AZ-900: Microsoft Azure Fundamentals Certification Cheat Sheet

Your Quick Reference Guide for AZ-900 Exam Preparation

Table of Contents

Fundamentals of Cloud Computing {#cloud-fundamentals}

What is Cloud Computing?

Cloud computing transmits computer services via the Internet to enable faster innovation, flexible resources, and scale economies. You typically only pay for the services you use.

Key Advantages:

- Reduce operational expenses
- Improve infrastructure efficiency
- Scale up or down based on business requirements
- Pay only for what you use (OpEx model)

Cloud Computing Services

Software as a Service (SaaS):

- No download/installation needed
- Accessible via web browser
- Cloud vendor manages everything
- Examples: Office 365, Google Docs, DropBox
- Users: End Customers

Platform as a Service (PaaS):

- Develop and maintain applications without managing infrastructure
- Cloud vendor manages: infrastructure, OS, middleware

- Examples: Heroku, Google App Engine, Azure Web Apps
- Users: Developers

Infrastructure as a Service (IaaS):

- Provides computation, storage, and networking resources on-demand
- Cloud vendor manages infrastructure; user manages OS, middleware, runtime
- Examples: AWS, Microsoft Azure, Google Cloud Platform
- Users: System administrators

Cloud Computing Models

Public Cloud: Services offered over the public internet, available to anyone

Private Cloud: Computing resources used exclusively by one organization

Hybrid Cloud: Combination of public and private clouds, with data/applications shared between them

Shared Responsibility Model

Cloud Provider Responsible For:

- Physical infrastructure (security, power, cooling, network)

Consumer Responsible For:

- Data and information stored in cloud
- Managing security access

Consumption-based Model

Capital Expenditure (CapEx):

- Upfront investment for physical assets
- Examples: Building datacenters, buying equipment

Operational Expenditure (OpEx):

- Day-to-day operations costs
- Cloud computing falls under OpEx

Benefits of Consumption-based Model:

- No upfront costs
- No need to buy/maintain expensive infrastructure
- Ability to pay for more resources when needed
- Ability to stop paying for unused resources

Cloud Pricing Models

Pay-as-you-go:

- Pay only for services used
- Plan and manage operational costs
- Run infrastructure more efficiently

Azure Reservations:

- Commit to one or three-year plans
- Save up to 72% compared to pay-as-you-go
- Good for predictable usage patterns

Azure Spot Instances:

- Use Microsoft's leftover capacity
- Save up to 90% compared to pay-as-you-go
- Best for stateless, non-critical workloads
- Not suitable for production environments

Azure Serverless Services

Serverless computing removes the need for infrastructure management. The cloud provider automatically provisions, scales, and oversees the infrastructure.

Azure Functions:

- Serverless computing service
- Supports: C#, F#, Node.js, Java, PHP
- Pay-as-you-go model
- Charges only when function is triggered
- Auto-scales automatically

Azure Core Architectural Components {#azure-core}

What is Azure?

Microsoft Azure is a cloud computing platform offering services through global datacenters.

Azure Regions, Region Pairs, and Sovereign Regions

Azure Regions:

- Geographical location with at least one datacenter
- Connected by low-latency network
- Azure has 60+ regions globally
- Resources must specify their region

Azure Region Pairs:

- Two Azure regions within same geography
- At least 300 miles apart

- For disaster recovery purposes
- If one region fails, services automatically failover to paired region

Sovereign Regions:

- Dedicated to specific sovereign entities
- Isolated in-country platforms
- May have restricted customer access
- Examples: Azure China 21Vianet, Azure Germany, Azure Government

Azure Availability Zones and Datacenters

Azure Datacenters:

- Unique physical buildings with networked computer servers
- Each contains power, cooling, and networking infrastructure
- Grouped into Regions/Availability Zones
- Not directly accessible to users

Azure Availability Zones:

- Physically distinct datacenters within an Azure region
- Self-contained with independent power, cooling, networking
- Connected through high-speed, private fiber-optic networks
- Allows redundant data storage for resilience

Azure Resources and Resource Groups

Azure Resources:

- Something used to manage services in Azure
- Can only belong to one resource group at a time
- Final component in Azure architectural hierarchy

Azure Resource Group:

- Logical mapping of resources
- Required for creating any resource
- Resource groups cannot be nested
- Resources in same group can be in different locations

Azure Subscriptions and Management Groups

Azure Subscriptions:

- Logical entity granting access to deploy Azure resources
- Purchased for specific time period
- Enables resource deployment and consumption

Azure Management Groups:

- Govern and manage access, compliance, rules for subscriptions
- Higher in hierarchy than subscriptions
- One subscription can have only one management group
- Allows managing multiple subscriptions as one unit

Hierarchy:
Management Groups > Subscriptions > Resource Groups > Resources

---

Azure Compute and Networking Services {#compute-networking}

Azure Virtual Machines

Overview:

- Infrastructure as a Service (IaaS) offering
- Cost-effective
- Multiple resources created with VM
- Users can choose configurations and OS

Connection Methods:

- Remote Desktop Connection (RDP)
- Azure Bastion Service

Azure Compute Types

Type	Use Case
Virtual Machines	Require maximum control over computing environment
Containers	Run batch jobs without managing infrastructure
Functions (Serverless)	Write less code, manage less infrastructure, save costs

Azure Availability Sets and Virtual Machine Scale Sets

Virtual Machine Availability Sets (VM AS):

- Provides high availability within datacenter
- Protects from rack/server failures
- **Fault Domains:** Rack-level protection (power/network failures)
- **Update Domains:** Server-level protection (patches/updates)
- 99.95% Azure SLA
- You pay for VMs, not for the Availability Set

Virtual Machine Scale Sets (VMSS):

- Create and manage group of identical load-balanced VMs
- Increases VM instances based on demand
- Easy to create and manage multiple VMs
- Optimizes costs by reducing redundant instances

Azure Virtual Desktop (AVD)

- Desktop virtualization service running on cloud
- Cloud-hosted Windows 10/11 desktops accessible from anywhere
- Works on: Windows, Mac, Android, Linux devices
- No additional license costs with Microsoft 365 or Windows license

Resources Required for Virtual Machines

- **Size:** Processor cores and RAM
- **Storage:** Hard drives, SSDs
- **Networking:** Virtual network, public IP, port configuration

Application Hosting Options in Azure

Option	Description
Virtual Machines	Maximum control over hosting environment
Containers	Strong separation and management of solution aspects
Azure App Service	HTTP-based service for hosting web applications

Azure App Service Features:

- High availability & automatic scaling
- Supports Windows and Linux
- Languages: .NET, .NET Core, Java, Ruby, Node.js, PHP, Python

Azure Virtual Networks

Overview:

- Azure VMs hosted in Azure Virtual Networks
- Must assign address space (example: 10.0.0.0/16)

Subnets:

- Small networks dividing VNet into sub-networks
- Range of IP addresses in VNet
- Each Network Interface Card (NIC) connects to one subnet

Virtual Network Peering (VNet Peering):

- Connect two virtual networks with private network
- Uses private IP address space
- No public IP needed
- **VNet Peering:** Same Azure region
- **Global VNet Peering:** Across Azure regions

Azure DNS

- **Purpose:** Translate service names to IP addresses
- Hosting service for DNS domains
- Benefits: Reliability, performance, security, ease of use
- Customizable VNets and alias records

Azure Virtual Private Network (VPN)

Overview:

- Encrypted tunnel within another network
- Connects trusted private networks over public internet

Azure VPN Gateway:

- Type of virtual network gateway
- Data encrypted in private tunnel
- Types: Policy-based or route-based
- Enables three types of connectivity:
    - On-premises to VNet (site-to-site)
    - Individual devices to VNet (point-to-site)
    - VNet to other VNets (network-to-network)

Azure ExpressRoute

- Extends on-premises networks to Microsoft cloud
- Private connection (not over public internet)
- Requires VNet Gateway and connectivity provider

Features & Benefits:

- Connectivity to Microsoft services in all regions
- Global connectivity with ExpressRoute premium
- Dynamic routing via Border Gateway Protocol
- Built-in redundancy for higher reliability
- Connection uptime SLA and QoS support

Azure Storage Services {#storage-services}

Azure Storage Types

Blob Storage:

- Store videos, images, large files, log files
- Stores data as objects
- Highly scalable object storage

Table Storage:

- Low-cost method for table-like data
- Key-attribute storage
- Most used for NoSQL data

File Storage:

- Uses Server Message Block Protocol
- Mount file shares on Windows, Linux, Mac
- Cloud file system functionality

Queue Storage:

- Messaging service
- Store and retrieve messages
- Can hold millions of messages

Azure Storage Tiers

Tier Comparison:

- **Hot:** Frequently accessed data, higher access costs, lower storage costs
- **Cool:** Infrequently accessed data, lower access costs, higher storage costs
- **Archive:** Rarely accessed data, lowest storage cost, highest access cost/latency

Choosing the Right Tier:

- Access frequency
- Data retention requirements
- Performance needs (latency/throughput)
- Budget for storage and access costs

Azure Redundancy Options

Primary Region Redundancy:

- **Locally Redundant Storage (LRS):** Copies data within single datacenter
- **Zone Redundant Storage (ZRS):** Copies data across availability zones
- **Geo-Redundant Storage (GRS):** Copies to secondary region

Secondary Region Redundancy:

- **Read-Access Geo-Redundant (RA-GRS):** Read access to secondary region
- **Geo-Zone-Redundant Storage (GZRS):** Combines ZRS and GRS

Azure File Movement Options

AzCopy:

- Command-line interface
- Copy blobs/files to/from storage account
- Upload, download, copy, synchronize files
- Works with other cloud providers

Azure Storage Explorer:

- Standalone app with graphical interface
- Manage files and blobs
- Runs on Windows, macOS, Linux
- Uses AzCopy backend

Azure File Sync:

- Transform Windows Server into cache for Azure file shares
- Supports SMB, NFS, FTPS protocols
- Centralize file shares in Azure Files
- Maintains on-premises performance

Azure Data Migration Options

Azure Migrate:

- Service for migrating on-premises to cloud
- Simplified migration, modernization, optimization
- Unified migration platform
- Range of tools for assessment and migration

Azure Data Box:

- Physical migration service
- Transfer large amounts of data quickly
- Best for data >40 TB with limited connectivity
- Use cases:
  - One-time migration
  - Media library offline to online
  - VM farm/SQL migration
  - Historical data analysis with HDInsight

Azure Identity, Access & Security {#identity-security}

Microsoft Entra

Suite of identity and network access solutions enabling organizations to:

- Adopt Zero Trust security framework
- Authenticate identities
- Assess access conditions
- Verify permissions
- Secure connection channels through encryption
- Monitor for compromise

Microsoft Entra ID

Overview:

- Cloud-based identity and access management service
- Market leader in managing directories
- Integrated cloud identity and access solution

Who Uses It:

- IT Admins: Manage app access by business needs
- App Developers: Standards-based authentication provider, SSO support

- Enterprise users: Already using if subscribed to Microsoft 365, Office 365, Azure, Dynamics CRM

License Types:

- Free
- P1
- P2
- External ID
- ID Governance
- Permissions Management

Differences: Azure AD vs Microsoft Entra ID

- **Rebranding:** Azure AD renamed to Microsoft Entra ID
- **Feature names updated:** "Azure AD Conditional Access" → "Microsoft Entra Conditional Access"
- Service plans updated accordingly

Azure Role-Based Access Control (RBAC)

Built-in Roles:

- **Owner:** Full access, can assign roles
- **Contributor:** Full access, cannot assign roles
- **Reader:** View-only access, no changes
- **User Access Administrator:** Manage user access to resources

Assigning Roles:

1. Navigate to resource in Azure portal
2. Go to Access Control (IAM)
3. Click 'Add role assignment'
4. Select role
5. Choose user/group/service principal/managed identity
6. Confirm assignment

Custom Roles:

- Create if built-in roles don't meet needs
- Define specific permissions tailored to requirements

Benefits:

- Simplified management
- Security through least privilege principle
- Minimum necessary permissions

Microsoft Entra Domain Services

Overview:

- Managed domain services
- Includes: domain joining, group policy, LDAP, Kerberos/NTLM
- No need to deploy/manage domain controllers

Key Features:

- One-way synchronization from Microsoft Entra ID
- Compatible with legacy applications
- On-premises AD DS integration via Microsoft Entra Connect

Azure Authentication Methods

Single Sign-On (SSO):

- Sign in once, access multiple resources
- Reduces password management burden
- Requires trust relationship between apps/providers
- Microsoft Entra ID Seamless SSO available

Multi-Factor Authentication (MFA):

- Two or more factors for access
- Factors: Something you know, possess, or are
- Examples: Password + phone code, password + fingerprint
- Global Administrator enables MFA in Microsoft Entra ID

Passwordless Authentication:

- Configure device as possession
- Authenticate with PIN or biometric
- Solutions: Windows Hello for Business, Microsoft Authenticator, FIDO2 keys

On-premises AD DS Authentication

- Azure file shares support AD DS authentication over SMB
- Maintain same authentication model during cloud migration
- Supports Kerberos authentication for hybrid identities

Microsoft Entra External ID

Overview:

- Solutions for collaborating with external users
- External users bring their own identities
- Works with corporate, government, social accounts

Capabilities:

B2B Collaboration:

- Collaborate with external users using their identity

- Share applications/services while controlling data
- Works without IT department on other side

B2B Direct Connect:

- Mutual trust with another Entra ID organization
- Seamless collaboration
- Currently supports Teams shared channels

B2C (Business-to-Customer):

- CIAM (Customer Identity Access Management) solution
- Millions of users, billions of authentications daily
- Automatic threat detection and response

Guest Access:

- Invite anyone with work, school, or social account
- Add guest users via Azure portal, PowerShell, or bulk invite
- Manage external identities and guest access

Microsoft Entra Conditional Access

Overview:

- Tool to allow/deny access based on identity signals
- Zero Trust policy engine
- Assesses signals from diverse sources

Key Features:

- **Conditional Access Policies:** Access controls based on location, device compliance, sign-in risk
- **Real-Time Risk Detection:** Works with Microsoft Entra ID Protection
- **Application Control:** Enforce policies for specific applications
- **MFA Support:** Require additional authentication for sensitive resources

Benefits:

- Empower users to be productive anywhere
- Protect organizational assets
- Granular MFA experience

Azure Managed Identity

System-Assigned Managed Identity:

- Service has identity instead of end-user
- Tightly coupled to Azure resource
- Advantages: Automatic credential rotation, identity lifecycle management

User-Assigned Managed Identity:

- Use when multiple resources share same target
- Identity independent of resource lifetime

- Useful for resource groups and scaling scenarios

Zero Trust and Defense in Depth Models

Zero Trust Concept:

- Assumes breach at outset
- Verifies each request as from uncontrolled network
- Three principles:
    - **Verify Explicitly:** Authenticate/authorize based on all available data
    - **Use Least Privilege Access:** Limit access with JIT/JEA, risk-based policies
    - **Assume Breach:** Verify end-to-end encryption, gain visibility, improve defenses

Defense-in-Depth:

- Multiple protective layers
- If one layer breached, next already in place
- Eliminates reliance on single protective layer
- Slows attacks, provides alerting information

Azure Cost Management {#cost-management}

Factors Affecting Costs in Azure

- Way resources are used
- Subscription type
- Pricing from third-party vendors through Azure Marketplace

Azure Meters:

- Used to create usage records for billing
- Always charged based on usage

Free Resources:

- Azure free trial: Access many products free for 12 months

Azure Cost Management and Billing

Cost Management:

- Analyze, manage, optimize costs
- Shows organizational cost and consumption patterns
- Advanced analytics for quick cost checks

Billing:

- Process of invoicing customers
- Manage invoices, payments, track expenses
- Multiple billing accounts supported

Azure Budgets

- Establish spending limits in Azure
- Configure at various scopes: Subscription, Resource Group, etc.
- Receive alerts when approaching limits
- Can automate actions (e.g., shut down VMs)

Azure Tags

Purpose:

- Organize Azure resources
- Metadata applied to resources

Structure:

- Key-value pairs
- Applied to resources, resource groups, subscriptions
- Help identify resources by organizational settings

Tools:

- Azure PowerShell: `New-AzTag`, `Update-AzTag`
- Azure CLI: `az tag create`, `az tag update`

Azure Pricing and TCO Calculators

Azure Pricing Calculator:

- Helps understand costs of Azure services
- Choose resources, modify settings, examine expenses
- Calculate exact service costs

Azure TCO Calculator:

- Calculates cost reductions from moving to Azure
- Produces comprehensive PDF report on savings
- Adjust factors: VM count, service tiers, etc.

Azure Monitoring Tools {#monitoring-tools}

Azure Advisor

Purpose:

- Recommendation tool providing suggestions
- Analyzes on four key aspects:
  - High availability
  - Security
  - Performance
  - Cost

Benefits:

- Maintain resource health
- Cost reduction opportunities
- Follow best practices

Azure Service Health

Overview:

- Informs about cloud resource health
- Tracks current/upcoming issues
- Combination of three services

Components:

- **Azure Status:** Global view of Azure service health across all regions
- **Service Health:** Personalized view of Azure services and regions
- **Resource Health:** Information about individual cloud resource health

Azure Monitor

Purpose:

- Improve performance and availability
- Complete solution for obtaining, evaluating, responding to telemetry
- Works across cloud, on-premises, hybrid, multi-cloud environments

Key Data:

- Metrics and Logs
- Create alerts based on metrics/logs
- Blade for service health monitoring

Features:

- Identify issues via diagnostic data
- Generate alerts based on health
- Proactive notifications for significant conditions

Azure Monitor Alerts

Purpose:

- Proactively notify of significant conditions
- Help identify and fix problems before customer impact
- Alert on any log/metric data source

Log Analytics and Application Insights

Log Analytics Workspace:

- Centralized environment for logging data
- Collects data from Azure Monitor, Microsoft Sentinel, Microsoft Defender for Cloud
- Write and run log queries
- Supports simple and complex queries
- Create multiple workspaces for:

    - Geographic data location
    - Access rights/permissions
    - Configuration settings (pricing tiers, data retention)

Application Insights:

- Feature of Azure Monitor
- Monitor web applications in-depth
- Supports Azure, on-premises, other cloud environments
- Provides extensible application performance management (APM)

Configuration Options:

- Install SDK in application
- Use Application Insights agent

Governance and Compliance {#governance}

Microsoft Purview

Overview:

- Comprehensive solutions for governing, protecting, managing data
- Unified platform addressing data fragmentation and visibility

Capabilities:

- Achieve comprehensive data visibility
- Protect and manage sensitive data throughout lifecycle
- Govern data innovatively
- Address data risks and regulatory requirements

Azure Policy

Purpose:

- Manage and prevent IT challenges
- Implement policy definitions establishing rules/effects
- Maintain organizational standards
- Evaluate compliance at scale

Benefits:

- **Ensure Compliance:** Resources and access conform to standards/regulations
- **Manage Resources:** Regulate costs, control resources via rules/effects
- **Enhance Security:** Impose resource configuration limitations
- **Mitigate IT Issues:** Prevent problems via policy enforcement

Policy Types:

- Built-in policies available
- Create custom policies as needed
- Examples: SKU limitations, mandatory tags, compliance requirements

Azure Resource Locks

Purpose:

- Safeguard resources from accidental deletion/modification
- Guarantee resources aren't inadvertently destroyed/changed

Scope Levels:

- Individual resources
- Resource groups
- Entire subscription
- Locks inherited (group lock applies to all resources)

Lock Types:

- **CanNotDelete:** User can view/change but not delete
- **ReadOnly:** User can read only, cannot change or delete
    - Effectively limits users to Reader role permissions

Management:

- Azure portal
- PowerShell
- Azure CLI
- Azure Resource Manager templates

Modifying Locked Resources:

1. Remove the lock
2. Make necessary changes (with appropriate permissions)
3. Resource locks take precedence over RBAC permissions

Additional Key Concepts {#additional}

Infrastructure as Code (IaC)

- Employs DevOps principles and version control
- Descriptive framework for establishing infrastructure components
- Consistent source code produces identical environments
- Enables collaborative DevOps practices
- Supports rapid, reliable large-scale deployment

Azure Resource Manager (ARM)

Overview:

- Deployment and management service for Azure
- Manage infrastructure through declarative templates
- Deploy, manage, monitor all subscription resources

Benefits:

- Declarative templates instead of scripts

- Manage complete subscription resources
- Apply access control to all services
- Apply tags for organization

Azure Resource Manager Templates

Purpose:

- Implement infrastructure as code (IaC)
- Use JavaScript Object Notation (JSON) syntax
- Define Azure infrastructure declaratively

Template Sections:

- Parameters
- Variables
- User-defined functions
- Resources
- Outputs

Azure Arc

Overview:

- Simplifies governance and management
- Consistent multi-cloud and on-premises management
- Centralized, unified way to manage entire environment

Capabilities:

- Project existing resources into Azure Resource Manager
- Manage VMs, Kubernetes clusters, databases as if in Azure
- Use familiar Azure services regardless of location
- Combine traditional ITOps with DevOps practices
- Configure custom locations on Arc-enabled Kubernetes

Managed Resources:

- Servers
- Kubernetes clusters
- Azure data services
- SQL Server
- Virtual machines

Features and Tools for Managing Azure Resources

Azure Portal:

- Web-based unified console
- Create and manage Azure resources
- Graphical user interface
- Manage subscriptions
- Build, manage, monitor simple to complex deployments
- Present in every Azure datacenter for resilience

- Continuous updates with no downtime

Azure PowerShell:

- Command-line tool for managing Azure
- Set of commands using PowerShell syntax
- Create, configure, manage Azure resources

Azure CLI:

- Command-line interface for managing Azure
- Built on Python
- Uses Bash commands
- Create, configure, manage resources

Azure Cloud Shell:

- Browser-based shell tool
- Accessible from Azure portal
- Supports both PowerShell and Azure CLI

Azure DevOps

Overview:

- Umbrella service for development services

Services:

- **Azure Boards:** Plan, track, discuss work across teams using agile methods
- **Azure Repos:** Version control (TFVS and Git support)
- **Azure Pipelines:** CI/CD solution with multiple deployment options
- **Azure Test Plans:** Testing tool for developer-tester communication
- **Azure Artifacts:** Private package manager
- **Azure DevTest Labs:** Create dev-test environments

Security Features in Azure

Microsoft Sentinel:

- Scalable, cloud-native security solution
- Combines SIEM and SOAR
- SIEM: Security Information and Event Management
- SOAR: Security Orchestration, Automation, Response
- Real-time threat intelligence
- Unified platform for threat visibility and proactive hunting

Microsoft Defender for Cloud:

- Monitoring tool for security posture management
- Threat protection
- Monitors cloud, on-premises, hybrid, multi-cloud environments

Azure DDoS Protection:

- Protects against Distributed Denial of Service attacks
    - **Basic:** Built-in to all Azure services, free
    - **Standard:** For sophisticated attacks, ~$3000/month, includes SLAs

Azure Key Vault:

- Cloud service for storing/accessing secrets
- Key management
- Secret management
- Certificate management
- Hardware model support
- Centralize application secrets
- Monitor access and usage
- Simplify resource management

Azure Network Security Group (NSG):

- Filter traffic to/from Azure resources in Virtual Network
- Default rules present
- Create custom inbound/outbound rules
- Deny or allow traffic

Azure Firewall:

- Fully managed, automatically scalable cloud network security service
- Protects Azure Virtual Network resources
- Define and enforce application and network connection policies

Azure Service Level Agreements (SLAs)

Overview:

- Microsoft's commitment to Azure services/products
- Individual SLAs for each service
- Specifies what happens if service fails
- Expressed as uptime and connectivity guarantees
- Performance targets: 99.9% to 99.99%

Composite SLA:

- When services are integrated and used together
- Formula: SLA of service 1 × SLA of service 2

Azure Service Lifecycle

Stages:

1. **Private Preview:** Available only to specific customers
2. **Public Preview:** Available to all customers, not suitable for production, no SLAs
3. **General Availability:** Available to all, supports SLAs, suitable for production

Azure Blueprints

Overview:

- Declarative way to orchestrate deployment of resource templates
- Step-by-step guide, design, or pattern

Artifacts:

- ARM Templates
- Resource Groups
- Azure RBAC
- Azure policies

Benefits:

- Save time in resource deployment
- Deploy resources quickly and efficiently

Microsoft Service Trust Portal

Overview:

- Public site for Microsoft compliance information
- Publishing audit reports and compliance data
- Associated with Microsoft cloud services

Content:

- Variety of tools and resources
- Shows Microsoft cloud service data protection
- Guidance on data security and compliance management

Access:

- Website: https://servicetrust.microsoft.com/
- Requires agreement to Microsoft Non-Disclosure Agreement

Last Updated: January 2026

This cheat sheet is a comprehensive quick reference guide for AZ-900 exam preparation. For detailed information, refer to official Microsoft Azure documentation.