**AZ-104 Exam Cram Guide – Part 1 (Identities & Storage)**

**Identities & Governance – Deep Review**

* **Azure AD vs RBAC**: Azure AD roles apply at the tenant directory level (e.g. Global Admin, User Admin). RBAC roles apply to Azure resources (Owner, Contributor, Reader).
* **RBAC Scope Hierarchy**: Management Group > Subscription > Resource Group > Resource. Permissions are inherited downwards.
* **Custom RBAC Roles**: Defined via JSON (actions, notActions, dataActions). Useful for very specific permissions.
* **Privileged Identity Management (PIM)**: Just-in-time role activation, approval workflows, audit history.
* **Resource Locks**: CanNotDelete (can update but not delete), ReadOnly (no delete or updates).
* **Azure Policy**: Enforce compliance (deny deployments, audit, append). Initiatives = multiple policies grouped.
* **Management Groups**: Organize subscriptions hierarchically for RBAC/Policy assignment.
* **Blueprints**: Bundle RBAC assignments, policies, ARM templates for consistent deployment across environments.

**RBAC vs AD Roles – Comparison**

| **Feature** | **Azure AD Roles** | **Azure RBAC Roles** |
| --- | --- | --- |
| Scope | Tenant-wide | Mgmt Group / Subscription / RG / Resource |
| Examples | Global Admin, User Admin | Owner, Contributor, Reader, Storage Blob Data Contributor |
| Purpose | Manage users/groups/directory | Manage Azure resources |

**Identities – Useful Commands**

* PowerShell:  
  New-AzADUser -DisplayName 'testuser1' -UserPrincipalName testuser1@contoso.com -AccountEnabled $true -PasswordProfile (New-Object -TypeName Microsoft.Open.AzureAD.Model.PasswordProfile)
* CLI:  
  az ad user create --display-name testuser1 --user-principal-name testuser1@contoso.com --password MyP@ssword123
* PowerShell:  
  New-AzADGroup -DisplayName 'FinanceTeam' -MailNickname 'FinanceTeam'
* CLI:  
  az role assignment create --assignee --role Reader --scope /subscriptions/

**Storage – Deep Review**

* **Storage Account Types**: General Purpose v2 (most common), Premium SSD (low latency), BlobStorage (legacy).
* **Blob Access Tiers**: Hot (frequent), Cool (30+ days), Archive (180+ days, offline).
* **Replication Options**:
  + LRS = single datacenter
  + ZRS = multiple zones in a region
  + GRS = primary + geo-paired region
  + RA-GRS = GRS + read access to secondary
* **Azure Files**: SMB/NFS shares, mountable. Azure File Sync keeps on-prem servers in sync.
* **SAS**: Temporary, limited access (service SAS, account SAS, user delegation SAS).
* **Soft Delete**: Recover deleted blobs/files for retention period.
* **Lifecycle Management**: Automate tiering/deletion based on age.
* **Encryption**: At-rest encryption by default. Can use CMK from Key Vault.

**Storage Redundancy Options**

| **Type** | **Copies** | **Location** | **Read Secondary?** |
| --- | --- | --- | --- |
| LRS | 3 | Single DC | No |
| ZRS | 3 | Across zones in region | No |
| GRS | 6 | Primary + geo-paired | No |
| RA-GRS | 6 | Primary + geo-paired | Yes |

**Storage – Useful Commands**

* PowerShell:  
  New-AzStorageAccount -ResourceGroupName RG1 -Name mystorageacct -Location 'UK South' -SkuName Standard\_LRS -Kind StorageV2
* CLI:  
  az storage account create -n mystorageacct -g RG1 -l uksouth --sku Standard\_LRS --kind StorageV2
* PowerShell:  
  New-AzStorageShare -Name fileshare1 -Context $ctx
* CLI:  
  az storage share create --name fileshare1 --account-name mystorageacct

**AZ-104 Exam Cram Guide – Part 2 (Compute & Networking)**

**Compute – Deep Review**

* **Availability Options**:
  + Availability Sets: Protect against hardware failures. 2+ fault domains, 5 update domains. SLA ~99.95%.
  + Availability Zones: Physically separate datacenters in a region. SLA ~99.99%.
  + VM Scale Sets (VMSS): Autoscaling identical VMs. Use with Load Balancers.
* **VM Sizes**: General purpose, Compute optimized, Memory optimized, Storage optimized, GPU, High Performance.
* **Disks**: Managed disks (Standard HDD, Standard SSD, Premium SSD, Ultra SSD). Ephemeral OS disks = temporary + fastest.
* **App Service**: PaaS hosting for web apps, autoscale built-in. Supports custom domains and SSL.
* **Containers**:
  + ACI: Fast container hosting, no infra.
  + AKS: Managed Kubernetes, orchestrated.
* **ARM Templates**: Declarative JSON infra as code. Deploy with New-AzResourceGroupDeployment or az deployment group create.

**Availability Comparison**

| **Feature** | **Availability Sets** | **Availability Zones** | **VM Scale Sets** |
| --- | --- | --- | --- |
| Fault Domain Protect | Yes | Yes | Yes |
| Update Domain Protect | Yes | Yes | Yes |
| Region-level Protect | No | Yes | No |
| Autoscaling | No | No | Yes |
| SLA | 99.95% | 99.99% | Varies |

**Compute – Useful Commands**

* PowerShell:  
  New-AzVM -ResourceGroupName RG1 -Name VM1 -Location 'UK South' -Image UbuntuLTS
* CLI:  
  az vm create --resource-group RG1 --name VM1 --image UbuntuLTS --admin-username azureuser --generate-ssh-keys
* PowerShell:  
  New-AzVmss -ResourceGroupName RG1 -VMScaleSetName myVMSS -Location 'UK South'
* CLI:  
  az vmss create --resource-group RG1 --name myVMSS --image UbuntuLTS --upgrade-policy-mode automatic

**Networking – Deep Review**

* **VNets**: Isolated network segments. Subnets divide address space.
* **NSG**: Control inbound/outbound traffic. Rules prioritized 100–4096. Lower number = higher priority.
* **ASG**: Group NICs for simplified NSG rule application.
* **VNet Peering**: Connect VNets. Enable *allow forwarded traffic* for transit. Not transitive by default.
* **VPN Gateway**: Encrypted tunnels between on-prem and Azure.
* **ExpressRoute**: Private connection to Azure datacenters. Premium SKU = global reach. FastPath = lower latency.
* **Load Balancer**: Layer 4, distributes TCP/UDP. Standard LB requires explicit NSG rules.
* **Application Gateway**: Layer 7, URL-based routing, SSL termination, WAF.
* **Traffic Manager**: DNS-based global routing (Priority, Weighted, Performance, Geographic).
* **Azure Firewall**: Stateful, logs traffic, integrates with Threat Intelligence. Premium adds TLS inspection & IDPS.
* **NAT Gateway**: Outbound SNAT for VNets.
* **Private DNS Zones**: Private resolution for PaaS services with Private Link.

**AZ-104 Exam Cram Guide – Part 3 (Monitoring, Backup/DR, Security)**

**Monitoring – Deep Review**

* **Azure Monitor**: Collects metrics (numeric, 1-min) + logs (activity, diagnostic, resource).
* **Log Analytics Workspace**: Stores logs, queried via KQL.
* **Alerts**:
  + Metric alerts: near real-time thresholds.
  + Log alerts: KQL-based, minutes latency.
* **Action Groups**: Notification targets (email, SMS, webhook, automation runbook).
* **Workbooks**: Visualization dashboards.
* **Application Insights**: APM (requests, dependencies, failures).
* **Service Health vs Resource Health**: Service Health = global Azure outages. Resource Health = specific resource status.
* **New agent**: Azure Monitor Agent (AMA) with Data Collection Rules (DCR).

**Mini KQL Reference**

* CPU averages:  
  Perf | where CounterName == "CPU Utilization" | summarize avg(CounterValue) by bin(TimeGenerated, 5m)
* VM deletes:  
  AzureActivity | where OperationName == "Delete Virtual Machine"

**Backup & DR – Deep Review**

* **Azure Backup**: Recovery Services Vault, VM/file backups, file-level restore, long-term retention.
* **Azure Site Recovery (ASR)**: Replicates VMs to secondary region, provides failover/failback.
* **Availability Zones**: Intra-region redundancy, SLA 99.99%.
* **Cross-Region Restore**: Only with GRS vaults.
* **Failover types**: Test Failover (sandbox), Planned Failover (coordinated DR).

**Security – Deep Review**

* **Key Vault**: Secrets, keys, certificates. Access controlled by RBAC or access policies. Supports CMK + purge protection.
* **Defender for Cloud**: Secure Score, recommendations, Just-in-Time VM access, threat detection.
* **Azure Bastion**: Secure RDP/SSH via portal without public IP.
* **Managed Identities**: Assigns Azure AD identities to resources. Removes need for secrets in code.
* **NSG vs Firewall**: NSGs = subnet/NIC rules. Firewall = central, stateful, logging, TI. Firewall Premium = TLS inspection, IDPS.

**AZ-104 Gotchas & ARM Templates**

**Gotchas**

* **RBAC vs AD roles**: RBAC = resource-level; AD roles = tenant-wide.
* **NSG priority**: Lower number wins (100–4096).
* **Availability**: Sets = 99.95%, Zones = 99.99%.
* **Storage**: Only RA-GRS allows read from secondary.
* **Alerts**: Metric = near real-time, Log = KQL/minutes.
* **Action Groups**: Always required for notifications.
* **Locks**: CanNotDelete vs ReadOnly.
* **Backup vs ASR vs AZs**: Backup = data, ASR = failover, AZs = intra-region resiliency.

**ARM Templates – Key Points**

* Arrays must be valid JSON when inline (--parameters arrayParam='["one","two"]').
* --template-file is for templates; --parameters for values.
* Use @params.json for file-based params.
* PowerShell uses -TemplateFile and -TemplateParameterFile.

**CLI Examples**

* Inline param:  
  az deployment group create -g RG1 --template-file template.json --parameters arrayParam='["val1","val2"]'
* Params file:  
  az deployment group create -g RG1 --template-file template.json --parameters @params.json

**PowerShell Examples**

* Params file:  
  New-AzResourceGroupDeployment -ResourceGroupName RG1 -TemplateFile template.json -TemplateParameterFile params.json
* Inline array:  
  New-AzResourceGroupDeployment -ResourceGroupName RG1 -TemplateFile template.json -arrayParam @("val1","val2")

**AZ-104 Exam Cram Guide – Part 4 (Hybrid Identity, Cost Mgmt, Automation, Hybrid, AMA)**

**Hybrid Identity – Deep Review**

* **Azure AD Connect**: Sync on-prem AD → Azure AD.
  + Password Hash Sync (PHS)
  + Pass-through Authentication (PTA)
  + Federation (AD FS)
* **Password Writeback**: Cloud SSPR → on-prem AD.
* **Device States**:
  + Registered = BYOD
  + Joined = cloud-only corp
  + Hybrid Joined = on-prem + cloud

**Cost Management & Advisor**

* **Cost Mgmt + Billing**: Actual + forecast spend, exports, analysis.
* **Budgets**: Alerts at thresholds (no hard stop).
* **Advisor**: VM rightsizing, RI, idle cleanup, cost savings.

**Monitoring – AMA & DCR**

* **AMA**: Unified agent replacing Log Analytics/Diagnostics.
* **DCR**: Defines data collection + destination (Log Analytics, Storage, Event Hub).
* **Diagnostic Settings**: Routes platform logs/metrics.

**Automation & VM Lifecycle**

* **Azure Automation**: Runbooks, Update Mgmt.
* **Automanage**: Auto best practices (backup, monitoring, patching, security).
* **DSC**: Desired State Configuration for compliance.

**Hybrid & Multi-cloud**

* **Azure Arc**: Manage non-Azure servers, clusters, DBs in portal.
* **Stack Hub**: Azure services on-prem.
* **Lighthouse**: Delegated multi-subscription management.

**AZ-104 Exam Cram Guide – Part 5 (Edge Cases & Gotchas)**

**VM Backup Limitations**

* Azure Backup **does not support**:
  + **Unmanaged disks**
  + **VMs encrypted with Azure Disk Encryption (ADE)**
* Always use **Managed Disks** for supported backup scenarios.

**App-Aware Backups**

* Azure Backup can perform **application-aware snapshots** via VM extensions.
* Supported workloads:
  + **SQL Server**
  + **Windows Server IIS**
* Provides **consistency** for transactional apps.

**Firewall Premium Features**

* **Azure Firewall Premium** adds advanced inspection on top of Standard:
  + **TLS inspection** (decrypt + inspect + re-encrypt traffic)
  + **Intrusion Detection & Prevention (IDPS)**
* Use Premium SKU when **regulatory or deep packet inspection** is required.

**Storage Security & Private Endpoints**

* **Private Endpoints** + **Storage firewall (Selected Networks only)**
  + Ensures storage accounts are only accessible through **approved VNets**.
  + Prevents **data exfiltration** over public endpoints.

**App Insights Metric Alerts**

* Application Insights telemetry (requests, failures, response times) can be surfaced as **metrics**.
* Example:
  + Alert when **average request duration > 2s**
  + Configure **Metric Alert + Action Group** for notification.

**AZ-104 Practice Questions**

**Identities & Governance**

Q1: You need to ensure a group can only view resources in a subscription, not modify them.  
A) Reader  
B) Contributor  
C) Owner  
D) Global Admin

Q2: You want to enforce all VMs to deploy only in “UK South.” Which feature?  
A) Azure Policy  
B) Resource Lock  
C) RBAC  
D) Blueprint

Q3: You need to prevent accidental deletion of a Resource Group while still allowing updates.  
A) CanNotDelete  
B) ReadOnly  
C) Deny Assignment  
D) Initiative

Q4: Which two are tenant-wide roles?  
A) Global Admin  
B) User Admin  
C) Owner  
D) Contributor

Q5: You need just-in-time elevation for Global Administrator.  
A) Privileged Identity Management (PIM)  
B) Azure Policy  
C) NSG  
D) Blueprint

**Storage**

Q6: Which replication option provides read access to the secondary region?  
A) LRS  
B) ZRS  
C) GRS  
D) RA-GRS

Q7: You must automatically move blobs to Cool storage after 30 days.  
A) Lifecycle Management  
B) Azure Policy  
C) SAS  
D) RBAC

Q8: Which two options provide temporary delegated access to storage?  
A) Account Keys  
B) SAS  
C) Azure AD RBAC  
D) Storage Explorer

Q9: Your company needs on-prem file servers to sync with Azure Files.  
A) Azure File Sync  
B) AzCopy  
C) Blob Storage  
D) Data Box

Q10: You need to enforce encryption with customer-managed keys. Where do you store the keys?  
A) Azure Key Vault  
B) Azure Monitor  
C) Azure Files  
D) Resource Locks

**Compute**

Q11: You need high availability for a VM within a single datacenter.  
A) Availability Set  
B) Availability Zone  
C) VM Scale Set  
D) Azure Backup

Q12: Your app needs autoscaling of identical web servers.  
A) Availability Zone  
B) VM Scale Set  
C) Availability Set  
D) App Service

Q13: Which disk type provides the lowest latency for I/O intensive workloads?  
A) Standard HDD  
B) Standard SSD  
C) Premium SSD  
D) Ultra SSD

Q14: Which disk type is best for mission-critical DBs needing highest IOPS?  
A) Standard HDD  
B) Standard SSD  
C) Premium SSD  
D) Ultra SSD

Q15: Which Azure compute option lets you run event-driven code without managing infrastructure?  
A) VM Scale Set  
B) Functions  
C) App Service  
D) Container Instances

**Networking**

Q16: You need DNS-based routing across multiple regions.  
A) Application Gateway  
B) Traffic Manager  
C) Azure Firewall  
D) Azure Load Balancer

Q17: A company wants to protect against SQL injection at the web tier.  
A) Azure Firewall  
B) Application Gateway WAF  
C) NSG  
D) ASG

Q18: Your VPN Gateway connects on-prem to VNet1. VNet1 is peered with VNet2. On-prem cannot reach VNet2. What’s missing?  
A) Enable “allow forwarded traffic” in peering  
B) Create UDR  
C) Reinstall VPN client  
D) Use Traffic Manager

Q19: Which service provides global HTTP distribution with edge caching?  
A) Traffic Manager  
B) Azure Front Door  
C) Application Gateway  
D) Azure Firewall

Q20: Which DNS option allows private resolution for PaaS services?  
A) Private DNS Zones  
B) Public DNS  
C) NSG rules  
D) Traffic Manager

Q21: Which Azure service is designed for outbound Internet connectivity from VNets?  
A) Azure Firewall DNAT  
B) NAT Gateway  
C) Application Gateway  
D) Public IP on VM

Q22: Which Load Balancer SKU supports availability zones?  
A) Basic only  
B) Standard only  
C) Both  
D) Neither

Q23: Which Traffic Manager routing method picks lowest latency?  
A) Priority  
B) Weighted  
C) Performance  
D) Geographic

**Monitoring**

Q24: You need near real-time alerts when VM CPU > 80%.  
A) Metric Alert  
B) Log Alert  
C) Action Group  
D) Workbook

Q25: Which two are required for an alert notification?  
A) Metric/Log condition  
B) Action Group  
C) Workbook  
D) VM Extension

Q26: You need to visualize application failures over time.  
A) Action Group  
B) Application Insights  
C) NSG  
D) App Gateway

Q27: Which log captures control-plane actions like VM delete?  
A) Activity Log  
B) Diagnostic Logs  
C) Metrics  
D) InsightsMetrics

Q28: Which table stores VM heartbeat pings?  
A) Heartbeat  
B) Perf  
C) AzureActivity  
D) InsightsMetrics

Q29: Which agent replaces the Log Analytics + Diagnostics extensions?  
A) Azure Monitor Agent (AMA)  
B) OMS Agent  
C) Telegraf  
D) Metrics Collector

Q30: What defines how AMA routes telemetry?  
A) Data Collection Rules (DCR)  
B) Workbook  
C) Action Group  
D) Diagnostic Settings

**Backup & DR**

Q31: Which service provides VM replication for DR?  
A) Backup  
B) ASR  
C) Availability Zones  
D) GRS

Q32: Which feature allows file-level restore from a VM backup?  
A) Azure Backup  
B) ASR  
C) Snapshot  
D) Traffic Manager

Q33: Which SLA applies to Availability Zones?  
A) 99.9%  
B) 99.95%  
C) 99.99%  
D) 100%

Q34: Which ASR operation simulates failover without production impact?  
A) Backup Restore  
B) Test Failover  
C) Planned Failover  
D) GRS Restore

Q35: Which backup redundancy is recommended for production vaults?  
A) LRS  
B) ZRS  
C) GRS  
D) RA-GRS

Q36: Which agent supports backups of on-prem servers?  
A) MARS Agent  
B) RS Vault only  
C) NSG rules  
D) File Sync

**Security**

Q37: Which service provides Just-in-Time VM access?  
A) Key Vault  
B) Defender for Cloud  
C) Bastion  
D) NSG

Q38: You need to store database connection strings securely for an app.  
A) Key Vault  
B) NSG  
C) Managed Identity  
D) Defender

Q39: Which service allows secure RDP/SSH access without a public IP?  
A) Bastion  
B) NSG  
C) Firewall  
D) App Gateway

Q40: Which tool shows compliance against CIS benchmarks?  
A) Defender for Cloud  
B) Bastion  
C) Monitor  
D) Firewall

Q41: Which service ensures encryption keys are FIPS 140-2 HSM backed?  
A) Key Vault Premium  
B) Defender  
C) Bastion  
D) NSG

Q42: Which feature prevents secret purge until retention expires?  
A) Soft Delete  
B) RBAC  
C) Purge Protection  
D) Immutable Storage

Q43: Which Azure AD feature is only in Premium P2?  
A) MFA  
B) Conditional Access  
C) Privileged Identity Management  
D) SSPR

Q44: Which is true of Managed Identities?  
A) Require manual secret rotation  
B) Tied to lifecycle of resource  
C) Shared across subscriptions by default  
D) Stored in Key Vault automatically

**Answer Key**

* **Q1**: A – Reader role allows view only.
* **Q2**: A – Azure Policy enforces allowed locations.
* **Q3**: A – CanNotDelete prevents deletion but allows updates.
* **Q4**: A & B – Global Admin and User Admin are tenant-wide.
* **Q5**: A – PIM provides JIT role activation.
* **Q6**: D – RA-GRS provides read access to secondary.
* **Q7**: A – Lifecycle Management moves blobs.
* **Q8**: B & C – SAS and AAD RBAC are delegated access options.
* **Q9**: A – Azure File Sync integrates on-prem with Azure Files.
* **Q10**: A – CMKs are stored in Key Vault.
* **Q11**: A – Availability Set = intra-datacenter HA.
* **Q12**: B – VM Scale Set = autoscaling identical VMs.
* **Q13**: D – Ultra SSD = lowest latency.
* **Q14**: D – Ultra SSD = highest IOPS for mission-critical DBs.
* **Q15**: B – Azure Functions = serverless compute.
* **Q16**: B – Traffic Manager = DNS-based global routing.
* **Q17**: B – App Gateway WAF protects against OWASP.
* **Q18**: A – Must enable “allow forwarded traffic.”
* **Q19**: B – Azure Front Door = global HTTP accel.
* **Q20**: A – Private DNS zones = private PaaS resolution.
* **Q21**: B – NAT Gateway = outbound SNAT.
* **Q22**: B – Standard LB supports AZs.
* **Q23**: C – Performance = lowest latency.
* **Q24**: A – Metric alerts are near real-time.
* **Q25**: A & B – Must define condition + Action Group.
* **Q26**: B – App Insights visualizes app failures.
* **Q27**: A – Activity Log tracks control-plane ops.
* **Q28**: A – Heartbeat table stores VM pings.
* **Q29**: A – AMA replaces older agents.
* **Q30**: A – DCR defines routing for AMA.
* **Q31**: B – ASR replicates VMs for DR.
* **Q32**: A – Azure Backup supports file-level restore.
* **Q33**: C – AZ SLA = 99.99%.
* **Q34**: B – Test Failover = safe DR drill.
* **Q35**: C – GRS is recommended for production vaults.
* **Q36**: A – MARS agent supports on-prem servers.
* **Q37**: B – Defender for Cloud provides JIT.
* **Q38**: A – Key Vault stores secrets securely.
* **Q39**: A – Bastion = secure RDP/SSH.
* **Q40**: A – Defender Secure Score shows CIS compliance.
* **Q41**: A – Key Vault Premium = FIPS HSM-backed.
* **Q42**: C – Purge protection prevents deletion.
* **Q43**: C – PIM is Premium P2 only.
* **Q44**: B – Managed Identity lifecycle tied to resource.

# 🔑 AZ-104 Final Cram Checklist (2025)

## 1. ****Identities & Governance****

* Entra ID licensing: **P1 vs P2** (e.g., PIM = P2, Conditional Access = P1).
* Azure AD roles (tenant-wide) vs RBAC roles (resource-scoped).
* RBAC inheritance: Mgmt Group → Subscription → RG → Resource.
* Azure Policy **effects**: deny, audit, append, deployIfNotExists.
* Resource locks: **CanNotDelete vs ReadOnly**.
* Management groups + Blueprints vs Policy vs ARM templates.
* Budgets & cost alerts (soft alerts only, not hard enforcement).

## 2. ****Storage****

* Storage account types: GPv2 (default), BlobStorage (legacy), Premium SSD, FileStorage.
* Replication: **LRS, ZRS, GRS, RA-GRS** (RA-GRS is the only one with read secondary).
* Access tiers: Hot, Cool, Archive (rehydration needed).
* Blob features: **Soft delete, Snapshots, Versioning, Lifecycle policies**.
* File storage: **Azure File Sync** for on-prem integration.
* Security: Keys vs SAS (account/service/user-delegation SAS), RBAC for fine-grained access.
* Customer-managed keys (CMKs) in **Key Vault**.

## 3. ****Compute****

* Availability Sets (fault + update domains, SLA 99.95%) vs Zones (SLA 99.99%).
* VM Scale Sets = autoscale identical VMs.
* **Disks**: Standard HDD (cheap), Standard SSD (balanced), Premium SSD (low latency), Ultra SSD (highest IOPS).
* App Services: deployment slots, custom domains, TLS/SSL, scale-out.
* Azure Functions = event-driven serverless.
* ARM Templates / Bicep: parameters vs variables, inline arrays, parameter files.

## 4. ****Networking****

* VNets & subnets: isolation, address space planning.
* NSG: priority numbers (100–4096), inbound vs outbound.
* ASGs: group NICs to simplify NSG rules.
* VNet peering: not transitive by default; enable “forwarded traffic” for VPN → peer scenarios.
* Connectivity: **VPN Gateway vs ExpressRoute (Premium = global reach)**.
* Load Balancer SKUs: Basic (no AZ support, no SLA) vs Standard (secure by default, AZ aware, SLA).
* App Gateway WAF = Layer 7 + OWASP protection.
* Traffic Manager = DNS-based routing; Front Door = global HTTP acceleration with caching.
* Private DNS Zones + Private Endpoints for PaaS name resolution.
* NAT Gateway = outbound Internet SNAT for VNets.

## 5. ****Monitoring & Backup****

* Azure Monitor: **Metrics (real-time, numeric) vs Logs (KQL, minutes latency)**.
* Activity log = control plane (e.g., “VM deleted”).
* Common log tables: Heartbeat (VM pings), Perf (metrics), AzureActivity (control plane).
* Alerts: metric alert (threshold, near real-time), log alert (KQL).
* Action Groups = required for notifications.
* AMA (Azure Monitor Agent) replaces legacy agents; **DCR (Data Collection Rules)** control routing.
* Backup: Recovery Services Vault, file-level restore, **MARS agent for on-prem**.
* Site Recovery (ASR): replication + failover (Test vs Planned).
* Backup redundancy: GRS recommended for vaults.

## 6. ****Security****

* Defender for Cloud: secure score, JIT VM access.
* Azure Bastion: RDP/SSH without public IP.
* Key Vault: secrets, keys, certs; Premium = HSM-backed FIPS 140-2.
* Purge Protection + Soft Delete = protect against accidental or malicious deletion.
* Managed Identities: lifecycle tied to resource; removes need for secrets.

## 7. ****Hybrid & Automation****

* Azure AD Connect: PHS, PTA, Federation; password writeback.
* Device states: registered, joined, hybrid joined.
* Azure Arc: manage on-prem or multi-cloud servers from Azure.
* Azure Lighthouse: delegated multi-tenant management.
* Automanage: auto-apply best practices (patching, backup, monitoring).
* Automation: runbooks, update management, DSC.