Microsoft Azure Fundamentals (AZ-900)

Full Learning Guide

This is a complete guide covering the **entire AZ-900 exam outline** in depth. It is written to function as a standalone study resource, but you are encouraged to cross-reference other materials to prepare.

Learning Objectives and Expectations

We'll cover:

- Every exam objective in detail.
- Every critical concept you must know and connect together.
- How to think like a cloud professional, not just memorize.

Each domain guide includes:

- Full concept breakdowns.
- Real-world examples.
- Exam tips and memory tricks.

AZ-900 Domains

Each domain is weighted differently on the exam:

- Domain 1: Cloud Concepts (25–30%)
- Domain 2: Azure Architecture and Services (35–40%)
- Domain 3: Azure Management and Governance (30–35%)

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Quick Reminder: How the Exam Works

- Number of Questions: ~35–40
- Format: Multiple choice, drag & drop, fill in the blank, hot area
- Time Limit: 45 minutes
- Passing Score: 700/1000 (about 70%)
- Test Provider: Pearson VUE or Certiport (onsite or online)

Top 10 AZ-900 Exam Tips

1. Understand Core Definitions: Be clear on cloud, IaaS, PaaS, SaaS, and deployment models.
2. Think in Scenarios: Know which service matches a scenario (VM = IaaS, App Service = PaaS, Office 365 = SaaS).
3. Focus on Service Purpose: Identify what each Azure service is *for* (App Service = web apps, Blob Storage = unstructured data, etc.).
4. Watch for Keywords: Look carefully for words like NOT, EXCEPT, BEST, FIRST.
5. Use Elimination: Narrow down choices quickly by crossing out the wrong ones.
6. Don't Overcomplicate: AZ-900 tests fundamentals — no deep configs, just purpose and concepts.
7. Manage Time: About 1 minute per question; skip and return if needed.
8. Remember Shared Responsibility: Who patches what depends on IaaS, PaaS, SaaS.
9. Answer Everything: No penalty for guessing — never leave blank answers.
10. Stay Calm: The pass mark is 700/1000 (~70%), so you don't need perfection.

Missing a few tricky questions won't ruin your chances, **stay calm**, trust your preparation, and keep moving forward.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale
Version 1.0

Domain 1: Cloud Concepts (25–30%)

1.1 What is Cloud Computing?

Cloud computing is the delivery of computing resources — servers, storage, databases, networking, applications, analytics — over the internet with **pay-as-you-go pricing**.

Key Features (from NIST definition):

- **On-demand self-service:** Provision resources instantly without human intervention.
- **Broad network access:** Access services from anywhere over the internet.
- **Resource pooling:** Multiple customers share infrastructure (multi-tenancy).
- **Rapid elasticity:** Scale up/down quickly as demand changes.
- **Measured service:** Usage is tracked, billed, and optimized.

Analogy: Like electricity. You don't build your own power plant; you consume electricity and pay for what you use. Azure provides the same model for computing.

Exam Tip: If asked "What is cloud computing?" → Answer: *on-demand, scalable IT resources delivered over the internet with consumption-based pricing.*

1.2 Cloud Deployment Models

Public Cloud:

- Infrastructure hosted by a provider like Microsoft Azure.
- Shared resources, multi-tenant.
- Example: A startup hosts its website on Azure Web Apps.

Private Cloud:

- Dedicated environment for a single organization (on-premises or hosted).
- Greater control, used for compliance or sensitive workloads.
- Example: A government agency running its own secure cloud.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Hybrid Cloud:

- Mix of on-premises and public cloud resources.
- Example: Company runs its core database on-premises but hosts the website in Azure.

Multi-Cloud:

- Using multiple cloud providers (Azure + AWS + GCP).
- Example: Enterprise runs analytics in Azure but hosts SaaS apps in AWS.

1.3 Service Models

IaaS (Infrastructure as a Service):

- You manage OS, applications, data.
- Azure manages physical hardware, networking.
- *Examples:* Azure VMs, Virtual Network, Managed Disks.

PaaS (Platform as a Service):

- You manage applications and data.
- Azure manages OS and runtime.
- *Examples:* Azure App Service, Azure SQL Database.

SaaS (Software as a Service):

- You only use the app.
- Azure manages everything (infra + app).
- *Examples:* Microsoft 365, Dynamics 365.

Comparison Table:

Model	Customer Manages	Azure Manages	Example
IaaS	OS, apps, data	Hardware, network	Azure VM
PaaS	Apps, data	+ OS, runtime, infra	App Service
SaaS	Data, identity	+ App + infra	Office 365

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

1.4 Shared Responsibility Model

- **Azure (provider):** Secures physical data centers, networking, hypervisors.
- **Customer:** Responsible for what they deploy (OS, apps, data, identity).

Breakdown by model:

- IaaS: You manage OS, apps, data.
- PaaS: You manage apps + data only.
- SaaS: You manage just data + access.

Example: Azure SQL Database (PaaS) → Azure patches SQL + OS, you manage the tables.

1.5 Benefits of Cloud

- **Scalability:** Scale up (bigger VM) or out (more VMs).
- **Elasticity:** Auto-adjust resources with demand.
- **High Availability:** Services remain online with redundancy (zones/regions).
- **Disaster Recovery:** Geo-redundancy + failover support.
- **Cost Efficiency:** Pay only for what you use.
- **Global Reach:** Deploy services in 60+ regions.
- **Agility:** Spin up resources in minutes.

Exam Tip: If a question asks "Which benefit lets you handle workload spikes automatically?" → Elasticity.

1.6 Cloud Economics

- **CapEx vs OpEx:**
  - CapEx = upfront hardware purchases.
  - OpEx = cloud subscription billing.
- **Consumption-based model:** Pay for resources as you use them (VM hours, GB of storage).
- **Reserved Instances:** Pre-pay for 1–3 years for discounts.
- **Spot Pricing:** Cheap compute for interruptible workloads.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 2: Azure Architecture and Services (35 to 40 percent)

2.0 Big Picture Map

Before diving into each service, visualize Azure as layers that work together:

- Global infrastructure: regions, availability zones, region pairs.
- Organization and access: tenants, subscriptions, management groups, resource groups, RBAC.
- Core building blocks: compute, networking, storage, data, identity, security, management, monitoring.
- App patterns: virtual machines, containers, web apps, serverless, data platforms, messaging.

Exam tip: Many questions are scenario based. Match a need to the right service. For example, private link to PaaS resource inside a VNet means Private Endpoint. Global HTTP load balancing with acceleration often means Front Door. DNS based traffic steering means Traffic Manager.

2.1 Azure Global Infrastructure

Regions

- A region is a geographic area that contains one or more datacenters.
- Examples: East US, West Europe, Japan East, Canada Central.
- You choose the region when creating most resources.

Availability Zones

- Physically separate datacenters within a region.
- Each zone has independent power, cooling, networking.
- Deploy across zones to achieve high availability for zonal capable services.
- Common pattern: spread VMs or instances across Zone 1, Zone 2, Zone 3.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Region Pairs

- Each Azure region is paired with another in the same geography when possible.
- Updates are rolled out in pairs to reduce simultaneous impact.
- Cross region replication features often use region pairs.

Service Types by Scope

- Zonal service: can pin an instance to a specific zone.
- Zone redundant service: automatically spans zones for resilience.
- Regional service: runs across the region but not tied to a zone.

Exam tip: If a question mentions surviving a full datacenter outage inside a region, think Availability Zones or zone redundant options.

2.2 Tenants, Subscriptions, Management Groups, Resource Groups

- **Tenant**: The Microsoft Entra ID directory for your organization.
- **Subscription**: Billing and resource boundary. Quotas, RBAC at subscription scope.
- **Management Group**: Container to organize multiple subscriptions. Apply policy and RBAC at scale.
- **Resource Group**: Logical container for related resources that share lifecycle, permissions, and tags.

Scope hierarchy for RBAC and Policy:
Management Group > Subscription > Resource Group > Resource

Exam tip: A resource group cannot span subscriptions. A resource can be moved between resource groups or subscriptions if the service supports it.

2.3 Compute

Virtual Machines (IaaS)

- Choose image, size (SKU), OS disk, data disks, VNet, NSG.
- Size series: General purpose (Dv, Av), compute optimized (F), memory optimized (Ev), storage optimized (L), GPU (NV, NC), HPC (HB, HC).

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

- Pricing options:
  - Pay as you go.
  - Reserved instances for 1 or 3 years discount.
  - Spot for interruptible, lowest cost.
- Availability features:
  - Availability Set spreads VMs across fault and update domains within a datacenter.
  - Availability Zones spread VMs across physically separate datacenters.
  - VM Scale Sets provide autoscale of identical instances with load balancing.
- Management helpers:
  - Azure Bastion for browser based RDP or SSH without exposing public IP on the VM.
  - VM extensions for agents and configuration.
  - Azure Automanage and Update Management for patching and baselines.
  - Azure Compute Gallery for custom images and versioning.

When to choose VMs:

- Full OS control needed.
- Legacy software not supported by PaaS.
- Specialized drivers or agents.

App Service (PaaS Web and API)

- Fully managed hosting for web apps and APIs.
- Supports .NET, Java, Node.js, Python, PHP, Ruby with Windows or Linux plan.
- App Service Plan controls compute, scaling, and pricing tier.
- Features: deployment slots, autoscale, managed certificates, custom domains, VNet integration, authentication providers.
- Use when you want to deploy code and avoid OS patching.

Containers

- **Azure Container Registry**: Private Docker registry for images.
- **Azure Container Instances**: Run containers without managing servers or orchestrators. Great for jobs and simple microservices.
- **Azure Kubernetes Service**: Managed Kubernetes. Azure runs the control plane, you run worker nodes. Integrates with CNI networking, ingress, autoscaling, secrets, identities.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

When to choose:

- ACI for quick, simple, ephemeral workloads.
- AKS for complex microservices with orchestration needs.

Serverless Compute

- **Azure Functions**: Event driven functions in multiple languages. Triggers include HTTP, queues, timers, event streams. Consumption plan bills per execution and time.
- **Logic Apps**: Low code workflow automation with hundreds of connectors. Great for integration and orchestration across SaaS and Azure services.
- **Event Grid**: Pub sub for events with push delivery and filters.
- **Event Hubs**: Big data event ingestion at scale.
- **Service Bus**: Enterprise messaging, queues and topics with sessions and dead letter.

Pattern primer:

- Functions plus Event Grid for reactive serverless.
- Logic Apps for workflow across services.
- Service Bus for reliable messaging and decoupling.

2.4 Networking

Virtual Network and Subnets

- Software defined private network in Azure.
- Choose RFC1918 address space, then carve into subnets by function: web, app, data, management.
- Subnet delegation to services like App Service Environment or AKS nodes is supported.

Network Security Groups

- Stateless allow or deny rules by source, destination, port, protocol.
- Apply to subnets and or NICs.
- Use Application Security Groups to group NICs by app role for simpler rules.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Routing

- System routes by default. Add User Defined Routes for custom paths.
- Common case: force traffic through a firewall or NVA in a hub subnet.

Name Resolution

- Azure provided DNS for internal VM to VM resolution inside a VNet.
- Azure DNS to host public zones.
- Private DNS zones for private name resolution across VNets linked to the zone.

Connectivity Options

- **VNet Peering**: Private connection between VNets. Same or different regions. Low latency.
- **Site to Site VPN**: IPSec tunnel over the internet between on prem and Azure VPN Gateway.
- **Point to Site VPN**: Client devices connect into VNet via VPN Gateway.
- **ExpressRoute**: Private dedicated circuit to Azure. Predictable latency and higher reliability.

When to choose:

- Need private, deterministic connectivity from datacenter means ExpressRoute.
- Temporary or cost sensitive site connectivity means Site to Site VPN.

Inbound and Global Routing

- **Azure Load Balancer**: Layer 4 for TCP or UDP traffic. Internal and external.
- **Application Gateway**: Layer 7 HTTP and HTTPS with Web Application Firewall.
- **Azure Front Door**: Global application acceleration plus layer 7 routing at edge. Supports caching, TLS offload, WAF.
- **Traffic Manager**: DNS based load balancing and failover across endpoints or regions.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Private Access to PaaS

- **Private Endpoint**: Maps a private IP in your subnet to a PaaS resource like Storage, SQL Database, Key Vault. Traffic stays on Microsoft backbone.
- **Service Endpoints**: Extend VNet identity to supported services. Still uses public endpoint but locked to VNet.

Prefer Private Endpoint when true private IP access is required.

Perimeter Security

- **Azure Firewall**: Stateful managed firewall with network, application rules, and Threat Intelligence.
- **DDoS Protection**: Basic is always on. Standard provides enhanced mitigation and telemetry for VNets.

2.5 Storage and Data Foundations

Storage Account Types

- General purpose v2 storage account is the common choice.
- Services inside:
    - **Blob Storage**: Object storage for unstructured data. Containers store blobs. Tiers:
        - Hot for frequent access.
        - Cool for infrequent.
        - Archive for rarely accessed and hours to rehydrate.
    - **Azure Files**: SMB or NFS file shares, mountable by VMs or on prem with Azure File Sync.
    - **Disks**: Managed disks for VMs. Premium SSD, Standard SSD, Standard HDD, Ultra SSD for high IOPS.
    - **Queues**: Simple message queues for decoupling work.
    - **Tables**: Key attribute store for simple NoSQL needs.

Redundancy Options

- LRS: Three copies in one datacenter.
- ZRS: Three copies across zones in one region.
- GRS: LRS in primary plus LRS in paired secondary region.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

- RA GRS: Same as GRS with read access to secondary.
- GZRS and RA GZRS: Combine zonal and geo redundancy.

Pick ZRS for zone level durability in region. Pick GRS or RA GRS for cross region DR.

Data Movement

- **AzCopy**: Command line copy tool optimized for speed.
- **Storage Explorer**: GUI management and transfers.
- **Azure File Sync**: Cache Azure Files on Windows Servers.
- **Data Box**: Ship a physical device for bulk offline transfer.
- **Azure Migrate**: Assess and move VMs and databases to Azure.

2.6 Databases and Analytics at a Glance

- **Azure SQL Database**: PaaS relational database based on SQL Server. Automatic patching, backup, HA. Models:
  - Single Database, Elastic Pool, Managed Instance for near full SQL Server compatibility.
- **Azure Database for MySQL or PostgreSQL**: Managed open source relational engines.
- **Cosmos DB**: Globally distributed NoSQL with low latency. Multi model APIs including Core SQL, Mongo API, Cassandra API. Choose consistency levels per request.
- **Azure Synapse Analytics**: Unified analytics for data warehousing and big data.
- **Data Lake Storage Gen2**: Hierarchical namespace over Blob for analytics at scale.
- **Event Hubs**: High throughput ingestion for telemetry.
- **Service Bus**: Enterprise messaging with queues and topics.
- **Azure Cache for Redis**: In memory data store for caching.

Exam tip: AZ 900 expects you to recognize the purpose, not to configure. Cosmos for global scale, SQL Database for managed relational, Service Bus for enterprise messaging, Event Hubs for streaming ingestion.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

2.7 Identity and Access

Microsoft Entra ID

- Cloud identity provider for users, groups, devices, applications.
- Supports SSO, MFA, Conditional Access, passwordless options, external identities.
- Tenants are the top identity boundary.

RBAC

- Assign built in or custom roles at scopes from management group down to resource.
- Common roles: Owner, Contributor, Reader, service specific roles.

Managed Identities

- System assigned identity for a resource or user assigned reusable identity.
- Use to obtain tokens for Azure services without storing secrets.

Azure AD Domain Services

- Managed domain join, LDAP, Kerberos for lift and shift scenarios without domain controllers.

Key Vault

- Secure storage for secrets, keys, certificates.
- Supports soft delete, purge protection, RBAC or access policies, and private endpoints.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

2.8 Security, Governance, Compliance

Defense in Depth Layers

- Physical, perimeter, network, compute, application, data, identity.
- Azure provides services at each layer. You align them with policy and RBAC.

Microsoft Defender for Cloud

- Posture management and threat protection.
- Secure score and hardening recommendations.
- Defender plans add workload protection for servers, containers, SQL, storage, and more.

Microsoft Sentinel

- Cloud native SIEM and SOAR. Ingests logs, correlates alerts, automated response.

Azure Policy

- Define and enforce rules such as allowed locations, VM SKUs, require tags, audit insecure settings.
- Assign at management group, subscription, or resource group.

Resource Locks

- CanNotDelete and ReadOnly locks to protect critical assets.

Blueprints

- Package ARM or Bicep templates, policies, and RBAC assignments to stamp out compliant environments.

Compliance

- Azure offers wide certifications and tools like Compliance Manager and Purview for data governance.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

2.9 Management, Deployment, Monitoring

Management Interfaces

- **Azure Portal**: Web UI for interactively managing resources.
- **Cloud Shell**: Browser shell with Azure CLI and Azure PowerShell preinstalled.
- **Azure CLI and PowerShell**: Scriptable automation.
- **ARM Templates and Bicep**: Declarative IaC for consistent deployments.
- **Azure Arc**: Bring servers and Kubernetes outside Azure under Azure management.

Monitor and Observability

- **Azure Monitor**: Metrics, logs, alerts for resources.
- **Log Analytics**: Central log store with KQL queries.
- **Application Insights**: Application performance monitoring, requests, dependencies, traces.
- **Service Health**: Personalized notifications about Azure issues affecting your resources.
- **Advisor**: Best practice recommendations for cost, performance, reliability, security.

Exam tip: Service Health is about Azure platform incidents that affect you. Azure Monitor and Log Analytics are about telemetry from your resources. Advisor is for optimization tips.

2.10 Choosing the Right Service Quickly

- Need full OS control or legacy software: Virtual Machines or VM Scale Sets.
- Need to deploy web or API without OS work: App Service.
- Need containers without managing clusters: Container Instances.
- Need Kubernetes orchestration: AKS.
- Need event driven compute: Functions.
- Need visual workflows across systems: Logic Apps.
- Need global web acceleration and WAF at edge: Front Door.
- Need HTTP layer 7 load balancing inside region: Application Gateway.
- Need TCP or UDP load distribution: Load Balancer.
- Need DNS based failover or geo routing: Traffic Manager.
- Need private IP to PaaS: Private Endpoint.
- Need hybrid connectivity:
    - Fast private link: ExpressRoute.
    - Encrypted over internet: Site to Site VPN.
- Need object storage tiers: Blob Hot, Cool, Archive.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

- Need SMB file shares: Azure Files, optionally with File Sync.
- Need managed relational database: Azure SQL Database or Managed Instance. Open source means Azure Database for MySQL or PostgreSQL.
- Need global NoSQL with low latency: Cosmos DB.
- Need messaging with advanced features: Service Bus. For streaming, use Event Hubs.
- Need secret management: Key Vault.
- Need policy enforcement at scale: Azure Policy. Package environments: Blueprints.

2.11 Mini Scenarios

1. You must expose a web app to global users with low latency and WAF.

- Use Azure Front Door with WAF, backend in multiple regions, health probes and path routing.

2. Your app must call Azure Storage without storing secrets.

- Enable a system assigned managed identity on the app and grant RBAC on the storage account.

3. You need to keep data within a country and survive a datacenter outage in region.

- Deploy in a region with Availability Zones and use zone redundant services. Consider region pair for DR.

4. On prem network must privately reach Azure workloads.

- Start with Site to Site VPN. For higher bandwidth and reliability, plan ExpressRoute.

5. You need to restrict resource creation to Canada regions and require cost center tags.

- Create policies for allowed locations and required tags at the subscription or management group.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Domain 3: Azure Management and Governance (30–35%)

3.1 Cost Management and Service-Level Agreements (SLAs)

Azure Pricing Models

- **Consumption-based (Pay-as-you-go):** Pay for what you use, no upfront costs.
- **Reserved Instances:** Prepay 1 or 3 years for up to 70% discounts. Applies to VMs, SQL DB, Cosmos DB.
- **Spot Pricing:** Use spare capacity at a lower price; workloads can be evicted.
- **Free Services:** Azure Free Account (12 months free services, $200 credit), always-free tier (e.g., 5GB Blob Storage).

TCO (Total Cost of Ownership) Calculator

- Estimates cost savings of moving workloads from on-premises to Azure.
- Shows CapEx → OpEx benefits.

Pricing Calculator

- Estimate cost of specific Azure resources.
- Useful for scenario questions like “Which option is most cost-efficient?”

Exam Tip: Pricing calculator = plan ahead. TCO calculator = compare on-prem vs cloud.

Azure SLAs

- Define uptime/availability guarantees.
- Example SLAs:
  - Single-instance VM: 99.9%
  - VM with Availability Zones: 99.99%
  - Azure SQL Database: up to 99.995%
- SLA depends on architecture. Redundancy improves SLA.

Composite SLA: Multiply SLAs of services. Example: 99.9% × 99.95% = ~99.85%.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

3.2 Azure Subscriptions, Accounts, and Billing

Accounts and Subscriptions

- One **Azure account** (user identity in Entra ID) can have multiple **subscriptions**.
- Subscriptions link to billing and quotas.
- Useful for separating environments (dev/test/prod) or departments.

Cost Management

- **Cost Analysis:** Visualize usage and spending.
- **Budgets:** Set budget alerts when nearing thresholds.
- **Exports:** Push cost data into storage for reporting.

Tags: Metadata key-value pairs applied to resources. Help organize and report cost by project, department, environment.

Exam Tip: Tags are for cost breakdowns and organization. Resource Groups are for lifecycle and management.

3.3 Azure Governance Tools

Azure Policy

- Enforce compliance at scale.
- Examples: restrict allowed regions, require tags, disallow unapproved VM sizes.
- Policies can audit, deny, or remediate.

Azure Blueprints

- Package templates (ARM/Bicep), policies, RBAC roles, resource groups.
- Deploy compliant environments consistently.

Management Groups

- Hierarchy above subscriptions.
- Apply RBAC and policy across multiple subscriptions.

Resource Locks

- **CanNotDelete:** Resource can't be deleted, only updated.
- **ReadOnly:** No changes allowed.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

3.4 Monitoring and Management

Azure Monitor

- Central platform for metrics, logs, alerts.
- Works with VMs, databases, apps, networking.

Log Analytics

- Query and analyze logs with **KQL (Kusto Query Language)**.
- Example: failed sign-ins, performance metrics.

Application Insights

- APM (Application Performance Monitoring).
- Tracks request performance, dependencies, exceptions.

Service Health

- Personalized view of Azure service issues.
- Three components:
  - **Service Issues:** Current outages.
  - **Planned Maintenance:** Upcoming downtime.
  - **Health Advisory:** Recommendations/updates.

Azure Advisor

- Best practice engine for:
  - Cost
  - Security
  - Performance
  - Reliability
  - Operational excellence

Exam Tip:

- Azure Advisor = best practices.
- Azure Monitor = metrics/logs.
- Service Health = Azure outages impacting you.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

3.5 Identity, Security, and Compliance

Microsoft Entra ID (formerly Azure AD)

- Core identity service.
- Features: SSO, MFA, Conditional Access, Identity Protection.

RBAC (Role-Based Access Control)

- Assigns permissions at scope (mgmt group → subscription → RG → resource).
- Common roles: Owner, Contributor, Reader.
- Exam trick: RBAC is NOT used for OS-level permissions. It's for Azure resources.

Authentication vs Authorization

- **Authentication:** Verify identity (password, MFA).
- **Authorization:** Define what the identity can do.

Security Tools

- **Microsoft Defender for Cloud:** Posture management + workload protection.
- **Microsoft Sentinel:** SIEM/SOAR for log analysis and incident response.
- **Key Vault:** Store secrets, keys, certs.

Compliance

- Azure has global certifications (ISO, SOC, GDPR, HIPAA).
- **Trust Center:** Lists certifications.
- **Compliance Manager:** Dashboard for audit readiness.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Services Overview (by Category)

Compute

Service	Purpose / What You Need to Know
Virtual Machines (VMs)	IaaS compute. Full OS control. Pricing: pay-as-you-go, reserved, spot.
VM Scale Sets	Autoscaling set of identical VMs.
Availability Sets	Spread VMs across fault/update domains in a datacenter.
Availability Zones	Spread VMs across datacenters for resiliency.
App Service	PaaS hosting for web apps/APIs. Supports multiple runtimes.
Azure Functions	Serverless, event-driven code execution. Pay per execution.
Logic Apps	Low-code workflows across SaaS, Azure, and on-prem.
Container Instances (ACI)	Run containers without infrastructure management.
Azure Kubernetes Service (AKS)	Managed Kubernetes orchestration.

Networking

Service	Purpose / What You Need to Know
Virtual Network (VNet)	Private network in Azure. Organize into subnets.
Network Security Groups (NSG)	Firewall rules by IP, port, protocol.
VPN Gateway	Site-to-site or point-to-site secure connections.
ExpressRoute	Dedicated private link to Azure.
Load Balancer	Layer 4 TCP/UDP load distribution.
Application Gateway	Layer 7 HTTP/S load balancing + WAF.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Azure Front Door	Global app acceleration and edge routing.
Traffic Manager	DNS-based routing and failover.
Private Endpoint	Private IP access to PaaS services.
Service Endpoints	Extend VNet identity to Azure services.

Storage

Service	Purpose / What You Need to Know
Blob Storage	Object storage for unstructured data. Hot, Cool, Archive tiers.
Azure Files	SMB/NFS file shares. Sync on-prem with File Sync.
Managed Disks	VM disks (SSD, HDD, Ultra).
Queues	Simple message queuing.
Tables	NoSQL key-value store.
Data Box	Physical device for offline bulk data transfer.

Databases

Service	Purpose / What You Need to Know
Azure SQL Database	PaaS relational database. Auto patching, backup, HA.
Azure SQL Managed Instance	Near full SQL Server compatibility.
Azure Database for MySQL/Postgres	Managed open-source relational databases.
Cosmos DB	Globally distributed NoSQL, multi-API, low latency.

Identity & Security

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Service	Purpose / What You Need to Know
Microsoft Entra ID (Azure AD)	Core identity. SSO, MFA, Conditional Access.
RBAC	Assign permissions at scope (mgmt group → resource).
Managed Identities	Secure app-to-service auth without secrets.
Key Vault	Secure storage for secrets, keys, certificates.
Defender for Cloud	Security posture management + workload protection.
Microsoft Sentinel	SIEM + SOAR for security monitoring/response.

Governance & Management

Service	Purpose / What You Need to Know
Resource Groups	Logical containers for resources.
Management Groups	Organize subscriptions for RBAC + Policy.
Azure Policy	Enforce compliance (locations, SKUs, tags).
Resource Locks	Protect critical resources from changes/deletion.
Tags	Metadata for organization and cost tracking.
Azure Monitor	Collect metrics, logs, alerts.
Log Analytics	Query logs using KQL.
Application Insights	Application performance monitoring.
Service Health	Personalized outage/maintenance info.
Azure Advisor	Best practice recommendations (cost, performance, security).

Cost & SLA

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale

Service	Purpose / What You Need to Know
Pricing Calculator	Estimate cost of resources before deployment.
TCO Calculator	Compare on-prem vs Azure costs.
Budgets	Set spending limits and alerts.
SLA (Service Level Agreement)	Defines uptime guarantees. Composite SLA = multiplication of services.

© 2025 · Curated by Artem Polynko · Follow on LinkedIn
Latest Guide Versions: https://linkedin.com/in/Artem-Polynko
Based on personal research and insights · Feel free to share with friends · Not for resale