Azure Infrastructure Scenario-Based Interview Questions and Answers (Part 1)

Compute (VMs, Scale Sets, AKS)

1. Your application runs on Azure VMs and experiences high traffic spikes. How would you handle auto-scaling?

Use Virtual Machine Scale Sets with autoscale rules based on metrics like CPU usage or queue length to scale out/in dynamically.

2. You need to migrate an on-premises application to Azure VMs with minimal downtime. How?

Use Azure Migrate with replication; perform test migration and plan cutover during off-peak hours.

3. Your VM's disk has run out of space. How can you increase it without downtime?

Resize the disk from the Azure Portal or CLI, then expand the partition inside the OS using disk management tools.

4. You need to restrict creation of specific VM SKUs. How?

Use Azure Policy to define allowed VM SKUs and assign the policy at the subscription or management group level.

5. Pods are failing in AKS due to insufficient resources. How would you resolve this?

Check pod events using 'kubectl describe pod'. Adjust resource requests/limits or scale node pools if needed.

Networking (VNet, Load Balancer, Firewall, NSG)

6. Users report intermittent issues behind Azure Load Balancer. Troubleshoot steps?

Check Load Balancer health probes, NSG rules, backend VM status, and metrics for dropped packets.

7. How to securely connect two VNets in different regions?

Use VNet Peering for low latency or VPN Gateway for encryption and cross-region support.

8. Inspect all internet-bound traffic for threats. What Azure service?

Use Azure Firewall or third-party NVA with Threat Intelligence-based filtering and logging.

9. Allow vendor access to a specific VM only. How?

Use NSG rules to limit access and Just-In-Time VM access in Defender for Cloud for secure time-based access.

10. Secure high-performance on-prem to Azure connection?

Use Azure ExpressRoute for private, high-speed, and reliable connectivity.

Storage (Azure Blob, Managed Disks, Files, Backup)

11. Store logs for a year, cost-efficiently?

Use Azure Blob Storage with Cool or Archive access tier for low-cost long-term storage.

12. Share files between VMs in different regions?

Use Azure File Sync with Premium File shares or Geo-redundant storage.

13. Recover deleted data from Azure Blob?

Enable soft delete and versioning for Blob Storage; recover via Azure Portal or CLI.

14. Secure sensitive data in Blob Storage?

Enable encryption (by default), use Private Endpoints, RBAC, and Customer-Managed Keys (CMK).

15. Automated backups for Azure VM?

Enable Azure Backup and configure a Recovery Services Vault with a backup policy.

Identity & Security (Azure AD, IAM, RBAC, Key Vault)

16. MFA for all users except some services. How?

Use Conditional Access policies to enforce MFA, excluding specific cloud apps or user groups.

17. Provide temporary access without new user accounts. Solution?

Use Azure AD Privileged Identity Management (PIM) or Shared Access Signatures (SAS) for time-bound access.

18. VM compromised. What steps?

Disconnect from network, take snapshot, review logs, run Microsoft Defender scan, and re-deploy from a clean image.

19. Developer needs DB access without exposing credentials. How?

Use Azure Key Vault to store secrets and grant access via RBAC or managed identity.

20. Restrict resource group access to specific users. How?

Use RBAC roles scoped to the resource group to assign specific permissions to users or groups.