Introduction to AZ-900 and Azure

The Microsoft Azure Fundamentals (AZ-900) exam is designed to validate your foundational knowledge of cloud services and how those services are provided with Microsoft Azure. It's not a technical, hands-on exam but rather a conceptual one, ensuring you understand cloud principles, Azure's architecture, services, pricing, and governance.

---

1. Cloud Concepts

1.1 Cloud Computing Overview

What is Cloud Computing? Cloud computing is the delivery of computing services—including servers, storage, databases, networking, software, analytics, and intelligence—over the Internet ("the cloud") to offer faster innovation, flexible resources, and economies of scale.

Instead of owning their own computing infrastructure or data centers, companies can rent access to anything from applications to storage from a cloud service provider. This eliminates the capital expense of buying hardware and software and the operational expense of running on-site datacenters.

Key Characteristics (The 5-4-3 of Cloud): * Five Essential Characteristics (as defined by NIST): 1. On-demand self-service: You can provision resources (like a VM or storage account) automatically without requiring human interaction from the service provider. 2. Broad network access: Services are available over the network and accessed through standard mechanisms (e.g., internet) by diverse client platforms (e.g., mobile, laptop). 3. Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. 4. Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. 5. Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth). You pay for what you use.

- Four Deployment Models:
    1. Public Cloud: Owned and operated by a third-party cloud service provider. All hardware, software, and supporting infrastructure is owned and managed by the provider. (e.g., Microsoft Azure, Amazon AWS, Google GCP).
    2. Private Cloud: Used exclusively by a single business or organization. It can be physically located at your on-site datacenter or hosted by a third-party provider. It offers more control and security.

3. Hybrid Cloud: Combines public and private clouds, bound together by technology that allows data and applications to be shared between them. This gives your business greater flexibility, more deployment options, and helps optimize existing infrastructure, security, and compliance.
4. Community Cloud: A collaborative effort where infrastructure is shared between several organizations from a specific community with common concerns (e.g., security, compliance, jurisdiction). It may be managed internally or by a third party.

- Three Service Models:
  1. Infrastructure as a Service (IaaS): The most basic category. You rent IT infrastructure—servers, VMs, storage, networks, operating systems—from a cloud provider on a pay-as-you-go basis. You manage the OS, storage, and deployed applications. The provider manages the physical hardware, networking, and virtualization. Example: Azure Virtual Machines.
  2. Platform as a Service (PaaS): Provides an on-demand environment for developing, testing, delivering, and managing software applications. It is designed to make it easier for developers to quickly create web or mobile apps without worrying about setting up or managing the underlying infrastructure. You manage your applications and data. The provider manages the OS, runtime, middleware, and infrastructure. Example: Azure App Service.
  3. Software as a Service (SaaS): Delivers software applications over the internet, on a subscription basis. The cloud provider hosts and manages the software application and underlying infrastructure, and handles any maintenance. Users connect to the application over the Internet, typically via a web browser. You manage nothing (except your data and user configuration). The provider manages everything else. Example: Microsoft 365.

1.2 Shared Responsibility Model

This is a critical security and compliance concept that divides responsibilities between the cloud provider and the cloud customer.

	IaaS	PaaS	SaaS
You Manage	Applications, Data, Runtime, OS, Middleware	Applications, Data	Data, Identity, and Access only

	IaaS	PaaS	SaaS
Provider Manages	Virtualization, Servers, Storage, Networking	Runtime, OS, Middleware, Virtualization, Servers, Storage, Networking	Applications, Runtime, OS, Middleware, Virtualization, Servers, Storage, Networking
Analogy	Renting a plot of land. You are responsible for the house, furniture, and utilities. The landlord is responsible for the land and perimeter security.	Renting a fully furnished apartment. You are responsible for your belongings and how you live in it. The landlord is responsible for the building, appliances, and maintenance.	Staying in a hotel. You are only responsible for your personal belongings and how you use the room. The hotel manages the building, room, cleaning, and all facilities.

Key Takeaway: As you move from IaaS to SaaS, your administrative overhead decreases, but so does your granular control over the IT stack.

---

2. Core Azure Architecture & Services

2.1 Geographic Infrastructure

- Region: A set of datacenters deployed within a latency-defined perimeter and connected through a dedicated regional low-latency network. (e.g., West US, North Europe, Southeast Asia). You deploy resources to a specific region to meet compliance, data residency, or latency requirements.
- Region Pair: Most Azure regions are paired with another region within the same geography (e.g., West US is paired with East US). This provides for disaster recovery and protects your data through replication.
- Availability Zone: One or more physically separate datacenters within an Azure region, each with independent power, cooling, and networking. They are connected by high-speed, private fiber-optic networks. Used for high availability and to protect against datacenter failure.
- Availability Set: A logical grouping of VMs within a datacenter that allows Azure to understand how your application is built to provide for redundancy and availability. It distributes VMs across Fault Domains (different racks of servers) and Update Domains (groups of VMs that can be rebooted at the same time).

2.2 Core Azure Services & Resources

- Resource: The basic building block of Azure. A manageable item (e.g., VM, storage account, SQL database, virtual network).
- Resource Group: A container that holds related resources for an Azure solution. It acts as a logical boundary to manage and aggregate resources for billing, monitoring, and access control. A resource can only exist in one resource group.
- Subscription: A logical container for your resources and resource groups. It is linked to an Azure account and is the unit of billing and management. You can have multiple subscriptions under a single account for different projects/departments.

2.3 Core Service Categories (Table)

Here is a categorized table of key Azure services for the AZ-900 exam.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
Compute	Azure Virtual Machines (VMs)	IaaS	On-demand, scalable computing resources. Full control over the OS.
	Azure App Service	PaaS	Fully managed platform for building, deploying, and scaling web apps, APIs, and mobile backends.
	Azure Container Instances (ACI)	PaaS	The simplest way to run a container in Azure without managing servers.
	Azure Kubernetes Service (AKS)	PaaS	Managed Kubernetes service for deploying and managing containerized applications.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
	Azure Functions	PaaS	Serverless compute service to run event-triggered code without provisioning infrastructure.
Storage	Azure Blob Storage	PaaS	Massively scalable object storage for unstructured data (text, binary, images, videos).
	Azure Files	PaaS	Managed file shares accessible via the SMB protocol (like a network drive).
	Azure Disk Storage	IaaS/PaaS	Persistent, high-performance block storage for Azure VMs.
	Azure Data Lake Storage	PaaS	Optimized storage for big data analytics workloads.
Networking	Azure Virtual Network (VNet)	IaaS	The fundamental building block for your private network in Azure.
	VPN Gateway	IaaS	Connect your on-premises network to Azure securely over the public internet.
	Azure ExpressRoute	IaaS	Establish private, high-speed connections from your on-premises infrastructure to Azure.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
	Azure Load Balancer	IaaS	Distributes incoming network traffic across backend resources (at Layer 4).
	Azure Application Gateway	IaaS	A web traffic load balancer that can make routing decisions based on additional attributes of an HTTP request (Layer 7).
Databases	Azure SQL Database	PaaS	Fully managed, intelligent relational database based on the SQL Server engine.
	Azure Cosmos DB	PaaS	Globally distributed, multi-model database for low-latency, scalable applications.
	Azure Database for MySQL/PostgreSQL	PaaS	Fully managed database services for open-source database engines.
Identity & Access (IAM)	Azure Active Directory (Azure AD)	PaaS/SaaS	Microsoft's cloud-based identity and access management service.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
	Azure AD B2C	PaaS	A customer identity access management (CIAM) solution for web and mobile apps.
Security	Azure Key Vault	PaaS	Securely store and manage secrets, keys, and certificates.
	Azure Security Center / Microsoft Defender for Cloud	PaaS/SaaS	A unified security management system that strengthens your security posture.
	Azure DDoS Protection	PaaS	Protects your Azure resources from Distributed Denial of Service (DDoS) attacks.
	Azure Firewall	PaaS	A managed, cloud-native network security service to protect your Azure VNet resources.
	Network Security Groups (NSGs)	IaaS	A basic firewall that controls traffic to/from Azure resources by allowing/denying network traffic.
AI & ML	Azure Machine Learning	PaaS	A cloud-based environment for training, deploying, and managing machine learning models.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
	Azure Cognitive Services	PaaS/SaaS	APIs for adding AI capabilities (vision, speech, language, decision) to your applications.
	Azure Bot Service	PaaS	A platform for creating intelligent, enterprise-grade bots.
Monitoring	Azure Monitor	PaaS/SaaS	A comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments.
	Azure Log Analytics	PaaS	A tool in the Azure portal to edit and run log queries on data collected by Azure Monitor.
Management	Azure Resource Manager (ARM)	Platform	The deployment and management service for Azure. You use its API/tools to manage resources.
	Azure Portal	Tool	A web-based, unified console for managing Azure services.
	Azure PowerShell / Azure CLI	Tool	Command-line tools for managing Azure resources.

Category	Azure Service	Type (IaaS, PaaS, SaaS)	Primary Usage
	Azure Cloud Shell	Tool	An interactive, browser-accessible shell for managing Azure resources.

3. Azure Management & Governance

3.1 Management Tools

- Azure Portal: The web-based GUI for managing all Azure services.
- Azure PowerShell & Azure CLI: Scripting and command-line tools for automation and bulk operations. PowerShell is task-based and runs on Windows, Linux, and macOS. The CLI is cross-platform and command-based.
- Azure Cloud Shell: A browser-based shell that provides both PowerShell and CLI interfaces, with storage persistence for your scripts. It's accessible directly from the portal.
- Azure Mobile App: Allows you to monitor your resources, check alerts, and run commands from your mobile device.

3.2 Governance & Compliance Tools

- Azure Resource Manager (ARM) Templates: JavaScript Object Notation (JSON) files that define the infrastructure and configuration for your project. They are declarative, meaning you define what you want to deploy, and ARM handles the how. This enables repeatable, consistent deployments known as Infrastructure as Code (IaC).
- Azure Policy: A service to create, assign, and manage policies that enforce rules and effects over your resources. This ensures compliance with corporate standards and service-level agreements. Example: "Allowed locations" to ensure resources are only created in specific regions.
- Azure Blueprints: A way to orchestrate the deployment of various resource templates and other artifacts (like policies, role assignments, and ARM templates) in a single, repeatable package. It's used for large-scale, governed environment setups (e.g., for a new department or application).
- Role-Based Access Control (RBAC): A system for managing access to Azure resources. You grant access by assigning roles (a collection of permissions) to users, groups, or service principals at a specific scope (Management Group, Subscription, Resource Group, or Resource). Example: "Reader" role, "Contributor" role, "Owner" role.

- Resource Tags: Key-value pairs that you can apply to resources and resource groups. They are metadata that help you logically organize your resources for:
  - Cost Management: Group and report on costs by department, project, or environment.
  - Operations: Quickly find and manage all resources for a specific application.
  - Security: Classify data sensitivity (e.g., "Confidential", "Public").
  - Governance & Compliance: Identify the owner of a resource.

---

4. Security, Compliance & Monitoring

4.1 Security Services

- Microsoft Defender for Cloud (formerly Azure Security Center): A unified infrastructure security management system that strengthens the security posture of your data centers and provides advanced threat protection across your hybrid workloads.
  - Secure Score: A measure of your security posture (higher is better).
  - Security Policy: Definitions of the controls recommended for your subscription.
  - Threat Protection: Detects and alerts you to potential threats.
- Azure Key Vault: Securely stores and tightly controls access to secrets like passwords, certificates, and encryption keys. It helps you manage the lifecycle of your security artifacts.
- Azure Firewall: A managed, cloud-native network security service that protects your Azure Virtual Network resources. It is a stateful firewall-as-a-service.
- Network Security Groups (NSGs): A basic layer of security that acts as a virtual firewall. It contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks.

4.2 Monitoring Services

- Azure Monitor: A comprehensive platform for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It maximizes the availability and performance of your applications.
  - Platform Metrics: Numerical values that describe aspects of a resource at a particular time (e.g., CPU percentage, disk reads).
  - Activity Log: A log of subscription-level events (e.g., creating a VM, deleting a resource group).
  - Azure Monitor Logs: Log data from various sources (e.g., VMs, containers, applications) stored in a Log Analytics workspace. You use the Kusto Query Language (KQL) to analyze this data.

  - Alerts: Proactively notify you when important conditions are found in your monitoring data.
  - Application Insights: A feature of Azure Monitor for monitoring live web applications, detecting performance anomalies, and diagnosing issues.

4.3 Compliance

- Microsoft Privacy Statement: Explains what personal data Microsoft processes, how it's processed, and for what purposes.
- Microsoft Trust Center: A website resource containing detailed information about Microsoft's security, compliance, and privacy practices.
- Service Trust Portal: Provides access to various compliance reports, audit reports, and compliance guides (requires login with your Azure account).
- Azure Compliance Manager: A workflow-based risk assessment dashboard within the Service Trust Portal that helps you track, assign, and verify your organization's compliance activities for regulations and standards.

---

5. Pricing, SLA & Support

5.1 Azure Pricing Models

- Pay-As-You-Go (Consumption-Based): Pay only for the individual services and resources you use, for as long as you use them. No upfront costs.
- Reserved Instances: A discount program for committing to a 1-year or 3-year term for Virtual Machines and certain other services. Can save up to 72% compared to pay-as-you-go prices.
- Spot Instances / Spot Virtual Machines: Purchase unused Azure capacity at a significant discount (up to 90%). Ideal for interruptible workloads like batch processing, dev/test environments, or large compute workloads.
- Azure Hybrid Benefit: A licensing benefit that helps you save money. It allows you to use your on-premises Windows Server and SQL Server licenses with Software Assurance on Azure.

5.2 Planning & Managing Costs

- Pricing Calculator: A tool to estimate the cost of Azure services before deploying them.
- Total Cost of Ownership (TCO) Calculator: A tool to estimate the cost savings you can achieve by migrating your on-premises workloads to Azure. You input your current infrastructure, and it generates a detailed report comparing on-premises costs to Azure costs.

- Azure Cost Management + Billing: A native service (powered by Cloudyn) that helps you monitor, allocate, and optimize your Azure spending. You can set budgets, create cost alerts, and analyze cost trends.

5.3 Service Level Agreement (SLA)

- Definition: A formal promise from Microsoft regarding the performance and uptime of an Azure service.
- Uptime Percentage: Expressed as a percentage of time the service will be available. For example:
  - 99.9% = "three nines" = ~8.76 hours of downtime per year.
  - 99.95% = ~4.38 hours of downtime per year.
  - 99.99% = "four nines" = ~52.6 minutes of downtime per year.
- Service Credits: If a service fails to meet its SLA, you can request service credits, which are a percentage discount on your monthly bill. An SLA is a financial guarantee, not a technical one.
- Composite SLA: For an application that depends on multiple services, the composite SLA is the product of the individual SLAs.
  - Example: A web app using App Service (99.95%) and SQL Database (99.99%) has a composite SLA of 0.9995 0.9999 = 0.9994, or 99.94%.*
- Improving SLA: You can improve the SLA of a single service by designing for high availability, such as deploying VMs across Availability Zones (which offers a 99.99% SLA) instead of in a single region.

5.4 Service Lifecycle

- Private & Public Previews: Services are released in stages. Preview features are offered for testing and feedback and are not covered by SLAs and should not be used for production workloads.
- General Availability (GA): The service is fully supported, covered by an SLA, and ready for production use.

5.5 Azure Support Plans

Support Plan	Use Case	Best For	Key Features
Free	Everyone	Getting started, non-critical dev/test	Billing & subscription support only; Access to community forums.

Support Plan	Use Case	Best For	Key Features
Developer	Experimenting	Non-production environments	Business hours support via email; <8hr initial response time for severity C.
Standard	Running production workloads	Production workloads with minimal downtime impact	24x7 support via email & phone; <4hr initial response for severity B.
Professional Direct	Business-critical workloads	Businesses relying heavily on Azure	<1hr initial response for severity A; Operational & architectural guidance.
Microsoft Unified (Highest)	Mission-critical dependence	Organizations with a complete, end-to-end Microsoft dependency	Technical Account Manager (TAM); Proactive guidance & workshops.

(Severity A: Critical impact | B: Moderate impact | C: Minimal impact)

This material provides a solid foundation for the AZ-900 exam. Be sure to complement it with the official Microsoft Learn AZ-900 learning path and practice exams. Good luck