AZ-900: AZURE FUNDAMENTALS

COURSE ON UDEMY, document v3.1

INSTRUCTOR: SCOTT DUFFY

WITH SEAN XIE

www.udemy.com/az900-azure

Table of Contents

SECTION 1: Intro to Course

The exam covers the topics on the following page:

- https://learn.microsoft.com/en-us/credentials/certifications/azure-fundamentals/

Passing the exam gets you the “Microsoft Certified Azure Fundamentals” badge. The certification has no expiry date. Good for “life”.

Optional exam. Not a prerequisite to any of the other Microsoft Exams. But it’s a good way to get a solid understanding of Azure before jumping in to the future exams.

Currently $99 USD. Available in English, Japanese, Chinese (Simplified), Korean, Spanish, German, French, Indonesian (Indonesia), Arabic (Saudi Arabia), Chinese (Traditional), Italian, Portuguese (Brazil), Russian

The exam covers:

- Describe cloud concepts (25-30%)
- Describe Azure architecture and services (35-40%)
- Describe Azure management and governance (30-35%)

Who’s the Exam For?

- Candidates with non-technical backgrounds, such as those involved in selling or purchasing cloud-based solutions and services or who have some involvement with cloud-based solutions and services, and
- Candidates with a technical background who have a need to validate their foundational level knowledge around cloud services.

SECTION 2: Cloud Concepts (25-30%)

Introduction to Cloud Computing

Cloud Computing Definition

Cloud computing refers to the **on-demand delivery of computing services** — such as **compute**, **storage**, **networking**, **databases**, **AI/ML**, and more — **over the internet**, with the following characteristics:

- **On-demand self-service** — deploy resources within minutes
- Pay-as-you-go (consumption-based) — only pay for what you use
- No upfront hardware costs
- Massive scalability & global availability
- Managed infrastructure — no need to buy or maintain physical servers

This ability unlocks so much value in the ability of businesses (like mine and yours) to deliver our products and services to the end users.

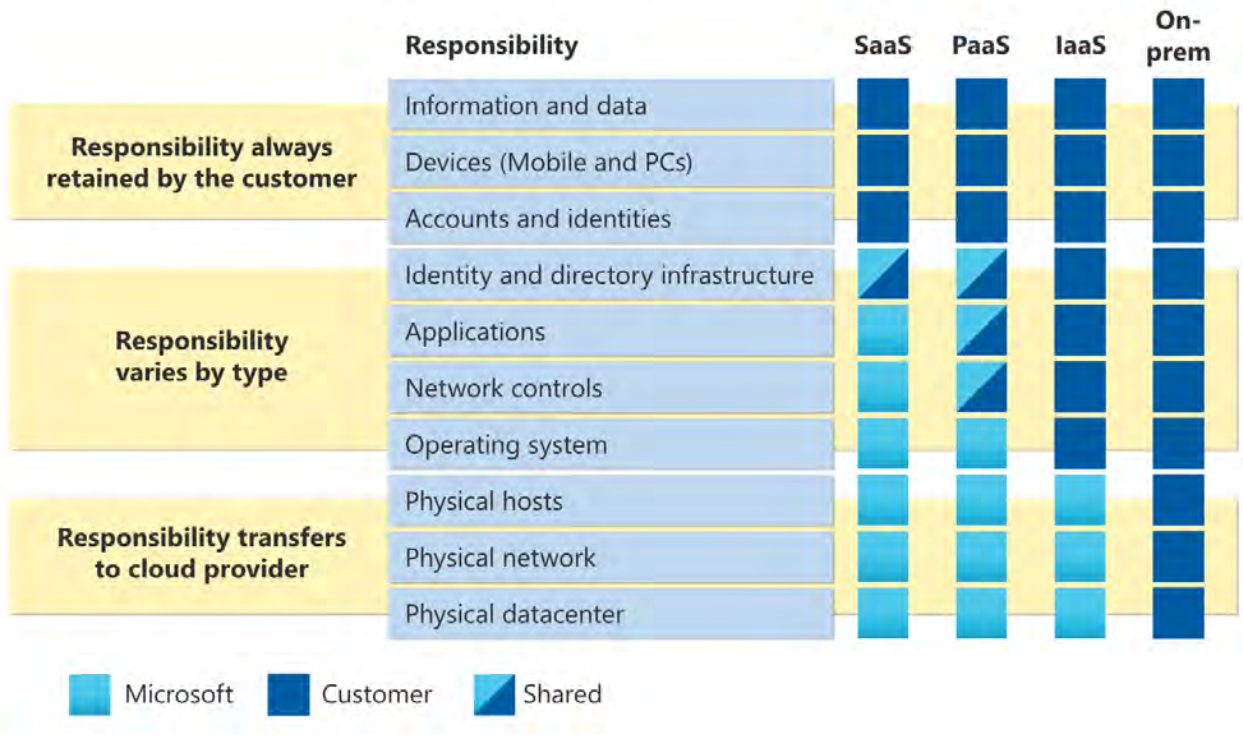
Business Benefits

- **Reduced CapEx** — no expensive hardware
- **Lower ongoing OpEx** with optimized usage
- **Access to enterprise-grade services** (AI, analytics, global networks)
- **Improved performance, security, and reliability**

Shared Responsibility Model

Cloud security is a **shared responsibility** between Microsoft and the customer.

Responsibility Breakdown



Source: *https://learn.microsoft.com/en-us/azure/security/fundamentals/media/shared-responsibility/shared-responsibility.svg*

Identity is always the customer's responsibility — managed through **Microsoft Entra ID** (previously Azure AD).

Cloud Models

Public Cloud — Cloud services provided over the public Internet to anyone who wants to sign up for them. Azure owns the hardware, and you rent it from them.

- Services delivered over the internet
- Hardware owned/managed by Azure
- Most flexible and scalable model

Use cases: start-ups, scalable apps, analytics, global workloads

Private Cloud — Cloud services offered only to select users. This is sometimes called an "internal cloud". Looks and acts like a cloud computing, but uses resources and servers available only to your company/organization. You own the hardware or have exclusive use of it.

- Cloud technologies running in your **own datacenter** or dedicated environment
- Hardware owned or exclusively used by your organization

Use cases: strict compliance, sensitive data, legacy systems

Hybrid Cloud — A mixture between your own private networks and servers, and using the public cloud for some things. Typically used to take advantage of the unlimited, inexpensive growth benefits of the public cloud.

- Combines **on-premises** resources and **Azure**
- Allows gradual migration
- Supports cloud bursting (scale to cloud during high demand)

Use cases: regulated industries, gradual modernization, backup & disaster recovery

Consumption-Based Model

Microsoft (and Google and AWS) can buy and run a server cheaper that you could ever possibly do yourself.

Capital Expenditure (CapEx) — A (usually large) amount of money invested in an asset (building, computers, equipment) spent up front, and it returns profits slowly over time; major cash drain or loan required; cannot be deducted from your taxes in one year, depreciated over several years.

- Large upfront purchase (servers, datacenters); depreciated over years

Operating Expenditure (OpEx) — An amount of money spent "every month" as an operating expense; hopefully you earn more money in revenue from it than you spend; can be deducted from your taxes immediately; many accountants prefer OpEx over CapEx for the tax and cash flow benefits.

- Monthly expense; paid as you consume; tax-deductible immediately

Consumption-Based Model — Paying for something based on how much you used, as opposed to paying for something no matter if you use it or not.

I.e. A monthly gym membership is a fixed-price model, you pay the same every month. But if you only paid when you actually went to the gym (like an entry fee), that would be a consumption model.

Most cloud services charge only when you use the thing, not a fixed-price per month.

Azure uses an **OpEx, consumption-based** model for most services.

Cloud Pricing Models

Free services — Some services are always free or have a free tier or free with a certain limit.

Pay for Time (per second/minute/hour) — Certain services charge by time.

Pay for Storage Capacity (per GB) — In addition to time, you may also have to pay per GB used.

Pay for Operations (per transaction) — Each operation can also cost, a fraction of a penny.

Pay per execution — Some serverless offers just charge you for each time the program runs.

Pay per user — Microsoft Entra ID Premium P1/P2 services charge per assigned user.

Serverless

Serverless Compute — Removes both the need to manage the infrastructure and the need to configure the environment that runs your code.

Serverless Examples: Azure Functions, Azure Container Apps, Azure App Service

Benefits:

- No VM management
- Automatic scaling
- Pay only for execution time

Benefits of using Cloud Services

High Availability and Scalability

Availability — What percentage of time does a system respond properly to requests, expressed as a percentage over time.

- Percentage of uptime for services
- Example: **99.99% availability ≈ 4 minutes acceptable downtime per month**

High Availability — A system specifically designed to be resilient/remain operational even when some component of the system fails.

Scalability — The ability of a system to grow its capacity "easily" when a system reaches its maximum capacity.

- **Vertical scaling** — keeping the same number of resources constant, but giving them more capacity (increase power of a single resource).
- **Horizontal scaling** — increasing or decreasing the number of resource instances.

Reliability and Predictability

Reliability — Consists of two principles: resiliency and availability. To restore the systems and applications after a failure occurs and provide consistent access to the systems and applications.

Disaster Recovery — The ability to recover from a big failure within an acceptable period (Recovery Time Objective (RTO)), with an acceptable amount of data lost (Recovery Point Objective (RPO)).

Predictability — Performance predictability or cost predictability.

Security and Governance

Security — To protect applications and data from threats.

Governance — The policies and procedures of your company that protect your account and your data.

Manageability

Management of the Cloud — Managed by Azure (hardware, network, datacenter)

Elasticity — The ability of a system to automatically grow when maximum capacity is reached and automatically shrink to minimize waste (automatically scale up/down based on load).

Agility — The ability to respond to change “rapidly” based on changes to market or environment.

Management in the Cloud — You can manage cloud your resources via web portal, CLI, APIs, and PowerShell, etc.

Cloud Service Types

Infrastructure-as-a-Service (IaaS) — This is the computing paradigm where Azure provides you the virtual hardware (Virtual machine, load balancer, virtual network), and you can have complete control over that. It replicates the exact function of equipment that you'd have in your own data center (like a server, firewall, router, etc).

IaaS Examples: Virtual machine, load balancer, application gateway, virtual network

Platform-as-a-Service (PaaS) — You lose some control over the hardware; generally, you upload your code and just configure the environment in Azure to run it.

PaaS Examples: App Services, Web Apps, SQL Database

Software-as-a-Service (SaaS) — You lose even more control over the hardware and the software; generally, Azure provides you an application that they developed, and you just configure it to your usage. You are a tenant using their software.

SaaS Examples: Azure Portal, Outlook 365, Windows Virtual Desktop, Azure DevOps

As you move from **IaaS** → **PaaS** → **SaaS**, your responsibility decreases, and Azure's increases.

For Further Reading

- *Azure Official definitions — https://azure.microsoft.com/en-ca/overview/cloud-computing-dictionary/*
- *What is IaaS — https://azure.microsoft.com/en-ca/overview/what-is-iaas/*
- *What is PaaS — https://azure.microsoft.com/en-ca/overview/what-is-paas/*
- *What is SaaS — https://azure.microsoft.com/en-ca/overview/what-is-saas/*
- *What is a Public cloud — https://azure.microsoft.com/en-ca/overview/what-is-a-public-cloud/*

- *What is a Private cloud — https://azure.microsoft.com/en-ca/overview/what-is-a-private-cloud/*
- *What is a Hybrid cloud — https://azure.microsoft.com/en-ca/overview/what-is-hybrid-cloud-computing/*
- *What is a Serverless Computing — https://azure.microsoft.com/en-us/overview/serverless-computing/*

SECTION 3: Azure Architecture and Services (35–40%)

Azure Core Architectural Components

Azure Global Infrastructure

Regions — A set of *physically separate* but interconnected datacenters which are no more than a few miles apart within a specific geographic area.

- You must choose a **region** when creating most Azure services
- Azure has **60+ regions** (largest of any cloud provider)
- Some regions are **restricted** (e.g., government or industry-specific)

Explore Microsoft datacenters: https://datacenters.microsoft.com/globe/explore/

Source: *https://azure.microsoft.com/en-ca/global-infrastructure/geographies/#overview*

Region Pairs — Each region is "paired" with one another within the same geography, which provides the highest-speed, lowest-latency connection between them; Azure treats them as a pair, trying to minimize the chance of them both going down at the same time. Good as a place to store backups and have redundant servers running.

- **High-speed replication**
- **Sequential updates** (Azure ensures only one region in a pair is updated at a time)
- **Isolation of failures** (lower chance both fail simultaneously)
- Recommended for: **disaster recovery** and **cross-region redundancy**

Sovereign Regions — The regions are dedicated to specific sovereign entities (e.g., governments or jurisdictions), and isolated from the rest of Azure regions. For example, Azure Government – US and Azure China. Used for workloads requiring **strict compliance or data residency**.

Availability Zones — Unique physical locations within an Azure region, made up of one or more datacenters.

- Minimum **three zones** per AZ-enabled region
- Each zone has **independent power, cooling, and networking**
- You can **manually place resources** in zones for higher availability

Used for:

- High availability architectures
- Zone-redundant storage/services

Source: *https://learn.microsoft.com/en-us/azure/reliability/media/availability-zones.png*

Azure Datacenter — A group of interconnected buildings in the same location that contain all the servers, storage hardware, power & cooling, networking infrastructure and internet connectivity to run Azure services.

Azure regions contain **multiple datacenters** for resiliency.

Azure Management Infrastructure

Azure Resources — The basic building block of Azure, for example, VM, VNets, database, container, etc.

Resource Groups — A folder structure (logical container) in Azure in which you organize resources like databases, virtual machines, virtual networks, or almost any resource.

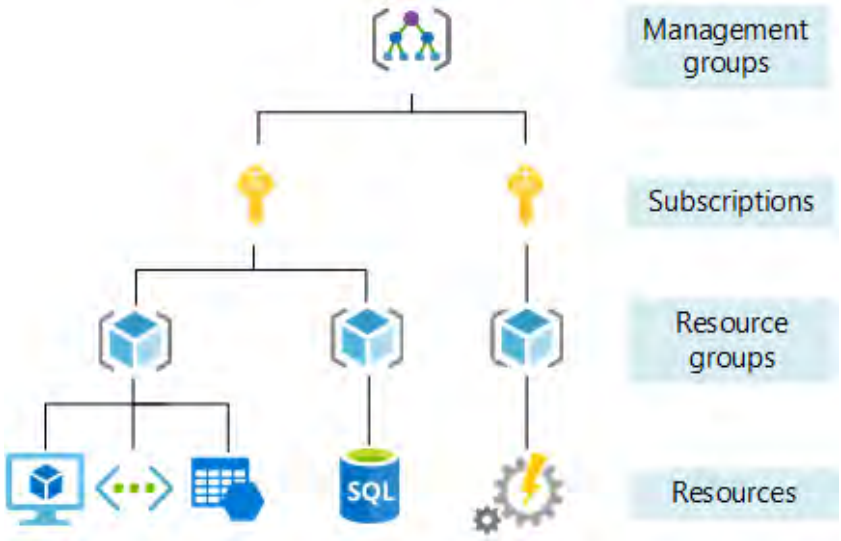
Subscriptions — A billing unit within Azure; all resources under a subscription get billed to a single owner.

Multiple Subscriptions — Possible to create multiple subscriptions to separate out billing. You can create multiple subscriptions for:

- Production vs non-production
- Department-level billing
- Isolation and governance

Management Groups — A hierarchy of subscriptions; can have many subscriptions, and group them, and put those groups into other groups.

Hierarchy of Resource Groups, Subscriptions and Management Groups



Source: *https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/azure-setup-guide/media/organize-resources/scope-levels.png*

Azure Compute and Networking Services

Compute Types

Compute Services — A category of services in Azure that provides **CPU, memory, and runtime environments** for applications.

Virtual Machines — Looks, acts, feels, tastes like a real server in front of you; except it's running inside Azure's data center in a virtualized environment. IaaS offering providing:

- Windows or Linux virtualized OS
- Full control over software and configuration
- Custom vCPU, RAM, storage selection

Hypervisor — A virtualization layer that runs on top of the physical server Operating System that allows multiple guest operating systems (virtual machines) to run in an isolated manner on top. Azure uses a highly optimized hypervisor for isolation and security.

Azure Container Instances (ACI) — The quickest way to create a container on Azure. You can deploy an image to Azure in about a minute. It can be used in production, but is not easily scalable.

Azure Kubernetes Services (AKS) — Kubernetes containers in Azure. Runs on Virtual Machine Scale Sets. Supports auto-scaling, but also requires more overhead to run.

Azure Functions — Small pieces of code that are designed to perform some tasks quickly; these are like connector code designed to do small things; serverless model; Ideal for automation and integrations.

VM Options

Azure Virtual Machines — Azure supports Windows and Linux virtual machines, with dozens of varieties of each; IaaS.

Azure Virtual Machine Scale Sets — A logical group of VMs on Azure that can be configured and managed as a single unit. Able to add more machines as demand grows (autoscaling); able to reduce machines as demand slows; can handle up to 1000 VMs in a single scale set.

Azure Virtual Machine Availability Sets — A logical group that is designed to provide for redundancy and availability to meet the Azure SLA.

Azure Virtual Desktop — Desktop version of Windows that runs in the cloud.

VM Resources

Compute — CPU, RAM

Storage — Hard Disk Drives (HDD), SSD, Managed Disks, etc.

Networking — VNet, Subnet, Public IP Address, Network Interfaces (NIC), etc.

Application Hosting Options

Azure App Services — Allows you to upload your code and configuration into Azure, and Azure will run the application as you specify; lots of integrations with Visual Studio, and other features and benefits provided on this platform; PaaS.

Azure Web Apps — Offers a completely managed platform for creating and hosting web applications with widely-used programming languages including .NET, Java, Node.js, Python, and PHP. Windows or Linux can be chosen as the host operating system.

API Apps — Let you create RESTful web APIs using any language or framework, similar to hosting a website. They include full Swagger/OpenAPI support, can be packaged and published to the Azure Marketplace, and can be accessed by any client that uses HTTP or HTTPS.

Containers — The preferred way to deploy and manage cloud applications, where code is isolated and packaged into running instances of images (snapshots). Many instances of images can be deployed, configured, and replicated with ease, thereby solving the problem of complicated deployments. For instance, code compiled into an image can be deployed identically where ever needed, and with Azure Container Instances management of virtual machines is not needed. Ideal for microservices architectures.

Networking Services

A category of services in Azure that provides network connectivity, performance, and monitoring services for inter-server and Internet communication.

Virtual Network — A representation of a real network; all virtual machines must be connected to a virtual network subnet, and this allows them to talk to each other and to the Internet as long as it follows the rules of the network that you define. A logically isolated network in Azure allowing:

- VM-to-VM communication
- On-prem to Azure connectivity
- Subnet-level control

Virtual Subnets — A subdivision of a virtual network (VNet) that you control, that has its own security rules (Network Security Groups (NSGs)).

Virtual Network Peering — Allows you to connect two or more virtual networks in Azure.

Azure DNS — Hosting domain name resolution service in Azure.

VPN Gateway — A device that allows encrypted private communication between a single computer or a network of servers, and an Azure network; Site-to-site or point-to-site VPN; uses IPSec tunneling.

Azure ExpressRoute — Through a connectivity provider, the ability to extend your Microsoft cloud networks to on-premises networks over a private connection; not routed over the public internet; Higher security, reliability, and throughput.

Public and Private Endpoints

Public Endpoint — Enables data access to your managed instance from the internet/ outside the VNet without using a VPN.

Private Endpoint — A network interface that allow you to securely access your resource in your VNet without exposing resource publicly.

Azure Storage Services

Storage Services

Azure Storage Services — A suite of scalable, durable, and cost-effective cloud storage options for blobs, files, tables, and queues. You pay only for the storage you use (per GB).

Azure Blobs — A highly scalable object storage service for text and binary data, with built-in support for big data analytics using Data Lake Storage Gen2.

Azure Files — Fully managed file shares that can be accessed from both cloud and on-premises environments.

Azure Queues — A reliable messaging service for decoupling and communicating between distributed application components.

Azure Disks — Block-level storage volumes designed for use with Azure virtual machines.

Azure Tables — A NoSQL key-value store for structured, non-relational data.

Managed Disk — Azure-managed block storage for virtual machines that removes the need to manage your own storage accounts; they cost slightly more than unmanaged disks but provide higher reliability, simplified management, and advanced features. Pricing is based on a fixed monthly rate per disk size. An IaaS offering.

Backup and Recovery Storage — As you'd expect, this is a specialized storage account that will manage your backups from virtual machines and perform recoveries.

Database Services — A category of services in Azure that provides fast, structured and unstructured data storage.

Cosmos DB — Extremely low latency (fast) storage designed for smaller pieces of data quickly; PaaS.

Azure SQL Database — Azure-managed database solution that is compatible with SQL Server; DBaaS/PaaS.

Azure SQL Database for MySQL — Managed MySQL database in Azure.

Azure SQL Database for PostgreSQL — Managed PostgreSQL database in Azure

SQL Managed Instance — A scalable cloud database platform as a service utilizing SQL server database engine.

Azure Synapse Analytics (formerly Azure SQL Data Warehouse) — An analytical data warehouse built for large-scale reporting and batch analytics. Not suitable for heavy transactional workloads such as frequent inserts or updates.

Storage Tiers

Storage Tiers — Optimized frequency access tiers for storage indicated as hot, cool, cold or archive.

- **Hot tier** — Best for data that you access frequently, such as website images.
- **Cool tier** — Designed for infrequently accessed data that will be stored for at least 30 days, like customer invoices.
- **Cold tier** — Intended for data that is seldom accessed and kept for a minimum of 90 days.
- **Archive tier** — Ideal for rarely accessed data stored for at least 180 days and where high retrieval latency is acceptable, such as long-term backups.

Redundancy Options

Redundancy in the primary region

Locally redundant storage (LRS) — Data is synchronously replicated three times within a local single data center in the primary region (three copies, one zone).

Zone-redundant storage (ZRS) — Data is synchronously replicated across three AZs in the primary region (three copies, three zones, three DCs, one copy in each zone/DC).

Redundancy in a secondary region

Geo-redundant storage (GRS) — Data is replicated three times using LRS, then it's replicated three times to a single DC in a secondary region (LRS + LRS, six copies, two DCs, two regions three copies in each DC/region).

Geo-zone-redundant storage (GZRS) — Data is replicated using ZRS, then the data is replicated three times in a secondary region using LRS (ZRS + LRS, six copies, three DCs, three AZs, two regions).

Storage Account and Storage Types

Storage Account — Provides access to your Azure storage resources.

Blob Storage — Microsoft's object storage solution for unstructured data in the Azure cloud.

Disk Storage — Block storage used by Azure virtual machines.

File Storage (Azure Files) – A fully managed cloud file share accessible over SMB and NFS, suitable for lift-and-shift workloads and shared file access.

Queue Storage — A messaging store for large volumes of lightweight messages, used for decoupling and asynchronous processing.

Table Storage — A NoSQL key–value store for semi-structured data, offering fast and scalable access to large datasets.

Moving Files Options

AzCopy — A command-line (CLI) utility for high-performance copying and transferring of blobs and files to and from Azure Storage.

Azure Storage Explorer — A graphical tool (web GUI) for managing Azure Storage resources, including blobs, files, queues, and tables.

Azure File Sync — A service that centralizes and synchronizes file shares in Azure while keeping on-premises file servers cached and in sync.

Migration Options

Azure Migrate — A suite of tools for discovering, assessing, and migrating on-premises servers, applications, and data to Azure.

Azure Data Box — A family of hardware appliances for securely transferring large volumes of on-premises data to Azure when network-based transfer is impractical or too slow.

Azure Identity, Access, and Security Services

Azure Directory Services

Authentication — The process of verifying your identity using credentials such as a username and password. Multi-factor authentication (MFA), including SMS codes or authenticator apps, is an additional verification step within this category.

Authorization — Determines what actions or resources a user is allowed to access after their identity has been authenticated.

Microsoft Entra ID — Microsoft's cloud-based Identity-as-a-Service (IDaaS) platform for managing users, groups, applications, and access.

Microsoft Entra Connect — A tool that synchronizes on-premises Active Directory with Microsoft Entra ID, enabling hybrid identity scenarios.

Microsoft Entra Domain Services — A managed domain service in Azure that provides legacy Active Directory capabilities (such as domain join, LDAP, Kerberos, and NTLM) without needing to deploy domain controllers.

Authentication Methods

Single-Sign On — Allows users to access multiple applications using a single set of credentials. Once authenticated, users can open any integrated application without re-entering their username and password. Enabled by Microsoft Entra ID.

Multi-Factor Authentication (MFA) — Adds an extra layer of security beyond a password by requiring something you have (such as a phone call, SMS code, or authenticator app) or something you are (biometrics). This reduces the risk of compromise since passwords can be guessed or stolen.

Passwordless — Removes traditional passwords and replaces them with more secure credentials, combining something you have (a trusted device such as a phone or Windows PC) with something you are or know (biometrics or a PIN).

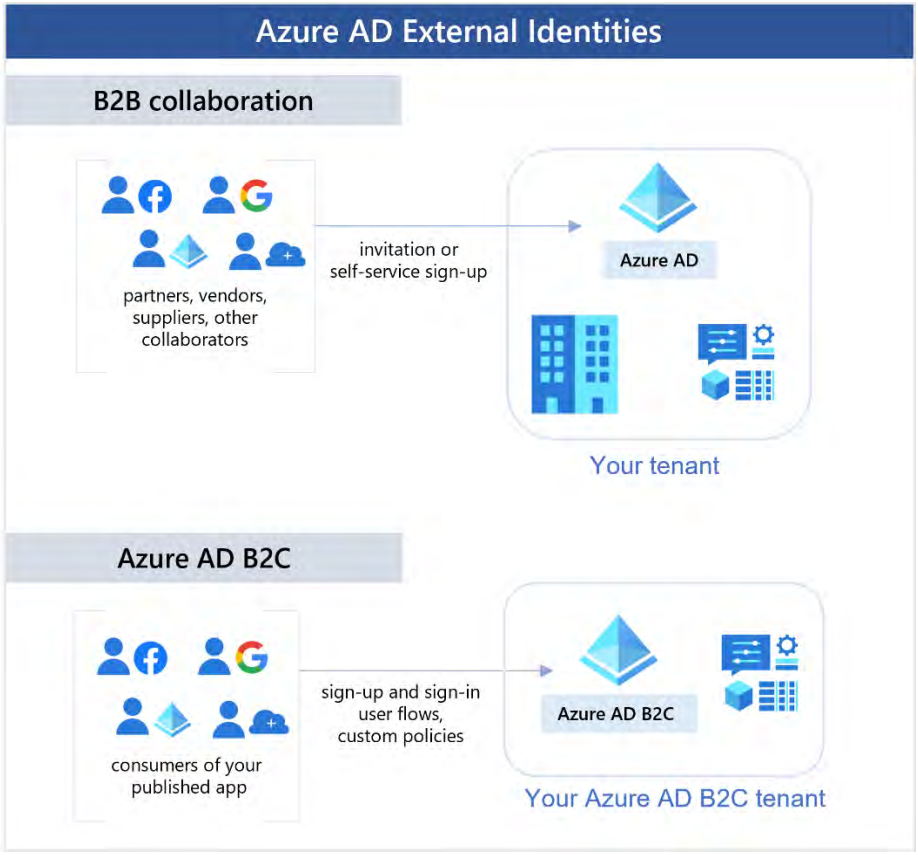
Windows Hello for Business — A passwordless authentication method using biometrics (facial recognition or fingerprint) or a device-specific PIN to securely sign in to Windows and Entra ID–integrated resources.

Microsoft Authenticator App — A mobile app used for MFA and passwordless sign-in, providing push approvals, verification codes, and device-based authentication.

FIDO2 security keys — Physical hardware keys that support passwordless authentication by cryptographically verifying your identity. They require possession of the key and are resistant to phishing attacks.

Azure External Identities

External Identities — external users can "bring their own identities" outside of your organization



Source: *https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-overview*

Business-to-Business (B2B) Collaboration — Enables secure access to your organization's resources for external users (partners, vendors, or guests) using their existing identities, simplifying cross-organization collaboration.

Business-to-Business (B2B) Direct Connect — Establishes a mutual trust relationship between two Microsoft Entra ID (Azure AD) organizations, allowing users to collaborate seamlessly without guest account management.

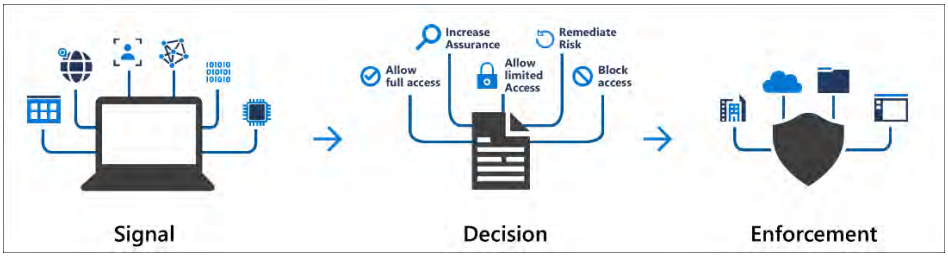
Microsoft Entra External ID (B2C) — A customer identity and access management service that manages external customer identities, providing customizable sign-up and sign-in experiences, and supporting multiple identity providers.

Entra Conditional Access

Conditional Access — A policy-based access control engine in Microsoft Entra ID that enforces Zero Trust by evaluating multiple signals (such as user, device, location, and risk) to determine whether access should be granted, blocked, or require additional controls.

In practice, it allows you to:

- Require **MFA** based on role, location, or network
- Restrict access to **approved client applications** only
- Allow access only from **managed and compliant devices**
- **Block access** from untrusted or high-risk locations



Source: *https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/media/overview/conditional-access-signal-decision-enforcement.png*

Azure role-based access control (RBAC)

Role Based Access Control (RBAC) — A system for managing access by assigning permissions to roles, which are then granted to users, groups, or applications, instead of assigning permissions individually.

RBAC scopes include:

- Management groups — collections of multiple subscriptions
- Subscriptions — a single Azure subscription
- Resource groups — containers for related resources
- Resources — individual Azure resources

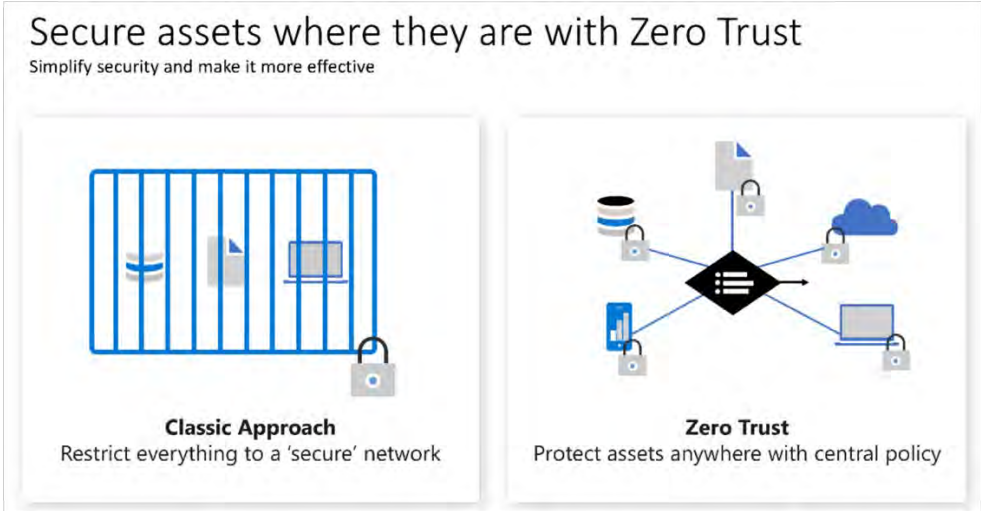
Tips:

- ***Authentication*** *= who you are*
- ***Authorization*** *= what you're allowed to do*
- ***RBAC*** *= what you can do (based on your role)*
- ***Conditional Access*** *= under what conditions you can do it*

Security Concepts

Zero Trust — A security model based on the principle "never trust, always verify ," where every access request is continuously validated using identity, device, location, and other signals before authorization is granted.

- **Verify explicitly** — Always authenticate and authorize using all available signals.
- **Use least privilege access** — Grant only the minimum access required, using JIT/JEA and risk-based policies.
- **Assume breach** — Limit blast radius through segmentation, encryption, monitoring, and threat detection.



Source: *https://learn.microsoft.com/en-us/azure/security/fundamentals/media/zero-trust/zero-trust-shift.png*

Defense-in-Depth Model — A security approach that uses multiple, layered controls so that if one layer is compromised, others still protect the system.

Security layers in cloud computing (outer → inner):

- **Physical** — Datacenter security such as locks, key cards, and biometric access
- **Identity & Access** — Identity verification and access control using Microsoft Entra ID, MFA, and RBAC
- **Perimeter** — Protection against large-scale attacks using firewalls and DDoS protection
- **Network** — Network segmentation and traffic control using virtual networks, subnets, and network security groups (NSGs)
- **Compute** — Securing virtual machines and workloads by limiting RDP/SSH access, applying OS updates, and using endpoint protection
- **Application** — Application-level protections such as API Management, secure authentication, and input validation
- **Data** — Protecting data through encryption, access restrictions, and endpoint controls (for example, limiting SQL permissions)

Microsoft Defender for Cloud

MS Defender for Cloud — A native Azure security management service that helps you protect cloud workloads by continuously assessing your security posture, strengthening resource configurations, and detecting, investigating, and responding to threats. It combines **Cloud Security Posture Management (CSPM)** and **Cloud Workload Protection (CWP)** to improve security across Azure, hybrid, and multi-cloud environments.

For Further Reading

- *Azure Global Infrastructure - https://azure.microsoft.com/en-ca/explore/global-infrastructure/*

SECTION 4: Azure Management and Governance (30–35%)

Cost Management in Azure

Factors Affecting the Cost

Azure shifts IT spending from the **capital expense (CapEx)** of purchasing and maintaining infrastructure to an **operational expense (OpEx)** model, where you pay only for the cloud resources you use—such as compute, storage, and networking.

Factors that affect your Azure bill include:

- **Resource type** — Different services are priced using different metrics, such as per GB stored, per execution, or per instance.
- **Consumption** — Some services are charged based on usage (for example, data stored or number of executions), while others are charged based on time (per minute or per hour, whether fully used or not).
- **Maintenance** — Using higher-level services (such as web apps or Azure Functions) can reduce operational overhead and help lower costs compared to managing infrastructure yourself.
- **Geography** — Pricing can vary by region, and data egress to the internet or between regions may incur additional charges.
- **Subscription type** — Dev/test subscriptions and special licensing offers can significantly reduce costs for non-production workloads.
- **Azure Marketplace** — Some third-party solutions have separate licensing or usage costs in addition to Azure infrastructure charges.

Pricing Calculator

Pricing Calculator — An online tool used to estimate the cost of Azure services based on selected resources, configurations, and expected usage.

Online tool: https://azure.microsoft.com/en-ca/pricing/calculator/

Tip: Spend 20 minutes playing around with this before taking the exam to understand how different services are priced.

Total Cost of Ownership (TCO) — The complete cost of running workloads, including hardware, software, human labor for installation and maintenance, electricity, cooling, backups, physical space, internet connectivity, etc.

Azure Cost Management Capabilities

Azure Cost Management — A service for monitoring, analyzing, and optimizing historical and current Azure spending across subscriptions.

Billing — Tools used to manage billing accounts, invoices, payments, and subscriptions.

Best Practices for Reducing Costs in Azure:

- Use **Azure Advisor** (Cost tab) for cost-optimization recommendations
- Configure **Budgets** to define expected spending limits
- Set up **Cost Alerts** to notify you when spending approaches or exceeds budget thresholds
- Enable **auto shutdown** for Dev/Test/QA and non-production resources
- Utilize **storage lifecycle management** - hot, cool, cold, archive tiers
- Utilize **reserved instances** (1 or 3 years) for predictable, long-running workloads
- Configure alerts when billing exceeds an expected level
- Implement **automatic scaling** to match capacity with demand
- **Downsize resources** such as reducing over-provisioned VMs or managed disks
- Use **Azure Policy** to prevent excessive spending like restricting VM SKUs
- Apply **tags** to resources to track costs by owner, project, or department in Azure

Tags

Purpose of Tags — Tags are name–value metadata used to organize resources and improve cost tracking, management, and support.

Tags can be used to:

- Group **related resources** (for example, by project, environment, or department)
- Track and allocate **costs** across teams or applications
- Identify **owners** or support contacts for resources
- Assist with **automation** and **governance**
- Improve **reporting** in Azure Cost Management

Azure Governance and Compliance

Microsoft Purview in Azure

Azure Purview — A unified data governance and compliance solution that helps organizations discover, classify, govern, and protect data across Azure, on-premises, and multi-cloud environments.

Key capabilities:

- Data discovery and classification
- Data catalog and lineage
- Sensitivity labeling integration
- Compliance and risk management across the data estate

Azure Policy

Azure Policy — A governance service that helps enforce organizational standards and assess compliance at scale across Azure resources. Policies can either block non-compliant actions or allow them while reporting compliance status.

Policy behavior:

- **Deny** — Prevents non-compliant resources from being created
- **Audit** — Reports non-compliance without blocking
- **Append / Modify** — Automatically adds or changes resource settings

Built-In Policies Examples:

- Require SQL Server 16.0 or higher
- Restrict allowed Storage Account SKUs
- Limit Regions where resources can be created
- Restrict Virtual Machine SKUs
- Require resources have tags
- Enforce encryption or security setttings

Custom Policies — You can create your own policies if the built-in ones don't meet your organization's governance or compliance requirements.

Resource Locks

Resource Locks — A protection mechanism that prevents accidental modification or deletion of critical Azure resources. Locks must be removed before changes can be made.

Lock types:

- **Read-only** — Allows viewing but blocks modifications
- **Delete** — Prevents deletion but allows changes

Locks Access Control — Resource Locks are managed using **RBAC**, so only authorized users can create, modify, or remove.

Azure Resources Managing and Deploying Tools

Azure Portal

Azure Portal — A web-based management interface (https://portal.azure.com) used to create, configure, and manage your Azure subscriptions and resources through a friendly graphical user interface.

Azure Mobile App — A native mobile application of the Azure portal.

Azure Cloud Shell

Azure Cloud Shell — A browser-based shell in the Azure Portal that provides access to Azure CLI and PowerShell consoles without local installation.

Azure PowerShell — A command-line and scripting tool based on PowerShell for managing Azure resources.

Azure Command Line Interface (CLI) — A cross-platform command line tool that allows you to manage your Azure subscription and resources using scripts or commands.

Azure Arc

Azure Arc — A hybrid and multi-cloud management tool that lets you manage non-Azure servers, Kubernetes clusters, and databases as if they were running in Azure.

Infrastructure as Code (IaC)

Infrastructure as Code (IaC) — A practice that uses code and version control to define, deploy, and manage infrastructure consistently and repeatedly, supporting DevOps and automation.

Most popular tools for implementing IaC with Azure:

- ARM templates

- Terraform

ARM and ARM Templates

Azure Resource Manager (ARM) — Azure's deployment and management service that handles all resource creation, updates, and deletions, regardless of whether you use the portal, CLI, PowerShell, or SDKs.

Azure Resource Manager Templates (ARM Templates) — An Infrastructure as Code approach that uses JSON files to declaratively define Azure resources and their configurations.

Azure Monitoring Tools

Azure Advisor

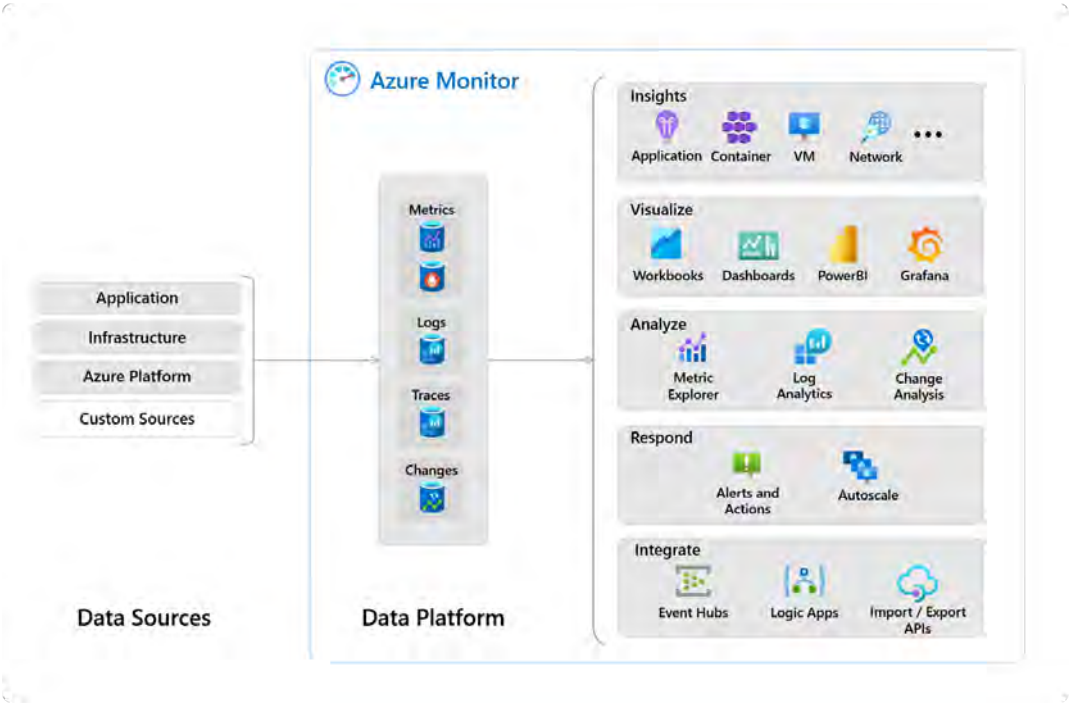
Azure Advisor — A recommendation service that analyzes your Azure usage and provides personalized best-practice guidance across cost, security, reliability (availability), performance, and operational excellence.

Azure Service Health

Azure Service Health — A customizable dashboard that shows the status of Azure services and regions you use, including service issues, planned maintenance, and health advisories.

Azure Monitor

Azure Monitor — A centralized monitoring platform that collects and analyzes metrics, logs, and events from Azure resources and applications.



Source: *https://learn.microsoft.com/en-us/azure/azure-monitor/media/overview/azure-monitor-overview-2022_10_15-add-prometheus-opt.svg*

Log Analytics — A feature of Azure Monitor used to query and analyze log data using KQL (Kusto Query Language).

Azure Monitor Alerts — Alerting rules based on metrics or logs that provide near-real-time notifications when thresholds or conditions are met.

Application Insights — An application performance monitoring (APM) service that tracks the availability, performance, and failures of web applications and APIs.

Service Level Agreements (SLA) — Formal uptime commitments that define the expected availability of Azure services.

Service credits — If Microsoft fails to meet an SLA, customers may receive a service credit (such as 10%, 25%, or more) applied to their bill, depending on the service and level of outage.

For Further Reading

- *Understanding the Total Cost of Ownership — https://techcommunity.microsoft.com/blog/finopsblog/understanding-the-total-cost-of-ownership/4419195/*
- *Azure Portal — https://learn.microsoft.com/en-us/azure/azure-portal/azure-portal-overview*
- *Azure Cloud Shell — https://learn.microsoft.com/en-us/azure/cloud-shell/overview*
- *Azure PowerShell — https://learn.microsoft.com/en-us/powershell/azure/what-is-azure-powershell?view=azps-15.1.0*
- *Azure CLI — https://learn.microsoft.com/en-us/cli/azure/install-azure-cli*
- *Azure Service Level Agreements — https://azure.microsoft.com/en-us/support/legal/sla/*

SECTION 5: Other Azure Services

Azure Security Services

Security

Microsoft Defender for Cloud (formerly Azure Security Center) — A unified cloud security management service that provides security posture management and advanced threat protection for Azure, hybrid, and multi-cloud workloads.

Azure Key Vault — Azure's security service for storing and managing secrets, keys, and certificates.

Microsoft Sentinel (formerly Azure Sentinel) — A cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution used to collect, detect, investigate, and respond to security threats.

Azure Dedicated Hosts — A service that provides dedicated physical servers to host your Azure virtual machines, ensuring isolation from other customers for compliance or licensing requirements.

Azure Firewall — A fully managed, stateful network firewall service that controls inbound and outbound traffic to and from Azure virtual networks.

Distributed Denial of Service attacks (DDoS) Attack — An attack that floods a network or service with massive amounts of traffic from the internet, attempting to disrupt legitimate access.

Azure DDoS Protection — Provides defense against DDoS attacks:

- Basic protection is enabled by default at no extra cost.
- Standard protection (paid) adds enhanced mitigation, logging, alerting, and attack analytics.

Network Security Group (NSG) — A set of inbound and outbound security rules that control network traffic to and from Azure resources based on source, destination, protocol, and port.

Application Security Group (ASG) — An Azure networking feature that logically groups virtual machines by application or role**,** making it easier to manage network security rules. All front-end VMs can be in one ASG, while the mid-tier is in another. And then, you can refer to them in the NSG rule by their ASG name.

User Defined Routes (UDR) — Custom routing rules that control how network traffic flows within Azure virtual networks, often used with Firewall devices or ExpressRoute.

Best practices for security:

- Use **NSGs** on all virtual networks to control traffic flow
- Treat NSGs as **basic protection**, similar to locking the doors of a house
- Enable **Azure DDoS Protection Standard** if workloads are likely to be targeted
- Use **Application Gateway with WAF** for production web applications
- Apply **Defense-in-Depth** — use multiple security layers so if one control is breached, others remain in place

Privacy and Compliance

Compliance — The process of meeting regulatory, legal, or industry standards related to data protection, privacy, and security.

General Data Protection Regulation (GDPR) — A European Union regulation governing how organizations collect, process, store, protect, and report personal data of EU citizens.

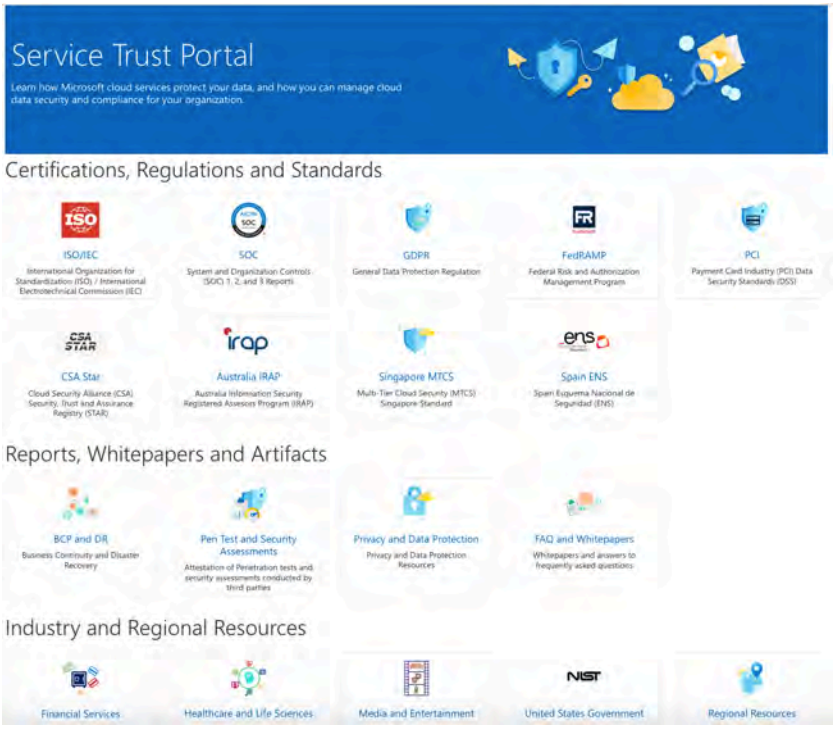
ISO Standards — Azure complies with multiple international ISO security and privacy standards, such as ISO/IEC 27001.

NIST Cybersecurity Framework (CSF) — A security framework that defines best practices for managing and reducing cybersecurity risk, often validated through audits or assessments.

Microsoft Privacy Statement — Explains how Microsoft collects, uses, and protects personal data. https://www.microsoft.com/en-ca/privacy

Microsoft Trust Center — A central portal providing information on Microsoft security, privacy, compliance, and transparency practices. https://www.microsoft.com/en-au/trust-center/product-overview

Service Trust Portal (STP) — A portal that provides access to Microsoft security, privacy, and compliance documentation, including certifications, audit reports, whitepapers, and regional compliance resources. https://servicetrust.microsoft.com/



Compliance Manager — A tool in Microsoft Purview that helps organizations assess, track, and manage their regulatory compliance posture using built-in assessments and improvement actions.

Azure Government — A separate, isolated Azure cloud designed for U.S. government agencies and partners, accessed via a different portal and service endpoints.

Department of Defense (DoD) Cloud — A highly restricted Azure environment for U.S. military workloads, isolated from both public Azure and Azure Government.

Private / Sovereign Clouds — Use different service endpoints and URLs than public Azure to meet regulatory and compliance requirements.

Other Azure Solutions

Governance, Marketplace & Updates

Azure Blueprints — A service used to define and deploy standardized subscription templates, including policies, role assignments, and resource configurations, so new subscriptions are compliant from day one.

Azure Marketplace — An online catalog where Microsoft and third-party vendors offer Azure-compatible solutions, such as virtual appliances, SaaS apps, and managed services.

Azure Updates — A public site that tracks new features, service updates, and announcements across Azure. https://azure.microsoft.com/en-us/updates/

Internet of Things (IoT)

Internet of Things (IoT) — A network of physical devices that collect data and send it to the cloud for processing and analysis.

IoT Central — A fully managed IoT application platform that simplifies building, deploying, and managing enterprise IoT solutions.

IoT Hub — A managed cloud service that enables secure, bi-directional communication between IoT devices and cloud applications.

Azure Sphere — A secure, end-to-end IoT solution that includes a certified microcontroller unit (MCU), operating system, and cloud security service for highly secure devices.

Analytics & Big Data

Azure Synapse Analytics — An analytics service that combines enterprise data warehousing and big data analytics for large-scale data processing and reporting.

HDInsight — A managed cloud service that provides popular open-source analytics frameworks such as Apache Hadoop, Spark, and Hive.

Azure Databricks — A collaborative analytics platform based on Apache Spark, used by data engineers, data scientists, and analysts to process and analyze big data.

Artificial Intelligence (AI)

Artificial Intelligence (AI) — Azure services and APIs that enable applications to analyze text, images, video, speech, and language, supporting scenarios such as chatbots, translation, transcription, and intelligent decision-making.

DevOps & Development Tools

Azure DevOps — A set of services that supports the full software development lifecycle, including project planning (Boards), source control, and CI/CD pipelines.

GitHub — A cloud-based platform for hosting source code using Git, supporting collaboration, version control, and code management.

GitHub Actions — A workflow automation service within GitHub used to build, test, and deploy applications.

Azure DevTest Labs — A service that helps development teams quickly create, manage, and control VMs and PaaS resources while minimizing cost and administrative overhead.

For Further Reading

- *Trusted Cloud: security, privacy, compliance, resiliency, and IP — https://azure.microsoft.com/en-us/blog/trusted-cloud-security-privacy-compliance-resiliency-and-ip/*

SECTION 6: Is That the End?

Thanks!

Thank you for signing up for this course, and for following along with this study guide.

If you have not left a review for the course, I would LOVE it if you could leave your feedback publicly for future students to read. Reviews help the course get found.

If you have any questions, leave them in the Q&A section of the course.

Don't forget that the Azure User Facebook Group is available for anyone to join to discuss more about Azure. Be the first to know when significant changes happen in the exams or in Azure itself. https://www.facebook.com/groups/azureusergroupunofficial/

AZ-900: AZURE FUNDAMENTALS

COURSE ON UDEMY, Study Guide v3.0

INSTRUCTOR: SCOTT DUFFY

WITH SEAN XIE

www.udemy.com/az900-azure