Seminar Microsoft Azure Design

DZ-Bank Hamburg, 23. -26. Februar 2026

https://github.com/www42/Hamburg

Tag 1 Einführung
- Einführung Azure
- Einführung Künstliche Intelligenz

Tag 2 Architektur
- Azure Well-Architected Framework
- Cloud Adoption Framework

Tag 3 Azure Services
- Compute, Applications, Network, Migrations
- Storage,Databases, Data Integration

Tag 4 Deep Dive
- Governance, Authentication, Authorization, Monitoring
- Backup, Disaster Recovery, High Availability

Theoria cum Praxi

Thomas Jäkel

Heidelberg

2013 ARM

brainymotion

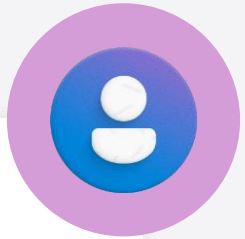
Lead Trainer Cloud Infrastructure

Microsoft Certified Trainer since 1999

https://github.com/www42/Hamburg

Let’s have a great time together

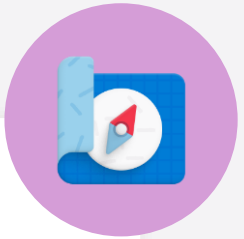
We all contribute to a great class



$9^{00} - 17^{00}$

$12^{00} - 12^{45}$

What you should know about our facilities



Get the most out of your Microsoft Learn profile

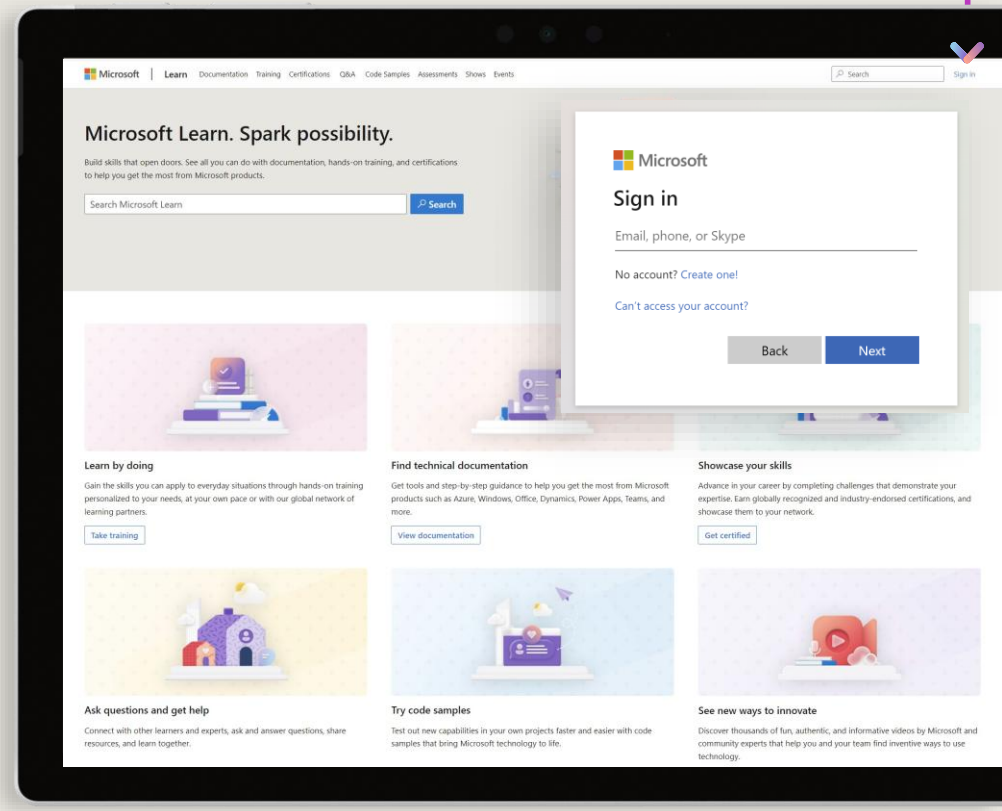
Verify, track, and share your training and certification progress and accomplishments—*all on one platform*

- Claim your achievement code for this course and share you have completed it.
- Access your course material and track progress on your learning activities.
- Share and verify your Microsoft Certifications via email, on social networking platforms, and on your résumé.
- Download and print transcripts and certificates.
- Manage your upcoming activities and certification exam appointments.

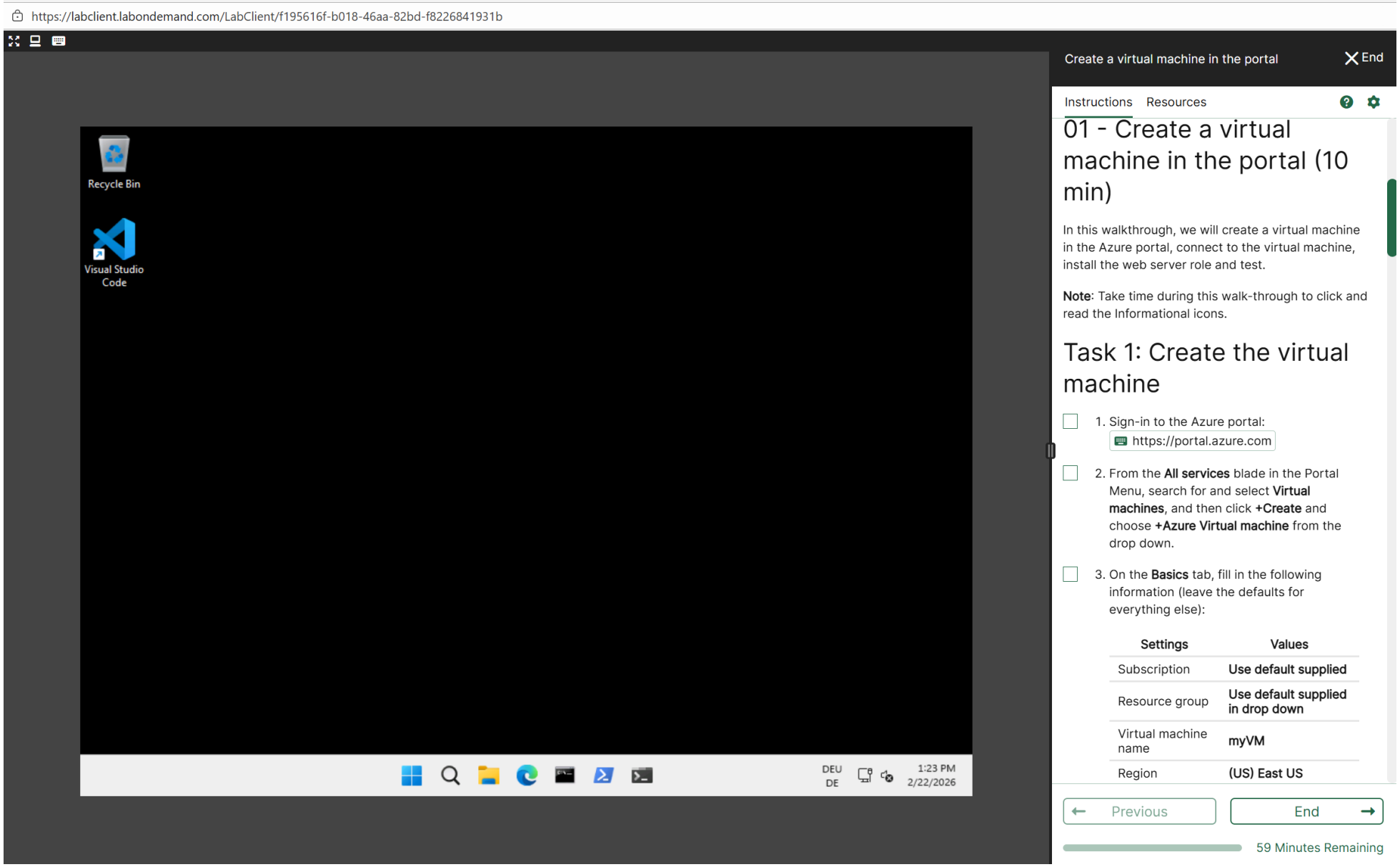
www.aka.ms/MyMicrosoftLearnProfile

Create your Microsoft Learn profile at learn.microsoft.com

- Select *Sign in* at the top, right corner of any Microsoft Learn page.
- Follow the Microsoft account authentication process.
- If the account that you have chosen to sign-in with doesn't already have a Microsoft Learn profile, you'll be guided to create one.



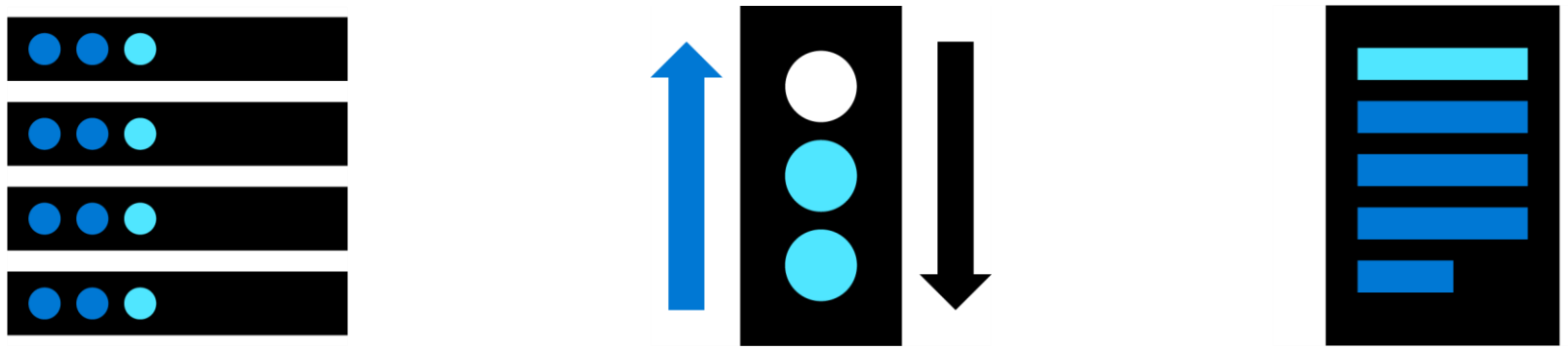
Lab Environment Skillable https://brainymotion.learnondemand.net



Cloud computing

What is cloud computing?

Cloud computing is the delivery of computing services over the internet, enabling faster innovation, flexible resources, and economies of scale.

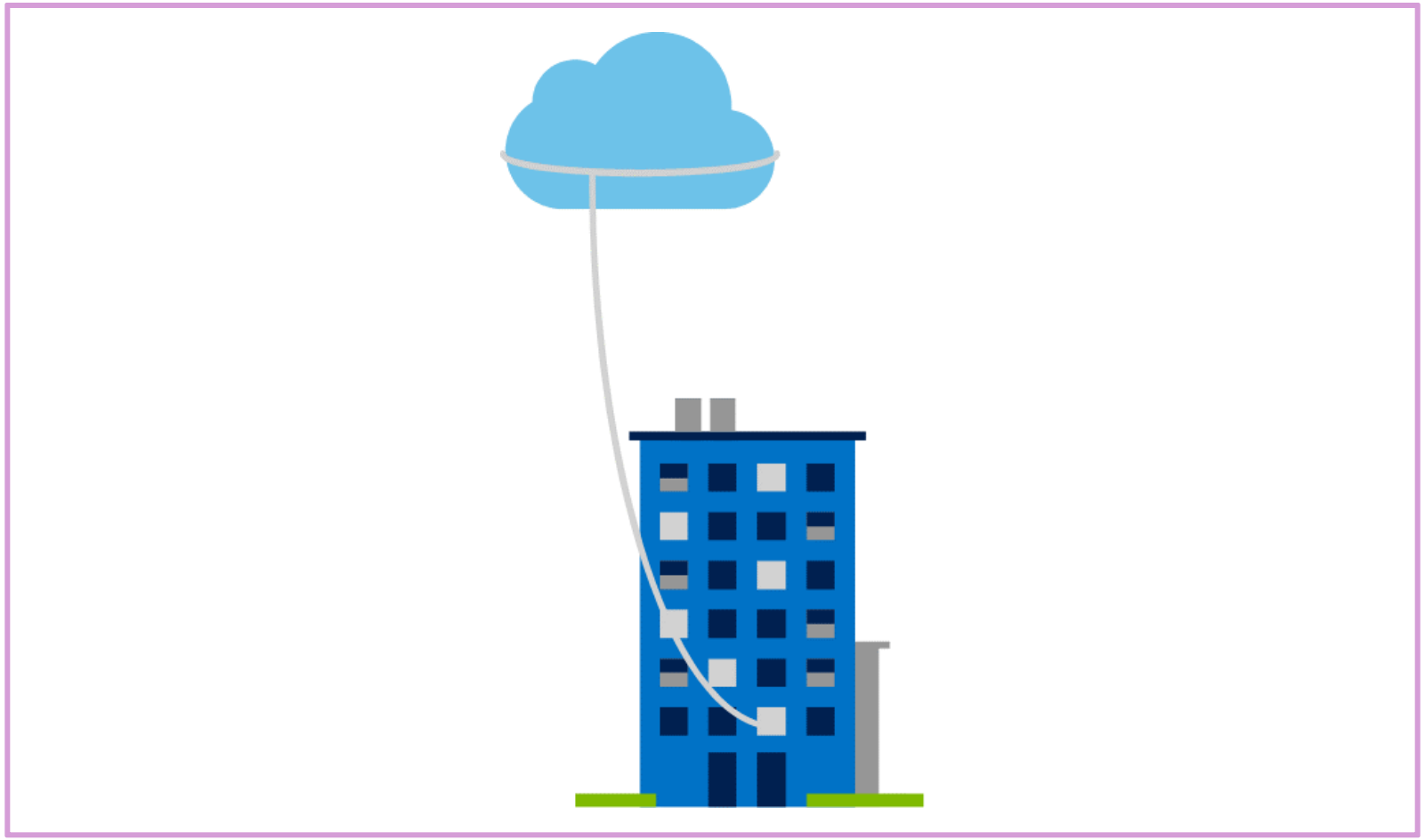


Private cloud

on Premises //

NIST 2011

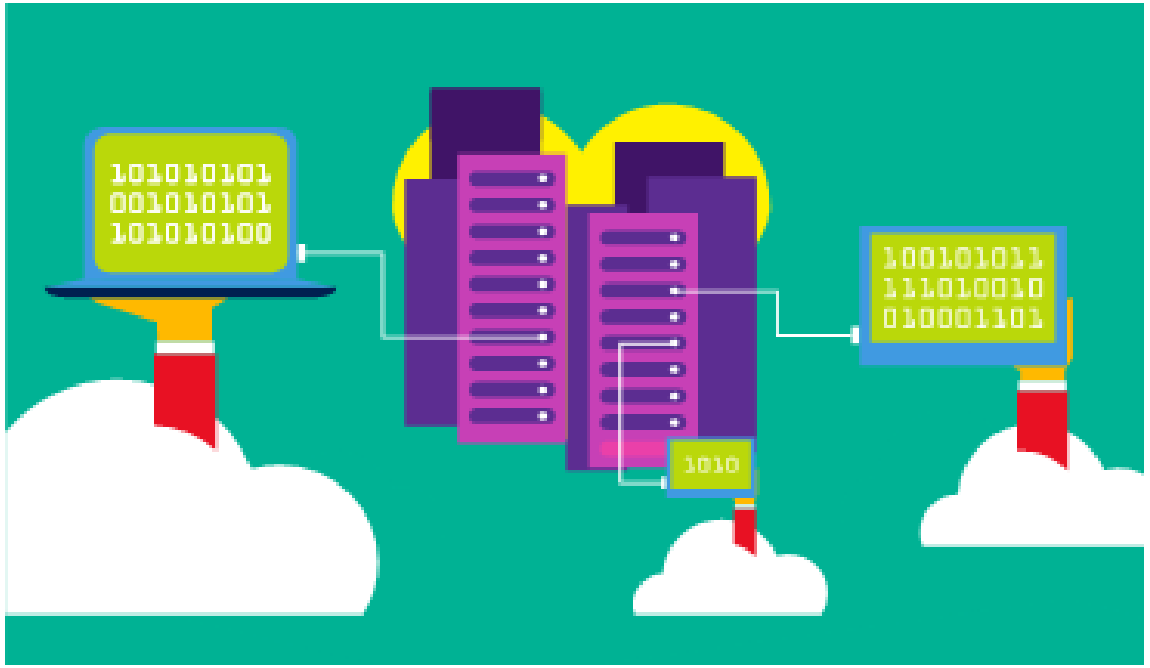
- Organizations create a cloud environment in their datacenter.
- Organizations are responsible for operating the services they provide.
- Does not provide access to users outside of the organization.



Public cloud

AWS
GCP
Azure
...

- Owned by cloud services or hosting provider.
- Provides resources and services to multiple organizations and users.
- Accessed via secure network connection (typically over the internet).



Hybrid cloud

Combines **public** and **private** clouds to allow applications to run in the most appropriate location.

Cloud model comparison

Public cloud

- No capital expenditures to scale up.
- Applications can be quickly provisioned and deprovisioned.
- Organizations pay only for what they use.

Private cloud

- Hardware must be purchased for start-up and maintenance.
- Organizations have complete control over resources and security.
- Organizations are responsible for hardware maintenance and updates.

Hybrid cloud

- Provides the most flexibility.
- Organizations determine where to run their applications.
- Organizations control security, compliance, or legal requirements.

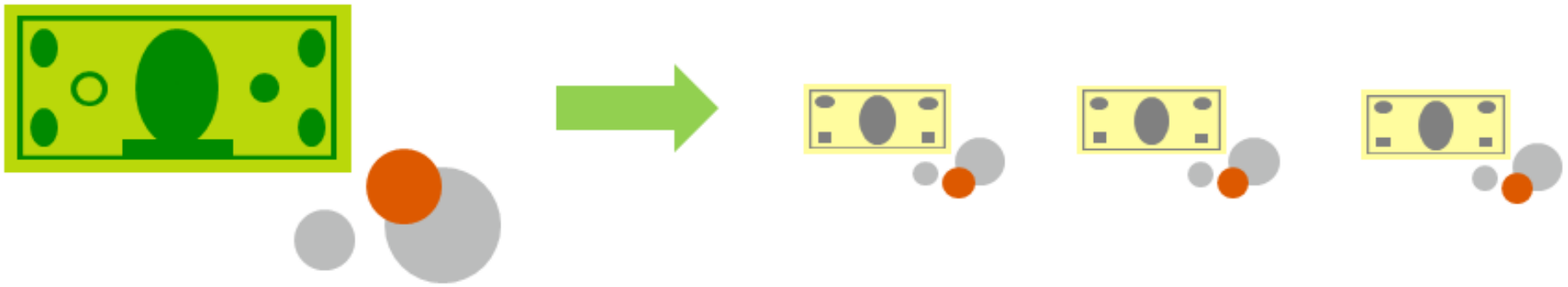
Compare CapEx vs. OpEx

Capital expenditure (CapEx)

- The upfront spending of money on physical infrastructure.
- Costs from CapEx have a value that reduces over time.

Operational expenditure (OpEx)

- Spend on products and services as needed, pay-as-you-go.
- Get billed immediately.



Consumption-based model

Cloud service providers operate on a consumption-based model, which means that end users only pay for the resources that they use.

- Better cost prediction.
- Prices for individual resources and services are provided.
- Billing is based on actual usage.

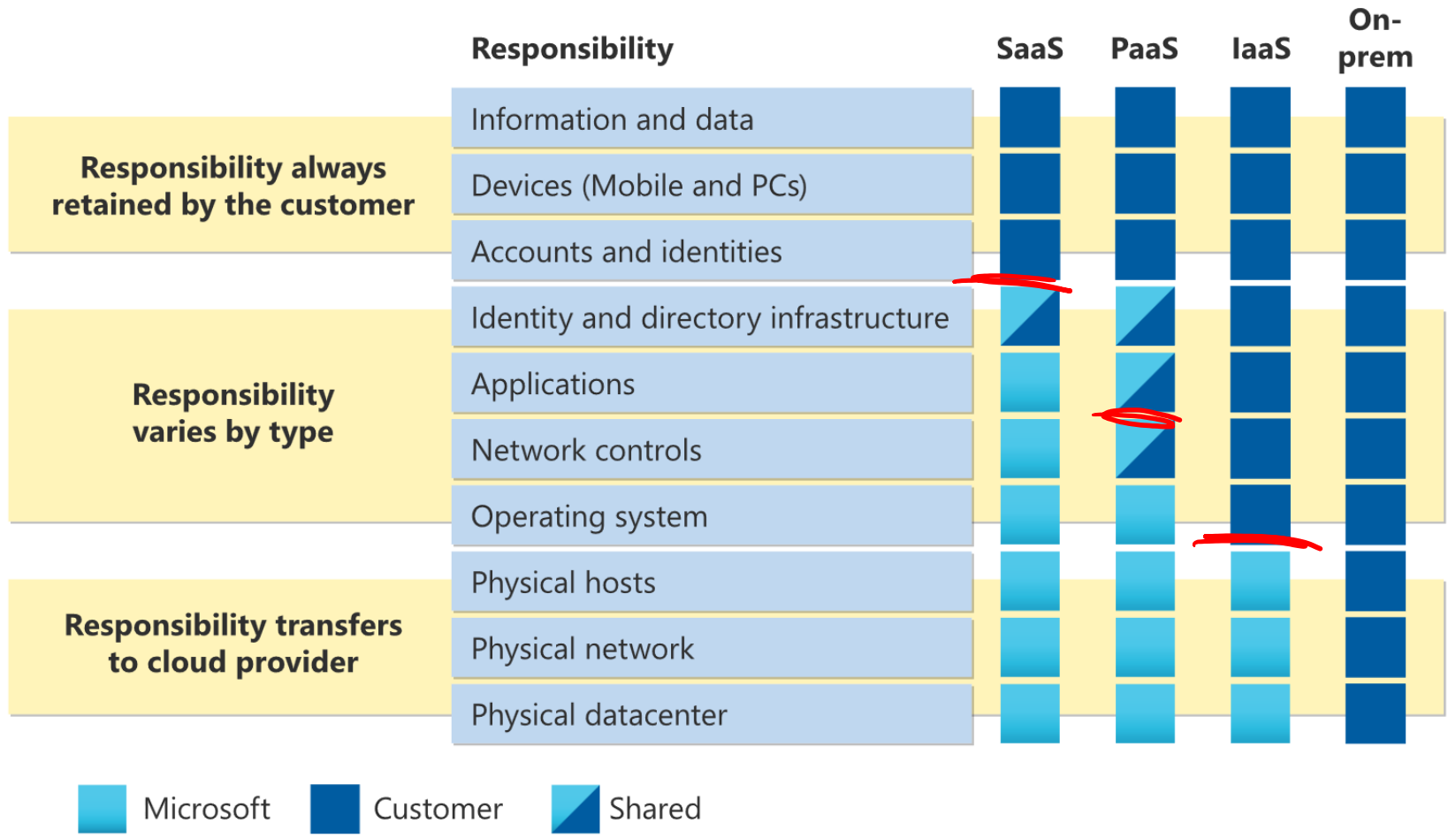
Cloud benefits

Cloud benefits

High availability	Elasticity
Scalability	Reliability
Predictability	Security
Governance	Manageability

Cloud service types

Shared responsibility model



Cloud service comparison

IaaS

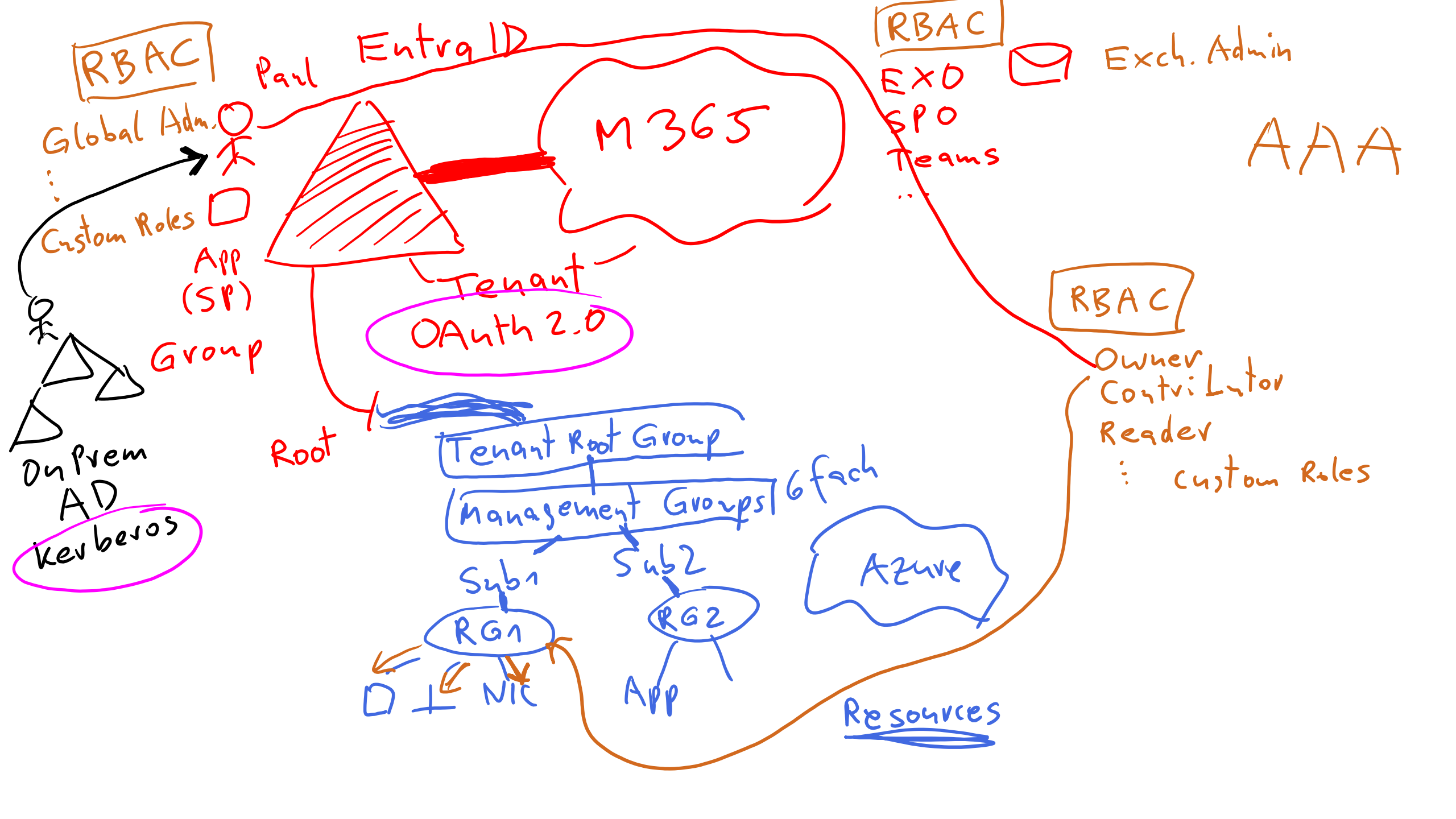
- The most flexible cloud service.
- You configure and manage the hardware for your application.

PaaS

- Focus on application development.
- Platform management is handled by the cloud provider.

SaaS

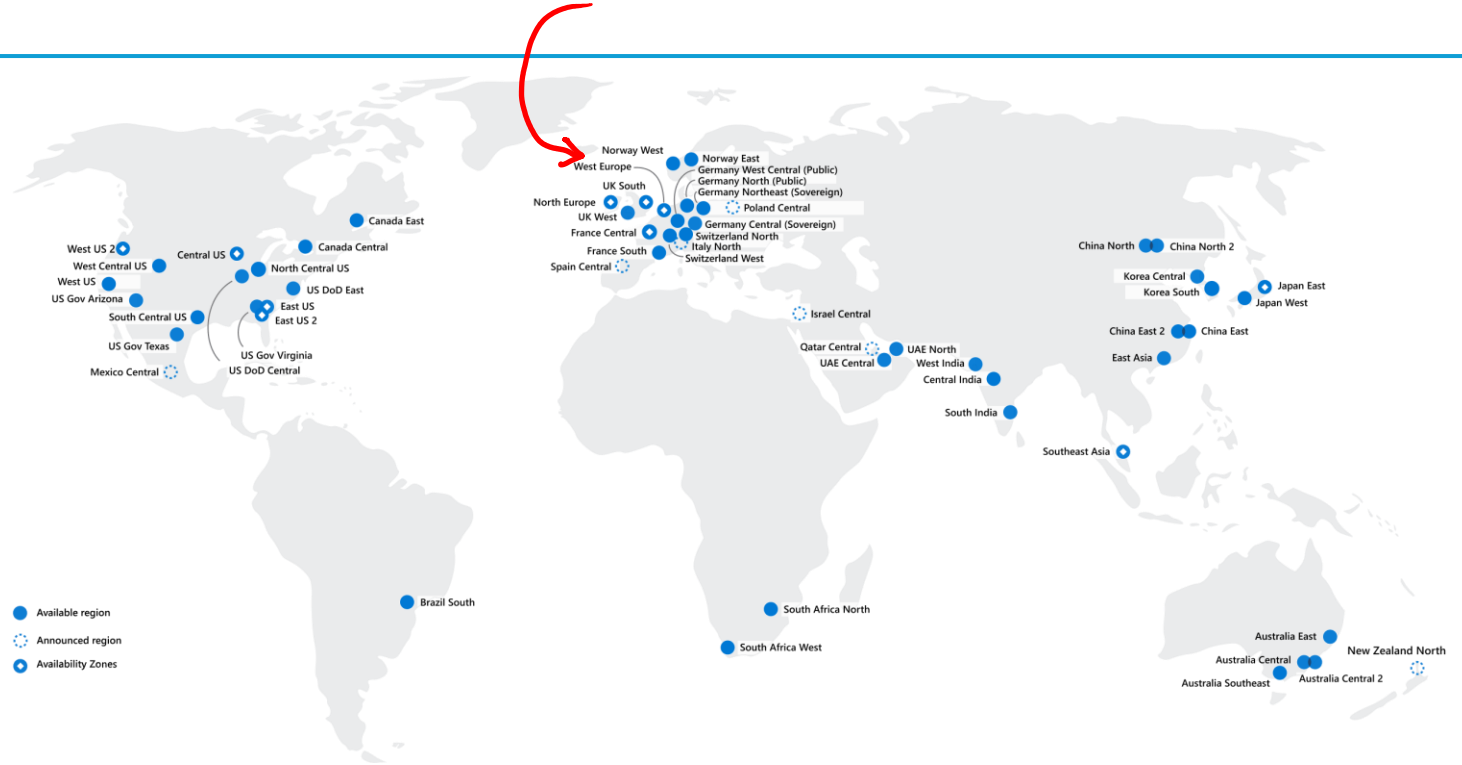
- Pay-as-you-go pricing model.
- Users pay for the software they use on a subscription model.


RBAC
Entra ID
Paul
Global Adm.
Custom Roles
App
(SP)
Group
M365
Tenant
OAuth 2.0
OnPrem
AD
Kerberos
Root
Tenant Root Group
Management Groups
6 each
Sub1
Sub2
RG1
RG2
VM
NIC
App
Azure
Resources
RBAC
EXO
SPO
Teams
...
Exch. Admin
AAA
RBAC
Owner
Contributor
Reader
: Custom Roles

Azure architectural components

Regions

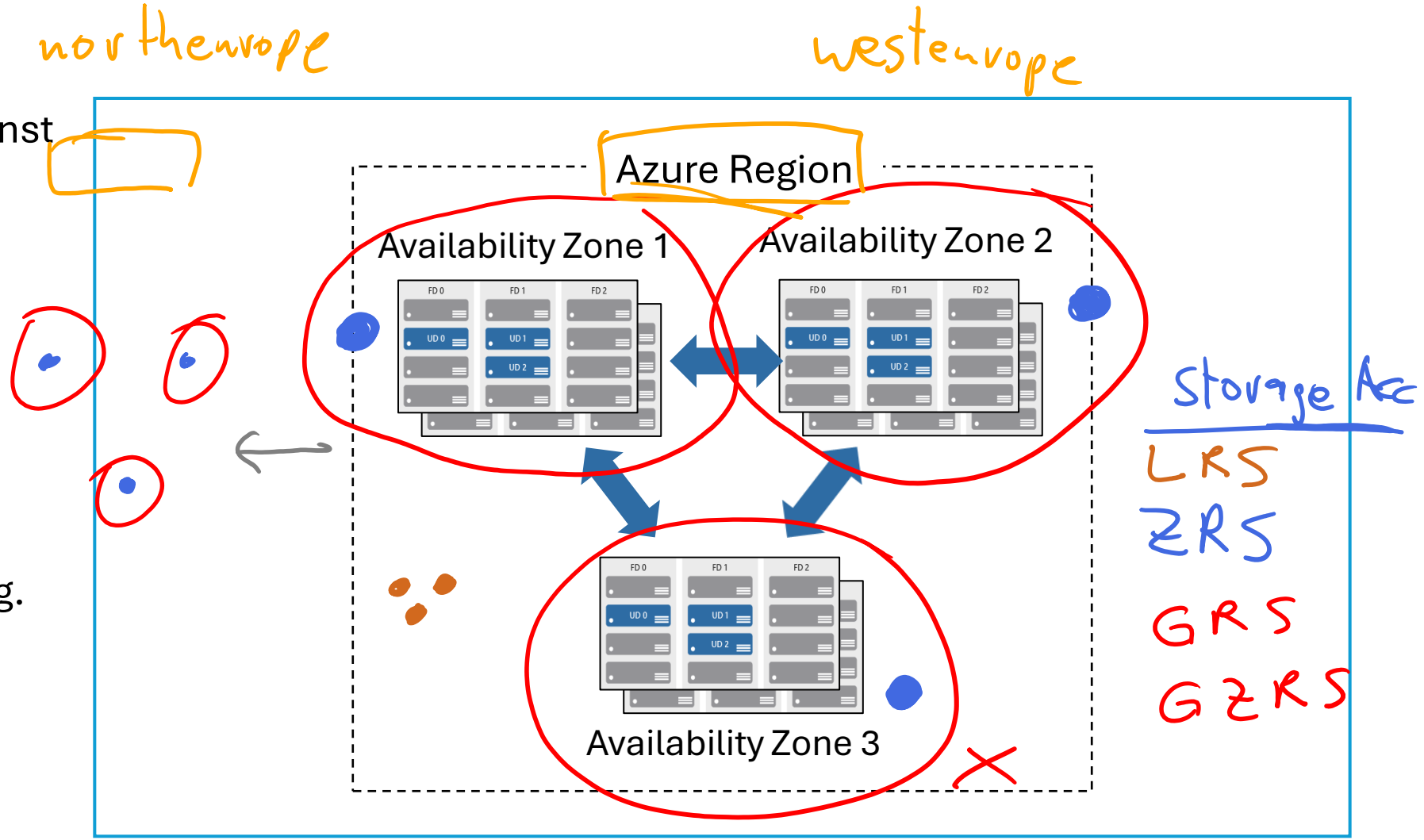
Azure offers more global regions than any other cloud provider with 60-plus regions representing over 140 countries



- Regions are made up of one or more datacenters in close proximity.
- They provide flexibility and scale to reduce customer latency.
- Regions 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 rolled out sequentially to minimize downtime.

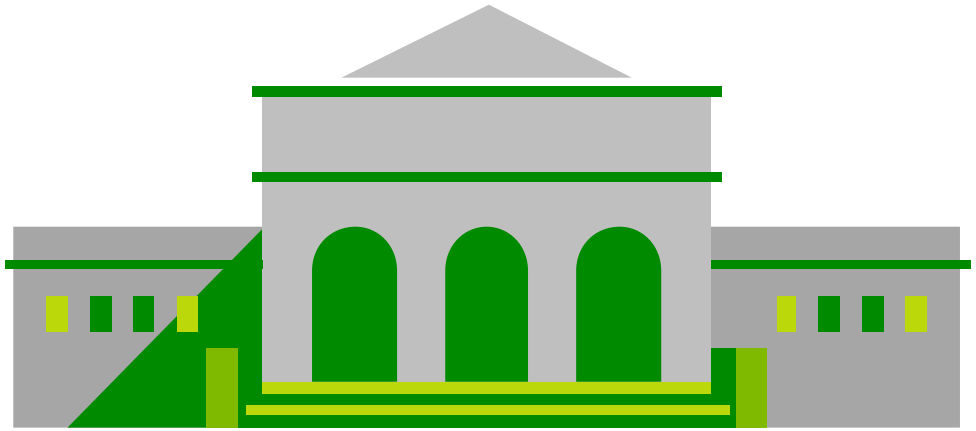
Region	Region
North Central US	South Central US
East US	West US
West US 2	West Central US
US East 2	Central US
Canada Central	Canada East
North Europe	West Europe
UK West	UK South
Germany Central	Germany Northeast
South East Asia	East Asia
East China	North China
Japan East	Japan West
Australia Southeast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

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.

Azure resources

Resource Provider

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

Microsoft.Storage/..... @ <API version>

Virtual machines

Storage accounts

Virtual networks

App services

SQL databases

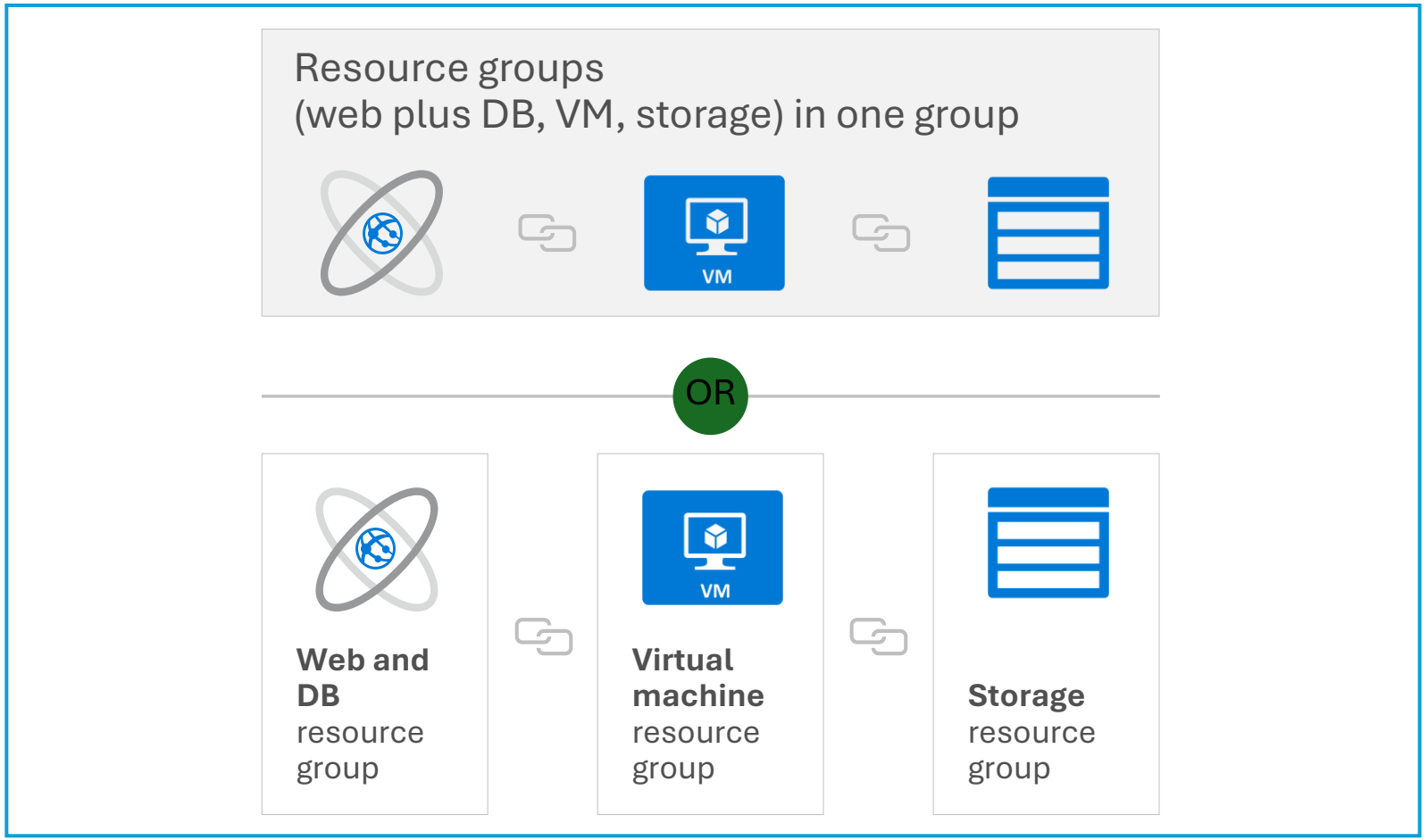
Functions

SKU

Resource groups

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

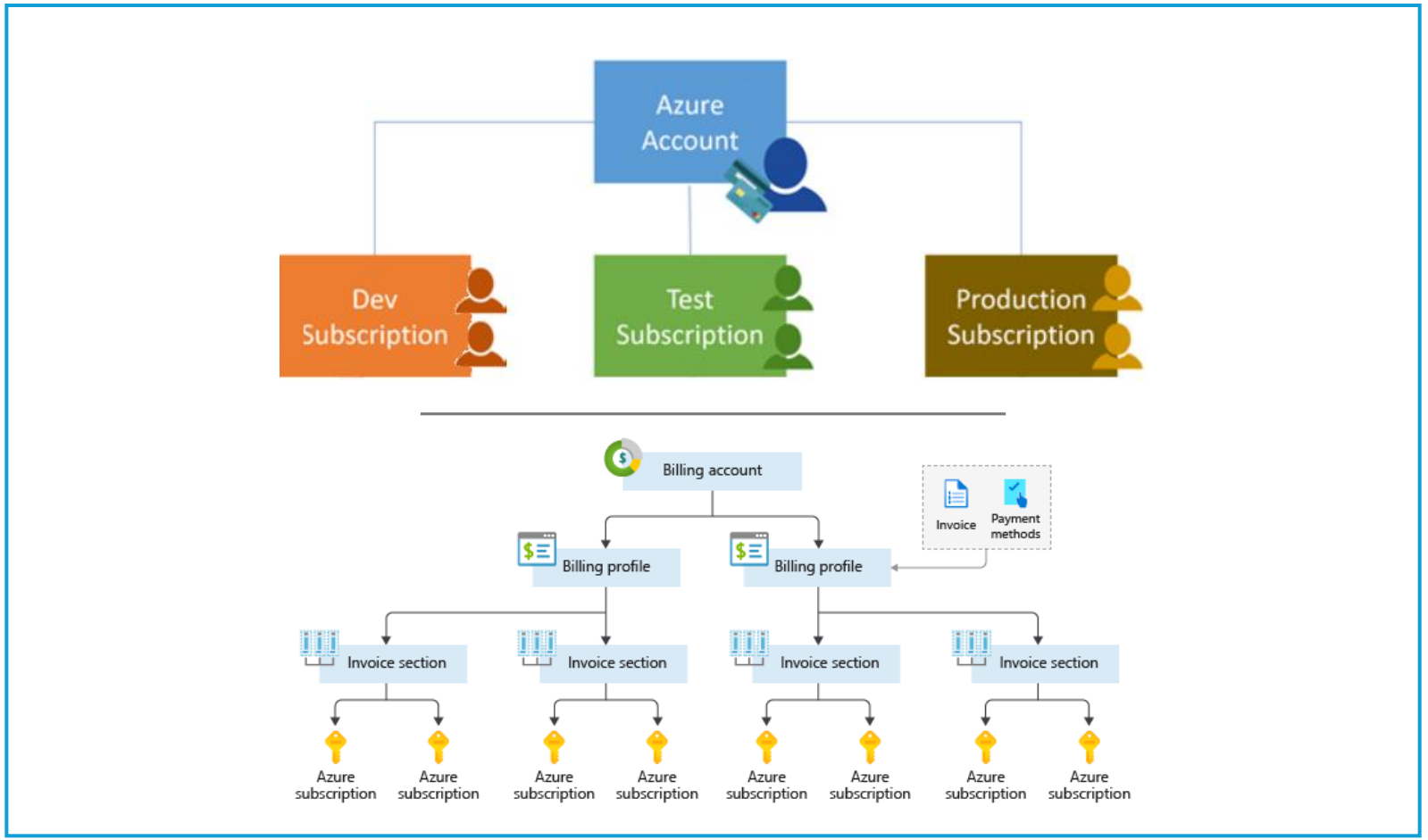
- Resources can exist in only one resource group.
- Resources can exist in different regions.
- Resources can be moved to different resource groups.
- Applications can utilize multiple resource groups.



Azure subscriptions

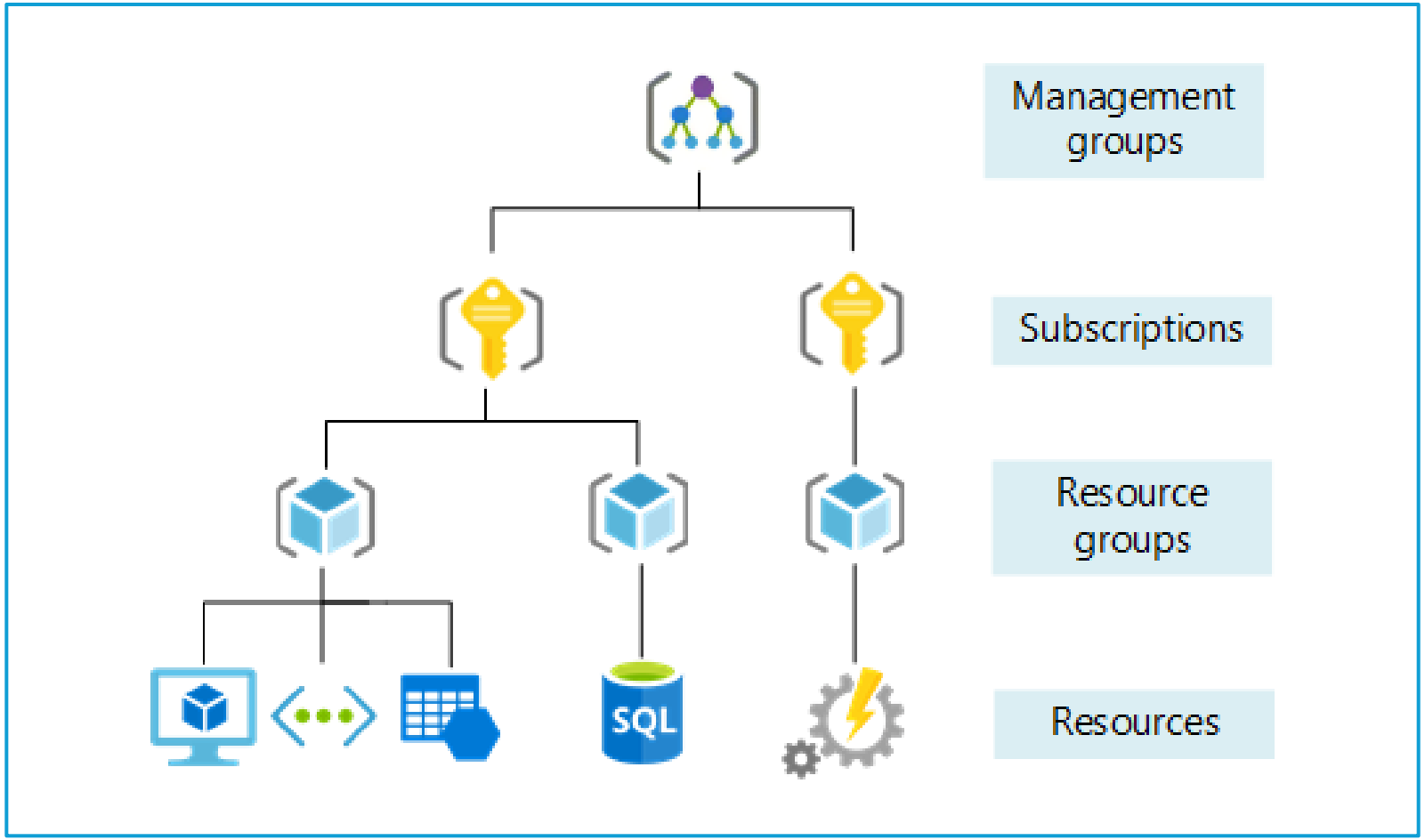
An Azure subscription provides you with authenticated and authorized access to Azure accounts.

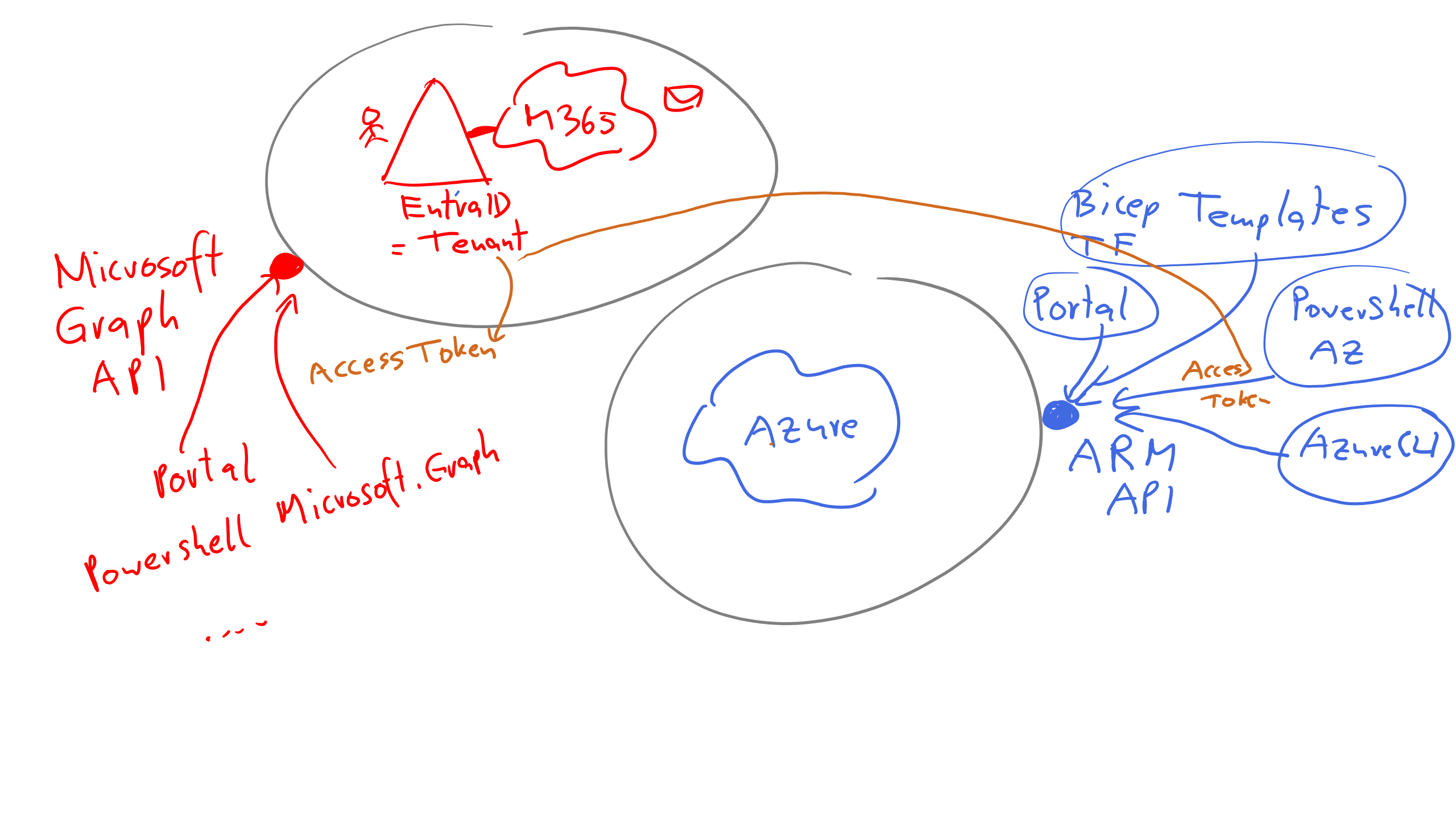
- **Billing boundary:** Generate separate billing reports and invoices for each subscription.
- **Access control boundary:** Manage and control access to the resources that users can provision with specific subscriptions.



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.

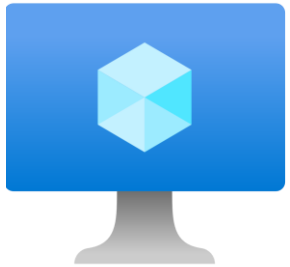



M365
EntraID
= Tenant
Microsoft
Graph
API
Portal
Powershell
...
Microsoft.Graph
Access Token
Azure
Bicep Templates
TF
Portal
Powershell
AZ
Access
Token
ARM
API
AzureCLI

Compute and networking

Azure compute services

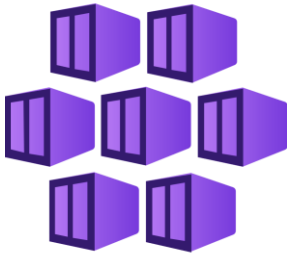
Azure **compute** is an on-demand service that provides computing resources such as disks, processors, memory, networking, and operating systems.



Virtual Machines

App Services

Container Instances



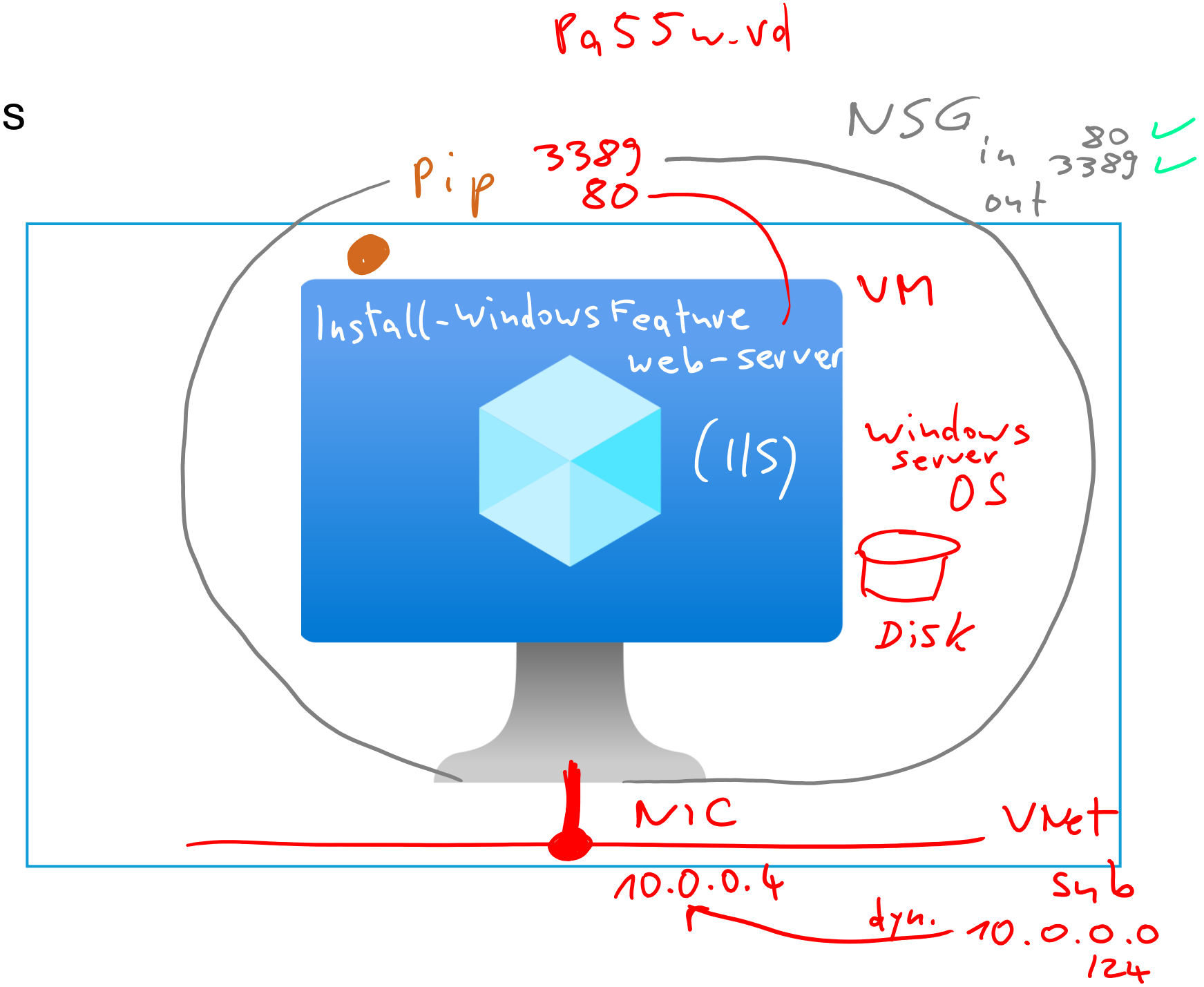
Azure Kubernetes Services (AKS)

Azure Virtual Desktop

Azure virtual machines

Azure **virtual machines (VMs)** are software emulations of physical computers.

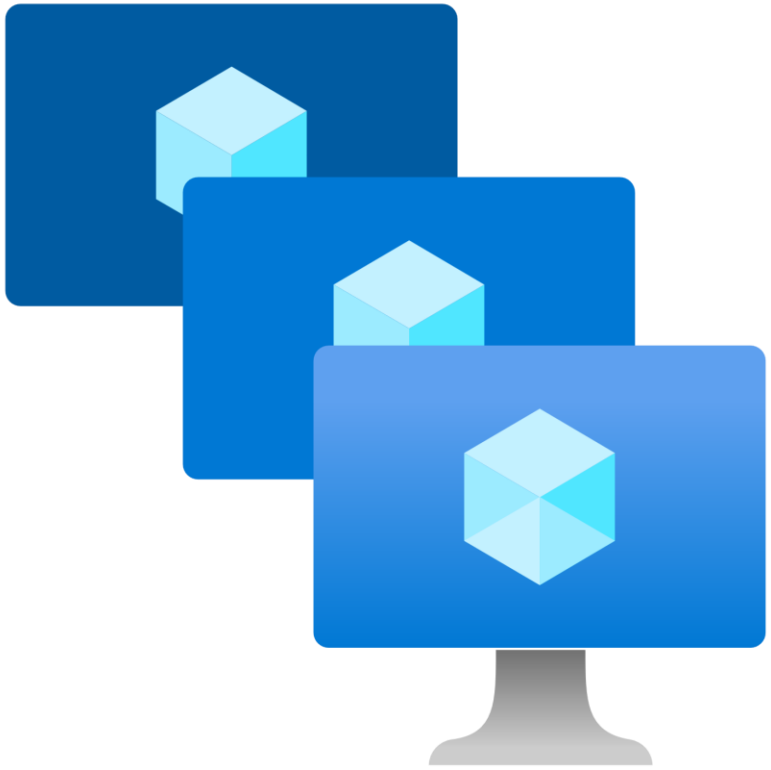
- Includes virtual processor, memory, storage, and networking.
- IaaS offering that provides total control and customization.



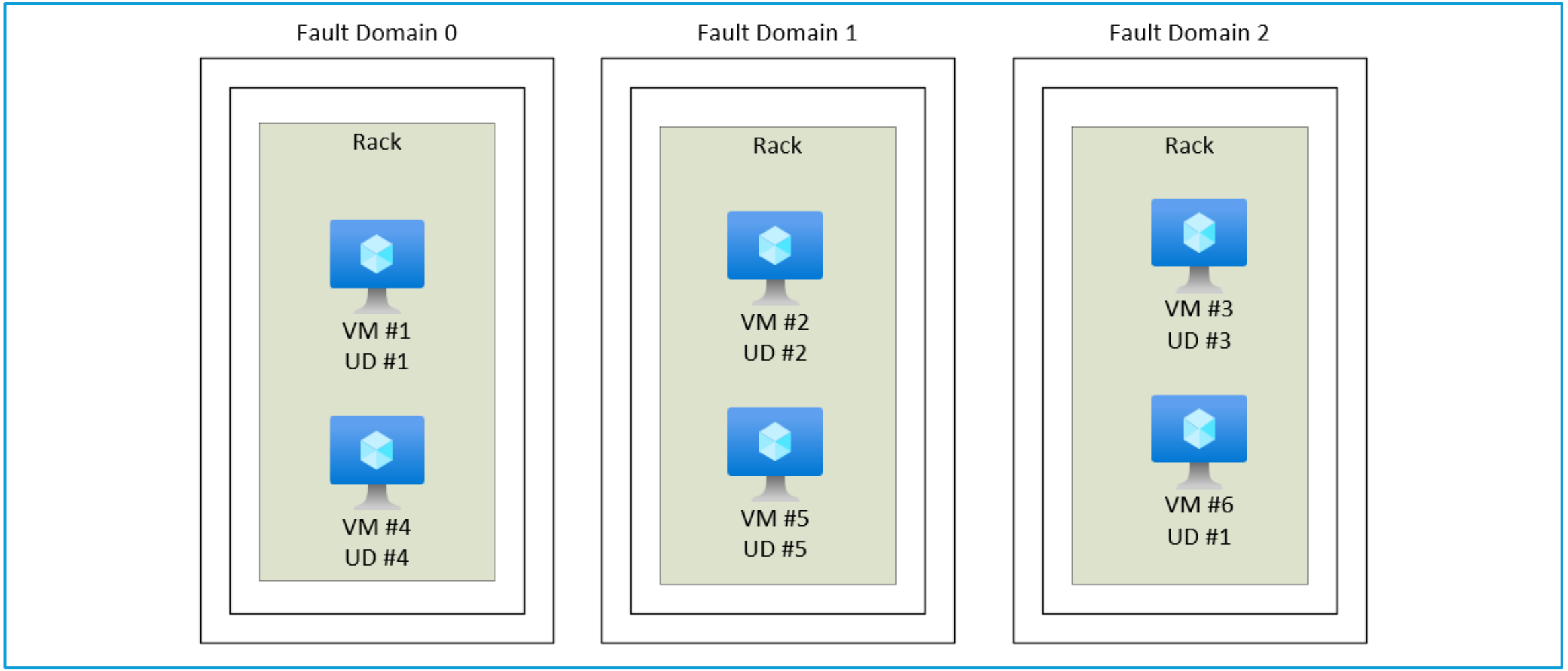
VM scale sets

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



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 multisession deployments.

Azure container services

Azure **containers** provide a lightweight, 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 or pod of containers in Azure.

Azure Container Apps: A PaaS offering, like container instances, that can load balance and scale.

K8S

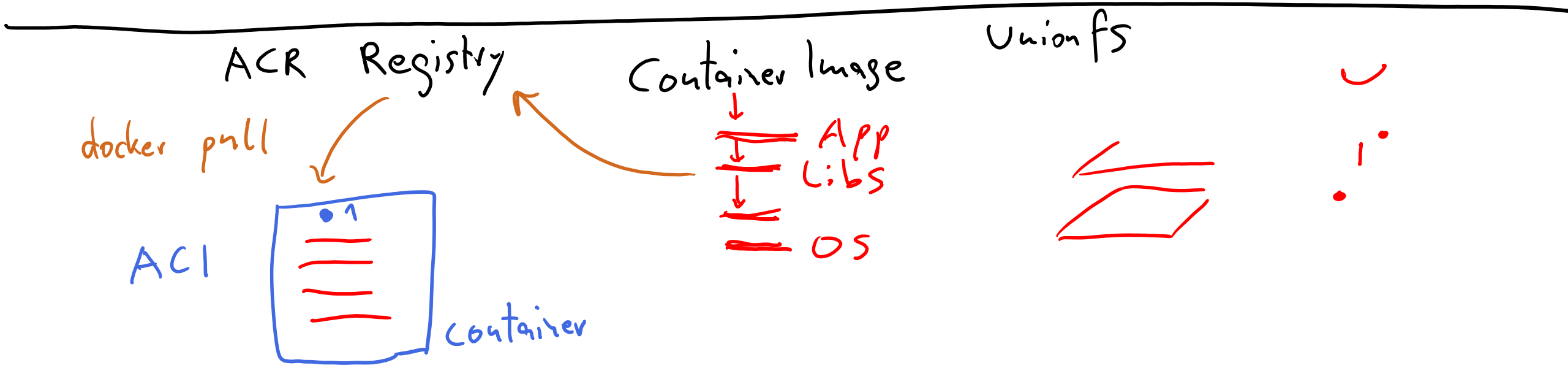
Azure Kubernetes Service: An orchestration service for containers with distributed architectures and large volumes of containers.

Azure Functions

Borg → 7/9

Brendan Burns

Azure Functions: A PaaS offering that supports serverless compute operations. Event-based code runs when called without requiring server infrastructure during inactive periods.



Comparing Azure compute options

Virtual machines

- Cloud-based server that supports either Windows or Linux environments.
- Useful for lift-and-shift migrations to the cloud.
- Complete operating system package, including the host operating system.

Virtual Desktop

- Provides a cloud-based personal computer Windows desktop experience.
- Dedicated applications to connect and use, or accessible from any modern browser.
- Multiclient login allows multiple users to log into the same machine at the same time.

Containers

- Lightweight, miniature environment well suited for running microservices.
- Designed for scalability and resiliency through orchestration.
- 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.

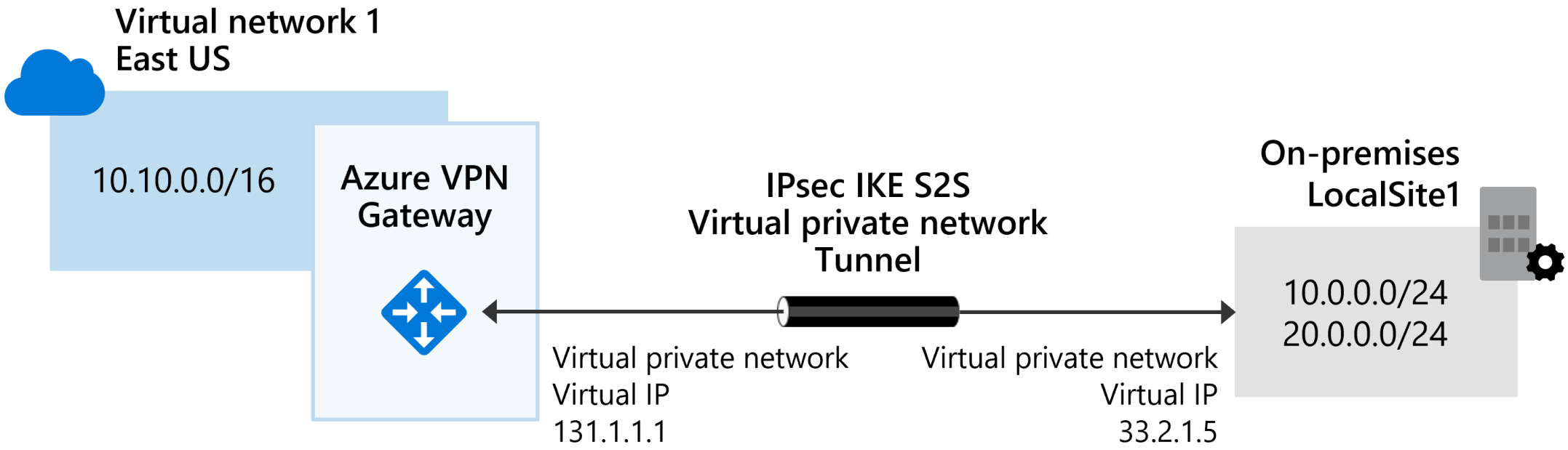
- Works with .NET, .NET Core, Node.js, Java, Python, or php.
- PaaS offering with enterprise-grade performance, security, and compliance requirements.

Azure networking services

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

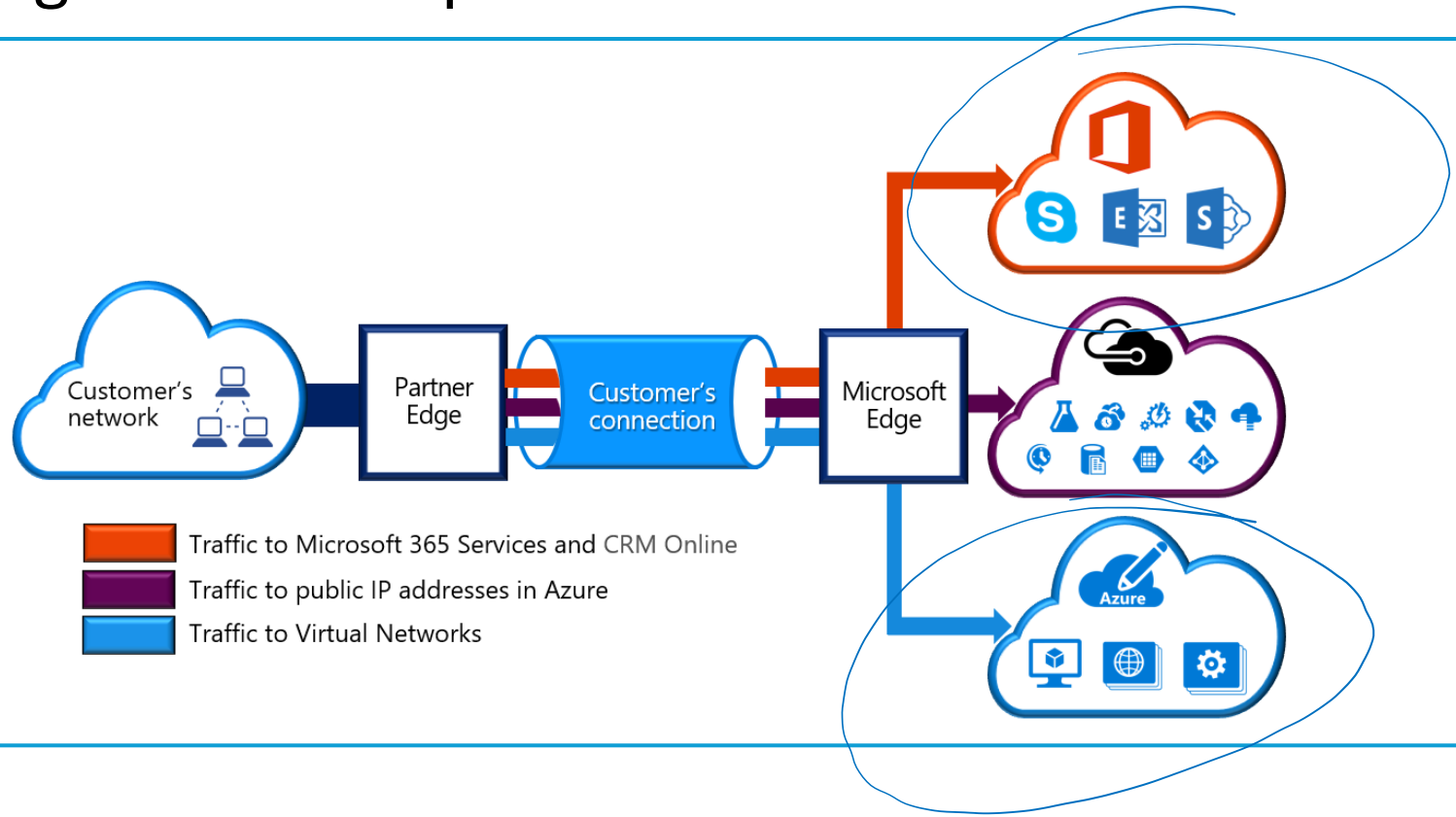
- Public endpoints, accessible from anywhere on the internet.
- Private endpoints, accessible only from within your network.
- Virtual subnets segment your network to suit your needs.
- Network peering connects your private networks directly together.

Azure networking services: VPN Gateway



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

Azure networking services: ExpressRoute



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

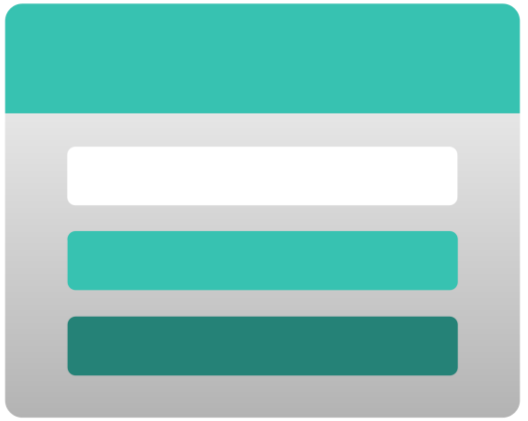
Azure DNS

- 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 your private virtual networks.
- Alias records support alias record sets to point directly to an Azure resource.

Storage

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 the secondary region	16 nines

Azure storage services

Azure Blob: Optimized for storing massive amounts of unstructured data, such as text or binary data.

Azure Disk: Provides disks for virtual machines, applications, and other services to access and use.

Azure Queue: Message storage service that provides storage and retrieval for large amounts of messages, each up up to 64 KB.

Azure Files: Sets up a highly available network file share that can be accessed by using the Server Message Block protocol.

Azure Tables: Provides a key/attribute option for structured nonrelational data storage with a schema-less design.

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

Hot	Cool	Cold	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 infrequently accessed and stored for at least 90 days.	Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements.