

# AZ-900 Azure Fundamentals - Comprehensive Study Guide

## AZ-900: Microsoft Azure Fundamentals - Comprehensive Study Guide

Audience: Experienced Azure Infrastructure Architect relearning fundamentals with deep, hands-on detail. Exam Version: Skills measured as of January 14, 2026

### 1. Describe Cloud Concepts (25-30%)

#### 1.1 Define Cloud Computing

Cloud computing delivers computing services over the internet with pay-as-you-go pricing.

**Key characteristics:** - On-demand self-service - Broad network access - Resource pooling (multi-tenant) - Rapid elasticity - Measured service

**Architectural significance:** Design for elasticity, not peak capacity.

##### Shared Responsibility Model

Responsibility	On-Prem	IaaS	PaaS	SaaS
Physical security	You	Microsoft	Microsoft	Microsoft
Network controls	You	You	Microsoft	Microsoft
Operating system	You	You	Microsoft	Microsoft
Middleware/runtime	You	You	Microsoft	Microsoft
Application	You	You	You	Microsoft
Data and access	You	You	You	You

**Critical:** Data and access is ALWAYS your responsibility.

##### Cloud Models

**Public Cloud:** Shared tenants, zero CapEx. NOT for: strict data sovereignty. **Private Cloud:** Single org, Azure Stack. NOT for: when you need rapid elasticity. **Hybrid Cloud:** Most enterprises end up here. Key decisions: identity bridge (Entra Connect), networking (ExpressRoute vs VPN), management (Azure Arc).

##### Consumption-Based Model

Pricing Model	Discount	Best For
Pay-As-You-Go	None	Dev/test, variable workloads
Reserved Instances	Up to 72%	Steady-state production
Spot Instances	Up to 90%	Batch, fault-tolerant (evictable!)
Azure Hybrid Benefit	License reuse	Enterprises with SA

## Serverless

**Azure Functions:** Event-driven, auto-scale 0-N, 5min timeout (consumption). Use for: APIs, events, scheduled tasks.

**Azure Logic Apps:** Visual workflow, 200+ connectors, pay per action. Use for: integration, approval workflows.

## 1.2 Benefits of Cloud Services

---

### High Availability

- Availability Sets: 2+ fault domains, 5+ update domains (99.95% SLA)
- Availability Zones: 3+ separate DCs (99.99% SLA)
- Region Pairs: 300+ miles apart, sequential updates, geo-replication target

### Scalability

- Vertical (Scale Up): Increase instance size. Quick but limited.
- Horizontal (Scale Out): Add instances. Unlimited. No downtime.
- Auto-scaling: Azure Monitor rules. Don't forget scale-in rules!

### Reliability Patterns

Circuit breaker, retry with exponential backoff, bulkhead, health endpoint monitoring.

### Security and Governance

- Defender for Cloud, DDoS Basic (free), encryption at rest (AES-256) and transit (TLS 1.2+)
- Azure Policy, RBAC, Blueprints, Microsoft Purview
- Implement governance from day one

## 1.3 Cloud Service Types

---

### IaaS

Provider: infrastructure. You: OS, apps, data. Services: VMs, VNets, Load Balancer, Storage.

### PaaS

Provider: infrastructure + platform. You: apps, data. Services: App Service, SQL Database, Functions, Cosmos DB.

### SaaS

Provider: everything. You: just use it. Examples: M365, Dynamics 365, Power BI.

```
# IaaS - Create VM
az group create --name myRG --location eastus
az vm create --resource-group myRG --name myVM --image Ubuntu2204 --size Standard_D2s_v5 --admin-username azureuser --generate-ssh-keys

# PaaS - Create App Service
az appservice plan create --name myPlan --resource-group myRG --sku B1 --is-linux
az webapp create --name mywebapp12345 --resource-group myRG --plan myPlan --runtime "NODE|18-lts"
```

## 2. Describe Azure Architecture and Services (35-40%)

---

## 2.1 Core Architectural Components

---

### Regions

Set of datacenters in a latency-defined perimeter. Region pairs for DR. Sovereign: Gov, China (21Vianet), Germany.

Decision: Close to users > service availability > data residency > DR pairs > pricing.

### Availability Zones

Min 3 zones per enabled region. Zone-redundant (auto-replicate) vs Zonal (you manage). Not all regions support AZ.

### Hierarchy

```
Management Group (Root)
├── Management Group (Production)
│   ├── Subscription (Prod-App1)
│   │   └── Resource Group (rg-app1-prod-eastus)
│   └── Subscription (Prod-App2)
└── Management Group (Non-Production)
    ├── Subscription (Dev)
    └── Subscription (Test)
```

Resource Groups: Group by lifecycle and RBAC scope. Naming: rg-{project}-{env}-{region}. Subscriptions: Billing boundary. Design: by environment, department, or workload. Management Groups: Policy/RBAC inheritance across subscriptions.

## 2.2 Compute and Networking

---

### VM Series

B (burstable/dev), D (general), E (memory), F (compute), N (GPU), H (HPC), L (storage).

### VM Storage

Premium SSD v2 (sub-ms, configurable IOPS), Premium SSD (production), Standard SSD (moderate), Standard HDD (backup), Ultra Disk (databases).

### VM Scale Sets

Identical load-balanced VMs, auto-scale, up to 1,000 VMs.

### App Service

Managed PaaS. Deployment slots (Standard+), Easy Auth, VNet integration (Premium+). Tiers: Free to Isolated.

### Container Options

- ACI: Fastest launch, no orchestration. Simple workloads.
- AKS: Managed Kubernetes. Free control plane. Complex microservices.
- Container Apps: Serverless containers, KEDA scaling, Dapr. No K8s expertise needed.

### VNet

Private network in Azure. Single region. RFC 1918 address space. First 3 IPs per subnet reserved.

### VNet Peering

Connect VNets over Microsoft backbone. NOT transitive. Billed per GB.

## VPN Gateway

Site-to-Site, Point-to-Site, VNet-to-VNet. Tiers: VpnGw1 (650 Mbps) to VpnGw5 (10 Gbps).

## ExpressRoute

Private dedicated connection. 10/100 Gbps Direct. \$\$\$\$\$. Use for: low latency, high bandwidth, regulatory.

## Endpoints

Public: internet-accessible. Private: private IP from VNet. Private endpoints: eliminate data exfiltration, enable NSGs on PaaS.

## 2.3 Storage Services

---

### Overview

Blob (unstructured), Files (SMB/NFS shares), Queues (messaging), Tables (NoSQL), Disks (VM block storage).

### Tiers

Tier	Storage Cost	Min Duration	Access Time
Hot	Highest	None	Instant
Cool	Lower	30 days	Instant
Cold	Low	90 days	Instant
Archive	Lowest	180 days	Hours

Lifecycle management: Auto-move between tiers based on rules.

### Redundancy

Option	Description	Use Case
LRS	3 copies, 1 DC	Non-critical
ZRS	3 copies, 3 zones	HA within region
GRS	LRS + paired region	Cross-region DR
GZRS	ZRS + paired region	HA + DR
RA-GRS	GRS + read secondary	Read during outage
RA-GZRS	GZRS + read secondary	Best

Production minimum: ZRS. Cross-region DR: GZRS.

### Data Movement

AzCopy (CLI), Storage Explorer (GUI), File Sync (hybrid), Azure Migrate (assessment+migration), Data Box (offline: 40TB-1PB).

## 2.4 Identity, Access, and Security

---

### Microsoft Entra ID

Cloud identity and access management. Protocols: OAuth 2.0, SAML, OIDC.

Entra ID vs AD DS: Cloud (REST/OAuth) vs On-prem (LDAP/Kerberos). Entra ID: no GPO, MFA, Conditional Access.

### Authentication

SSO (one credential set), MFA (blocks 99.9% attacks), Passwordless (FIDO2, Authenticator, Windows Hello).

### Conditional Access

If-then policy engine. Signals: user/group, IP, device, app, risk. Controls: block, grant with MFA/device.

**Key policies:** Require MFA for all, block non-compliant devices, block legacy auth.

### Azure RBAC

Roles + Scope. Owner (full+delegate), Contributor (full, no delegate), Reader (view), User Access Admin.

Scope: MG > Subscription > RG > Resource. Inheritance applies.

Best practices: Least privilege, use groups not individuals, separate duties, PIM for JIT access.

### Zero Trust

Never trust, always verify. Verify explicitly, least privilege, assume breach.

### Defense-in-Depth

7 layers: Physical > Identity > Perimeter > Network > Compute > Application > Data.

### Microsoft Defender for Cloud

Secure Score (0-100%), CSPM (posture), CWP (workload protection). Plans: Servers, Databases, Storage, Containers, App Service, Key Vault, DNS, Resource Manager.

---

## 3. Describe Azure Management and Governance (30-35%)

---

### 3.1 Cost Management

---

Factors: resource type, consumption, region, network traffic.

Tools: Pricing Calculator, Cost Analysis, Budgets, Cost Alerts, Azure Advisor recommendations.

Tags: Key-value pairs. 50 per resource. NOT inherited from RG (use Policy for inheritance).

### 3.2 Governance and Compliance

---

#### Microsoft Purview

Data Map (discovery), Data Catalog (inventory), Data Estate Insights (visibility).

#### Azure Policy

Definitions (rules), Assignments (scope), Initiatives (collections).

Effects: Deny (block), Audit (log), DeployIfNotExists (auto-deploy), Modify (add/change tags).

Common: Allowed locations, allowed VM SKUs, require tags, enforce HTTPS, enforce encryption.

```
az policy assignment create --name "allowed-locations" \
  --policy "/providers/Microsoft.Authorization/policyDefinitions/e56962a6-4747-49cd-b67b-bf8b01975c4c" \
  --params '{ "listOfAllowedLocations": { "value": [ "eastus" ] } }' \
  --scope "/subscriptions/{sub-id}"
```

## Resource Locks

CanNotDelete: read/modify, no delete. ReadOnly: read only. Apply to ALL users including Owners.

## 3.3 Managing and Deploying Resources

---

### Azure Portal

GUI. Good for: exploration, one-time tasks. NOT for: repeatable deployments (use IaC).

### Cloud Shell

Browser shell with CLI and PowerShell pre-installed. Persist via Azure Files.

CLI: `az vm create` (JSON output, Bash-friendly). PowerShell: `New-AzVM` (objects, pipeline-friendly).

### Azure Arc

Extend Azure management to on-prem and multi-cloud. Servers, K8s, SQL Server, Data services.

### IaC

**ARM Templates:** Declarative JSON, idempotent, modular. Verbose. **Bicep:** DSL for ARM. Cleaner syntax, type checking, compiles to ARM JSON.

```
param location string = resourceGroup().location
param vmSize string = 'Standard_D2s_v5'

resource vm 'Microsoft.Compute/virtualMachines@2024-03-01' = {
  name: 'myVM'
  location: location
  properties: {
    hardwareProfile: { vmSize: vmSize }
    osProfile: {
      computerName: 'myVM'
      adminUsername: 'azureuser'
      linuxConfiguration: { disablePasswordAuthentication: true }
    }
  }
  storageProfile: {
    imageReference: {
      publisher: 'Canonical'
      offer: 'UbuntuServer'
      sku: '22_04-lts'
      version: 'latest'
    }
    osDisk: {
      createOption: 'FromImage'
      managedDisk: { storageAccountType: 'Premium_LRS' }
    }
  }
  networkProfile: {
    networkInterfaces: [{ id: nic.id }]
  }
}
```

```
}  
}
```

## 3.4 Monitoring Tools

### Azure Advisor

Free recommendations: Reliability, Security, Performance, Cost, Operational Excellence.

### Azure Service Health

Service issues, planned maintenance, health advisories, security advisories. Personalized to your resources.

### Azure Monitor

Metrics (93 days), Logs (KQL, 30-730 days), Alerts (rules + action groups), Application Insights (APM).

```
# Create Log Analytics workspace  
az monitor log-analytics workspace create --resource-group myRG --workspace-name myWorkspace  
  
# Create metric alert  
az monitor metrics alert create --name "HighCPU" --resource-group myRG \  
  --scopes "/subscriptions/{sub-id}/resourceGroups/myRG/providers/Microsoft.Compute/virtualMachines/myVM" \  
  --condition "avg Percentage CPU > 80"
```

### KQL Examples:

```
Perf | where ObjectName == "Processor" and CounterName == "% Processor Time"  
| where TimeGenerated > ago(1h)  
| summarize AvgCPU = avg(CounterValue) by Computer  
| where AvgCPU > 80
```

```
SigninLogs | where TimeGenerated > ago(24h) and ResultType != 0  
| summarize FailedLogins = count() by UserDisplayName, ClientAppUsed
```

## Quick Reference: Key Azure Services

Category	Services
Compute	VMs, VMSS, App Service, AKS, ACI, Container Apps, Functions, Virtual Desktop
Networking	VNet, VPN Gateway, ExpressRoute, Load Balancer, App Gateway, Front Door, DNS, Bastion
Storage	Blob, Files, Queues, Tables, Disks, Data Box
Identity	Entra ID, Domain Services, B2B, B2C, PIM
Security	Defender for Cloud, Key Vault, DDoS Protection, WAF, Sentinel
Management	Monitor, Advisor, Automation, Arc, Policy, Resource Graph
Governance	Policy, Blueprints, Purview, RBAC, Resource Locks