AZ-104 Azure Administrator Study Notes

Disclaimer

These study notes are based on the official Microsoft AZ-104: Microsoft Azure Administrator certification course. The content has been compiled from Microsoft Learn materials and official documentation. While these notes have been structured and expanded for clarity, they are intended as a supplement to, not a replacement for, the official Microsoft training materials. Please refer to Microsoft Learn for the most up-to-date and comprehensive information.

Resources

These notes were prepared using the following official Microsoft training resources:

Microsoft AZ-104 Course Playlist: AZ-104: Microsoft Azure Administrator

Table of Contents

Azure Active Directory (Azure AD)

Overview

Azure Active Directory is Microsoft's cloud-based identity and access management service. It provides authentication and authorization services for Azure resources, Microsoft 365, and thousands of other SaaS applications.

Key Concepts

Tenant: An instance of Azure AD representing an organization. Each tenant has a unique directory and domain name (e.g., `contoso.onmicrosoft.com`).

Directory: A logical container within a tenant that holds users, groups, applications, and devices.

Subscription: A billing and management boundary for Azure resources. Each subscription is associated with a single Azure AD tenant, but a tenant can have multiple subscriptions.

User and Group Management

User Types:

- **Cloud Identity**: Users created directly in Azure AD
- **Directory-synchronized Identity**: Users synced from on-premises Active Directory using Azure AD Connect
- **Guest User**: External users invited for collaboration (B2B scenarios)

Group Types:

- **Security Groups**: Used for managing access to resources
- **Microsoft 365 Groups**: Used for collaboration, includes shared mailbox, calendar, files, etc.

Assignment Types:

- **Assigned**: Members are manually added
- **Dynamic User**: Membership based on user attributes using rules
- **Dynamic Device**: Membership based on device attributes using rules

Administrative Units: Allow you to subdivide your organization for administrative delegation. Useful for large organizations with autonomous divisions.

Azure AD Roles

Role Assignment Components:

- **Security Principal**: The who (user, group, service principal, or managed identity)
- **Role Definition**: The what (collection of permissions like read, write, delete)
- **Scope**: The where (management group, subscription, resource group, or resource)

Common Built-in Roles:

- **Global Administrator**: Full access to all administrative features
- **User Administrator**: Can manage users and groups
- **Billing Administrator**: Can make purchases and manage subscriptions
- **Security Administrator**: Can manage security-related features and policies

- **Application Administrator**: Can manage all aspects of app registrations

Custom Roles: Can be created when built-in roles don't meet specific requirements. Defined using JSON with specified permissions.

Self-Service Password Reset (SSPR)

Requirements:

- Azure AD Premium P1 or P2 license
- Users must be enabled for SSPR
- Users must register authentication methods

Authentication Methods (need to configure how many required):

- Mobile app notification
- Mobile app code
- Email
- Mobile phone (SMS)
- Office phone
- Security questions

Scope Options:

- None: SSPR disabled
- Selected: Enabled for specific groups
- All: Enabled for all users

Password Writeback: Allows password changes in Azure AD to be written back to on-premises Active Directory (requires Azure AD Connect).

Azure Resource Manager (ARM)

Overview

Azure Resource Manager is the deployment and management service for Azure. It provides a consistent management layer for creating, updating, and deleting resources in your Azure account.

Key Concepts

Resource: A manageable item available through Azure (VM, storage account, web app, database, virtual network, etc.).

Resource Group: A container that holds related resources for an Azure solution. The resource group includes resources you want to manage as a group.

Resource Provider: A service that supplies Azure resources. For example, `Microsoft.Compute` supplies the VM resource, `Microsoft.Storage` supplies the storage account resource.

ARM Template: A JSON file that defines the infrastructure and configuration for your deployment (Infrastructure as Code).

Resource Groups

Characteristics:

- Resources can only exist in one resource group
- Resource groups cannot be nested
- Resources can be moved between resource groups
- Resource groups cannot be renamed
- Resource groups can contain resources from different regions
- Deleting a resource group deletes all resources within it

Best Practices:

- Group resources by lifecycle (resources deployed, managed, and deleted together)
- Use consistent naming conventions
- Apply tags for organization and cost tracking
- Consider access control requirements when designing resource groups

Resource Locks

Prevent accidental deletion or modification of critical resources.

Lock Types:

- **CanNotDelete**: Authorized users can read and modify, but cannot delete
- **ReadOnly**: Authorized users can read, but cannot delete or modify

Lock Inheritance: Locks applied at a parent scope (subscription, resource group) apply to all resources within that scope.

Important Note: To delete a resource with a lock, you must first remove the lock.

Azure Policy

Enforce organizational standards and assess compliance at scale.

Policy Definition: Describes the compliance condition and the effect to take (deny, audit, append, modify, etc.).

Initiative Definition: A collection of policy definitions that are grouped toward a specific goal.

Assignment: A policy or initiative assigned to a specific scope (management group, subscription, resource group).

Policy Effects:

- **Deny**: Prevents the resource request
- **Audit**: Creates a warning event in the activity log
- **Append**: Adds additional fields to the resource
- **Modify**: Adds, updates, or removes properties or tags
- **DeployIfNotExists**: Deploys a resource if it doesn't exist
- **AuditIfNotExists**: Audits if a related resource doesn't exist

Common Use Cases:

- Enforce allowed VM SKUs
- Require specific tags
- Enforce naming conventions
- Restrict allowed locations
- Require encryption for storage accounts

Azure Blueprints

Enable quick creation of governed subscriptions by packaging artifacts like ARM templates, policy assignments, role assignments, and resource groups.

Components:

- **Artifacts**: The components included in the blueprint (policies, roles, templates, resource groups)
- **Blueprint Definition**: The reusable package
- **Blueprint Assignment**: The instance of a blueprint applied to a scope

Versioning: Blueprints support versioning, allowing you to track changes and assign different versions.

Virtual Networking

Overview

Azure Virtual Networks (VNets) enable Azure resources to securely communicate with each other, the internet, and on-premises networks.

VNet Fundamentals

Address Space: The private IP address space for the VNet defined using CIDR notation (e.g., `10.0.0.0/16`).

Subnets: Segmentation of the VNet address space into smaller networks (e.g., `10.0.1.0/24`, `10.0.2.0/24`).

Reserved IP Addresses: Azure reserves 5 IP addresses in each subnet:

- `.0`: Network address
- `.1`: Default gateway
- `.2` and `.3`: Azure DNS IPs
- `.255`: Network broadcast address

Region and Subscription: VNets are scoped to a single region and subscription, but can be connected across regions using VNet peering.

Network Security Groups (NSGs)

Filter network traffic to and from Azure resources in a VNet.

Rules Components:

- **Priority**: 100-4096 (lower number = higher priority)
- **Name**: Unique within the NSG
- **Source/Destination**: IP address, CIDR block, service tag, or application security group
- **Protocol**: TCP, UDP, ICMP, or Any
- **Port Range**: Single port or range
- **Action**: Allow or Deny

Default Rules (cannot be deleted but can be overridden):

- Allow all inbound from VNet
- Allow inbound from Azure Load Balancer
- Deny all other inbound
- Allow all outbound to VNet

- Allow all outbound to Internet
- Deny all other outbound

Association: Can be associated with subnets and/or network interfaces. Rules are evaluated separately for inbound and outbound traffic.

Service Tags: Represent groups of IP address prefixes from Azure services (e.g., `Storage`, `Sql`, `AzureMonitor`).

Application Security Groups (ASGs)

Group virtual machines and define network security policies based on workload rather than explicit IP addresses.

Benefits:

- More intuitive than managing IP addresses
- Easier to manage as infrastructure scales
- Supports application-centric security

Example: Create ASGs for Web, App, and Database tiers, then create NSG rules allowing traffic from Web to App, App to Database, etc.

VNet Peering

Connect VNets to enable resources to communicate across different VNets.

Types:

- **VNet Peering**: VNets in the same region
- **Global VNet Peering**: VNets in different regions

Characteristics:

- Non-transitive (if VNet A peers with VNet B, and VNet B peers with VNet C, VNet A cannot communicate with VNet C without explicit peering)
- No downtime during creation
- Low latency, high bandwidth
- Traffic stays on Microsoft backbone network
- Can peer across subscriptions and Azure AD tenants

Use Cases:

- Hub-and-spoke network topology
- Cross-region resource communication
- Cross-subscription resource communication

VPN Gateway

Establish encrypted connections between Azure VNets and on-premises networks or between VNets.

Connection Types:

- **Site-to-Site (S2S)**: IPsec/IKE VPN tunnel between on-premises VPN device and Azure VPN Gateway
- **Point-to-Site (P2S)**: VPN connection from individual computers to Azure VNet
- **VNet-to-VNet**: IPsec/IKE VPN tunnel between Azure VNets (alternative to VNet peering)

Gateway SKUs: Basic, VpnGw1, VpnGw2, VpnGw3, VpnGw1AZ, VpnGw2AZ, VpnGw3AZ (AZ = Availability Zone support)

Gateway Types:

- **Policy-based**: Static routing using IP address combinations
- **Route-based**: Dynamic routing using IP routing tables (recommended for most scenarios)

Requirements for Site-to-Site:

- Gateway subnet (minimum /29, recommended /27 or larger)
- Public IP address for the VPN gateway
- Compatible on-premises VPN device with public IP address
- Local network gateway representing on-premises network

Azure DNS

Host DNS domains and manage DNS records using Azure infrastructure.

Private DNS Zones: Provide name resolution for VMs within a VNet without custom DNS solution.

Public DNS Zones: Host publicly resolvable domain name records.

Record Types Supported:

- **A**: IPv4 address
- **AAAA**: IPv6 address
- **CNAME**: Canonical name (alias)
- **MX**: Mail exchange
- **TXT**: Text records

- **NS**: Name server
- **SOA**: Start of authority
- **SRV**: Service location
- **PTR**: Pointer (reverse DNS)

Auto-registration: VMs in a linked VNet can automatically register their DNS records in a private DNS zone.

Virtual Machines

Overview

Azure Virtual Machines provide on-demand, scalable computing resources with flexibility and control over the operating system and configuration.

VM Planning Considerations

Factors to Consider:

- **Network**: VNet, subnet, public IP, NSG requirements
- **Name**: Should follow naming convention, cannot be changed after creation
- **Location**: Region where VM resources are deployed (affects availability and pricing)
- **Size**: Determines CPU, memory, storage, and network capacity
- **Pricing Model**: Pay-as-you-go, Reserved Instances, Spot Instances
- **Storage**: OS disk, data disks, temporary disk
- **Operating System**: Windows or Linux distribution

VM Sizes and Families

General Purpose (B, Dsv3, Dv3, Dasv4, Dav4): Balanced CPU-to-memory ratio. Good for testing, development, small to medium databases, and low to medium traffic web servers.

Compute Optimized (Fsv2): High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.

Memory Optimized (Esv3, Ev3, Easv4, Eav4, Mv2, M): High memory-to-CPU ratio. Good for relational databases, medium to large caches, and in-memory analytics.

Storage Optimized (Lsv2): High disk throughput and IO. Good for Big Data, SQL, NoSQL databases, data warehousing, and large transactional databases.

GPU (NC, NCv2, NCv3, ND, NV): Specialized for graphics rendering and video editing. Available with single or multiple GPUs.

High Performance Compute (HB, HC, H): Fastest and most powerful CPU VMs. Available with optional high-throughput network interfaces (RDMA).

VM Availability Options

Availability Sets:

- Logical grouping of VMs that allows Azure to understand application redundancy
- **Fault Domains**: Physical separation (different power source and network switch) - up to 3 per availability set
- **Update Domains**: Logical separation for planned maintenance - up to 20 per availability set
- Provides 99.95% SLA when 2 or more VMs are in the same availability set

Availability Zones:

- Physically separate datacenters within an Azure region
- Each zone has independent power, cooling, and networking
- Minimum of 3 zones in enabled regions
- Provides 99.99% SLA for VMs deployed across 2 or more zones
- Protects against datacenter-level failures

Virtual Machine Scale Sets (VMSS):

- Create and manage group of load-balanced VMs
- Number of VM instances can automatically increase or decrease based on demand or schedule
- Provides high availability and application resilience
- Supports up to 1,000 VM instances (3,200 with custom images)

Azure Site Recovery:

- Replicates workloads to a secondary Azure region
- Provides disaster recovery (DR) capabilities
- Enables failover and failback operations
- Supports replication of Azure VMs, on-premises VMs, and physical servers

VM Storage

Disk Types:

- **OS Disk**: Contains the operating system (C: on Windows, /dev/sda on Linux) - required
- **Temporary Disk**: Provides short-term storage for page/swap files (D: on Windows, /dev/sdb on Linux) - data may be lost during maintenance events
- **Data Disks**: Managed disks attached for application data (E:, F:, etc. on Windows, /dev/sdc, /dev/sdd on Linux) - optional

Managed Disk Performance Tiers:

- **Ultra Disk**: Highest performance, up to 160,000 IOPS - mission-critical workloads
- **Premium SSD**: High performance, up to 20,000 IOPS - production workloads
- **Standard SSD**: Consistent performance, up to 6,000 IOPS - web servers, dev/test
- **Standard HDD**: Cost-effective, up to 2,000 IOPS - backup, non-critical workloads

Disk Encryption:

- **Azure Disk Encryption (ADE)**: Uses BitLocker (Windows) or DM-Crypt (Linux) to encrypt OS and data disks
- **Server-Side Encryption (SSE)**: Encryption at rest using platform-managed keys, customer-managed keys, or double encryption
- **Encryption at Host**: Encrypts data on the VM host before it flows to the storage service

VM Extensions

Small applications that provide post-deployment configuration and automation on Azure VMs.

Common Extensions:

- **Custom Script Extension**: Downloads and runs scripts on VMs (Windows and Linux)
- **Desired State Configuration (DSC)**: Apply and monitor PowerShell DSC configurations
- **Azure Diagnostics**: Collect monitoring data
- **VM Access Extension**: Reset credentials, RDP/SSH configuration
- **Antimalware Extension**: Microsoft Antimalware protection
- **Azure Monitor Agent**: Collect monitoring data for Azure Monitor

Deployment Methods:

- Azure Portal
- Azure CLI / PowerShell

- ARM Templates
- Azure Policy (for compliance enforcement)

Backup and Recovery

Azure Backup:

- Application-consistent backups for Windows VMs
- File-consistent backups for Linux VMs
- Retention up to 9,999 recovery points
- Supports instant restore, selective file recovery
- Encryption in transit and at rest
- No impact on VM performance

Recovery Services Vault:

- Storage entity for backup data
- Supports geo-redundant storage (GRS) and locally redundant storage (LRS)
- Stores recovery points for Azure Backup and Azure Site Recovery

Backup Policy Components:

- **Backup Schedule**: Frequency (daily or weekly) and time
- **Retention Range**: How long to keep recovery points (daily, weekly, monthly, yearly)
- **Instant Recovery**: Keep snapshot for 1-5 days for faster recovery

Azure Storage

Overview

Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios, offering highly available, massively scalable, durable, and secure storage.

Storage Account Types

General Purpose v2 (GPv2):

- Supports all storage services (Blob, File, Queue, Table)
- Supports all performance and redundancy options
- Lowest per-gigabyte pricing
- Recommended for most scenarios

General Purpose v1 (GPv1):

- Legacy account type

- Supports all storage services but lacks some newer features
- May have lower transaction costs in some scenarios

BlockBlobStorage:

- Premium performance for block blobs and append blobs
- Used for high transaction rates or low storage latency requirements
- Not recommended for large objects

FileStorage:

- Premium performance for file shares
- Recommended for enterprise or high-performance applications
- Supports NFS and SMB protocols

BlobStorage:

- Legacy account type for block and append blobs only
- Use GPv2 instead for new accounts

Storage Services

Blob Storage: Object storage for unstructured data (text, binary data, images, videos, backups).

Types:

- **Block Blobs**: Optimized for uploading large amounts of data efficiently (documents, media files)
- **Append Blobs**: Optimized for append operations (logging scenarios)
- **Page Blobs**: Optimized for random read/write operations (VM disks)

Access Tiers:

- **Hot**: Optimized for frequent access - higher storage costs, lower access costs
- **Cool**: Optimized for infrequent access, minimum 30 days - lower storage costs, higher access costs
- **Archive**: Optimized for rarely accessed data, minimum 180 days - lowest storage costs, highest access and retrieval costs (offline storage, requires rehydration)

File Storage: Fully managed file shares in the cloud accessible via SMB or NFS protocols.

Use Cases:

- Lift and shift applications requiring file shares
- Shared storage for cloud and on-premises applications

- Replace or supplement on-premises file servers
- Cross-platform file sharing

Performance Tiers:

- **Standard**: HDD-based, good for general purpose workloads
- **Premium**: SSD-based, low latency for IO-intensive workloads

Queue Storage: Message storage for reliable messaging between application components.

Table Storage: NoSQL key-value store for rapid development using structured datasets.

Storage Redundancy

Locally Redundant Storage (LRS):

- 3 synchronous copies in a single datacenter
- 11 nines (99.999999999%) durability
- Lowest cost option
- Protects against server rack and drive failures
- Does not protect against datacenter-level disasters

Zone-Redundant Storage (ZRS):

- 3 synchronous copies across 3 availability zones in the primary region
- 12 nines durability
- Recommended for high availability requirements
- Available in regions with availability zones

Geo-Redundant Storage (GRS):

- 3 synchronous copies in primary region (LRS)
- 3 asynchronous copies in secondary region (LRS)
- 16 nines durability
- Protects against regional disasters
- Data in secondary region not accessible unless failover occurs

Geo-Zone-Redundant Storage (GZRS):

- 3 synchronous copies across 3 availability zones in primary region
- 3 asynchronous copies in secondary region (LRS)
- 16 nines durability
- Maximum availability and durability

- Combines benefits of ZRS and GRS

Read-Access Options:

- **RA-GRS**: GRS with read access to secondary region
- **RA-GZRS**: GZRS with read access to secondary region

Access Control

Storage Account Keys:

- Two 512-bit keys for full access to storage account
- Should be rotated regularly and stored securely (Azure Key Vault recommended)
- Grants full access - use with caution

Shared Access Signature (SAS):

- URI that grants restricted access to storage resources
- Controls what resources client can access, permissions, and time validity

SAS Types:

- **Account SAS**: Delegated access to resources in one or more storage services
- **Service SAS**: Delegated access to a resource in a single storage service
- **User Delegation SAS**: Secured with Azure AD credentials (blobs only)

Stored Access Policy:

- Defined at container level
- Groups SAS constraints (start time, expiry time, permissions)
- Allows you to revoke or extend SAS without regenerating keys

Azure AD Integration:

- Supports Azure AD authentication for Blob and Queue services
- Use built-in RBAC roles (Storage Blob Data Reader, Storage Blob Data Contributor, etc.)
- Recommended for most scenarios requiring access control

Blob Lifecycle Management

Automate transitioning data to appropriate access tiers or deleting data at the end of its lifecycle.

Rule Components:

- **Filters**: Limit actions to subset of blobs (prefix match, blob types)
- **Actions**: Tier to cool, tier to archive, delete blob, delete blob snapshot

- **Conditions**: Based on days since creation, days since last modification, days since last access

Example Use Cases:

- Transition data to cool tier after 30 days of inactivity
- Archive data after 90 days
- Delete data after 365 days
- Delete old snapshots

Azure Storage Explorer

Standalone application for easily managing Azure Storage data on Windows, macOS, and Linux.

Features:

- Upload, download, and manage blobs, files, queues, tables
- Manage access permissions and policies
- Connect to storage accounts using account keys, SAS, or Azure AD
- Generate SAS tokens
- Manage storage account properties

AzCopy

Command-line utility for copying data to and from Azure Storage.

Common Uses:

- Upload files to blob or file storage
- Download blobs or files
- Copy data between storage accounts
- Sync local directory with blob container

Features:

- Resume failed operations
- Parallel uploads for better performance
- Built-in retry logic
- Works with Blob, File, and Table storage

Azure App Services

Overview

Azure App Service is a fully managed platform for building, deploying, and scaling web apps, mobile backends, and RESTful APIs.

App Service Plans

Defines the compute resources for your web apps.

Pricing Tiers:

Free and Shared (Preview):

- Shared compute resources
- No SLA
- 60 minutes CPU time per day (Free), 240 minutes (Shared)
- Limited to 1 GB disk space
- No custom domains on Free tier
- Good for development and testing

Basic:

- Dedicated compute resources
- 99.95% SLA
- Up to 3 instances (B1, B2, B3)
- Custom domains and SSL
- No autoscale
- Good for low-traffic apps

Standard:

- Dedicated compute resources
- 99.95% SLA
- Up to 10 instances (S1, S2, S3)
- Autoscale support
- Deployment slots (5 slots)
- Daily backups
- Good for production apps

Premium:

- Enhanced performance and scale
- 99.95% SLA
- Up to 30 instances (P1v2, P2v2, P3v2, P1v3, P2v3, P3v3)
- Deployment slots (20 slots)

- Higher backup frequency
- VNet integration
- Good for high-traffic production apps

Isolated:

- Dedicated Azure Virtual Network
- 99.95% SLA
- Maximum scale and isolation
- 100 instances
- Good for apps requiring network isolation or high scale

Characteristics:

- Apps in same plan share compute resources
- Deployment slots share resources
- All apps scale together
- Can host multiple apps in single plan

App Service Features

Deployment Slots:

- Live apps with their own hostnames
- Swap content and configuration between slots
- Enable validation before production deployment
- Minimize downtime during deployment
- Easy rollback capability
- Available in Standard tier and above

Swap Operation:

- Settings from target slot applied to source
- Source instances restarted
- Swap can be canceled before completion
- Can configure specific settings to be "slot settings" (not swapped)

Autoscaling:

- Scale out (increase instances) or scale in (decrease instances)
- Based on metrics (CPU, memory, HTTP queue length, custom metrics)
- Based on schedule (scale up during business hours)
- Minimum and maximum instance limits

- Cool-down period between scale events

Custom Domains:

- Map custom domain to your app
- Requires CNAME or A record in DNS
- Validate domain ownership
- Support for root domain and subdomains
- Multiple domains supported

SSL/TLS Certificates:

- Free managed certificates (App Service Managed Certificate)
- Upload your own certificate
- Import from Key Vault
- SNI SSL and IP-based SSL supported
- Enforce HTTPS (redirect HTTP to HTTPS)

Application Settings and Connection Strings:

- Stored securely and encrypted at rest
- Available as environment variables to application
- Can be marked as "slot settings" to prevent swapping
- Better than hardcoding values in application

Continuous Deployment

Supported Sources:

- **Azure DevOps**: Azure Pipelines for CI/CD
- **GitHub**: Automated deployment from GitHub repositories
- **Bitbucket**: Support for Bitbucket repositories
- **Local Git**: App Service hosts a Git repository
- **OneDrive/Dropbox**: File synchronization-based deployment
- **External Git**: Any external Git repository

Deployment Process:

- Configure deployment source
- Authenticate and authorize access
- Select repository and branch
- App Service monitors branch and deploys on commit
- Build automation (if supported by source)

Networking Features

VNet Integration:

- Access resources in or through a VNet
- Outbound traffic from app routed through VNet
- Requires Standard, Premium, or Isolated tier
- Regional VNet Integration (same region)
- Gateway-required VNet Integration (cross-region or classic VNet)

Hybrid Connections:

- Access on-premises resources without VPN
- Based on Azure Relay
- Each connection targets specific host:port
- Works with any protocol over TCP
- Windows and Linux support

Private Endpoints:

- Assign private IP from VNet to your app
- Removes public internet access
- App accessed only from within VNet or connected networks
- Requires Premium v2, Premium v3, or Isolated tier

Access Restrictions:

- Define allow or deny rules for inbound traffic
- Based on IP address or VNet/subnet
- Priority-based rules
- Service endpoints for Azure services

Azure Container Services

Overview

Azure provides multiple services for running containerized applications, offering flexibility in orchestration, management, and deployment.

Azure Container Instances (ACI)

Simplest and fastest way to run a container in Azure without managing virtual machines.

Features:

- Serverless containers
- Pay per second of execution
- Fast startup (seconds)
- Public IP and DNS name
- Custom sizing (CPU and memory)
- Persistent storage with Azure Files
- Linux and Windows containers

Use Cases:

- Simple applications
- Task automation
- Build jobs
- Batch processing
- Testing and development

Container Groups:

- Collection of containers scheduled on same host
- Share lifecycle, resources, local network, and storage volumes
- Similar to Kubernetes pod concept
- Support for multi-container deployments

Azure Container Registry (ACR)

Managed Docker registry service for storing and managing private container images.

Tiers:

- **Basic**: Cost-optimized for development, lower throughput and storage
- **Standard**: Increased storage and throughput for production workloads
- **Premium**: Highest storage and concurrent operations, geo-replication, content trust, private link

Features:

- Geo-replication (Premium tier): Replicate images across multiple Azure regions
- Image quarantine: Scan and verify images before making available
- Content trust: Sign and verify image integrity
- VNet and firewall rules: Restrict access to registry
- Customer-managed keys: Encrypt registry data with your own keys

- Azure AD authentication: Role-based access control

ACR Tasks:

- Automate container image builds
- Multi-step task workflows
- Build on commit or pull request
- Scheduled builds
- Cross-registry replication

Azure Kubernetes Service (AKS)

Managed Kubernetes service for deploying and managing containerized applications.

Features:

- Automated Kubernetes version upgrades
- Automated node patching
- Cluster autoscaling (nodes and pods)
- Integrated Azure Active Directory
- Azure Policy integration
- Azure Monitor integration
- Virtual network integration
- Azure CNI or kubenet networking
- HTTP application routing

Node Pools:

- **System Node Pool**: Hosts critical system pods (CoreDNS, metrics-server)
- **User Node Pools**: Host application workloads
- Support for Windows and Linux nodes
- Multiple node pools with different VM sizes

Cluster Components:

- **Control Plane**: Managed by Azure (API server, scheduler, controller manager)
- **Nodes**: VMs running kubelet, container runtime, and kube-proxy
- **Pods**: Smallest deployable units, can contain one or more containers
- **Services**: Stable network endpoint for accessing pods

Authentication and Authorization:

- Azure AD integration for cluster access
- Kubernetes RBAC for fine-grained permissions

- Azure RBAC for AKS resources
- Managed identities for pod authentication

Scaling Options:

- **Manual Scaling**: Manually increase/decrease replicas or nodes
- **Horizontal Pod Autoscaler (HPA)**: Automatically scale pods based on CPU, memory, or custom metrics
- **Cluster Autoscaler**: Automatically add/remove nodes based on pending pods
- **Virtual Nodes**: Provision additional capacity in ACI for burst scenarios

Networking Models:

- **kubenet**: Default, simpler, uses Azure-assigned IP addresses
- **Azure CNI**: Pods get IP addresses from VNet, direct VNet connectivity

Storage Options:

- **Azure Disks**: Block storage, attached to single pod
- **Azure Files**: SMB or NFS file shares, accessible by multiple pods
- **Persistent Volumes**: Kubernetes abstraction for storage
- **Storage Classes**: Define different storage tiers and properties

Container Deployment Comparison

When to Use ACI:

- Simple containerized workloads
- Quick testing and development
- Event-driven scenarios
- Batch jobs and task automation
- No orchestration needed

When to Use AKS:

- Microservices architectures
- Complex containerized applications
- Need for orchestration (scaling, networking, load balancing)
- Production workloads with high availability requirements
- Integration with DevOps pipelines
- Multi-container applications with dependencies

Monitoring and Backup

Azure Monitor

Comprehensive solution for collecting, analyzing, and acting on telemetry from cloud and on-premises environments.

Data Collection

Data Types:

- **Metrics**: Numerical values at specific points in time (CPU %, memory usage, network throughput)
- **Logs**: Event data stored in Log Analytics workspace (activity logs, diagnostic logs, custom logs)
- **Traces**: Distributed tracing for understanding application flow
- **Changes**: Change tracking and inventory data

Data Sources:

- **Application**: Application Insights for application performance monitoring
- **Operating System**: Performance and event data from VM guest OS
- **Azure Resources**: Resource metrics and diagnostic logs
- **Subscription**: Service Health and Activity Log
- **Tenant**: Azure AD audit logs

Metrics

Platform Metrics: Automatically collected from Azure resources at no cost.

Guest OS Metrics: Collected from VM operating system using diagnostics extension (requires Azure Monitor agent).

Application Metrics: Collected by Application Insights for web applications.

Custom Metrics: Metrics you define and send to Azure Monitor.

Metrics Explorer:

- Visualize and analyze metrics
- Create charts with multiple metrics
- Apply splitting and filtering
- Pin charts to dashboards
- Set up metric alerts

Logs and Log Analytics

Log Analytics Workspace:

- Centralized repository for log data
- Query logs using Kusto Query Language (KQL)
- Retention configurable (30-730 days)
- Role-based access control
- Data export capabilities

Common Log Tables:

- **AzureActivity**: Azure Resource Manager activity log
- **AzureMetrics**: Platform metrics
- **AzureDiagnostics**: Diagnostic logs from Azure services
- **Syslog**: Linux system logs
- **Event**: Windows Event Log
- **Heartbeat**: Agent health status
- **Perf**: Performance counters

Kusto Query Language (KQL) Basics:

- Pipe-based syntax: `Table | where condition | summarize aggregation`
- Time range filtering: `where TimeGenerated > ago(1h)`
- Aggregation: `summarize count() by Computer`
- Visualization: `render timechart`

Alerts

Proactively notified when issues are found in monitoring data.

Alert Components:

- **Alert Rule**: Defines condition and logic
- **Resource**: Target resource to monitor
- **Condition**: Signal (metric, log, activity log) and threshold
- **Action Group**: Set of actions (email, SMS, webhook, Logic App, Function, ITSM)
- **Alert Severity**: 0 (Critical) to 4 (Informational)

Alert Types:

- **Metric Alerts**: Based on metric threshold (near real-time)
- **Log Alerts**: Based on log query results
- **Activity Log Alerts**: Based on events in Activity Log
- **Smart Detection Alerts**: Application Insights automatic detection

Alert States:

- **New**: Alert just fired
- **Acknowledged**: Administrator reviewed
- **Closed**: Issue resolved

Application Insights

Application performance management (APM) service for developers and DevOps professionals.

Features:

- **Request rates, response times, failure rates**: Monitor web application performance
- **Dependency rates, response times, failure rates**: Track external dependencies (databases, APIs)
- **Exception tracking**: Detailed exception information
- **Page views and load performance**: Browser-based metrics
- **User and session counts**: Understand usage patterns
- **Performance counters**: Windows and Linux server metrics
- **Custom events and metrics**: Define your own telemetry

Application Map: Visualizes application architecture and component dependencies.

Live Metrics Stream: Real-time metrics with 1-second latency.

Availability Tests:

- **URL Ping Test**: Simple availability check from multiple locations
- **Multi-step Web Test**: Complex multi-request scenarios (deprecated, use availability tests)
- **Custom Track Availability**: Programmatic availability tests

Smart Detection: Automatically warns about potential performance problems and anomalies.

Network Watcher

Network monitoring, diagnostics, and analytics service.

Features:

IP Flow Verify: Check if packet is allowed or denied to/from VM based on NSG rules.

Next Hop: Determine next hop type and IP address for traffic from VM.

Connection Troubleshoot: Check connectivity between VM and destination (another VM, FQDN, URI, or IP).

NSG Flow Logs: Log information about IP traffic flowing through NSG.

- Source and destination IPs
- Source and destination ports
- Protocol (TCP/UDP)
- Allow or deny decision

Packet Capture: Capture network traffic to and from VM for analysis.

VPN Troubleshoot: Diagnose issues with virtual network gateways and connections.

Connection Monitor: Monitor connectivity and latency between VMs, applications, or services.

Traffic Analytics: Analyzes NSG flow logs to provide insights into traffic patterns.

Service Health

Personalized view of the health of Azure services and regions you're using.

Components:

Service Issues: Current problems in Azure services affecting you.

Planned Maintenance: Upcoming maintenance that could affect resource availability.

Health Advisories: Changes in Azure services requiring attention (deprecations, breaking changes).

Health Alerts: Notifications when Azure issues affect you.

Resource Health: Health status of individual Azure resources.

- **Available**: No problems detected
- **Unavailable**: Platform or non-platform event affecting availability
- **Degraded**: Performance issues detected
- **Unknown**: No information received for 10+ minutes

Azure Backup

Backup Solutions:

Azure VM Backup:

- Application-consistent backups (Windows) or file-consistent (Linux)
- No agent required for Azure VMs
- Backup and restore individual files or entire VM
- Retention up to 9,999 recovery points
- Geo-redundant storage option

Azure Files Backup:

- Snapshot-based backup
- No impact on performance
- Incremental backups after initial full backup
- Integration with Azure Backup policies

SQL Server in Azure VM:

- Application-aware backups
- Support for transaction log backups (every 15 minutes)
- Point-in-time restore
- Long-term retention (up to 10 years)

Recovery Services Vault:

- Storage for backups and recovery points
- Supports GRS and LRS
- Soft delete feature (retain deleted backups for 14 days)
- Encryption using platform-managed or customer-managed keys

Backup Policies:

- Define backup schedule (daily, weekly)
- Define retention (daily, weekly, monthly, yearly)
- Instant restore snapshot retention (1-5 days)
- Timezone for backup schedule

Backup Security:

- Encryption in transit (HTTPS/TLS)
- Encryption at rest (automatic)
- Soft delete (protection against accidental deletion)
- MFA for critical operations
- RBAC for access control

Azure Site Recovery (ASR)

Disaster recovery service for business continuity.

Capabilities:

- Replicate Azure VMs to secondary region
- Replicate on-premises VMs to Azure
- Replicate on-premises VMs to secondary site
- Orchestrate failover and failback
- Test disaster recovery without impact

Recovery Plans:

- Group machines for failover
- Define failover order
- Add manual actions or Azure Automation runbooks
- Test failover without affecting production

Replication Process:

1. Enable replication for VM
2. Mobility service installed (if needed)
3. Initial replication to target location
4. Delta replication (ongoing, async)
5. Failover when needed
6. Failback after primary site recovery

RPO and RTO:

- **RPO (Recovery Point Objective)**: How much data you can afford to lose - typically 60-90 seconds for Azure VM replication
- **RTO (Recovery Time Objective)**: How quickly you need to recover - automated orchestration reduces RTO

Exam Tips and Best Practices

General Exam Strategy

Time Management:

- 40-60 questions in approximately 100-120 minutes
- Mark questions for review
- Don't spend too much time on any single question
- Review marked questions if time permits

Question Types:

- Multiple choice (single answer)
- Multiple choice (multiple answers)
- Drag and drop
- Build list (ordering)
- Case studies (multiple questions based on scenario)
- Hot area (select region in image)

Passing Score: 700 out of 1000 (varies slightly)

Key Study Areas

Identity and Governance (15-20%):

- Azure AD users, groups, and RBAC
- Subscriptions and resource groups
- Azure Policy and Blueprints
- Cost management

Storage (15-20%):

- Storage accounts and redundancy
- Blob storage and access tiers
- Azure Files
- Access control (SAS, Azure AD)

Compute (20-25%):

- Virtual machines (sizes, availability, scaling)
- App Services and deployment slots
- Container services (ACI, ACR, AKS)
- VM extensions and automation

Networking (20-25%):

- VNets, subnets, and peering
- NSGs and application security groups
- VPN Gateway and ExpressRoute
- Azure DNS and Traffic Manager
- Load Balancer and Application Gateway

Monitoring and Backup (10-15%):

- Azure Monitor and Log Analytics

- Alerts and action groups
- Application Insights
- Azure Backup and Site Recovery
- Network Watcher

Hands-On Practice

Microsoft Learn Sandbox: Free Azure environment for completing Microsoft Learn modules.

Azure Free Account: $200 credit for 30 days plus 12 months of free services.

Practice Tasks:

- Create and configure VMs with availability sets
- Set up VNet peering between regions
- Configure NSG rules and test connectivity
- Create App Service with deployment slots
- Implement Azure Backup for VMs
- Set up Azure Monitor alerts
- Deploy AKS cluster and simple application
- Configure Azure Policy and review compliance

Common Pitfalls to Avoid

Resource Locks: Remember you must remove locks before deleting resources.

NSG Rule Priority: Lower number = higher priority. Default rules cannot be deleted.

VNet Peering: Non-transitive. If A peers with B and B peers with C, A cannot reach C without explicit peering.

Storage Account Names: Must be globally unique, 3-24 characters, lowercase letters and numbers only.

VM Temporary Disk: Data can be lost during maintenance or VM redeployment.

Availability Sets vs. Availability Zones: Different SLAs and protection levels.

Backup Retention: Maximum 9,999 recovery points for Azure VM backup.

Role Assignments: Security principal, role definition, and scope must all be correctly configured.

Managed Disk Encryption: Server-side encryption is automatic; Azure Disk Encryption requires configuration.

Documentation Resources

Official Microsoft Learn: https://learn.microsoft.com/en-us/certifications/exams/az-104

Microsoft Documentation: https://docs.microsoft.com/azure

Azure Updates: https://azure.microsoft.com/updates

Azure Architecture Center: https://docs.microsoft.com/azure/architecture

Final Notes

These study notes provide a comprehensive overview of the AZ-104 exam topics. However, Microsoft Azure is constantly evolving with new features and services. Always refer to the official Microsoft Learn platform and documentation for the most current information.

Recommended Study Approach:

1. Review these notes thoroughly
2. Complete Microsoft Learn learning paths for AZ-104
3. Practice hands-on in Azure Portal and with Azure CLI/PowerShell
4. Take practice exams to identify weak areas
5. Review and reinforce weak areas
6. Schedule and take the exam

Good luck with your AZ-104 certification!

About the Author

Jasmin Kahriman, MCT

Microsoft Certified Trainer passionate about Azure and cloud technologies.

For more Azure resources, tutorials, and certification guides, visit:

https://techwithjasmin.com/microsoft/how-to-pass-az-104-material-notes-practice-exam/

Connect on LinkedIn: https://www.linkedin.com/in/jasminkahriman/

Good luck with your AZ-104 certification journey!