AZ-104 – Detailed Learning and Study Guide

Azure Core Concepts

Cloud computing models: IaaS provides virtual machines and networking; PaaS provides managed platforms such as App Services; SaaS delivers complete applications. Understand regions, availability zones, region pairs, and SLAs. Know the difference between high availability, scalability, elasticity, and fault tolerance. Resources are logical objects deployed inside Resource Groups which belong to Subscriptions. Management Groups allow hierarchical governance. ARM is the deployment layer for Azure.

Identity and Access Management

Azure AD (Entra ID) is the identity provider for Azure. It is different from on■premises AD. Objects include users, groups, devices, app registrations and enterprise applications. Authentication proves identity; authorization controls access. MFA, Conditional Access and SSPR enhance security. RBAC controls access to Azure resources using roles such as Owner, Contributor and Reader. Scopes include management group, subscription, resource group and resource.

App Registrations and Service Principals

An App Registration represents an application in Azure AD. When an app is registered, a Service Principal is created in the tenant. Enterprise Applications are service principal instances used for access control. Authentication can use client secrets or certificates. Permissions are either delegated (user context) or application (app-only). Managed Identities provide identity to Azure resources without secrets.

Governance

Azure Policy enforces rules on resources. Initiatives are collections of policies. Blueprints help deploy repeatable environments. Tags help organize resources and cost tracking. Locks prevent accidental deletion or modification. Cost Management allows budgets and alerts. Advisor gives best-practice recommendations.

Networking

VNets provide isolated networks in Azure. Subnets divide VNets logically. NSGs filter traffic using priority-based rules. ASGs allow grouping of VMs for rules. UDR controls routing. VNet Peering connects VNets privately. VPN Gateway provides site-to-site or point-to-site connectivity. ExpressRoute gives private dedicated connectivity. Load Balancer works at Layer 4; Application Gateway works at Layer 7. Service Endpoints keep traffic on Azure backbone; Private Endpoints provide private IP access to PaaS. Azure Bastion enables secure RDP/SSH without public IPs.

Virtual Machines

VMs provide IaaS compute. Managed disks include Standard HDD, Standard SSD, Premium SSD and Ultra Disk. Availability Sets protect from hardware failure; Availability Zones protect from datacenter failure. Scale Sets provide auto-scaling. Snapshots capture disk state; Images capture reusable VM templates. Extensions enable configuration such as monitoring agents.

Storage

Storage accounts host blobs, files, queues and tables. Access can be controlled using keys, SAS tokens or Azure AD. Redundancy options include LRS, ZRS, GRS and GZRS. Blobs support Hot, Cool and Archive tiers. Lifecycle management automates tiering and deletion. Azure File Sync synchronizes on■premises file servers with Azure.

Backup and Disaster Recovery

Recovery Services Vault manages backups. Azure Backup protects VMs, files and workloads. Azure Site Recovery replicates VMs to another region for disaster recovery. Failover and failback operations restore services after outages.

Monitoring

Azure Monitor collects metrics and logs. Log Analytics enables advanced querying using KQL. Alerts trigger actions through Action Groups. Diagnostic settings route platform logs. Application Insights monitors application performance.

App Services and Containers

App Service Plans define compute for Web Apps and Function Apps. Deployment slots enable safe releases. Containers can run in Azure Container Instances or AKS. Azure Container Registry stores container images.

Automation

ARM Templates and Bicep automate deployments. Azure CLI and PowerShell manage resources via scripts. Automation Accounts and Runbooks enable scheduled automation.

Security

Microsoft Defender for Cloud provides security posture management. Just-in-Time VM access reduces attack surface. Key Vault stores secrets, keys and certificates securely.

Migration

Azure Migrate assesses on■premises workloads. Database Migration Service assists database movement. Data Box enables offline large data transfers.

Key Exam Comparisons

Understand differences: App Registration vs Enterprise App, Service Principal vs Managed Identity, NSG vs ASG, Service Endpoint vs Private Endpoint, VPN vs ExpressRoute, Policy vs RBAC, Availability Set vs Availability Zone, Metrics vs Logs.