AZ-104 – Interview Question Bank (Scenario Based)

1. What is the difference between Azure AD and On-Prem Active Directory?

Azure AD is a cloud-based identity provider focused on authentication and authorization for cloud resources. On■prem AD is designed for domain services like GPO, LDAP and Kerberos. Azure AD is identity as a service, not a domain controller replacement.

2. What is RBAC and how does it work?

RBAC (Role Based Access Control) assigns permissions to users or groups at a specific scope such as subscription, resource group or resource. Built-in roles include Owner, Contributor and Reader. Custom roles can also be created.

3. Explain Service Principal vs Managed Identity.

A Service Principal is an identity for applications created from an App Registration and uses secrets or certificates. Managed Identity is an automatically managed identity for Azure resources and does not require credentials.

4. Difference between App Registration and Enterprise Application?

App Registration defines an application in Azure AD. Enterprise Application is the service principal instance of that application in a specific tenant used for access control.

5. NSG vs ASG?

NSG contains security rules for subnets or NICs. ASG is used to logically group VMs so that NSG rules can be applied based on application groups instead of IP addresses.

6. Service Endpoint vs Private Endpoint?

Service Endpoint keeps traffic on Azure backbone but still uses public IP of the service. Private Endpoint assigns a private IP inside VNet and provides true private connectivity.

7. Load Balancer vs Application Gateway?

Load Balancer works at Layer 4 and distributes TCP/UDP traffic. Application Gateway works at Layer 7 and supports HTTP routing, SSL termination and WAF.

8. VPN Gateway vs ExpressRoute?

VPN Gateway uses encrypted internet connectivity. ExpressRoute provides private dedicated connectivity without using the public internet.

9. What are Availability Sets and Availability Zones?

Availability Sets protect against hardware failures within a datacenter. Availability Zones protect against datacenter level failures across physically separate locations.

10. How would you provide access only to one VM for a user?

Create an RBAC role assignment at the scope of that specific VM with Contributor or Reader role for that user.

11. What is Azure Policy and how is it different from RBAC?

Azure Policy enforces compliance rules on resources (prevent or audit). RBAC controls who can perform actions. Policy is about governance; RBAC is about permissions.

12. What is SAS token?

SAS (Shared Access Signature) provides time-limited delegated access to storage resources without sharing account keys.

13. How to secure secrets in Azure?

Use Azure Key Vault to store secrets, keys and certificates. Access should be granted using RBAC or access policies and preferably through Managed Identities.

14. What is Azure Monitor?

Azure Monitor collects metrics and logs from resources. Alerts and Action Groups notify administrators. Log Analytics enables advanced querying using KQL.

15. How do you backup an Azure VM?

Create a Recovery Services Vault, define a backup policy and enable backup for the VM. Restore can be full VM restore or file-level restore.

16. What is VNet Peering?

VNet Peering connects two virtual networks privately with low latency using Microsoft backbone without needing a gateway.

17. What are deployment slots in App Service?

Deployment slots allow staging environments for safe testing before swapping to production with minimal downtime.

18. What is Lifecycle Management in Storage?

Lifecycle rules automatically move blobs between Hot, Cool and Archive tiers or delete them based on age.

19. What is Azure Bastion?

Azure Bastion provides secure RDP/SSH access to VMs directly from Azure portal without exposing public IP addresses.

20. Metrics vs Logs?

Metrics are numeric time-series data for performance. Logs are detailed event data used for troubleshooting and stored in Log Analytics.

21. What is Just-in-Time VM Access?

It is a Defender for Cloud feature that restricts VM management ports and opens them only for approved time windows.

22. What is Azure Migrate?

Azure Migrate assesses on-premises workloads and helps plan and execute migration to Azure.

23. Explain Delegated vs Application permissions.

Delegated permissions act on behalf of a signed-in user. Application permissions allow an app to act without a user context.

24. What is a Snapshot vs Image?

A snapshot captures the state of a single disk. An image is a reusable template created from a generalized VM.

25. How would you troubleshoot VM connectivity issues?

Use Network Watcher tools such as IP Flow Verify, NSG Flow Logs, Connection Monitor and verify routing and NSG rules.