Microsoft AZ-500 Certification Study Notes

Code: AZ-500

Identity & Access (25-30%)

Zero Trust & Core Security Concepts

Security principles, Zero Trust model, and shared responsibility

> **Domain Weight**
>
> Manage Identity and Access accounts for 25-30% of the AZ-500 exam. This domain covers Azure RBAC, Microsoft Entra ID, PIM, Conditional Access, and external identities.

Zero Trust Model

Verify Explicitly

Always authenticate and authorize based on all available data points — identity, location, device, service/workload, data classification, and anomalies.

Use Least Privilege Access

Limit user access with just-in-time (JIT) and just-enough-access (JEA), risk-based adaptive policies, and data protection.

Assume Breach

Pillar	Focus	Key Microsoft Solution
Identities	Verify with strong authentication, risk-based access	Microsoft Entra ID, ID Protection
Endpoints (Devices)	Validate device health and compliance before granting access	Microsoft Intune, Defender for Endpoint
Applications	Govern app permissions, shadow IT, in-app privileges	Defender for Cloud Apps, Entra App Proxy
Data	Classify, label, and encrypt; protect regardless of location	Microsoft Purview, AIP/MIP sensitivity labels
Infrastructure	Assess versions, configurations, and JIT access	Defender for Cloud, Azure Policy
Networks	Segment, encrypt, and limit lateral movement	Azure Firewall, NSG, DDoS Protection, WAF

Shared Responsibility Model

Responsibility	On-Premises	IaaS	PaaS	Sa

Responsibility	On-Premises	IaaS	PaaS	Sa
Application	Customer	Customer	Customer	Sh
Identity & Access	Customer	Customer	Customer	Cu
Data	Customer	Customer	Customer	Cu

Key Security Concepts

- Defense in depth: Layered security approach — physical, identity, perimeter, network, compute, application, data
- Encryption at rest: Protects stored data (Azure Storage Service Encryption, Transparent Data Encryption for SQL)
- Encryption in transit: Protects data moving over networks (TLS, HTTPS, VPN)
- Hashing: One-way function for integrity verification — cannot be reversed (SHA-256, bcrypt for passwords)
- Authentication vs Authorization: Authentication = who are you; Authorization = what can you do
- Accountability (Auditing): Recording what an authenticated user did for forensic and compliance purposes
- Federation: Cross-organization trust — user authenticates at home IdP, partner trusts the token
- Passwordless authentication: Windows Hello for Business, FIDO2 security keys, Microsoft Authenticator — no password in auth flow

Secure Networking (20-25%)

Secure Networking accounts for 20-25% of the AZ-500 exam. Topics include NSGs, Azure Firewall, WAF, DDoS Protection, Private Link, Azure Bastion, and VPN/ExpressRoute security.

Network Security Groups (NSGs)

- Layer 4 filter: Allow/deny rules based on source/destination IP, port, and protocol (TCP/UDP/Any)
- Priority-based evaluation: Rules evaluated lowest to highest priority number — first match wins. Default rules (65000-65500) allow VNet traffic and deny all internet inbound
- Can be associated with subnets or individual VM NICs — subnet-level preferred for manageability
- Application Security Groups (ASGs): Tag VMs into logical groups (e.g., 'WebServers', 'DBServers') — NSG rules reference ASGs instead of individual IPs
- NSG Flow Logs: Log accepted and denied flows to Storage Account — queryable via Traffic Analytics in Network Watcher
- Effective security rules: View the merged NSG rules actually applied to a NIC from both NIC-level and subnet-level NSGs

Azure Firewall vs NSGs

Key Distinction

NSGs are stateful Layer 4 packet filters attached to subnets/NICs — applied per resource. Azure Firewall is a centralized managed Layer 4+7 gateway in a dedicated subnet (AzureFirewallSubnet) inspecting all traffic. Use both: NSGs for micro-segmentation, Azure Firewall for centralized egress, FQDN filtering, and threat intelligence.

Feature	Azure Firewall Standard	Azure Firewall Premiu

Feature	Azure Firewall Standard	Azure Firewall Premiu
Threat Intelligence	Alert/deny known malicious IPs/FQDNs	Same + enhanced IDF signatures
IDPS	No	Yes — intrusion detection/prevention - alert or deny
TLS Inspection	No	Yes — decrypt, inspec re-encrypt HTTPS traffic
Web Categories	No	Yes — block by category (gambling, adult content)

Web Application Firewall (WAF)

WAF Deployment	Scope	SKU Required
Application Gateway + WAF	Regional load balancer for web apps	Application Gateway WAF v2
Azure Front Door + WAF	Global edge — CDN + WAF at PoPs worldwide	Front Door Premium / Standard + WAF policy
Azure CDN + WAF	CDN-delivered static content protection	Verizon Premium CDN (classic WAF)

- Custom WAF rules: Applied before OWASP rules — allow trusted IP ranges, block specific geo-locations or URIs
- Rate limit rules (Front Door WAF): Limit requests per IP per minute — mitigates Layer 7 DDoS and scraping attacks

Azure DDoS Protection

Tier	Cost	Capabilities
Basic (infrastructure)	Free — included by default	Always-on monitoring — common volumetric attack mitigation at platform level
DDoS Network Protection	Per month per protected VNet	Adaptive tuning per public IP, rapid response team, cost protection, post-attack reports, Attack metrics
DDoS IP Protection	Per month per public IP	Same capabilities as Network Protection but scoped to individual IP — cost-effective for single IP

- Protects against: Volumetric (bandwidth floods), Protocol (SYN flood, ping of death), Resource/Application layer attacks (HTTP floods)
- DDoS Standard auto-tunes mitigation thresholds per protected IP based on historical normal traffic
- Pair with Azure WAF: WAF handles Layer 7 HTTP-based attacks; DDoS Protection handles Layers 3+4 volumetric attacks — complementary

Private Link & Private Endpoints

- DNS override required: Create private DNS zone (e.g., privatelink.blob.core.windows.net) so FQDN resolves to the private IP inside VNet
- Disable public access: After creating Private Endpoint, disable public network access on the PaaS resource to enforce private-only connectivity
- Private Link Service: Expose YOUR OWN service over Private Link so consumers in other VNets/tenants can connect privately

Azure Bastion

- Browser-based RDP/SSH access to VMs via Azure Portal — no public IP required on the VM
- Traffic tunneled over TLS port 443 to the Bastion host in AzureBastionSubnet (/27 or larger) — no RDP 3389 / SSH 22 inbound rules needed on NSG
- Basic SKU: Portal-based RDP/SSH only. Standard SKU: Native RDP/SSH client support, VM copy/paste, VNet peering, shareable access links
- Eliminates jump-server VMs and reduces attack surface — no management ports exposed to internet

VPN & ExpressRoute Security

Connection Type	Encryption	Key Use Case
Site-to-Site VPN	IPsec/IKEv2 — encrypted over public internet	On-prem datacenter persistent tunnel to Azure VNet
Point-to-Site VPN	SSL/TLS or IKEv2	Individual remote workers connecting to Azure VNet

Connection Type	Encryption	Key Use Case
ExpressRoute + VPN (MACSec or IPsec)	IPsec tunnel over private ER circuit	Compliance requiring both private circuit AND encryption

Secure Compute/Storage/DB (20-25%)

Secure Compute, Storage, and Databases

JIT VM access, disk encryption, Key Vault, storage security, database security, and containers

> **Domain Weight**
>
> Secure Compute, Storage, and Databases accounts for 20-25% of the AZ-500 exam. Topics include JIT VM access, Azure Disk Encryption, Key Vault, storage access control, SQL security, and container registry/AKS security.

Azure Key Vault

Object Type	Purpose	Examples
Secrets	Secure storage of small sensitive text values	Connection strings, API keys, passwords, SAS tokens

Object Type	Purpose	Examples
Certificates	X.509 certificate lifecycle — create, import, auto-renew	SSL/TLS certs for apps, mutual TLS service auth

- Access control: Vault access policy (legacy per-vault) vs Azure RBAC (recommended — granular per secret/key/certificate, auditable via IAM)
- Soft-delete: Deleted objects retained for 7-90 days — recoverable, protects against accidental deletion. Purge protection prevents permanent deletion of soft-deleted objects
- HSM-backed keys: Standard tier — FIPS 140-2 Level 2 HSM. Premium tier — FIPS 140-2 Level 3 HSM-backed keys. Managed HSM — dedicated single-tenant FIPS 140-2 Level 3
- Managed Identity integration: App's managed identity authenticates to Key Vault without any credentials in code or configuration
- Private Endpoint for Key Vault: Disable public access, route Key Vault API calls through private IP in your VNet

Just-in-Time (JIT) VM Access

- Feature of Microsoft Defender for Servers P2 (Defender for Cloud) — requires Defender for Servers plan enabled
- Locks down NSG management ports (RDP 3389, SSH 22, WinRM 5985) with Deny rules by default
- Time-limited access: Requestor specifies source IP/CIDR and time window (max 3 hours default) → Defender for Cloud temporarily adds Allow rule to NSG, then auto-removes it
- All JIT requests logged in Azure Activity Log and Defender for Cloud — who requested, source IP, approved by whom, time window

Azure Disk Encryption Options

Method	Layer	Key Storage
SSE with CMK (BYOK)	Azure Storage layer — disks encrypted with customer key	Customer-Managed Keys in Key Vault or Managed HSM
Azure Disk Encryption (ADE)	OS volume inside the VM — BitLocker (Windows) / DM-Crypt (Linux)	Key wrapped by Key Vault — OS-level encryption, covers boot volume
Encryption at host	VM host cache encrypted before writing to storage — end-to-end	PMK or CMK — also covers temp disk and OS/data disk cache

> **ADE vs SSE**
>
> SSE with CMK encrypts at the Azure Storage layer (applied by Azure outside the VM). ADE encrypts at the OS level inside the VM using BitLocker or DM-Crypt. ADE is required when workloads need OS-level encryption visible to the guest OS. Both can be combined for defense in depth.

Azure Storage Security

Access Method	Best For	Notes
Azure RBAC	Azure identities (users, service principals,	Use storage data roles: Storage Blob Data

Access Method	Best For	Notes
Service SAS	Time-bound access to single service (blob, queue, table, file)	Signed with storage account key — rotatable
Account SAS	Time-bound access across multiple services	Signed with storage account key — broadest SAS scope
Storage Account Keys	Full admin access — emergency/legacy use only	Two keys for zero-downtime rotation — avoid using in applications

- Secure transfer required: Enforce HTTPS on all REST API calls — disable HTTP to prevent cleartext data in transit
- Storage Firewall: Restrict access to specific VNet subnets, IP ranges, or trusted Azure services
- Anonymous public access: Disable at the storage account level unless explicitly required — prevents container-level public blob access
- Defender for Storage: Detects anomalous access patterns, malware uploaded to blob storage, and sensitive data exposure

Azure SQL Database Security

- Transparent Data Encryption (TDE): Encrypts database, backups, and log files at rest — enabled by default. Use CMK (BYOK) for customer-controlled keys stored in Key Vault
- Always Encrypted: Column-level encryption — plaintext data never leaves the client; SQL Server/Azure SQL only sees ciphertext. Keys held by client app
- Row-Level Security (RLS): Database-enforced row filtering via predicate

- SQL Auditing: Logs all database-level events to Storage Account, Log Analytics, or Event Hub — required by many compliance frameworks
- Server-level firewall rules: IP whitelist rules for Azure SQL logical server — use Private Endpoint for private-only connectivity

Container Security

- Azure Container Registry (ACR): Private registry — use Azure RBAC roles (AcrPull, AcrPush) instead of admin credentials, disable anonymous pull access
- Defender for Containers: Scans ACR images for known OS/package vulnerabilities — zero-day CVE alerts. Also provides runtime protection for AKS workloads
- AKS security: Enable Kubernetes RBAC, integrate with Microsoft Entra ID for authentication, apply Kubernetes Network Policies to restrict pod-to-pod traffic
- Workload Identity (AKS): Pods use managed identity via OIDC federation — replaces pod-level service principals, eliminates credential management in containers
- Azure Policy for AKS: Enforces pod security standards (no privileged containers, required resource limits, disallowed host paths) via Azure Policy add-on

Security Operations (25-30%)

Defender for Cloud & Microsoft Sentinel

CSPM, workload protection plans, SIEM/SOAR, and Azure security governance

> **Domain Weight**
>
> Manage Security Operations accounts for 25-30% of the AZ-500 exam.

CSPM — Cloud Security Posture Management

- Foundational CSPM: FREE — assesses all Azure resources against Microsoft Cloud Security Benchmark (MCSB)
- Secure Score: 0-100% rating based on completed security recommendations — prioritized by impact
- Regulatory Compliance Dashboard: Maps MCSB controls to frameworks (CIS Benchmarks, NIST SP 800-53, PCI DSS, ISO 27001, SOC 2)
- Enhanced CSPM (paid): Attack path analysis, agentless scanning, data security posture management (DSPM), external attack surface management

CWPP — Cloud Workload Protection Plans

- Defender for Servers P1: MDE integration, OS-level vulnerability assessment, adaptive application controls
- Defender for Servers P2: P1 + JIT VM access, File Integrity Monitoring (FIM), 500 GB/month free Log Analytics data
- Defender for SQL: Advanced Threat Protection + vulnerability assessment for Azure SQL and SQL on VMs
- Defender for Storage: Malware scanning on upload, anomalous access detection, sensitive data discovery
- Defender for Containers: AKS runtime threat detection, ACR image vulnerability scanning, Kubernetes hardening

Defender for Cloud — Key Capabilities

Capability	What It Does
Security Recommendations	Prioritized list of configuration actions to improve Secure Score — each with affected resources, remediation steps, and impact score
Security Alerts	Real-time threat detection linked to MITRE ATT&CK tactic/technique — VM

Capability	What It Does
Attack Path Analysis	Visualizes how an attacker could chain exposed resources to reach sensitive data — prioritizes critical remediation
Workflow Automation	Logic Apps triggered by specific alert type or recommendation severity — auto-open ITSM ticket, send Teams alert, trigger remediation
Cloud Security Explorer	Graph-based query of resource relationships and security posture — find 'internet-exposed VMs with critical vulnerabilities'

Microsoft Sentinel — SIEM + SOAR

- Built on Log Analytics Workspace: All ingested data stored as tables — queried with KQL (Kusto Query Language)
- Data Connectors: 300+ built-in connectors — Microsoft 365 Defender, Azure Activity, AWS CloudTrail, Syslog, CEF, REST API
- Analytics Rules: Scheduled KQL queries (run every X minutes, look back Y time window) that create Incidents on match. Also Near-Real-Time (NRT) rules for sub-minute detection
- Fusion: ML-based multi-signal correlation — combines low-fidelity anomalies across products into high-confidence multi-stage attack incidents to reduce alert fatigue
- UEBA: Baseline normal user/entity behavior — anomaly scoring enriches incidents with peer group comparisons and entity timelines
- Playbooks (SOAR): Azure Logic Apps triggered by incidents or alerts — auto-respond: isolate VM via MDE, create ServiceNow ticket, post Teams card, block IP in firewall
- Threat Hunting: Proactive KQL queries against raw telemetry before alerts

Stage	Activity	Sentinel Feature
Detect	Analytics rule fires on KQL query match or Microsoft incident creation	Scheduled / NRT Analytics Rules
Triage	Analyst reviews incident — entities (IPs, users, hosts), timeline, MITRE mapping, evidence	Incident page, entity pages, UEBA enrichment
Investigate	Explore entity relationships, pivot to raw logs, run ad-hoc KQL hunting queries	Investigation graph, Log Analytics, Hunting
Respond	Auto-remediation via playbook or manual analyst action — contain, eradicate, recover	Playbooks (Logic Apps), manual analyst tasks
Close	Classify (True Positive / False Positive / Benign) and close — feeds ML learning loop	Incident close with classification and comment

Azure Policy & Security Governance

- Azure Policy: Define, assign, and enforce organizational rules over Azure resources — effects: Audit, Deny, DeployIfNotExists, Modify, Append
- Policy Initiatives (Policy Sets): Group related policies applied together — Azure Security Benchmark initiative applies 200+ security policies at once
- Scope: Management Group → Subscription → Resource Group → Resource — policies inherit downward, exclusions can be added at any level
- Deny effect: Blocks non-compliant resource creation/update at deployment

Azure Monitor & Diagnostic Logging

- Diagnostic Settings: Configure each Azure resource to export Activity Logs and Resource Logs to Log Analytics Workspace, Storage Account, Event Hub, or Partner solution
- Activity Log: Subscription-level control plane events — who created/deleted/modified resources, role assignments, policy changes — 90-day default retention
- Resource Logs (formerly Diagnostic Logs): Data plane logs within a service — Key Vault access logs, NSG flow logs, SQL audit logs, Storage transaction logs
- Log Analytics Workspace: Central log aggregation — used by both Defender for Cloud and Sentinel for KQL querying
- Azure Monitor Alerts: Metric threshold alerts and scheduled log query alerts — send to Action Groups (email, SMS, webhook, ITSM, Logic App, Automation Runbook)

Brakto