Azure-Interview-Question

1. What is Azure and what are its key services?

Microsoft Azure is a cloud computing platform offering a wide range of services such as:

- **Compute**: Virtual Machines, App Services, AKS (Kubernetes)
- **Storage**: Blob Storage, Disk Storage, File Storage
- **Networking**: Virtual Network, Load Balancer, Application Gateway

2. Difference between Azure Resource Manager (ARM) and classic deployment model?

Feature	ARM Model	Classic Model
Deployment	Declarative (JSON templates)	Manual or script-based
Grouping	Uses **Resource Groups** to manage resources	No resource grouping
RBAC support	Full RBAC support	Limited/no RBAC
Management tools	Portal, CLI, PowerShell, SDKs	Mostly portal & PowerShell
Recommendation	Modern, preferred model	Deprecated, legacy use

3. What is the difference between Azure VM and Azure App Service?

Feature	Azure VM	Azure App Service
Type	IaaS (Infrastructure as a Service)	PaaS (Platform as a Service)
Use Case	Full control over OS and software stack	Deploy web apps and APIs quickly
Management	User-managed patching, scaling	Auto-managed by Azure
Scaling	Manual or script-based	Built-in auto-scaling
Deployment	Any software, any OS	Only supported languages (Node.js, .NET, Python, etc.)

Azure-Interview-Question

4. What is Azure Resource Group?

An **Azure Resource Group** is a container that holds related resources (VMs, databases, NICs, etc.) for an application. It allows:

- Logical grouping for easier management
- Unified access control via RBAC
- Consistent deployment and deletion (delete the group = delete all inside)
- Tagging for billing and automation

5. What are Azure Regions and Availability Zones?
- **Azure Region**: A geographical area where Microsoft has one or more data centers (e.g., East US, West Europe)
- **Availability Zone**: A **physically separate data center** within a region — provides high availability

Feature	Region	Availability Zone
Scope	Large geographic area	Subset of a region
Redundancy	Region-pair disaster recovery	Zone-level HA within a region
Example Use	Geo-distributed services	99.99% SLA for VMs with zone redundancy

6. Explain the difference between Availability Sets and Availability Zones.

Feature	Availability Set	Availability Zone
Concept	Logical grouping of VMs within a data center	Physical separation across multiple data centers in a region
Fault Tolerance	Across **fault** and **update domains**	Across **zones** (data centers)
SLA	99.95%	99.99%
Use Case	Protect against rack/server failure	Protect against data center failure

- **Availability Sets** distribute VMs across multiple fault/update domains in the **same data center**.
- **Availability Zones** spread resources across **different data centers** in the same region.

Azure-Interview-Question

7. What is Azure Virtual Network (VNet)?

Azure Virtual Network (VNet) is a **private network** in Azure where you can securely run Azure resources like VMs, containers, and databases.

Key features:

- IP address ranges using **CIDR notation**
- **Subnets** for segmenting resources
- Integration with **on-prem networks** via VPN Gateway or ExpressRoute
- **NSG** and **UDR** for traffic control
- Supports **peering** between VNets

8. What is Network Security Group (NSG)?

A **Network Security Group (NSG)** is a **firewall-like** feature that controls inbound and outbound traffic to Azure resources like VMs and subnets.

Key points:

- Contains **rules** based on 5-tuple (Source, Destination, Protocol, Port, Action)
- Can be applied to:
    - **Network interfaces (NICs)**
    - **Subnets**
- Deny rule is the default if no rule matches
- Prioritized with a **priority number (lower = higher priority)**

9. How do you implement high availability for Azure VMs?

High availability (HA) for Azure VMs can be implemented using:

- **Availability Sets**: Distribute VMs across update and fault domains
- **Availability Zones**: Place VMs in separate physical data centers
- **Load Balancers**: Distribute traffic across healthy instances
- **Auto-scaling** (for stateless workloads)
- **Azure Site Recovery**: For DR (disaster recovery) between regions

10. What is Azure Load Balancer vs. Application Gateway?

Azure-Interview-Question

Feature	Azure Load Balancer	Azure Application Gateway
Type	Layer 4 (TCP/UDP)	Layer 7 (HTTP/HTTPS)
Use Case	Distribute traffic to VMs/VMSS	HTTP routing, SSL termination, WAF
Health Probes	TCP-based or custom	HTTP-based, path-aware
SSL Termination	❌ Not supported	✅ Supported
Routing Logic	Simple round-robin, hash-based	URL path, host headers, rules

- Use **Load Balancer** for general-purpose L4 balancing (e.g., backend VMs).
- Use **Application Gateway** for **web apps** needing smart routing and **WAF protection**.

◇ Storage

11. What types of storage does Azure provide?

Azure provides several types of storage services for different use cases:

- **Blob Storage** – For unstructured data like images, videos, backups
- **File Storage** – Fully managed file shares over SMB/NFS protocol
- **Queue Storage** – Message queues for decoupling app components
- **Table Storage** – NoSQL key-value store for semi-structured data
- **Disk Storage** – Managed disks used with Azure VMs (OS/Data)

12. Difference between Blob Storage, File Storage, and Disk Storage?

Feature	Blob Storage	File Storage	Disk Storage

Type	Object storage	Network file share (SMB/NFS)	Block storage
Use Case	Media, backups, logs	File sharing between VMs	VM OS/data disks
Access Protocol	HTTP/HTTPS (REST API)	SMB/NFS	Attached to VMs
Managed by	Application	User/VM	Azure
Scalability	High	Medium	Per VM limits

- **Blob**: Best for storing large files (videos, backups)
- **File**: Used like a shared network drive
- **Disk**: Attached to VMs, similar to hard drives

13. **What is Azure Storage Account and its types (Standard vs Premium)?**

An **Azure Storage Account** is a container for all Azure Storage services like blobs, files, queues, tables, and disks.

Tier	Standard	Premium
Media	HDD-backed	SSD-backed
Use Case	General-purpose workloads	Low-latency, high IOPS workloads
Cost	Lower	Higher
Services	Blob, File, Queue, Table, Disk	Blob, File, Disk (depending on type)

Types of Storage Accounts:

- **General-purpose v2 (GPv2)** – Supports all storage services and access tiers
- **Blob Storage Account** – Optimized for blob storage only
- **Premium Performance Account** – For IOPS-heavy scenarios

14. **How is data secured in Azure Storage?**

Azure-Interview-Question

Azure Storage secures data in multiple ways:

- **Encryption at Rest**:
  - Enabled by default using **Azure Storage Service Encryption (SSE)**
  - Uses **Microsoft-managed** or **customer-managed keys (CMK)**
- **Encryption in Transit**:
  - Data is encrypted using **HTTPS/TLS**
- **Shared Access Signatures (SAS)**:
  - Grant fine-grained access to storage resources with expiry time
- **Azure Active Directory (AAD) and RBAC**:
  - Used for identity-based access control to storage resources
- **Private Endpoints**:
  - Ensure storage access stays within your VNet (no public internet)

15. What is Azure Active Directory (AAD)?

Azure Active Directory is a **cloud-based identity and access management (IAM) service** from Microsoft.

- Provides **authentication** and **authorization** for users, apps, and devices.
- Supports **SSO (Single Sign-On)**, **MFA (Multi-Factor Authentication)**, and **Conditional Access**.
- Integrates with **Microsoft 365**, **Azure services**, and thousands of SaaS applications.

16. What is the difference between Azure AD and traditional AD?

Feature	Azure AD	Traditional AD
Deployment	Cloud-based	On-premises
Protocol	OAuth2, OpenID Connect, SAML	Kerberos, NTLM
Device Management	Azure-joined devices	Domain-joined devices
Primary Use	Web apps, cloud services	Windows PCs, legacy apps
Trust Model	Internet-first	LAN/domain-based

Azure AD is ideal for **modern, cloud-based apps**, while traditional AD is better for **on-prem infrastructures**.

17. **How do you manage role-based access (RBAC) in Azure?**

RBAC in Azure allows you to **assign permissions to users, groups, or services** at various scopes:

- **Scope levels**: Management Group > Subscription > Resource Group > Resource
- **Built-in roles**:
    o **Owner** – full access
    o **Contributor** – can manage resources but not permissions
    o **Reader** – read-only
- You can also create **custom roles**.

Roles are assigned using:

- **Azure Portal**
- **Azure CLI / PowerShell**
- **ARM Templates / Bicep**

18. **What is Managed Identity?**

A **Managed Identity** is an automatically managed **identity for Azure resources**.

Types:

- **System-assigned** – tied to a single resource
- **User-assigned** – independent and reusable across multiple resources

Use Case:

- Allow a VM, Function App, or Logic App to **authenticate securely** to other services (e.g., Key Vault, Azure SQL) **without hardcoding credentials**.

19. How does Azure Key Vault help with secrets management?

Azure Key Vault is a secure service for storing and managing:

- **Secrets** (e.g., API keys, connection strings)
- **Keys** (encryption keys for apps or disks)
- **Certificates**

Key features:

- **Access control** via Azure AD & RBAC
- **Logging** via Azure Monitor
- **Integration** with Managed Identity for seamless secret retrieval
- **Hardware Security Modules (HSM)** support for secure key storage

20. What is Azure Monitor and how does it differ from Log Analytics?

Azure Monitor is an end-to-end **monitoring and observability platform** in Azure. It collects, analyzes, and acts on telemetry data from Azure resources, applications, and on-prem systems.

- Provides insights into:
    - Application performance
    - Infrastructure health
    - Network and service availability

Azure-Interview-Question

Log Analytics is a **feature within Azure Monitor** that enables querying and analyzing log and telemetry data using **Kusto Query Language (KQL)**.

Feature	Azure Monitor	Log Analytics
Scope	Full monitoring platform	Data analysis engine
Function	Collection, visualization, alerting	Querying and analysis
Use Case	Alerts, dashboards, metrics	Deep dive into logs, debugging

21. How do you configure alerts and diagnostics in Azure?

To configure **alerts** and **diagnostics** in Azure:

✅ **Alerts:**

- Use **Azure Monitor > Alerts**
- Set up **alert rules** based on:
    - Metrics (CPU %, memory, etc.)
    - Logs (from Log Analytics queries)
- Define **action groups** (email, SMS, webhook, automation runbooks)

✅ **Diagnostics:**

- Enable **diagnostic settings** on a resource (VM, Storage, etc.)
- Choose data categories: **Metrics, Logs, Activity Logs**
- Send data to:
    - **Log Analytics**
    - **Event Hub**
    - **Storage Account**

22. What are Azure Cost Management and Budgets?

Azure Cost Management is a set of tools that help you monitor, control, and optimize cloud spending.

Key capabilities:

- Analyze **cost by resource, service, or department**

Azure-Interview-Question

- Set **alerts and budgets**
- Detect **anomalies** in spending
- Use **recommendations** to save money (e.g., reserved instances)

Budgets allow you to:

- Define a **spending limit** (e.g., $1,000/month)
- Trigger **alerts** when usage exceeds thresholds (e.g., 80%)