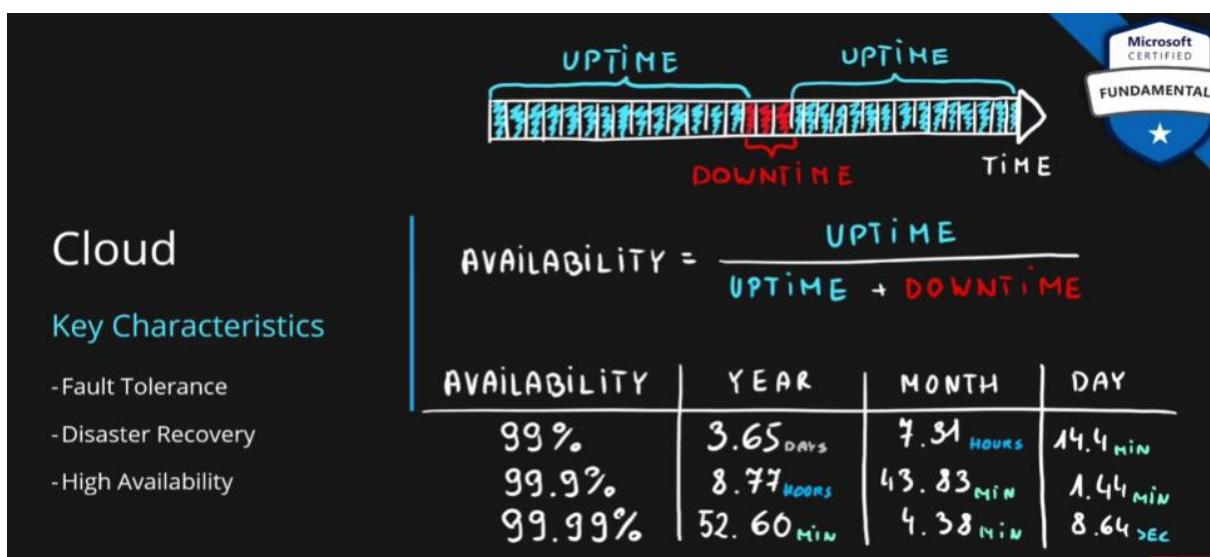
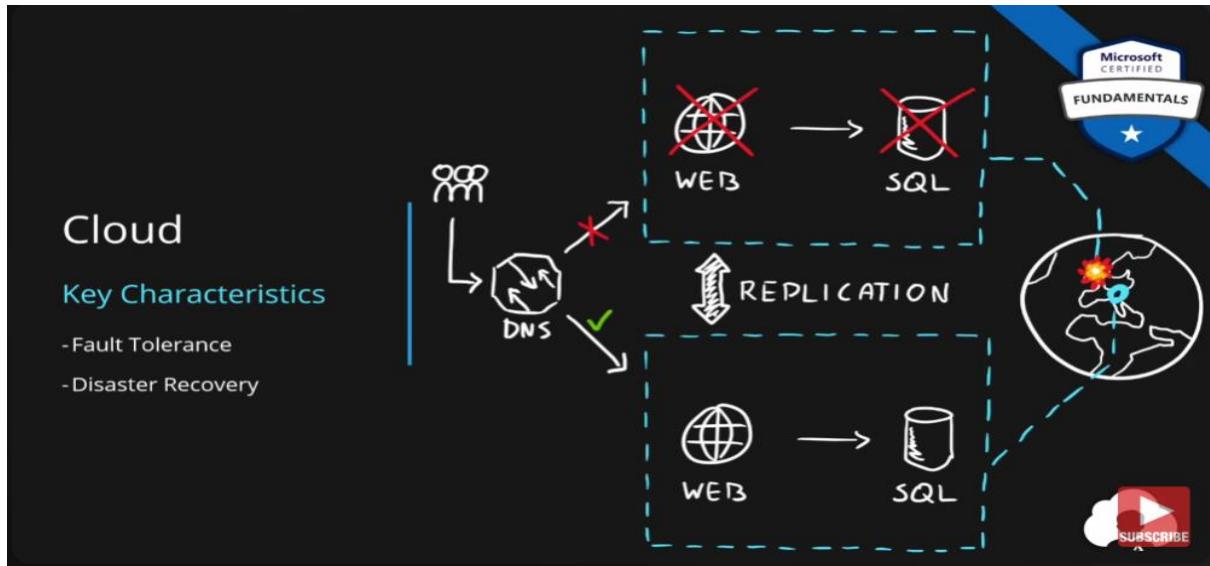


Fault Tolerance: - It is the ability to remain up & running during component or service failures.



Disaster is a serious disruption of services caused by natural or human-induced causes.

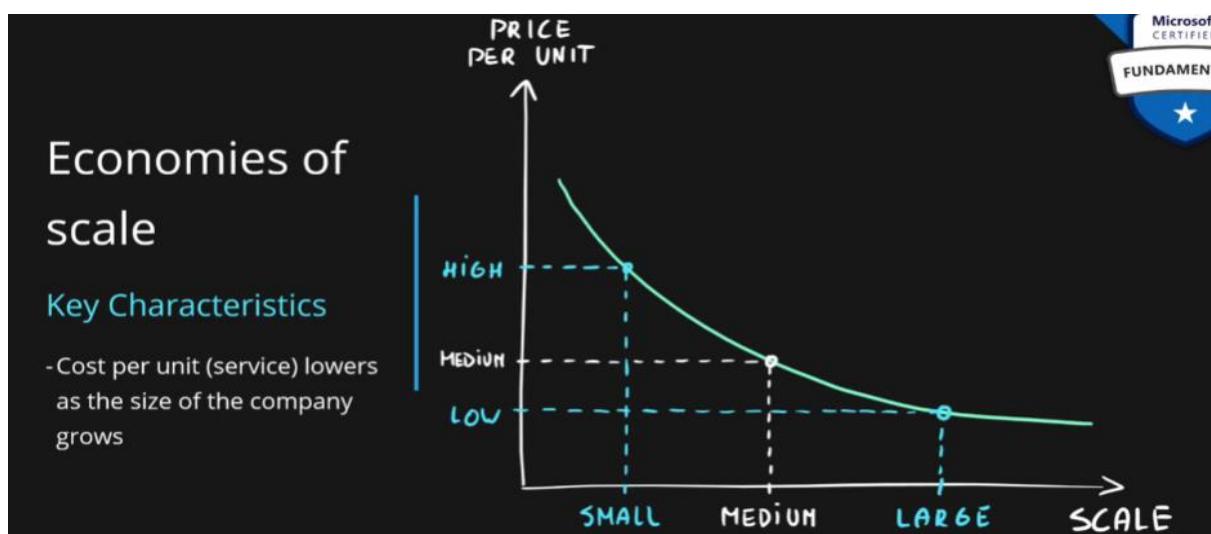
Disaster Recovery: - Ability to recover from an event that has taken down the service.



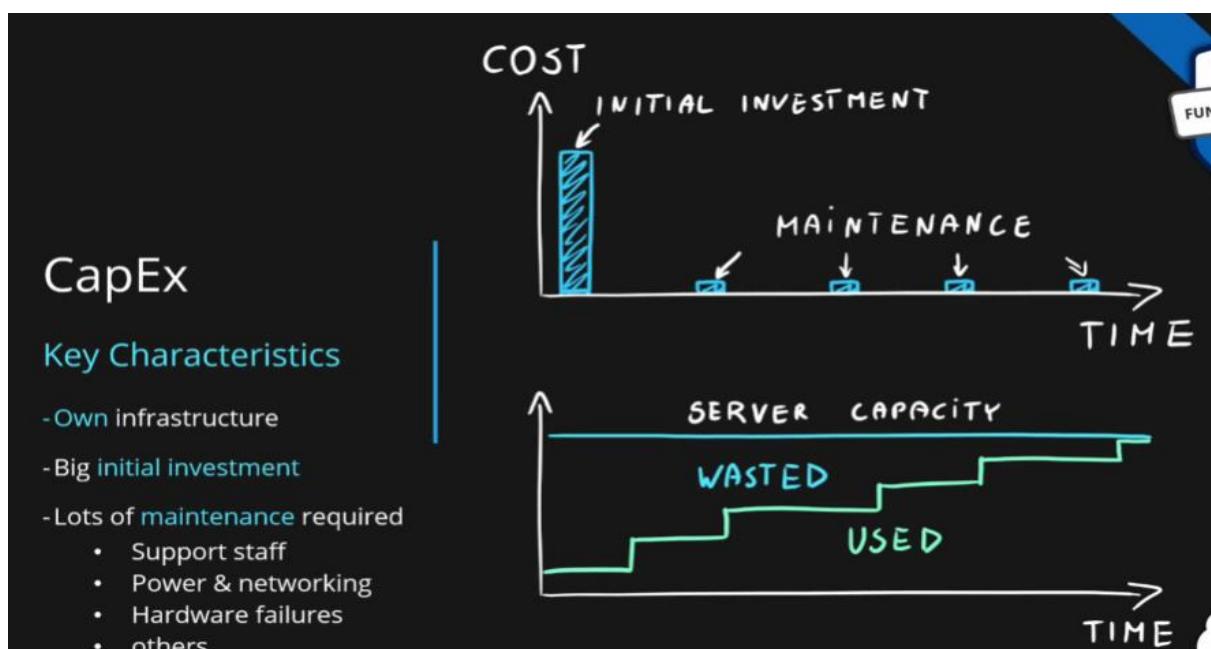
Economies of scale

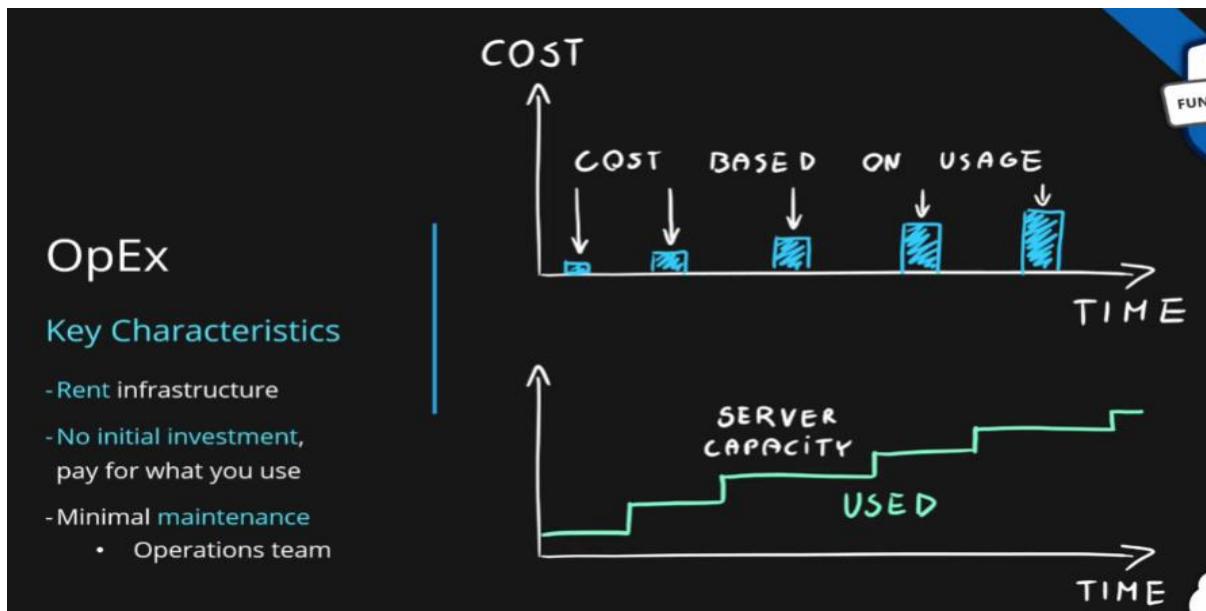
Key Characteristics

SCALE	DELIVERY COMPANY		
	x 3	x 300	
CAR	INDIVIDUAL PURCHASE \$10K	BULK PURCHASE \$ 9K	
MAINTENANCE	INDIVIDUAL \$100	CONTRACT \$ 90	
INSURANCE	INDIVIDUAL \$ 500	BULK PURCHASE \$ 400	
OTHER	INDIVIDUAL \$100	SHARED \$ 80	
CUSTOMERS	888	888 888 888 888 888	
PRICE PER UNIT	\$10	\$ 9	

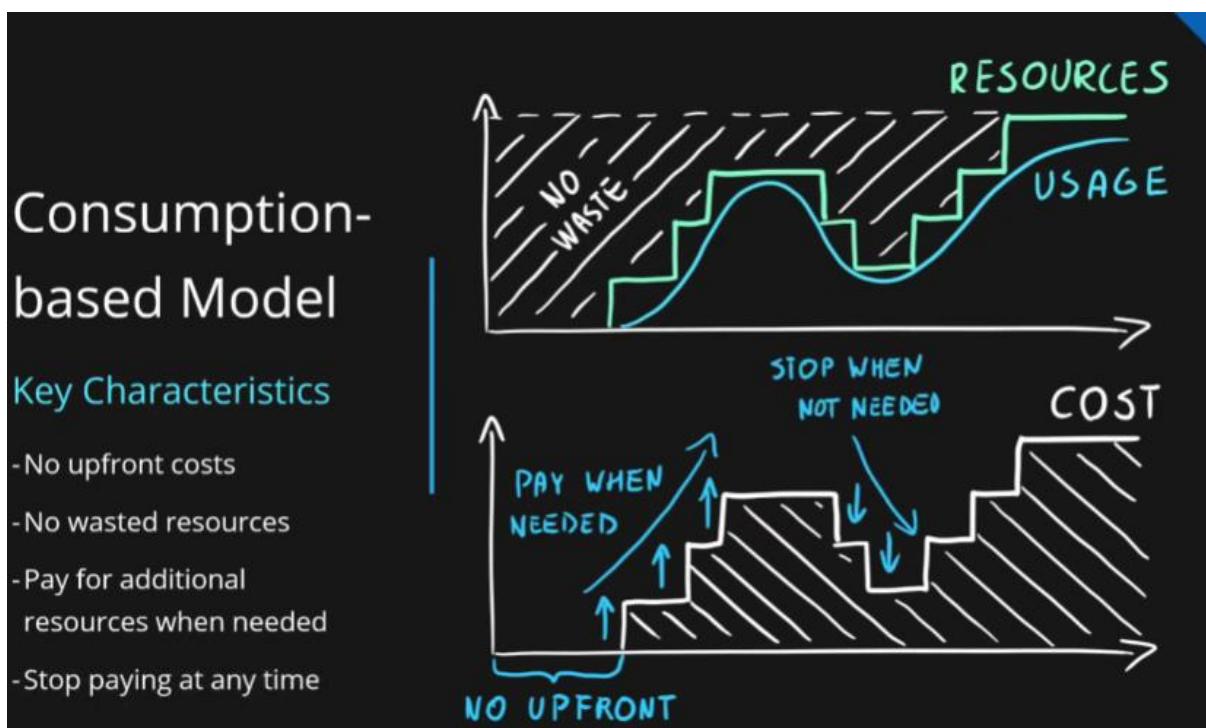


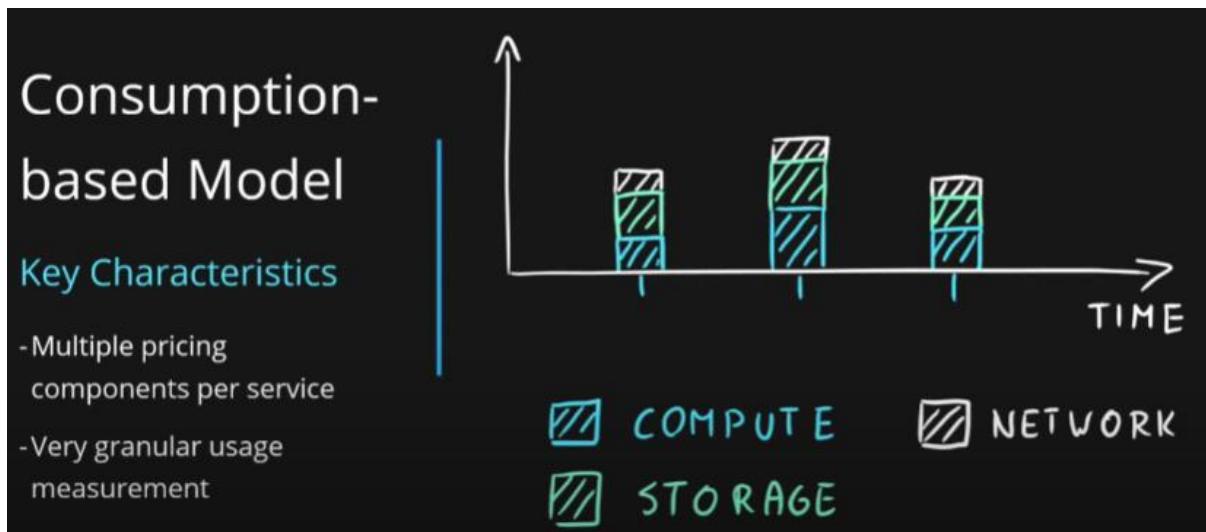
CapEx & OpEx



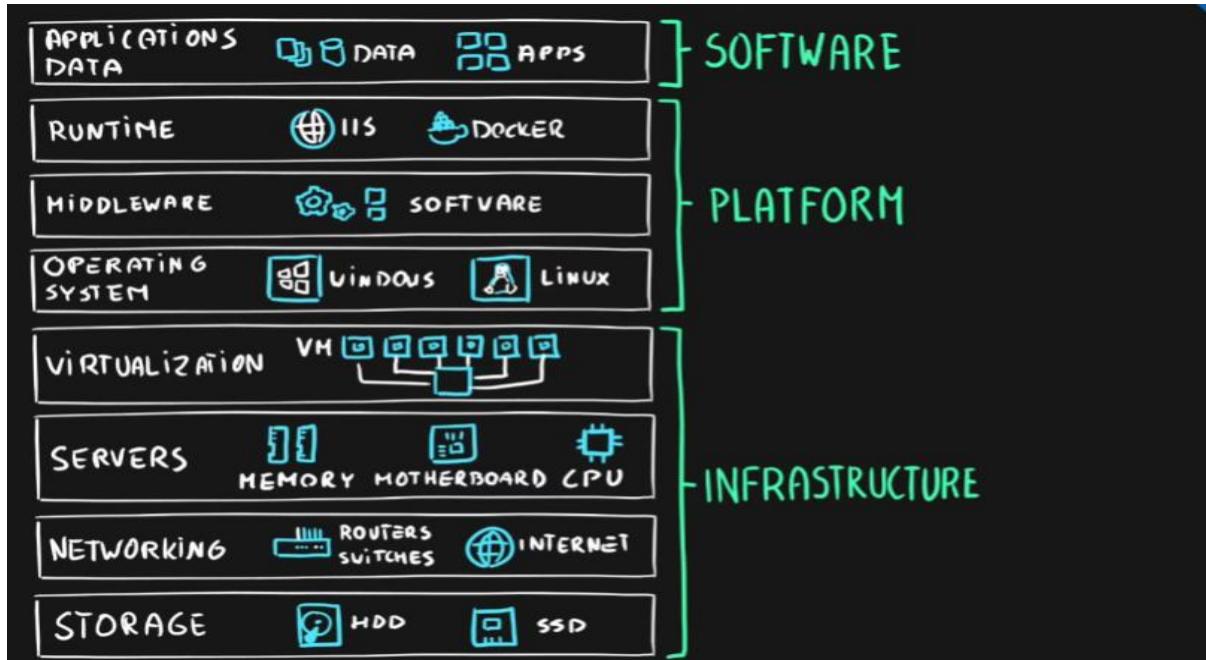
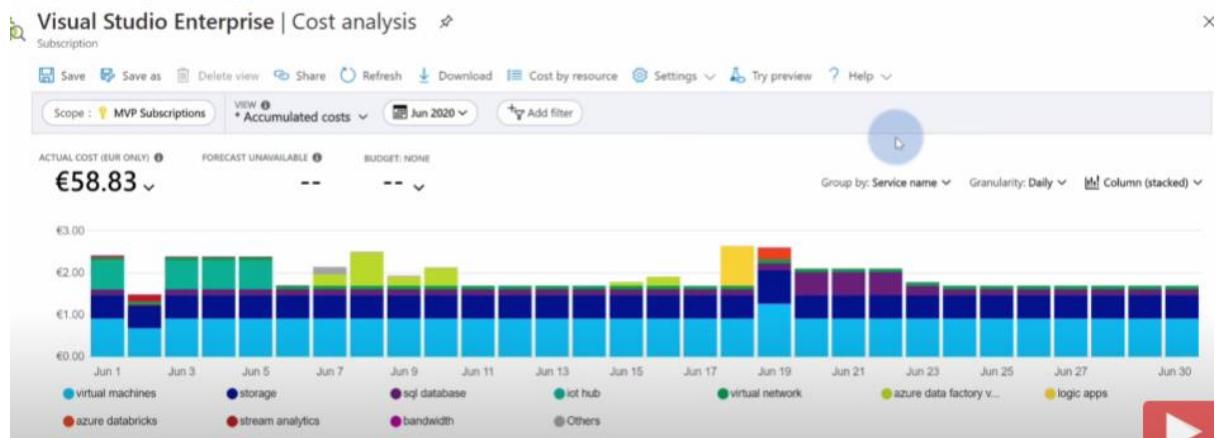


	CapEx	OpEx
Up front cost	Significant	None
Ongoing cost	Low	Based on usage
Tax Deduction	Over time	Same year
Early Termination	No	Anytime
Maintenance	Significant	Low
Value over time	Lowers	No change





Real time cost analysis example.



Service Type Models.

ON PREMISE: - If we are maintaining all the layers.

IAAS: - If the INFRASTRUCTURE is maintained by azure and others are given for us.

Infrastructure as a Service (IaaS)

Key Characteristics

Ownership

- Cloud provider manages **infrastructure**
 - Infrastructure – networking, hardware & virtualization
- You manage **platform & software**
 - Platform – operating system, middleware, runtime
 - Software – data & applications

Use cases

- Migration of workloads
- Test & development
- Storage, backups and recovery

VIRTUAL MACHINE (Icon: square with a smaller square inside)

VIRTUAL NETWORK (Icon: three dots in a horizontal line)

MANAGED DISK (Icon: cylinder)

Platform as a Service (PaaS)

Key Characteristics

Ownership

- Cloud provider manages infrastructure & platform
 - Infrastructure – networking, hardware & virtualization
 - Platform – operating system, middleware, runtime
- You manage **software**
 - Software – data & applications

Use cases

- Development framework
- Analytics & business intelligence

SQL (Icon: cylinder)

APP SERVICE (Icon: globe)

LOGIC APPS (Icon: curly braces with two small squares)

FUNCTION APPS (Icon: lightning bolt)

Software as a Service (SaaS)

Key Characteristics

Ownership

- Cloud provider manages **infrastructure, platform & software**
 - Infrastructure – networking, hardware & virtualization
 - Platform – operating system, middleware, runtime
 - Software – data & applications
- You manage **nothing**

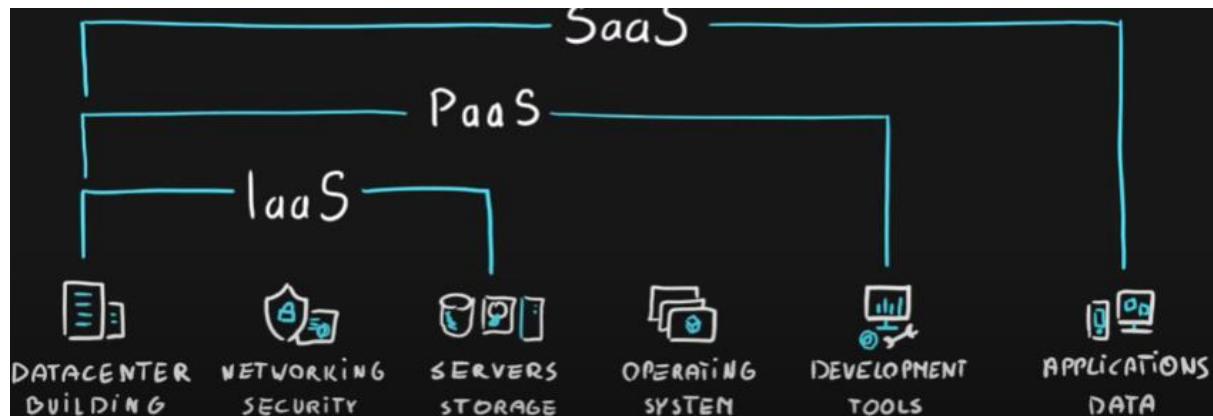
Use cases

- Buying of-the-shelf applications

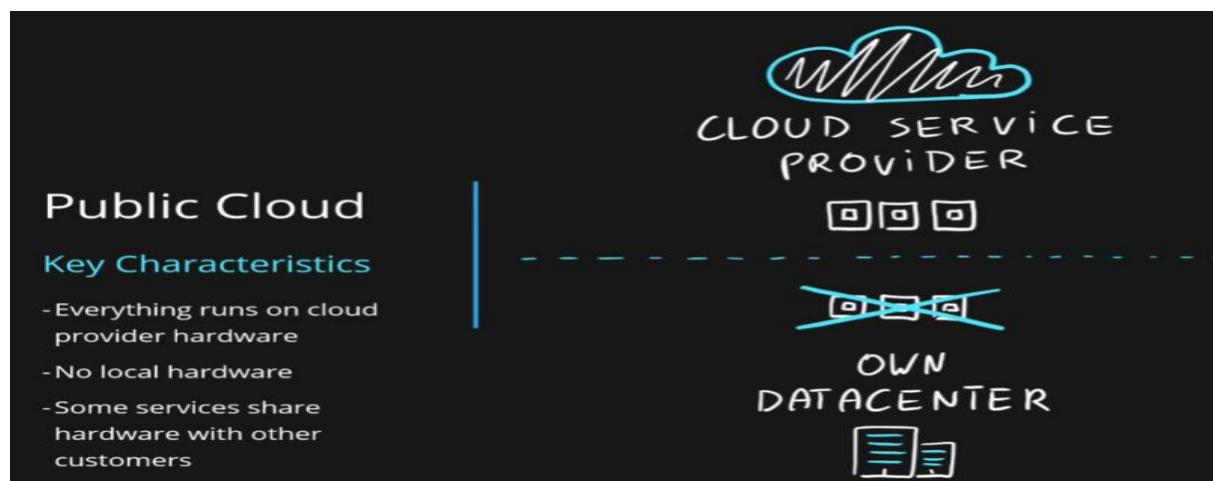
ONE DRIVE (Icon: cloud with zigzag lines)

OUTLOOK (Icon: envelope)

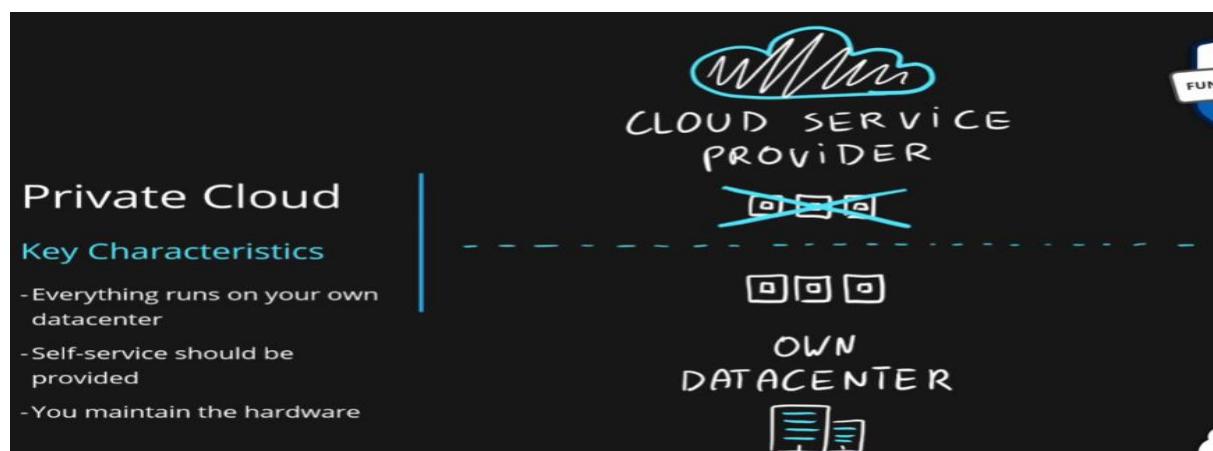
SKYPE (Icon: stylized 'S' inside a cloud)



Deployment Models.



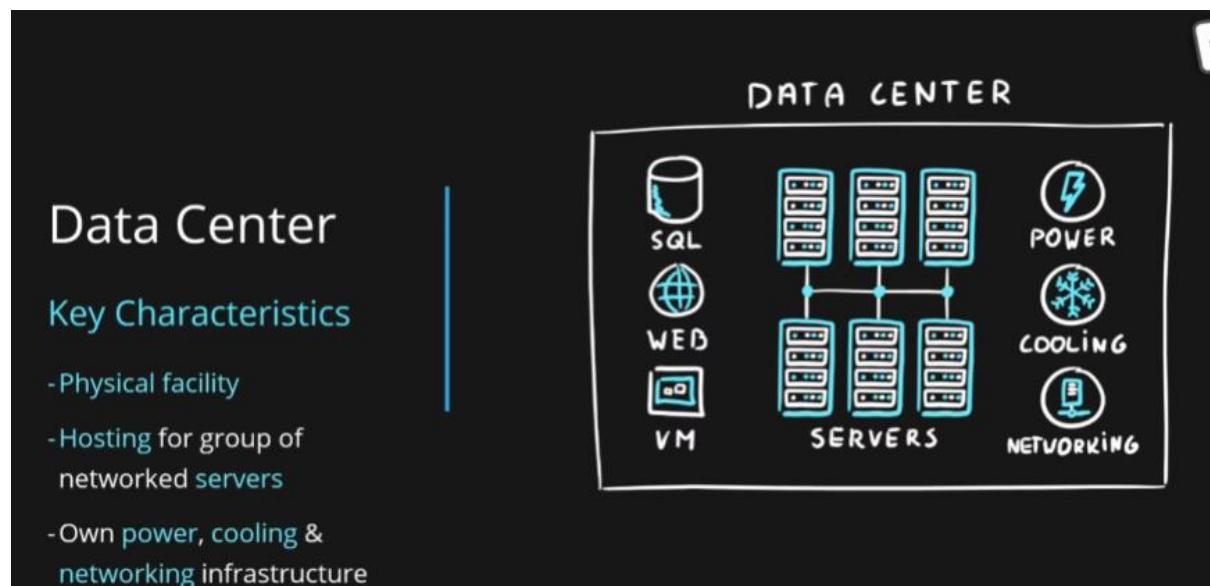
Advantages	Disadvantages
No CapEx	Security & Compliance
High availability & Agility	Ownership
Pay as you go pricing	Specific scenarios with unique business req.
No hardware maintenance	
No deep technical skills required	



Advantages	Disadvantages
Can support any scenario	Initial CapEx
Control over security	Limited Agility
Can meet any security & compliance requirements	IT skills & expertise are mandatory



Advantages	Disadvantages
Great flexibility	Can be more expensive
Run legacy apps in private cloud	Complicated to manage
Utilize existing infrastructure	IT skills & expertise are mandatory
Meet any security requirements	



Availability Zone

Key Characteristics

- Regional feature
- Grouping of physically separate facilities
- Designed to protect from data center failures
- If zone goes down others continue working

Availability Zone

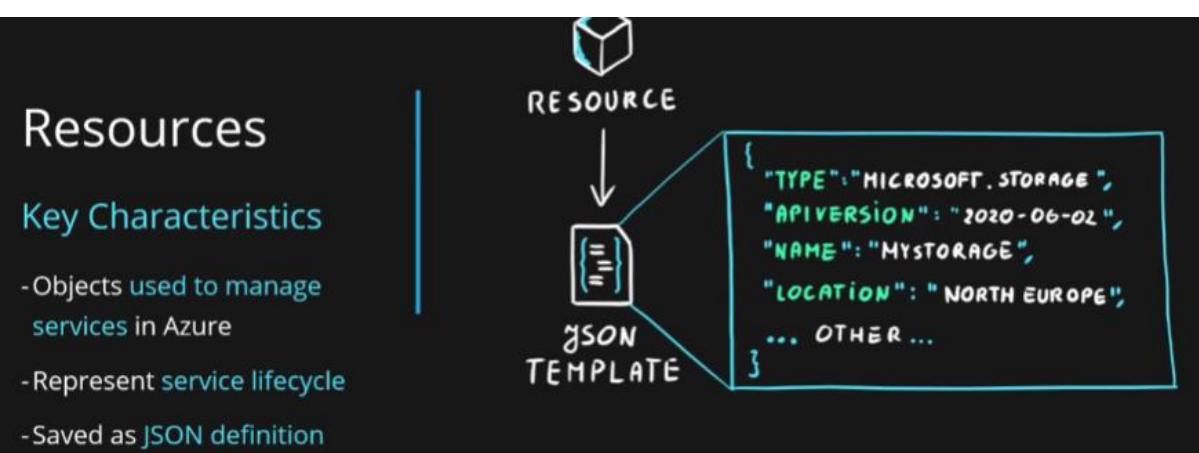
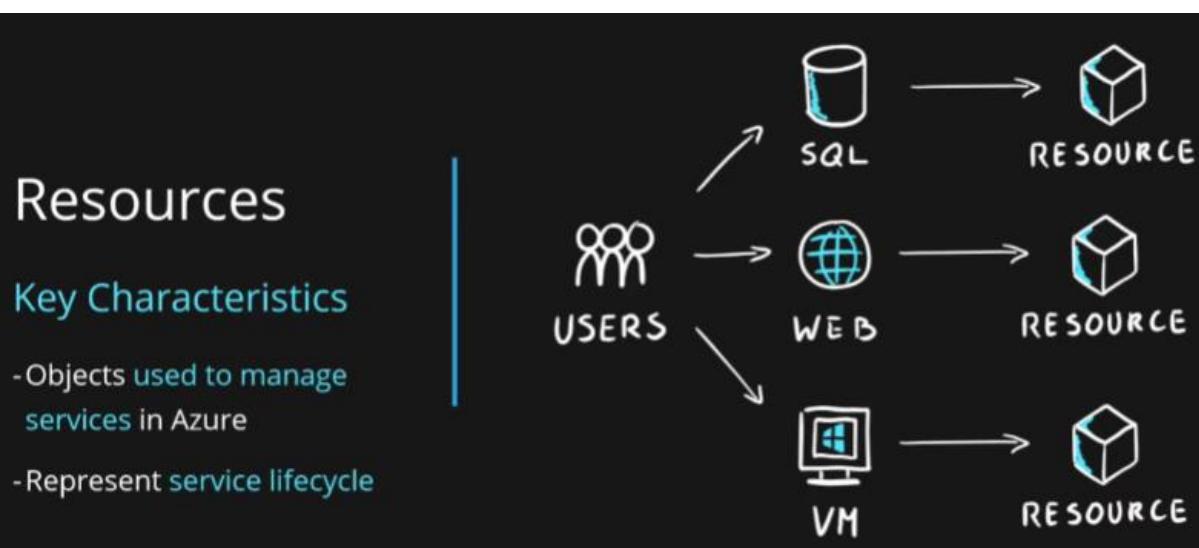
Key Characteristics

- Two service categories
 - Zonal services (Virtual Machines, Disks, etc.)
 - Zone-redundant services (SQL, Storage, etc.)

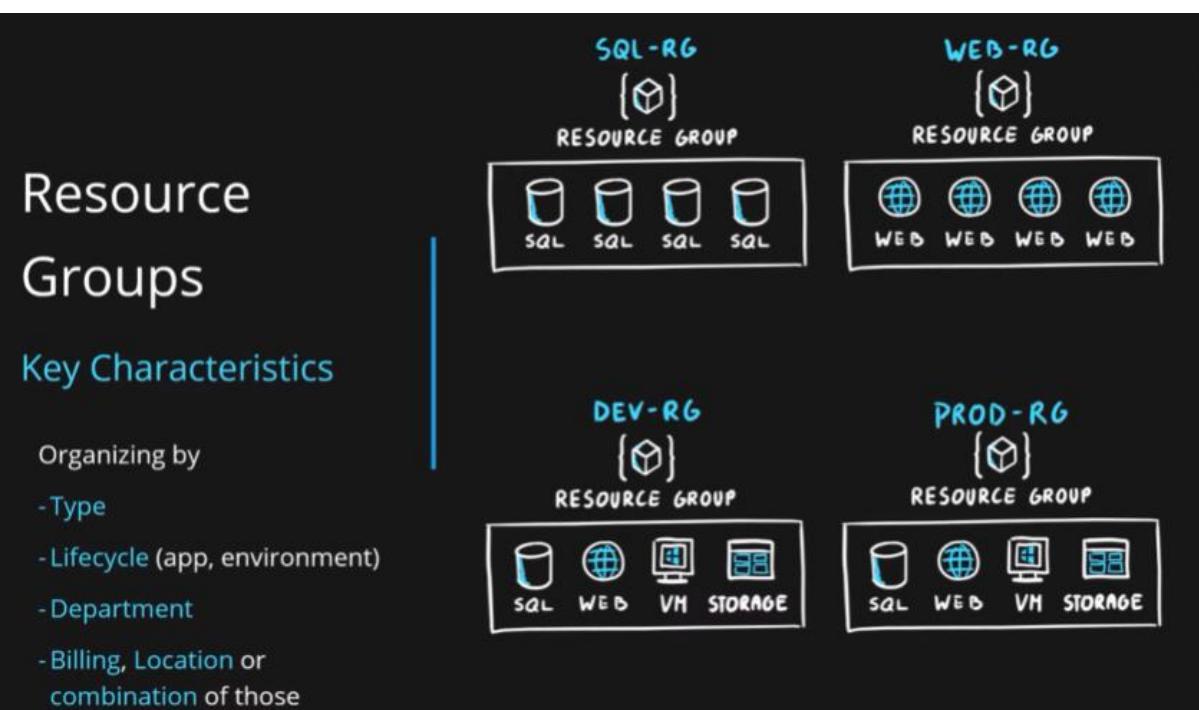
Azure Infrastructure Overview

GEOGRAPHY

13:34 / 14:50 · Geographies >



Resources are created under resource groups.



Resource Groups

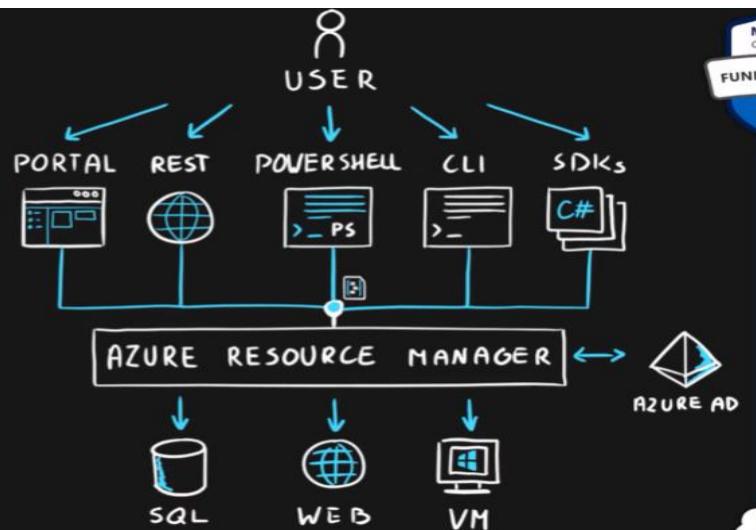
Additional information

- Each resource must be in one, and only one resource group
- Resource groups have their own location assigned
- Resources in the resource groups can reside in a different locations
- Resources can be moved between the resource groups
- Resource groups can't be nested
- Organize based on your organization needs but consider
 - Billing
 - Security and access management
 - Application Lifecycle

Resource Manager

Key Characteristics

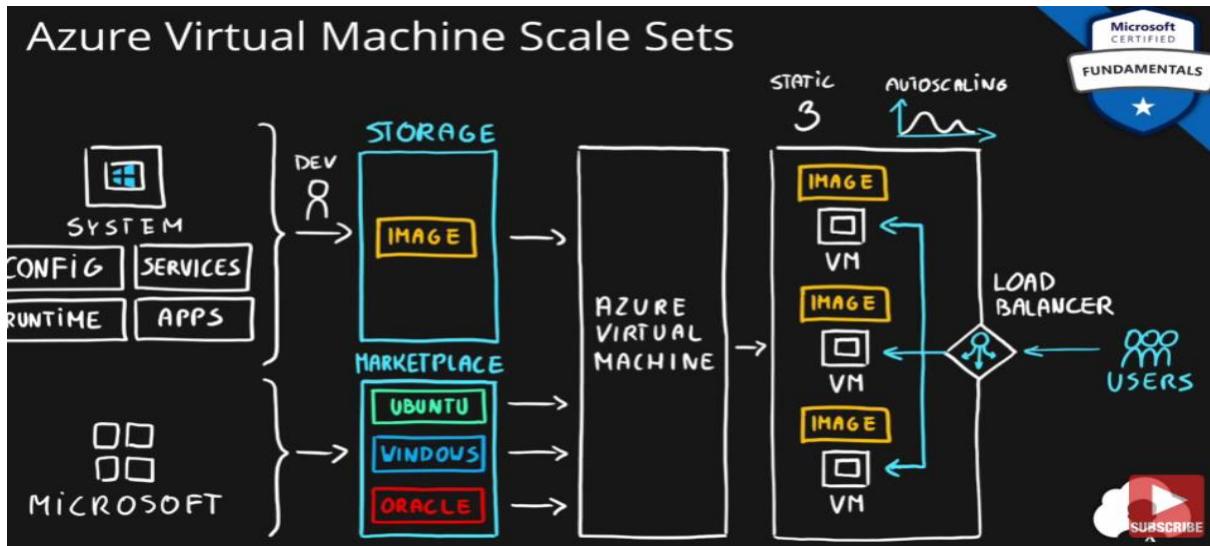
- Management Layer for all resources and resource groups
- Unified language
- Controls access and resources



Virtual Machines

Key Characteristics

- Infrastructure as a Service (IaaS)
- Total control over the operating system and the software
- Supports marketplace and custom images
- Best suited for
 - Custom software requiring custom system configuration
 - Lift-and-shift scenarios
- Can run any application/scenario
 - web apps & web services,
 - databases,
 - desktop applications,
 - jumpboxes,
 - gateways, etc.



Virtual Machine Scale Sets

Key Characteristics

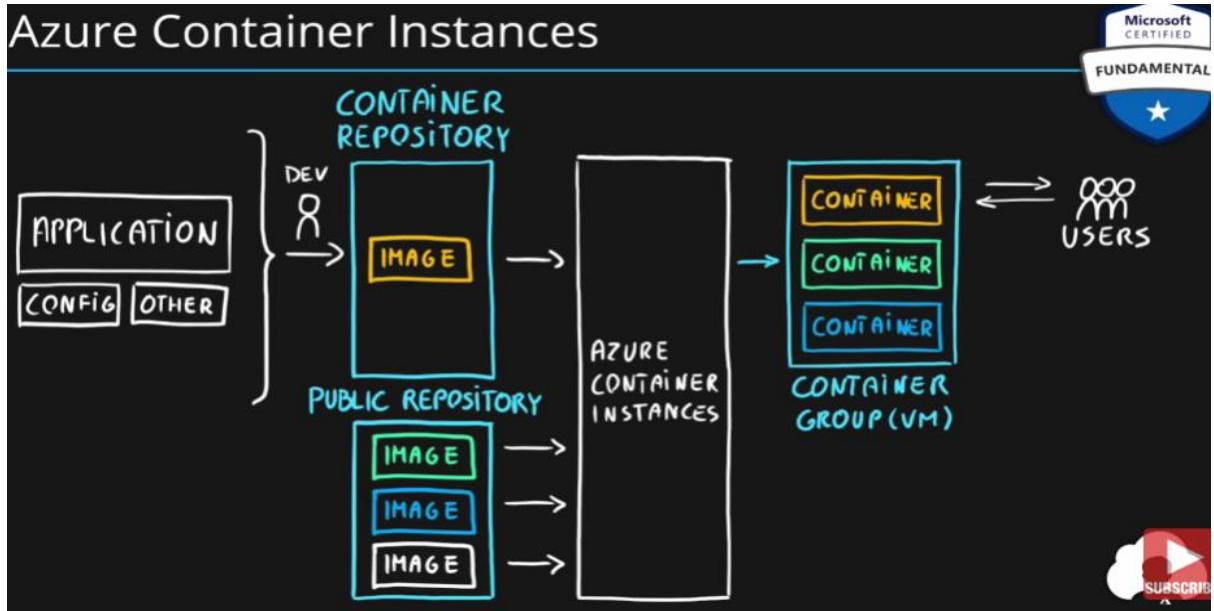
- Infrastructure as a Service (IaaS)
- Set of identical virtual machines
- Built-in auto scaling features
- Designed for manual and auto-scaled workloads like web services, batch processing, etc.

Containers

Key Characteristics

- Use host's operating system
- Emulate operating system (VMs emulate hardware)
- Lightweight (no O/S)
 - Development Effort
 - Maintenance
 - Compute & storage requirements
- Respond quicker to demand changes
- Designed for almost any scenario

Azure Container Instances

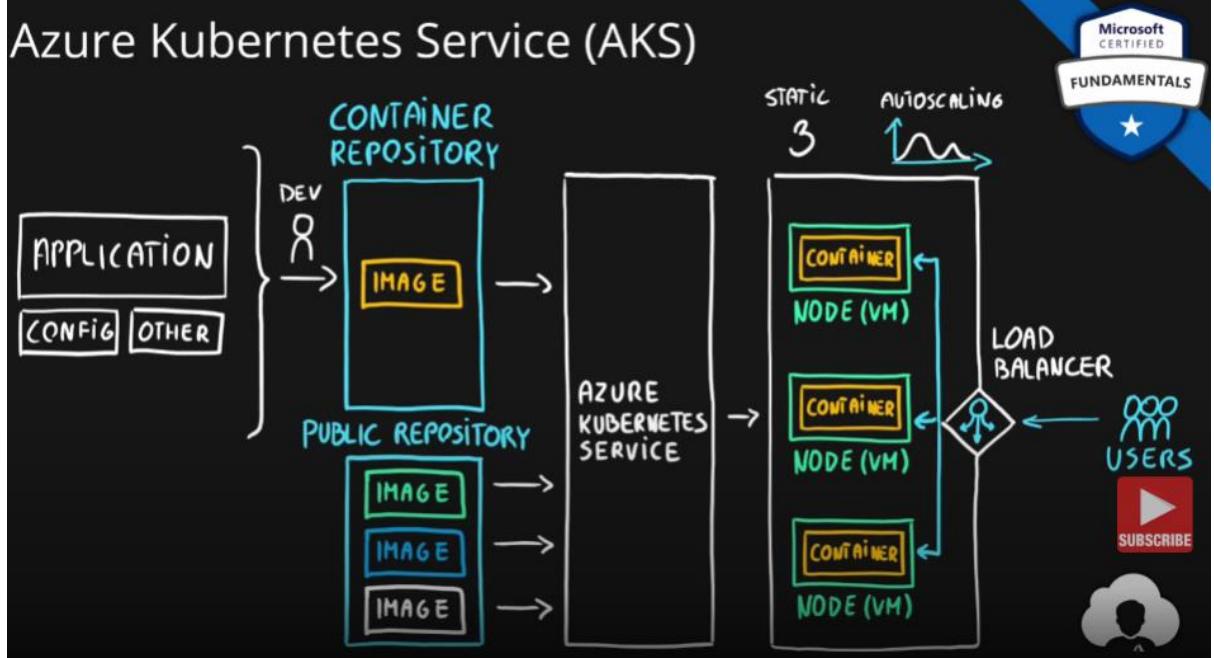


Azure Container Instances

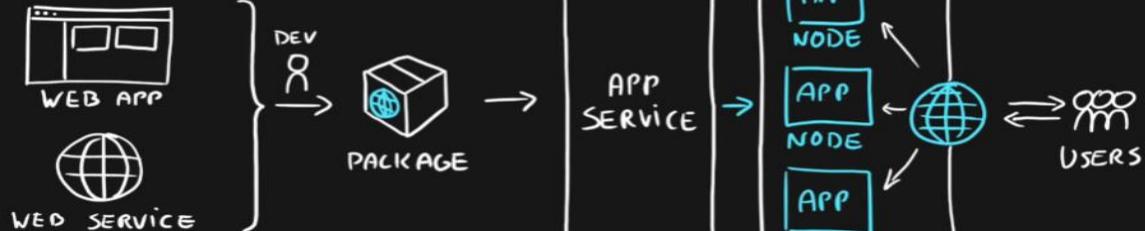
Key Characteristics

- Simplest and fastest way to run a container in Azure
- Platform as a Service
- Serverless Containers
- Designed for
 - Small and simple web apps/services
 - Background jobs
 - Scheduled scripts

Azure Kubernetes Service (AKS)



App Service

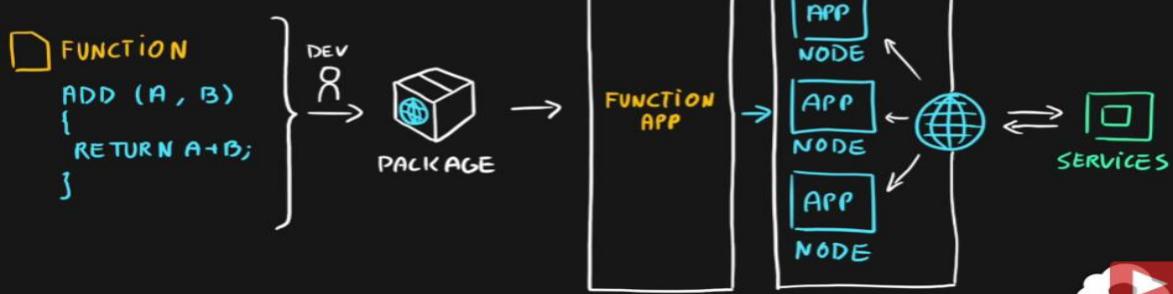


App Service

Key Characteristics

- Designed as enterprise grade web application service
- Platform as a Service
- Supports multiple programming languages and containers

Azure Functions (Function Apps)



Azure Functions (Function Apps)

Key Characteristics

- Platform as a Service
- Serverless
- Two hosting/pricing models
 - Consumption-based plan
 - Dedicated plan
- Designed for micro/nano-services

Azure Compute Services

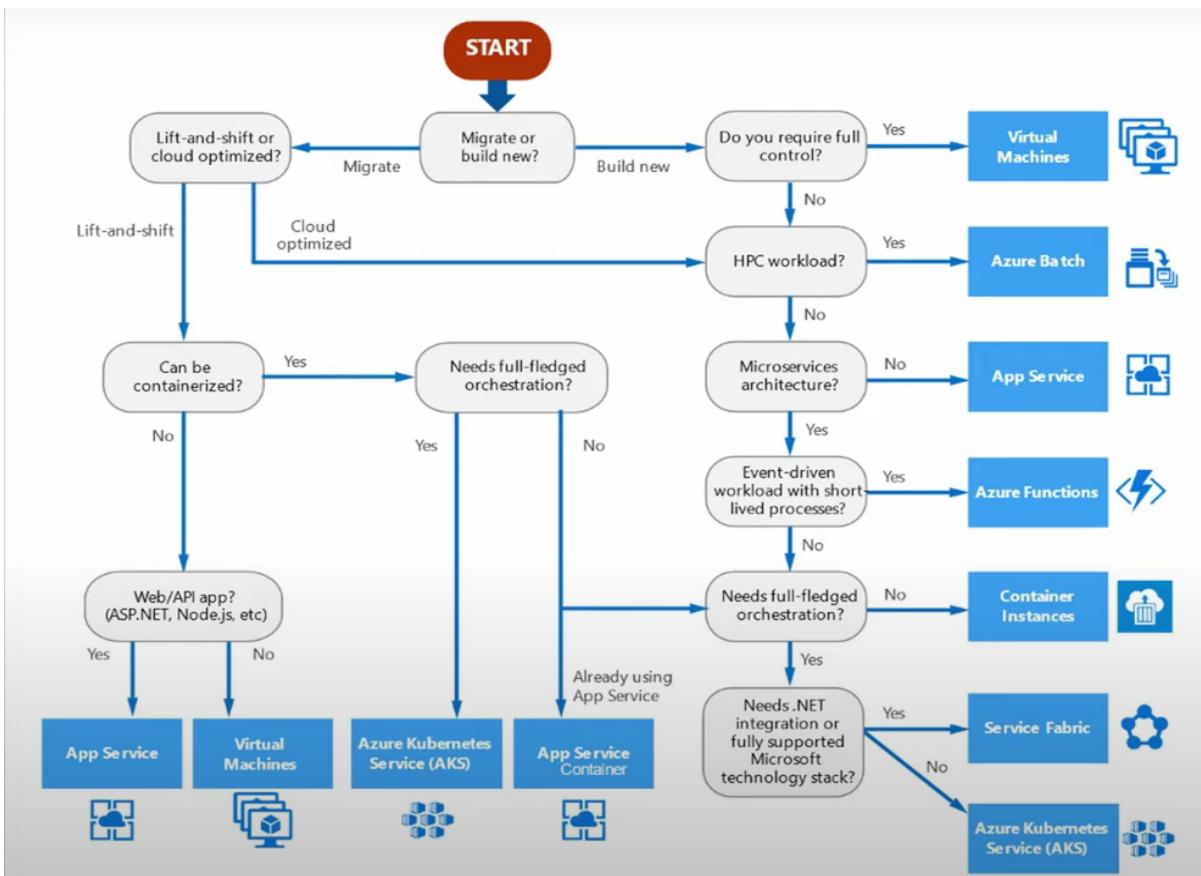
Summary

Service	Configuration Control / Maintenance	Autoscaling	Min Nodes	Max Nodes	Scalability
Virtual Machines	★★★★★	No	1	1	★
VM Scale Sets	★★★★★	Yes	1	1000/600	★★★★★
Container Instances	★★★	No	0	20	★★
Kubernetes Service	★★★★	Yes	3	100	★★★★
App Service	★★	Yes	1	20/100	★★
Functions	★	Yes	0	200	★★★★

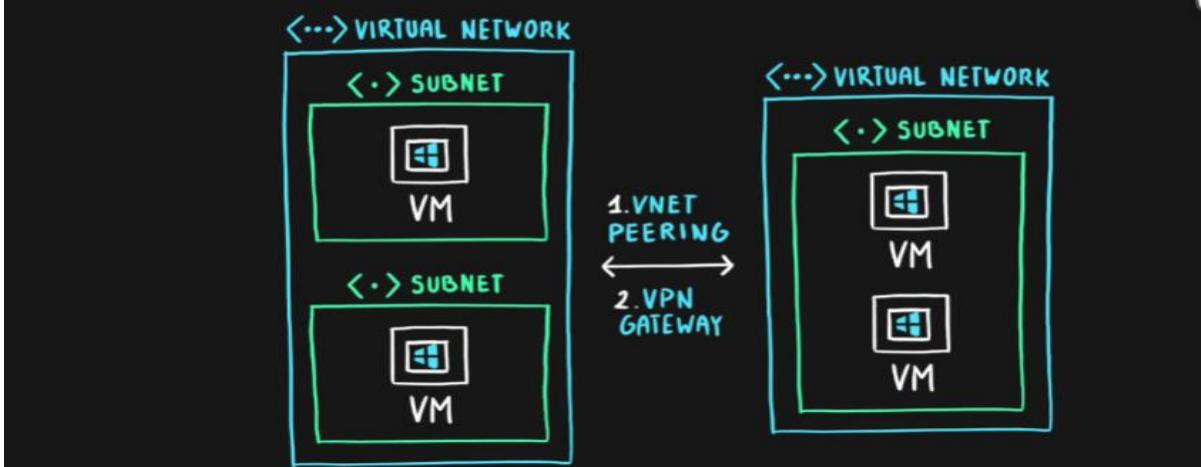
Azure Compute Services

Summary

- **Virtual Machines** (IaaS)
Custom software, custom requirements, very specialized, high degree of control
- **VM Scale Sets** (IaaS)
Auto-scaled workloads for VMs
- **Container Instances** (PaaS)
Simple container hosting, easy to start
- **Kubernetes Service** (PaaS)
Highly scalable and customizable container hosting platform
- **App Services** (PaaS)
Web applications, a lot of enterprise web hosting features, easy to start
- **Functions** (PaaS) (Function as a Service) (Serverless)
micro/nano-services, excellent consumption-based pricing , easy to start



Virtual Network



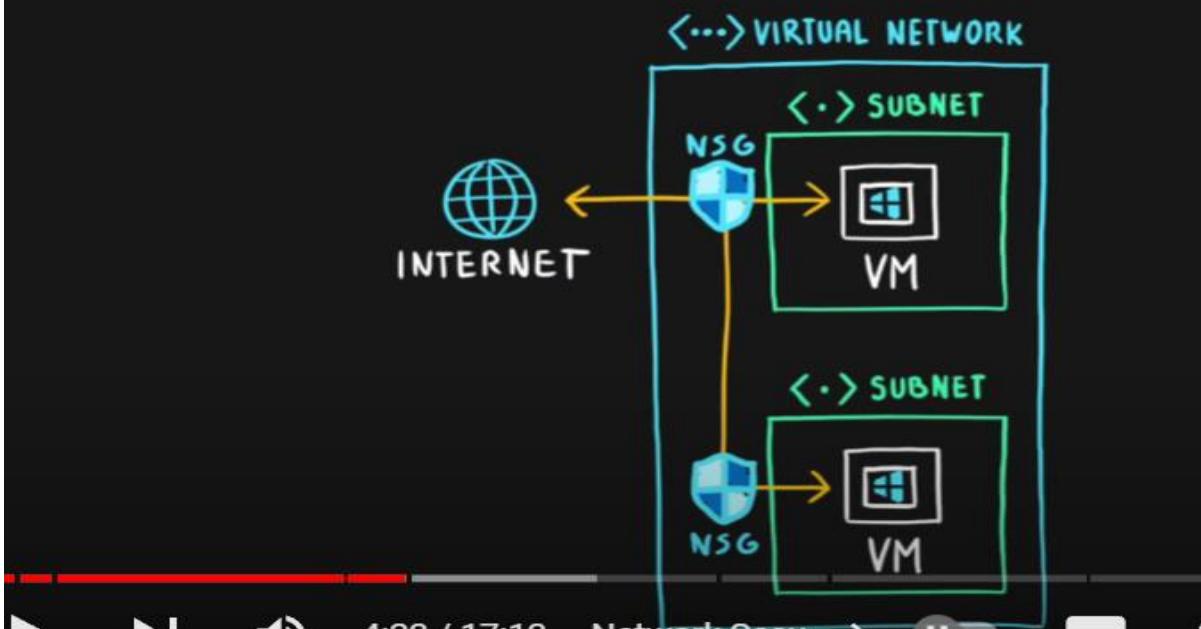
Azure Virtual Network



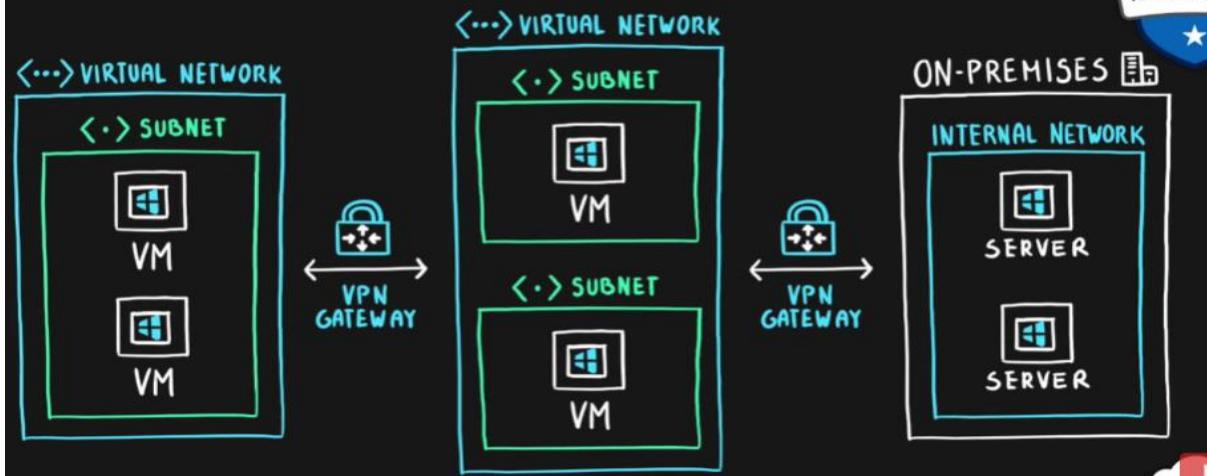
Key Characteristics

- Emulation of physical networking infrastructure
- Designed for **isolation**, **segmentation**, **communication**, **filtering**, **routing** between resources (internet and on-premises)
- Scoped to a single region
- VNet Peering or VPN Gateway allow cross VNet communication
- Segmented into one or more **subnets**
- **Subnets** are discrete sections used for
 - effective **address allocation** and
 - network filtering via **Network Security Groups** (NSG) or **Application Security Groups** (ASG)

Network Security Groups



VPN Gateway

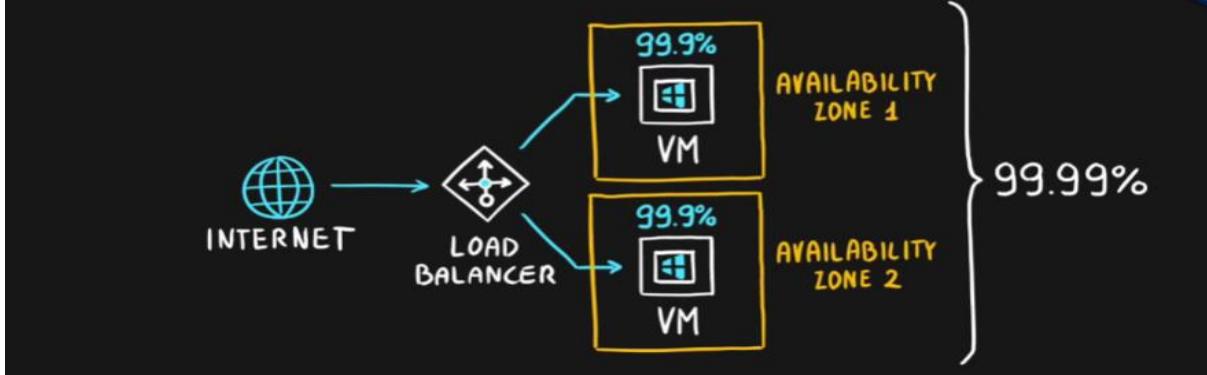


Azure VPN Gateway

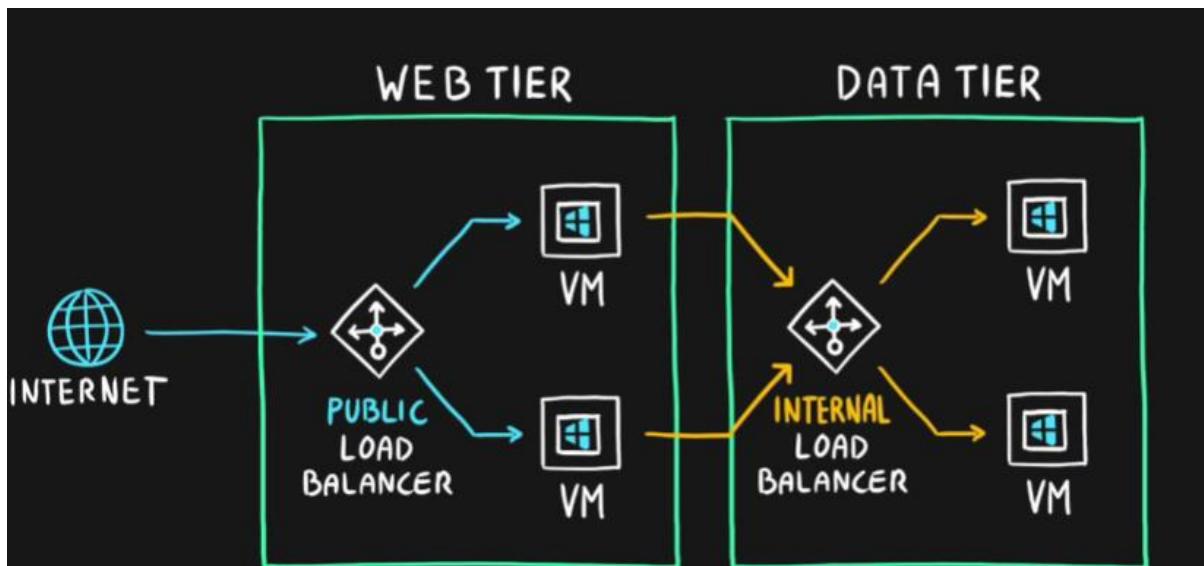
Key Characteristics

- On-premises to azure traffic over the public internet
- Cross-regional communication of azure virtual networks
 - VNet peering vs VPN gateway should be chosen based on the organization needs

Azure Load Balancer



Web tier & data tier



Azure Load Balancer

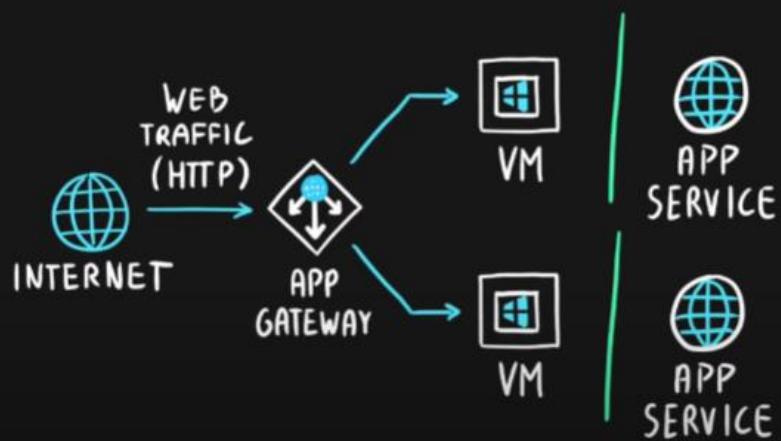


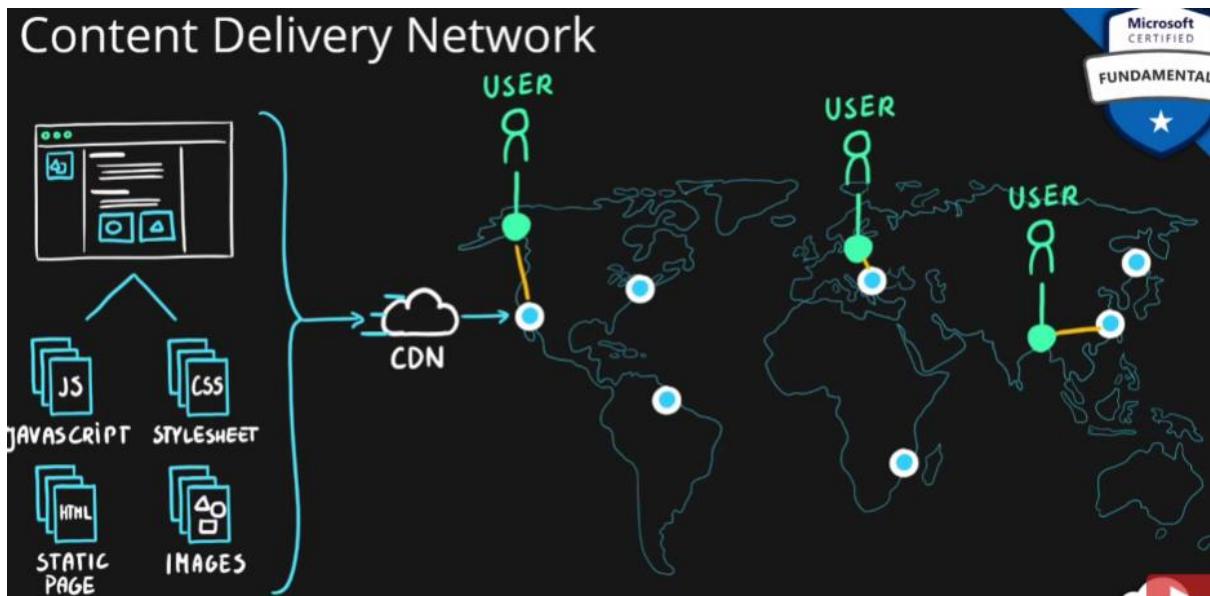
Key Characteristics

- Even traffic distribution
- Supports both inbound and outbound scenarios
- High-availability and scalability scenarios
- Both TCP (transmission control protocol) and UDP (user datagram protocol) applications
- External and internal traffic

Especially web traffic means we can use azure application gateway

Azure Application Gateway





Content Delivery Network

Key Characteristics

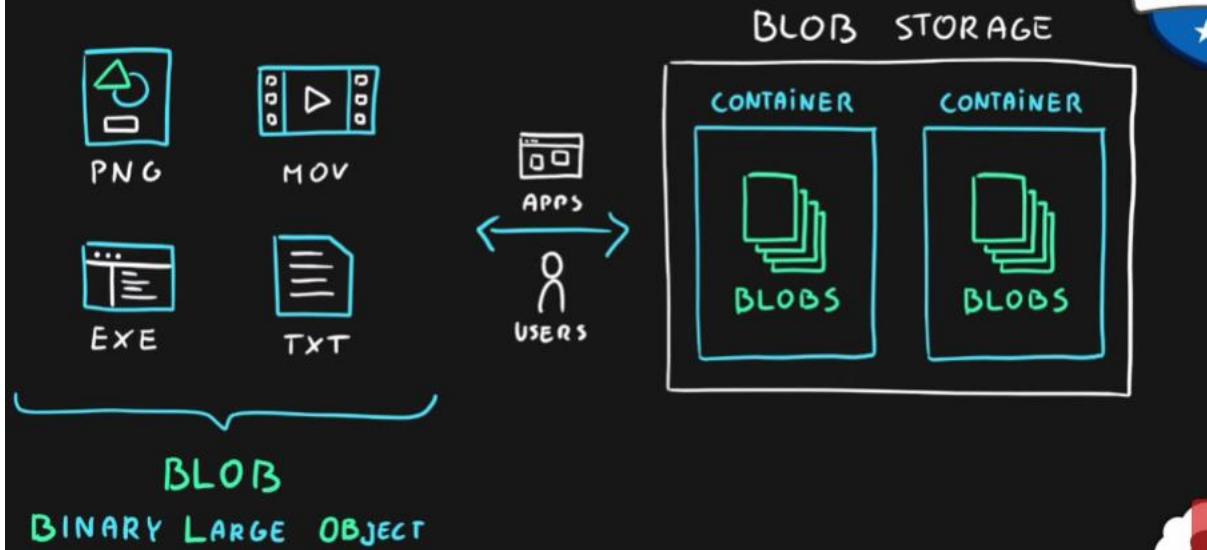
- Deliver web content to users
- Minimize latency
- POP (points of presence) locations

Azure Networking Services

Summary

- Azure [Virtual Network](#) – Emulation/representation of physical networking in the cloud, grouping, filtering and segmentation of network related resources
- Azure [VPN Gateway](#) – Connecting On-Premises with the Virtual Network and Virtual Networks with each other (remember about VNet Peering)
- Azure [Load Balancer](#) – Even traffic distribution for non-HTTP (non-web) traffic
- Azure [Application Gateway](#) – Even traffic distribution for HTTP (web) traffic
- Azure [Content Delivery Network \(CDN\)](#) – Global content caching & distribution to offload web applications and reduce latency

Azure Blob Storage

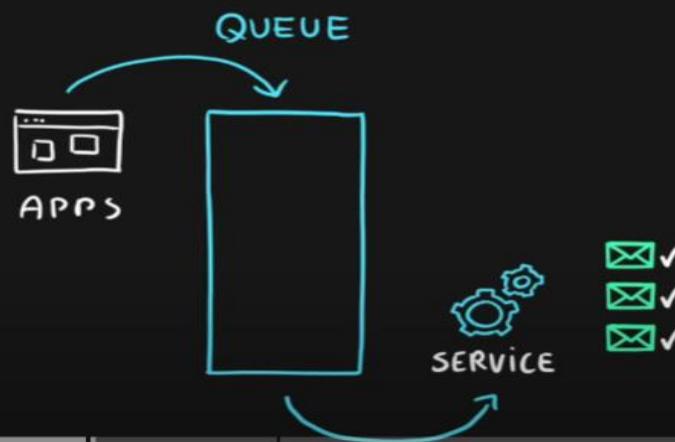


Azure Blob Storage

Key Characteristics

- Designed for storage of files of any kind (BLOB – Binary Large OBject – file)
- Three storage tiers
 - Hot – frequently accessed data
 - Cool – infrequently accessed data (lower availability, high durability)
 - Archive – rarely (if-ever) accessed data

Azure Queue Storage

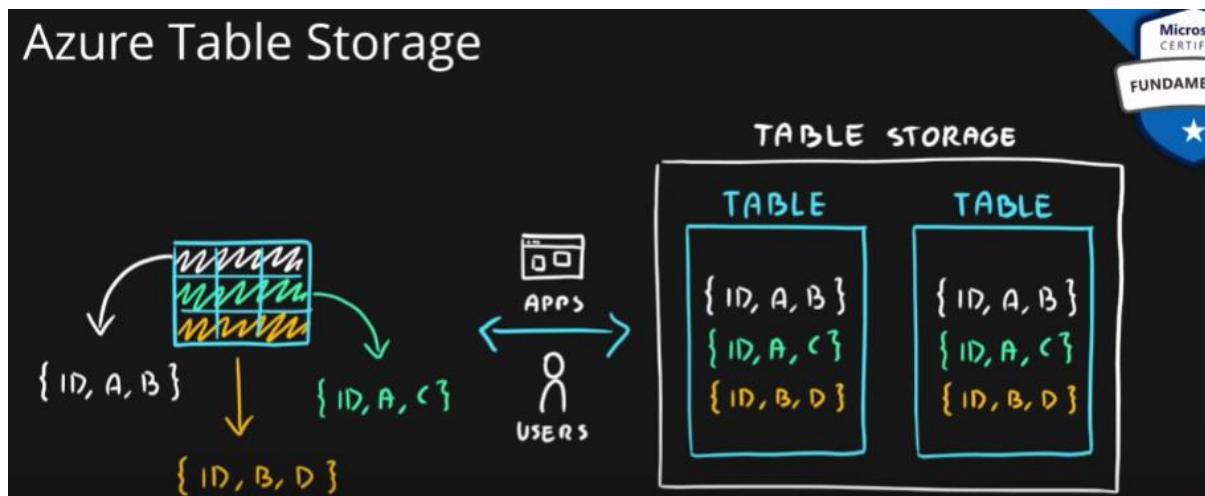


Azure Queue Storage

Key Characteristics

- Storage for small pieces of data (**messages**)
- Designed for **scalable asynchronous processing**

Azure Table Storage



Azure Table Storage

Key Characteristics

- Storage for **semi-structured data (NoSQL)**
 - No need for foreign joins, foreign keys, relationships or strict schema
 - Designed for fast access
- Many programming interfaces and SDKs

Azure File Storage

Key Characteristics

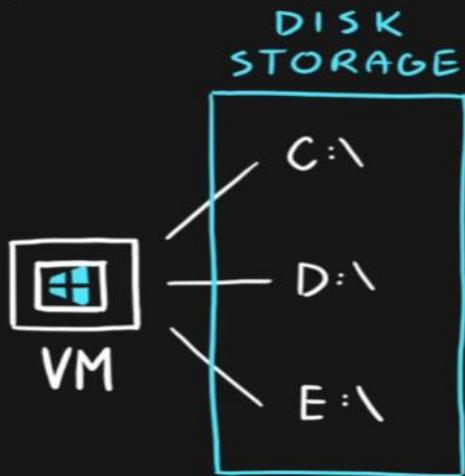
- Storage for **files** accessed via **shared drive** protocols
- Designed to **extend on-premise file shares** or implement **lift-and-shift** scenarios

Azure Storage Account

Key Characteristics

- Group of services which include
 - blob storage,
 - queue storage,
 - table storage, and
 - file storage
- Used to store
 - files,
 - messages, and
 - semi-structured data
- Highly scalable (up to petabytes of data)
- Highly durable (99.99999999% - 11 nines, up to 16 nines)
- Cheapest per GB storage

Azure Disk Storage



Azure Disk Storage

Key Characteristics

- Disk emulation in the cloud
- Persistent storage for Virtual Machines
- Different
 - sizes,
 - types (SSD, HDD)
 - performance tiers
- Disk can be unmanaged or managed



Microsoft Confidential

Azure Storage Services



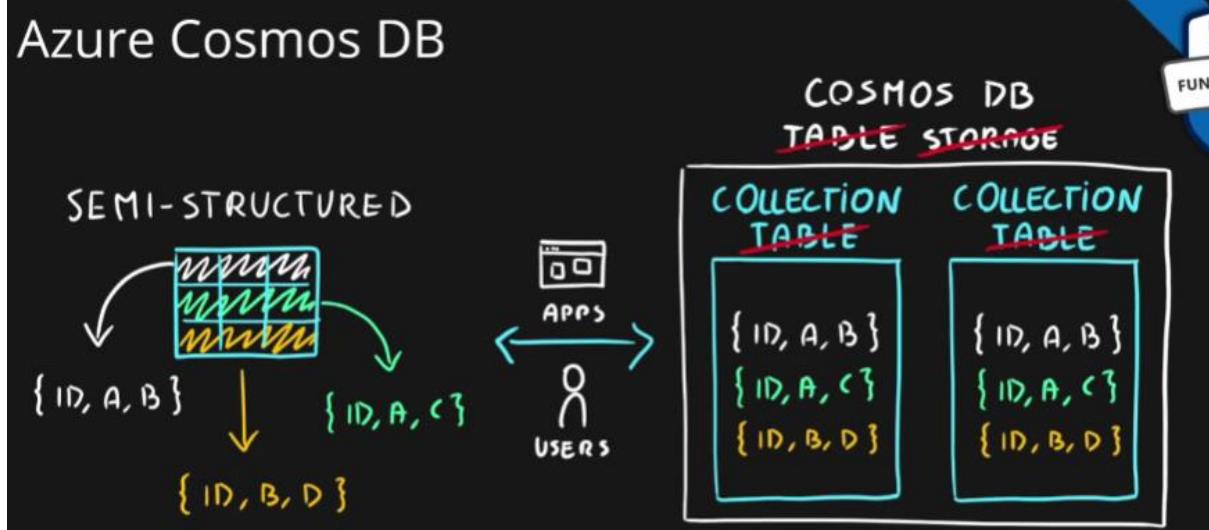
Summary

- Azure **Storage Account** – Highly scalable and highly durable storage service consisting group of smaller services (blob, file, queue and table storage services)
- Azure **Blob Storage** – General purpose (blob) file storage, fits any scenario
- Azure **File Storage** – File share service in the cloud, lift-and-shift scenarios
- Azure **Queue Storage** – Service for storing small messages for asynchronous processing
- Azure **Table Storage** – Scalable NoSQL storage service for semi-structured data
- Azure **Disk Storage** – Disk emulation service in the cloud

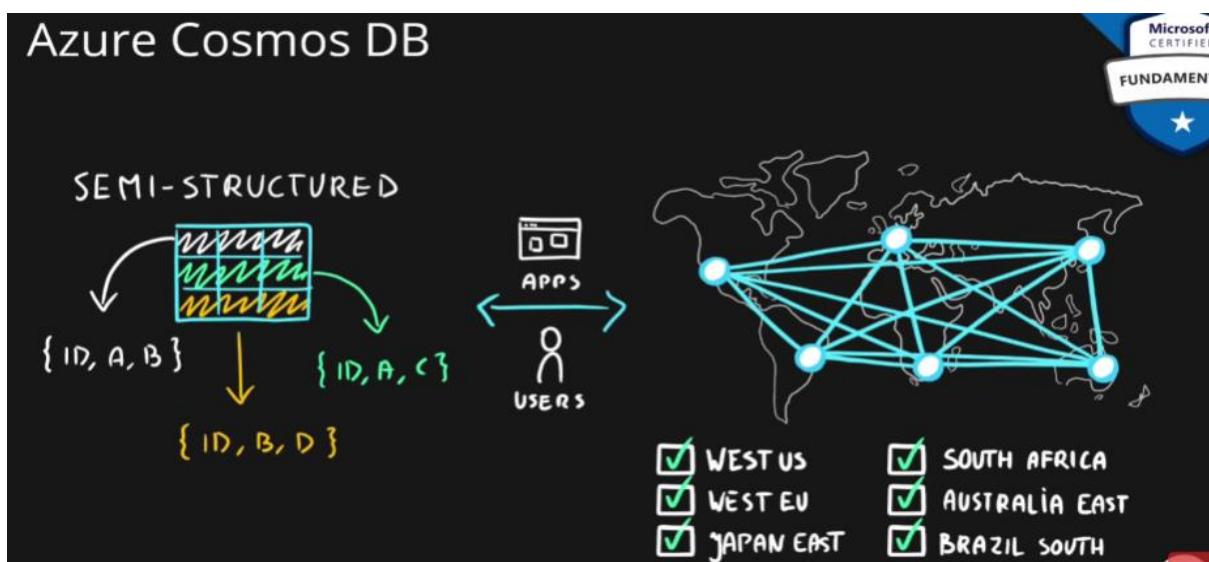
Azure COSMOS-DB:- it is the ability to replicate Geographically

Because it is available in many regions so the data replication is very much easier.

Azure Cosmos DB



Azure Cosmos DB

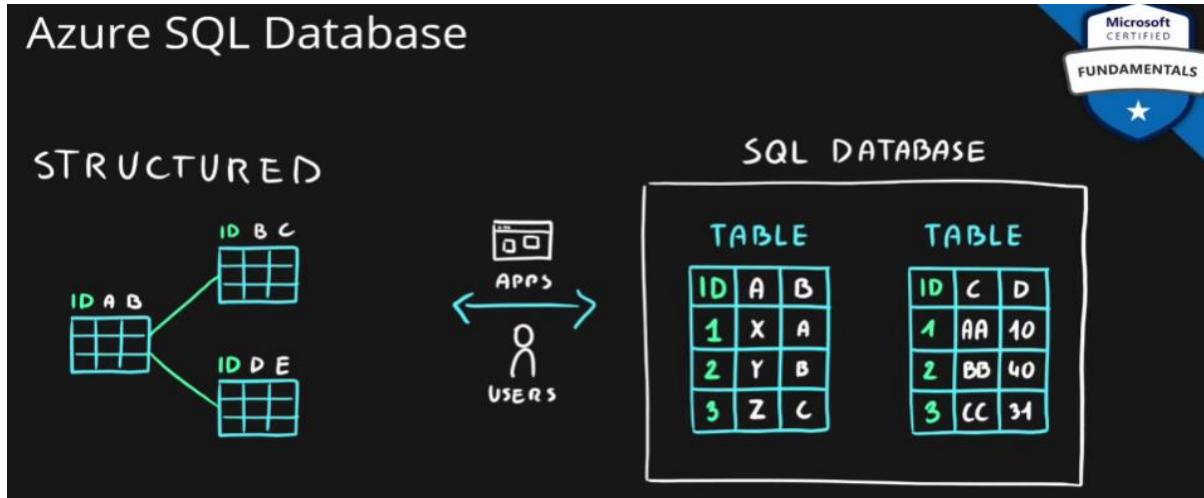


Azure Cosmos DB

Key Characteristics

- Globally distributed NoSQL (semi-structured data) Database service
- Schema-less
- Multiple APIs (SQL, MongoDB, Cassandra, Gremlin, Table Storage)
- Designed for
 - Highly responsive (real time) applications with super low latency responses <10ms
 - Multi-regional applications

Azure SQL Database

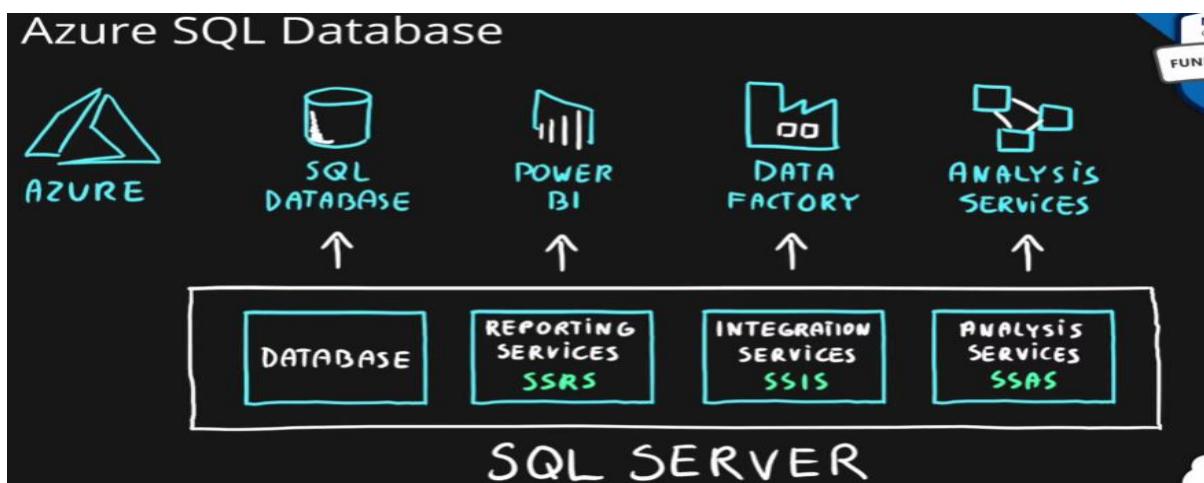


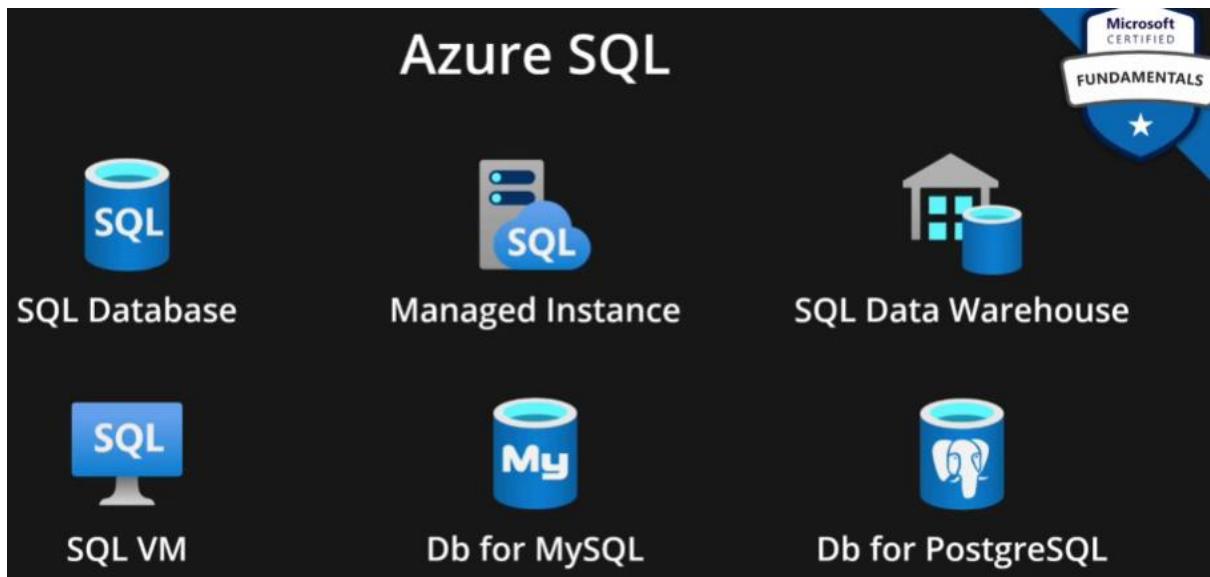
Azure SQL Database

Key Characteristics

- Relational database service in the cloud (PaaS) (DBaaS - Database as a Service)
- Structured data service defined using schema and relationships
- Rich Query Capabilities (SQL)
- High-performance, reliable, fully managed and secure database for building applications

Azure SQL Database





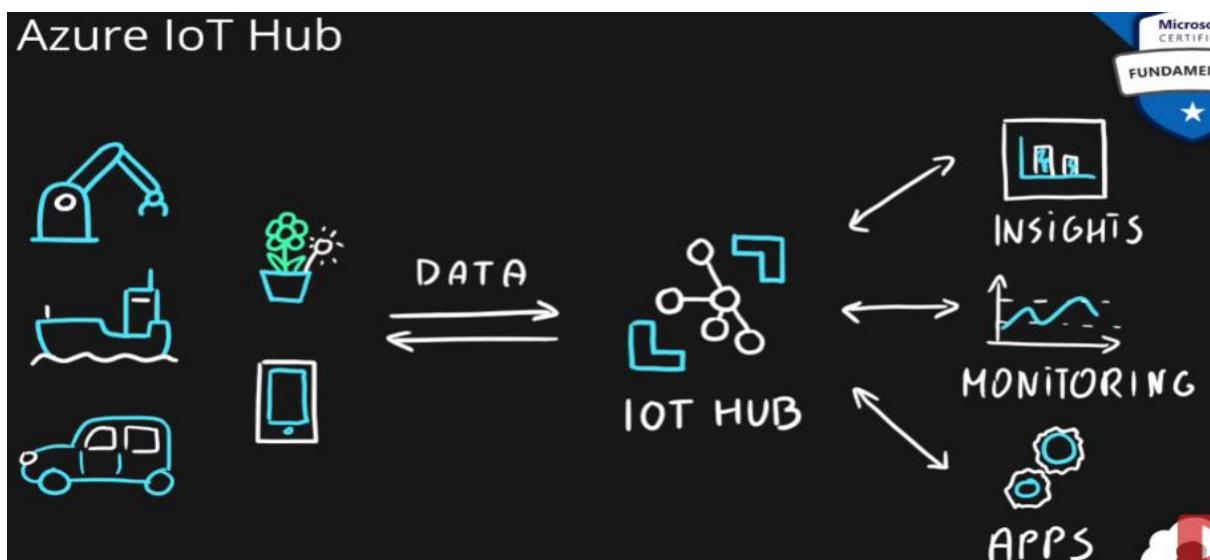
Azure Database Services

Summary

- Azure [Cosmos DB](#) – Globally distributed NoSQL database, low latency, multi-master, perfect for serverless
- Azure [SQL Database](#) – Reliable relational database based on SQL Server
- Azure [Database for MySQL](#) – Azure SQL version for MySQL database engine
- Azure [Database for PostgreSQL](#) – Azure SQL version for PostgreSQL database engine
- Azure [SQL Managed Instance](#) – Fully fledged SQL Server managed by cloud provider
- Azure [SQL on VM](#) – Fully fledged SQL Server on IaaS
- Azure [SQL DW \(Synapse\)](#) – Massively Parallel Processing (MPP) version of SQL Server

IOT Services

Azure IoT Hub



Azure IoT Hub

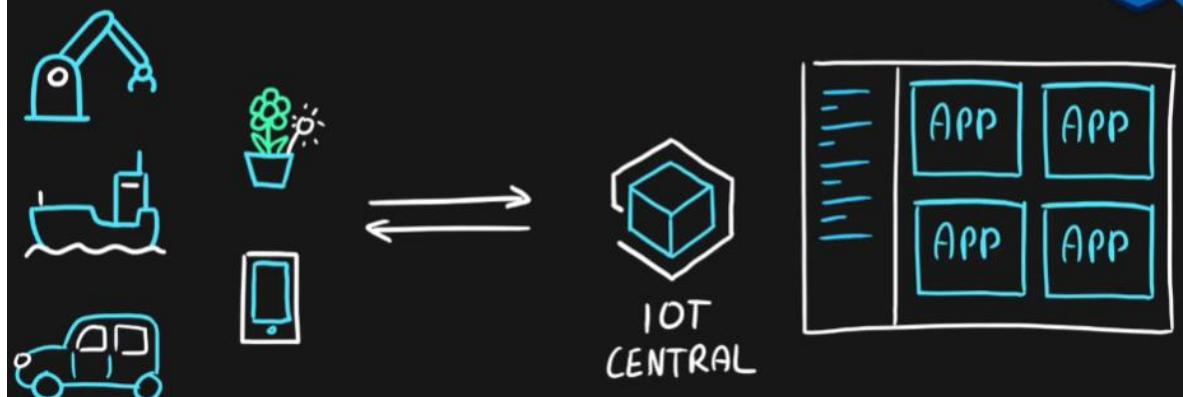


Key Characteristics

- Managed service for **bi-directional communication**
- **Platform as a Service** (PaaS)
- Highly **secure, scalable and reliable**
- Integrates with a lot of Azure Services
- Programmable **SDKs** for popular languages (C, C#, Java, Python, Node.js)
- Multiple protocols (HTTPS, AMQP, MQTT)

Azure IOT Central :- it also helps building application templates.

Azure IoT Central

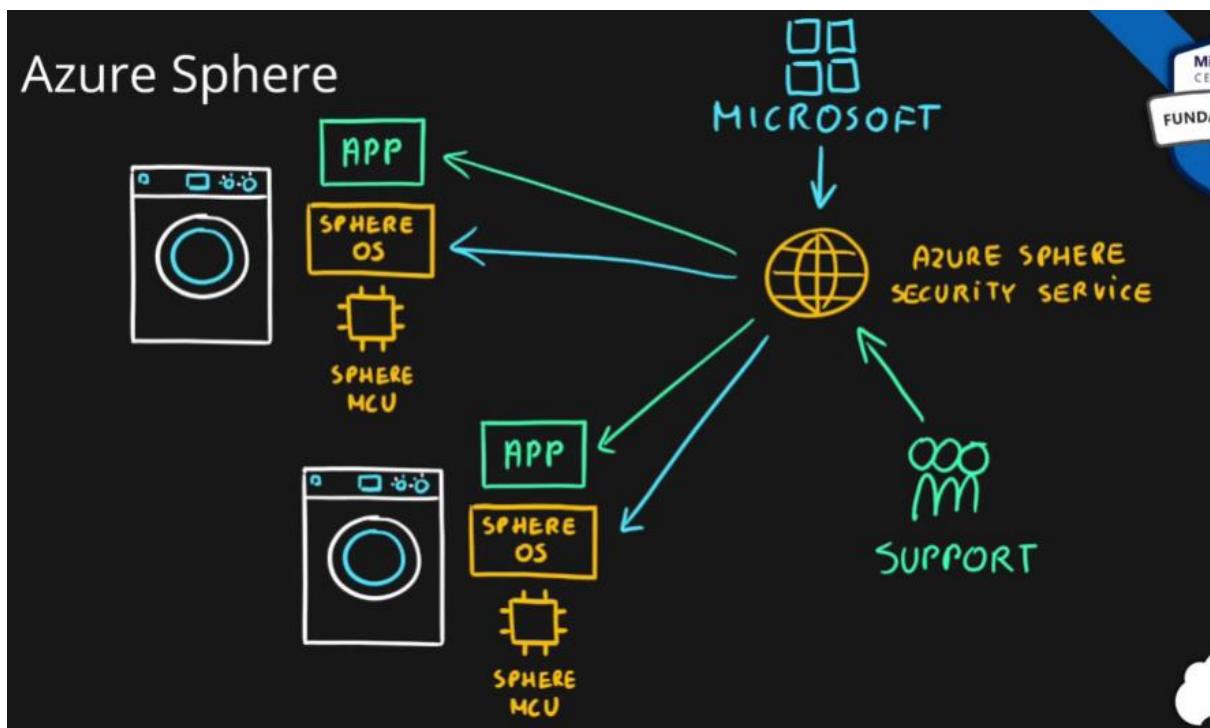


Azure IoT Central



Key Characteristics

- IoT App Platform - Software as a Service (SaaS)
- Industry specific app **templates**
- No deep technical knowledge required
- Service for **connecting, management and monitoring** IoT devices
- Highly **secure, scalable and reliable**
- Built on top of the **IoT Hub** service and 30+ other services



Azure Sphere

Key Characteristics

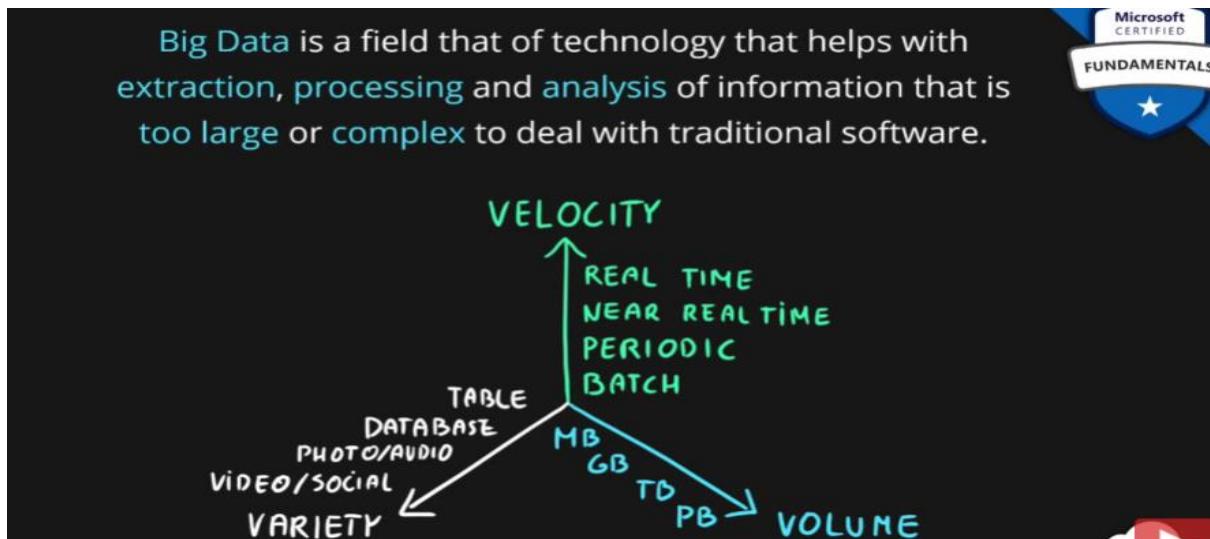
- Secure end-2-end IoT Solutions
 - Azure Sphere certified chips (microcontroller units - MCUs)
 - Azure Sphere OS based on Linux
 - Azure Security Service trusted device-to-cloud communication

Azure IoT Services

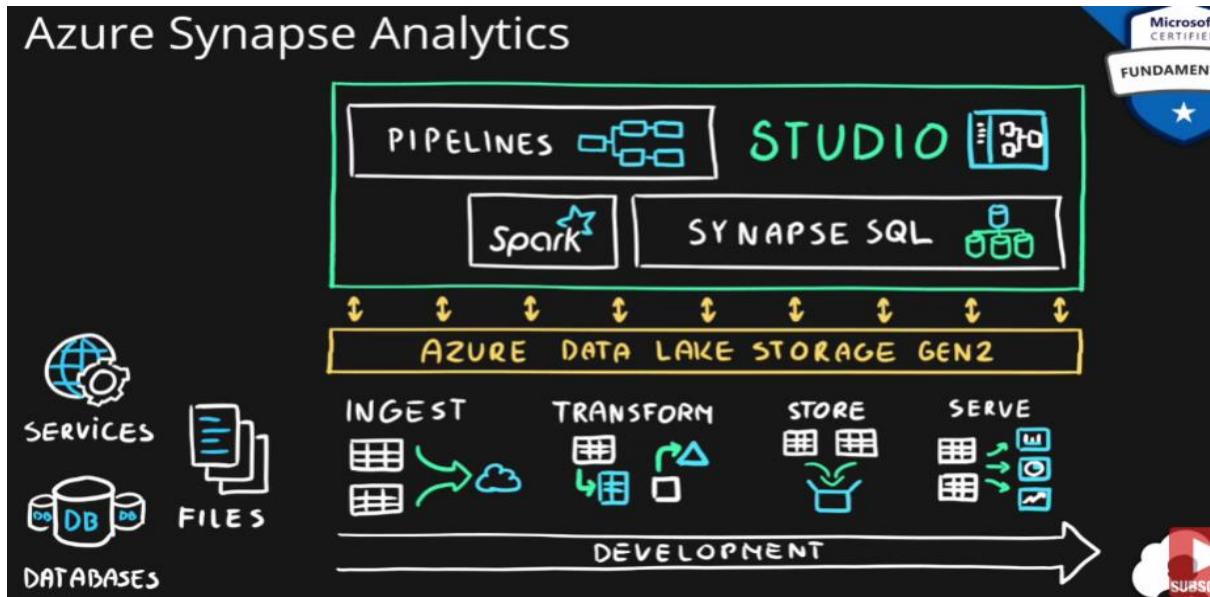
Summary

- IoT Hub - managed service for bi-directional communication with IoT devices, PaaS
- IoT Central - IoT application platform, dozen of functionalities, SaaS
- Azure Sphere - end-2-end approach for building secure IoT solutions

BIG DATA



Azure Synapse Analytics



Azure Synapse Analytics

Key Characteristics

- Big data analytics platform (PaaS)
- Multiple components
 - Spark
 - Synapse SQL
 - SQL pools (dedicated - pay for provisioned performance)
 - SQL on-demand (ad-hoc - pay for TB processed)
 - Synapse Pipelines (Data Factory - ETL)
 - Studio (unified experience)

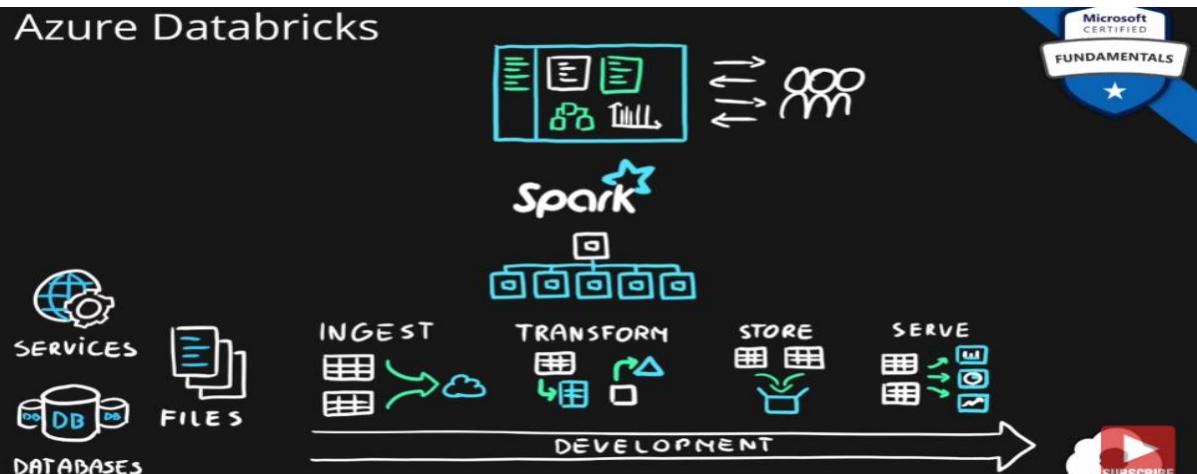


Azure HDInsight

Key Characteristics

- Flexible multi-purpose big data platform (PaaS)
- Multiple technologies supported (Hadoop, Spark, Kafka, HBase, Hive, Storm, Machine Learning)

Azure Databricks



Azure Databricks

Key Characteristics

- Big data collaboration platform (PaaS)
- Unified workspace for notebook, cluster, data, access management and collaboration
- Based on Spark
- Integrates very well with common Azure data services

Azure Big Data & Analytics Services



Summary

- Azure Synapse Analytics – Modern workspace for end-to-end enterprise data warehousing & analytics with a lot of integrated tools like Data Factory, Spark, SQL, etc.
- Azure HDInsight – Fully-managed open source analytics service with a lot of supported frameworks & tools like Hadoop, Spark, Kafka, Hive, etc.
- Azure Databricks – Apache Spark based analytics platform for data transformation and collaborative analytics

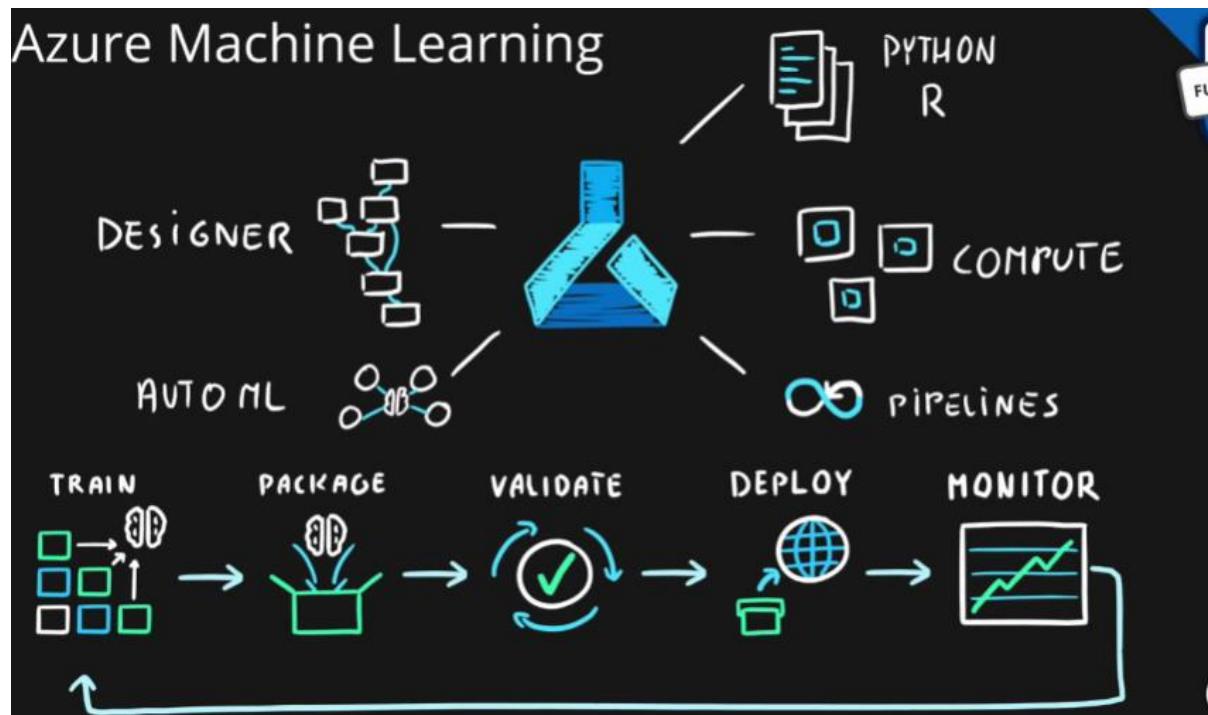
Azure Machine Learning



Key Characteristics

- Cloud-based platform for **creating, managing and publishing** machine learning models
- **Platform as a Service** (PaaS)
- **Machine Learning Workspace** – top level resource
- **Machine Learning Studio** – web portal for end-to-end development
- **Features**
 - Notebooks – using Python and R
 - Automated ML – run multiple algorithms/parameters combinations, choose the best model
 - Designer – graphical interface for no-code development
 - Data & Compute – management of storage and compute resources
 - Pipelines – orchestrate model training, deployment and management tasks

Azure Machine Learning



AZURE Serverless computing services.

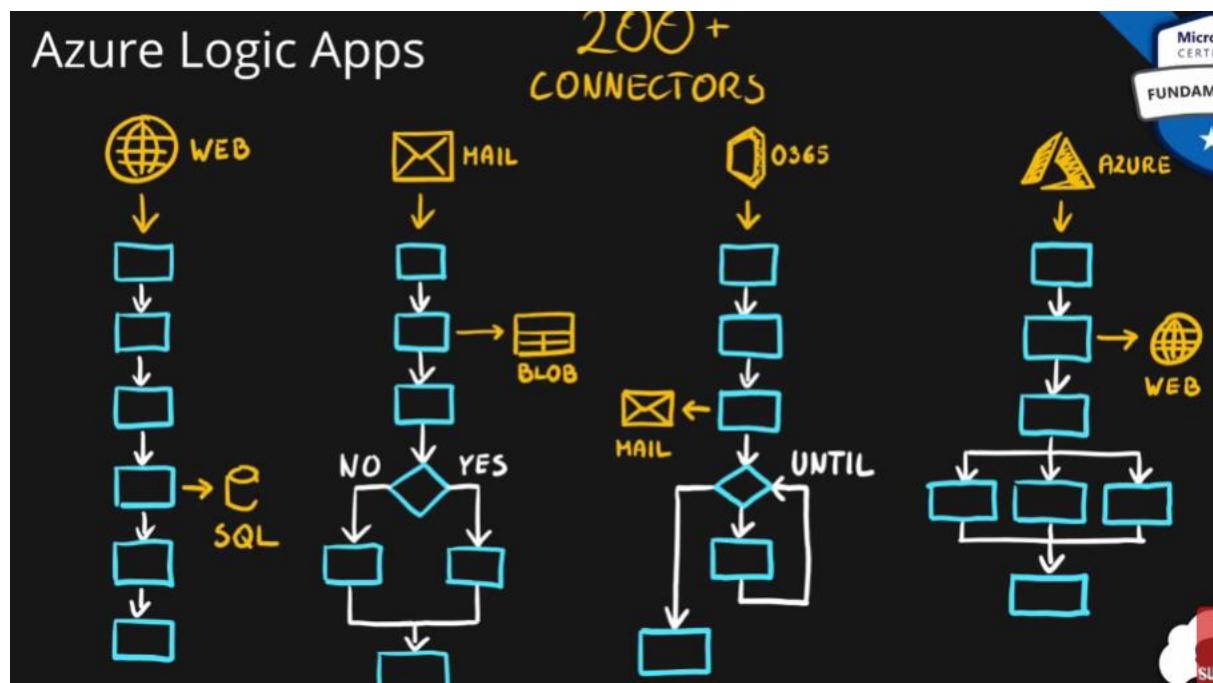
Serverless computing is cloud-hosted execution environment that allows customers to run their applications in the cloud while completely abstracting underlying infrastructure.

Azure Functions

Key Characteristics

- Serverless coding platform (Functions as a Service, FaaS)
- Designed for nano-service architectures and event-based applications
- Scales up and down very quickly
- Highly scalable
- Supports popular languages and frameworks (.NET & .NET Core, Java, Node.js, Python, PowerShell, etc.)

AZURE Logic Apps:- It helps us to build workflows step by step.

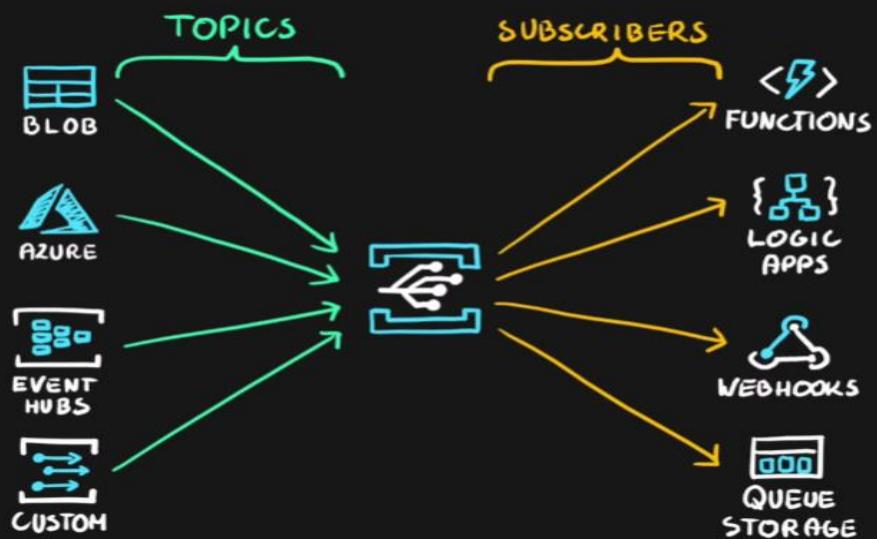


Azure Logic Apps

Key Characteristics

- Serverless enterprise integration service (PaaS)
- 200+ connectors for popular services
- Designed for orchestration of
 - business processes,
 - integration workflows for applications, data, systems and services
- No-code solution

Azure Event Grid



Azure Event Grid

Key Characteristics

- Fully managed serverless event routing service
- Uses publish-subscribe model
- Designed for event-based and near-real time applications
- Supports dozen of built-in events from most common Azure services

Azure Functions – application development platform for nano-services and event-based applications using popular languages/frameworks

Azure Logic Apps – enterprise integration services for orchestration of business and application workflows

Azure Event Grid – scalable event routing service for integration and near-real time applications

DevOps Services

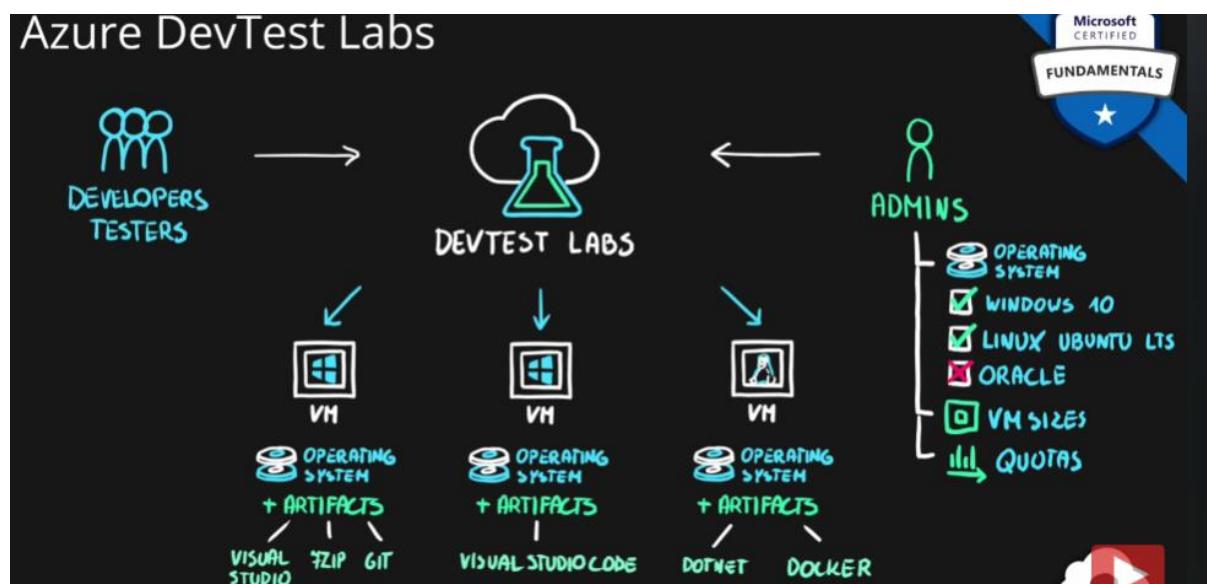


Azure DevOps

Key Characteristics

- Collection of services for building solutions using DevOps practices
- Services included
 - Boards – tracking work
 - Pipelines – building CI/CD workflows (build, test and deploy apps)
 - Repos – code collaboration and versioning with Git
 - Test Plans – manual and exploratory testing
 - Artifacts – manage project deliverables
- Extensible with Marketplace – over 1000 of available apps
- Evolved from TFS (Team Foundation Server), through VSTS (Visual Studio Team Services)

Azure DevTest Labs



Azure DevTest Labs



Key Characteristics

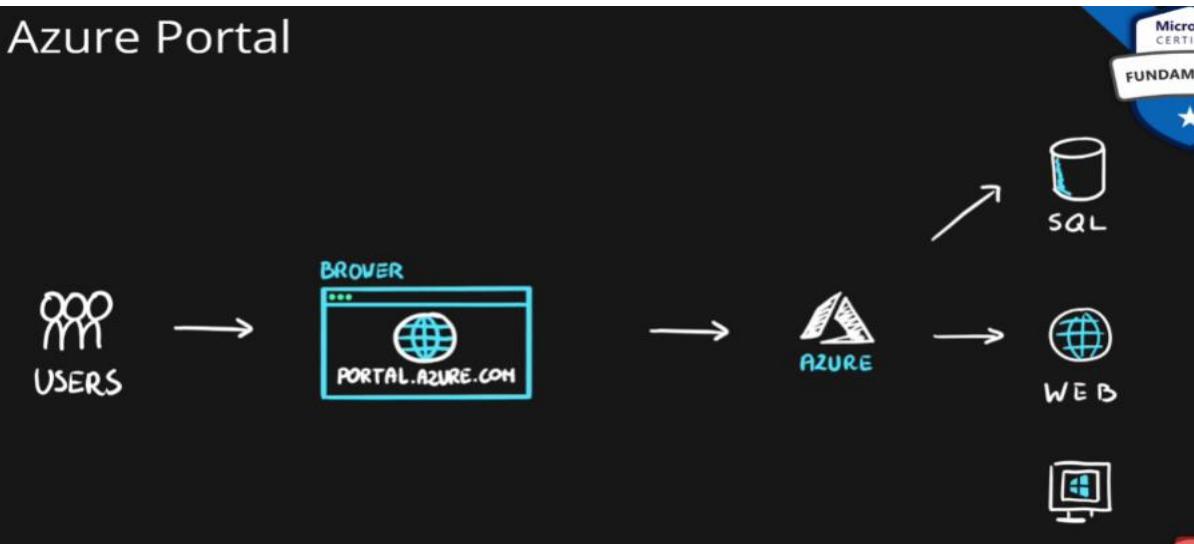
- Service sandbox environment for developers/testers (PaaS)
- Quick setup of self-managed virtual machines
- Preconfigured templates for VMs
- Plenty of additional artifacts (tools, apps, custom actions)
- Lab policies (quotas, sizes, auto-shutdowns)
- Share and automate labs via custom images
- Premade plugins/API/tools for CI/CD pipeline automation

Azure DevOps – end to end platform for building CI/CD pipelines, code versioning, tracking work and managing project deliverables

Azure DevTest Labs – cloud-based environments for developers and testers with self-serve environments, reusable templates, cost management and multiple integrations

Azure Tools

Azure Portal

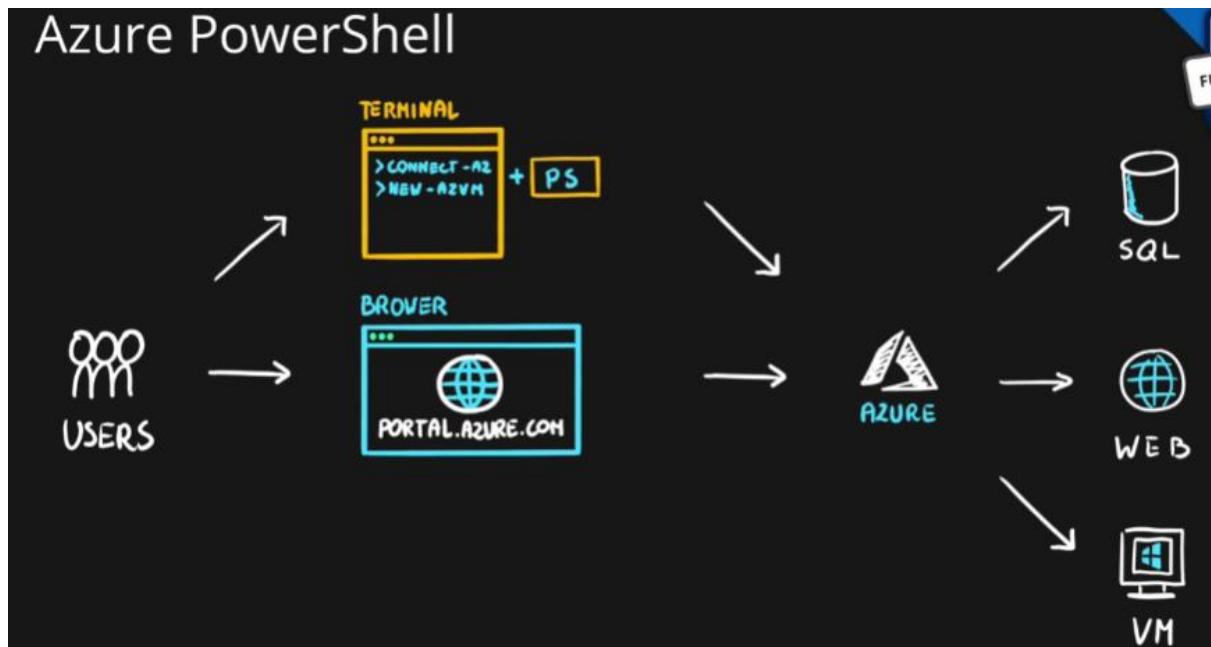


Azure Portal

Key Characteristics

- Public web-based interface for management of Azure platform
- Designed for self-service
- Customizable
- Simple tasks

Azure PowerShell

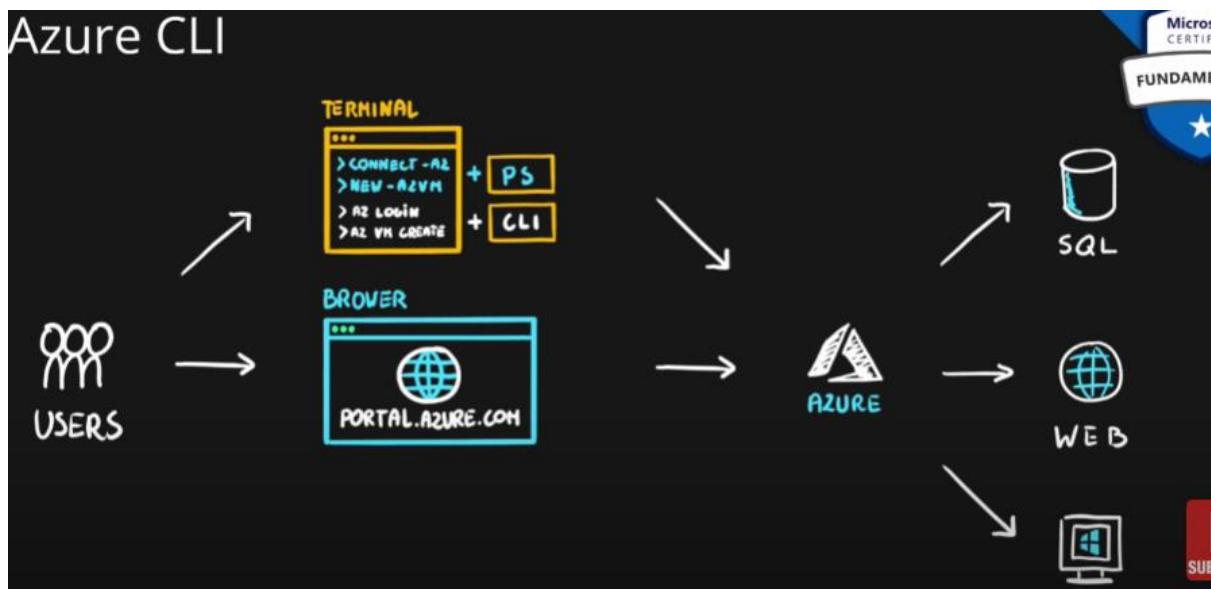


Azure PowerShell

Key Characteristics

- PowerShell and module
- Designed for automation
- Multi-platform with PowerShell Core
- Simple to use
 - Connect-AzAccount – log into Azure
 - Get-AzResourceGroup – list resource groups
 - New-AzResourceGroup – create new resource group
 - New-AzVm – create virtual machine

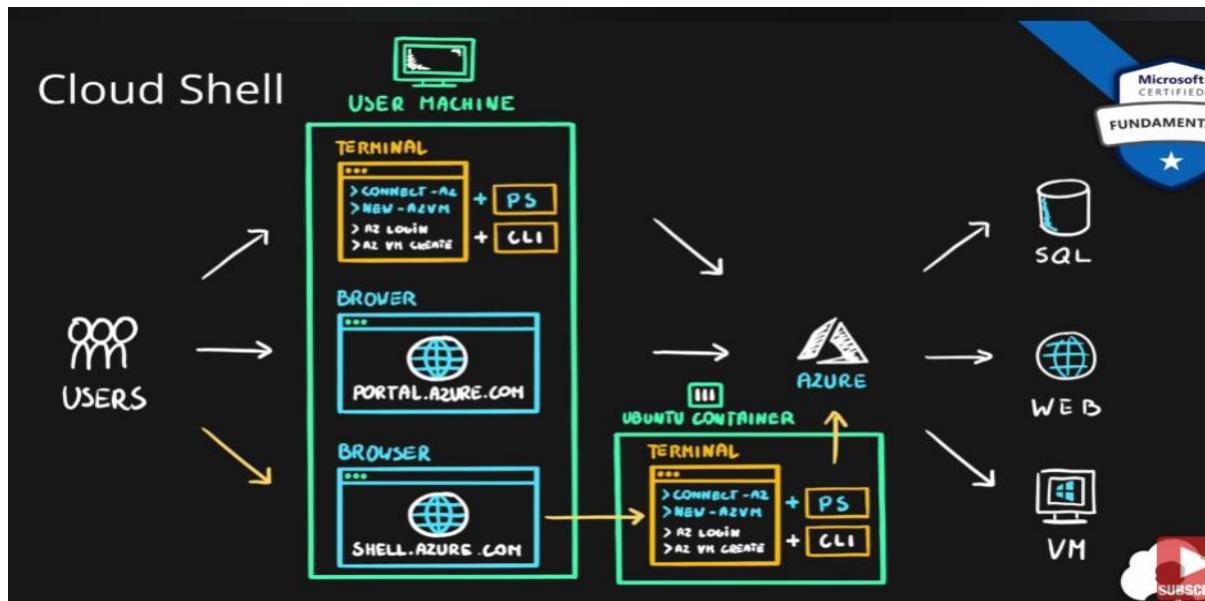
Azure CLI



Azure CLI

Key Characteristics

- Command Line Interface for Azure
- Designed for automation
- Multi-platform (Python)
- Simple to use
 - az login – log into Azure
 - az group list – list resource groups
 - az group create – create new resource group
 - az vm create – create virtual machine
- Native OS terminal scripting



Azure Cloud Shell

Key Characteristics

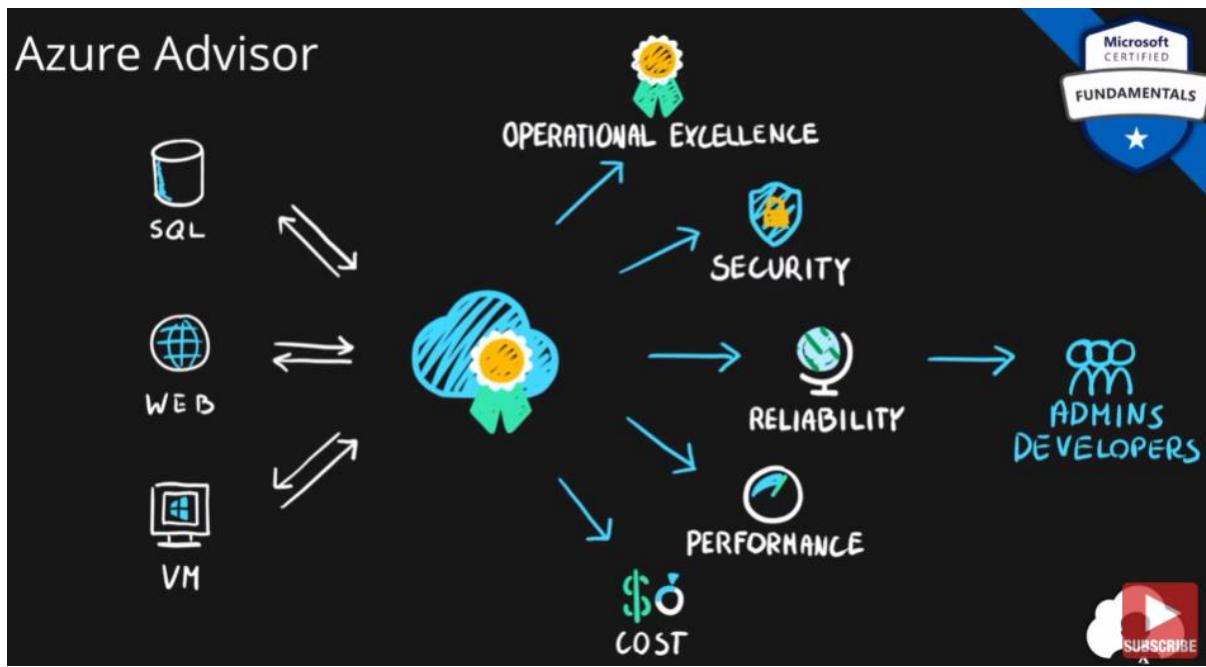
- Cloud-based scripting environment
- Completely free
- Supports both Azure PowerShell and Azure CLI
- Dozen of additional tools
- Multiple client interfaces
 - Azure Portal integration (portal.azure.com)
 - Shell Portal (shell.azure.com)
 - Visual Studio Code Extension
 - Windows Terminal
 - Azure Mobile App
 - Microsoft Docs integration

Azure Portal – Web based portal for self-service management of Azure platform

Azure CLI – automation module for terminal

Azure PowerShell – automation module for PowerShell

Azure Cloud Shell – free cloud-based scripting environment

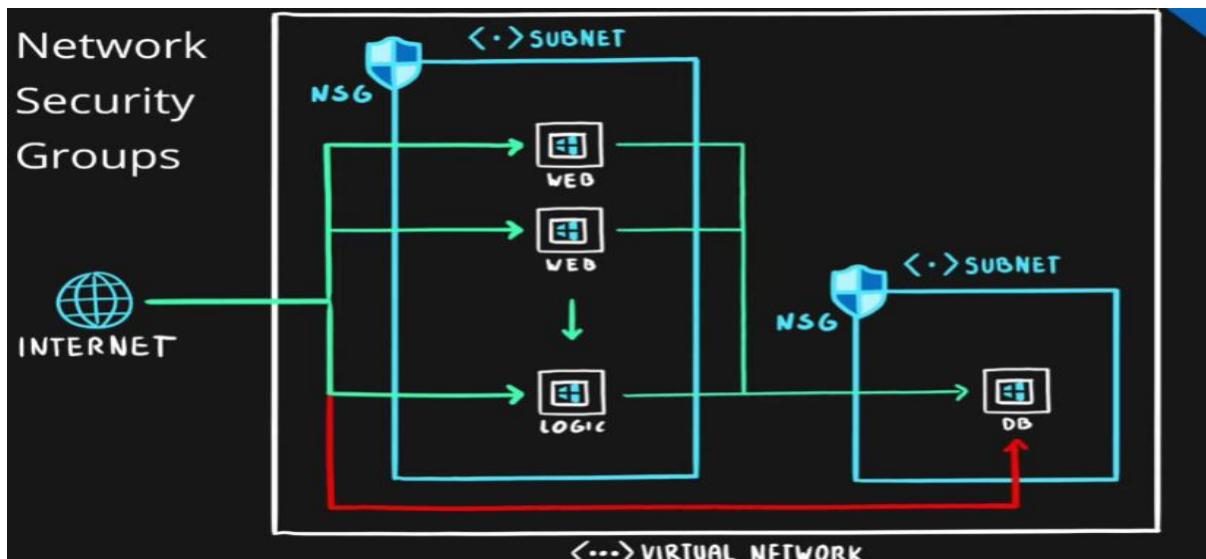


Azure Advisor

Key Characteristics

- Personalized consultant service
- Designed to provide **recommendations** and **best practices** for
 - **Cost** (SKU sizes, idle services, reserved instances, etc.)
 - **Security** (MFA settings, vulnerability settings, agent installations, etc.)
 - **Reliability** (redundancy settings, soft delete on blobs, etc.)
 - **Performance** (SKU sizes, SDK versions, IO throttling, etc.)
 - **Operational Excellence** (service health, subscription limits, etc.)
- Actionable recommendations
- Free!

Network Security Groups.

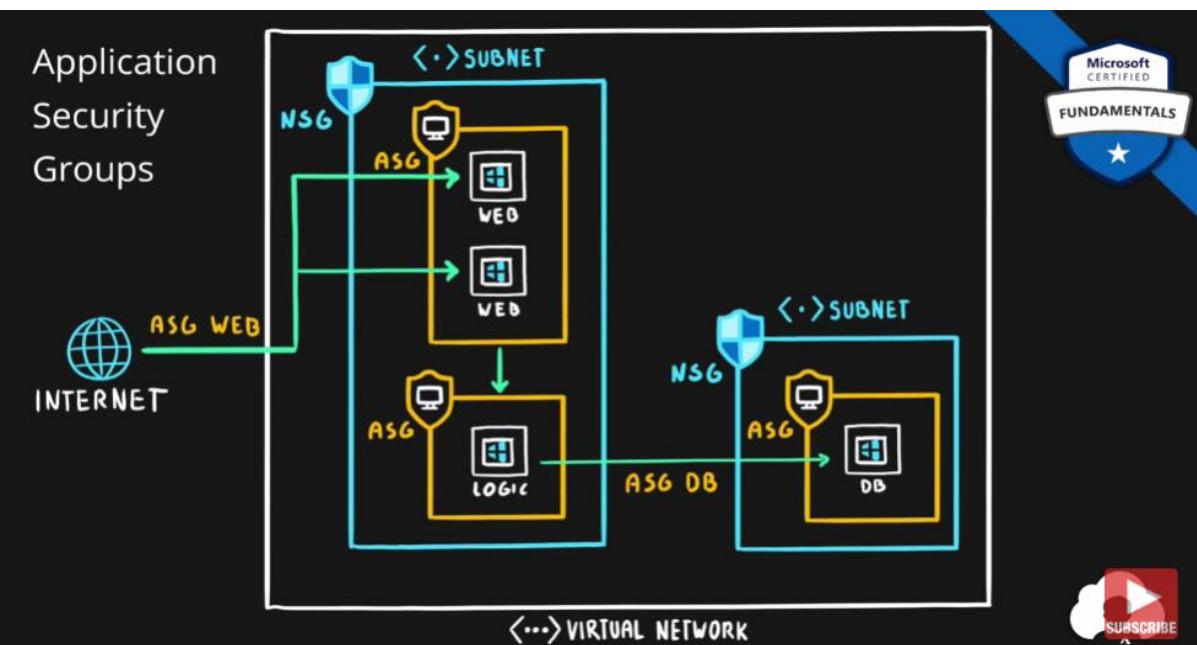


Network Security Groups



Key Characteristics

- Designed to filter traffic to (inbound) and from (outbound) Azure resources located in Azure Virtual Network
- Filtering controlled by rules
- Ability to have multiple inbound and outbound rules
- Rules are created by specifying
 - Source/Destination (IP addresses, service tags, application security groups)
 - Protocol (TCP, UDP, any)
 - Port (or Port Ranges, ex. 3389 – RDP, 22 – SSH, 80 HTTP, 443 HTTPS)
 - Direction (inbound or outbound)



Network Security Groups – Filtering of incoming and outgoing traffic for virtual network resources

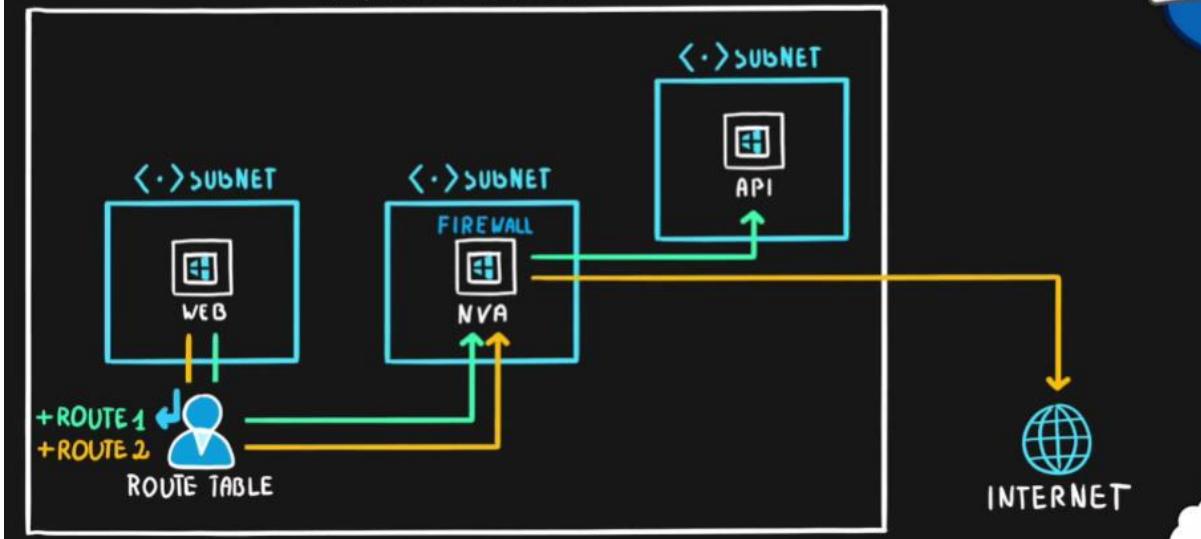
Application Security Groups – Logical grouping of virtual network resources for easier maintenance

Routing

Process of finding/selecting a path for a traffic in one or across multiple networks.

User-defined Routes

<...> VIRTUAL NETWORK



User Defined Routes

Custom (user-defined, static) routes (UDRs)

Designed to override Azure default routing or add new routes

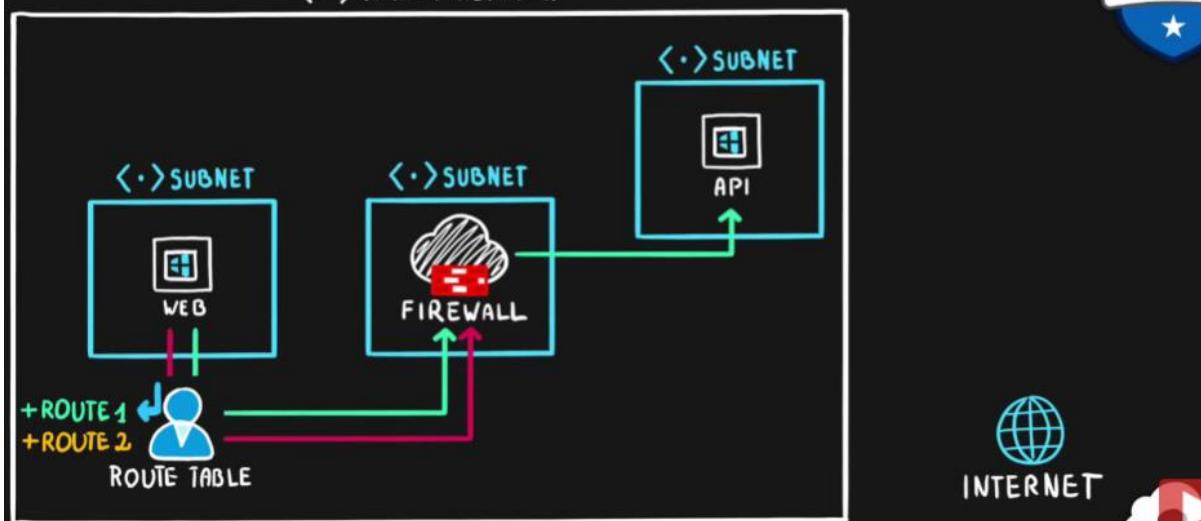
Managed via Azure Route Table resource

Associated with a zero or more Virtual Network subnets

Firewall is a network security service that monitors and controls incoming and outgoing traffic.

Azure Firewall

<...> VIRTUAL NETWORK



Azure Firewall

Key Characteristics

- Managed, cloud-based firewall service (PaaS, Firewall as a Service)
- Built-in high availability
- Highly Scalable
- Inbound & outbound traffic filtering rules
- Support for FQDN (Fully Qualified Domain Name), ex. microsoft.com
- Fully integrated with Azure monitor for logging and analytics

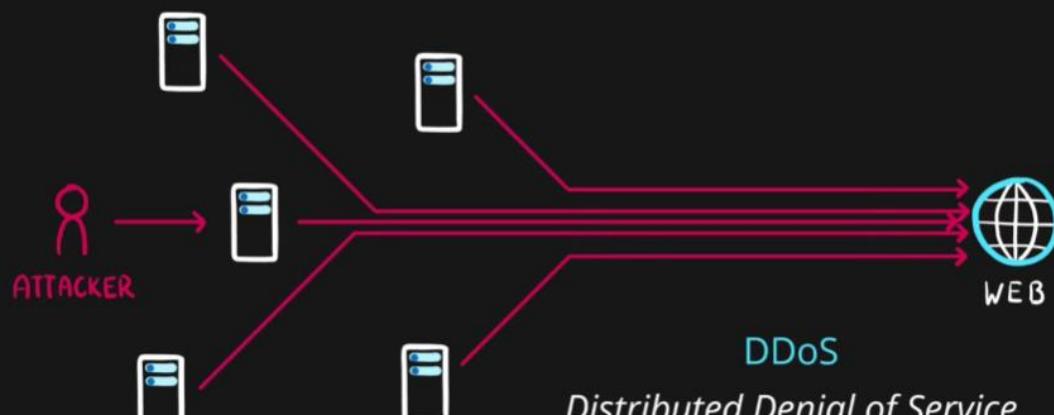
What is DoS?

DoS - Denial of Service

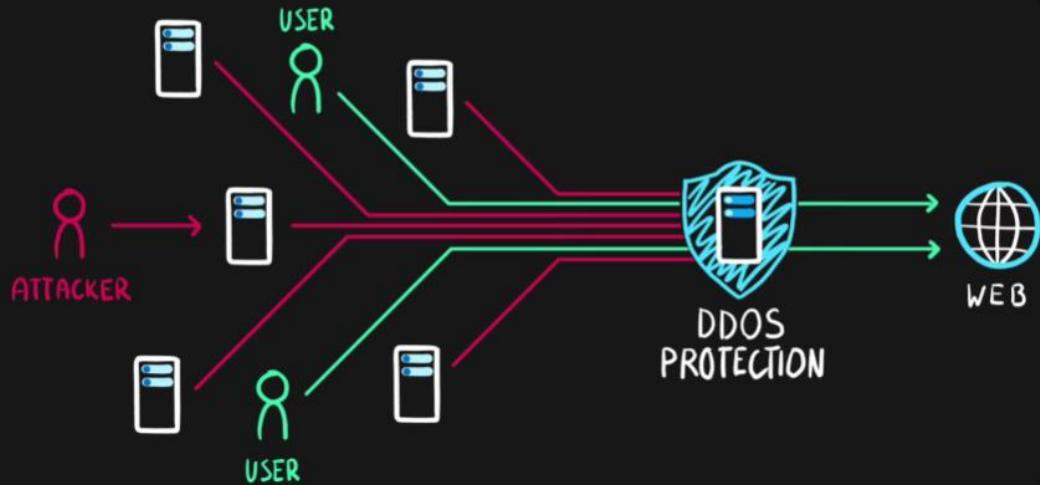
Cyber-attack with intent to cause temporary or indefinite disruption of service



What is DDoS?



What is DDoS?



DDoS Protection



Key Characteristics

- DDoS protection service in Azure
- Designed to
 - Detect malicious traffic and block it while allowing legitimate users to connect
 - Prevent additional costs for auto-scaling environments
- Two tiers
 - Basic – automatically enabled for Azure platform
 - Standard – additional mitigation & monitoring capabilities for Azure Virtual Network resources
- Standard tier uses machine learning to [analyze traffic patterns](#) for better accuracy

IAM-Active Directories.

Identity

The fact of being something or someone.

A user with a username and password.

Also applications or other servers with secret keys or certificates.

ADAM

LISA

TOM

APP

SERVER

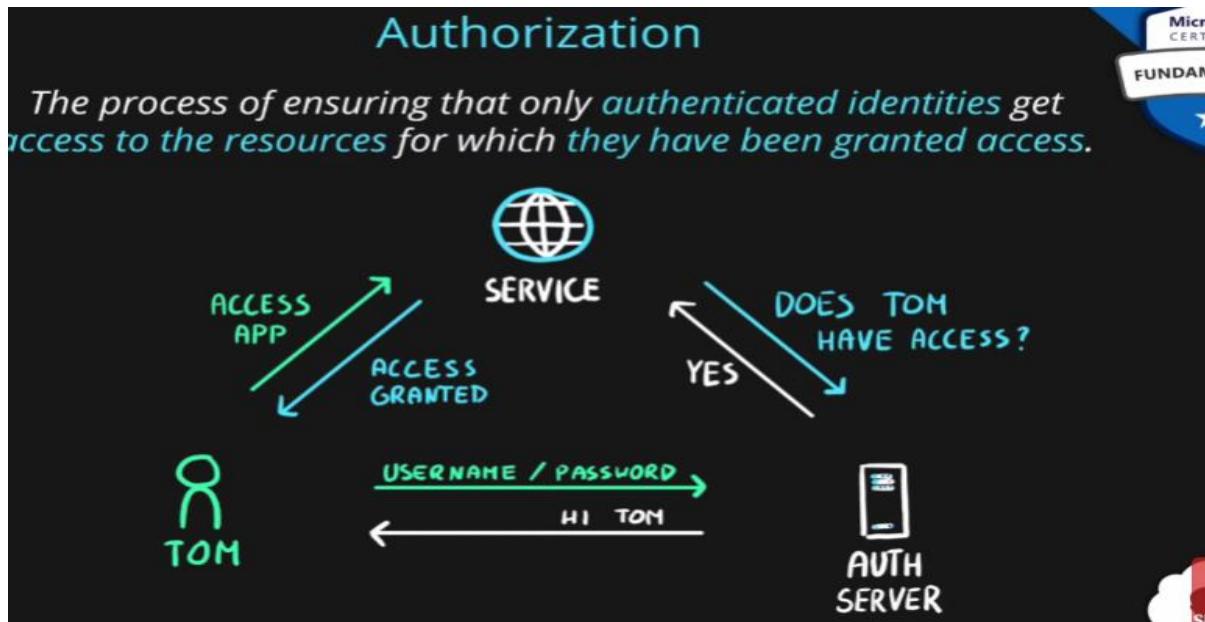
Authentication

The process of verification/assertion of identity



Authorization

The process of ensuring that only authenticated identities get access to the resources for which they have been granted access.

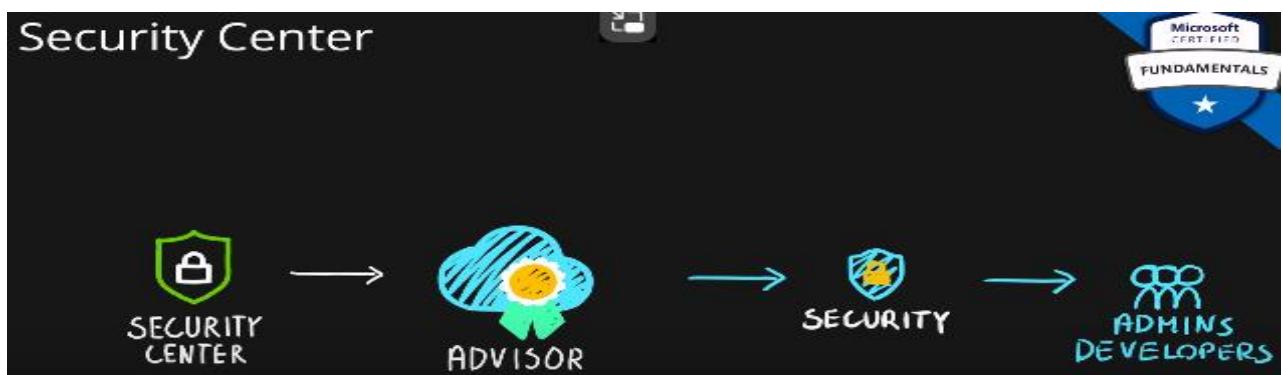
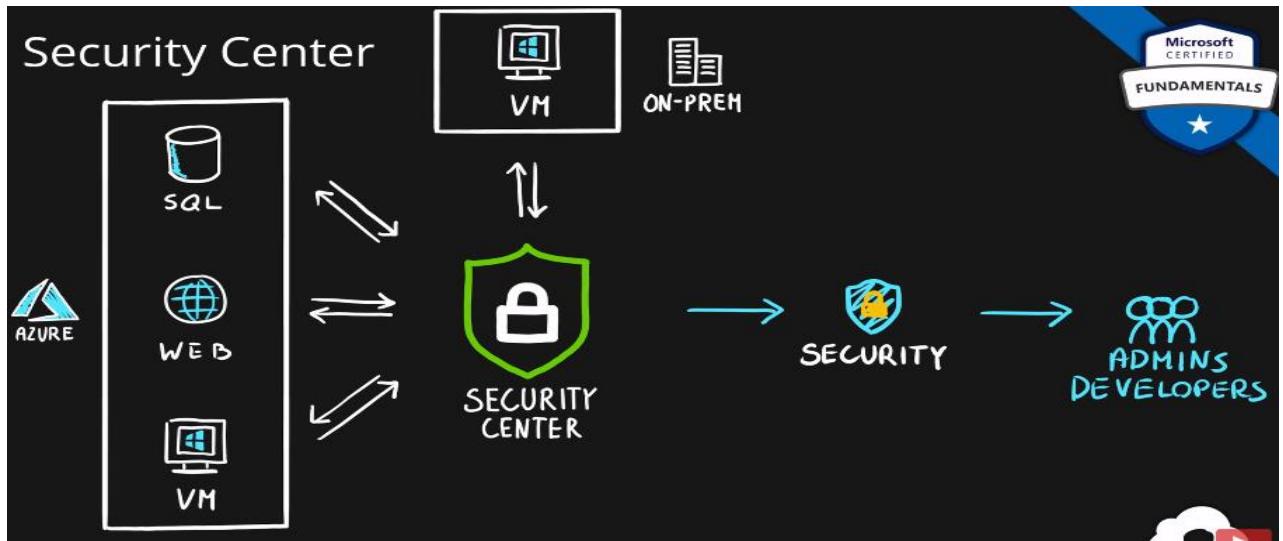


Azure Active Directory

Key Characteristics

- Identity and Access Management service in Azure
- Identities management – users, groups, applications
- Access management – subscriptions, resource groups, roles, role assignments, authentication & authorization settings, etc.
- Used by multiple Microsoft cloud platforms
 - Azure
 - Microsoft 365
 - Office 365
 - Live.com services (Skype, OneDrive, etc.)
- Syncs with on-premises Active Directory via sync services

Security Center: - It continuously scans your services & resources for threat protection & gives recommendations on them & also installs agents on ONPREMISE to extend the functionality of its security services.

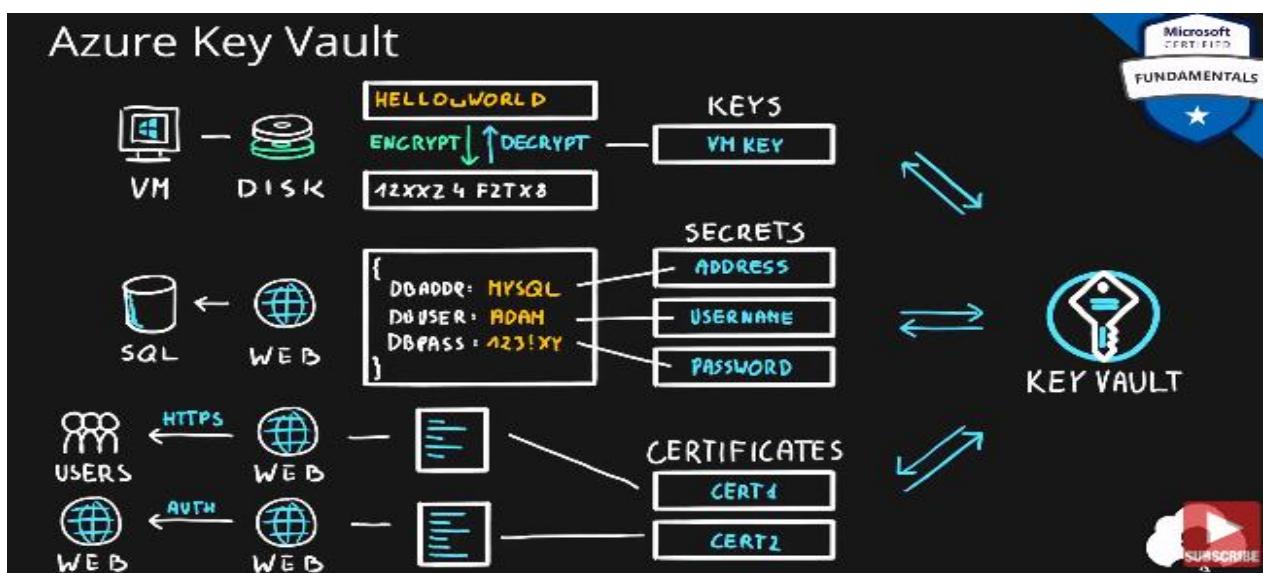


A secure score will show us how secure the environment is.



Certificates:- They are complex forms of cryptography, used to encrypt the requests which go to users & as well certificates can be used to Authentication of outgoing web server requests.

Azure Key Vault

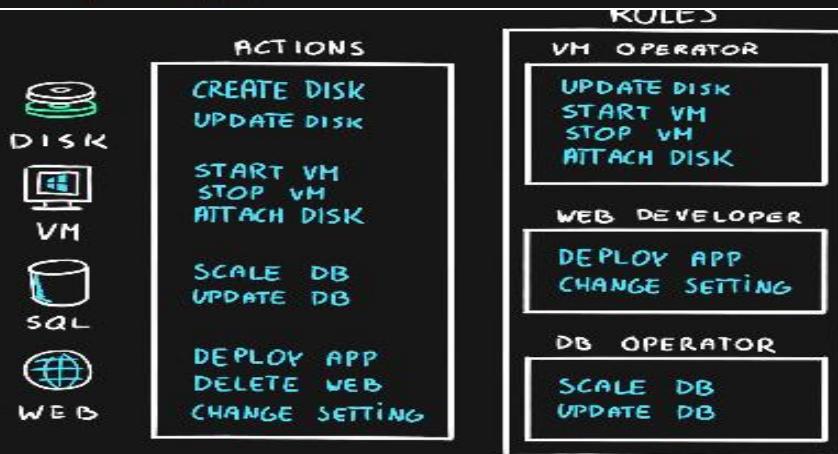


Azure Key Vault

Key Characteristics

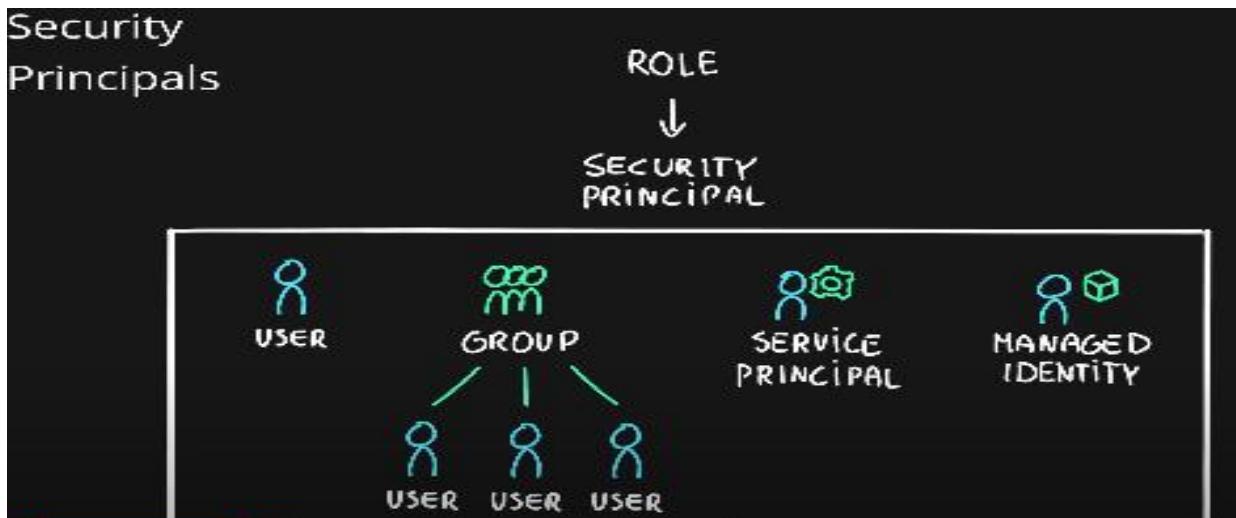
- Managed service for **securing sensitive information** (application/platform) (PaaS)
- Secure storage service for
 - Keys,
 - Secrets and
 - Certificates
- Highly integrated with other Azure services (VMs, Logic Apps, Data Factory, Web Apps, etc.)
- Centralization
- Access monitoring and logging

Roles

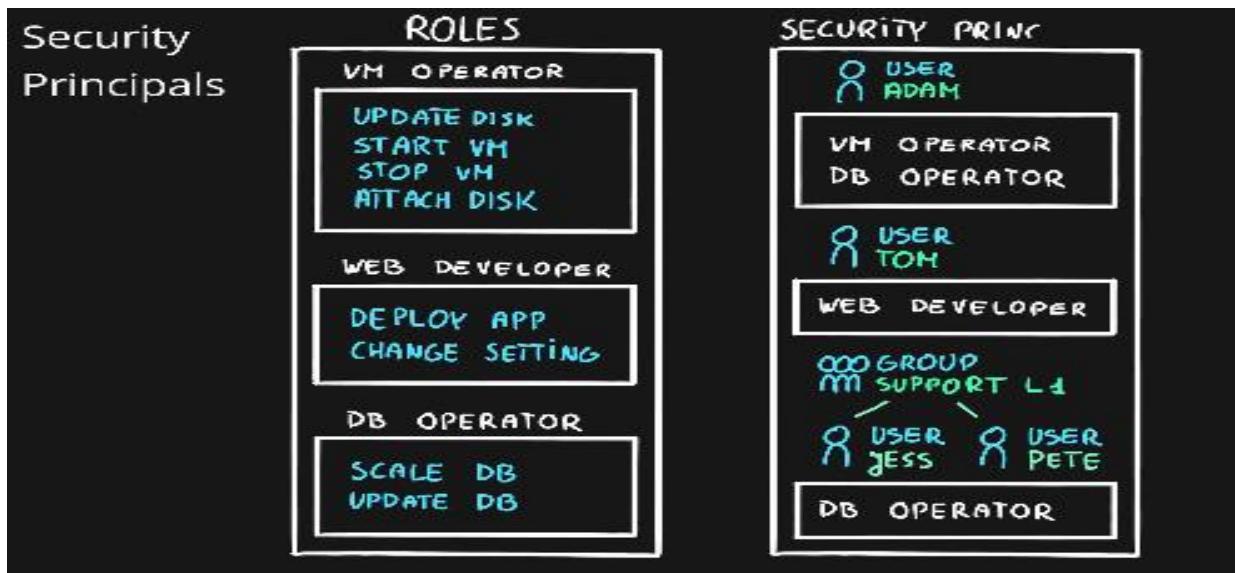


Roles: - Collections of actions that the assigned identity will be able to perform. We can give multiple roles to a single user or groups.

Security Principles



Security Principles



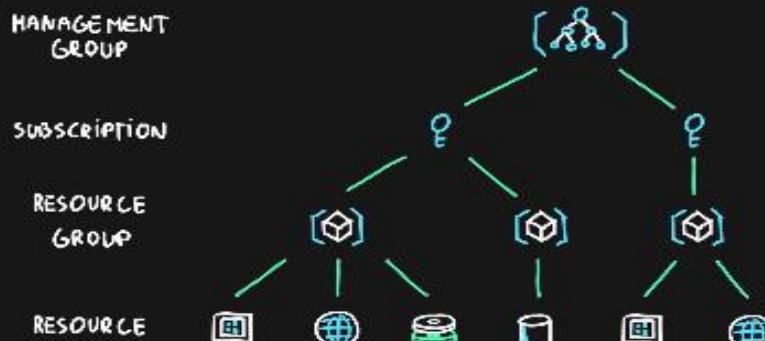
Security Principal is an Azure object(identity) that can be assigned to a role. (ex: users, groups or applications).

Security principles assignment will tell who can do it or who can access the resources.

Scope: - Access applying to one or more azure resources.

Scopes

ROLE
↓
SCOPE



"What can be done?"

OWNER - EVERYTHING

"Who can do it?"

USER - ADAM

"Where can it be done?"

VM RESOURCE - DEV-VM

Role assignment is a combination of the role definition, security principal and scope

Role-Based Access Control (RBAC)

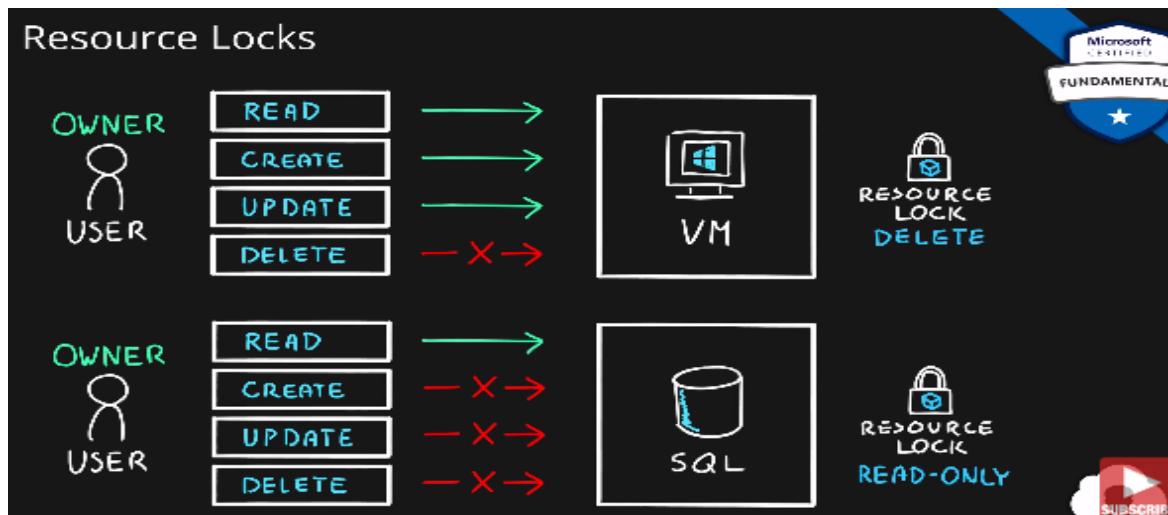


Key Characteristics

- Authorization system built on Azure Resource Manager (ARM)
- Designed for fine-grained access management of Azure Resources
- Role assignment is combination of
 - Role definition – list of permissions like create VM, delete SQL, assign permissions, etc.
 - Security principal – user, group, service principal and managed identity and
 - Scope – resource, resource groups, subscription, management group
- Scopes are hierarchical
 - Management Groups > Subscriptions > Resource Groups > Resources
- Built-in and Custom roles are supported

Resource Locks: - Better to not apply lock on resources because there will be multiple resources, so only we apply lock for Resource Group level.

The highest level that resource lock can be applied is to subscription level.



Better we will use these resource locks on production account where none should be deleted.

Resource Locks

Key Characteristics

- Designed to prevent accidental deletion and/or modification
- Used in conjunction with RBAC
- Two types of locks
 - Read-only (ReadOnly) – only read actions are allowed
 - Delete (CanNotDelete) – all actions except delete are allowed
- Scopes are hierarchical (inherited)
 - Subscriptions > Resource Groups > Resources
- Management Groups can't be locked
- Only Owner and User Access Administrator roles can manage locks (built-in roles)

Organization of Azure resources with Azure resources Tags.

We can't change the resource group name if I want to add the resources which are not related to resource group name.

So instead, TAGS allows you to add extra information to name the resources in a unique way so that it can be understandable to everyone.

We can also apply multiple tags to a single resource.

HEY, WE CAN ALSO ASSIGN RESOURCE tags to Resource Groups level.

We can make use of TAGS for doing automation, applying securities. Finding relevant resources.

Resource Tags



Name ↑↓	Subscription ↑↓	Location ↑↓	Tags
az-900	Visual Studio Enterprise	North Europe	...
az-900-aci	Visual Studio Enterprise	West Europe	...
az-900-appservice	Visual Studio Enterprise	West Europe	...
az-900-bastion	Visual Studio Enterprise	West Europe	owner: adam.marczak cost_center: 1...
az-900-bigdata	Visual Studio Enterprise	West Europe	application: app1 spoc: adam@mar...
az-900-ddos	Microsoft Azure Sponsorship	West Europe	...
az-900-devops	Visual Studio Enterprise	West Europe	...
az-900-devtest-labs	Microsoft Azure Sponsorship	West Europe	...
az-900-devtest-labs3280528466001	Visual Studio Enterprise	West Europe	...
az-900-devtest-labs317310543000	Visual Studio Enterprise	West Europe	...

We can also check cost estimation and all by filtering tags also.

Key Characteristics

- Tags are simple Name (key) - Value pairs
- Designed to help with organization of Azure resources
- Used for resource governance, security, operations management, cost management, automation, etc.
- Typical tagging strategies
 - Functional - mark by function (ex: environment = production)
 - Classification - mark by policies used (ex: classification = restricted)
 - Finance/Accounting - mark for billing purposes (ex: department = finance)
 - Partnership - mark by association of users/groups (ex: owner = adam)
- Applicable for resources, resource groups and subscriptions
- NOT inherited by default

A Microsoft Certified Fundamental badge is visible in the top right corner.

Azure Policy: - Check for certain azure resource properties through which the further resource decisions will be done.

Here policies will check for only resource properties.

