

Microsoft-Azure-Administrator
AZ-104/AZ-103

Module 01 - Identity
Module 02 – Governance and Compliance
Module 03 – Azure Administration
Module 04 – Virtual Networking
Module 05 – Intersite Connectivity
Module 06 – Network Traffic Management
Module 07 – Azure Storage
Module 08 – Azure Virtual Machines
Module 09 - Serverless Computing
Module 10 – Data Protection
Module 11 – Monitoring

MODULE 1: IDENTITY: AZURE AD & USERS AND GROUPS
AZURE ACTIVE DIRECTORY
AZURE AD CONCEPTS
AD DS VS. AZURE ACTIVE DIRECTORY
AZURE ACTIVE DIRECTORY EDITIONS
AZURE AD JOIN
MULTI-FACTOR AUTHENTICATION
SELF-SERVICE PASSWORD RESET

Identity

What is Identity?

Definition first

Identity

*A thing that can get **authenticated**.*

*Can be a **user** with a **username** and **password**.*

*Also **applications** or **other servers** with **secret keys** or **certificates**.*

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*

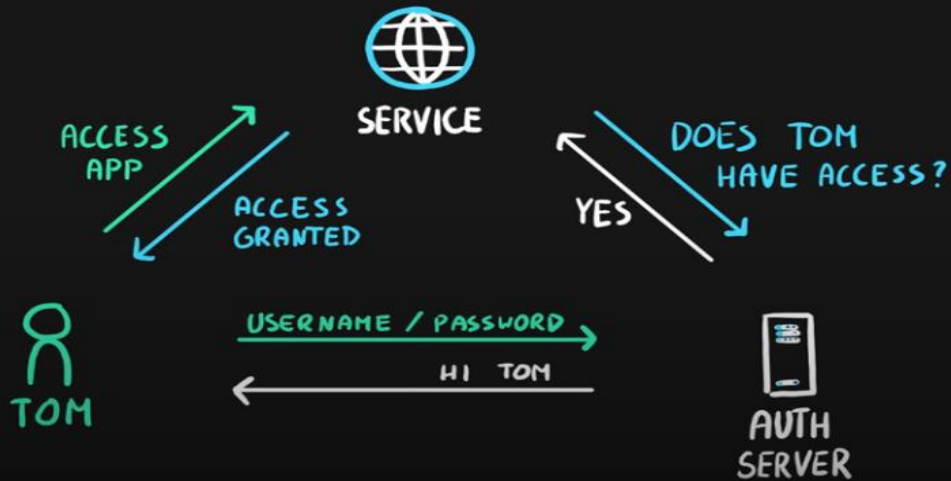

TOM




AUTH
SERVER

Authorization

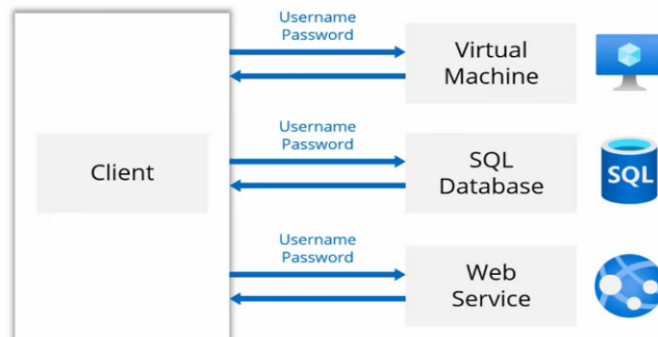
The process of ensuring that only *authenticated identities* get access to the resources for which they have been granted access.



Classic Approach

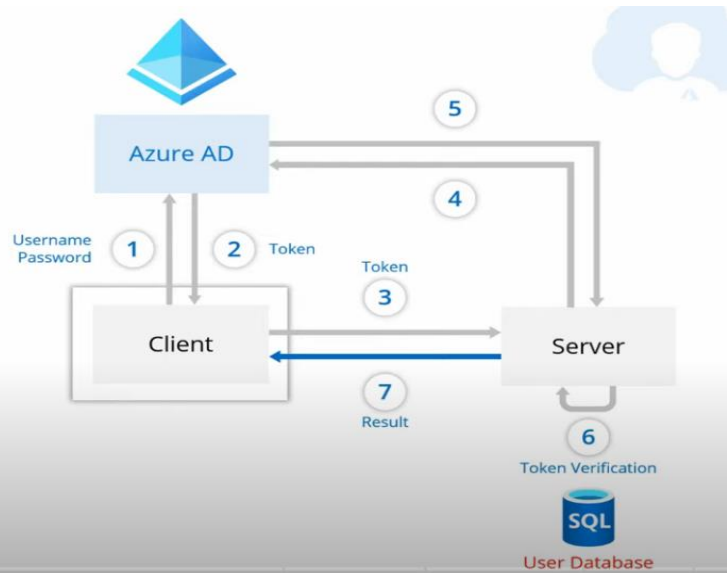
Challenges

- Implementing security features takes time and money
- Security risk by maintaining user database
- User credentials change per application/service



Identity Provider

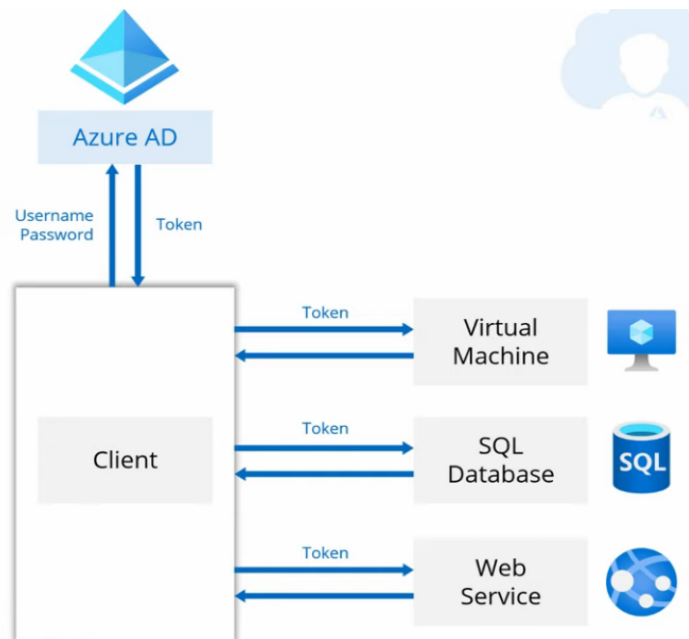
Benefits



Identity Provider

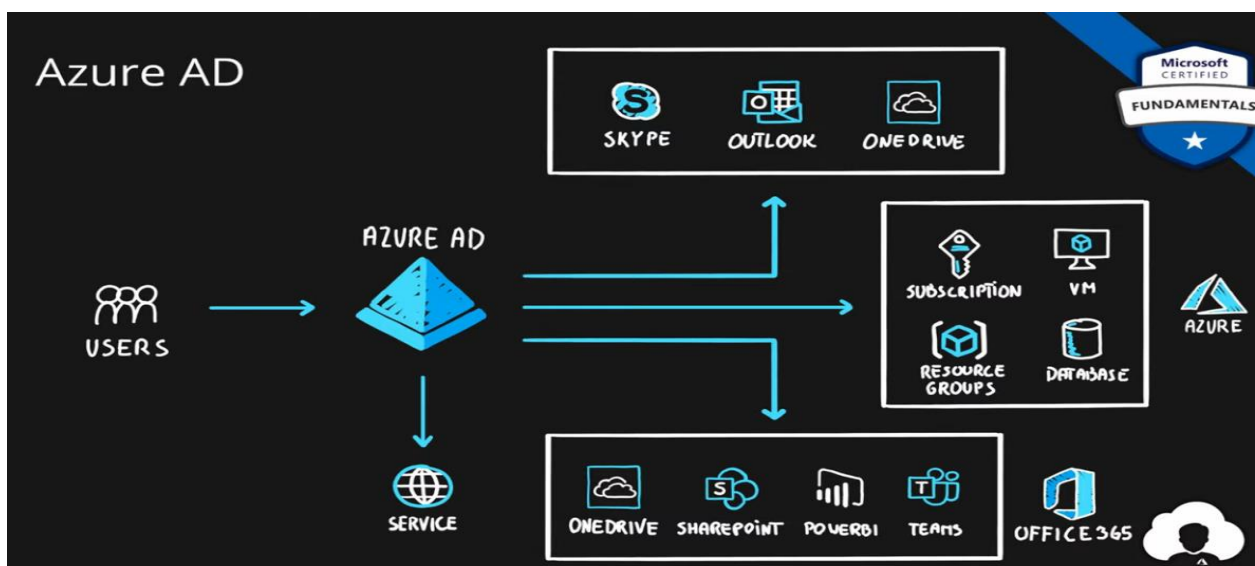
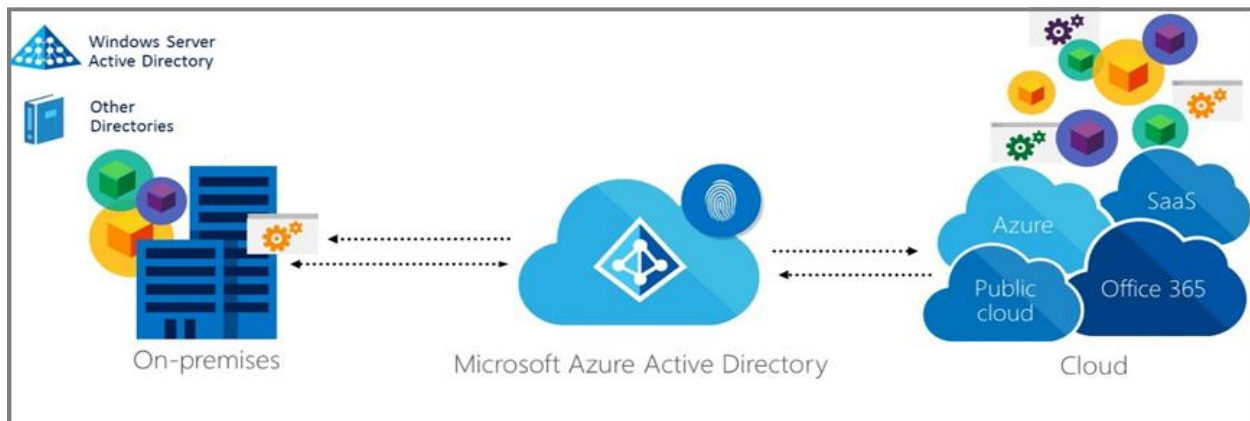
Benefits

- Centralized user management
- Top notch security
- Multitude additional features like MFA, conditional access, etc.



What is the Azure Active Directory?

- Azure Active Directory is Microsoft's multi-tenant, cloud-based directory and identity management service.
- For an organization, Azure AD helps employees sign up to multiple services and access them anywhere over the cloud with a single set of login credentials.

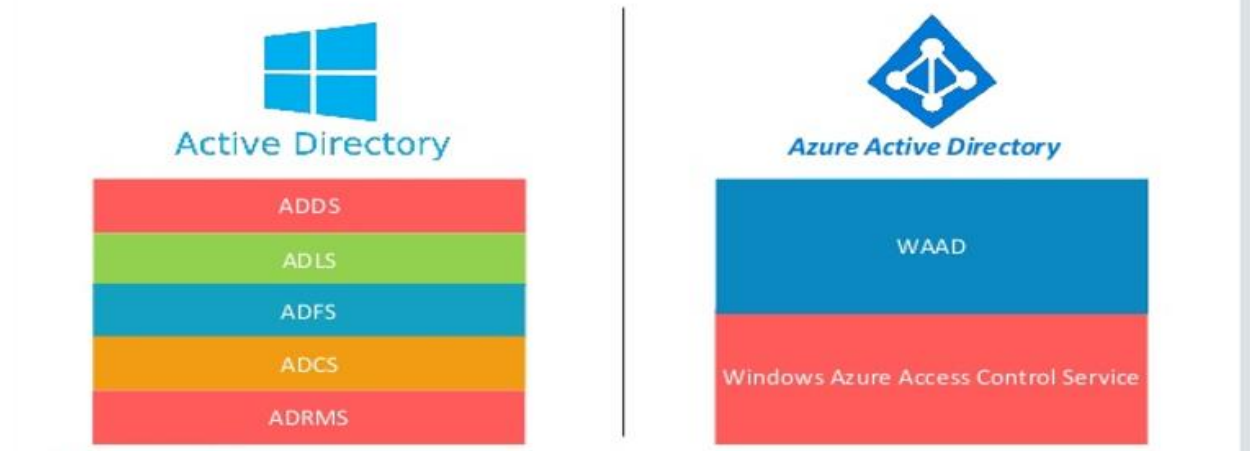


Azure AD vs ADDS vs Azure ADDS

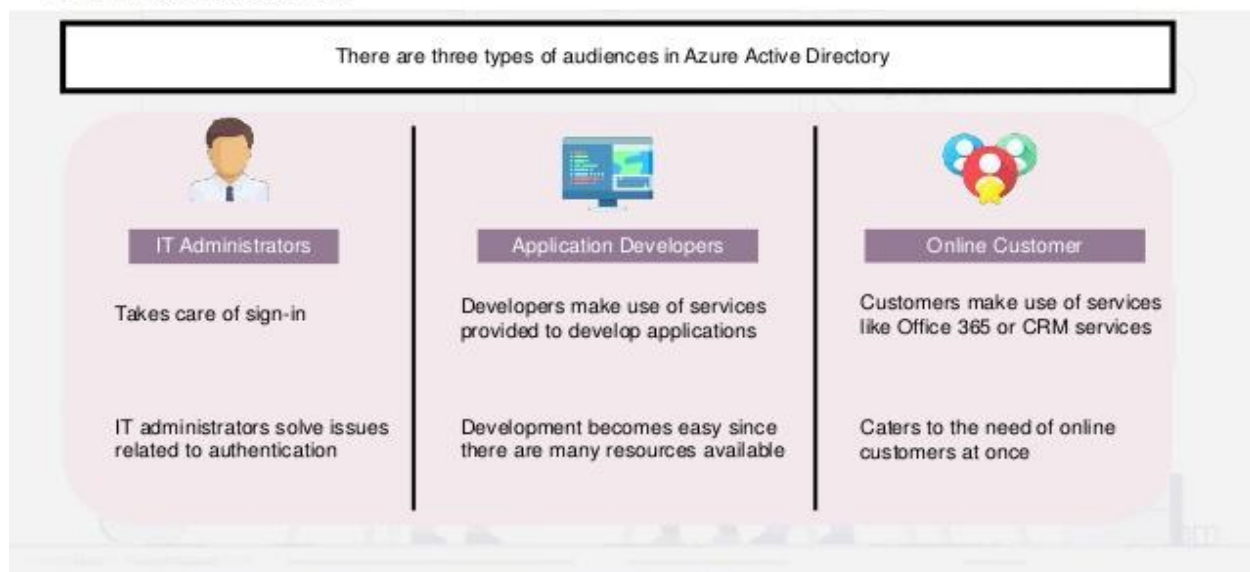
What are the differences

	Active Directory Domain Services (AD DS)	Azure Active Directory (AAD)	Azure Active Directory Domain Services (Azure AD DS)
	 Azure AD Connect  Synchronization 		
Extensible Schema	✓	✗	✗
LDAP, Kerberos, NTLM	✓	✗	✓ LDAP Read Only
OAuth, SAML	✗	✓	✗
Cloud Based	✗	✓	✓
Domain Enterprise Admin, Forest Trusts	✓	✗	✗
Group Policy	✓	✗	✓
High Availability	Manual Config	✓	✓

Windows AD Vs Azure AD



Service Audience



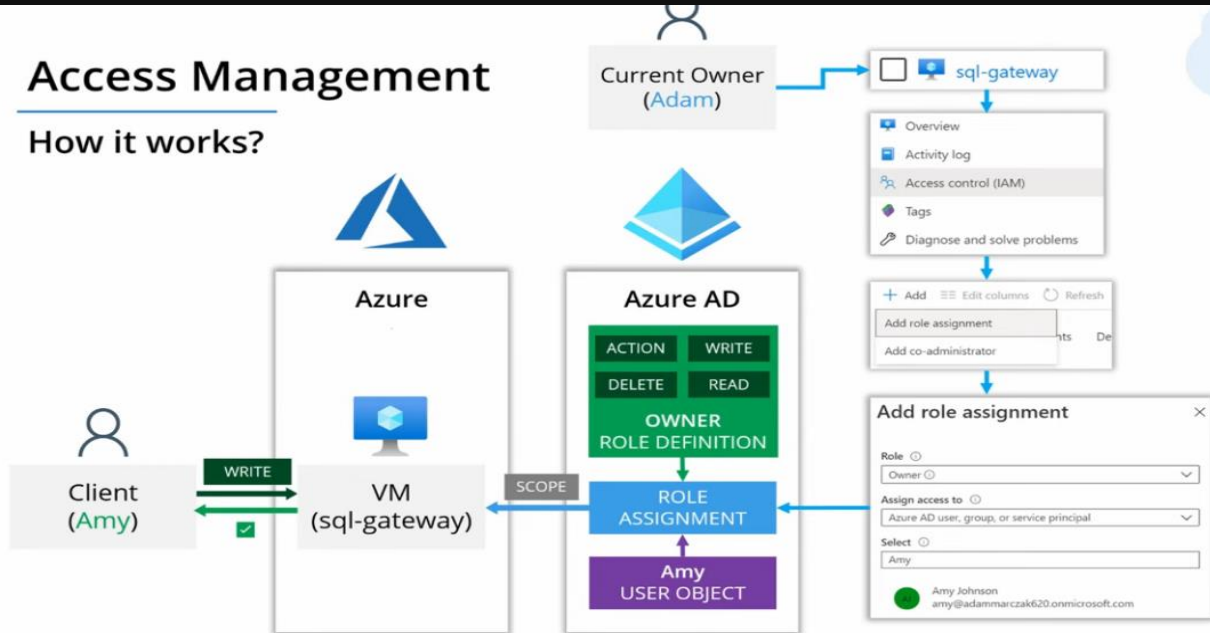
Azure Active Directory

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

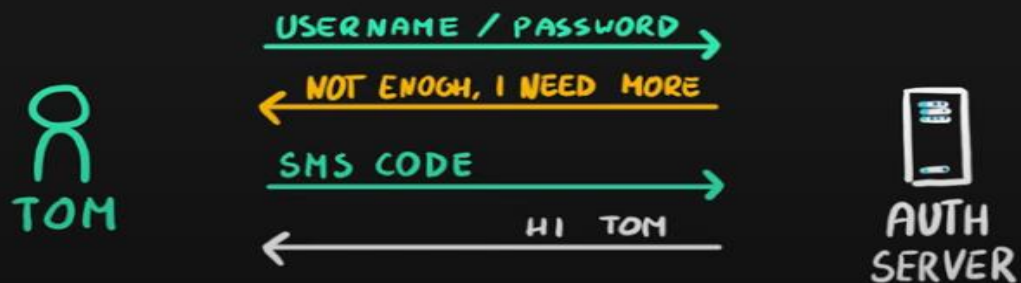
Access Management

How it works?



Multi-factor Authentication

*Process of presenting **two or more** pieces of evidence to prove one's identity*



Multi-factor Authentication

Key Characteristics

- Process of authentication using more than one **factor** (evidence) to prove identity
- Factor types
 - **Knowledge** Factor – “Something you know”, ex. password, pin
 - **Possession** Factor – “Something you have”, ex. phone, token, card, key
 - **Physical Characteristic** Factor – “Something you are”, ex. fingerprint, voice, face, eye iris
 - **Location** Factor – “Somewhere you are”, ex. GPS location
- Supported by **Azure AD** by default (simple on-off switch)

Azure AD User Types

Cloud identities

- Local Azure AD
- External Azure AD

Hybrid identities

- Directory-synchronized

Guest identities

- Azure AD B2B Collaboration
- External identities



Azure AD Groups

Security	Owners	Dynamic membership
Microsoft 365	Assigned membership	Group-assigned roles and licenses



Group

- Bulk add using CSV template in the portal

Dynamic Group

- Rule based assignment
- Can be group-assigned roles and licenses
- Cannot manually add users/devices

Administrative Units



Azure AD user and group container analogous to organizational unit (OU) in local Active Directory

Logically organize your Azure AD users

Delegate administrative permissions

Manage user and group properties



Modify user profile in the portal

Modify group properties in the portal

Modify using PowerShell

- AzureAD module

User Administrator or Global Administrator role

Manage device settings



Cloud device administrator

- Add, Enable, disable, delete devices in Azure AD
- Cannot modify properties

Device administrator

- Local machine administrator, cannot modify object in Azure AD

Perform bulk user updates



Bulk add to groups using CSV template in the portal

Programmatically using PowerShell

Manage guest accounts



Requires Azure AD Premium P2

Guest identities

- Azure AD B2B collaboration
- External identities

Can be invited by:

- Administrators
- Users

Roles required for guest review

- Global administrator
- User administrator

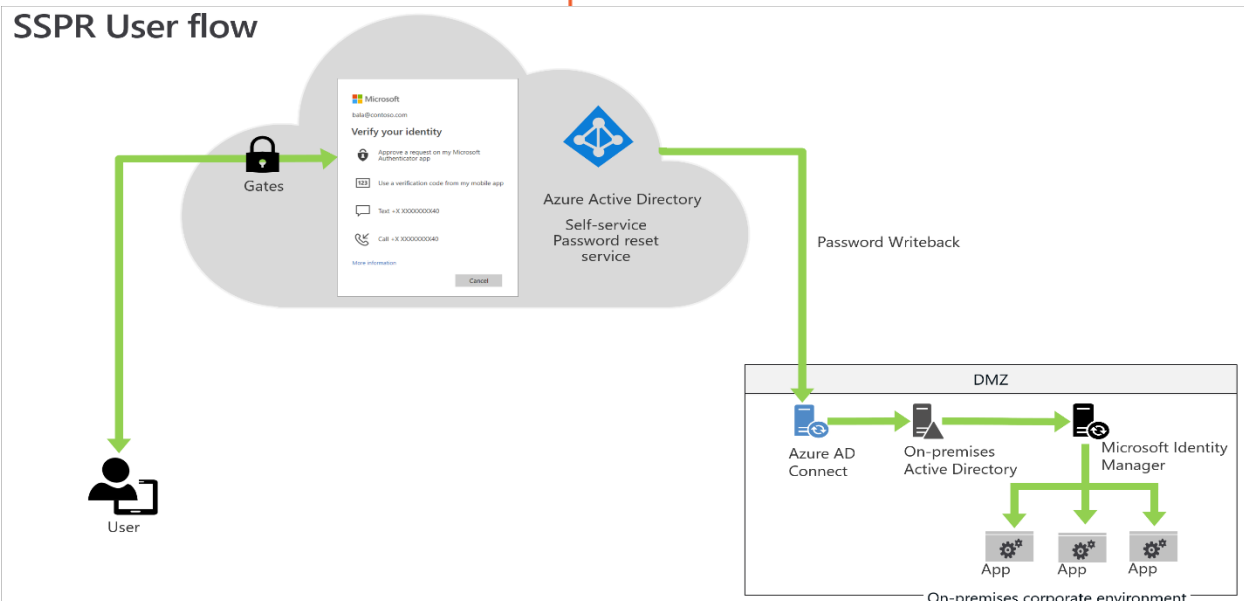
Azure AD Join Options

Azure AD Registered

Personally owned device
MSA or local account sign-in
Windows 10
iOS
Android
macOS

Azure AD Joined

Organization owned device
Azure AD sign-in
Windows 10
Windows Server 2019 VMs in Azure



SUBSCRIPTION AND ACCOUNTS
AZURE POLICY
ROLE-BASED ACCESS CONTROL

Azure Management Groups

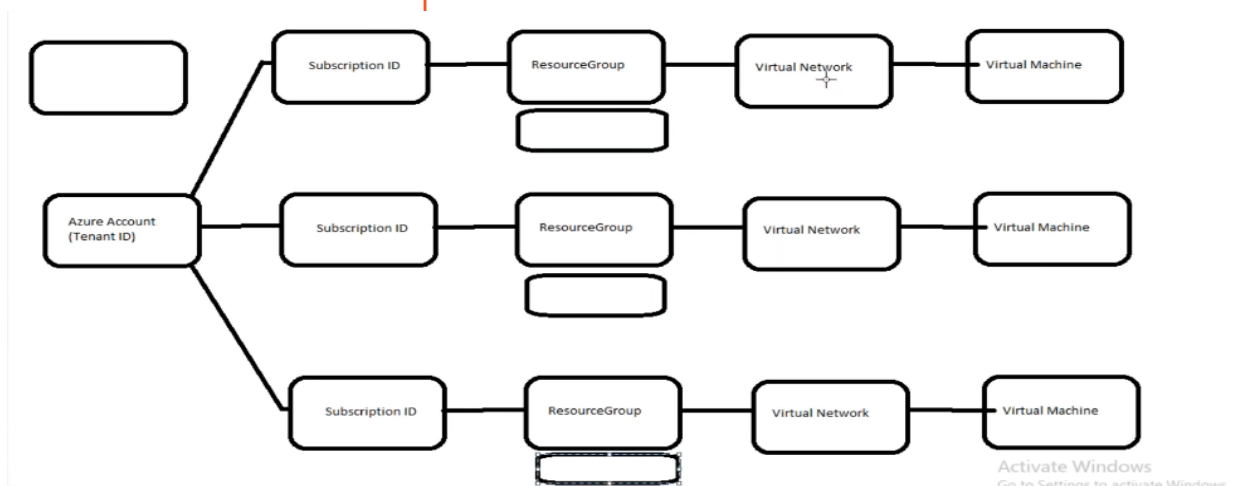
Azure Management Groups



Used to efficiently manage access, policies and compliance

Provides a level of scope over subscriptions

Subscriptions within a group inherit policies applied to the group



Azure
Active Directory

Microsoft
Azure

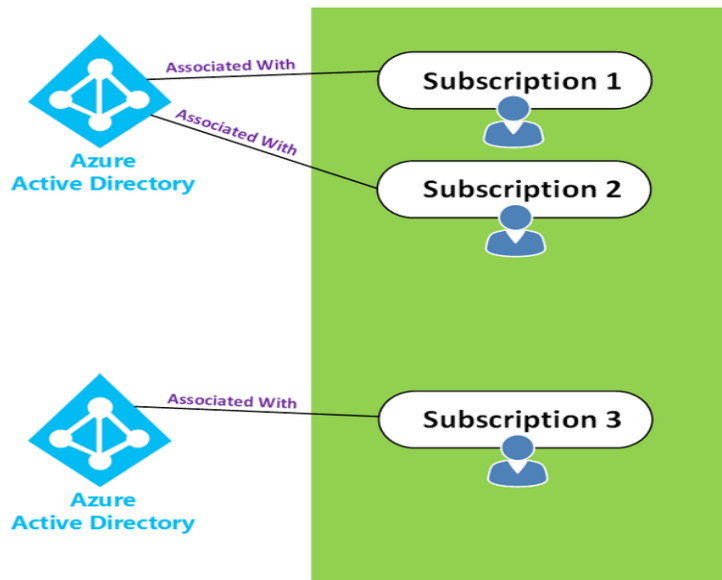
Single Tenant

Azure
subscription

Can have Multiple
Subscriptions

Resource group

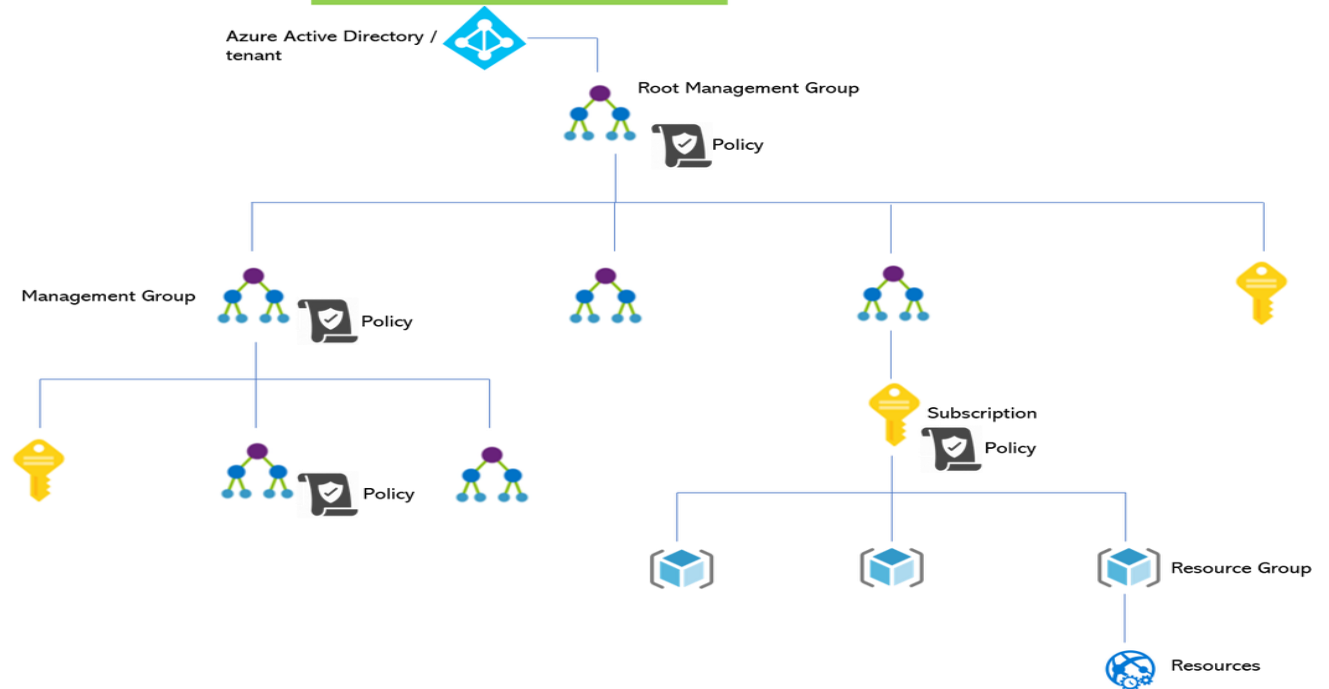
Can have multiple
Resource Groups

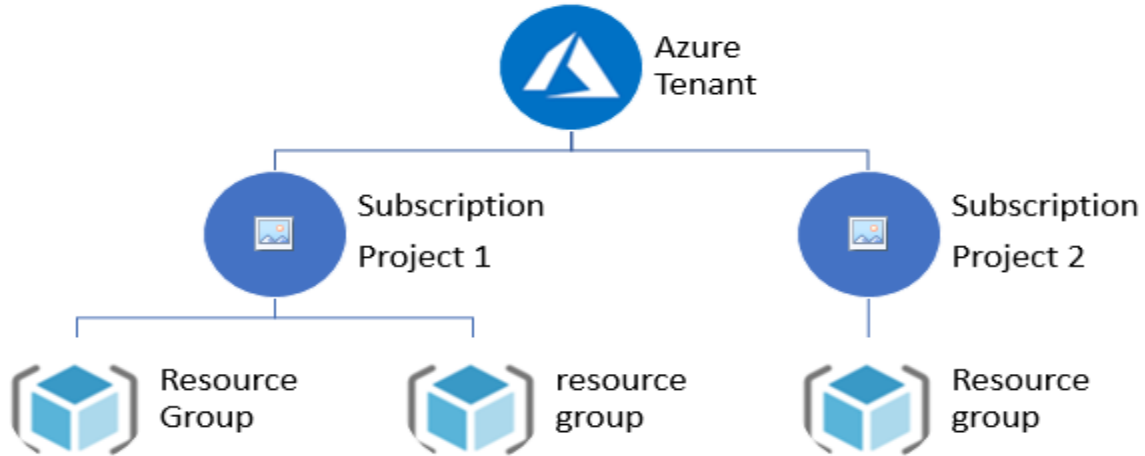


- Reader**
- Let's you view everything, but not make any changes

- Contributor**
- Let's you manage everything except access to resources

- Owner**
- Let's you manage everything, including access to resources
 - Same access privileges as co-administrator

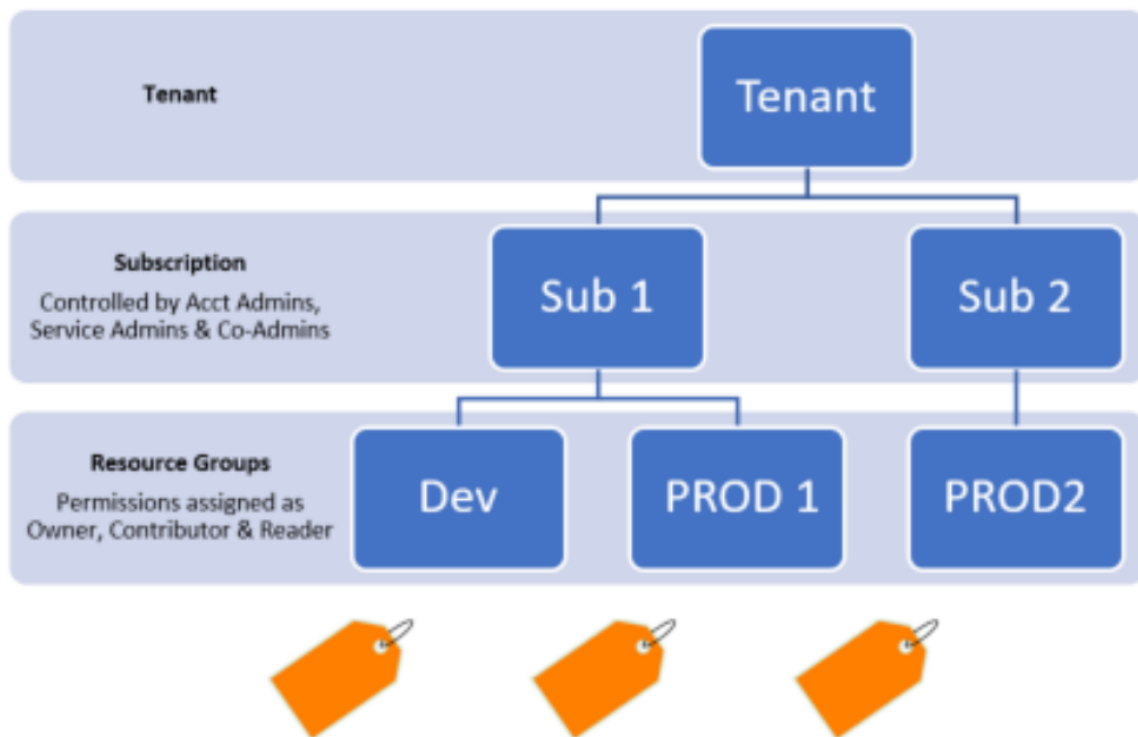




What is a Tenant?

A tenant may have multiple Azure subscriptions and one or more domains can be possible

A very large enterprise may use multiple subscriptions to better manage billing between divisions.



What Are Azure Subscriptions?



Subscriptions

What is a Subscription?



Construct for creating separate billing and management boundaries



Is managed in <https://portal.azure.com>



Can be linked to existing identity stores for single-sign on, or segregated into a separate area



Becomes the major separation for assignment of RBAC within services



You can create multiple subscriptions in your Azure account to create separation



Subscription



Resource Groups



Resources

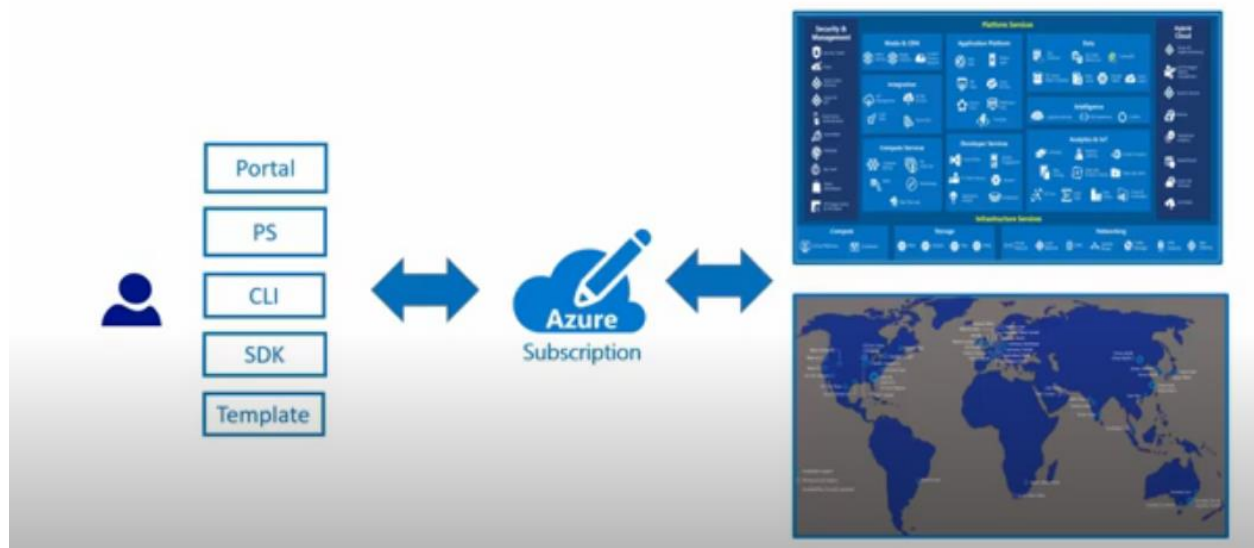


You can move resources between subscriptions

You can transfer subscriptions between different tenants

A single tenant can have multiple subscriptions

Azure Subscription



Azure Subscription Types

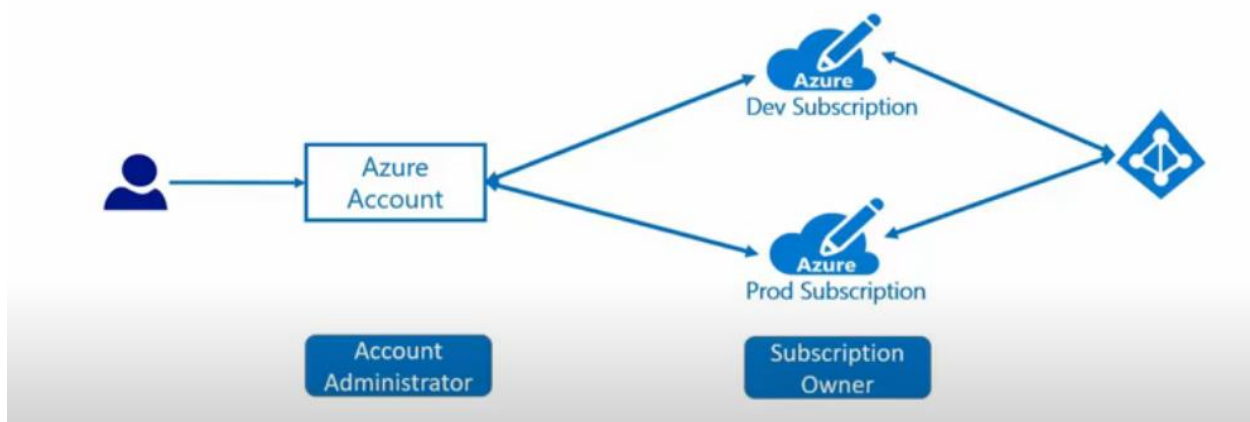
Microsoft Azure Offer Details

The tables below list all of our active offers. The first table lists our offers that are currently available for purchase. The second table lists those offers that are no longer available for purchase, although existing customers can continue to be on these rate plans.

Current Offers

OFFER NAME	OFFER NUMBER	SPENDING LIMIT
Enterprise Agreement Support		
Pay-As-You-Go	0003P	
Support Plans	0041P, 0042P, 0043P	
Free Trial	0044P	✓
Visual Studio Professional subscribers	0059P	✓
Visual Studio Test Professional subscribers	0060P	✓
MSDN Platforms subscribers	0062P	✓
Visual Studio Enterprise subscribers	0063P	✓
Visual Studio Enterprise (BizSpark) subscribers	0064P	✓
Visual Studio Enterprise (MPN) subscribers	0029P	✓

Azure Subscription



It's just an ownership account.

Azure subscription is a logical bundle of Azure resources, which serves as a single billing unit for the resources that are present in that service.

An Azure subscription can be mapped to only one account. However, an account can have multiple subscriptions.

What's a Resource Group?



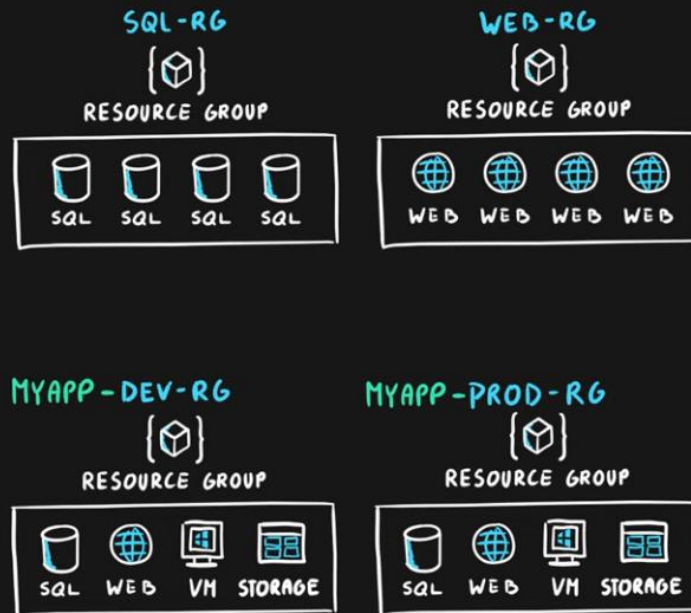
Resource groups

Resource Groups

Key Characteristics

Organizing by

- Type
- Lifecycle (app, environment)
- Department
- Billing, Location or combination of those



Resources can be moved from one resource group to another if that is supported by that resource

Moving resources does not change the location/region where it was originally created

Deleting a resource group deletes all resources in that resource group

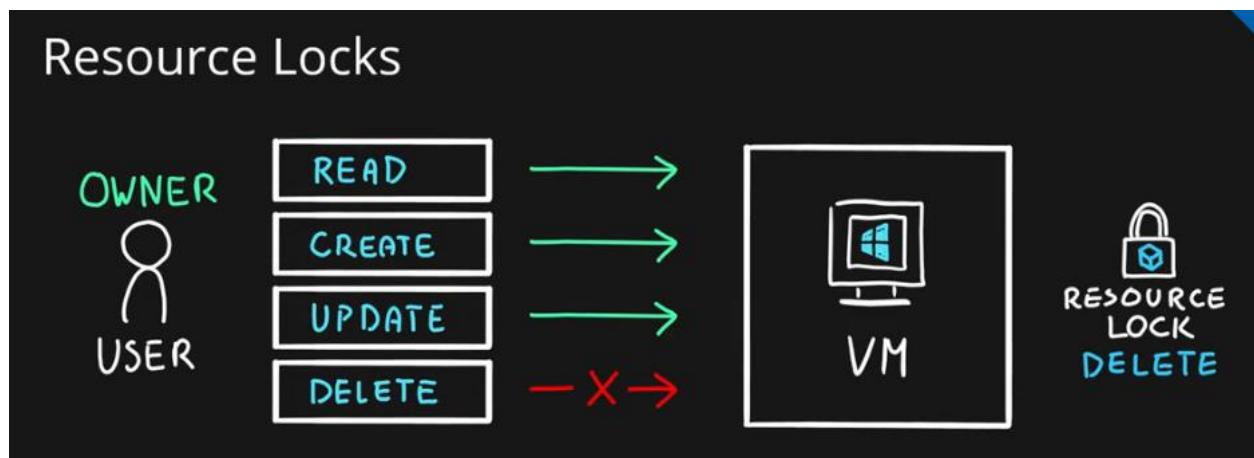
Managing Access to Resources



Resource locks



Resource Groups



Resource Locks



Each resource can have a lock applied

Locks types include:

- Read-only
- Delete

Can apply to all resources and resource groups

Can be inherited from parent scopes

- For both existing and new resources

Applies to all users and roles

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 Tags



Used to organize resources and management hierarchy

Each tag consists of name and value pair

Must have write access to `Microsoft.Resources/tags`

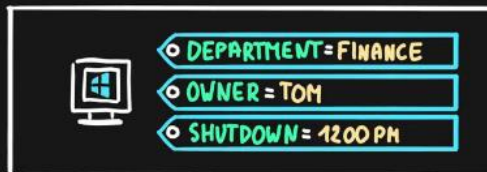
Resource Tags


RESOURCE GROUP
APP 1



OWNER=ADAM
COST_CENTER=324


RESOURCE GROUP
APP 2



OWNER=ADAM
COST_CENTER=581


RESOURCE GROUP
APP 3



OWNER=TOM
COST_CENTER=123

Apply Tags



Used to organize resources and management hierarchy

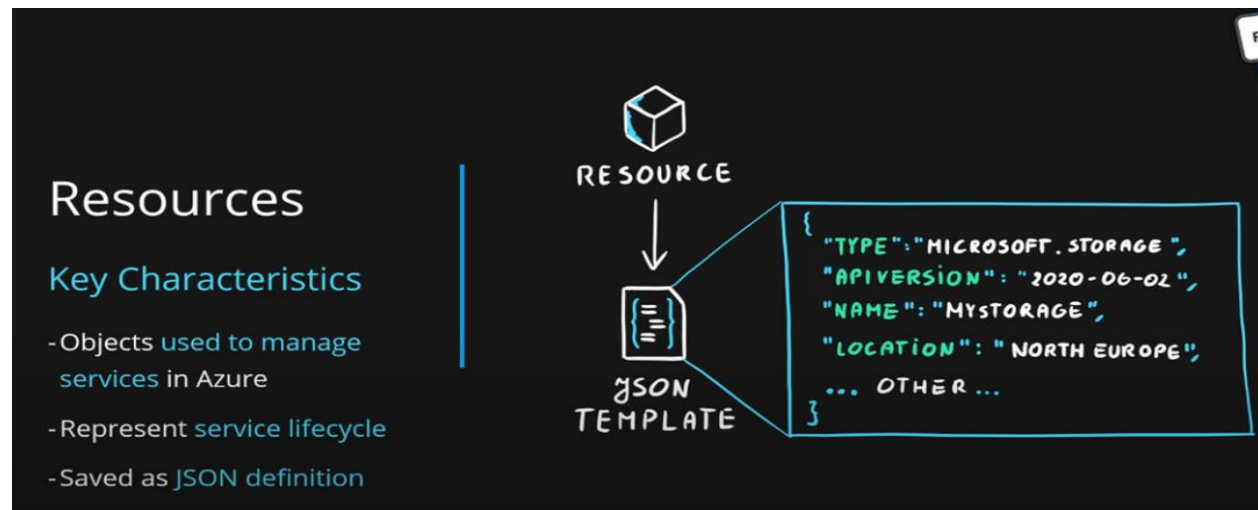


Each tag consists of name and value pair



Must have write access to Microsoft.Resources/tags

Resource



Configure Cost Management



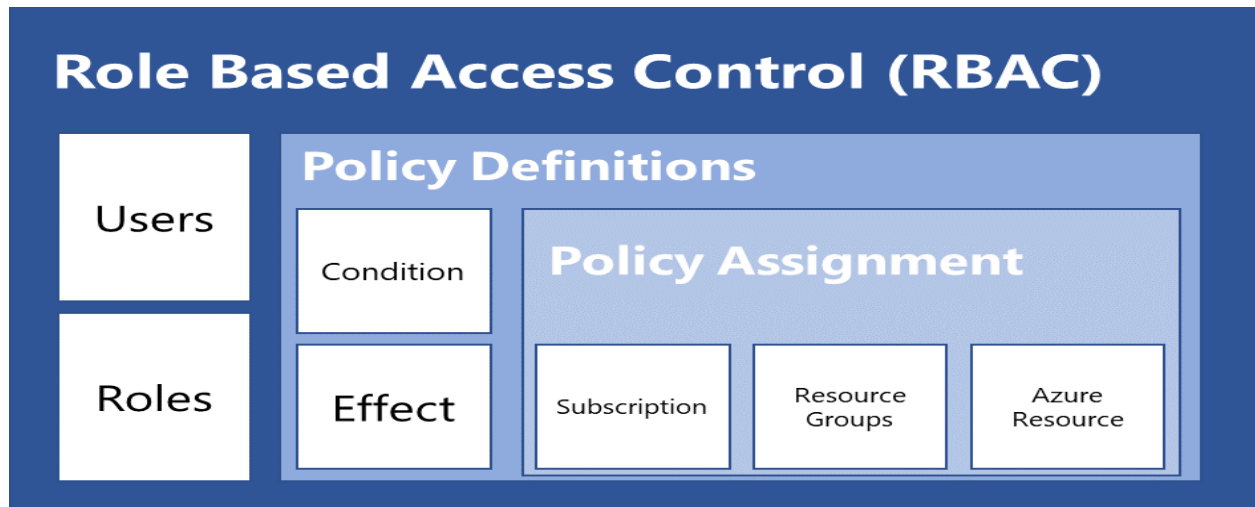
Analyze costs and trends using **Cost Analysis**

Cost Alerts can be generated to alert when a threshold you define is met

Apply **Budgets** to apply cost thresholds and limits to control your Azure spend

Recommendations displays ways to control costs through identifying trends in your usage

Role-Based Access Control



Role-based Access Control



Role-based access control can be used to assign permissions to:

- Users
- Groups
- Applications

The scope of role assignment can be:

- Subscription
- Resource Group
- Single resource

Role-based Access Control



Allow one user to manage virtual machines in a subscription and another user to manage virtual networks

Allow a DBA group to manage SQL databases in a subscription

Allow an application to access all resources in a resource group

Security Principals



User who has a profile in Azure AD, can be assigned to users in other tenants



Multiple users are assigned to a **group**, roles assigned to group impact all the users



A **service principal** is a security ID for applications or services



A **managed identity** is typically used in developing cloud applications to handle credential management

Roles



Owner has full access to all resources and grant access



Contributor can create/manage all resources, cannot grant access



Reader can view existing resources



User Access Administrator lets you manage user access

Deny Assignments



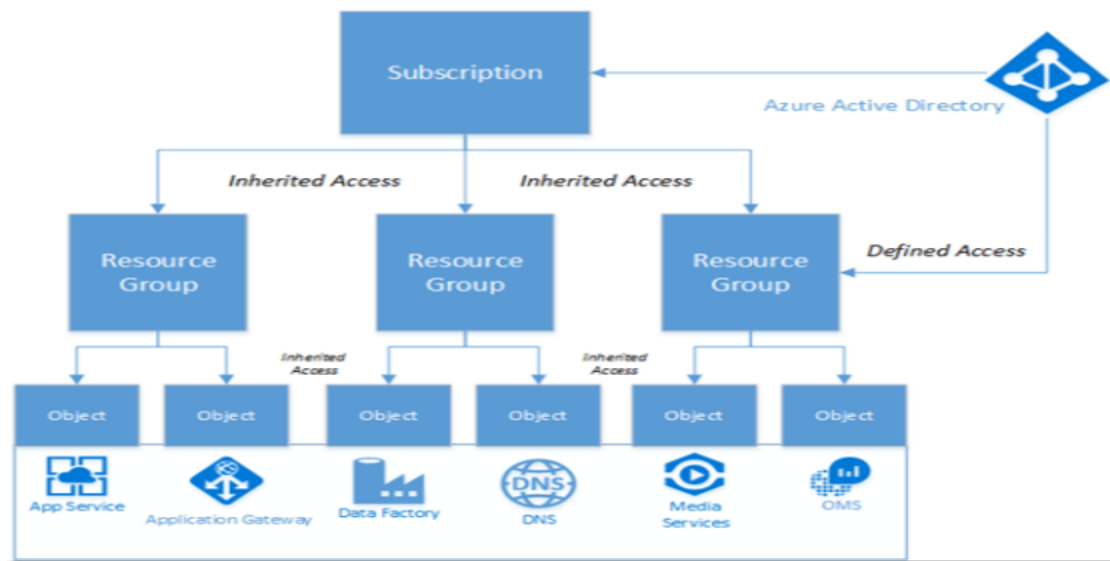
Blocks users from performing specific actions even if a role assignment allows it



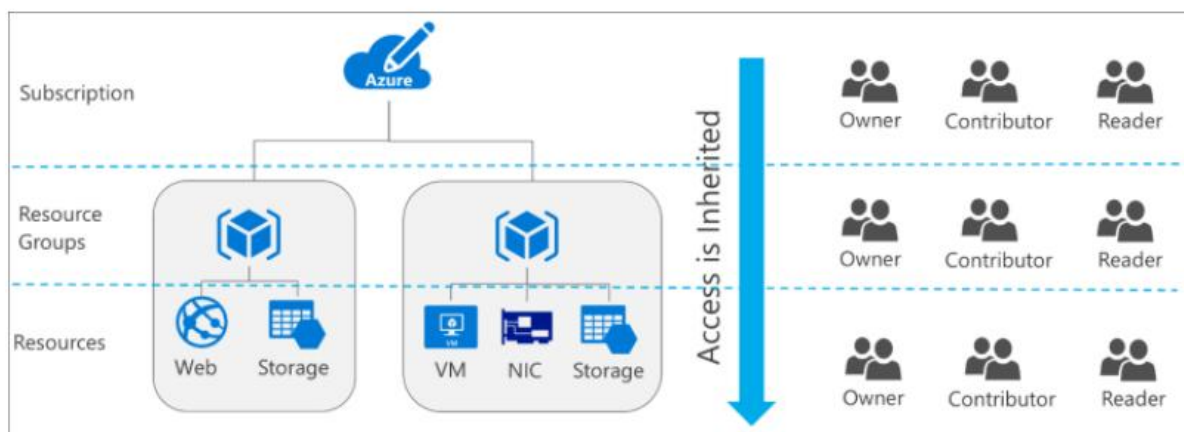
Created and managed in Azure to protect resources



Can only be created using Azure Blue Prints or managed apps



Scope	Role			
	Reader	Resource-specific or custom role	Contributor	Owner
	 Subscription Observers	Users managing resources		Admins
	 Resource group  Resource Automated processes			



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

Create a Custom Role



Portal

- Clone existing role

ARM Template

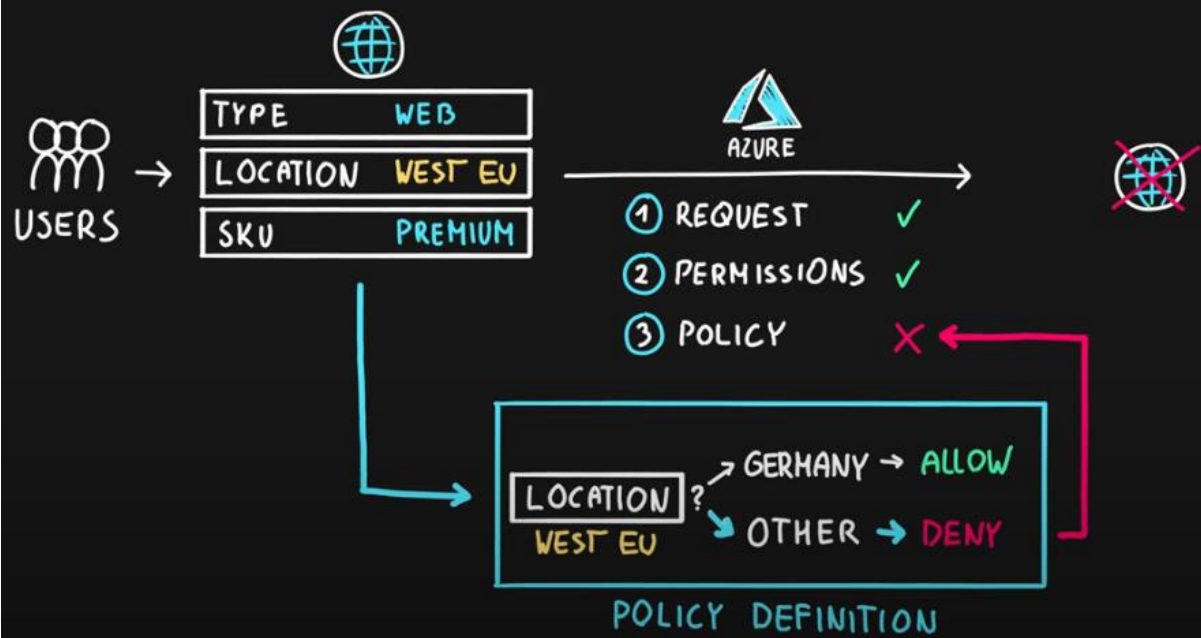
PowerShell

- Modify existing role definition
- Create new role using modified definition

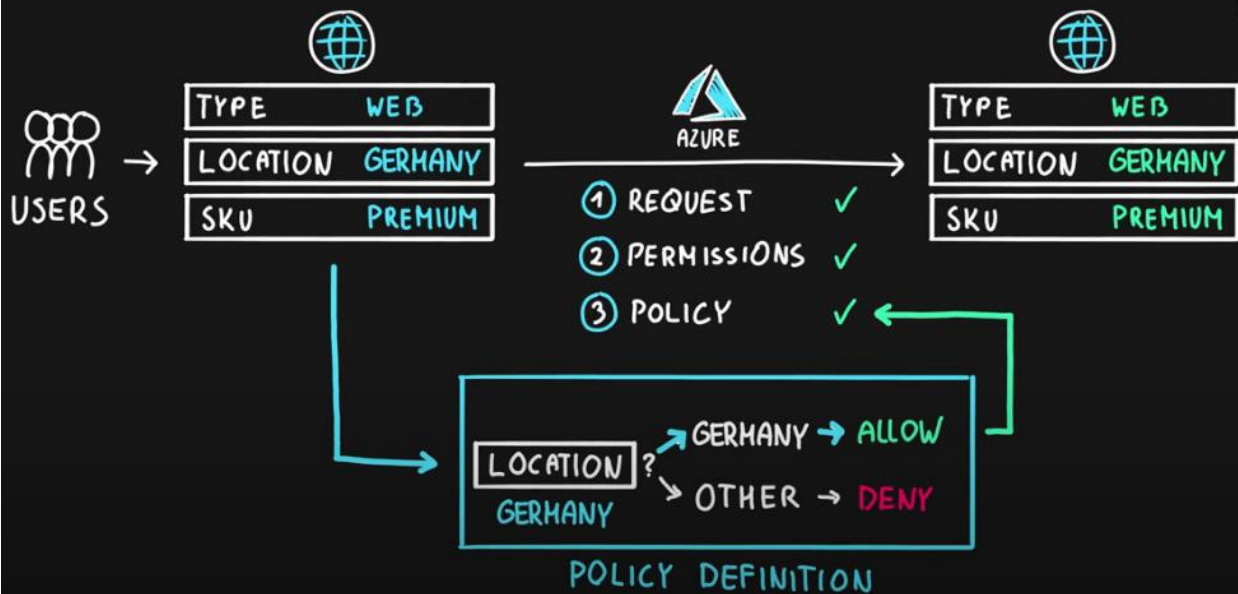
Azure and Azure AD offer two types of RBAC roles

Azure RBAC roles	Azure AD administrator roles
Manage access to Azure resources	Manage access to Azure AD objects
Support custom roles	Does not support custom roles
Scope can be specified at multiple levels	Scope is at the tenant level
Role information can be accessed in the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure portal, Office 365 admin portal, Microsoft Graph, Azure Active Directory PowerShell for Graph

Azure Policy



Azure Policy



Azure Policy



Used to create, assign and manage policies in Azure

Enforce rules to ensure your resources remain compliant

Focuses on resource properties for both new deployments and existing

It does not apply remediations to resources that are not compliant

Policy Concepts



A policy definition is a rule

An assignment is an application of an initiative or a policy to a specific scope

An initiative is a collection of policy definitions

Azure Policy



Key Characteristics

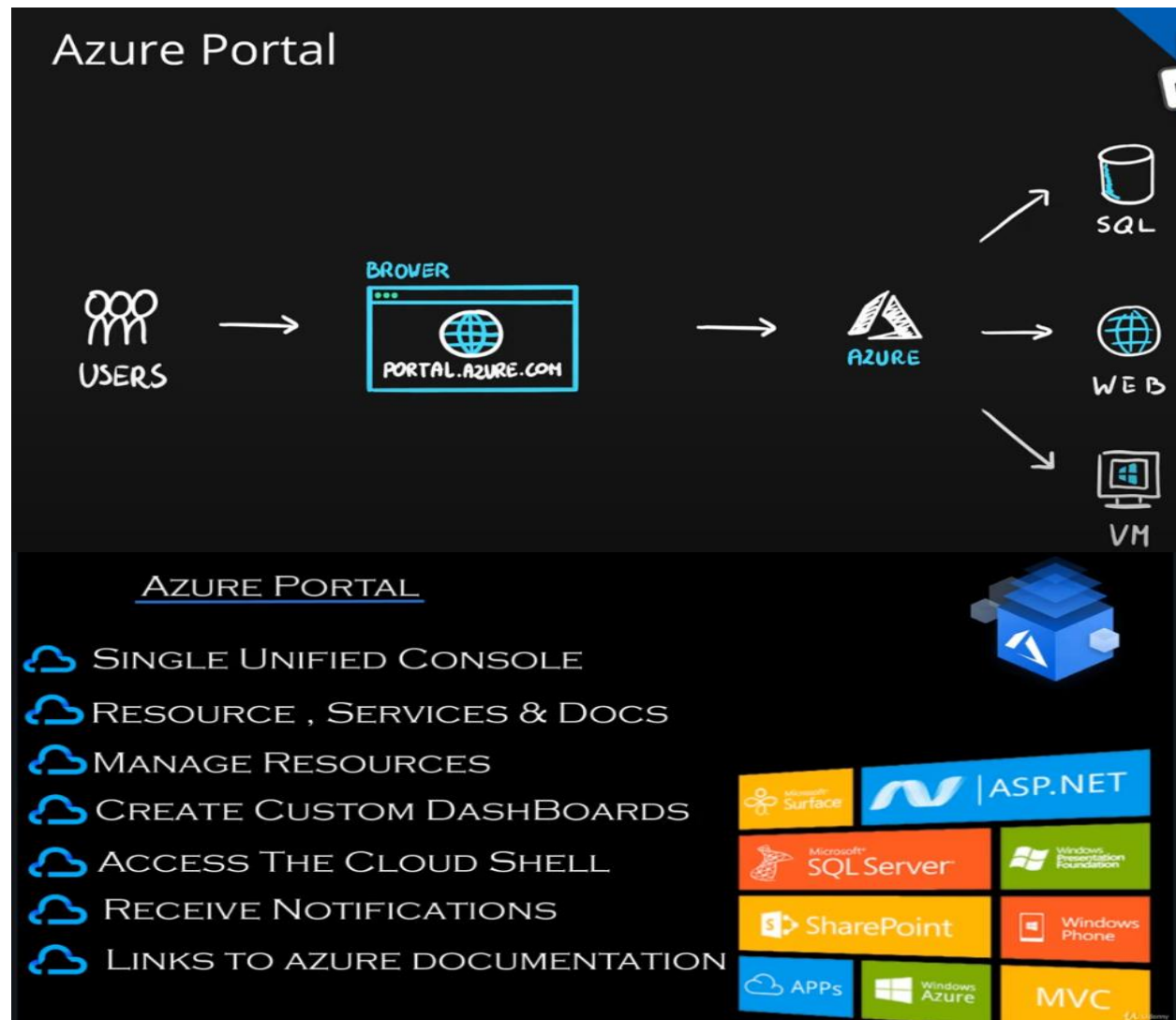
- Designed to help with resource **governance**, **security**, **compliance**, **cost management**, etc.
- Policies focus on **resource properties** (RBAC focused on **user actions**)
- Policy **definition** – Defines what should happen
 - Define the **condition** (if/else) and the **effect** (deny, audit, append, modify, etc.)
 - Examples include *allowed resource types*, *allowed locations*, *allowed SKUs*, *inherit resource tags*
 - **Built-in** and **custom** policies are supported
- Policy **initiative** – a **group** of policy definitions
- Policy **assignment** – assignment of a policy definition/initiative to a scope
 - **Scopes** can be assigned to **management groups**, **subscriptions**, **resource groups** and **resources**
 - Policies allow for **exclusions of scopes**

MODULE 3: AZURE ADMINISTRATION

RESOURCE MANAGER

AZURE PORTAL AND CLOUD SHELL

AZURE POWERSHELL AND CLI

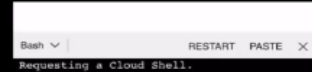


Azure Portal

Key Characteristics

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

Azure Mobile App



Stay Connected to Azure

Check Status and critical metrics

Run commands to manage Azure resources

Diagnose and Fix issues quickly

ARM Templates

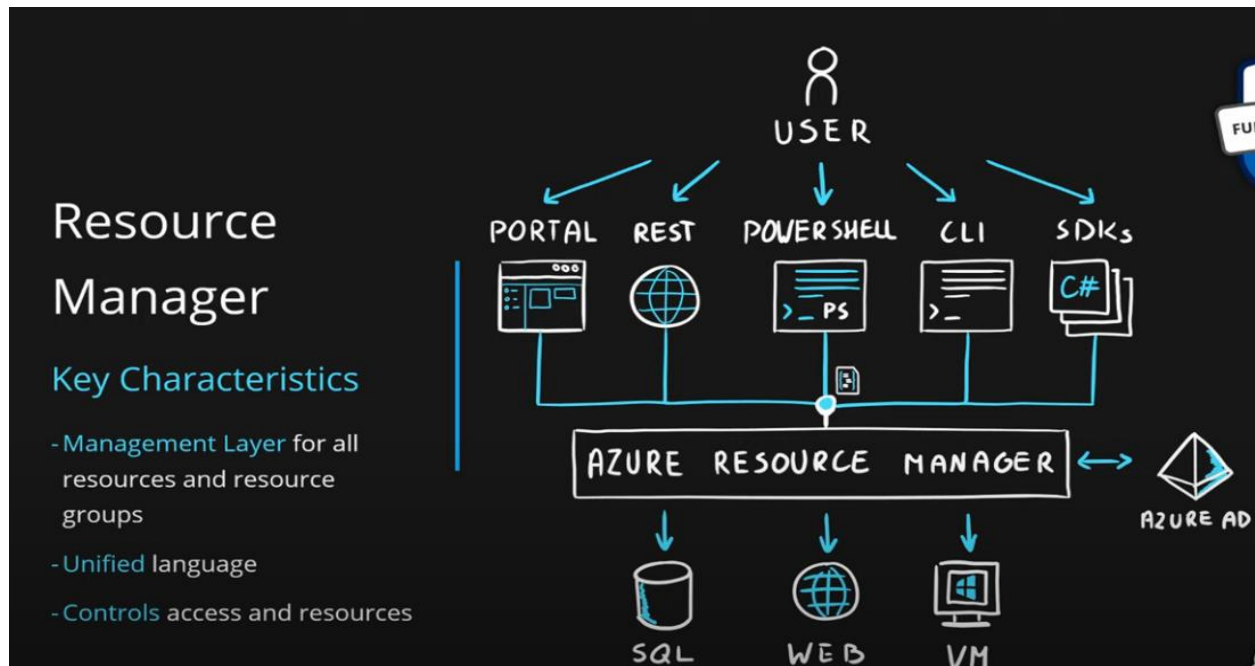


JSON format

Contains the resources to create in Azure

Submit template to the Azure Resource Manager

Tracked deployments

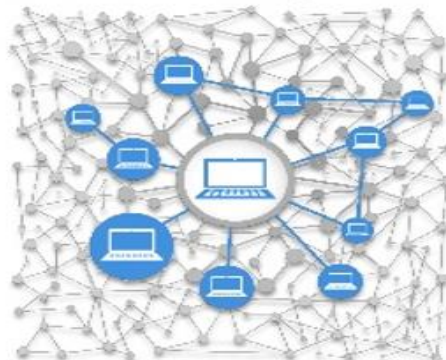


MODULE 4: VIRTUAL NETWORKING
VIRTUAL NETWORKS
IP ADDRESSING
NETWORK SECURITY GROUPS
AZURE FIREWALL
AZURE DNS

Module 04 – Virtual Networking

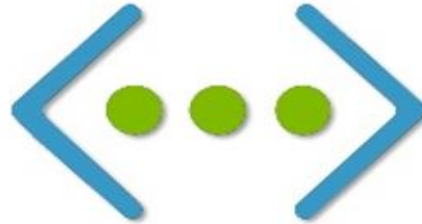
Why Virtual Networks?

Virtual Networks act as a communication channel between resources launched in the cloud. Why Virtual? Because there are no physical wires involved in connecting these resources.

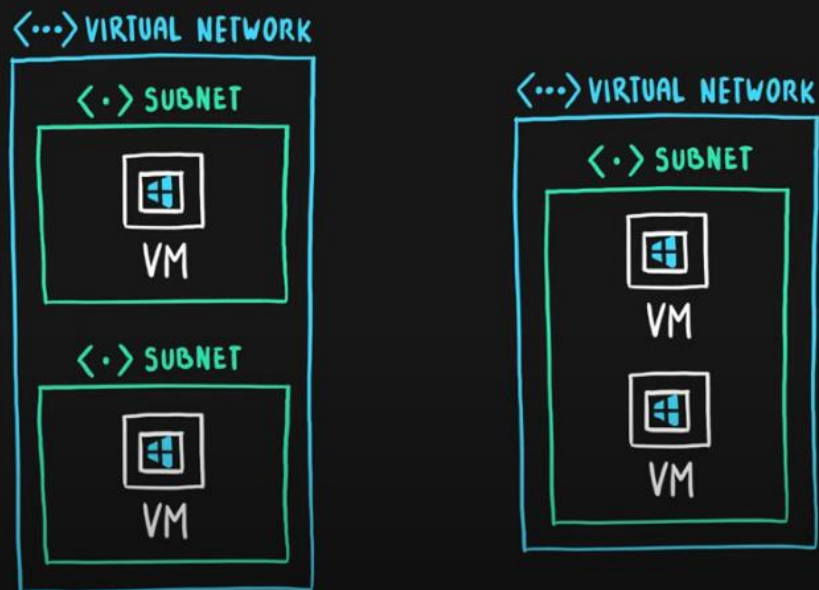


What is a Virtual Network?

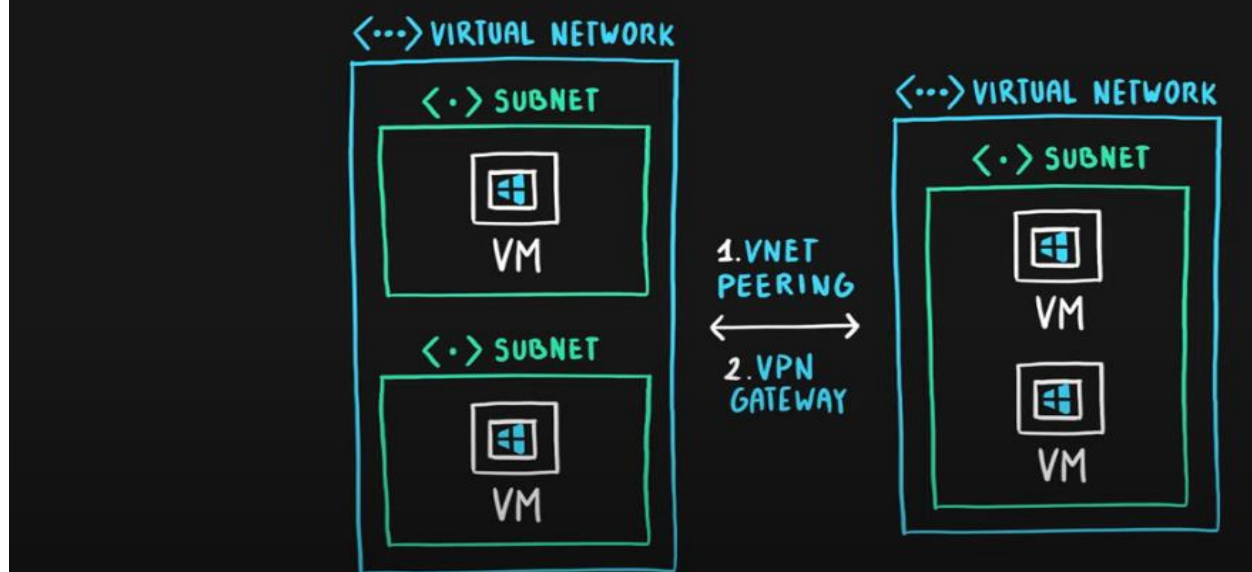
An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription



Virtual Network



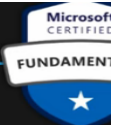
Virtual Network



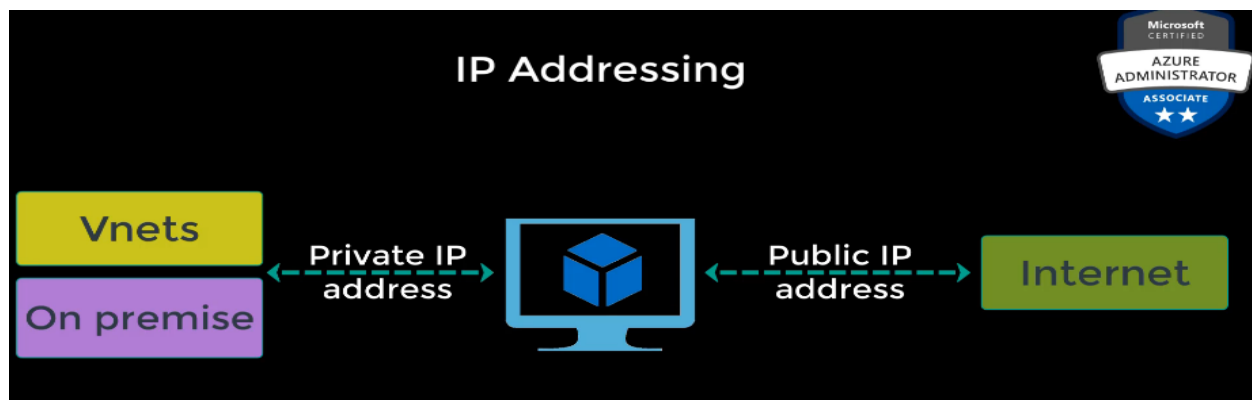
Azure Virtual Network

Key Characteristics

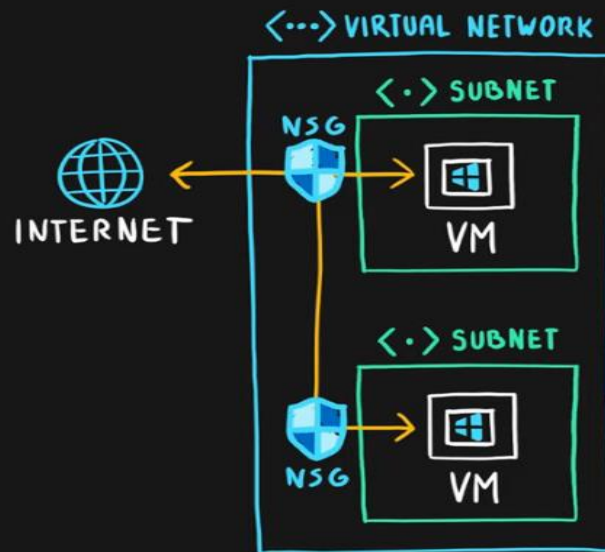
- Emulation of physical networking infrastructure
- Designed for **isolation**, **segmentation**, **communication**, **filtering**, **routing** between resources (internet and on-premises)
- Scoped to a single region
- **VNet Peering** or **VPN Gateway** allow cross VNet communication
- Segmented into 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)**



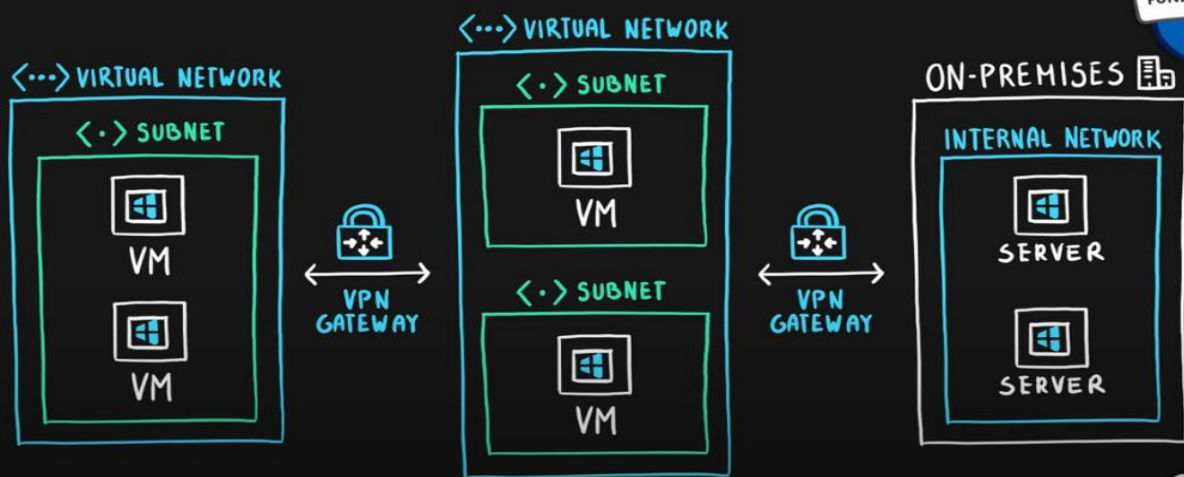
IP Addressing



Network Security Groups



VPN Gateway



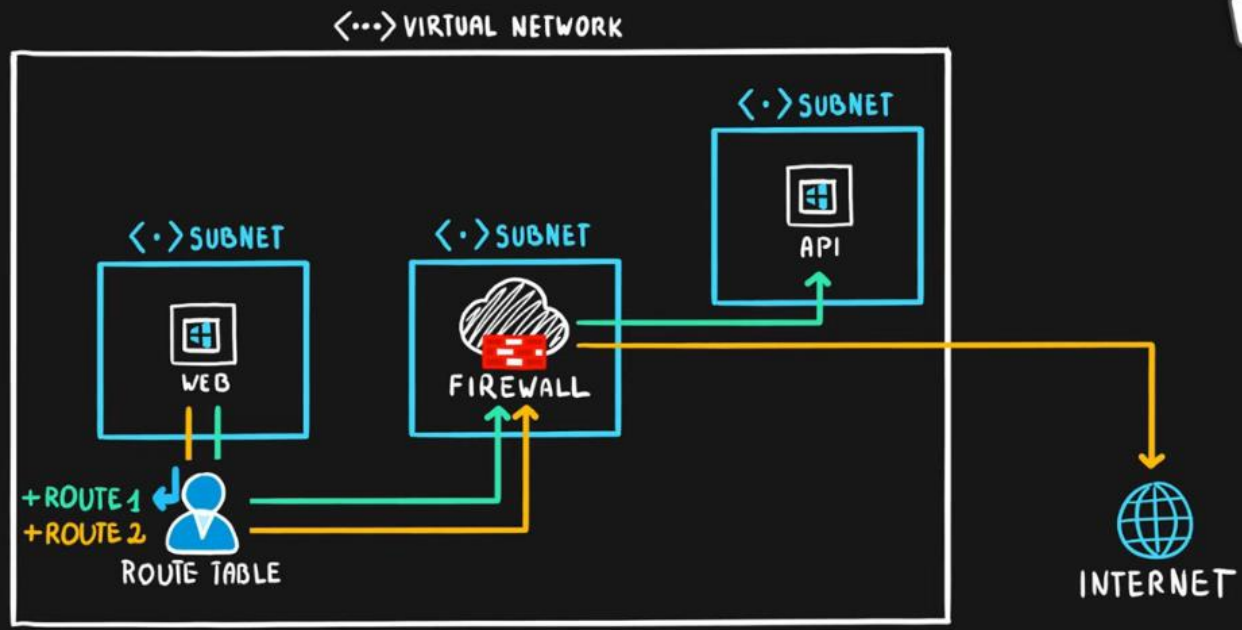
Azure VPN Gateway

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

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

Azure Firewall



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

Azure DNS

Is a Hosting Service

Manage DNS records using Azure Service

Resolvable Externally

MODULE 5: INTERSITE CONNECTIVITY

VNET PEERING

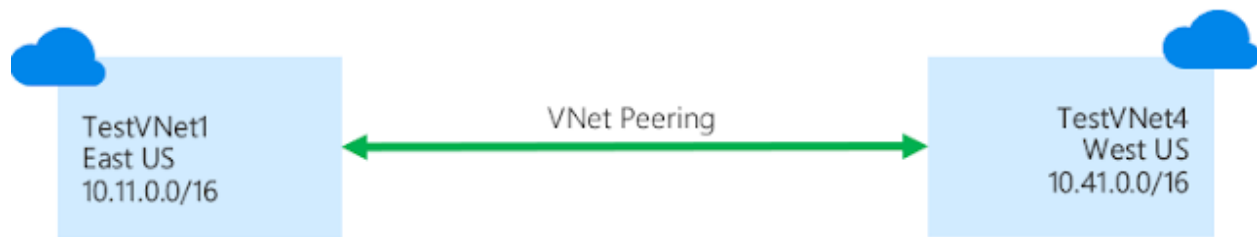
VPN GATEWAY CONNECTIONS

EXPRESSROUTE AND VIRTUAL WAN

Interconnectivity

Vnet Peering

Virtual Network Gateway



<...> Vnet Peering - Benefits

Private

Performance

Communication

No Disruption

Seamless

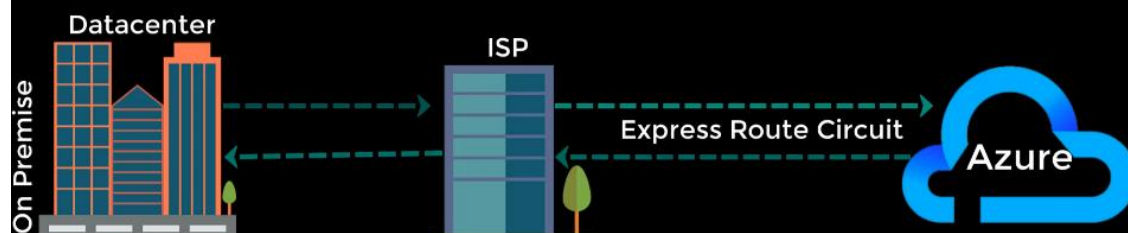
Express Route

Make your connections fast, reliable & private

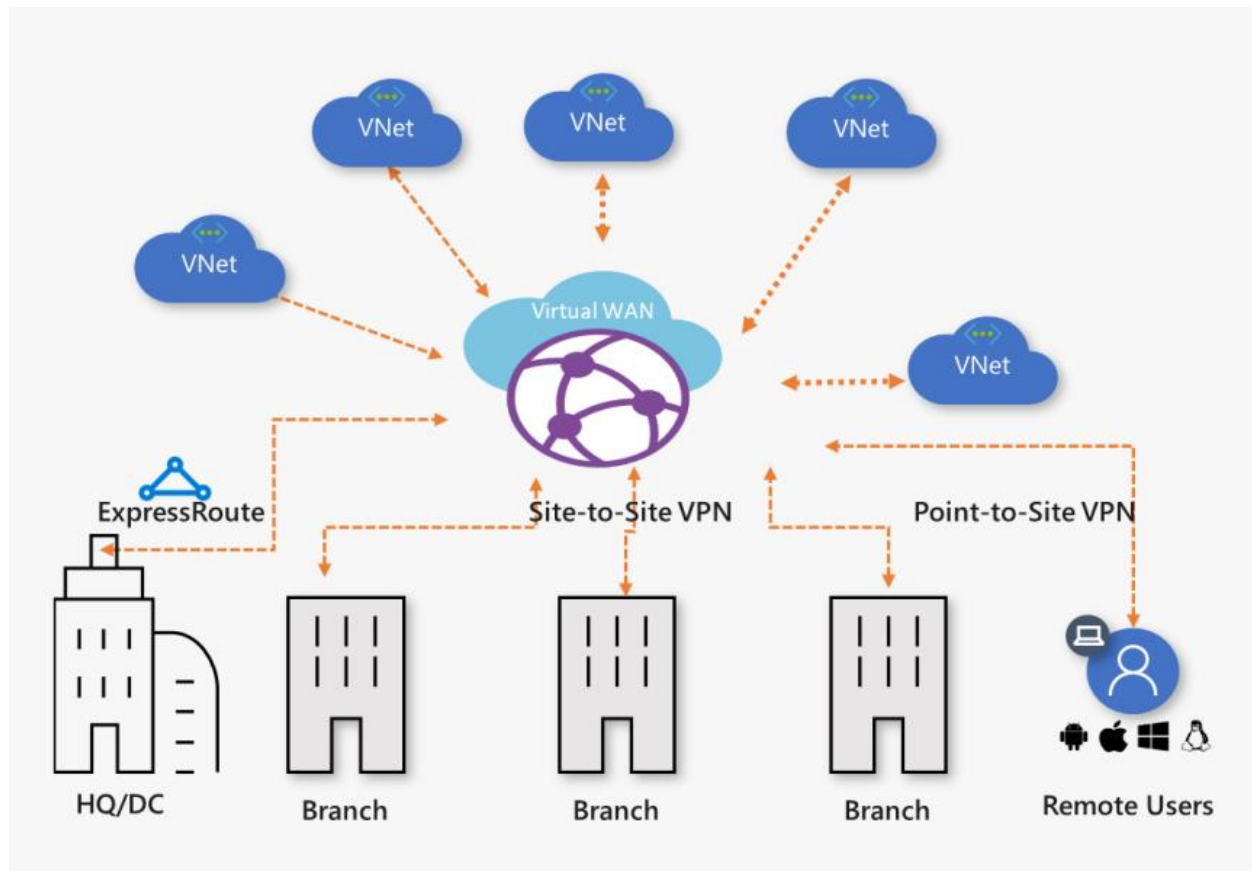
Use a Virtual private cloud for storage and recovery

Extend & Connect your datacenters

Build Hybrid Applications



VIRTUAL WAN



MODULE 6: NETWORK TRAFFIC MANAGEMENT
NETWORK ROUTING AND ENDPOINTS
AZURE LOAD BALANCER
APPLICATION GATEWAY
TRAFFIC MANAGER

Network Traffic Management

What is Azure Traffic Manager service?

Azure Traffic Manager is a

- **DNS-based traffic load balancer.**

Used to **distribute traffic** optimally to services while providing high availability and responsiveness.



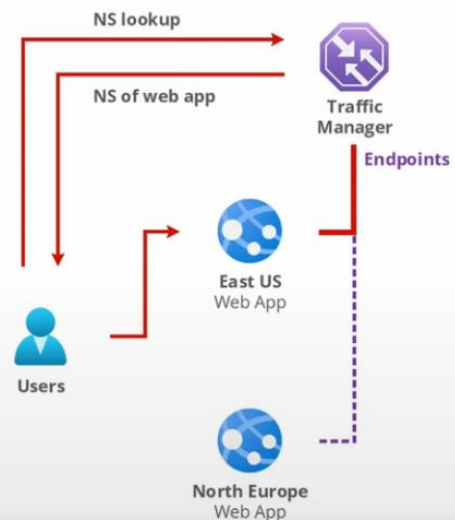
How it works?

Traffic Manager registers **endpoints**.

Endpoint is any Internet-facing service hosted inside or outside of Azure.

Traffic Manager uses **DNS** to direct traffic to **endpoint** based on

- **traffic-routing method** and
- **health** of the endpoints.



Routing methods

Performance designed for endpoints in **different geographic locations** and you want end users to use the "**closest**" endpoint in terms of the **lowest network latency**.

	North Europe Web App	East US Web App
Europe Users	18ms	78ms
Brazil Users	120ms	18ms



Routing methods

Weighted designed to distribute traffic across a set of endpoints, either evenly or according to weights, which you define.

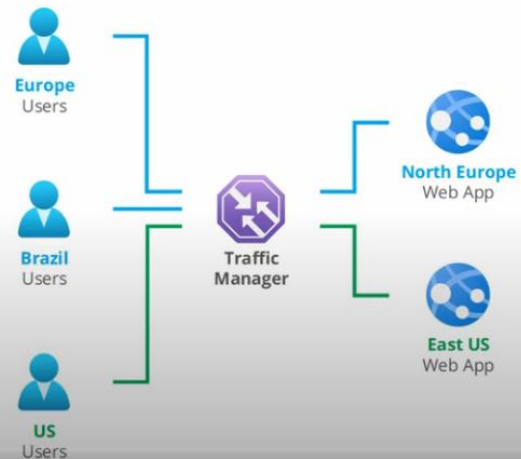
	North Europe Web App	East US Web App
Weight	1	9



Routing methods

Geographical designed to route users based on which **geographic location** their **DNS query originates from**.

	North Europe Web App	East US Web App
All Users	Global	
US Users		United States



Routing methods

Priority designed to route all user traffic based on priority.

	North Europe Web App	East US Web App
Priority	1	2
Health	Not Healthy	Healthy



Routing methods

Multivalue method getting multiple healthy endpoints in a single DNS query response.



Routing methods

Subnet method allows for mapping a set of end user IP address ranges to specific endpoints in a profile.

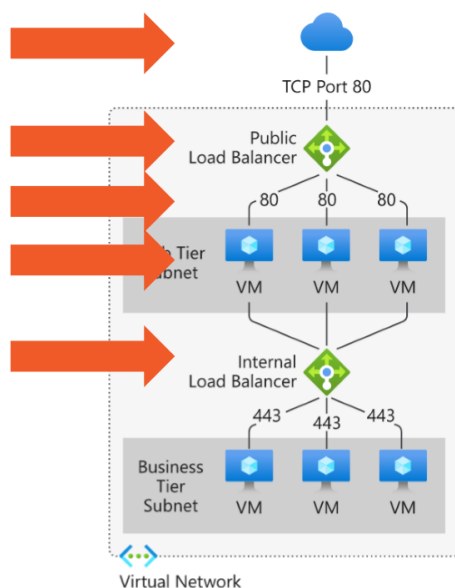


Additional features

Azure Traffic Manager additionally provides

- Endpoint monitoring
- Azure integrated endpoints
- Nested endpoints
- Traffic views
- Real user measurements
- Metrics and alerts

Load Balancer Use Cases



High availability



Scalable performance



Best consumer experience

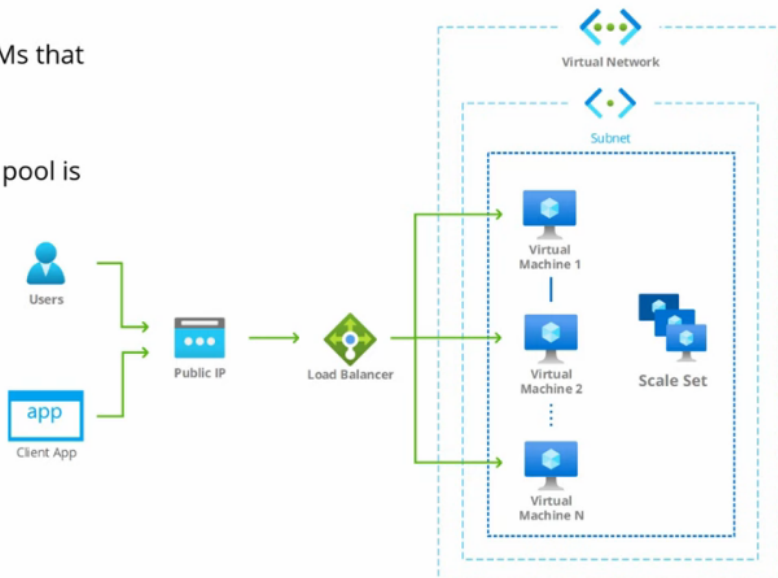
How it works?

Backend Pool is a group of VMs that will handle the request.

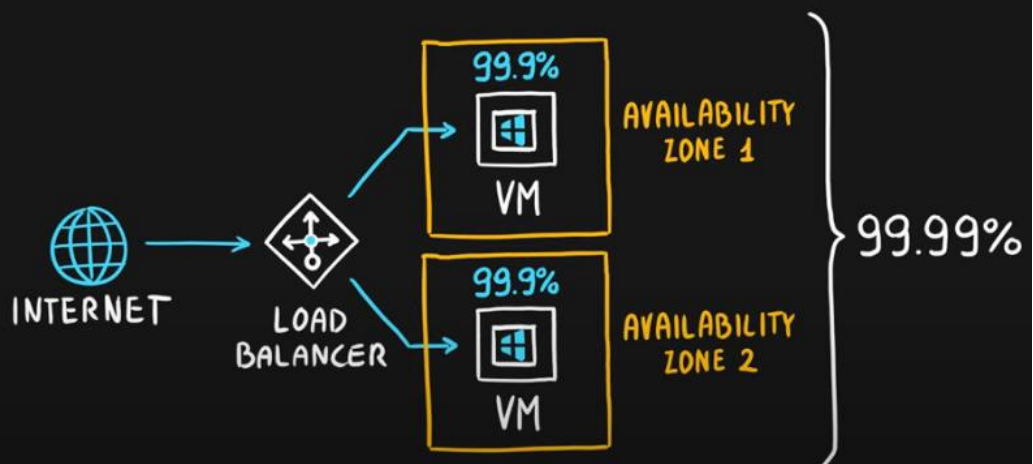
In case of **scale sets** backend pool is **updated automatically**.

A **static public** (virtual) **IP** can be assigned thus making it a **public load balancer**.

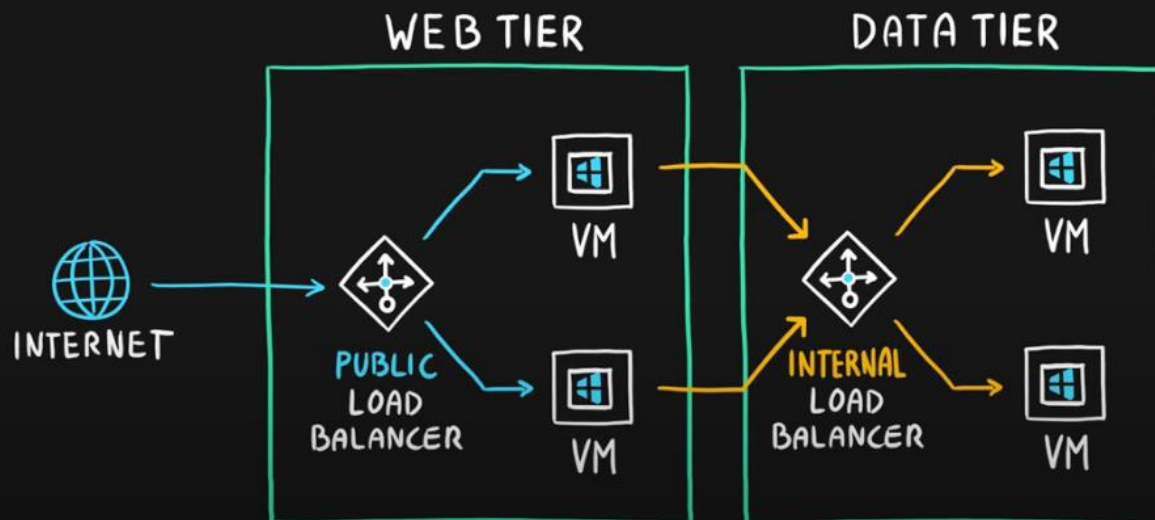
Otherwise for **private IP** it is **internal load balancer**.



Azure Load Balancer



Azure Load Balancer



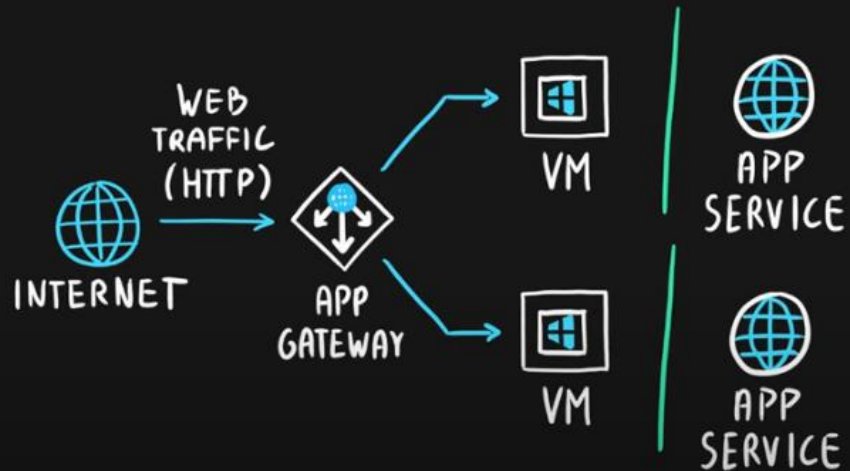
Azure Load Balancer



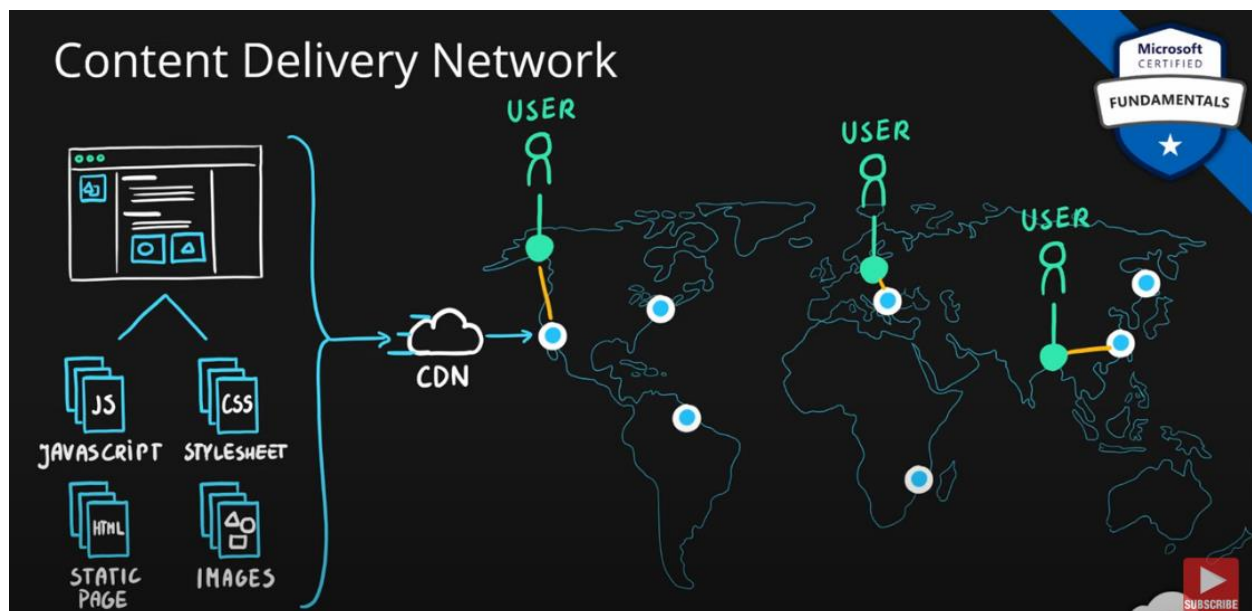
Key Characteristics

- 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

Azure Application Gateway



Content Delivery Network

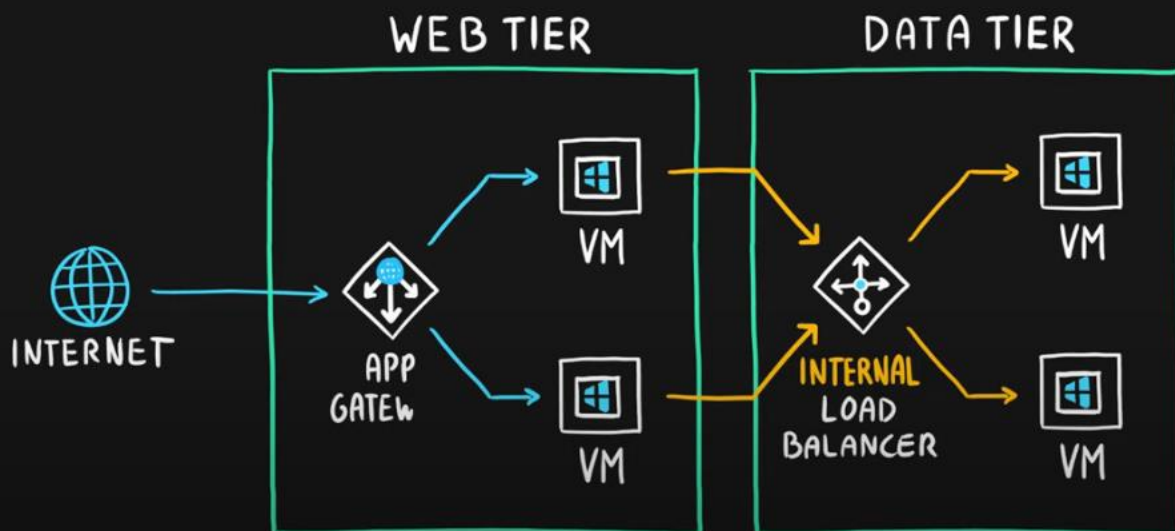


Content Delivery Network

Key Characteristics

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

Azure Application Gateway



Azure Application Gateway

Key Characteristics

- Web traffic load balancer
- Web application firewall
- Redirection
- Session affinity
- URL Routing
- SSL termination



Load Balancer terms

Typical terms for Load Balancers are

- **Frontend IP Configurations** – private or public IP
- **Backend pools** – group of servers
- **Health probes** – monitoring of backend pool health
- **Load balancing rules** – traffic distribution to backend pool
- **Inbound NAT rules** – binding of specific IP/port to specific instance in backend pool
- **Outbound rules** – control outgoing traffic

Azure Load Balancer SKUs

Basic	Standard
Backend pool: 300 instances	Backend pool: 1000 instances
Backend pool: Availability set, VMSS	Backend pool: Any VM in a single VNet
No availability zones	Availability zone-aware

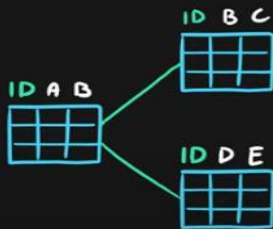
Azure LB SKU is not mutable

Azure Application Gateway	Azure Load Balancer
OSI Layer 7	OSI Layer 4
HTTP(S) workloads only	Any workload
Public and internal	Public and internal
Web Application Firewall (WAF)	
SSL/TLS offload	
Scalability	
Multi-site routing	
Path-based routing	

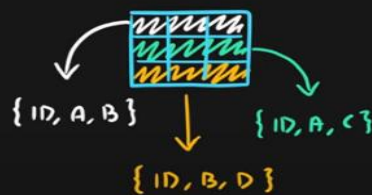
BLOB STORAGE
STORAGE SECURITY
AZURE FILES AND FILE SYNC
MANAGING STORAGE

Types of data

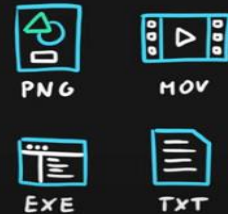
STRUCTURED



SEMI-STRUCTURED



UNSTRUCTURED



Azure Storage

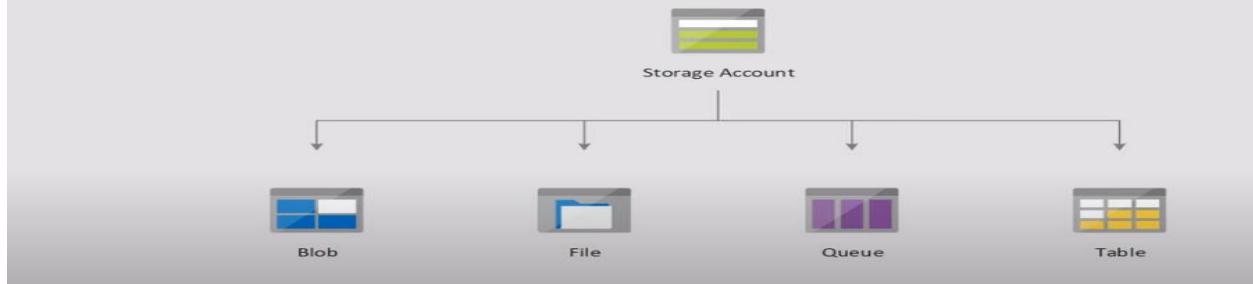
Azure Storage offers a massively scalable object store for **data objects**, a **file** system service for the cloud, a **messaging** store for reliable messaging, and a **NoSQL store**.

Azure Storage is

- Durable
- Secure
- Scalable
- Managed
- Accessible



Azure Storage



Azure Storage Accounts



Contains all Azure storage objects

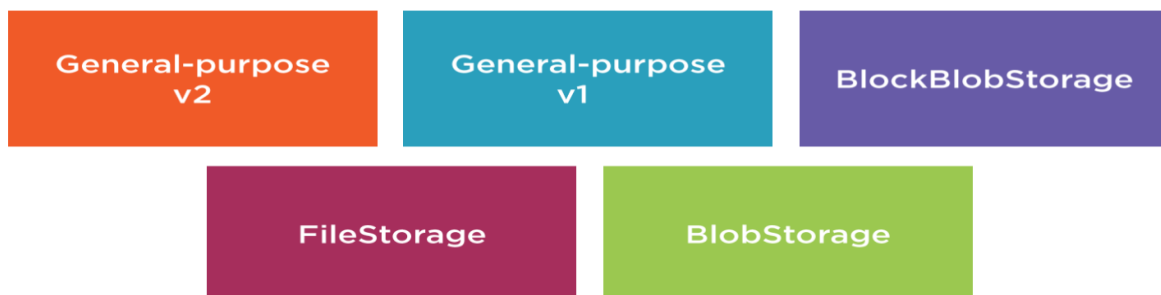
Unique namespace access to storage resources

- <https://stblobstorage001.blob.core.windows.net/demo/az-104-outline.pdf>

Highly Available

Secure and Scalable

Type of Storage Accounts



Access Tiers



Highest storage cost
Lower access cost



Lower storage cost
Higher access cost
30 day minimum



Lowest storage cost
Highest access cost
180 day minimum

Replication Options

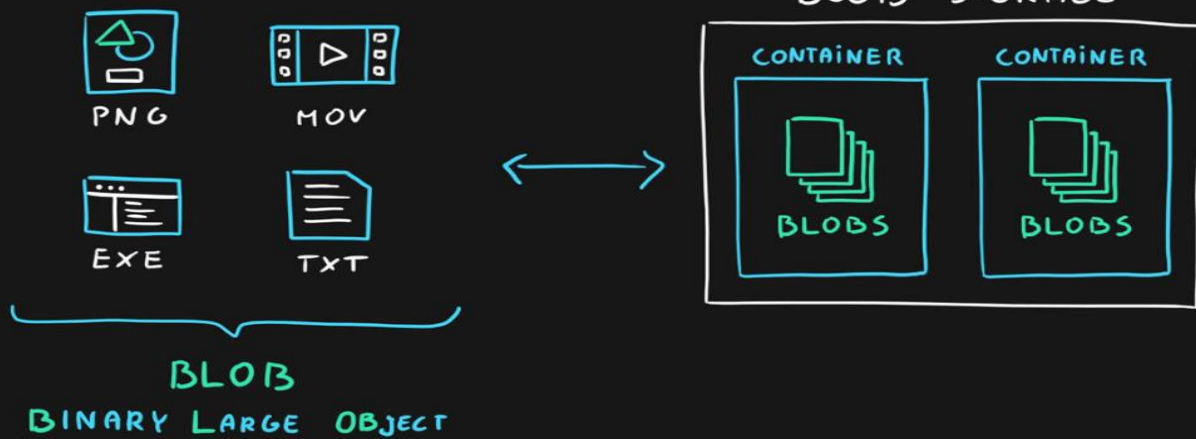


Replication



What if an Azure datacenter fails?
What if an Azure region fails?
Do you need Read access?

Azure Blob Storage



Azure Binary Large Objects (BLOB)

-  Unstructured data objects of various types
-  Support Hot, Cool, and Archive tiers
-  Supported in BlobStorage, General Purpose v1 and General Purpose v2 storage accounts
-  Support various replication options depending on Storage Account used

Blob Storage

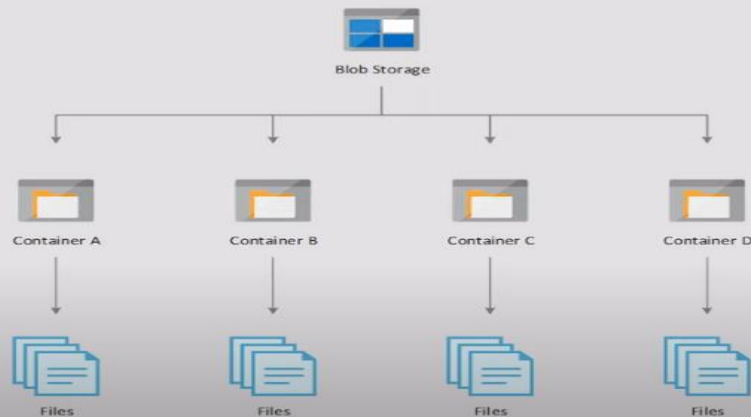
A massively scalable object store for text and binary data.

Ideal for

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.



Blob Storage



Blob Storage Access Tier

Azure Storage provides different options for accessing block blob data based on usage patterns.

- **Hot** - optimized for frequent access of objects
- **Cool** - optimized for storing large amounts of data that is infrequently accessed and stored for at least 30 days
- **Archive** - optimized for data that can tolerate several hours of retrieval latency and will remain in the Archive tier for at least 180 days



Blob Types in Azure



Block

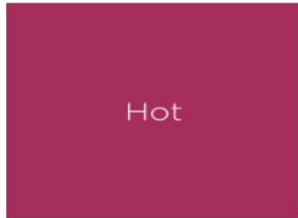


Append



Page

Access Tiers



Highest storage cost
Lower access cost



Lower storage cost
Higher access cost



Lowest storage cost
Highest access cost
Requires rehydration

Lifecycle Management



Automate tiering of Blob objects
Deploy with multiple tools
24 hrs to deploy

Azure Blob Storage

Key Characteristics

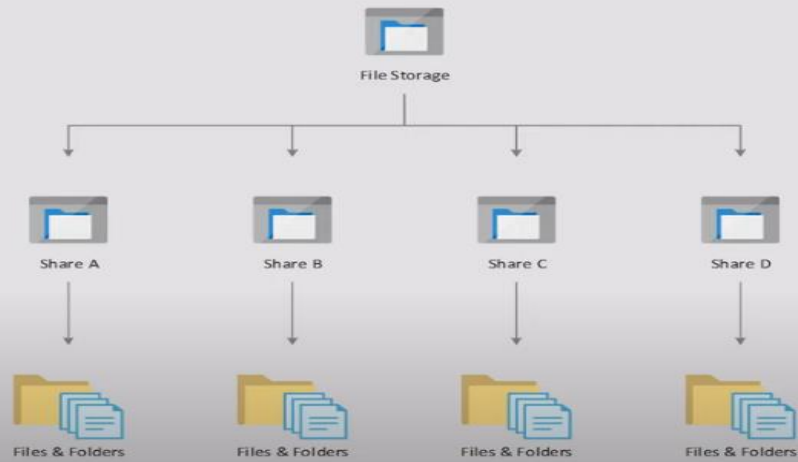
- Designed for storage of files of any kind (BLOB – Binary Large Object – file)
- Three storage tiers
 - Hot – frequently accessed data
 - Cool – infrequently accessed data (lower availability, high durability)
 - Archive – rarely (if-ever) accessed data

File Storage

Managed file shares for cloud or on-premises deployments.



File Storage



Storage Queue

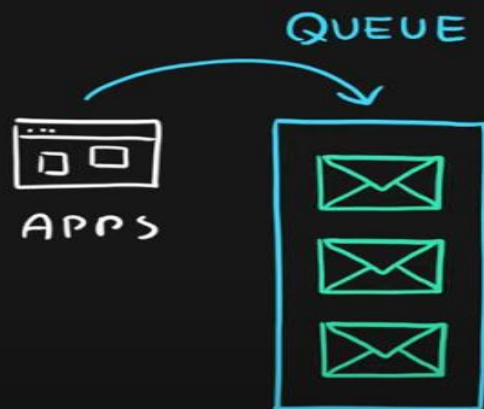
A messaging store for reliable messaging between application components.



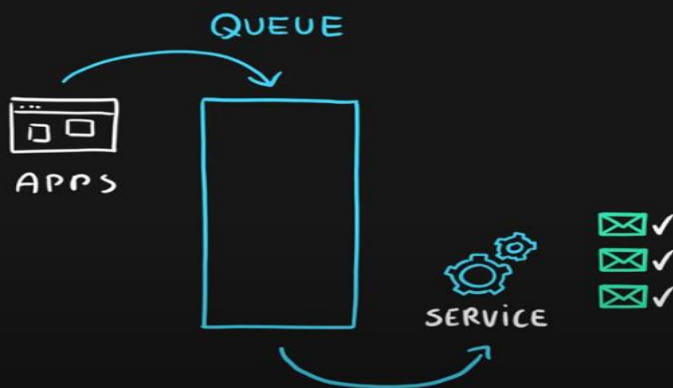
Azure Queue Storage



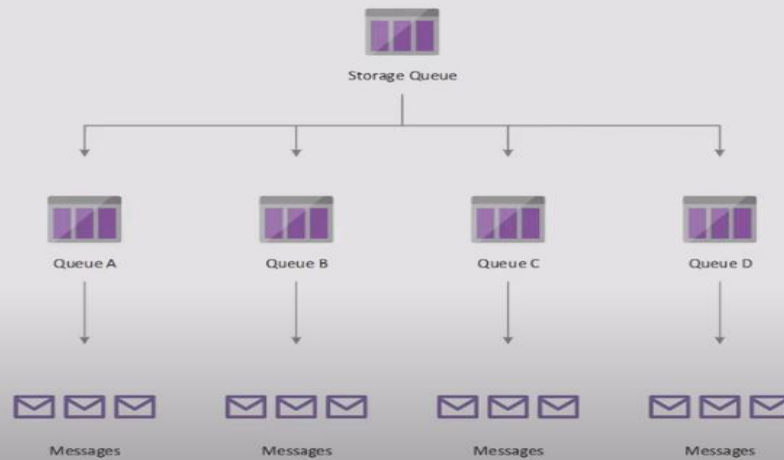
Azure Queue Storage



Azure Queue Storage



Storage Queue



Azure Queue Storage

Key Characteristics

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

Table Storage

A NoSQL store for schemaless storage of structured data.



Azure Table Storage

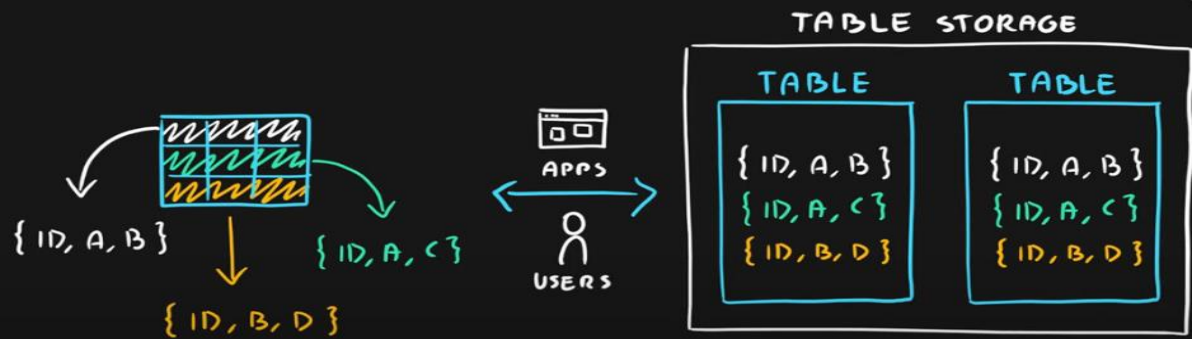
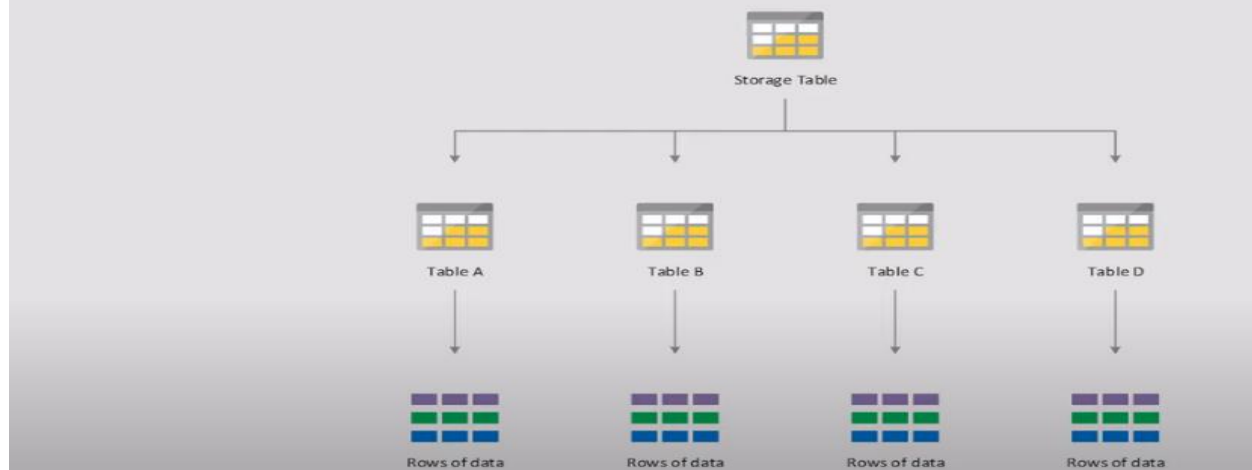


Table Storage



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

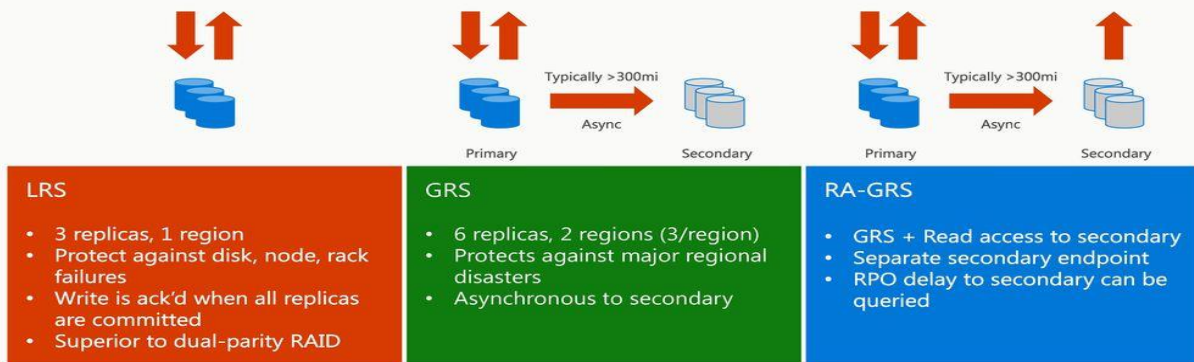
Storage Performance Tier

General-purpose storage accounts may be configured for either of the following **performance tiers**

- A **standard** performance tier for storing blobs, files, tables, queues, and Azure virtual machine disks.
- A **premium** performance tier for storing unmanaged virtual machine disks only.



Azure Storage Durability



Strong consistency, checksums/CRC and background scrubbing to preserve data integrity

MODULE 8: AZURE VIRTUAL MACHINES

VIRTUAL MACHINE PLANNING

CREATING VIRTUAL MACHINES

VIRTUAL MACHINE AVAILABILITY

VIRTUAL MACHINE EXTENSIONS

What is a Virtual Machine?

In computing, a **virtual machine (VM)** is an emulation of a computer system. **Virtual machines** are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.



What is Azure Virtual Machine service?

Azure **Virtual Machine** service provides

- **scalable,**
 - **on-demand,** with
 - **rich toolkit**
- virtual machine hosting environment.**



Benefits of Azure Virtual Machine



Easy development and test



Agility and scale



Enhanced performance



Pay-as-you-go pricing



Extended data center



Disaster recovery

©Simplilearn. All Rights reserved.

Virtual Machine Components

Operating System

It is one of the main components of Azure. Here, the OS creates connections to Remote Desktop Session Host



You can also set the OS disk size in the Virtual Machine so that the memory is not wasted

Few OS available for Azure Virtual Machine are – Ubuntu, RedHat, Linux, Windows Server Datacenter and CentOS

©Simplilearn. All Rights reserved.

Virtual Machine Components

Disks

Azure Virtual Machines use attached virtual hard disks (VHD) for storage. There are two types of VHDs:

Image: It is a template for the creation of a new Azure VM
Disks: It is a bootable VHD that can be used as a mountable disk for a VM



Page blobs back all the disks in Azure Storage and they inherit the benefits of blob storage

The disks are mounted as drives on the VM

© Microsoft. All rights reserved.

Virtual Machine Components

Virtual Network

On a physical infrastructure, many components operate the virtual machines in a scalable and secure manner

The components could include equipment such as separate network, load balancers, firewalls, and more



These components are deployed in an Azure Virtual Network

Azure Virtual Network provides many features like- Subnet, IP address, Load balancer and, Network security group

© Microsoft. All rights reserved.

Virtual Machine Components

Availability Sets

Sometimes, there is a slight chance that there could be a failure in physical servers

If in case a failure occurs, the Azure platform will migrate the failed VM to a healthy host server to reconstitute the VM



Hence, it is recommended to deploy at least two instances of the VM

VMs placed in an availability set should perform an identical set of functionalities

© Microsoft. All rights reserved.

How do I create my first Azure vm?

There are several ways of creating your Azure Virtual Machine:

It totally depends on the Environment you are working on for creating Azure vm:

- Azure Portal

It creates a Virtual Machine Running Windows as the portal

- Templates

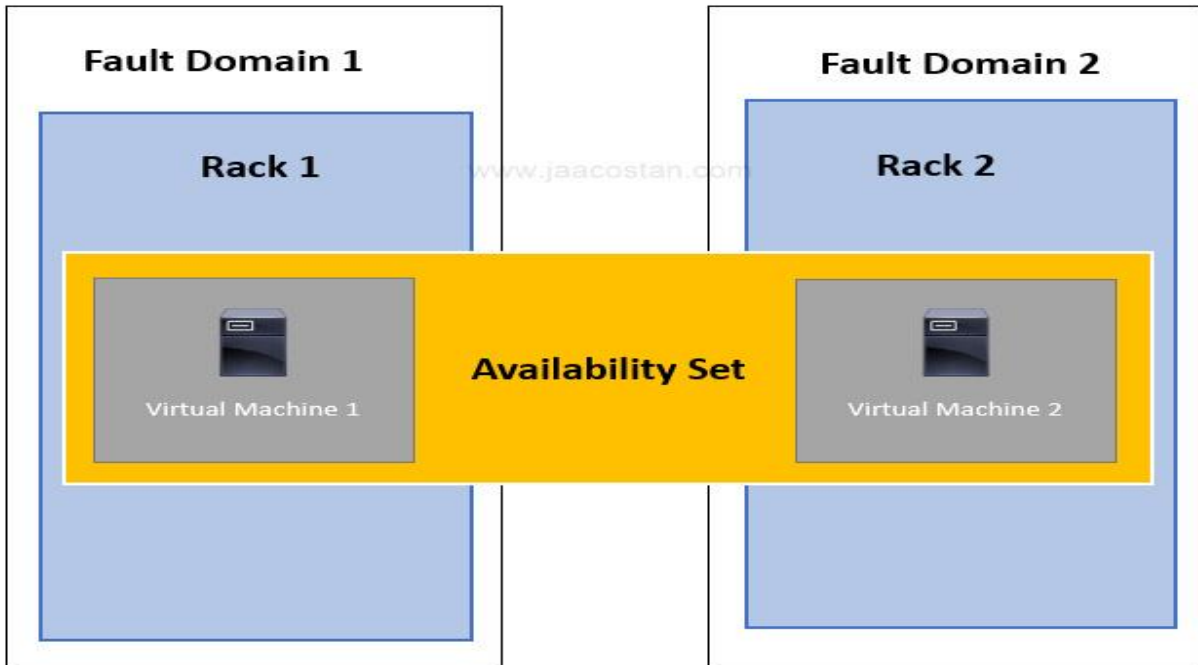
With the help of the Resource Manager Template a Windows Virtual Machine can be created

- Client Disks

By using C# one can deploy Azure Resources

- REST API's

Create or Update a Virtual Machine



Scale Sets

Identical VMs

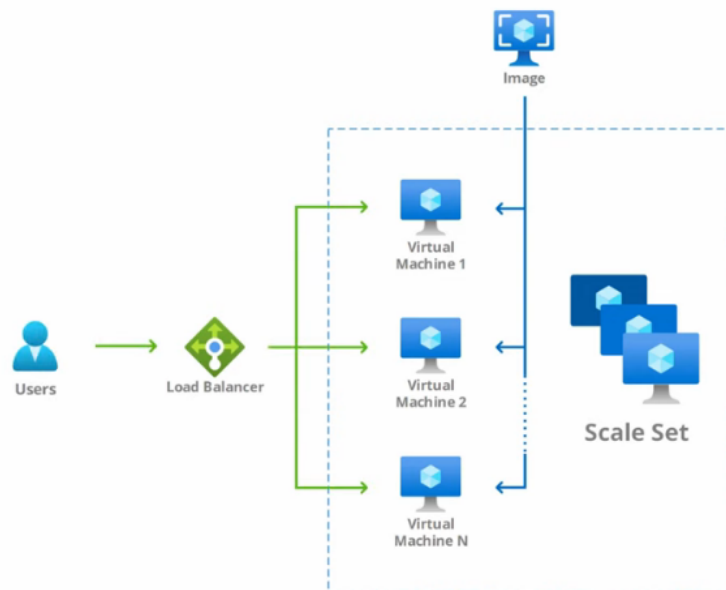
Scale sets are group of identical virtual machines created from the same image

Load balanced

Traffic to VMs is controlled by a load balancer

Auto-scaled

Number of VMs in Scale set is defined by auto-scaler rules based on schedule or demand



Availability Zones

Availability zone

Group of servers that has its own **cooling, power** and **networking** within Azure Region

Data center outages

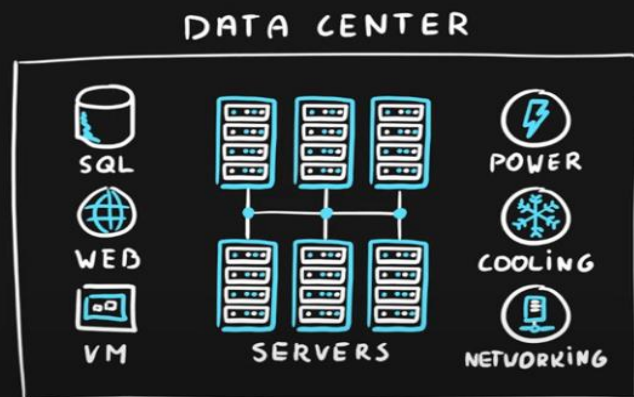
Availability zones protect virtual machines from data center outages



Data Center

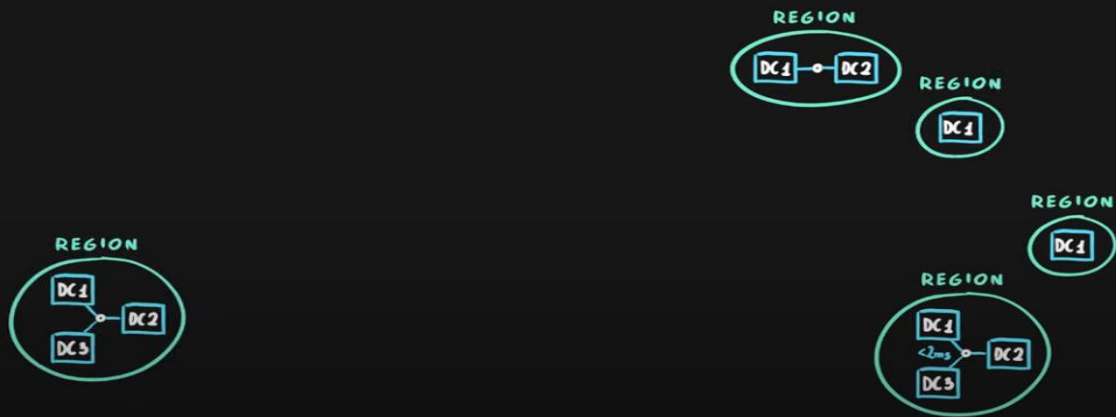
Key Characteristics

- Physical facility
- Hosting for group of networked servers
- Own power, cooling & networking infrastructure



Azure Infrastructure

Overview



Azure Infrastructure

Regions



Region

Key Characteristics

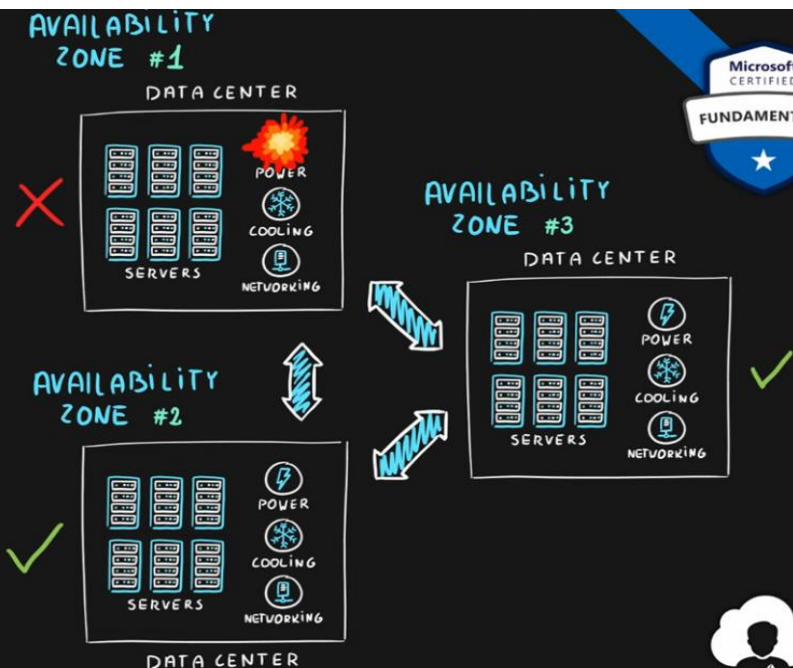
- Geographical area on the planet
- One but usually more datacenters connected with low-latency network (<2 milliseconds)
- Location for your services
- Some services are available only in certain regions
- Some services are global services, as such are not assigned/deployed in specific region
- Globally available with 50+ regions
- Special government regions (US DoD Central, US Gov Virginia, etc.)
- Special partnered regions (China East, China North)



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



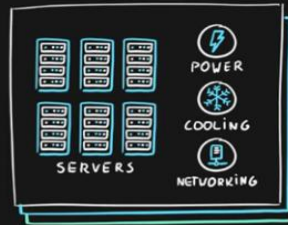
Availability Zone

Key Characteristics

- Not all regions are supported
- Supported region has three or more zones
- A zone is one or more data centers

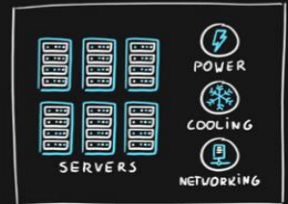
AVAILABILITY ZONE #1

DATACENTER



AVAILABILITY ZONE #2

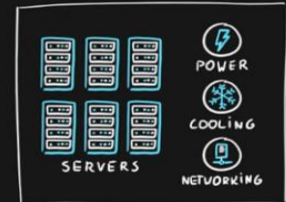
DATACENTER



DATACENTER

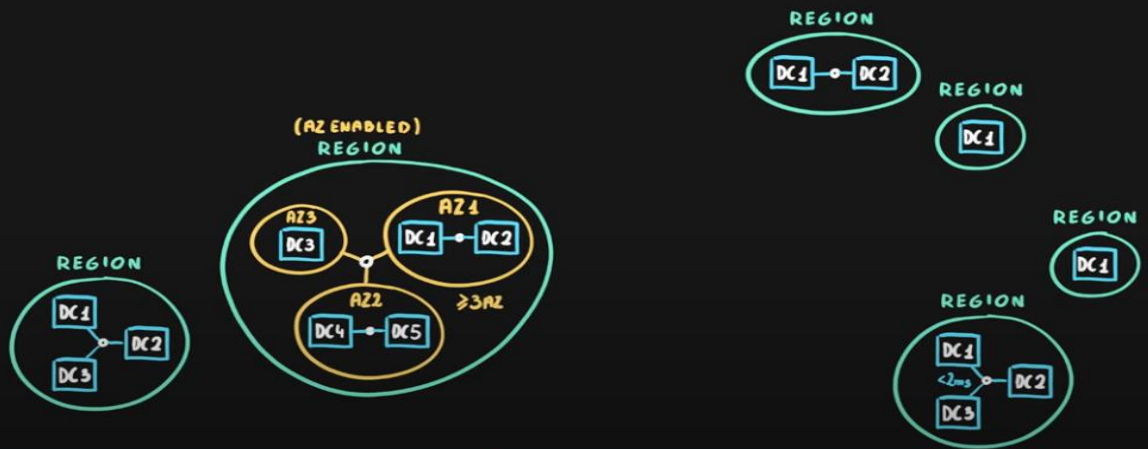
AVAILABILITY ZONE #3

DATACENTER



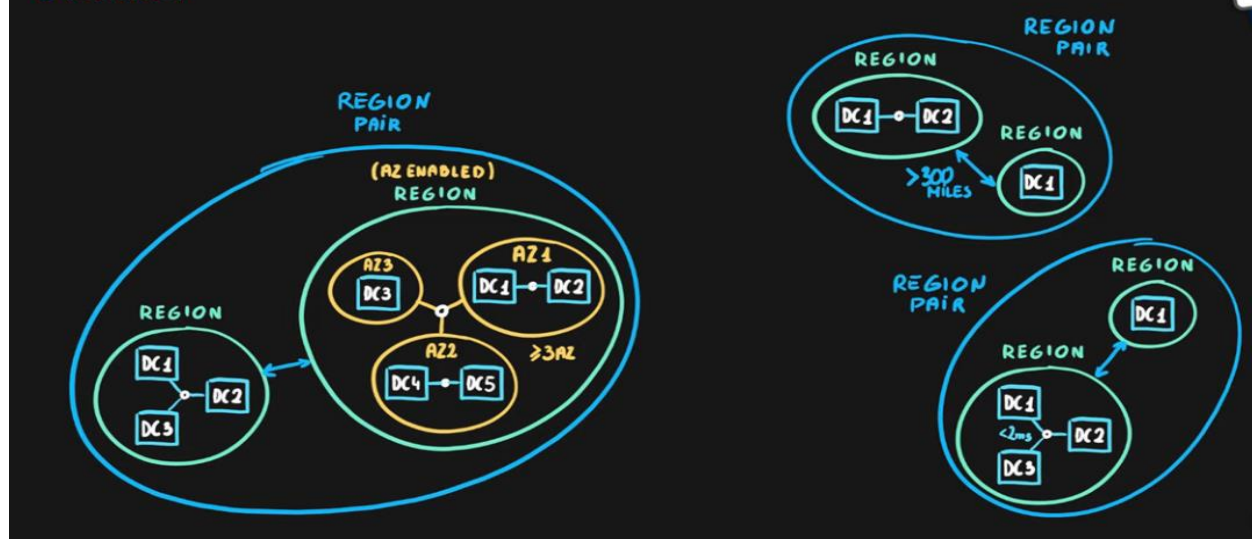
Azure Infrastructure Overview

Overview



Azure Infrastructure

Overview



Region Pairs

Key Characteristics

- Each region is paired with another region making it a region pair
- Region pairs are static and cannot be chosen
- Each pair resides within the same geography*
 - Exception is Brazil South
- Physical isolation with at least 300 miles distance (when possible)
- Some services have platform-provided replication
- Planned updates across the pairs
- Data residency maintained for disaster recovery

Region Pairs

Key Characteristics

Region Pair A

East US

UK West

North Europe (Ireland)

East Asia (Hong Kong)

Region Pair B

West US

UK South

West Europe (Netherlands)

Southeast Asia (Singapore)

Geographies

Key Characteristics

- Discrete market
- Typically contains two or more regions
- Ensures data residency, sovereignty, resiliency, and compliance requirements are met
- Fault tolerant to protect from region wide failures
- Broken up into areas
 - Americas,
 - Europe,
 - Asia Pacific,
 - Middle East and Africa
- Each region belongs only to one Geography

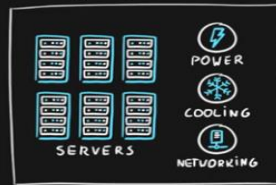
Availability Zone

Key Characteristics

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

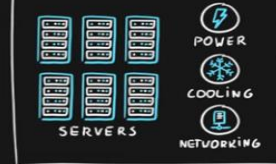
AVAILABILITY ZONE #1

DATACENTER



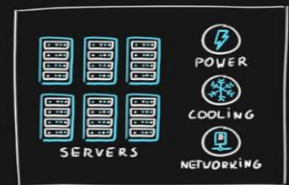
AVAILABILITY ZONE #2

DATACENTER



AVAILABILITY ZONE #3

DATACENTER



MODULE 9: SERVERLESS COMPUTING

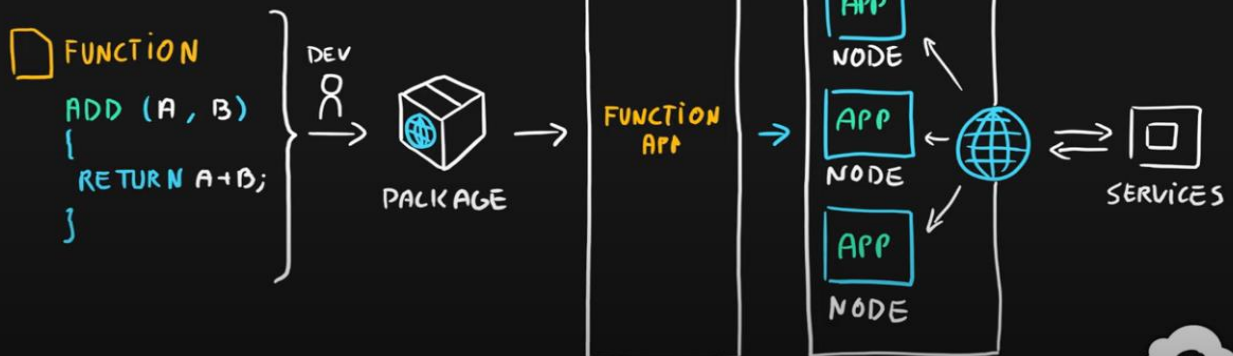
AZURE APP SERVICE PLANS

AZURE APP SERVICE

CONTAINER SERVICES

AZURE KUBERNETS SERVICE

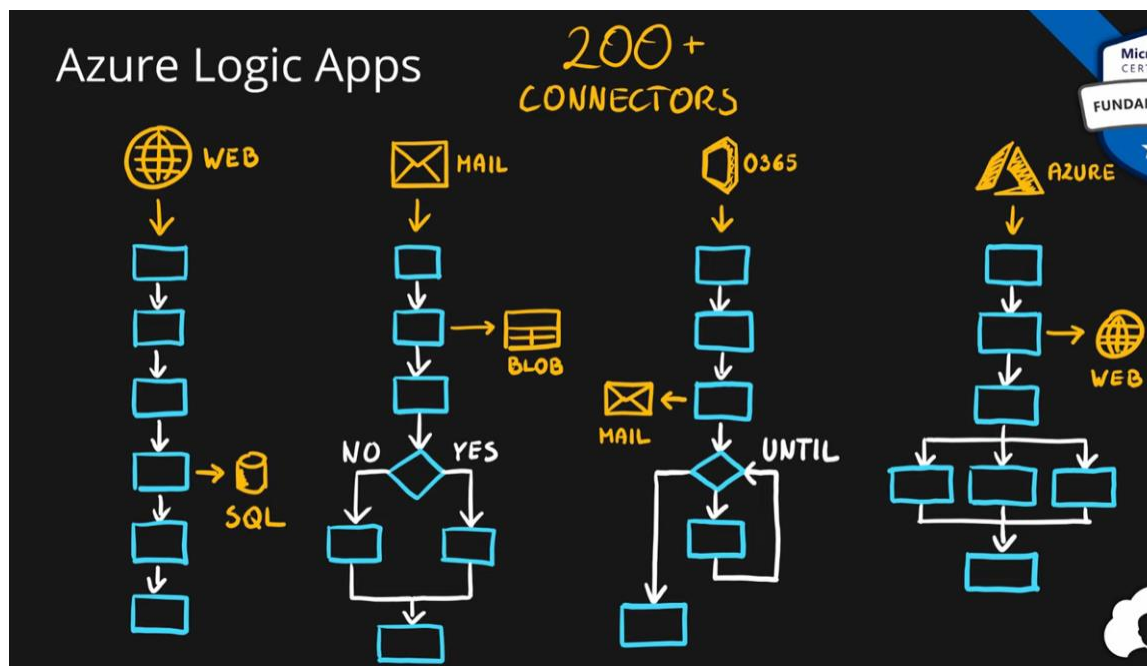
Azure Functions (Function Apps)



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.)

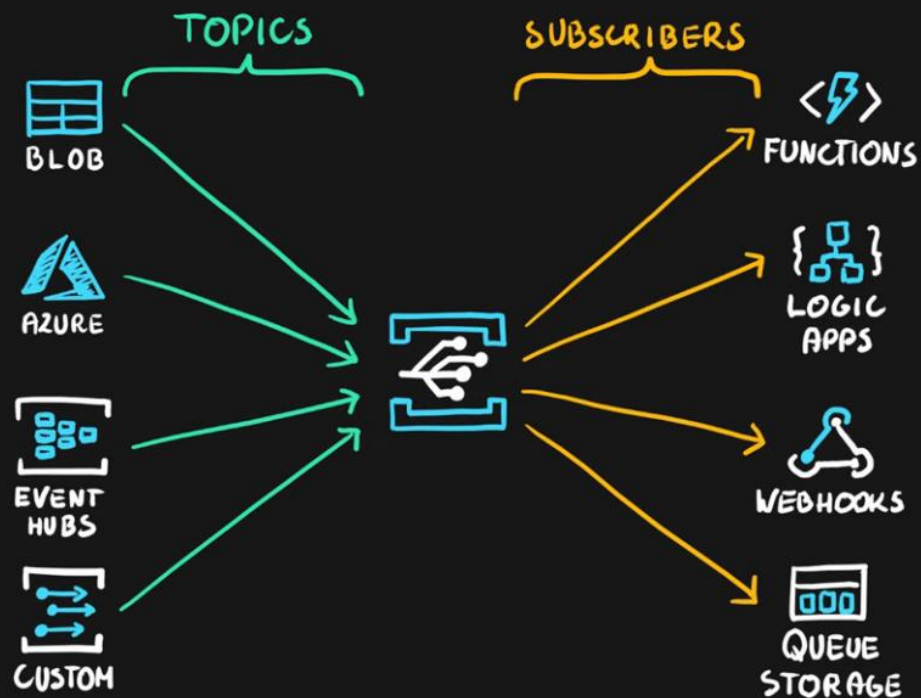


Azure Logic Apps

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 Serverless Services

Summary

- [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

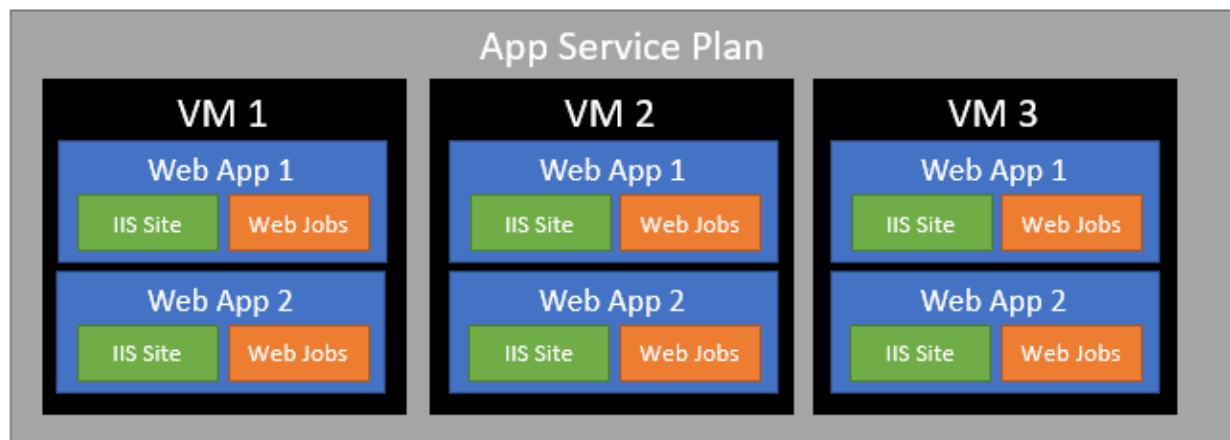
Azure App Service

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.

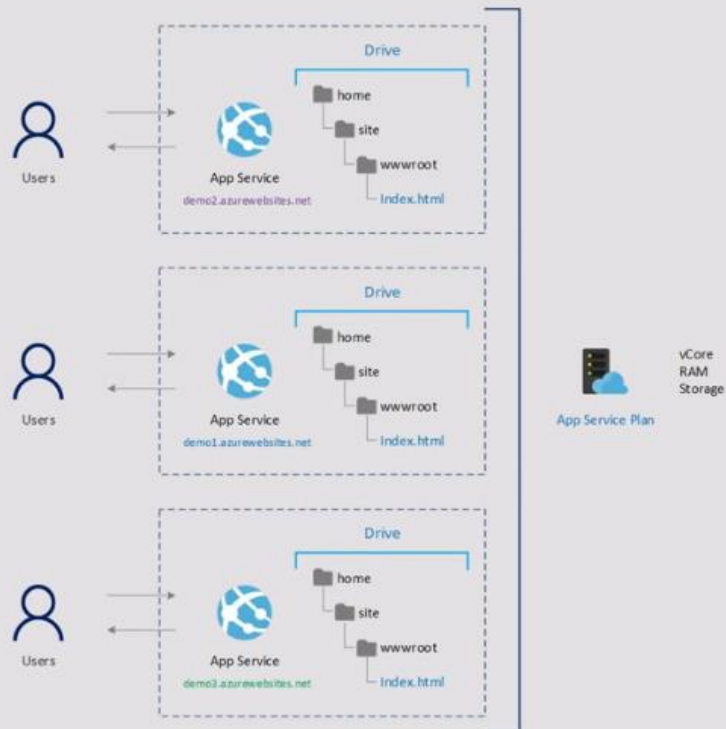
It offers **auto-scaling** and **high availability**, supports both **Windows** and **Linux**, and enables automated deployments from GitHub, Azure DevOps, or any Git repo.



Using App Service Plans to manage topology



Azure App Service Overview



Global scale with High Availability

- Guaranteed 99.95% availability for App Service
- Scale Up
- Scale Out

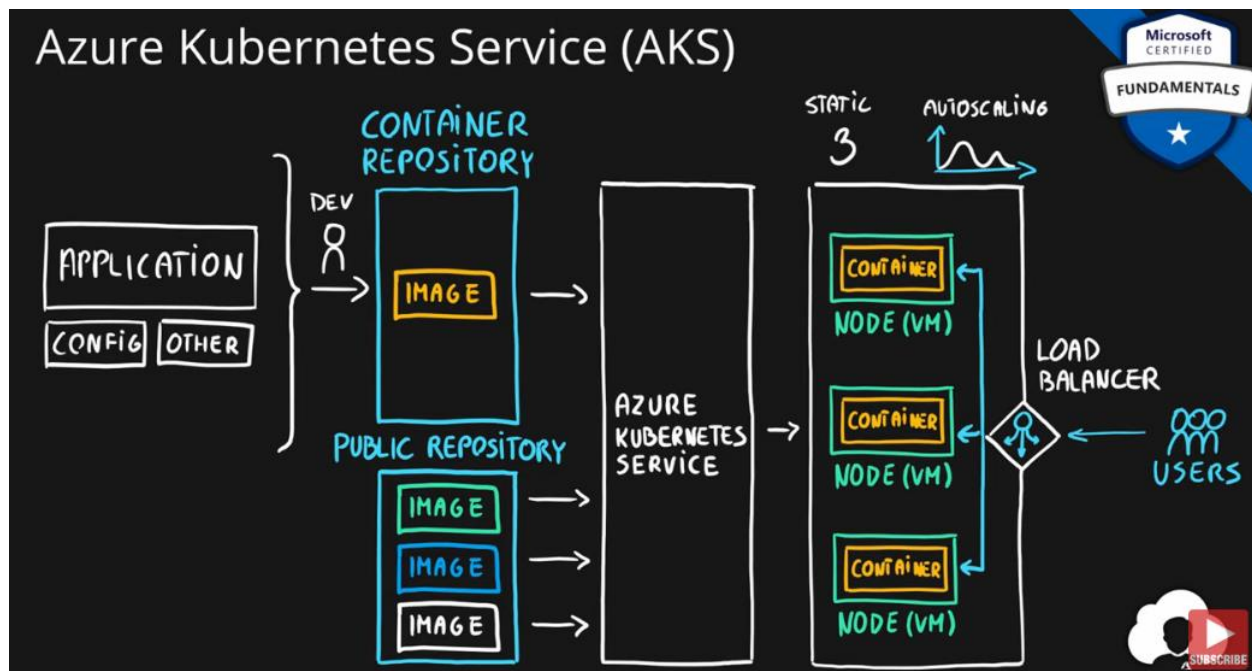


Other features

Other features include

- Security and compliance
 - ISO, SOC and PCI compliant
 - Authentication features with Azure AD and other Identity Providers like Google, Facebook, Twitter, Microsoft Live etc.
- Visual Studio Integration
- API and mobile features including CORS and push notifications
- And many others...

Azure Kubernetes Service (AKS)



Azure Kubernetes Service (AKS)

Key Characteristics

- Open-source container orchestration platform
- Platform as a Service
- Highly scalable and customizable
- Designed for high scale container deployments (anything really!)

MODULE 10: DATA PROTECTION
FILE AND FOLDER BACKUPS
VIRTUAL MACHINE BACKUPS

Data Protection

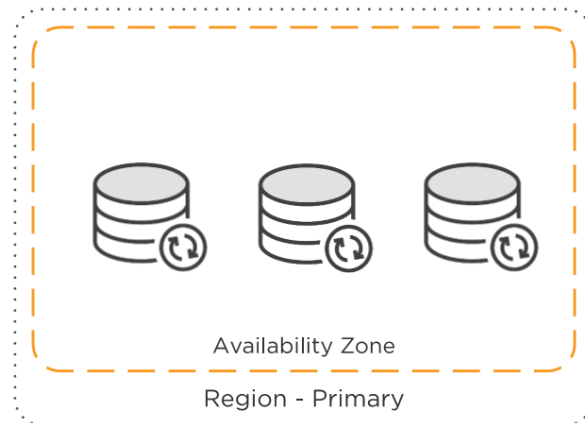
Data Redundancy

Azure Storage replicates multiple copies of your data.

Replication options for a storage account include:

- Locally-redundant storage (**LRS**)
- Zone-redundant storage (**ZRS**)
- Geo-redundant storage (**GRS**)
- Read-access geo-redundant storage (**RA-GRS**)

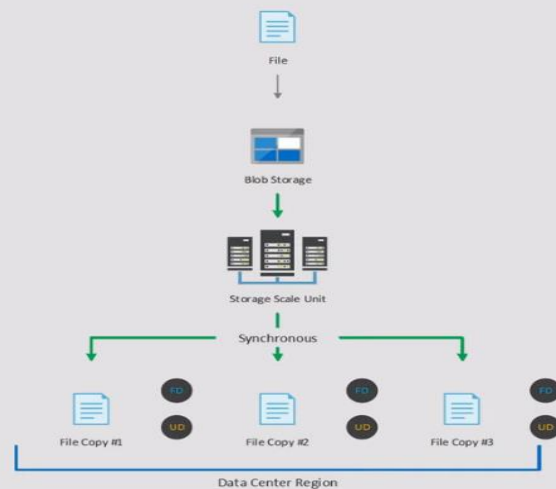
Local-Redundant Storage (LRS)



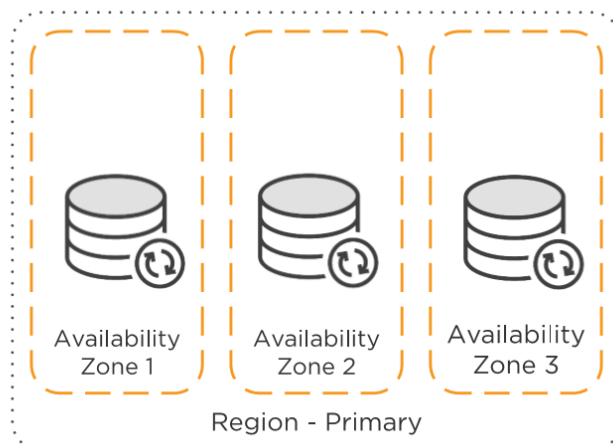
Locally-redundant storage (LRS)

A simple, low-cost replication strategy.

Data is replicated within a single storage scale unit.



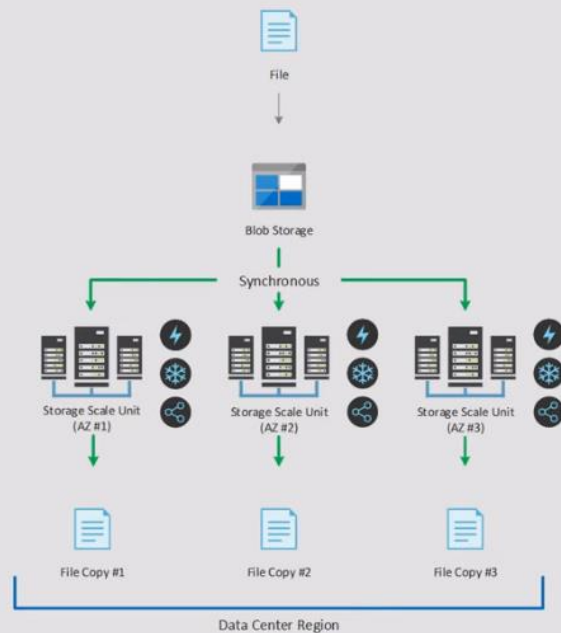
Zone-Redundant storage (ZRS)



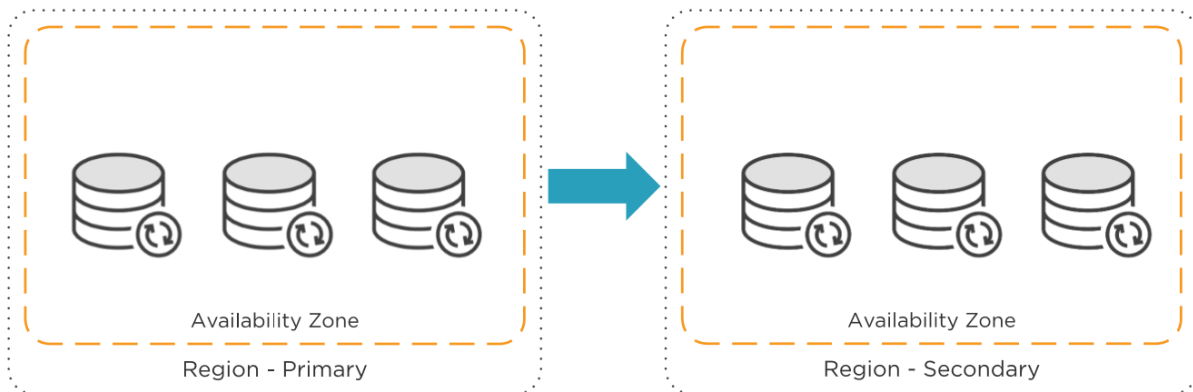
Zone-redundant storage (ZRS)

Replication for high availability and durability.

Data is replicated synchronously across three availability zones.

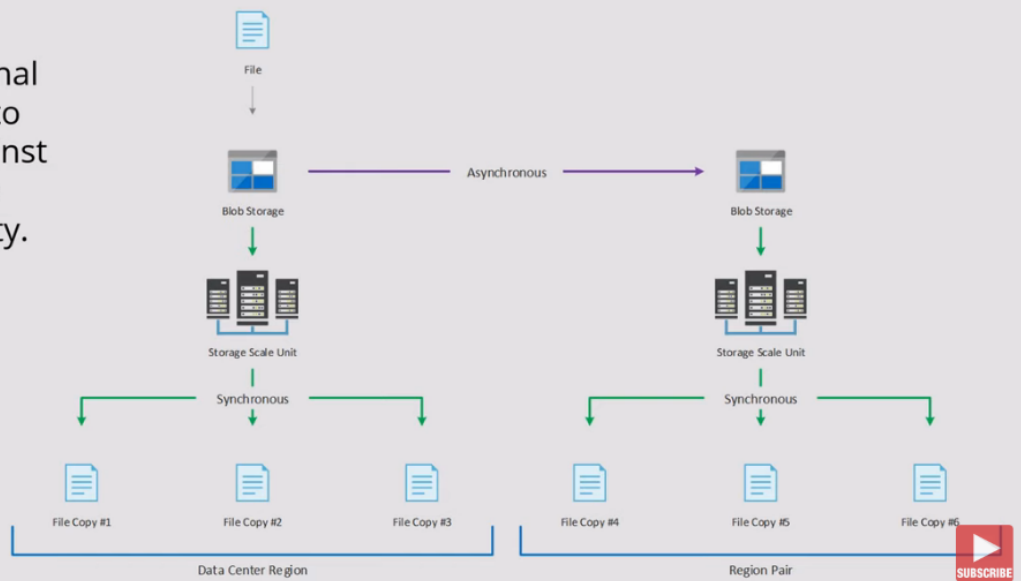


Geo-Redundant Storage (GRS)



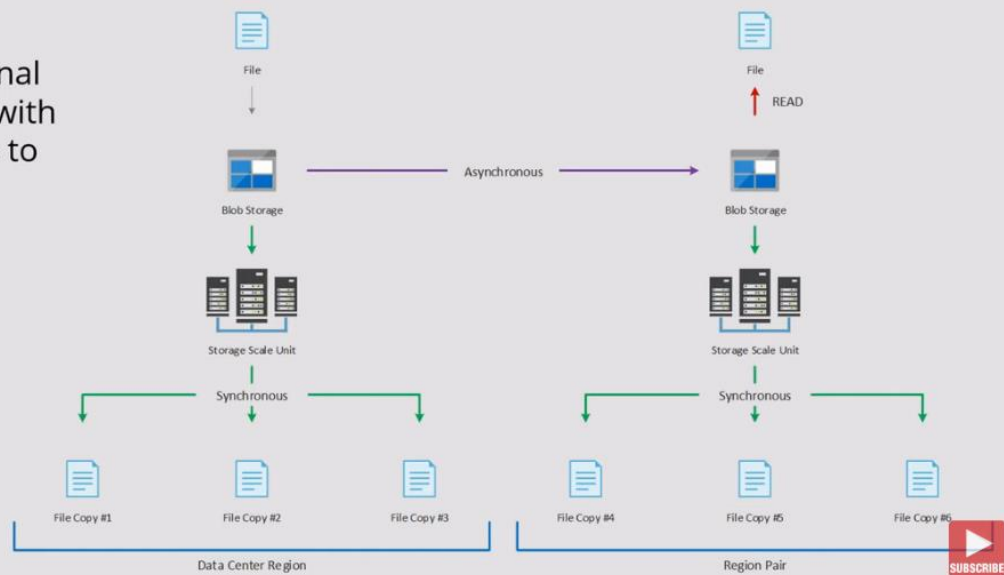
Geo-redundant storage (GRS)

Cross-regional replication to protect against region-wide unavailability.

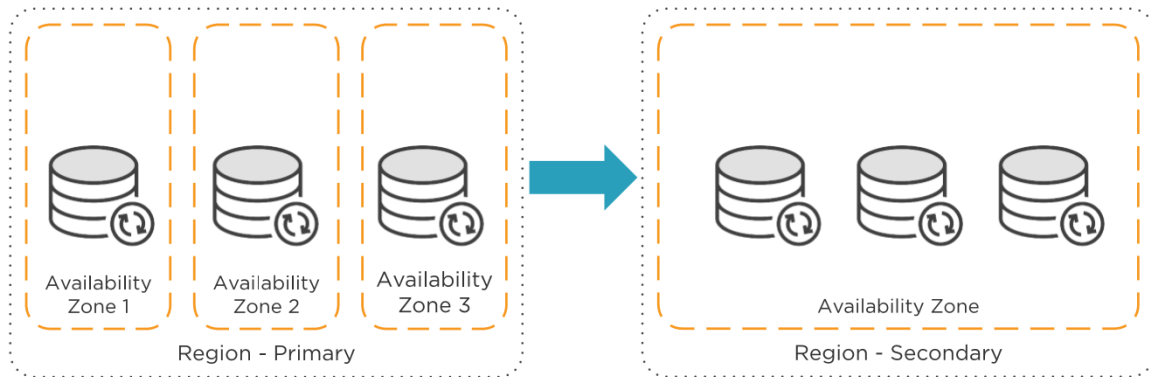


Read-access geo-redundant storage (RA-GRS)

Cross-regional replication with read access to the replica.



Geo-Zone-Redundant Storage (GZRS)



Read Access in a Secondary Region



Read-Only without failover

Applications can use secondary storage

Available in Geo-redundant storage

Read-Access Geo-Redundant Storage (RA-GRS)

Read-Access Geo-Zone-Redundant Storage (RA-GZRS)

Append *-secondary* to storage account name

<https://<StorageAcctName>-secondary.blob.core.windows.net>

Storage Security

Encryption

Authentication

Data in Transit

Disk Encryption

Shared Access Signatures (SAS)

Data Storage Authorization



Anonymous

- Azure blobs only

Authenticated

- Shared Key authorization
- Shared Access Signatures (SAS)
- Azure AD

Shared Access Key Authorization



- Access to entire storage account
- Protect from view
- Regenerate keys
- Consider Azure AD instead
- Use Azure Key Vault

Shared Access Signatures (SAS)



User Delegation



Service



Account

Shared Access Signatures

Use Case

Grant Permissions for specified duration

Granting permissions to Blobs ONLY

Give READ permissions ONLY

Allow access from a particular network range

Use HTTPS ONLY

Generate
Shared Access
Signatures

Provide time-limited access to resources in a storage account.

Allow granular permissions

Can be applied at storage account or data object level

Generate SAS keys in multiple tools

Be familiar with generating and applying SAS keys

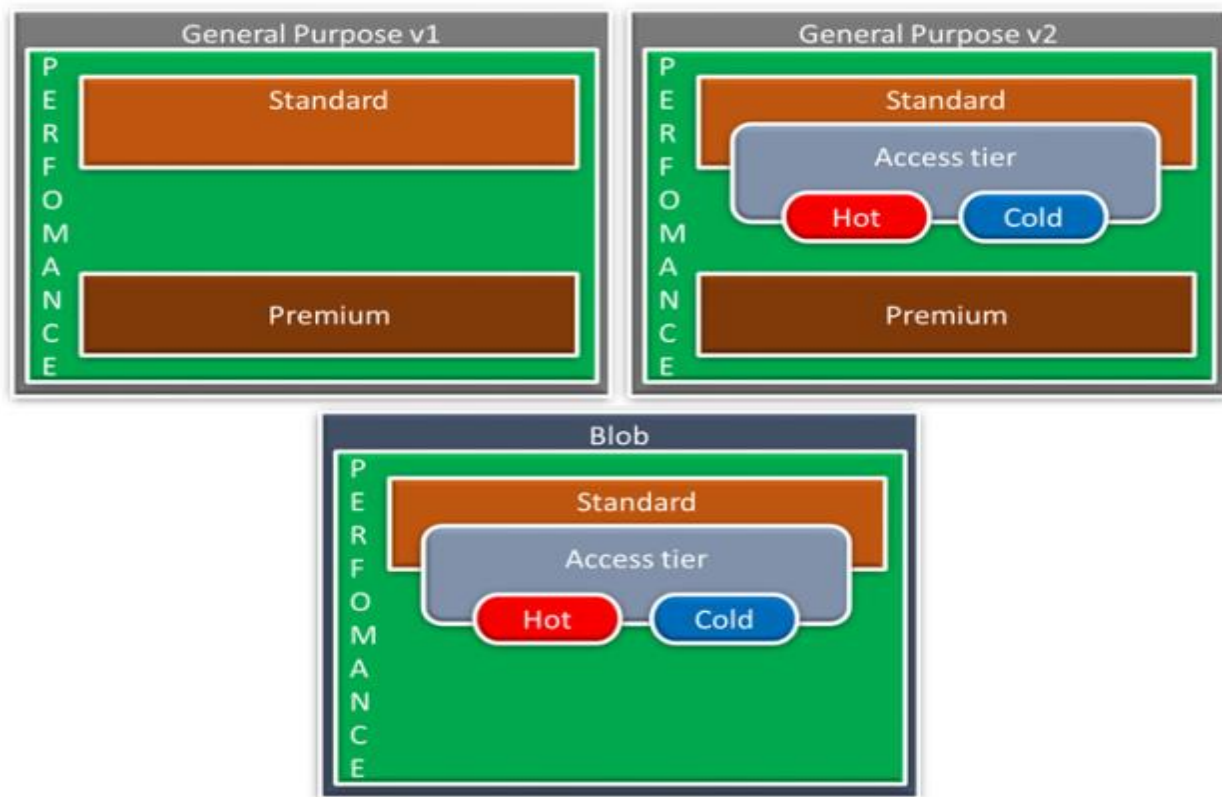
Azure AD Authorization



Supported for Blob and Queue storage

Uses role-based access control (RBAC)

Microsoft recommended approach



Azure Storage Accounts Explained

- General Purpose v1
 - Only support Hot Storage
 - No 'Cool' or 'Archival' storage
 - Higher storage costs
 - Lower transaction costs
- General Purpose v2
 - Support Hot/Cool/Archival Storage
 - Lower storage costs
 - Higher transaction costs
- Blob (Legacy)
 - Support Hot/Cool/Cold Storage
 - Only support Block blobs (not page blobs)
 - Almost identical pricing to GPv2
 - Migrate to GPv2

Azure Files

Key Service Characteristics

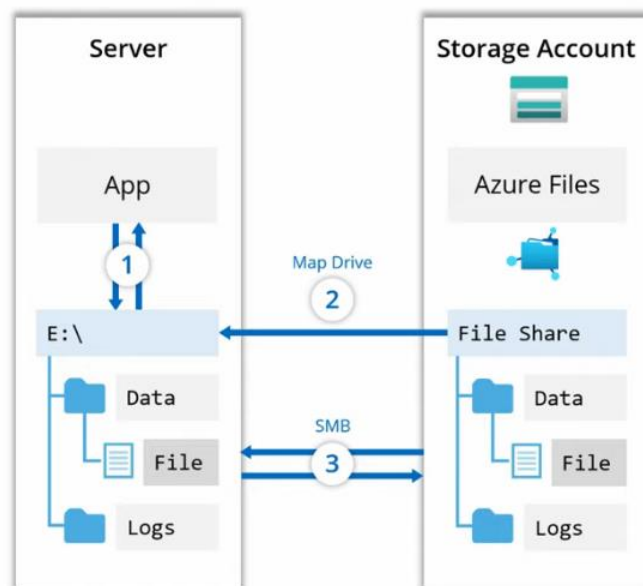
- Fully managed file shares in the cloud accessible via
 - SMB (Server Message Block)
 - HTTP (FileREST)
- Subservice of Azure Storage Account



Azure Files

Common Scenarios

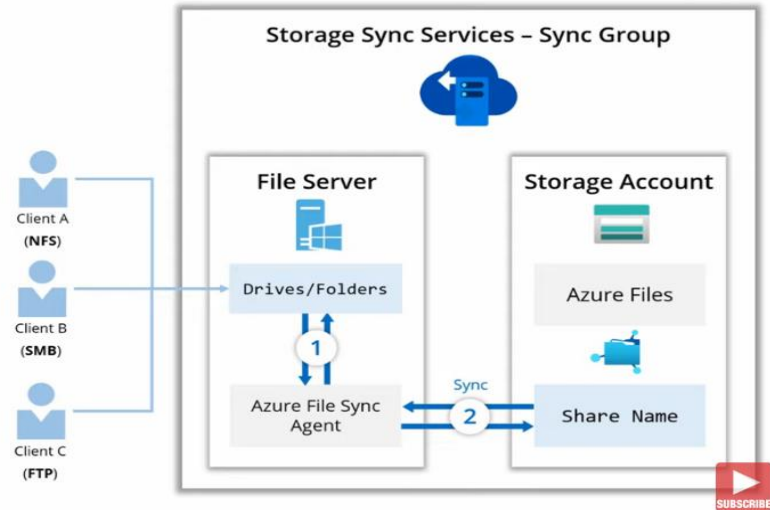
- "Lift and shift" applications



Azure Files

Common Scenarios

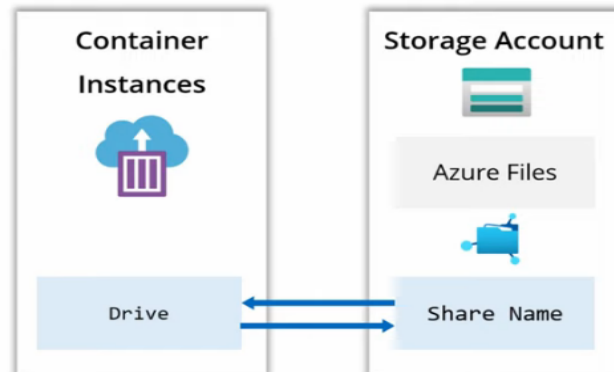
- "Lift and shift" applications
- Replace/extend on-premise servers as a cache with Azure File Sync



Azure Files

Common Scenarios

- "Lift and shift" applications
- Replace/extend on-premise servers as a cache with Azure File Sync
- Persistent Storage for containers

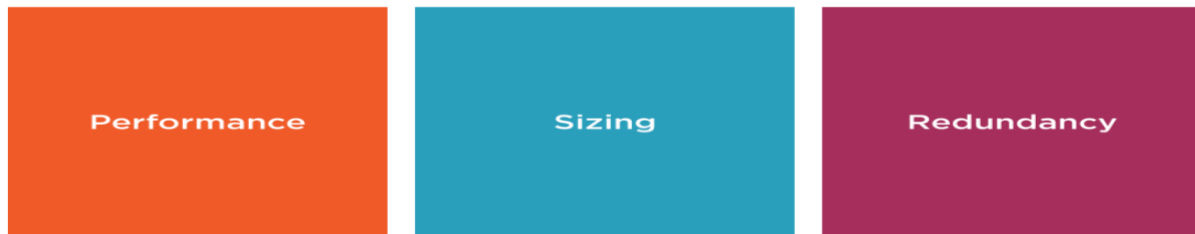


Azure File Share

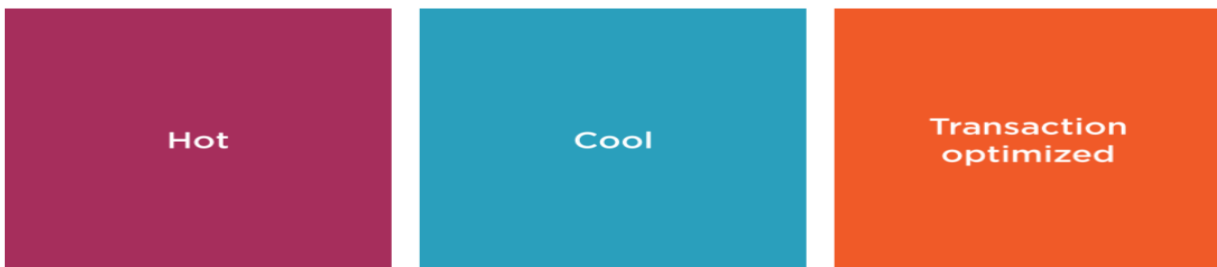


- Cloud-based SMB or NFS file share
- Accessible from Windows, MacOS, and Linux
- Clients use port 445
- Supported in GPv1, GPv2 and FileStorage Storage Accounts
- Replication available depending on Storage Account

Azure File Share Requirements



Azure Files Access Tiers



Authentication



Azure Active Directory Domain Services and Active Directory Domain Services

- Provides identity-based access for hybrid environments
- Allows granular share-level and file-level permissions
- Recommended best practice

Storage Account Key or Shared Access Signature

- Less granular control
- Secure the keys

Azure File Sync



Provides an on-premises caching solution on Windows Server

Replicates data between on-premises datacenters and Azure

Integrates with Azure File Shares

Seamless integration into file share infrastructure

Includes tools for managing cached data

Azure File Sync Management Components



Cloud Endpoint
Azure File Share

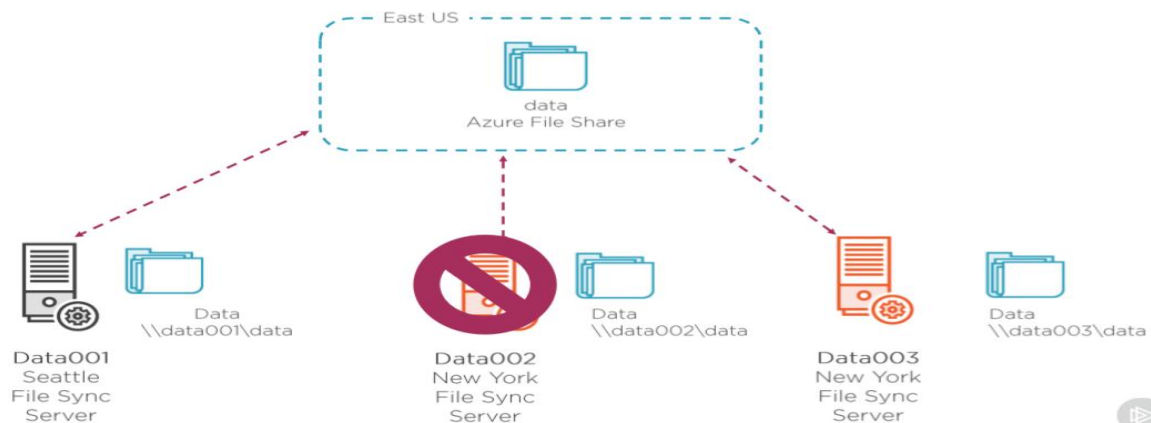


Server Endpoint



Sync Group

Azure File Sync In Action



Deploying Azure File Sync



Deploy the Storage Sync Service



Create a sync group and cloud endpoint



Install the Azure File Sync agent on Windows Servers

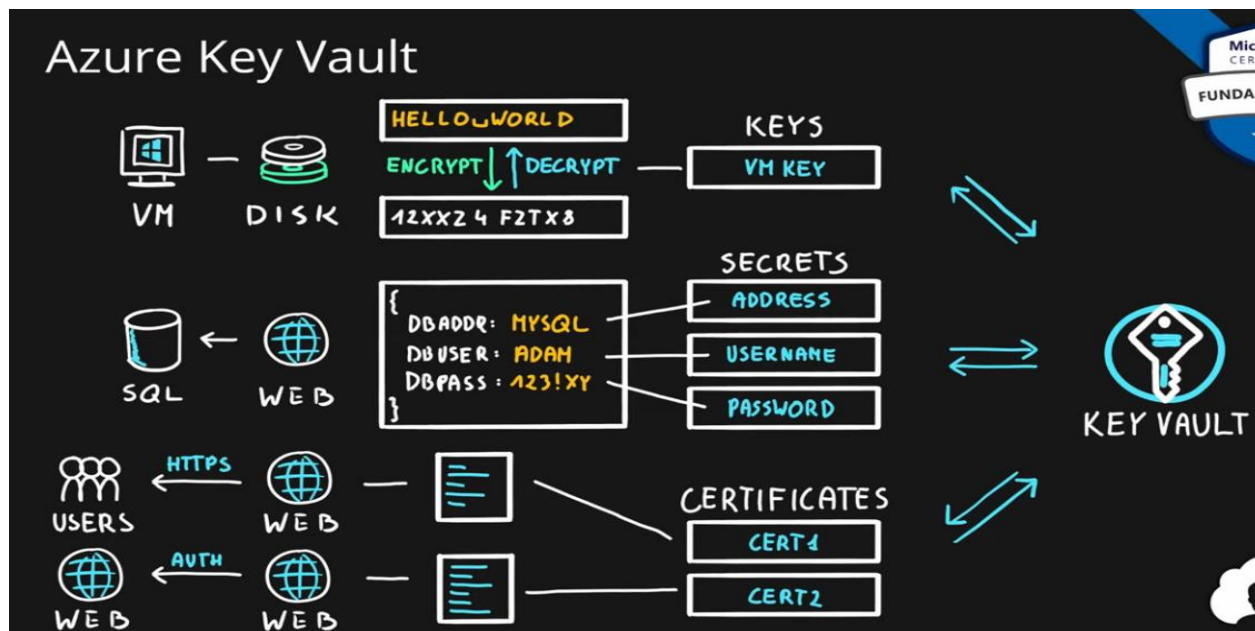


Register Windows Server with the Storage Sync Service



Create a server endpoint and wait for sync

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

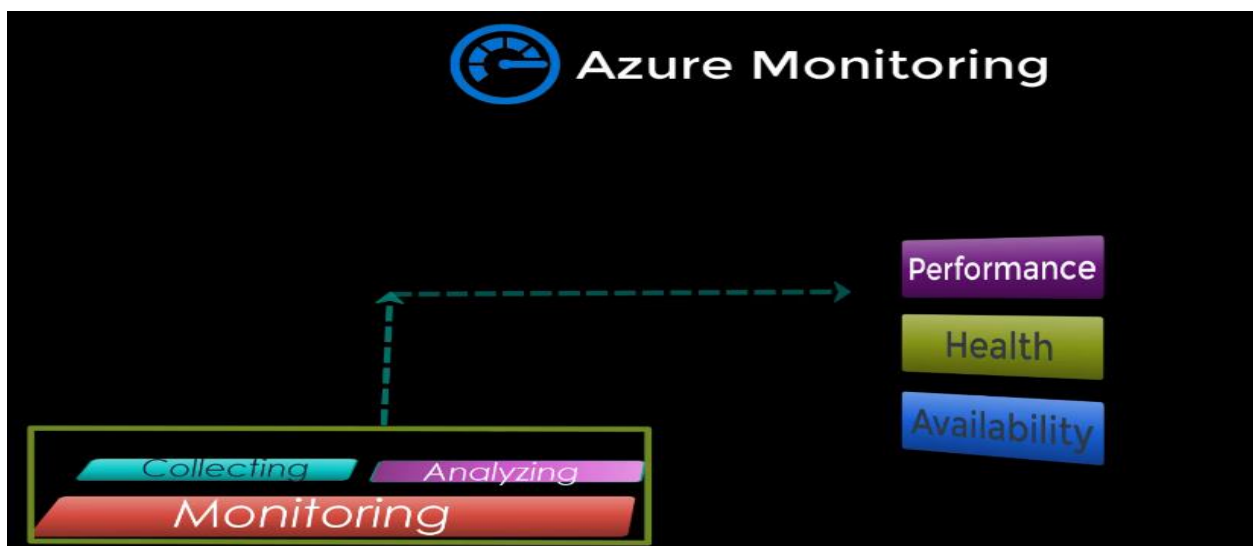
MODULE 11: MONITORING

AZURE MONITOR

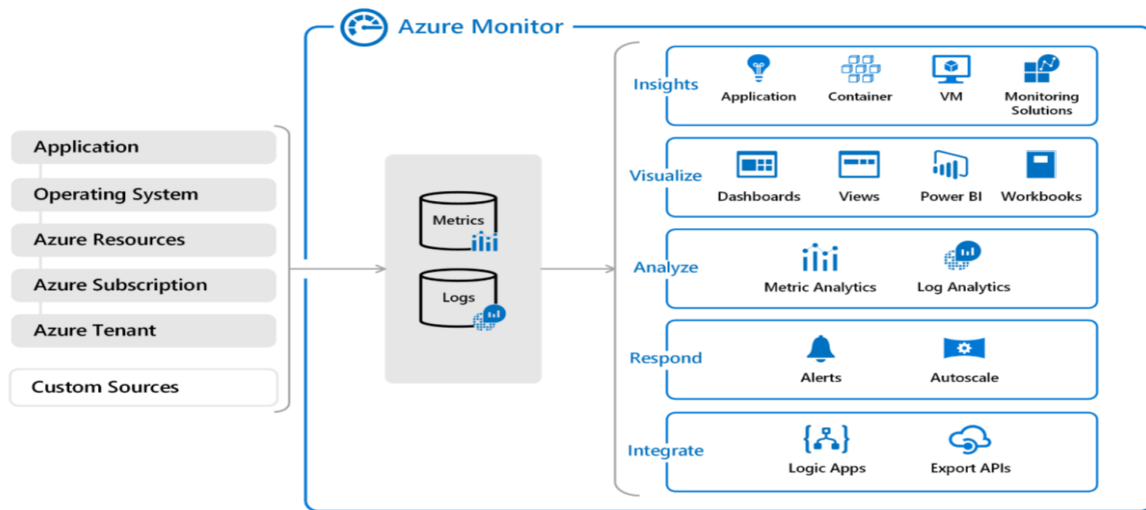
AZURE ALERTS

LOG ANALYTICS

NETWORK WATCHER

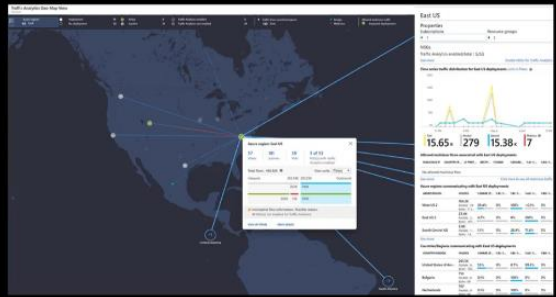


Azure Monitor





Azure Monitor Key Capabilities



Microsoft
CERTIFIED

AZURE
ADMINISTRATOR
ASSOCIATE

★ ★

Monitor & Visualize Metrics

Query & Analyze Logs

Setup Alerts & Actions

Diagnostic Settings - Logs and Metrics



Log Analytics
workspace



Event Hub



Storage account

Azure Virtual Machine Agents



VM Diagnostics extension



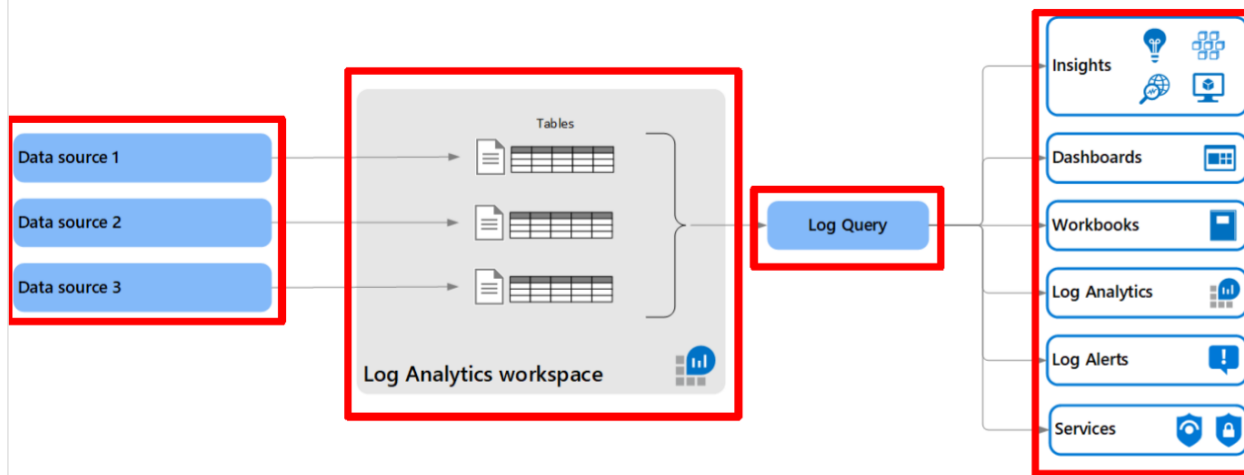
Log Analytics agent



Dependency agent



Azure Log Analytics (Azure Monitor Logs)



Application
Insights



Application Performance Management (APM) service

Visualize application performance

- Host telemetry
- Dependencies
- User behavior
- Performance anomalies

Web tests with synthetic transactions



Log Search Workflow



Application Insights Components

Smart detection

- Live anomaly detection

Application map

- Visualize dependencies

Profiles

- Execution data for web requests

Usage analysis

- User segmentation and retention

Live metrics

- Stream to dashboards

Azure Advisor



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
Watcher



Monitoring toolset for Azure virtual networks

Analyze VNet topologies

Diagnose and solve

- VNet traffic filtering problems
- Network routing problems
- VPN/gateway connectivity problems

Network Performance Monitor



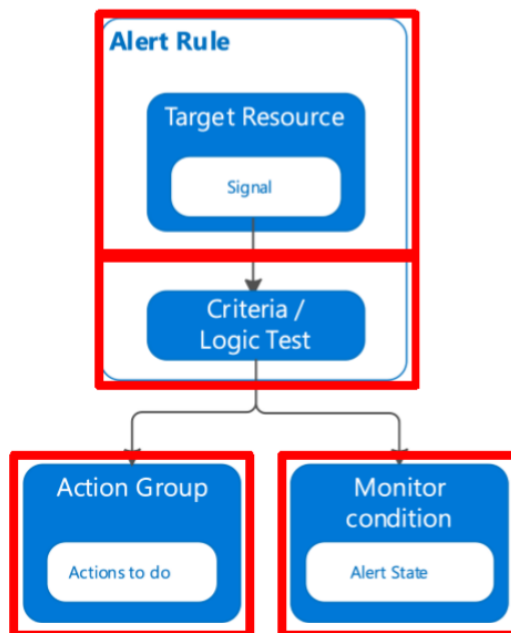
One of several Azure management solutions

Dependent on an Azure Log Analytics workspace

- Sometimes called "Azure Monitor Logs"

Visibility into Azure and/or local networks

Azure Monitor Alert Workflow



<https://timw.info/haw>