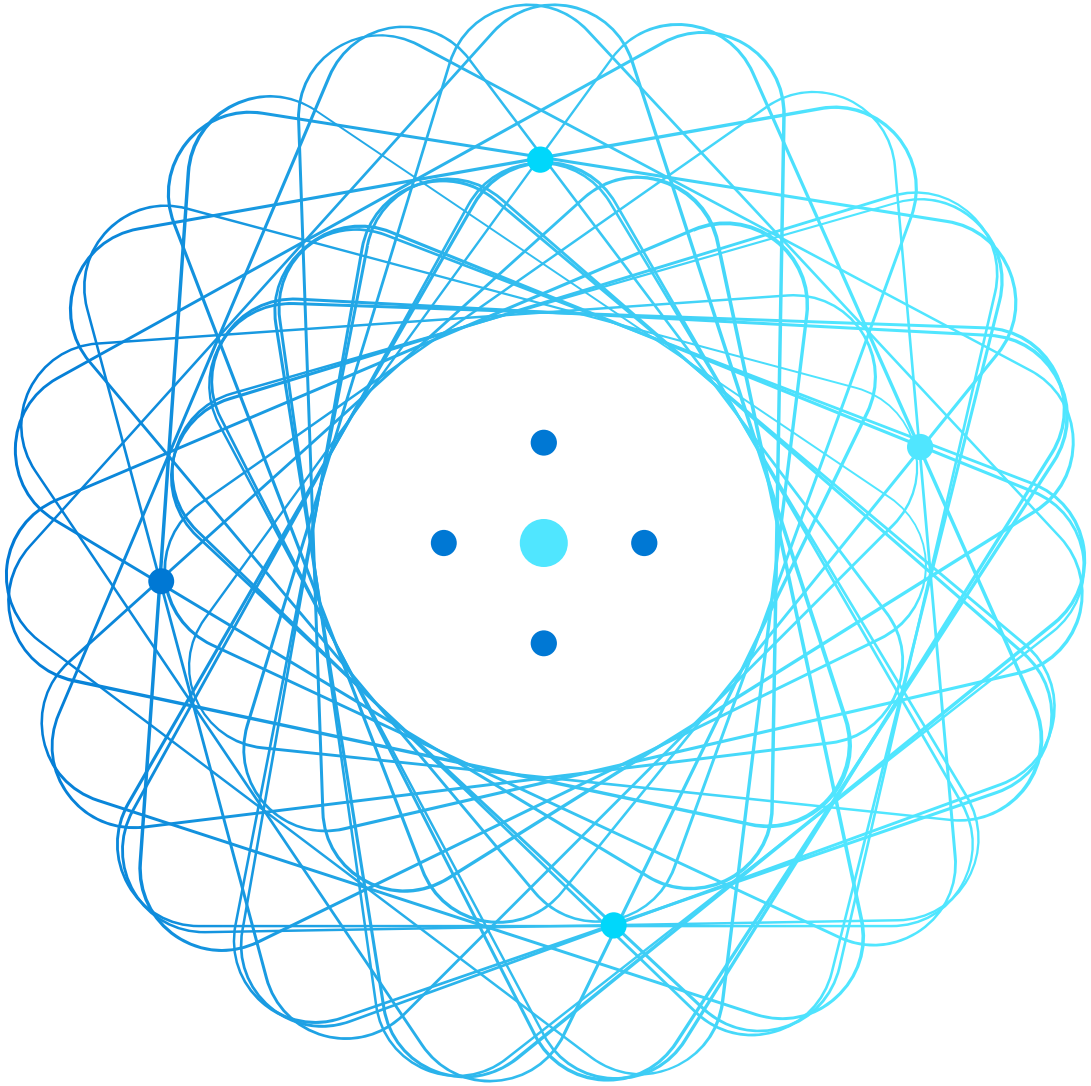
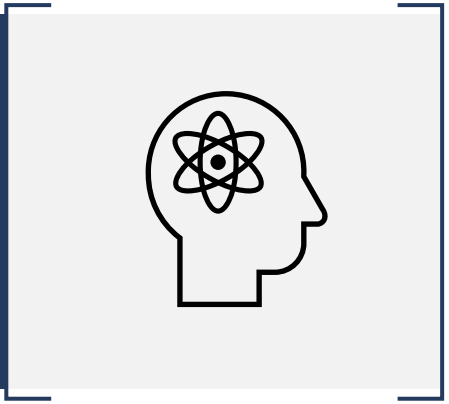
Microsoft Azure

AZ-900

Learning Path 02: Azure Architecture and Services



Learning Path Outline



Learning Path 02 – Outline

You will learn the following concepts:

- **Azure Architectural Components**
  - Regions and Availability Zones
  - Subscriptions and Resource Groups
- **Compute and Networking**
  - Compute types
  - Application hosting
  - Virtual networking
- **Storage**
  - Storage services
  - Redundancy options
  - File management and migration
- **Identity, Access, and Security**
  - Directory services
  - Authentication methods
  - Security models

Azure Accounts

Legal

- Enterprise Agreement EA
- Azure account
- Azure free account
- Azure free student account
- Microsoft Learn sandbox
- Skillable

Classic Administrators
- Account Admin
- Service Admin

Walkthrough – Create an Azure Account

Create an Azure free account

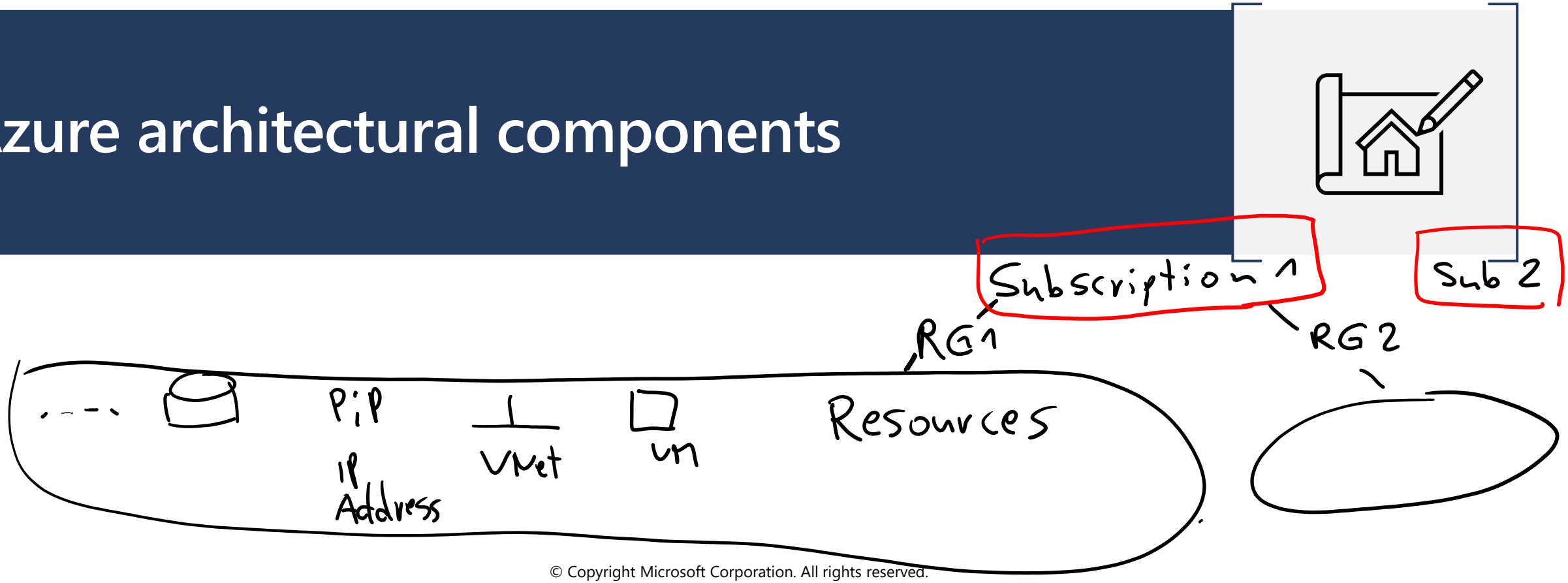
1. Create an Azure free account

Exercise – Explore the Learn sandbox

Explore the Learn sandbox

1. Activate the sandbox
2. Use PowerShell
3. Shift to BASH
4. Shift to Azure Interactive mode
5. Navigate the portal

Azure architectural components

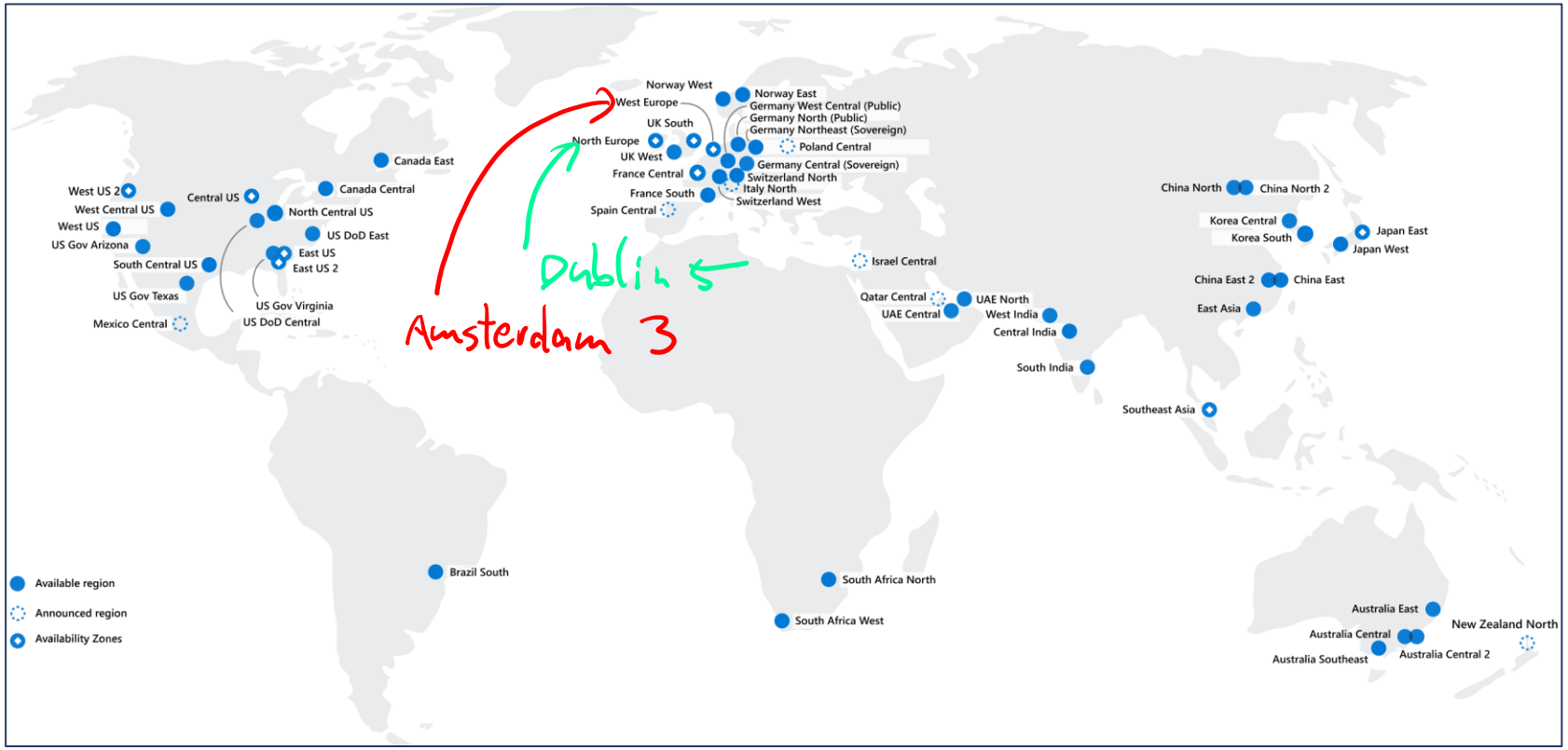


Core Azure architectural components – Objective Domain

- Describe Azure regions, region pairs, and sovereign regions.
- Describe Availability Zones.
- Describe Azure datacenters.
- Describe Azure resources and Resource Groups.
- Describe subscriptions.
- Describe management groups.
- Describe the hierarchy of resource groups, subscriptions, and management groups.

Regions

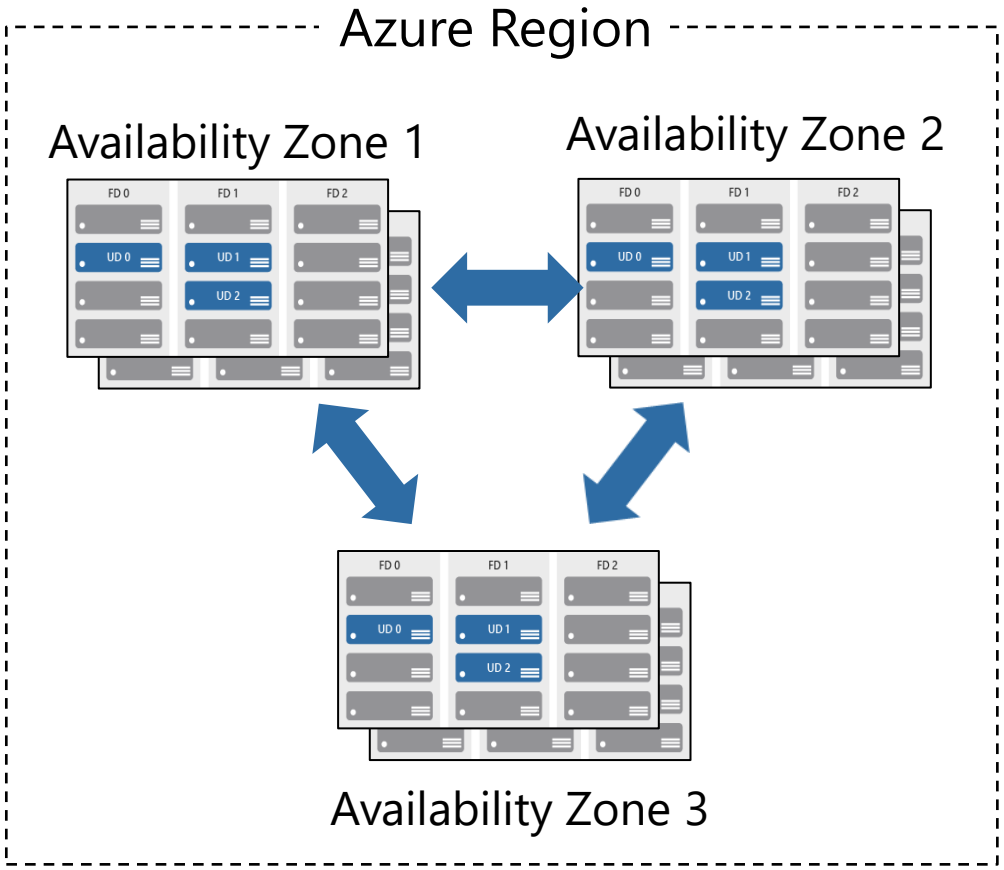
Azure offers more global regions than any other cloud provider with 60+ regions representing over 140 countries



- Regions are made up of one or more datacenters in close proximity.
- Provide flexibility and scale to reduce customer latency.
- Preserve data residency with a comprehensive compliance offering.

Availability zones

- Provide protection against downtime due to datacenter failure.
- Physically separate datacenters within the same region.
- Each datacenter is equipped with independent power, cooling, and networking.
- Connected through private fiber-optic networks.

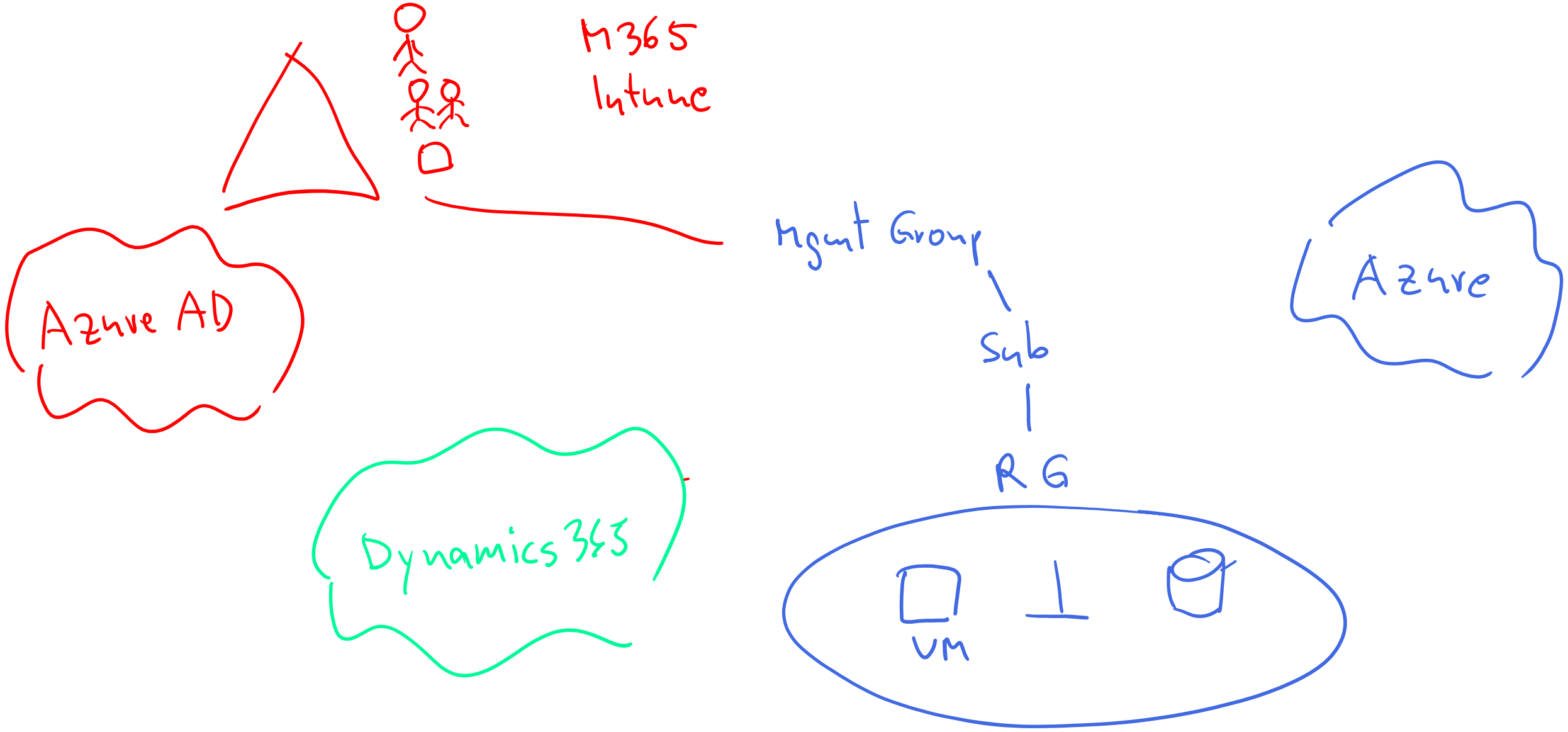


Region Pairs

- At least 300 miles of separation between region pairs.
- Automatic replication for some services.
- Prioritized region recovery in the event of outage.
- Updates are rollout sequentially to minimize downtime.

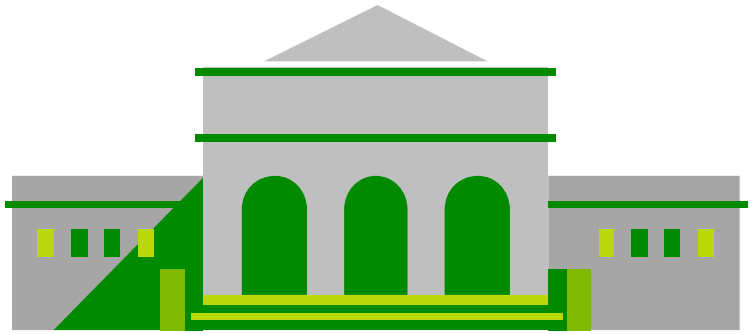
Web Link: https://aka.ms/PairedRegions

Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast	Australia East
India South	India Central
Brazil South (Primary)	South Central US


M365
Intune
Azure AD
Dynamics 365
Mgmt Group
Sub
RG
VM
Azure

Azure Sovereign Regions (US Government services)

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



Azure Government:

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

Azure Sovereign Regions (Azure China)

Microsoft is China's first foreign public cloud service provider, in compliance with government regulations.

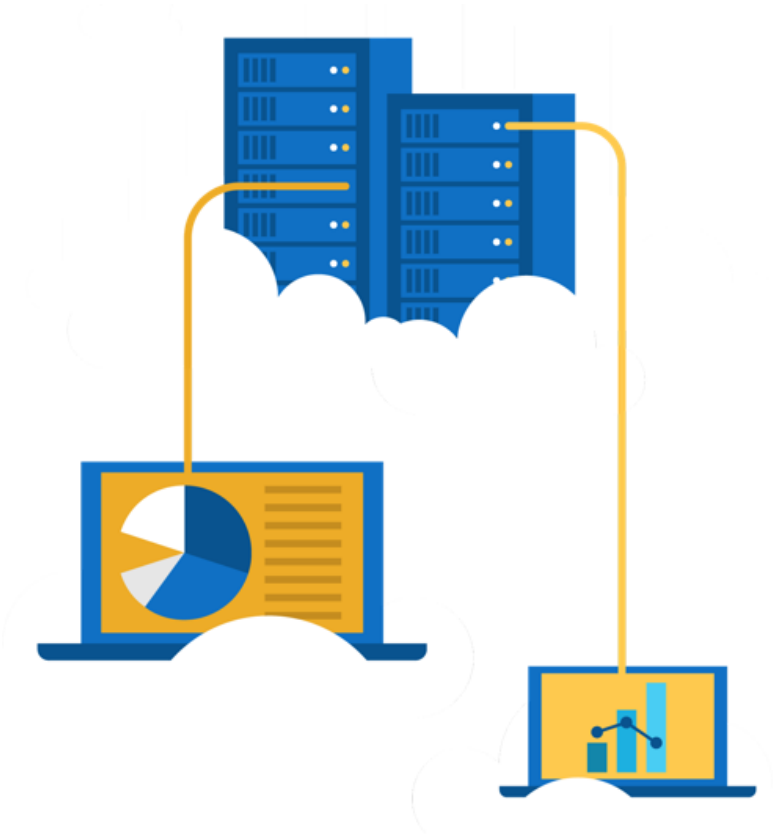
Azure China features:

- Physically separated instance of Azure cloud services operated by 21Vianet
- All data stays within China to ensure compliance

Walkthrough – Explore the Azure Global infrastructure

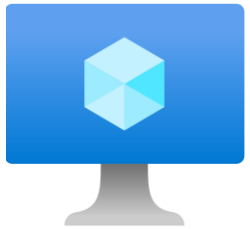
Explore the Azure global infrastructure

1. Select **Explore the Globe** (after intro).
2. Notice the different icons (geography, regions, points of presence (PoP), and so on).
3. Find your location on the globe, then find the nearest PoP and region to your location.



Azure Resources

Azure **resources** are components like storage, virtual machines, and networks that are available to build cloud solutions.



Virtual Machines

Storage Accounts

Virtual Networks

App Services

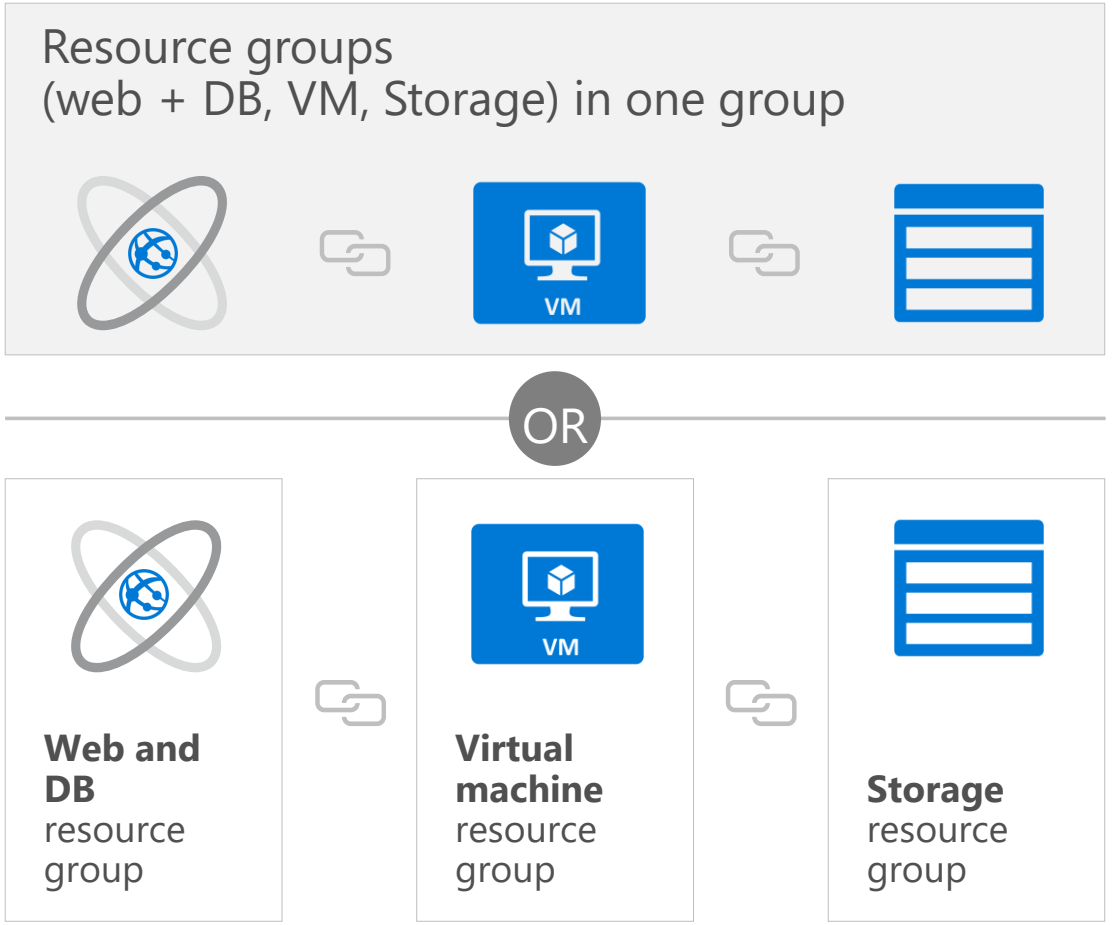
SQL Databases

Functions

Resource groups

A **resource group** is a container to manage and aggregate resources in a single unit.

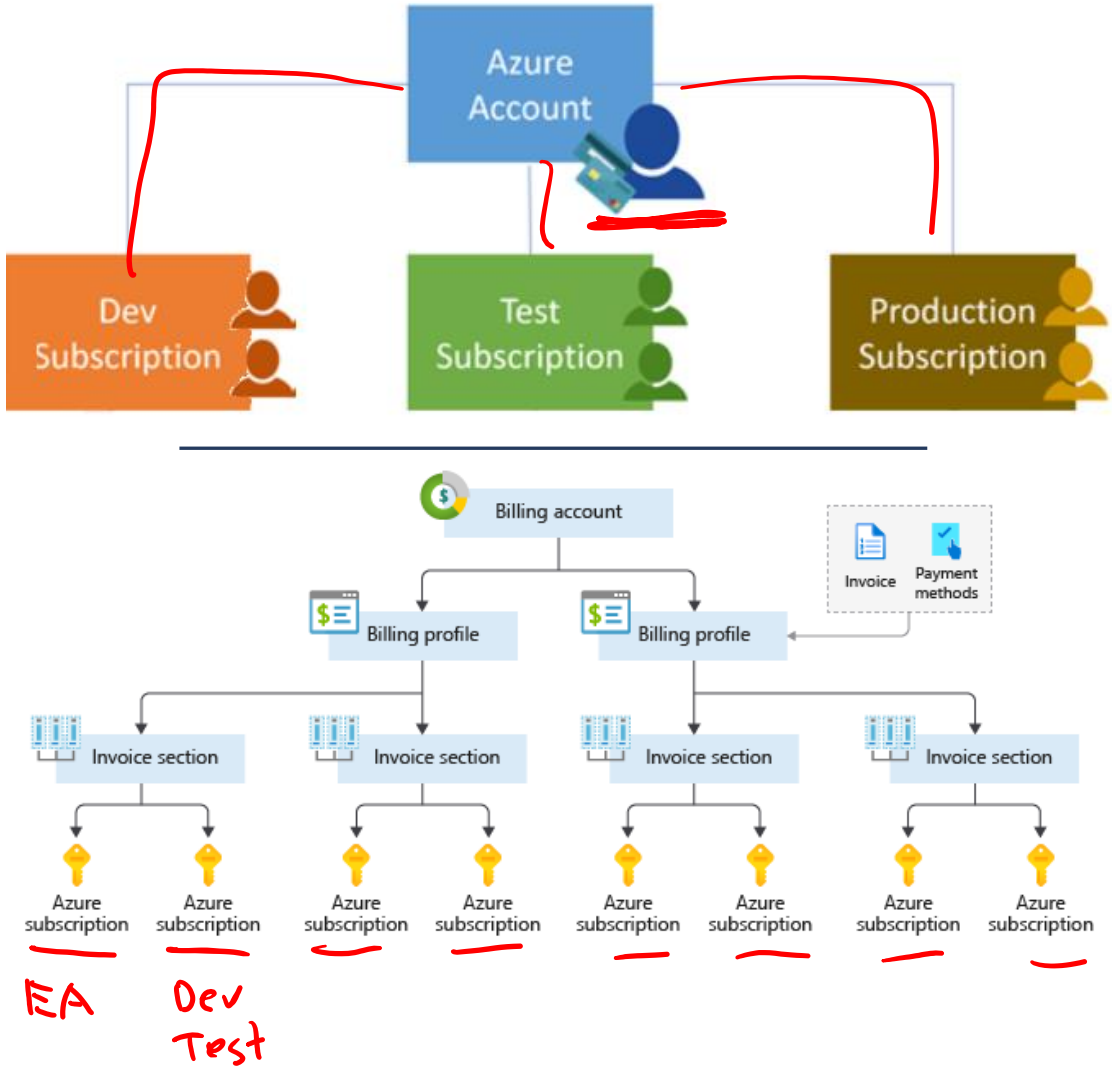
- Resources can exist in only one resource group.
- Resources can exist in different regions.
- Resources can be moved to different resource groups.
- Applications can utilize multiple resource groups.



Azure Subscriptions

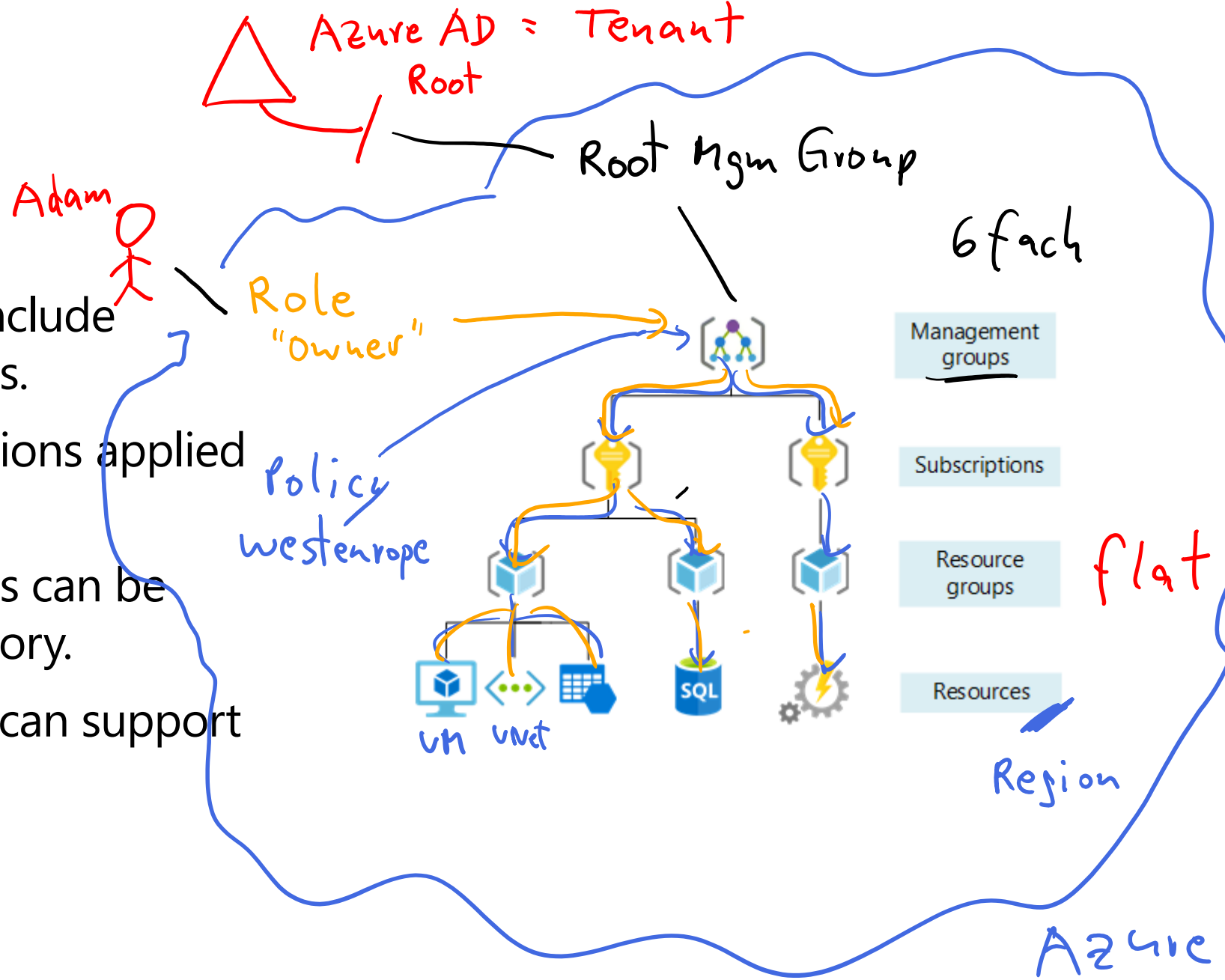
An Azure subscription provides you with authenticated and authorized access to Azure accounts.

- **Billing boundary:** generate separate billing reports and invoices for each subscription.
- **Access control boundary:** manage and control access to the resources that users can provision with specific subscriptions.



Management Groups

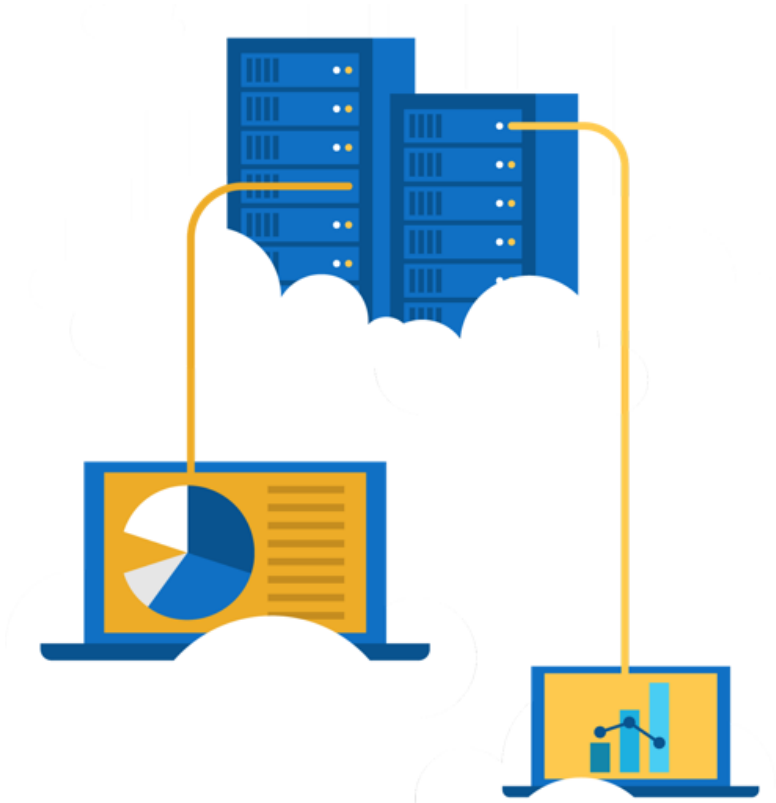
- Management groups can include multiple Azure subscriptions.
- Subscriptions inherit conditions applied to the management group.
- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth.



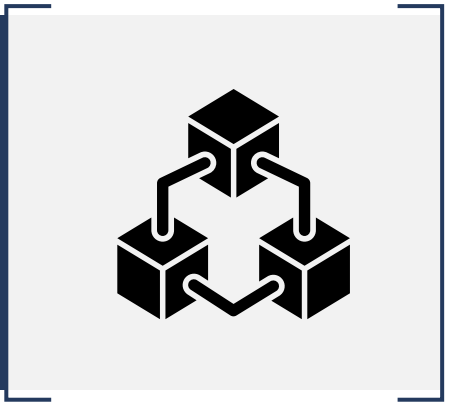
Exercise – Create an Azure resource

Create an Azure resource, monitor the resource group for needed resources being created in the same group

1. Create a virtual machine.
2. Monitor the resource group.



Compute and Networking



Compute and Networking- Objective Domain

Describe the benefits and usage of:

- Compare compute types, including container instances, virtual machines, and functions.
- Describe virtual machine options, including virtual machines (VMs), virtual machine scale sets, virtual machine availability sets, and Azure Virtual Desktop.
- Describe resources required for virtual machines.
- Describe application hosting options, including Azure Web Apps, containers, and virtual machines.
- Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, VPN Gateway, and ExpressRoute.
- Define public and private endpoints.

Azure compute services

On Prem

RDS
(Terminal Server)

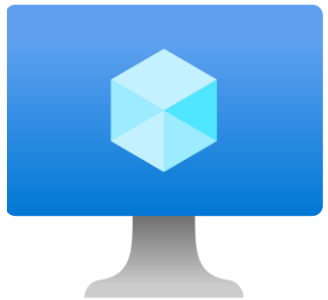
Azure **compute** is an on-demand computing service that provides computing resources such as disks, processors, memory, networking, and operating systems.

IaaS

PaaS

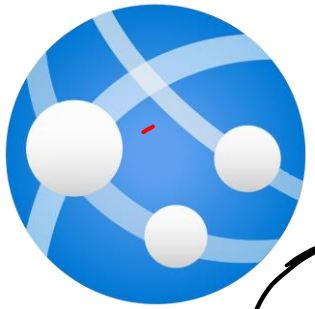
CaaS

App Groups
Host Pools
Session Hosts



Virtual Machines

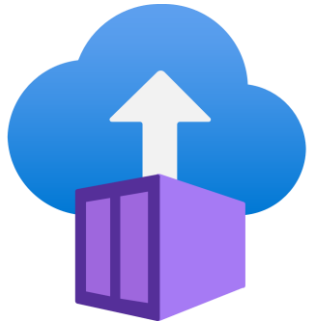
1.



App Services

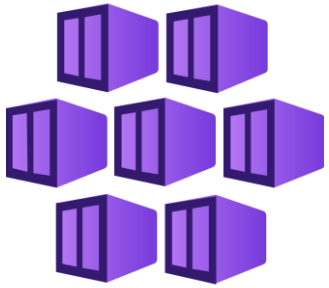
3.

web
API
mobile



Container Instances

2.



Azure Kubernetes Services (AKS)

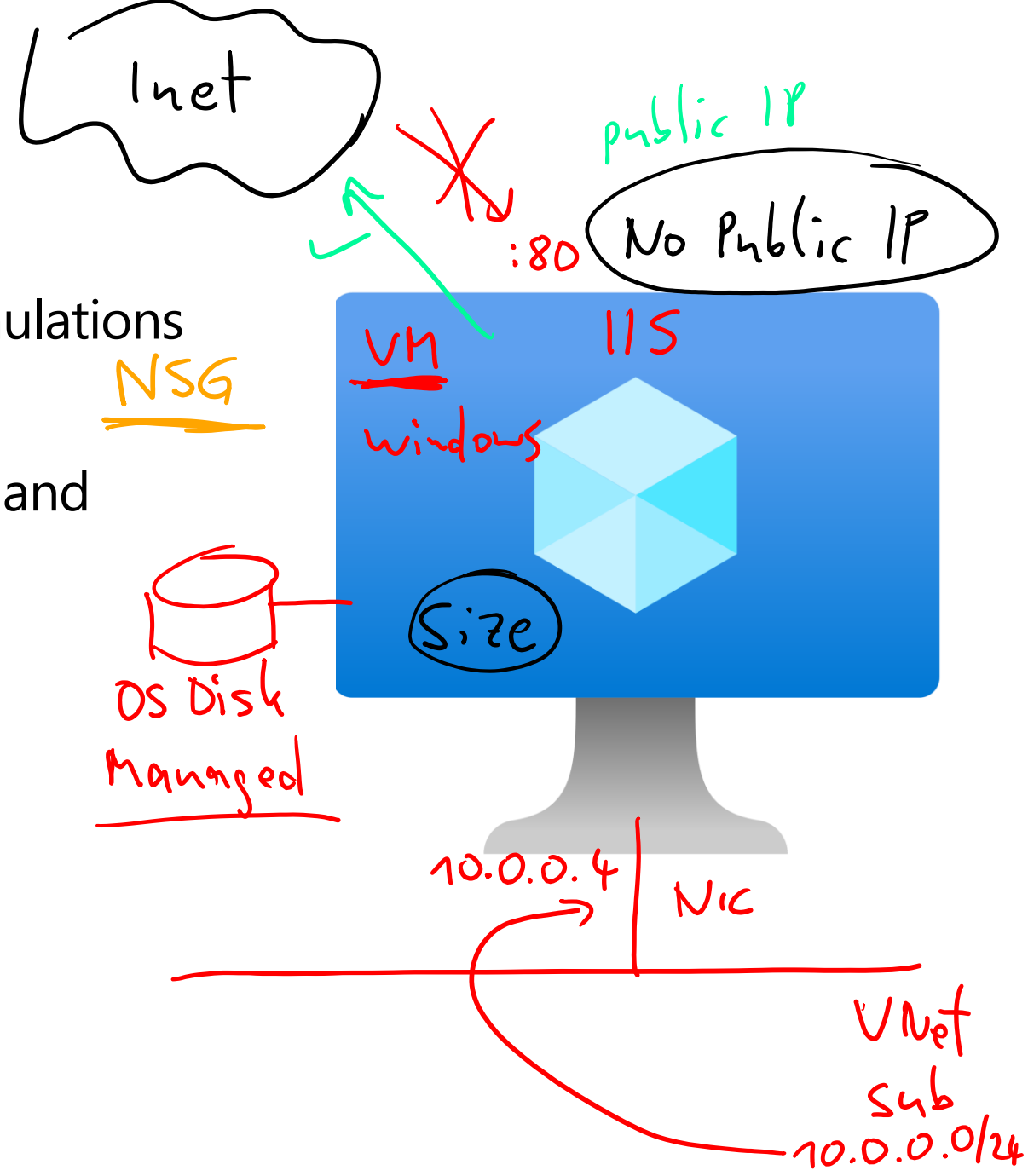
Azure Virtual Desktop

VDI

Azure virtual machines

Azure **Virtual Machines (VM)** are software emulations of physical computers.

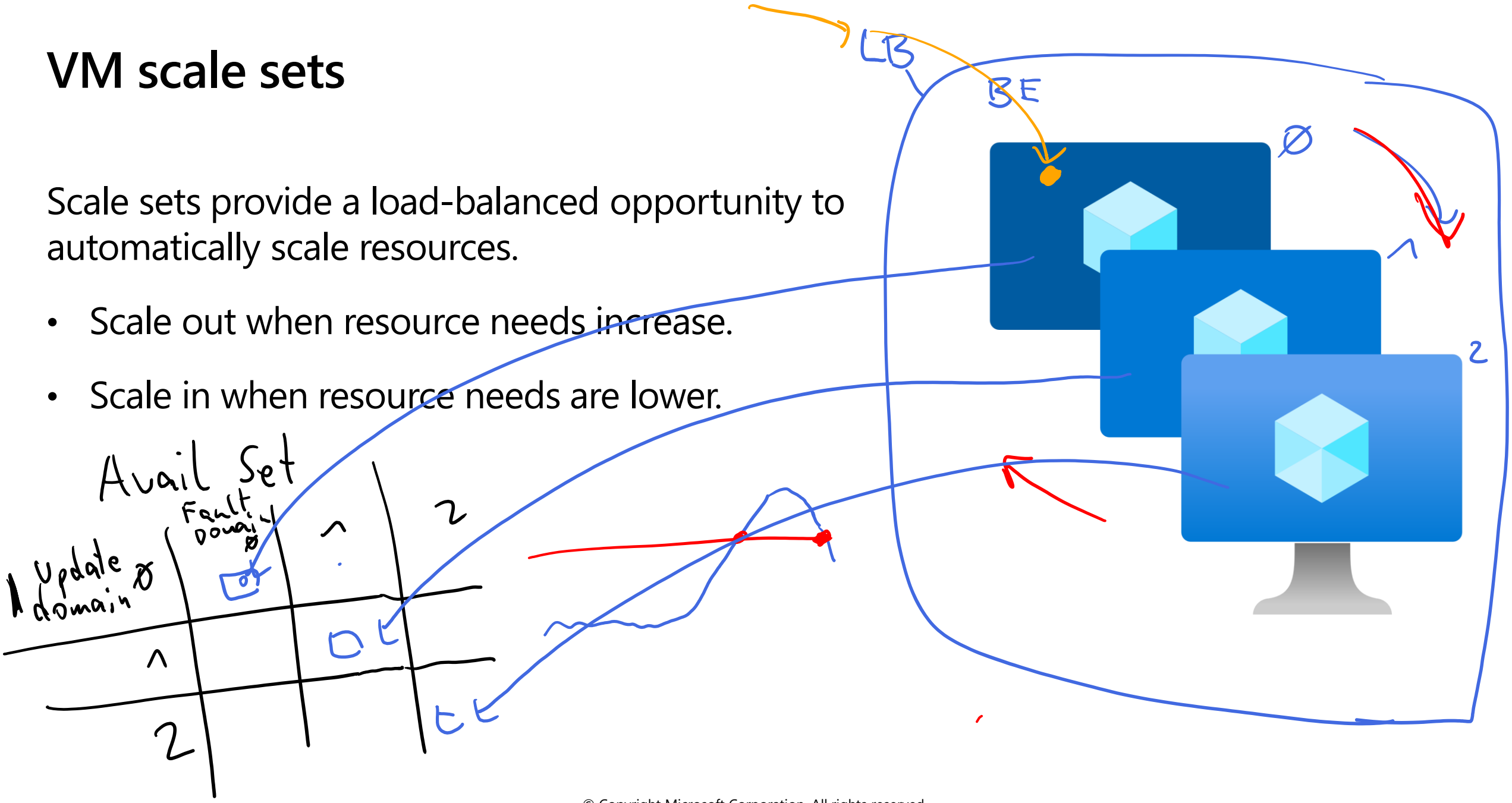
- Includes virtual processor, memory, storage, and networking.
- IaaS offering that provides total control and customization.



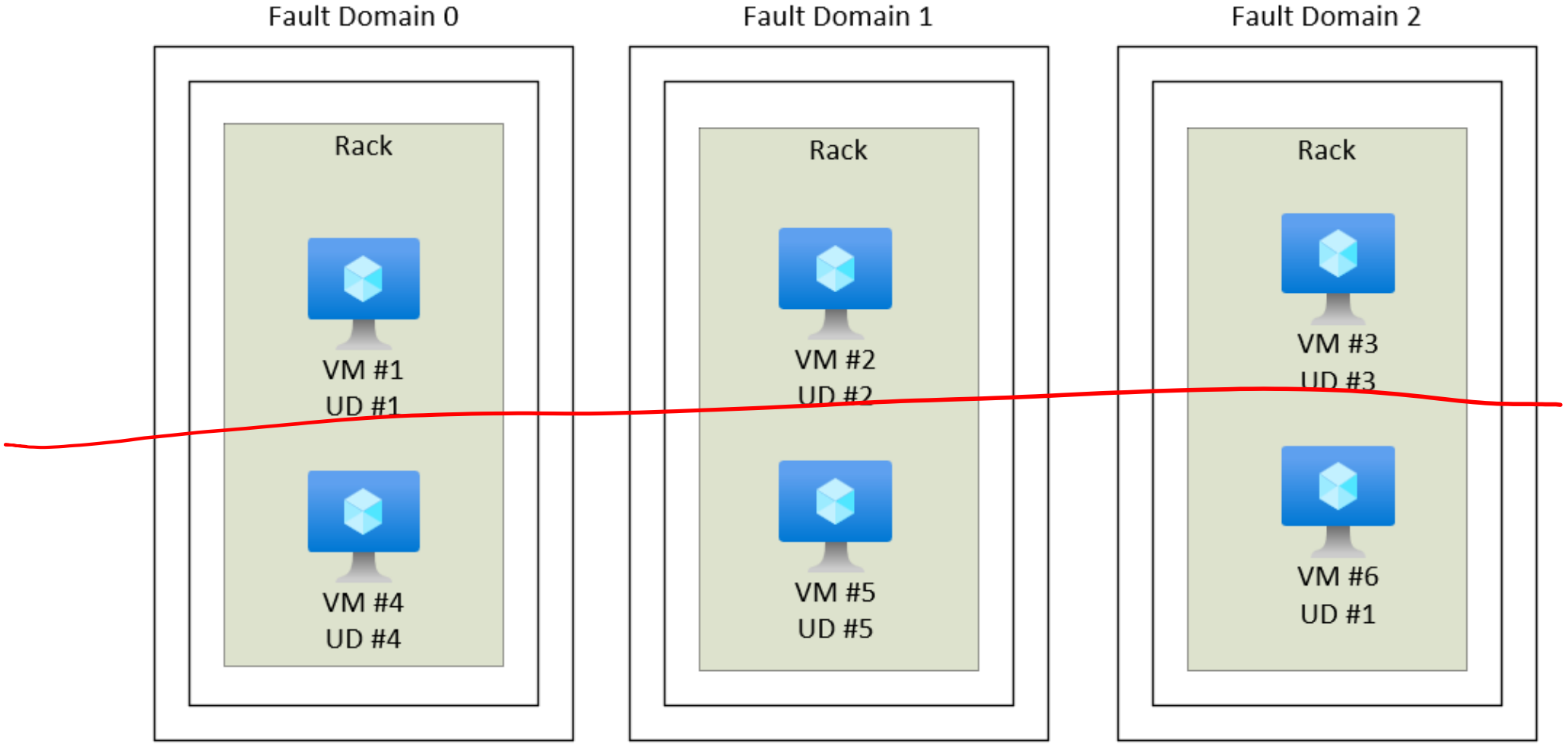
VM scale sets

Scale sets provide a load-balanced opportunity to automatically scale resources.

- Scale out when resource needs increase.
- Scale in when resource needs are lower.



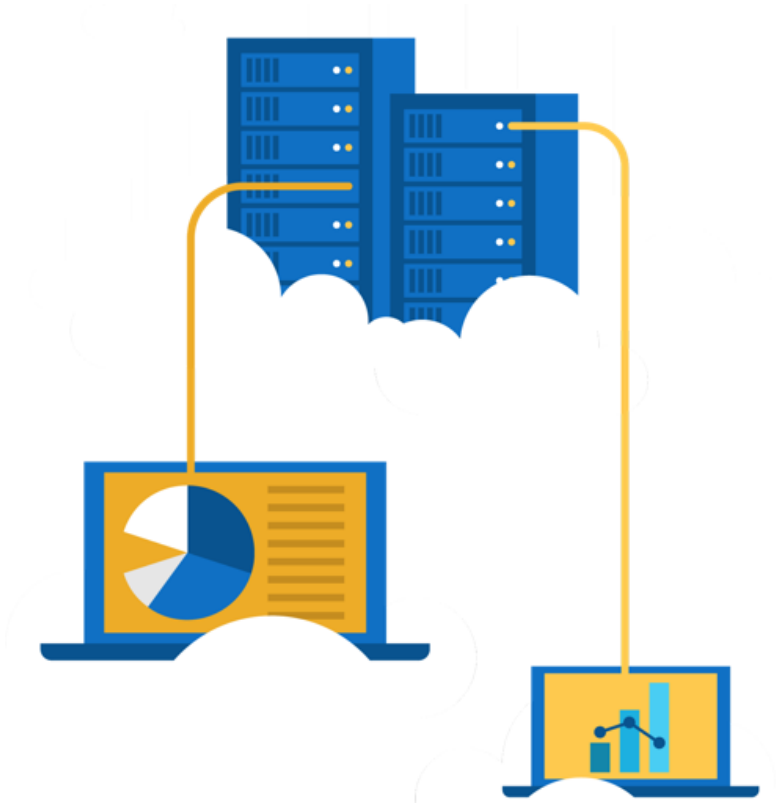
VM availability sets



Exercise – Create a Virtual Machine

Create a virtual machine in the Azure Portal, connect to the virtual machine, install the web server role, and test.

1. Create the virtual machine.
2. Install the web server package.



Azure Virtual Desktop

Azure Virtual Desktop is a desktop and app virtualization that runs in the cloud.

- Create a full desktop virtualization environment without having to run additional gateway servers.
- Reduce risk of resource being left behind.
- True multi-session deployments.

Docker Container

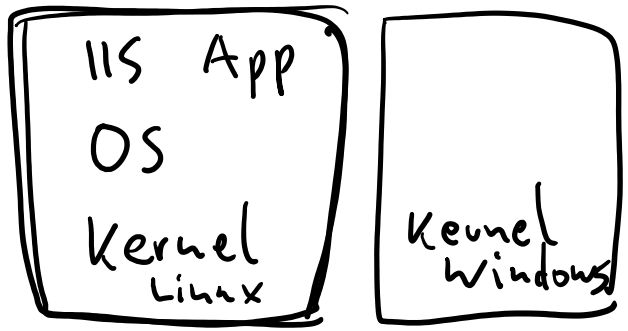
Azure Container Services

Azure **Containers** are a light-weight, virtualized environment that does not require operating system management, and can respond to changes on demand.

Azure Container Instances: a PaaS offering that runs a container in Azure without the need to manage a virtual machine or additional services.

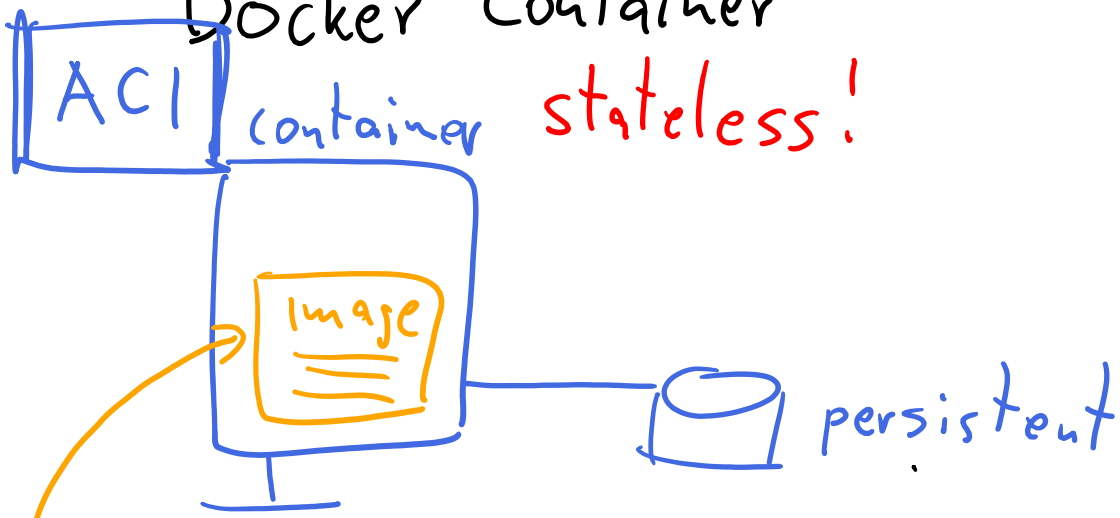
Azure Kubernetes Service: an orchestration service for containers with distributed architectures and large volumes of containers.

VM



Hypervisor

Docker Container



Docker Engine

shared Kernel

Cloud Native?

AKS

Kubernetes

Dockerfile

docker build .

ACR Registry

Read only!

Docker Image (FS)

Azure Functions

Azure Functions

Event based code running your service and not the underlying infrastructure.

Comparing Azure compute options

Virtual machines	Virtual Desktop	Containers
Cloud based server that supports either Windows or Linux environments.	Provides a cloud based personal computer Windows desktop experience.	Lightweight, miniature environment well suited for running microservices.
Useful for lift-and-shift migrations to the cloud.	Dedicated applications to connect and use, or accessible from any modern browser.	Designed for scalability and resiliency through orchestration.
Complete operating system package, including the host operating system.	Multi-client login allows multiple users to log into the same machine at the same time.	Applications and services are packaged in a container that sits on-top of the host operating system. Multiple containers can sit on one host OS.

Azure App Services

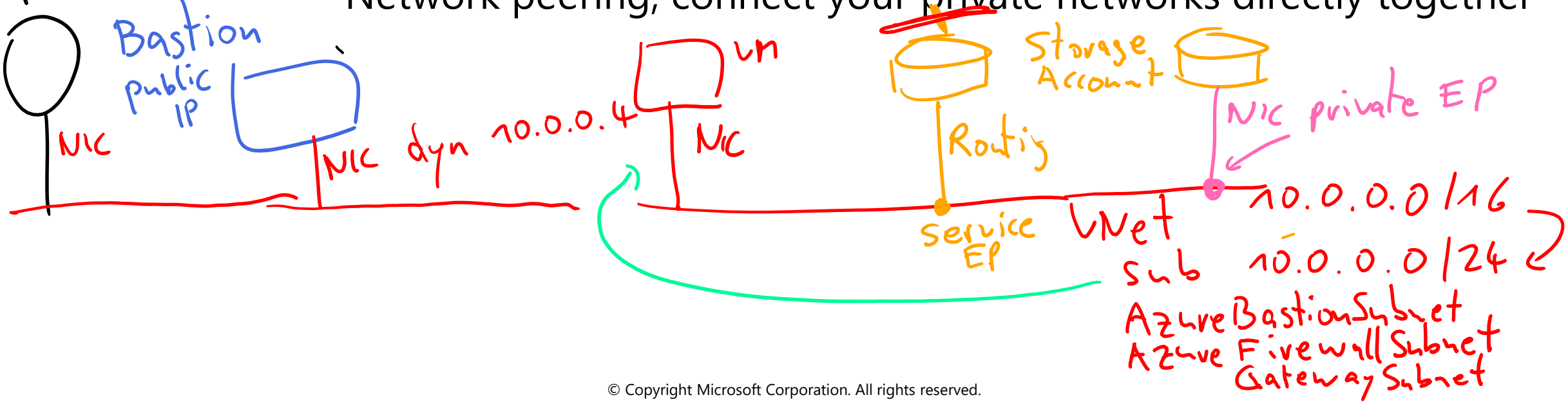
Azure **App Services** is a fully managed platform to build, deploy, and scale web apps and APIs quickly.

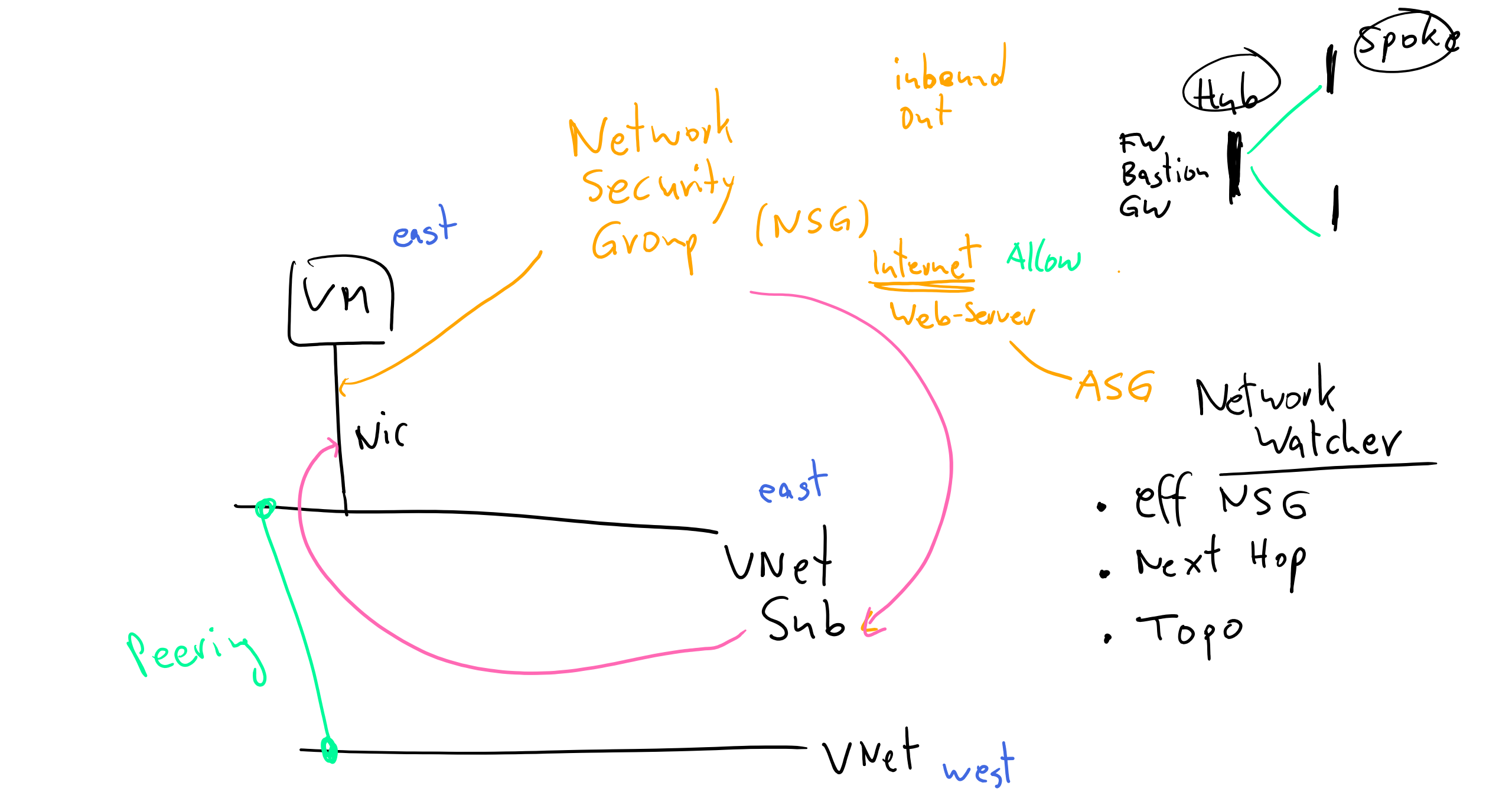
- Works with .NET, .NET Core, Node.js, Java, Python, or php.
- PaaS offering with enterprise-grade performance, security, and compliance requirements.

Azure networking services

Azure Virtual Network (VNet) enables Azure resources to communicate with each other, the internet, and on-premises networks.

- Public endpoints, accessible from anywhere on the internet
- Private endpoints, accessible only from within your network
- Virtual subnets, segment your network to suit your needs
- Network peering, connect your private networks directly together





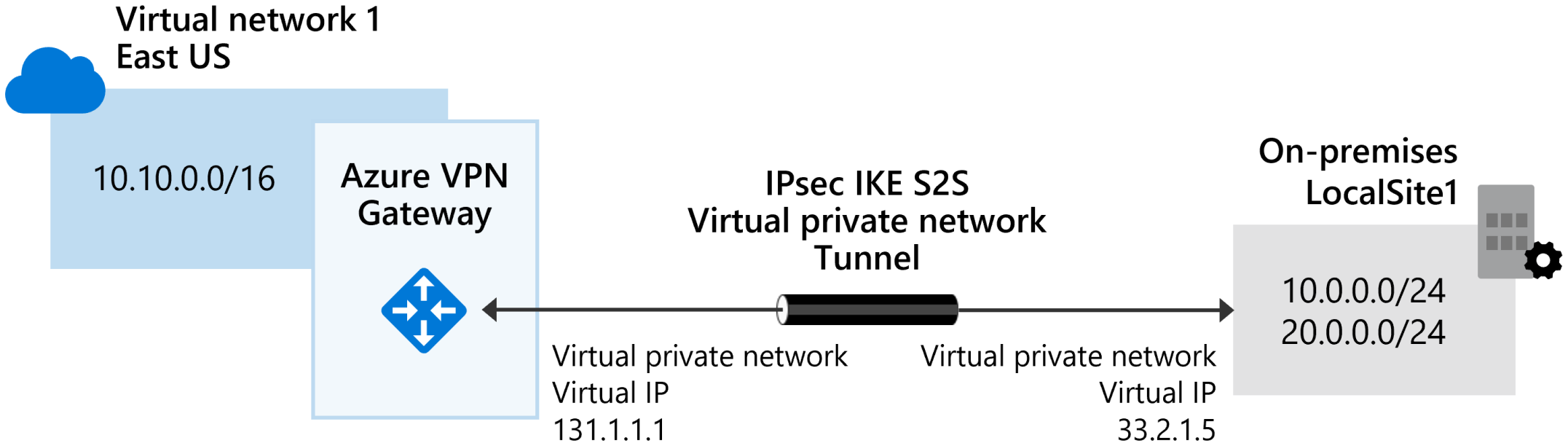
Walkthrough – Configure network access

Configure public access to the virtual machine created earlier.

1. Verify currently open ports.
2. Create a network security group
3. Configure HTTP access (port 80)
4. Test the connection.

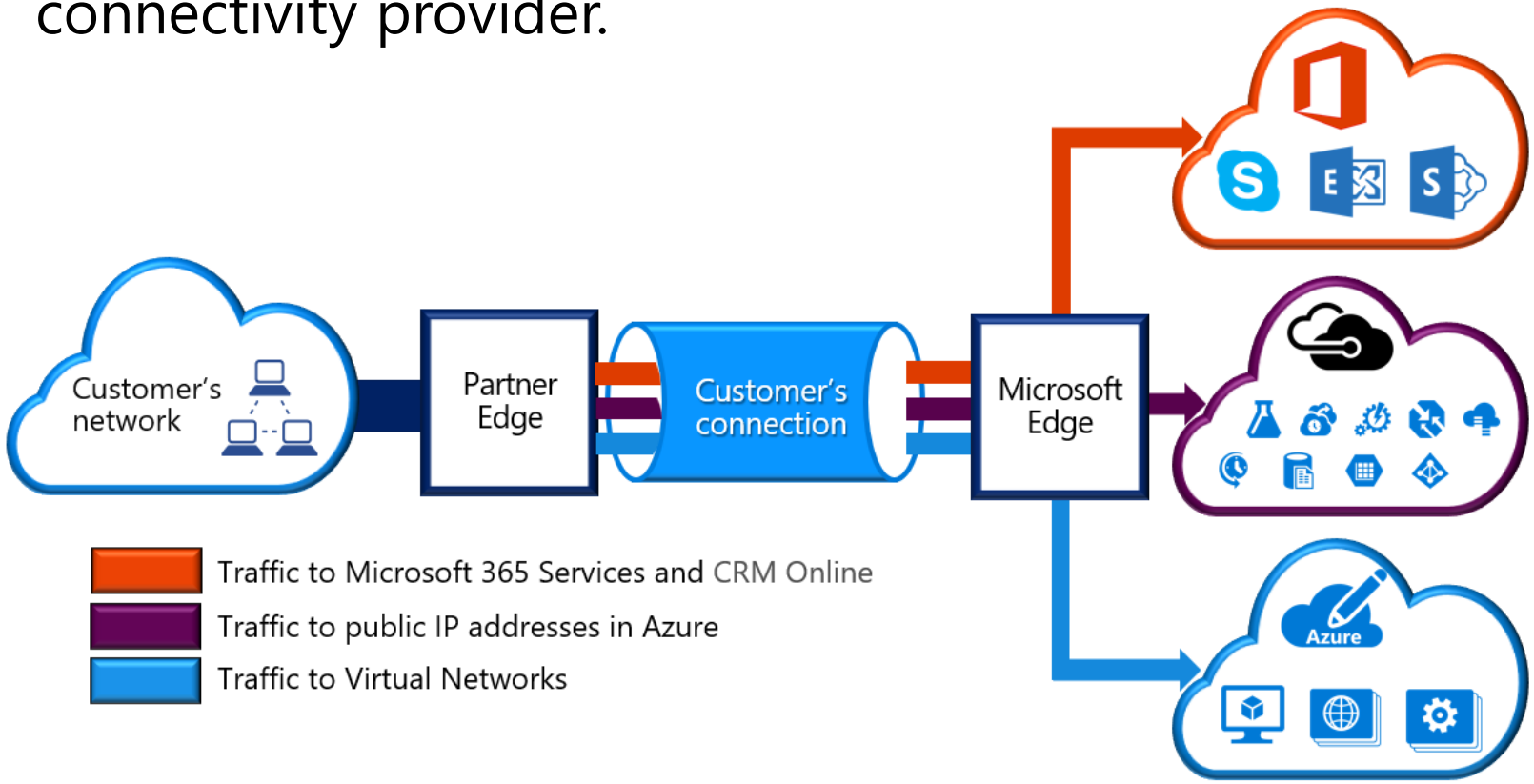
Azure networking services

Virtual Private Network Gateway (VPN) is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet.



Azure networking services

Azure Express Route extends on-premises networks into Azure over a private connection that is facilitated by a connectivity provider.



Azure DNS

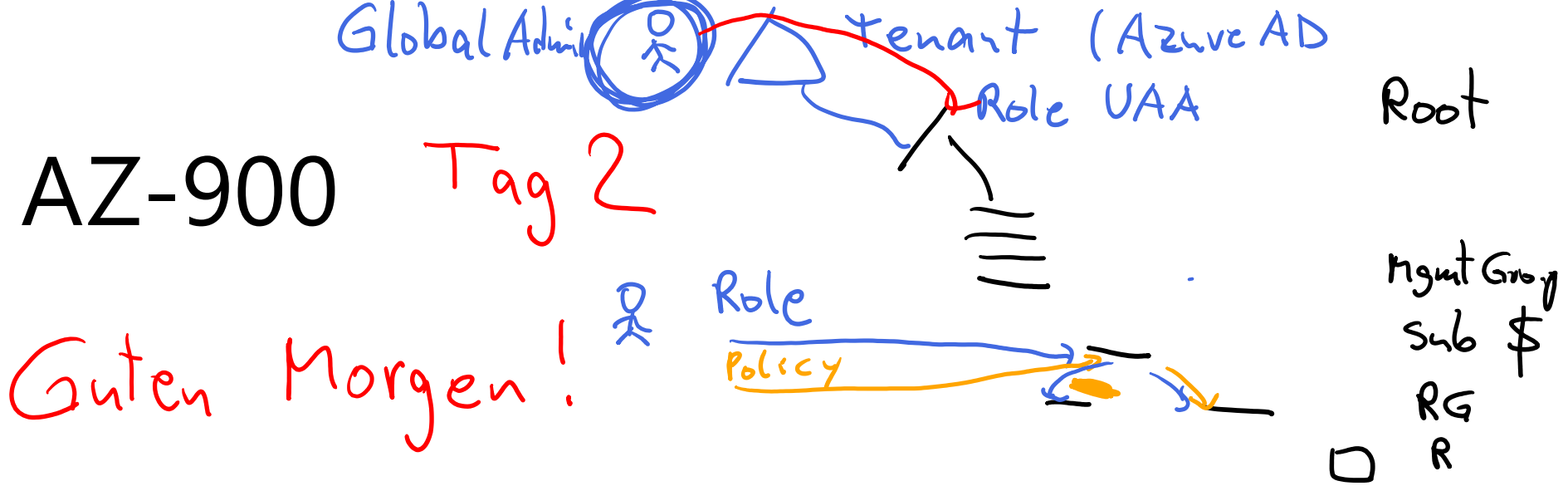
- Reliability and performance by leveraging a global network of DNS name servers using Anycast networking.
- Azure DNS security is based on Azure resource manager, enabling role-based access control and monitoring and logging.
- Ease of use for managing your Azure and external resources with a single DNS service.
- Customizable virtual networks allow you to use private, fully customized domain names in you private virtual networks.
- Alias records supports alias record sets to point directly to an Azure resource.

Course Agenda

AZ-900

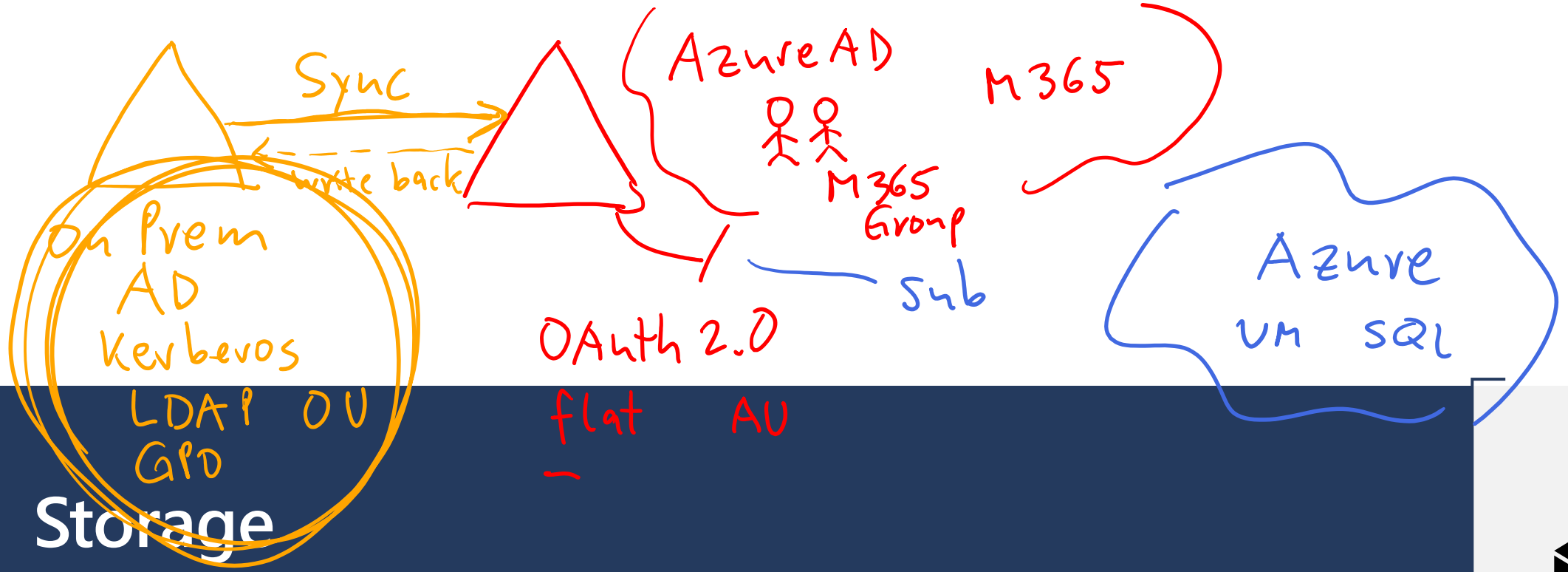
Tag 2

Guten Morgen!

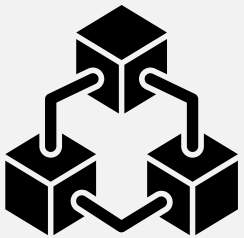


Learning Path 01 – Cloud concepts
Learning Path 02 – Azure architecture and services
Learning Path 03 – Azure management and governance

App PaaS



Storage



Storage Account

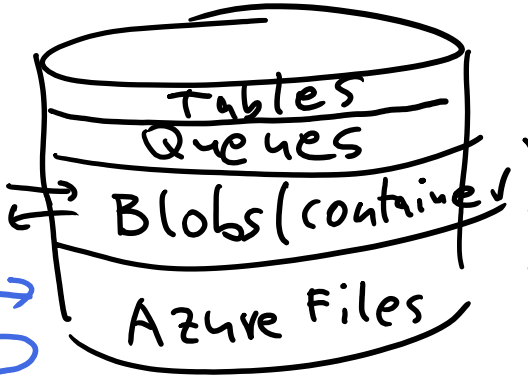
Queue

Maschinendaten → IOT Hub → Routing

Fotos

Disk (Block Storage)

Z:



SMB

share perm

AD Auth

Storage - Objective Domain

Cloud Shell

Compute
ACI
Ubuntu linux
1
TTY

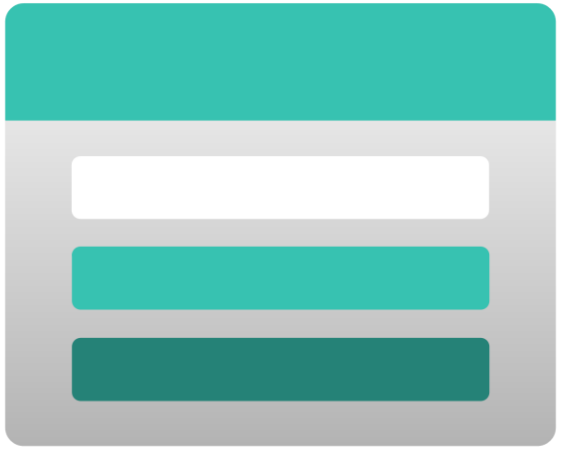
Storage
SA
File Share

Describe the benefits and usage of:

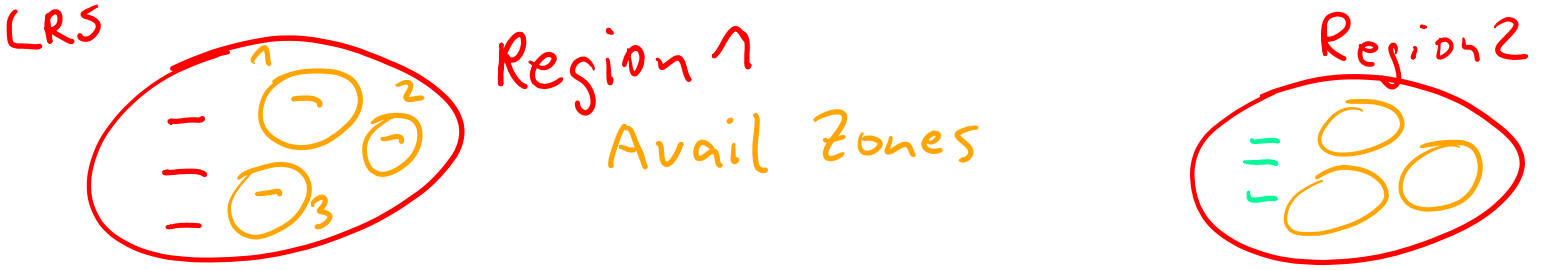
- Compare Azure storage services.
- Describe storage tiers.
- Describe redundancy options.
- Describe storage account options and storage types.
- Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync.
- Describe migration options, including Azure Migrate and Azure Data Box.

Storage accounts

- Must have a globally unique name
- Provide over-the-internet access worldwide
- Determine storage services and redundancy options



Storage redundancy

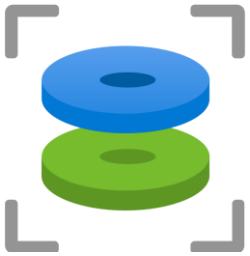


Redundancy configuration	Deployment	Durability
Locally redundant storage (LRS)	Single datacenter in the primary region	11 nines
Zone-redundant storage (ZRS)	Three availability zones in the primary region	12 nines
Geo-redundant storage (GRS)	Single datacenter in the primary and secondary region	16 nines
Geo-zone-redundant-storage (GZRS)	Three availability zones in the primary region and a single datacenter in secondary region	16 nines

GRS-RA
GZRS-RA

Azure storage services

Container storage (blob) is optimized for storing massive amounts of unstructured data, such as text or binary data.



Disk storage provides disks for virtual machines, applications, and other services to access and use.

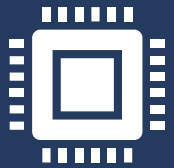
Azure Files sets up a highly available network file shares that can be accessed by using the standard Server Message Block (SMB) protocol.

Storage service public endpoints

Storage service	Public endpoint
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net

Azure storage access tiers

GP v2

 Hot	 Cool	 Archive
Optimized for storing data that is accessed frequently.	Optimized for storing data that is infrequently accessed and stored for at least 30 days.	Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements.

You can switch between these access tiers at any time.

Exercise - Create a storage blob

Create a storage account with a blob storage container. Work with blob files.

1. Create a storage account.
2. Create a blob container.
3. Upload and access a blob.

Azure Migrate

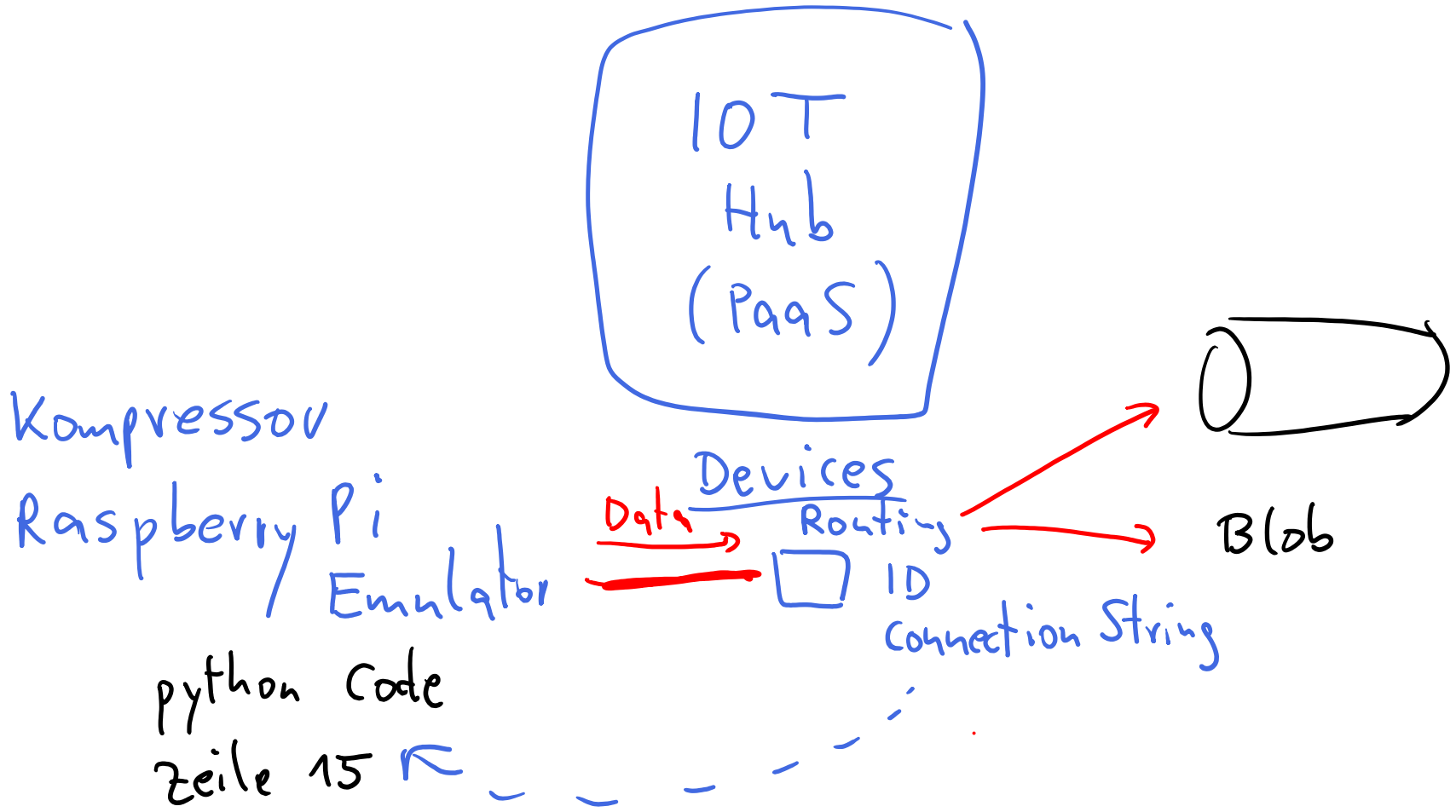
- Unified migration platform
- Range of integrated and standalone tools
- Assessment and migration

Azure Data Box

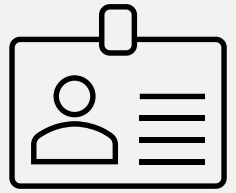
- Store up to 80 terabytes of data.
- Move your disaster recovery backups to Azure.
- Protect your data in a rugged case during transit.
- Migrate data out of Azure for compliance or regulatory needs.
- Migrate data to Azure from remote locations with limited or no connectivity.

File management options

AzCopy	Azure Storage Explorer	Azure File Sync
Command line utility	Graphical user interface (similar to Windows Explorer)	Synchronizes Azure and on premises files in a bidirectional manner
Copy blobs or files to or from your storage account	Compatible with Windows, MacOS, and Linux	Cloud tiering keeps frequently accessed files local, while freeing up space
One-direction synchronization	Uses AzCopy to handle file operations	Rapid reprovisioning of failed local server (install and resync)


IOT
Hub
(PaaS)
Kompressor
Raspberry Pi
Emulator
python Code
Zeile 15
Data
Devices
Routing
ID
Connection String
Blob

Identity, Access, and Security



Identity, Access, and Security - Objective Domain

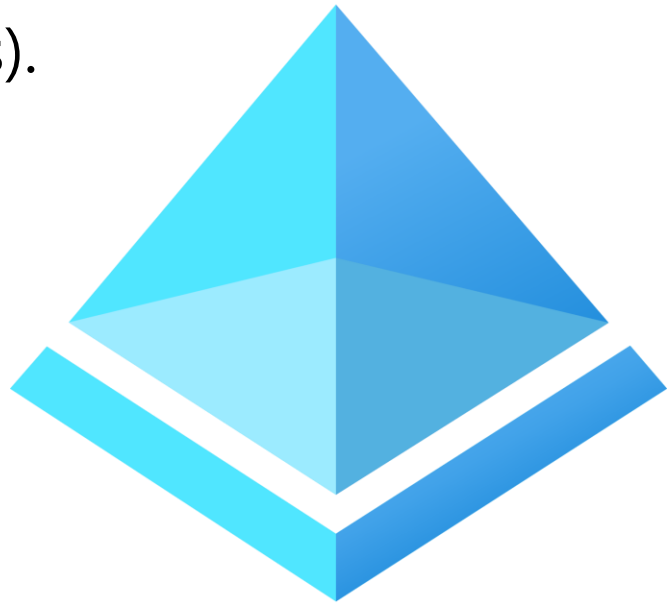
Describe the benefits and usage of:

- Describe directory services in Azure, including Azure Active Directory (AD) and Azure AD DS, part of Microsoft Entra.
- Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and passwordless.
- Describe external identities and guest access in Azure.
- Describe Azure AD Conditional Access.
- Describe Azure Role Based Access Control (RBAC).
- Describe the concept of Zero Trust.
- Describe the purpose of the defense in depth model.
- Describe the purpose of Microsoft Defender for Cloud.

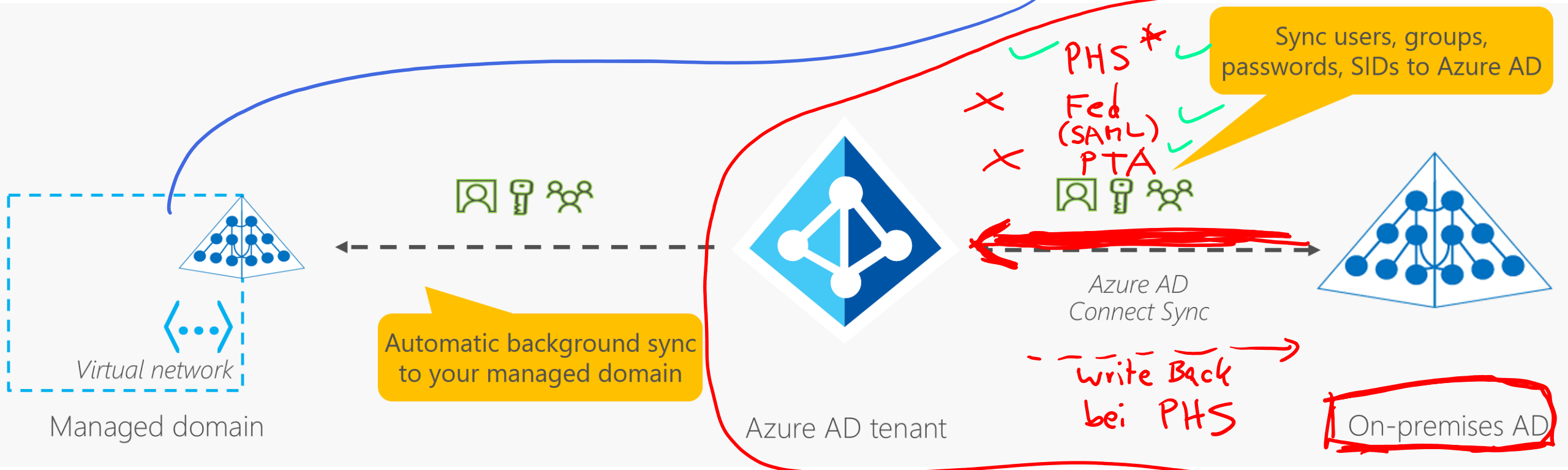
Azure Active Directory (AAD)

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

- Authentication (employees sign-in to access resources).
- Single sign-on (SSO).
- Application management.
- Business to Business (B2B).
- Business to Customer (B2C) identity services.
- Device management.



Azure Active Directory Domain Services (Azure AD DS)



- Gain the benefit of cloud-based domain services without managing domain controllers
- Run legacy applications (that can't use modern auth standards) in the cloud
- Automatically sync from Azure AD

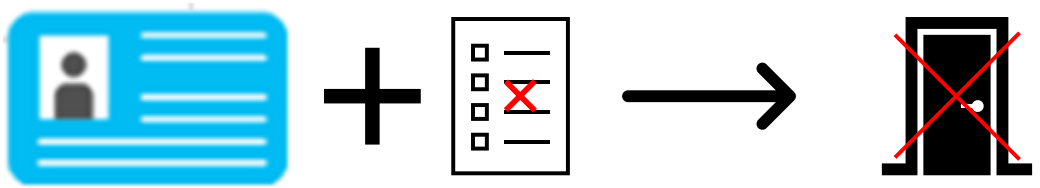
Compare Authentication and Authorization

Authentication

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

Authorization

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

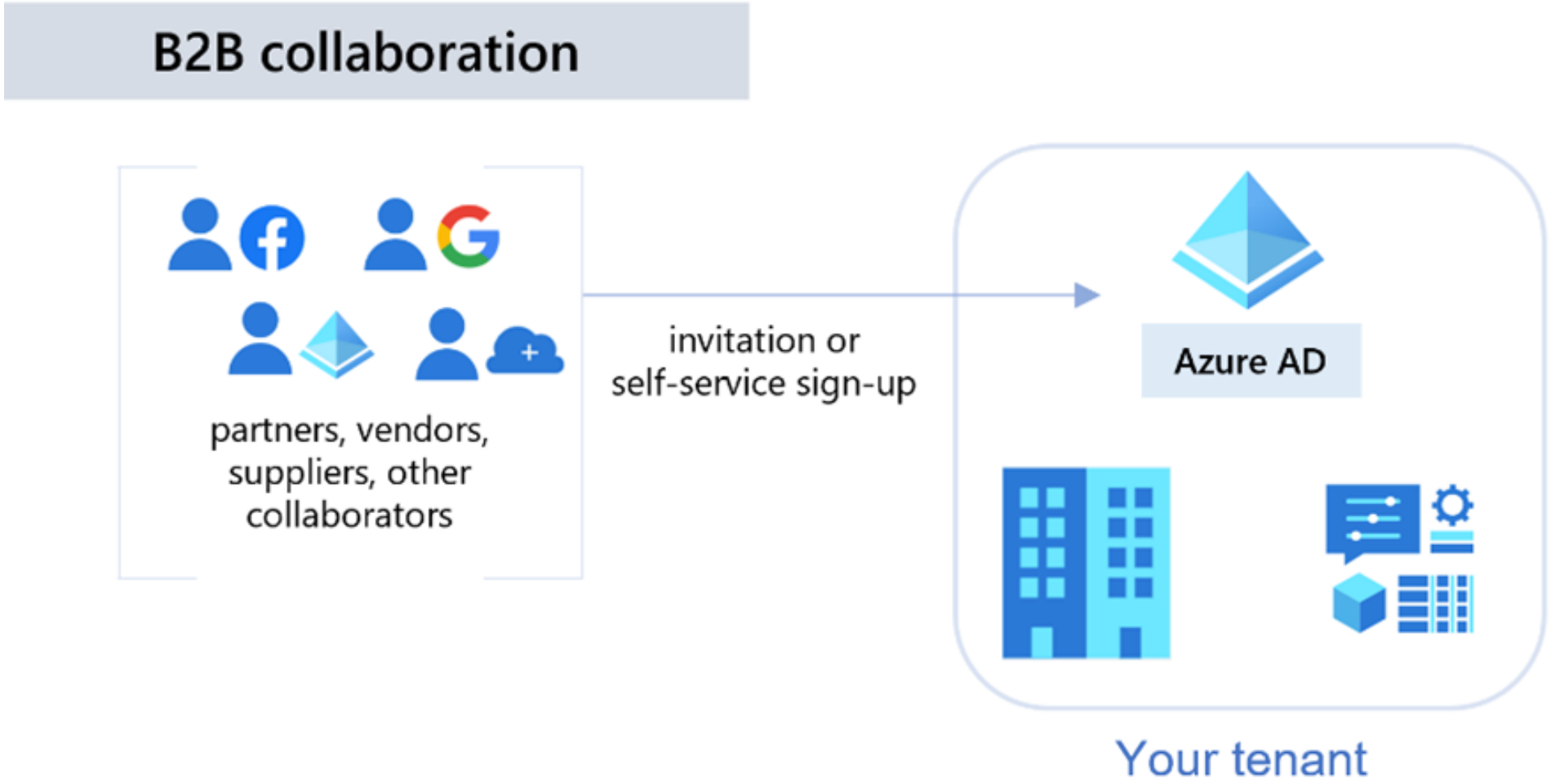


Azure Multi-Factor Authentication

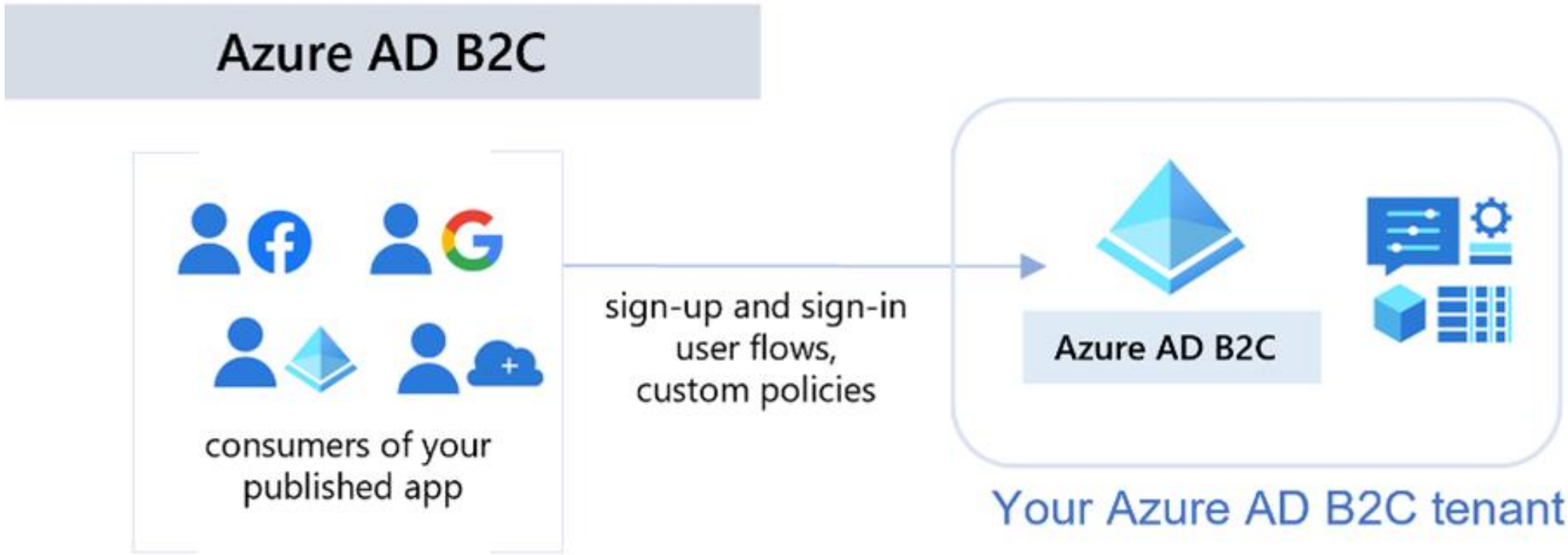
Provides additional security for your identities by requiring two or more elements for full authentication.

- Something you know ←→ Something you possess ←→ Something you are

External Identities B2B



External Identities B2C



Conditional Access

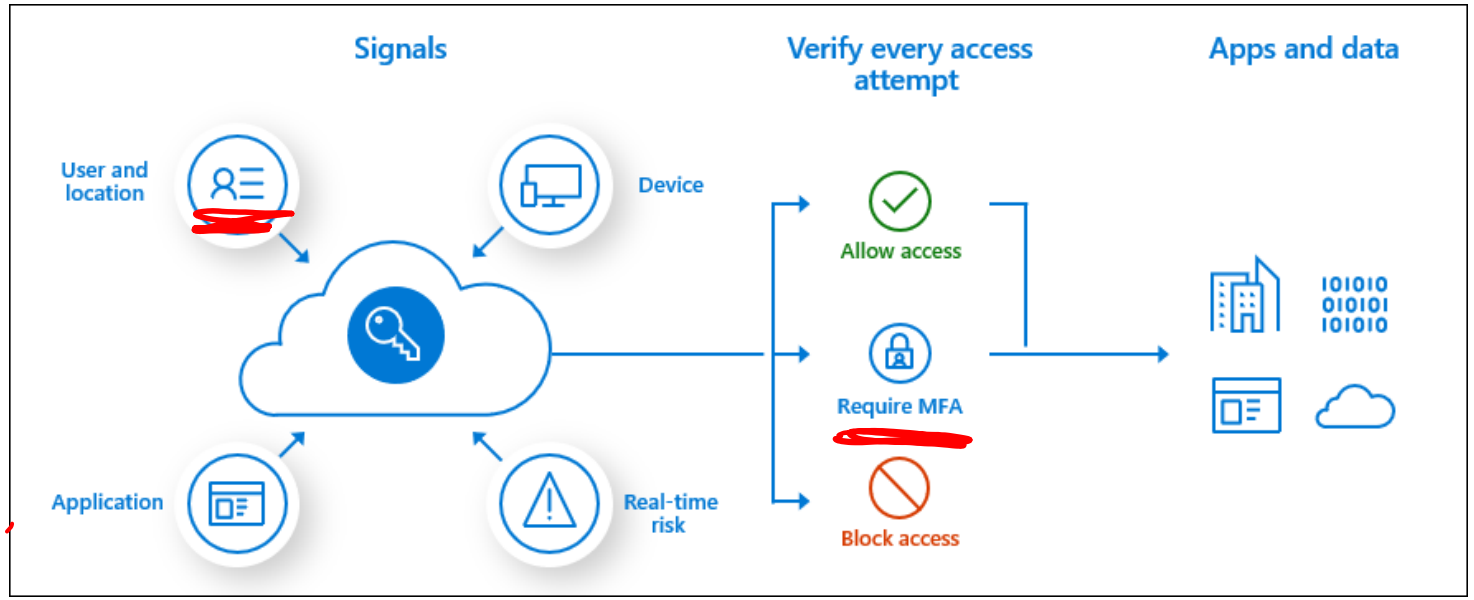
CA

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

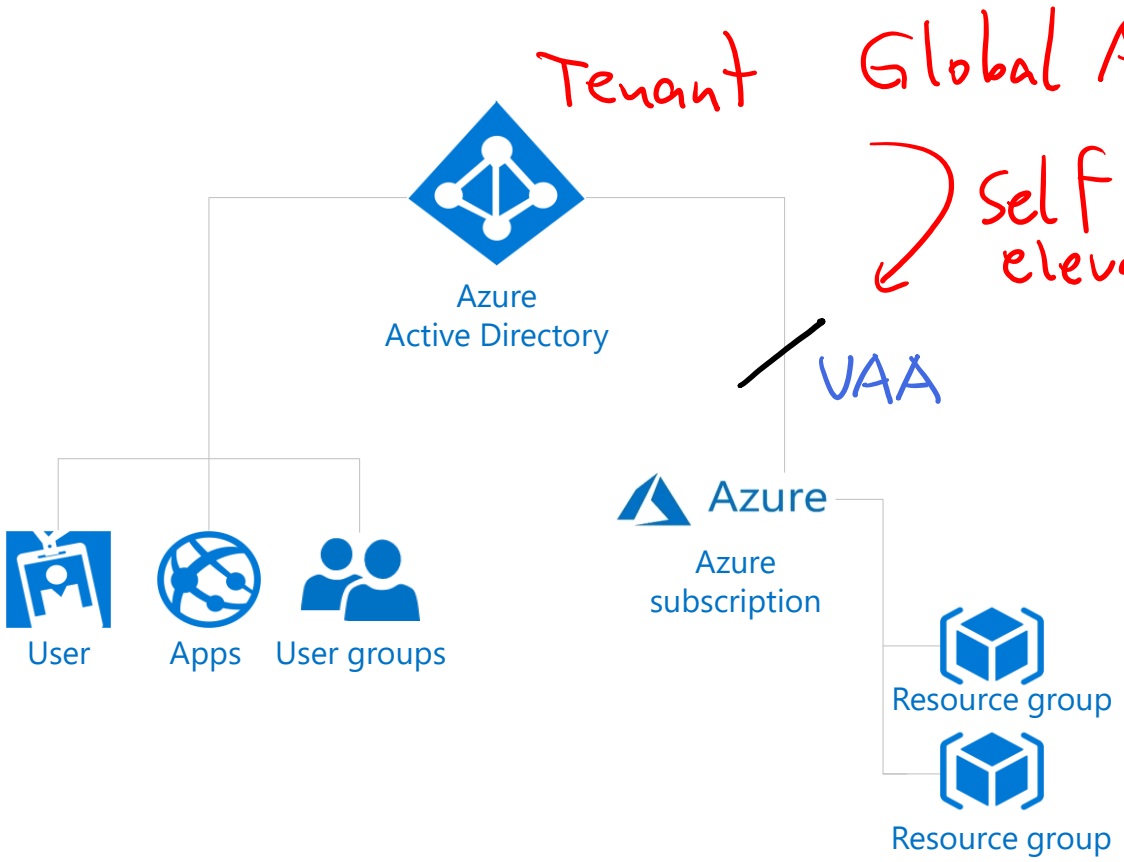
- User or Group Membership
- IP Location
- Device
- Application
- Risk Detection

Mgmt App

High
Medium
Low
None



Azure role-based access control (Azure RBAC)

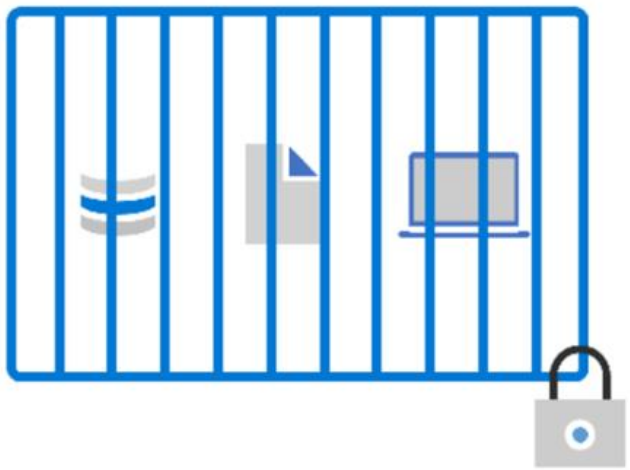


- Fine-grained access management.
- Segregate duties within the team and grant only the amount of access to users that they need to perform their jobs.
- Enables access to the Azure portal and controlling access to resources.

Zero Trust

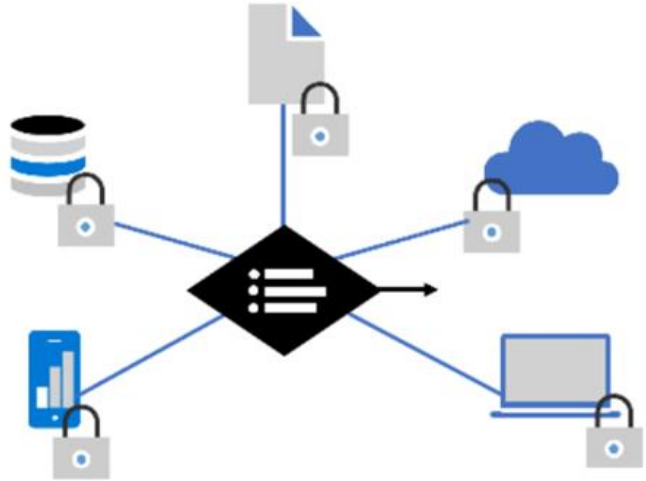
Secure assets where they are with Zero Trust

Simplify security and make it more effective



Classic Approach

Restrict everything to a 'secure' network

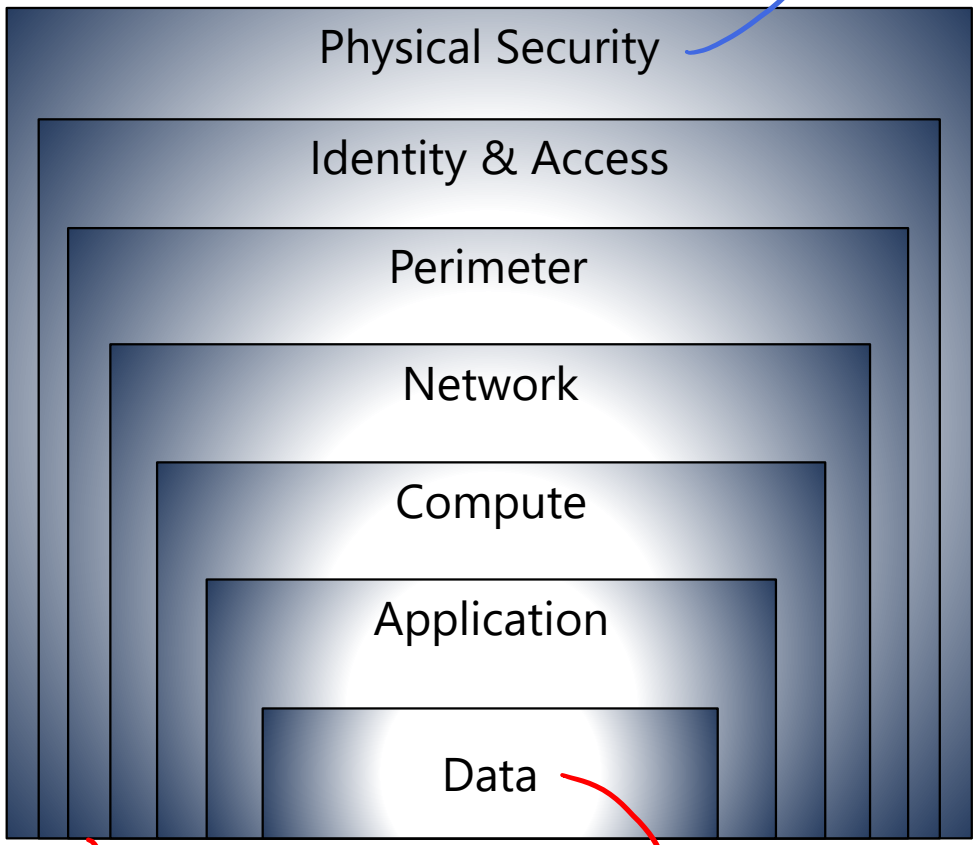


Zero Trust

Protect assets anywhere with central policy

Defense in depth

- A layered approach to securing computer systems.
- Provides multiple levels of protection.
- Attacks against one layer are isolated from subsequent layers.



Azure

On Prem
Key Vault

Fips-140
On → On

Key Vault (Premium)
Hardware

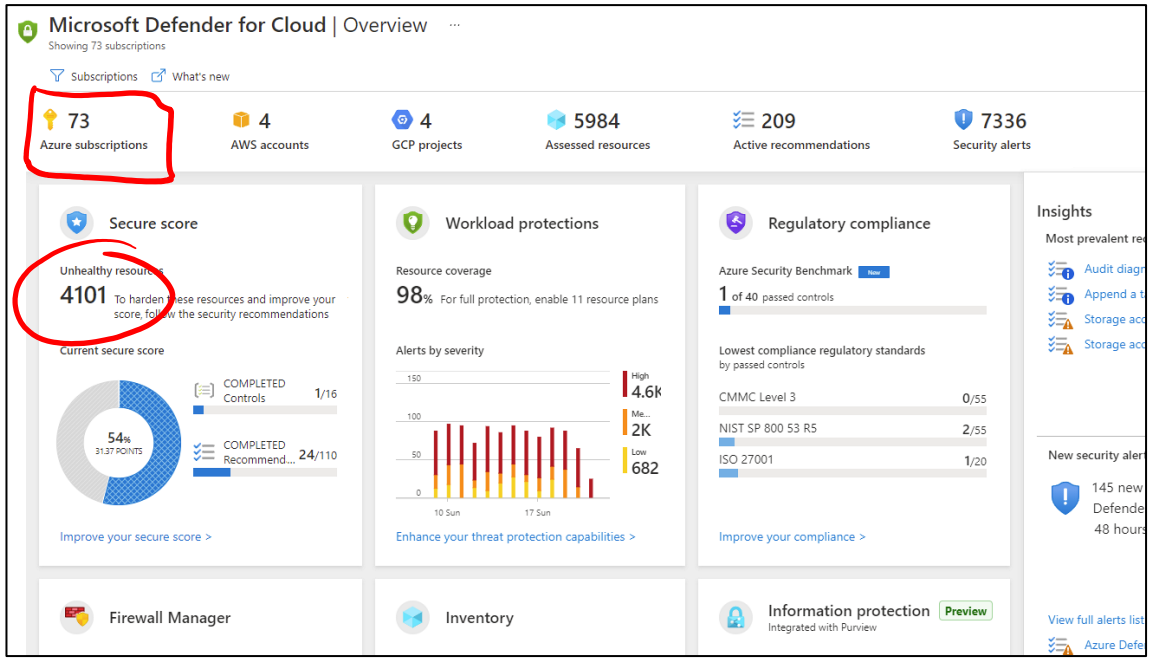
Customer

Microsoft Defender for Cloud

Defender for M365

Microsoft Defender for Cloud is a monitoring service that provides threat protection across both Azure and on-premises datacenters.

- Provides security recommendations
- Detect and block malware
- Analyze and identify potential attacks
- Just-in-time access control for ports

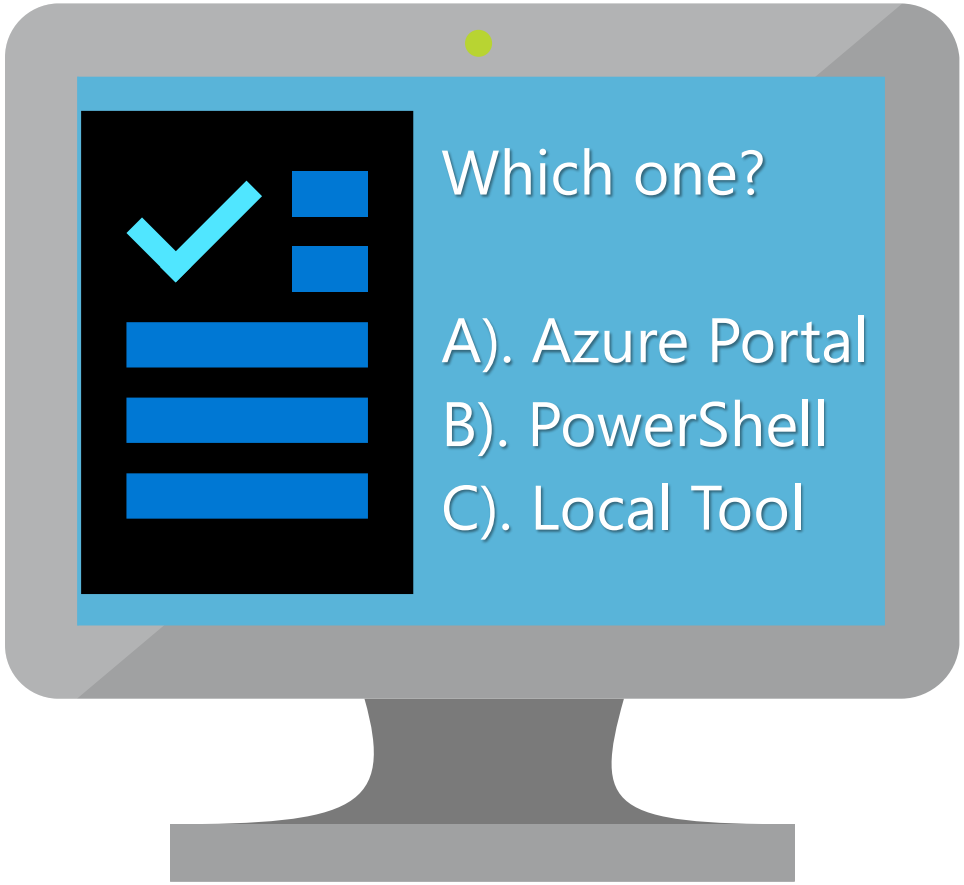


Knowledge Check

Populate with instructions to use the polling tool of your choice

Learning Path 2

1. Use your Smartphones or Mobile Devices
2. Go to *(insert polling app link of your choice)*
3. Enter Code: 123-45-678
4. Please participate in the quiz for this section



Learning Path 02 Review

Microsoft Learn Modules
(docs.microsoft.com/Learn)

- Physical and management infrastructure of Microsoft Azure
- Compute and networking services
- Storage services
- Identity, access, and security