Azure Complete Reference

Azure Complete Reference — All Topics

Generated April 23, 2026

PART 1: NETWORKING

Topic 1: Virtual Network (VNet)

A Virtual Network is a logically isolated network in Azure. Similar to a physical network in an on-prem data center, but virtual.

Key Properties: - **Region-bound** — lives in one Azure region. Cannot span regions. Use VNet peering for cross-region. - **Subscription-bound** — belongs to one subscription. Can have multiple VNets in one subscription. - **Address Space** — defined using CIDR notation. Can add multiple address spaces (e.g., 10.0.0.0/16 + 192.168.0.0/16). - **Cannot overlap** — if you peer VNets or connect to on-prem, address spaces must not overlap.

CIDR Reference:

CIDR	Total IPs	Usable (Azure reserves 5)
/29	8	3
/28	16	11
/27	32	27
/26	64	59
/25	128	123
/24	256	251
/22	1,024	1,019
/20	4,096	4,091
/16	65,536	65,531
/8	16,777,216	16,777,211

Azure reserves 5 IPs per subnet: 1. Network address (first) 2. Default gateway (second) 3. Azure DNS mapping (third) 4. Azure internal services (fourth) 5. Broadcast (last)

Subnets: - A subnet is a segment of the VNet’s address space - Must be within VNet address space, cannot overlap with other subnets - Practical minimum: /27 (27 usable IPs) - By default, all subnets in a VNet can communicate with each other

Special Subnets:

Name	Purpose	Rules
GatewaySubnet	VPN/ExpressRoute Gateway	Must be named exactly this. Min /27. No other resources.

Name	Purpose	Rules
AzureBastionSubnet	Azure Bastion	Must be named exactly this. Min /26. No other resources.
Delegated subnet	App Service, SQL MI, etc.	Delegated to a specific service type.

Default Traffic Behavior (no NSGs):

Traffic	Default
VM to VM in same subnet	Allowed
VM to VM in different subnet (same VNet)	Allowed
VM to Internet	Allowed (outbound)
Internet to VM	Blocked (unless public IP)
VM to On-prem	Not possible
VM to Other VNet	Not possible

Common Mistakes: - Using 10.0.0.0/16 everywhere — overlap when peering or connecting on-prem - Making subnets too small — run out of IPs quickly - Not reserving GatewaySubnet and AzureBastionSubnet upfront - Changing address space after deployment — disruptive

---

Topic 2: Network Security Groups (NSG)

An NSG is a firewall at the subnet or NIC level. Contains inbound and outbound rules that allow or deny traffic.

Rule Properties:

Property	Description
Priority	100-4096, lower = evaluated first
Direction	Inbound or Outbound
Action	Allow or Deny
Source	IP, CIDR, Service Tag, ASG
Source Port	Port range or *
Destination	IP, CIDR, Service Tag, ASG
Destination Port	Port range
Protocol	TCP, UDP, ICMP, Any
Name	Unique identifier

Evaluation: Lowest priority number first. First match wins — processing stops.

Default Rules (cannot delete):

Inbound: | Priority | Action | Source | |———-|———-|———-| | 65000 | Allow | VNet | | 65001 | Allow | AzureLoadBalancer | | 65500 | Deny | Any |

Outbound: | Priority | Action | Destination | |———-|———-|————-| | 65000 | Allow | VNet | | 65001 | Allow | Internet | | 65500 | Deny | Any |

Where NSGs Attach: 1. **Subnet** (recommended) — applies to ALL resources in that subnet 2. **NIC** — applies to one VM only, use for exceptions 3. **Both** — effective rules = combined. Inbound: NIC first then subnet. Outbound: subnet first then NIC. If either denies, denied.

Source/Destination Options:

Option	Example	When to Use
IP/CIDR	10.0.1.0/24	Specific range
Service Tag	Internet, VirtualNetwork, Storage, Sql	Predefined service IPs
ASG	asg-web, asg-db	Logical VM grouping
Any	*	All

Key Service Tags:

Tag	Represents
VirtualNetwork	All IPs in your VNet + peered VNets
Internet	Everything outside Azure publicly
AzureLoadBalancer	Azure infrastructure health probes
Storage	Azure Storage public IPs
Sql	Azure SQL public IPs
AzureCloud	All Azure datacenter IPs (broad)

Application Security Groups (ASGs): - Group VMs by role (asg-web, asg-app, asg-db) - Reference ASG in NSG rule instead of individual IPs - One rule covers all VMs in the ASG - Add/remove VMs from ASG without changing NSG rules

3-Tier NSG Example:

Frontend NSG: Allow 80/443 from Any, Allow 22 from admin-IP Backend NSG: Allow 8080 from asg-web only, Allow 22 from admin-IP Database NSG: Allow 3306 from asg-app only, Allow 22 from admin-IP

Limits: 300 rules per NSG, 1 NSG per subnet, 1 NSG per NIC.

Common Mistakes: - Leaving SSH/RDP open to 0.0.0.0/0 - Forgetting outbound rules (default allows internet) - Mixing subnet + NIC NSGs without clear strategy - Hardcoding IPs instead of using ASGs - Not leaving priority gaps (use 100, 110, 120 — not 100, 101, 102)

Topic 3: Azure Load Balancer

Distributes incoming network traffic across multiple backend VMs. Ensures no single VM is overwhelmed.

Types:

Type	SKU	Layer	When to Use
Public Load Balancer	Basic/Standard	Layer 4 (TCP/UDP)	Distribute internet traffic to VMs
Internal Load Balancer	Basic/Standard	Layer 4 (TCP/UDP)	Distribute traffic internally between tiers

Basic vs Standard SKU:

Feature	Basic	Standard
Backend pool size	100	1,000
Health probes	Yes	Yes (more options)
Availability Zones	No	Yes (zone-redundant)
Outbound SNAT	Yes	Yes (more control)
HTTPS probing	No	Yes
SLA	None	99.99%
Cost	Free	~$18/month
Security	Open by default	Closed by default (NSG required)

Always use Standard SKU for production. Basic is being deprecated.

Key Components:

Component	What it Does
Frontend IP	Public or private IP that receives traffic
Backend Pool	Set of VMs or NICs that receive distributed traffic
Health Probes	Check if backend VMs are healthy. Unhealthy VMs removed from rotation.
Load Balancing Rules	Define how traffic is distributed (port, protocol, algorithm)
Inbound NAT Rules	Forward specific port traffic to a specific VM

Health Probes:

Property	Description
Protocol	TCP, HTTP, or HTTPS
Port	Port to probe (e.g., 80)
Interval	How often to probe (default 5 sec)
Unhealthy threshold	Consecutive failures before marking unhealthy (default 2)
Request path	For HTTP/HTTPS probes (e.g., /health)

Load Distribution Methods:

Method	How it Works
Round-robin (default)	Distribute evenly across all healthy VMs
Source IP affinity	Same client IP always goes to same backend VM

HA Ports: Load balance ALL ports. Use case: NVAs. Only on Internal Standard LB.

Topic 4: Azure Application Gateway

Application-level (Layer 7) load balancer with WAF, SSL termination, URL-based routing.

When to use Application Gateway instead of Load Balancer:

Need	Use
Layer 4 (TCP/UDP) distribution only	Azure Load Balancer
Layer 7 (HTTP/HTTPS) routing	Application Gateway
SSL termination	Application Gateway
URL-based routing	Application Gateway
WAF	Application Gateway
Cookie-based session affinity	Application Gateway

SKUs:

SKU	Features
Standard_v2	Auto-scale, zone-redundant, no WAF
WAF_v2	Same as Standard_v2 + WAF (OWASP protection)

Key Components:

Component	What it Does
Frontend IP	Public and/or private IP for incoming traffic
Listeners	Listen on specific port/protocol/hostname
Routing Rules	Map listener to backend pool with path-based rules
Backend Pools	Target VMs, App Service, IP addresses
HTTP Settings	Port, protocol, cookie affinity, connection draining, health probe
Health Probes	Check backend health (HTTP/HTTPS, custom path)
SSL Certificate	For SSL termination at the gateway

SSL Termination: - Client sends HTTPS to App Gateway - App Gateway decrypts using its certificate - App Gateway sends HTTP or HTTPS to backend VMs - Can also re-encrypt: decrypt at gateway, re-encrypt to backend (end-to-end SSL)

Multi-Site Hosting: - One App Gateway can serve multiple websites - Listener 1: www.shop.com to shop-pool - Listener 2: www.blog.com to blog-pool

WAF Modes: | Mode | Behavior | |——|———| | Detection | Logs violations, lets traffic through | | Prevention | Blocks violations (returns 403), logs them |

Topic 5: Azure Firewall

Fully managed, cloud-native firewall service. Inspects all outbound and inbound traffic at the network level.

Azure Firewall vs NSG:

Feature	NSG	Azure Firewall
Layer	Layer 3/4	Layer 3/4/7
Filtering	IP, port, protocol	IP, port, protocol, FQDN, application
Stateful	No	Yes
FQDN filtering	No	Yes
Threat intelligence	No	Yes

Feature	NSG	Azure Firewall
DNAT	No	Yes
Cost	Free	~$500/month + per-GB
Centralization	Per subnet	Centralized for all VNets

SKUs:

SKU	Features	Cost
Basic	Simplified, small businesses	~$150/month
Standard	FQDN filtering, DNAT, threat intel	~$500/month
Premium	Standard + TLS inspection, IDPS, URL filtering	~$900/month

Deployment: - Requires dedicated subnet named AzureFirewallSubnet (min /26) - Typically in hub VNet of hub-spoke topology - All spoke VNets route traffic through firewall using UDRs

Firewall Rules:

Type	What it Filters
NAT rules	DNAT — translate inbound traffic to internal IPs
Network rules	IP/port/protocol — allow/deny network traffic
Application rules	FQDN/URL — allow/deny outbound to specific domains

Evaluation order: NAT rules, then Network rules, then Application rules. First match wins.

Topic 6: VNet Peering

Connects two VNets so they can communicate privately over the Azure backbone.

Key Properties: - **Non-transitive** — if A peers with B, and B peers with C, A cannot reach C through B - **Cross-region** — Global VNet Peering connects VNets in different regions - **Cross-subscription** — VNets in different subscriptions can be peered - **No downtime** — peering is created without affecting resources

Peering Configuration Options:

Setting	When to Enable
Allow virtual network access	Always yes
Allow forwarded traffic	Yes if firewall/NVA routes traffic
Allow gateway transit	Yes if hub has gateway, spokes need on-prem access
Use remote gateways	Yes for spoke VNets that need hub's gateway

Cost:

Traffic Type	Cost per GB
Same region peering	Free
Cross-region peering	~$0.01/GB both directions

Hub-Spoke Pattern: - Hub peers with each spoke - Spokes do NOT peer with each other - Spoke-to-spoke traffic goes through hub firewall - All spokes use hub's gateway for on-prem connectivity (gateway transit)

Common Mistakes: - Forgetting peering is non-transitive - Not enabling gateway transit on hub - Overlapping IP address spaces

---

Topic 7: ExpressRoute

Private, dedicated connection from on-premises to Azure. Does NOT go over the public internet.

ExpressRoute vs VPN Gateway:

Feature	VPN Gateway	ExpressRoute
Connection	Internet (IPsec)	Private (through provider)
Bandwidth	Up to 10 Gbps	Up to 100 Gbps
Latency	Variable	Low, consistent (<10ms)
Cost	~$150-500/month	~$1,000-5,000/month
Setup time	Minutes	Weeks
Use case	Low bandwidth, non-critical	High bandwidth, latency-sensitive

Peering Types:

Peering	What it Connects To
Private Peering	Azure VNets (IaaS VMs)
Microsoft Peering	Azure PaaS (M365, Azure SQL, Storage)

Gateway SKUs:

SKU	Bandwidth	Cost/month
ErGw1AZ	1 Gbps	~$300
ErGw2AZ	2 Gbps	~$600
ErGw3AZ	10 Gbps	~$1,500

Global Reach: Connect two ExpressRoute circuits together across regions.

FastPath: Bypasses gateway for data plane traffic. Improves performance.

Topic 8: VPN Gateway

Encrypted IPsec/IKE tunnel between on-prem and Azure over the public internet.

Types:

Type	What it Does
Site-to-Site (S2S)	Connect on-prem network to Azure VNet
Point-to-Site (P2S)	Connect individual clients to Azure VNet
VNet-to-VNet	Connect two Azure VNets via IPsec

VPN Gateway SKUs:

SKU	S2S Tunnels	Bandwidth	Cost/month
VpnGw1	10	650 Mbps	~$140

SKU	S2S Tunnels	Bandwidth	Cost/month
VpnGw2	10	1 Gbps	~$370
VpnGw3	30	1.25 Gbps	~$900
VpnGw5	30	5 Gbps	~$2,800

BGP with VPN Gateway: Dynamic route exchange between Azure and on-prem. Routes learned automatically.

P2S Authentication: Certificate, RADIUS, or Entra ID.

Best practice: ExpressRoute primary + VPN Gateway as backup.

Topic 9: Azure Bastion

Secure RDP/SSH access to VMs over TLS (port 443) from the Azure Portal.

Why Bastion instead of public RDP/SSH: - No public IP needed on VMs - No open port 22/3389 on NSG - All traffic stays inside Azure backbone - Audited, logged

SKUs:

SKU	Features	Cost
Basic	RDP/SSH, 2 concurrent sessions	~$140/month
Standard	More sessions, shareable links	~$140/month+
Premium	Private-only connect, Kerberos	Higher

Topic 10: User Defined Routes (UDR) / Route Tables

Custom routing rules that override Azure's default routing.

Route Properties:

Property	What it Means
Address prefix	Destination CIDR
Next hop type	VirtualAppliance, VirtualNetworkGateway, Internet, None, VNetLocal
Next hop IP	IP of firewall/NVA (when next hop = VirtualAppliance)

Common UDR Patterns:

Destination	Next Hop	Purpose
0.0.0.0/0	VirtualAppliance (firewall IP)	Force all internet traffic through firewall
192.168.0.0/16	VirtualNetworkGateway	Route on-prem traffic through gateway
10.99.0.0/16	None	Blackhole (drop) traffic

Topic 11: Azure DNS

Two services:

Service	What it Does
Azure DNS (Public)	Host public DNS zones
Azure Private DNS	Host private DNS zones, resolve only within VNets

Private DNS: - Auto-registration: VMs automatically get DNS records - Critical for Private Endpoints

Record Types: A, AAAA, CNAME, MX, NS, PTR, SOA, SRV, TXT

Alias Records: Point to Azure resources. Auto-update if resource IP changes.

Topic 12: Private Link and Private Endpoints

Access Azure PaaS services over a private IP address inside your VNet.

Service Endpoints vs Private Endpoints:

Feature	Service Endpoint	Private Endpoint
IP type	Public (Azure backbone)	Private (in your VNet)
Access from on-prem	No	Yes
Access from peered VNets	No	Yes
Per-resource granularity	No	Yes
Cost	Free	~$7/month per endpoint

Always prefer Private Endpoints for production.

Topic 13: Azure Front Door

Global HTTP/HTTPS load balancer with CDN, WAF, and SSL termination.

Front Door vs Application Gateway vs Traffic Manager:

Feature	Front Door	App Gateway	Traffic Manager
Layer	Layer 7	Layer 7	Layer 3 (DNS)
Scope	Global	Regional	Global
SSL termination	Yes	Yes	No
WAF	Yes	Yes	No
Failover speed	Seconds	N/A	30-120 sec (DNS TTL)
CDN	Built-in	No	No

Topic 14: Azure DDoS Protection

SKU	Cost	What it Protects
Basic	Free	Azure infrastructure
Standard	~$2,944/month	Your specific VNets and resources

Standard includes: adaptive tuning, metrics, alerts, rapid response, cost protection.

Topic 15: Network Watcher

Network monitoring and diagnostic service.

Key Features:

Feature	When to Use
IP Flow Verify	“Why can’t VM1 reach VM2?”
Next Hop	“Where is this traffic going?”
NSG Flow Logs	Security auditing, compliance
Connection Troubleshoot	“Can VM1 reach the database?”
Packet Capture	Deep network troubleshooting
Topology	Visual map of network

Traffic Analytics: Process NSG flow logs to show top talkers, traffic patterns, visualization.

Topic 16: Azure Virtual WAN

Unified networking for global connectivity. For 10+ branch offices.

Types: Basic (S2S + P2S only), Standard (everything including ExpressRoute).

Key benefit: Transit routing built-in. Branch-to-branch automatic. Single pane of glass.

Topic 17: Azure Route Server

Simplifies dynamic routing between NVAs and Azure VNets. BGP-based. Free.

Topic 18: Service Endpoints (Legacy)

Brings Azure service traffic onto Azure backbone. Less secure than Private Endpoints. Free. Prefer Private Endpoints.

Topic 19: Azure NAT Gateway

Managed outbound NAT. Stable, predictable outbound IPs. ~$32/month + per-GB.

When to use: VMs need stable outbound IP for whitelisting, or high outbound connection volume.

Topic 20: Network Virtual Appliances (NVAs)

Third-party firewalls as VMs (Palo Alto, Fortinet, Cisco). Use when you need vendor-specific features Azure Firewall doesn’t offer.

PART 2: COMPUTE

Topic 21: Virtual Machines

VM Families:

Family	Optimized For	Use Case
B	Burstable, low cost	Dev/test, low-traffic
D	General purpose	Web/app servers
E	Memory optimized	In-memory databases
F	Compute optimized	Batch, gaming
L	Storage optimized	Big data
N	GPU	ML, rendering
H	HPC	Simulation
M	Memory extreme	SAP HANA

VM Naming Convention: D4s_v5 = D (family) + 4 (vCPU) + s (premium storage) + v5 (generation)

VM Disk Types:

Disk Type	IOPS	Throughput	Cost (1TB/month)	Use Case
Standard HDD	~500	~60 MB/s	~$20	Backup
Standard SSD	~6,000	~300 MB/s	~$50	Web servers
Premium SSD	~7,500	~250 MB/s	~$125	Production
Premium SSD v2	~80,000	~1,200 MB/s	~$80+	High-perf DB
Ultra Disk	~160,000	~2,000 MB/s	~$140+	Mission-critical DB

Availability Options:

Option	SLA	Cost
Single VM (premium disk)	99.9%	Base
Availability Set	99.95%	No extra
Availability Zone	99.99%	No extra
VM Scale Sets	99.95%+	No extra

Availability Set Domains: - Fault Domain: different physical rack (max 3) - Update Domain: different maintenance schedule (max 20)

VMSS Autoscale Rules: - CPU > 75% for 5 min → add 1 VM - CPU < 25% for 10 min → remove 1 VM - Schedule-based: min 3 at 8 AM, min 1 at 8 PM

Custom VM Images: Generalize VM, capture as managed image, deploy from image.

Shared Image Gallery: Share images across subscriptions, regions, tenants. Versioning support.

Topic 22: Azure App Service

Fully managed PaaS for web apps, REST APIs, mobile backends.

App Service Plan Tiers:

Tier	Auto-Scale	Deployment Slots	Cost/month
Free (F1)	No	No	Free
Basic (B1)	No	No	~$13
Standard (S1)	Yes	5	~$70
Premium (P1v3)	Yes	20	~$140

Deployment Slots: Deploy to staging, test, swap to production. Zero downtime. Standard tier+.

VNet Integration: App can access VNet resources (outbound). Private Endpoints for inbound.

App Service for Containers: Deploy containerized apps. Linux containers. Standard tier+.

Topic 23: Azure Container Apps

Serverless container platform. Scale to zero. KEDA-based autoscaling. Built-in Dapr.

Why Container Apps: Containers without managing Kubernetes. Pay per vCPU-second. Scale to zero = no cost when idle.

Topic 24: Azure Kubernetes Service (AKS)

Managed Kubernetes. Microsoft manages control plane (free). You manage node pools (paid).

Networking: kubenet (simple) or Azure CNI (advanced, pods get VNet IPs).

Security: Entra ID integration, private cluster, network policies, workload identity, Key Vault CSI.

Add-ons: Monitor, Policy, Ingress controller, Key Vault provider, Dapr, Open Service Mesh.

Topic 25: Azure Container Instances (ACI)

Run containers without VMs. Fastest way. Good for one-off tasks, prototyping. Not for long-running production.

Topic 26: Azure VMware Solution (AVS)

Run VMware workloads natively on Azure. HCX migration. NSX-T networking. ~$8K-12K/month per host (3 minimum).

Topic 27: Azure Functions

Serverless event-driven compute. Pay per execution. Triggers: HTTP, Timer, Blob, Queue, Service Bus, Event Grid, Cosmos DB.

Hosting Plans: - Consumption: auto-scale, scale to zero, cold start - Premium: pre-warmed, no cold start, VNet integration - Dedicated: on your App Service plan

---

Topic 28: Azure Batch

Run large-scale parallel and HPC workloads. Manage hundreds of VMs for batch processing.

PART 3: STORAGE

Topic 29: Azure Storage Accounts

Foundational storage service. General-purpose v2 is the default.

Replication Options:

Option	What it Does	RPO
LRS	3 copies in single DC	0
ZRS	3 copies across 3 AZs	0
GRS	LRS + async to paired region	~15 min
GZRS	ZRS + async to paired region	~15 min

Always use ZRS or GZRS for production.

Access Tiers (Blob):

Tier	Storage Cost	Retrieval Cost	Min Duration
Hot	Highest	Lowest	None
Cool	Lower	Higher	30 days
Cold	Very low	Very high	90 days
Archive	Lowest	Highest	180 days

Lifecycle Management: Automatically move blobs between tiers based on rules.

Access Keys: 2 keys per account. Never use in apps. Use SAS or Entra ID instead.

SAS (Shared Access Signatures): Limited, time-bound access. User Delegation SAS (Entra ID) is most secure.

Topic 30: Azure Blob Storage

Object storage. Block Blob (files), Append Blob (logs), Page Blob (VHDs).

Soft Delete: Deleted blobs retained 1-365 days. Recoverable.

Versioning: Every write creates a new version. Restore any previous version.

Immutable Storage (WORM): Time-based retention or legal hold. Data cannot be modified/deleted. For compliance.

Topic 31: Azure Files

Managed file shares via SMB/NFS. Replace on-prem file servers.

Azure File Sync: Sync on-prem file shares with Azure Files. Cloud tiering for hot/cold.

Topic 32: Azure Managed Disks

Block storage for VMs. Azure manages storage accounts.

Disk Encryption: - SSE (Storage Side Encryption): always on, platform-managed keys - SSE + CMK: customer-managed keys in Key Vault - ADE (Azure Disk Encryption): OS-level (BitLocker/DM-Crypt). Legacy — prefer SSE+CMK.

Shared Disks: Some Premium SSDs shared across VMs. For clustered databases (SQL Server FCI, Oracle RAC).

Topic 33: Azure Data Lake Storage

Built on Blob Storage. Hierarchical namespace for analytics. True directories, POSIX ACLs. Enable at creation time (cannot add later).

PART 4: IDENTITY AND ACCESS

Topic 34: Microsoft Entra ID

Cloud identity and access management.

Editions:

Edition	Cost	Key Features
Free	Free	SSO, basic MFA
P1	~$6/user/month	Conditional Access, PIM, dynamic groups
P2	~$9/user/month	P1 + Identity Protection, Access Reviews

Users: Cloud-only, synced (from on-prem via Connect), guest (B2B).

Groups: Assigned (manual), Dynamic user (rule-based), Dynamic device. P1 required for dynamic.

App Registrations: Register apps, define API permissions, get client ID/secret.

Enterprise Applications: Deployed app instances. User assignment. SSO configuration.

Topic 35: Entra Connect (Hybrid Identity)

Authentication Methods:

Method	How it Works	Recommendation
Password Hash Sync (PHS)	Password hash synced to cloud. Auth in cloud.	Recommended — simplest, most resilient
Pass-through Auth (PTA)	Auth forwarded to on-prem agent	If no password hash in cloud

Method	How it Works	Recommendation
Federation (AD FS)	All auth via on-prem AD FS	Complex scenarios only

---

Topic 36: Role-Based Access Control (RBAC)

Role Assignment = Security Principal + Role Definition + Scope

Key Built-in Roles:

Role	What it Allows
Owner	Full access + delegate access
Contributor	Full access, no delegation
Reader	Read-only
Virtual Machine Contributor	Manage VMs
Network Contributor	Manage networking
User Access Administrator	Manage RBAC

Scope Hierarchy: Management Group > Subscription > Resource Group > Resource

RBAC is additive. Custom roles via JSON definition.

Topic 37: Privileged Identity Management (PIM)

Just-in-time privileged access. No permanent admin roles.

Key Concepts: Eligible assignment (can activate), Active assignment (has role now), Activation (request with MFA + approval + justification), Max duration, Access Reviews.

Best Practices: - All privileged roles should be eligible, not permanently active - Require MFA for every activation - Require approval for high-privilege roles - Quarterly access reviews - P2 license required

---

Topic 38: Conditional Access

If-then policies for access control.

Conditions: Users/groups, cloud apps, client apps, device platform, location, sign-in risk, user risk.

Controls: Block, Grant (with MFA, compliant device, etc.), Session (sign-in frequency, app restrictions).

Common Policies: - Require MFA for all users - Block legacy authentication - Require compliant device for M365 - MFA for risky sign-ins - Block untrusted countries

Best Practice: Start in report-only mode. Exclude break-glass accounts.

Topic 39: Managed Identities

Azure resources authenticate to other services without stored credentials.

Types: - System-assigned: tied to one resource. Deleted with resource. - User-assigned: standalone. Assigned to multiple resources.

How it works: VM calls IMDS endpoint, gets access token, authenticates to Azure service. No credentials in code or config.

PART 5: DATABASE

Topic 40: Azure SQL Database

Managed SQL Server. PaaS.

Deployment Options: Single database, Elastic pool, SQL Managed Instance.

Purchasing Models: DTU (simple) or vCore (flexible).

vCore Tiers: General Purpose (most workloads), Business Critical (high IOPS), Hyperscale (10TB+).

Compute Tiers: Provisioned (always-on) or Serverless (auto-scale, scale to zero).

HA/DR: Zone-redundant, active geo-replication, auto-failover groups, PITR (7-35 days), LTR (up to 10 years).

Security: Firewall, VNet rules, Private Endpoint, Entra ID auth, Always Encrypted, TDE.

Topic 41: Azure Database for PostgreSQL

Managed PostgreSQL. Flexible Server is current deployment option.

Tiers: Burstable, General Purpose, Memory Optimized. Zone-redundant HA available.

Topic 42: Azure Database for MySQL

Same pattern as PostgreSQL Flexible Server.

Topic 43: Azure Cosmos DB

Globally distributed, multi-model NoSQL.

Consistency Levels: Strong, Bounded staleness, Session (default), Consistent prefix, Eventual.

APIs: NoSQL (native), MongoDB, PostgreSQL, Cassandra, Gremlin, Table.

Unique Features: Multi-region writes, automatic indexing, serverless, autoscale, change feed, TTL.

PART 6: MONITORING

Topic 44: Azure Monitor

Unified monitoring. Metrics (numeric), Logs (KQL), Traces (distributed).

Components: Metrics, Log Analytics, Alerts, Dashboards, Workbooks, Application Insights.

Log Analytics Workspace: Central log repository. KQL queries. 30-day default retention, up to 2 years.

Diagnostic Settings: Configure each resource to send logs/metrics to Log Analytics, Storage, or Event Hub.

Topic 45: Azure Alerts

Types: Metric alert, Log search alert, Activity log alert, Smart alert.

Components: Alert rule, Action group (email, SMS, webhook, Function, Logic App), Alert processing rule.

Severity: Sev0 (Critical) to Sev4 (Verbose).

Topic 46: Application Insights

APM for web apps. Tracks request rate, response time, failure rate, dependencies, exceptions, page load, user behavior.

Live Metrics Stream (real-time). Application Map (visual dependency graph).

PART 7: BACKUP AND DR

Topic 47: Azure Backup

What can be backed up: Azure VMs, SQL on VMs, Azure Files, Azure Blob, Azure SQL, SAP HANA, on-prem files (MARS agent), VMware (MABS).

Recovery Services Vault: Container for backup data. LRS or GRS. Soft delete enabled by default.

Topic 48: Azure Site Recovery (ASR)

DR as a service. Replicates VMs from primary to secondary region.

Workflow: Enable replication → Initial replication → Delta replication → Test failover → Failover → Commit → Reprotect → Failback.

Multi-VM Consistency: Group VMs for consistent failover.

Cost: ~$25/month per protected VM + storage/egress.

PART 8: SECURITY

Topic 49: Microsoft Defender for Cloud

CSPM and CWP. Secure Score, recommendations, regulatory compliance, threat detection, JIT VM access.

Defender Plans: Servers (~$15/VM/mo), App Service (~$7/app/mo), SQL (~$15/server/mo), Storage, Key Vault, DNS, Containers.

JIT VM Access: Management ports closed by default. Request access → NSG temporarily opens → auto-closes.

Topic 50: Azure Key Vault

Store secrets, keys, certificates.

Access Models: Vault access policy (legacy) or Azure RBAC (preferred).

Key Vault RBAC Roles: Administrator, Secrets User, Secrets Officer, Crypto User, Crypto Officer, Certificate User, Certificate Officer.

Security: Soft delete (90 days, on by default), Purge protection, Firewall, Private Endpoint, Diagnostic logging.

Managed HSM: FIPS 140-2 Level 3. ~$2,160/month. Dedicated single-tenant.

Key Rotation: Auto-rotate on schedule. Applications use latest version.

Topic 51: Microsoft Sentinel

Cloud-native SIEM and SOAR.

Components: Data connectors, Analytics rules, Incidents, Workbooks, Playbooks (SOAR), Hunting queries, Watchlists, Threat intelligence.

Analytics Rule Types: Scheduled, NRT, Microsoft security, Fusion (ML-based).

Playbooks: Logic Apps triggered by incidents. Auto-block IPs, create tickets, notify teams.

Cost: ~$2.46/GB ingested. First 5GB/day free with Defender plan.

Topic 52: Zero Trust Architecture

“Never trust, always verify.”

Principles: Verify explicitly, Use least privilege, Assume breach.

Implementation by Pillar:

Pillar	Services
Identity	Entra ID, Conditional Access, PIM, MFA

Pillar	Services
Endpoints	Intune, Compliance policies, SharePoint.

PART 20: IoT

Topic 86: Azure IoT Hub

Managed IoT connectivity. Millions of devices. MQTT/AMQP/HTTPS. Per-device auth. Device twins. Cloud-to-device messages.

Tiers: Free (8K msgs/day), B1/S1 (400K-8M), B2/S2 (6M-120M), S3 (300M-2B).

Device Provisioning Service (DPS): Zero-touch provisioning at scale. TPM, X.509, symmetric key.

Topic 87: Azure IoT Operations

New edge IoT platform on Azure Arc. MQTT broker, data flows, asset management. Runs Kubernetes at the edge. Managed from Azure.

Topic 88: Azure Digital Twins

Model physical environments. Twins with properties and relationships. Ingest IoT data, query model, trigger actions. Smart buildings, cities, manufacturing.

Topic 89: Azure Stream Analytics

Real-time stream processing. SQL-like queries on streaming data. Input from Event Hubs/IoT Hub. Output to SQL/Power BI/Functions. Tumbling/hopping/sliding windows.

Topic 90: Azure Databricks

Apache Spark analytics platform. Collaborative notebooks. Auto-scaling clusters. Delta Lake built-in. Integration with ADLS, Key Vault, Synapse.

Topic 91: Azure Machine Learning

End-to-end ML platform. Workspace, Compute, Pipelines, Models, Endpoints, AutoML, MLflow.

Deployment: Managed online endpoint (real-time), Batch endpoint (periodic), Kubernetes (AKS).

Architect role: Design secure infrastructure (Private Endpoint, VNet, Key Vault, API Management), not build models.

PART 21: DATA GOVERNANCE

Topic 92: Microsoft Purview

Data governance and compliance. Data Map (auto-scan), Data Catalog (searchable), Classification (auto-classify sensitive data), Information Protection (sensitivity labels), Audit (unified log), Compliance Manager (score against frameworks).

PART 22: COMPLIANCE DEEP DIVE

Topic 93: Defender for Cloud Regulatory Compliance

Microsoft maps regulatory controls to Azure Policy. Evaluate resources. Get compliance score. Remediate failed controls. Supported: HIPAA/HITRUST, ISO 27001, SOC 2, PCI DSS, NIST 800-53, CIS, FedRAMP, CMMC, and custom.

Continuous Export to Log Analytics, Event Hub, Power BI.

PART 23: NETWORKING REFERENCE

Topic 94: Azure Service Tags

IP prefixes for Azure services. Use in NSGs and Firewall rules. Microsoft auto-updates ranges.

Key Tags: VirtualNetwork, Internet, AzureLoadBalancer, Storage, Sql, AzureKeyVault, AzureContainerRegistry, MicrosoftCloud, AzureActiveDirectory, AppService, EventHub, ServiceBus, AzureMonitor, AzureResourceManager, GuestAndHybridManagement.

Topic 95: Azure Resource Mover

Move resources between regions. Replicate VMs, recreate VNets/NSGs/LBs/Public IPs. For relocating workloads to closer regions.

PART 24: DEVELOPER TOOLS

Topic 96: Azure DevTest Labs

Self-service VM environments for developers. Custom images, formulas, artifacts, policies (max VMs, allowed sizes, auto-shutdown), cost tracking, claimable VMs.

PART 25: ADVANCED COMPUTE

Topic 97: Azure App Service Environment (ASE)

Isolated App Service in your VNet. Dedicated infrastructure. Max 100+ instances. Internal or External LB. ~$1K-3K/month. For compliance requiring isolation or >30 instances.

Topic 98: Azure Red Hat OpenShift (ARO)

Managed OpenShift. Jointly managed by Microsoft + Red Hat. Built-in registry, CI/CD, monitoring. For Red Hat shops wanting consistency with on-prem OpenShift. More expensive than AKS.

PART 26: HYBRID

Topic 99: Azure Stack

Portfolio: - Azure Stack HCI: Hyper-converged on your hardware. Run VMs and AKS on-prem. Azure Arc managed. - Azure Stack Hub: Integrated system. Run Azure IaaS + some PaaS on-prem. Connected or disconnected. - Azure Stack Edge: Ruggedized edge device. Run compute + ML at the edge. Factory floor, retail, oil rigs.

PART 27: SECURITY OPERATIONS

Topic 100: Azure Customer Lockbox

Control Microsoft engineer access to your data during support. Engineer requests access, you approve/deny. Time-limited, audited. Free but requires Premier/Unified support.

PART 28: SOVEREIGN CLOUDS

Topic 101: Azure Sovereign Clouds

Cloud	Who
Azure Commercial	General public
Azure Government	US government agencies
Azure China (21Vianet)	Organizations in China
Azure Secret	US intelligence
Azure Top Secret	US intelligence (highest)

Different endpoint URLs, different compliance, different service availability.

PART 29: LICENSING AND SUPPORT

Topic 102: Azure Programs, Licensing, and Support

Agreements: EA (enterprise, 3-year), MCA (modern, pay-as-you-go), CSP (via partner/MSP).

Azure Hybrid Benefit: Use existing Windows Server/SQL Server licenses with Software Assurance. Save 40-85%.

Free Services: 200+ services have free tiers. 12 months free for new accounts. Always-free: App Service F1, Functions 1M executions, Cosmos DB 400 RU/s + 5GB.

Support Plans:

Plan	Cost	Response
Basic	Free	Self-service
Developer	~$29/mo	Business hours, 1 day
Standard	~$100/mo	24/7, 4 hours (Sev C)
Professional Direct	~$1,000/mo	24/7, 1 hour (Sev A)
Premier/Unified	Custom	24/7, <1 hour (Sev A)

APPENDIX: Decision Frameworks

A. Load Balancer Decision

Need	Choose
Layer 4 TCP/UDP, single region	Azure Load Balancer
Layer 7 HTTP/HTTPS, single region	Application Gateway
Layer 7 HTTP/HTTPS, global	Front Door
DNS-based, any protocol, global	Traffic Manager
Need WAF	App Gateway or Front Door
Need CDN	Front Door
Non-HTTP (database, custom)	Load Balancer or Traffic Manager

B. Compute Decision

Need	Choose
Full control, legacy apps	VMs
Web app, no OS management	App Service
Containers, no Kubernetes	Container Apps
Kubernetes, complex microservices	AKS
One-off task, quick container	ACI
VMware workloads	AVS
Event-driven, serverless	Functions

Need	Choose
Parallel processing, HPC	Batch

C. Database Decision

Need	Choose
Relational, SQL Server compatible	Azure SQL Database
Relational, SQL Server + instance features	SQL Managed Instance
Relational, open source	PostgreSQL Flexible or MySQL Flexible
NoSQL, global scale, multi-model	Cosmos DB
In-memory caching	Azure Cache for Redis

D. Messaging Decision

Need	Choose
Reliable command delivery	Service Bus
Event routing, reactive	Event Grid
High-volume streaming	Event Hubs
Simple queue, low cost	Storage Queue

E. Storage Decision

Need	Choose
Unstructured data (files, images)	Blob Storage
File shares (SMB/NFS)	Azure Files
VM disks	Managed Disks
Analytics, big data	Data Lake Storage
High-performance file shares	NetApp Files

F. Security Decision

Need	Choose
Per-subnet firewall	NSG
Centralized network firewall	Azure Firewall
Web attack protection	WAF (App Gateway or Front Door)
SIEM/SOAR	Microsoft Sentinel
Secret/key/certificate management	Key Vault
Cloud security posture	Defender for Cloud
Privileged access management	PIM
Identity-based access control	Conditional Access

G. IaC Decision

Need	Choose
Azure-only, Microsoft recommended	Bicep

Need	Choose
Multi-cloud	Terraform
Existing ARM templates	ARM JSON (migrate to Bicep)

End of Azure Complete Reference — 102 Topics