Microsoft Azure

- **On-demand resources**: Offers **elasticity** and **scalability** based on demand.
- **Trust Center**: Provides customers with documentation on Azure's **security standards and compliance controls**.
- **Free Trial Subscription**: Each **Microsoft account** is eligible for **one free Azure trial subscription**.

Cloud Deployment Models

- **Private Cloud**: Full control over resources. Uses **CapEx (Capital Expenditure)**, involving **one-time upfront costs** like hardware purchases.
- **Public Cloud**: Cloud resources are **owned and operated by a service provider** and delivered via the **Internet**.
- **Hybrid Cloud**: A combination of **on-premises infrastructure** and cloud-based services for **greater flexibility**.

Cloud Computing Advantages

- **Economy of Scale**: Reduces costs and improves efficiency as **operational scale increases**.
- **Cost-Effectiveness**: **Pay only for what you use**.
- **Scalability**: Adapts to **increased workload** by upgrading hardware or adding more nodes.
- **Elasticity**: Adjusts resource allocation **automatically** based on demand.

Types of Cloud Computing

- **Infrastructure as a Service (IaaS)**: Provides **scalable computing resources** that adjust automatically to workload changes.
- **Platform as a Service (PaaS)**: Eliminates infrastructure management, focusing on **application deployment and management**. Examples: **Azure App Service, Azure Functions, Azure SQL Database, Azure Cosmos DB**.
- **Software as a Service (SaaS)**: A **fully managed product** delivered via **monthly or annual subscriptions**. Includes servers, storage, networking, and software. Example: **Microsoft 365**.

Cloud Pillars

- **Governance**: Tools and practices that **ensure compliance** with corporate policies and standards.
- **Reliability**: Guarantees **stable and continuous** service operation, minimizing failures and maximizing uptime, regardless of demand fluctuations.
- **Predictability**: Helps anticipate **costs and workload behavior**, ensuring system performance remains as expected.
- **Manageability**: Simplifies **monitoring, management, and administration** of cloud resources.
- **Security**: Covers **resource protection**, including **patch management** and **network control**.
- **Agility**: Enables **quick reconfiguration** to adapt to changing business requirements.

Azure Regions and Infrastructure

- **Region:** A specific **geographical location** where Azure data centers are hosted.
- **Paired Regions:** Two **interconnected** Azure regions designed for **failover and redundancy**.
- **Availability Zones (AZ):** Provide **high availability within a region** by distributing workloads across physically separate data centers. Each AZ consists of **one or more data centers** that are **isolated from disasters**. Regions with availability zones have at least **three AZs**.
- **Point of Presence (PoP):** A **physical interconnection point** between different networks that enables **fast and reliable content delivery**.

Azure Resource Organization

- **Resource:** A **manageable element** in Azure, such as **VMs, databases, and virtual networks**.
- **Resource Group:** A **logical container** that holds related Azure resources. It does **not generate additional costs**, but is **mandatory** when creating a resource.
- **Subscriptions:** Used to **organize, control access, manage costs, and handle billing**. A single **Azure account** can have multiple subscriptions. To merge two **pay-as-you-go** subscriptions, you need to **contact Microsoft Azure support**.
- **Management Group:** A **hierarchical structure** that allows organizing and managing **multiple Azure subscriptions**. It **sets roles and permissions** at a group level to **unify access management**. Non-root management groups can have **one parent group** and **multiple child groups**.

Global Azure Services

- **Azure Active Directory (Azure AD): Identity and access management** service.
- **Azure Traffic Manager: DNS-based traffic load balancer** (does not handle HTTPS).

Azure Administration Tools

- **Azure Portal:** A **web-based unified console** to manage Azure resources. On **Chromebooks**, both **Azure Portal** and **Azure Cloud Shell** (PowerShell & Bash) are available. https://portal.azure.com/
- **Azure CLI:** A **command-line tool** based on **Bash**, available for **Windows, macOS, and Linux**.
- **Azure PowerShell:** A command-line tool for managing Azure resources, accessible from the **Azure Portal**.
- **Azure Resource Manager (ARM): Centralized resource management and orchestration** platform.
- **Azure Advisor:** Provides **best practice recommendations** to enhance **performance, security, and reliability**, while also identifying **cost-saving opportunities**.

Azure Virtual Machines (VMs)

- **Azure VMs** operate under the **IaaS (Infrastructure as a Service) model** and can be deployed in:
  - **Availability Zones**
  - **Regions**
  - **Subscriptions**
  - **Resource Groups**
- **Cost Considerations:**
  - VMs **continue generating storage costs** even after deletion if the associated disks are not removed.
  - Pricing is based on **size, uptime, additional resources, data input/output, and data transfer**.
  - Charges apply **whether the VM is actively used or not**.
  - **Deletion locks** can be applied to prevent accidental VM removal.

Azure Compute and Scaling Solutions

- **Availability Set:** Groups **two or more VMs** within the same physical Azure data center location. If a VM fails, only the subset within the same set is affected.
- **Spot Instances:** Cost-effective **intermittent workloads** with lower reliability since they can be interrupted. Not recommended for critical workloads.
- **Virtual Machine Scale Sets (VMSS):** A **group of identical, load-balanced VMs** that can be **automatically scaled** as demand increases. You only pay for the VM, storage, and network resources used—there are no additional costs for scale sets.

Scaling Strategies

- **Vertical Scaling:** Increases **CPU/RAM** by deploying the application or database on a **larger instance**. This may cause **downtime**.
- **Horizontal Scaling:** Adds **more instances** of a resource (e.g., VMs or containers) to a resource group.
    - Can be performed **without downtime**.
    - Can be **automated based on demand** (elasticity, auto-scaling).

High Availability

- Ensures applications/systems run in **at least two Availability Zones**.
- In a **public cloud**, high availability depends on the **Service Level Agreement (SLA)** chosen by the user.

Azure App and Container Services

- **App Service (PaaS):** A **fully managed platform** for deploying, managing, and scaling web applications. Integrates **VMs, scale sets, load balancers, Azure SQL Database**, and other services.
- **Azure Container Instances (ACI):** The **main Azure service for running containerized workloads**.
    - **On-demand model** → Saves costs by provisioning container instances only when needed.
- **Azure Kubernetes Service (AKS):** An **open-source container orchestration system** for **automating deployment, scaling, and management** of containerized applications.

Serverless Computing in Azure

- **Azure Functions:**
    - **Serverless architecture** (supports Azure App Service, Azure Event Grid, and Azure Logic Apps).
    - **Auto-scaling** and **event-driven execution**—only runs when data needs to be processed.
    - **Pay-as-you-go** model—no charges when inactive.
- **Azure Logic Apps:** Connects and automates workflows between multiple systems **without writing code**.

Azure Networking

- **Azure Virtual Network (VNet):** Provides an **isolated private network** in the cloud for running Azure resources securely.
- **Subnets:** Can be secured individually, improving **IP address allocation** and grouping related services within a **VNet**.
- **VNet Peering:** Enables **private connectivity** between two VNets, even across different regions, using Azure's backbone network.
- **Azure Load Balancer:** Distributes **incoming traffic** across multiple **VM instances** in different **Availability Zones**, ensuring **high availability**.
- **Azure VPN Gateway:** Creates **secure connections** between Azure networks and **on-premises infrastructure** using **encrypted VPN tunnels**.
- **Azure Application Gateway:** A **web traffic load balancer** that routes traffic based on **URL paths**.
- **Azure ExpressRoute:** Provides **private, high-speed connectivity** between **on-premises infrastructure and Azure**, bypassing the public Internet.
- **Network Security Group (NSG):** A **traffic filter** that enforces security rules for resources within a **VNet**.
    - Cannot be directly associated with a **VNet**, only with **subnets** inside the VNet.

Azure Storage Services

- **Azure Blob Storage:** Stores **large unstructured data** such as images and documents, accessible directly via a browser.
- **Storage Access Tiers:**
    - **Hot:** Frequently accessed data (**lower access time, higher cost**).
    - **Cool:** Less frequently accessed data (**lower storage cost, higher access time**). Data must remain in this tier for **at least 30 days**.
    - **Archive: Lowest storage cost**, but **highest access time** for rarely accessed data.

Disk Storage Types

- **Premium SSD: Ultra-fast, low-latency storage** designed for **critical workloads**.
- **Ultra Disk:** Supports workloads with **high data intensity** (up to **64TB per disk**).

Other Storage Solutions

- **Azure File Storage:** Secure, serverless, **enterprise-grade file shares** for cloud-based collaboration.
- **Azure Archive Storage: Cost-effective** solution for **long-term storage** of infrequently accessed data.
    - Supports **encryption, authentication, and industry compliance**.

Azure Storage Redundancy

If a copy fails or becomes inaccessible, Azure Storage ensures **data availability** by automatically creating **multiple copies**.

Storage Redundancy Options

- **Single Region:**
    - **Locally Redundant Storage (LRS):** The most **cost-effective** storage option, protecting against **hardware failures** within a **single region**.
        - **No protection** against **zone or regional outages**.
        - **Free** data transfer within the same Azure region.
    - **Zone-Redundant Storage (ZRS):** Unlike LRS, ZRS replicates data across **multiple Availability Zones** within the **same region**, increasing **durability and availability**.

- **Multiple Regions:**
    - **Geo-Redundant Storage (GRS):** Replicates data to **geographically separated data centers**, providing protection against **regional disasters**.
        - In case of a failure in the primary region, data remains accessible in the **secondary region**.
    - **Geo-Zone-Redundant Storage (GZRS):**
        - Combines the **benefits of ZRS and GRS** for **maximum protection**.
        - Data is stored in **three Availability Zones** in the primary region and replicated to a **secondary region**.

Azure Storage Management Tools

- **AzCopy:** A command-line tool for **transferring data to and from Azure Storage**.
    - Used for **blob storage, Azure Files, and large-scale data transfers**.

- **Azure Storage Explorer:** A **graphical UI tool** for **managing Azure Storage**.
    - Allows users to **upload, download, delete, rename, and explore** stored data.
- **Azure File Sync: Syncs Azure Files with on-premises file servers**, allowing **remote users** to access cloud-stored files.
- **Azure Data Box:** A **physical device provided by Microsoft** for transferring **large amounts of data** when **bandwidth is limited**.
- **Azure Migrate:** Analyzes and **automatically assesses on-premises applications and servers** for smoother cloud migration.
    - Provides **cost estimation** for migrating workloads to Azure.
- **Premium Page Blobs:** High-performance **premium storage solution** designed for **intensive workloads**.
- **Azure Files: Enterprise-grade** shared cloud storage that supports **SMB and NFS protocols**.
- **Queue Storage:** A **message queueing service** that enables communication between **cloud application components**.

Azure Security and Protection Services

- **Azure Information Protection (AIP):** Protects **emails, PDFs, and Office documents**, but **not virtual hard disks (VHDs)**.

Microsoft Entra ID & Identity Management

- **Microsoft Entra ID:** Cloud-based **identity and access management** service from Microsoft.
    - Supports **Single Sign-On (SSO)** and **Multi-Factor Authentication (MFA)**.
    - Offers **advanced security features** via **Microsoft Entra ID Protection**.
    - An **Azure subscription** can only be linked to **one Microsoft Entra ID directory**.
    - Supports **hybrid architectures** (Azure Cloud + on-premises data center).
- **Azure Privileged Identity Management (PIM):**
    - A **security service** within **Entra ID** for **managing and monitoring privileged access** across **Azure, Entra ID, and Microsoft 365**.
- **Tenant:** A **dedicated instance** of Microsoft Entra ID representing an **organization within Azure**.
    - Users typically belong to **one tenant** but can be **invited as external (guest) users** in up to **499 other tenants**.
- **Microsoft Entra Connect:** A **local Microsoft application** enabling **hybrid identity synchronization** by linking on-premises **Active Directory with Microsoft Entra ID**.
- **Zero Trust:** A **security strategy** requiring **continuous verification of all access attempts**, regardless of location.
- **Multi-Factor Authentication (MFA):**
    - Can be implemented **without a federated solution**.
- **Conditional Access:**
    - Collects **signals** to **enforce policies and make access decisions**.
    - Often used to **implement MFA across an organization**.
- **Passwordless Authentication in Microsoft Entra ID:**
    - **Windows Hello**
    - **Microsoft Authenticator App** (mobile MFA)
    - **FIDO2 Security Keys**

Azure Government & External Access

- **Azure Government Cloud:** Dedicated **regions for government data isolation** and **restricted personnel access**.
- **External User Access:**
    - Azure **guest users** can be **invited** to a **tenant**, allowing them to collaborate using their **existing account** (**B2B collaboration**).
- **Azure Active Directory Domain Services (Azure AD DS):**
    - A **fully managed domain service** for authentication, authorization, and security policies in Azure.
    - Supports **legacy authentication protocols** like **NTLM**.
- **Single Sign-On (SSO) in Microsoft Entra ID:**
    - Enables **seamless access** to multiple applications using **a single credential**.

Azure Networking & Security

- **Cloud Connectivity Options:**
    - **Internet**
    - **Point-to-Site (P2S) and Site-to-Site (S2S) VPN**
    - **Azure ExpressRoute** (private high-speed connection)
- **Private Endpoints:**
    - Secure **private network connections**, reducing public exposure.
- **Microsoft Defender for Cloud:**
    - **Cloud-native security platform** providing **threat alerts** and **compliance monitoring**.
    - **Multi-cloud support** (Azure, AWS, GCP) via **Azure Arc registration**.
- **Role-Based Access Control (RBAC):**
    - Defines **who (security principal) can perform which actions** on **Azure resources**.
    - **Assigns roles and permissions** at different **scopes (resource, resource group, subscription)**.
- **Resource Locks:**
    - Prevent **accidental deletion or modification** of **critical resources**.
    - Can be applied at **resource, resource group, or subscription level**.

Azure Monitoring & Compliance

- **Azure Monitor:**
    - Provides **real-time monitoring, logging, and alerting**.
    - Tracks **CPU usage, network activity, and subscription-wide metrics**.
    - Enables **proactive alerts** (e.g., **high CPU usage on a VM**).
    - Alert setup requires **alert rules and action groups**.
- **Azure Policy:**
    - Ensures **organization-wide compliance** by enforcing **governance standards**.
- **Azure Blueprints:**

    - Enables **repeatable infrastructure deployment** with **predefined templates** (ARM templates, policies, and RBAC roles).

- **Azure Resource Manager (ARM):**
    - **Infrastructure as Code (IaC) solution** for **deploying Azure resources** like **VMs and databases**.
- **Log Analytics:**
    - **Stores and queries Azure Monitor data** using **Kusto Query Language (KQL)**.
- **Application Insights:**
    - Focused on **web application performance monitoring** and **user interaction analysis**.
- **Azure Service Health:**
    - Provides **incident reports and maintenance alerts** to mitigate downtime.
- **Azure Arc:**
    - Extends Azure management services to **on-premises and multi-cloud environments**.
    - Enables **RBAC, Azure Blueprints, and Azure Policy for hybrid infrastructure**.
    - Supports **serverless execution of Azure Functions** on **local containers**.
    - Required for **managing AWS EC2 instances** and **securing them via Microsoft Defender for Cloud**.

Azure Cost Management & Optimization

- **Azure Cost Management:**
    - **Monitors, controls, and optimizes costs** for Azure resources.
    - Costs vary **by region**, with **monthly billing cycles (30-60 days)**.
    - Enables **budget creation** and **alerts for unexpected high expenses**.
    - Integrates with **Azure Advisor** for cost-saving recommendations.
- **Azure Pricing Calculator:**
    - Estimates **Azure service costs** for better financial transparency.
- **Total Cost of Ownership (TCO) Calculator:**
    - Compares **on-premises vs. Azure infrastructure costs**.
- **Data Transfer Costs:**
    - **Inbound data (to Azure) is free**.
    - **Outbound data (leaving Azure) incurs charges**.
- **Resource Tagging (Tags):**
    - Helps **classify and track resources** based on **projects or departments**.
    - **Tags applied to a resource group are NOT inherited** by resources within the group.
- **Azure Advisor:**
    - Provides **personalized recommendations** for **cost, performance, and security optimization**.
- **Reserved Instances:**
    - **Long-term commitment** in exchange for **discounted VM pricing**.