Top 50 Azure Interview Q&A for MNCs - Nensi Ravaliya

BEGINNER LEVEL QUESTIONS
1. What is Microsoft Azure?

Answer:

Microsoft Azure is a cloud computing platform provided by Microsoft that offers a comprehensive suite of services for computing, analytics, storage, networking, and databases. Azure enables organizations to build, deploy, and manage applications and services through a global network of Microsoft-managed data centers.

Key characteristics include:

Multi-cloud capability: Supports multiple programming languages, frameworks, and operating systems

Global presence: Available in 60+ regions worldwide

Pay-as-you-go pricing: Users pay only for resources they consume

Integrated services: Over 200 services covering every aspect of cloud computing

Azure is used by approximately 80% of Fortune 500 companies for various workloads including hosting applications, databases, and infrastructure.

2. What are the different types of Azure Services?

Answer:

Azure services are categorized into the following domains:

Compute Services:

- Virtual Machines (IaaS)

- App Services (PaaS)

- Azure Functions (Serverless)

- Azure Container Instances

- Azure Kubernetes Service (AKS)

Storage Services:

- Blob Storage (unstructured data)

- Disk Storage (VM disks)

- File Storage (file shares via SMB)

- Queue Storage (messaging)

- Table Storage (NoSQL key-value)

Networking Services:

- Virtual Networks (VNet)

- Load Balancer

- Application Gateway

- Azure CDN

- VPN Gateway

- ExpressRoute

Database Services:

- Azure SQL Database

- Azure Cosmos DB

- Azure Database for PostgreSQL/MySQL/MariaDB

- Azure Data Lake

Identity and Security:

- Azure Active Directory (AAD)

- Azure Key Vault

- Azure Security Center

- Azure Identity Protection

Developer Tools:

- Azure DevOps

- Visual Studio

- Azure Repos

- GitHub Actions

Analytics and BI:

- Azure Synapse Analytics

- Power BI

- Data Factory

- Data Explorer

3. What is Azure Virtual Machine (VM)?

Answer:

An Azure Virtual Machine is an on-demand, scalable computing resource that allows you to host applications on the Azure cloud platform.

Characteristics:

- Provides flexibility in OS selection (Windows or Linux)

- Custom hardware configuration (CPU, RAM, storage)

- Suitable for development, testing, or production workloads

- Pay-per-minute billing model

- Can be resized or deleted instantly

Use cases:

- Legacy application modernization

- Development and testing environments

- High-performance computing

- Running specific workloads requiring OS-level control

4. What is Azure Blob Storage?

Answer:

Azure Blob Storage is Microsoft's cloud object storage solution designed for storing massive amounts of unstructured data.

Key features:

- **Scalability**: Can store petabytes of data

- **Accessibility**: Can be accessed via HTTP/HTTPS from anywhere

- **Durability**: Multiple redundancy options ensure data protection

Components:

1. **Storage Account**: Container for all blob storage operations, either General-purpose or Blob Storage type

2. **Container**: Logical grouping mechanism for blobs (similar to folders)

   - Names must start with lowercase

   - Can store unlimited blobs

3. **Blob Types**:

   - **Block Blobs**: For text and binary files up to 195GB (50,000 blocks × 4MB each)

- **Append Blobs**: Optimized for append operations like logging
- **Page Blobs**: For frequent read/write operations, used as VM disks

Example access path:

```
https://storageaccount.blob.core.windows.net/container/blobname
```

5. What is Azure Active Directory (Azure AD)?

Answer:

Azure Active Directory is Microsoft's cloud-based identity and access management service.

Core functions:

- **Authentication**: Verifies user identity through multi-factor authentication (MFA)
- **Authorization**: Controls access to resources based on roles and permissions
- **Single Sign-On (SSO)**: Users authenticate once and gain access to multiple applications
- **Conditional Access**: Risk-based policies that determine when and how users access resources

Key scenarios:

- Managing user identities for cloud and hybrid environments
- Enabling secure access from anywhere
- Enforcing compliance and security policies
- Integration with third-party SaaS applications

Enterprise edition includes advanced security features like identity protection and conditional access policies.

6. What are the types of storage available in Azure?

Answer:

Azure offers four primary storage services:

Storage Type	Pur pose	Use Case
Blob Storage	Unstructured data (text, images, videos)	Media files, backups, archives
Queue Storage	Message queues for async communication	Decoupling services, job processing
Table Storage	NoSQL key-value store	Logs, diagnostics, time-series data
Disk Storage	Persistent storage for VMs	Operating systems, application data

Additional storage options:

- **File Storage**: SMB-based file shares (like traditional network drives)

- **Data Lake Storage**: Hierarchical storage optimized for big data analytics

- **Archive Storage**: Lowest cost option for rarely accessed data

7. What is Azure Resource Manager (ARM)?

Answer:

Azure Resource Manager is the deployment and management service that provides a consistent management layer for all Azure resources.

Key responsibilities:

- **Resource Management**: Create, modify, delete, and organize resources

- **Access Control**: Implement role-based access control (RBAC)

- **Security**: Apply locks and policies to resources

- **Organization**: Group resources into resource groups for easier management

- **Template Deployment**: Deploy infrastructure using JSON ARM templates or Bicep

Core concepts:

- **Resource Group**: Logical container for related resources

- **Resource**: Individual services (VMs, databases, storage accounts)

- **Regions**: Geographic locations where resources are deployed

- **Subscriptions**: Billing and entitlement units

Advantages:

- Consistent API for all Azure services

- Declarative infrastructure-as-code approach

- Better resource organization and lifecycle management

8. What is an Azure Region?

Answer:

An Azure Region is a set of data centers deployed within a specific geographic location, providing local presence and data residency.

Characteristics:

- Each region contains multiple data centers

- Regions are distributed globally (60+ regions worldwide)

- Provides **redundancy** and **disaster recovery** capabilities

- Enables **low-latency** access for users in that geography

- Subject to regional compliance requirements

Region pairing:

- Each region is paired with another region for disaster recovery

- Automatic failover between paired regions is possible

- Ensures business continuity

Example regions:

- East US, West US, Central US

- North Europe, West Europe

- Southeast Asia, East Asia

- Australia East

Important consideration: Some services are not available in all regions, so region selection affects service availability.

9. What is Azure Load Balancer?

Answer:

Azure Load Balancer is a fully managed load balancing service that distributes incoming network traffic across multiple resources.

Operating level:

- Works at Layer 4 (Transport layer) of the OSI model

- Handles TCP and UDP traffic

Key features:

- **High availability**: Automatically routes traffic away from unhealthy endpoints

- **Session persistence**: Sticky sessions for stateful applications

- **Health probes**: Monitors backend resource health

- **No database round trips**: Improves performance

Load balancing algorithms:

- Hash-based distribution (source IP, source port, destination IP, destination por t)

- Five-tuple hash for connection persistence

SKUs:

- **Basic**: Suitable for dev/test environments

- **Standard**: Recommended for production with enhanced security and monitor ing

10. What is Azure App Service?

Answer:

Azure App Service is a fully managed platform for building, deploying, and scaling web apps, APIs, and mobile backends.

Supported environments:

- ASP.NET, ASP.NET Core
- Java
- Node.js
- PHP
- Py thon
- Ruby
- Windows and Linux operating systems

Key capabilities:

- **Integrated DevOps**: Built-in continuous deployment from Git repositories
- **Automatic scaling**: Handle traffic spikes without manual intervention
- **Security**: HTTPS/SSL, authentication, authorization
- **Monitoring**: Application Insights integration
- **Cost-effective**: App Service Plans group resources for efficient billing

Plan types:

- **Free/Shared**: Development and testing
- **Basic**: Small production workloads
- **Standard**: Production applications with auto-scaling
- **Premium**: High-performance applications
- **Isolated**: Apps requiring highest performance and security

INTERMEDIATE LEVEL QUESTIONS
11. What is the difference between Azure Blob Storage and Azure File Storage?

Answer:

Aspect	Blob Storage	File Storage
Data Type	Unstructured data (images, videos, documents)	Structured file shares
Access Protocol	HTTP/HTTPS REST API	SMB 3.0 protocol
Use Case	Content delivery, backups, media storage	Legacy app file sharing, home directories
Mounting	Cannot mount as drive	Mount as network drive (\ser ver\share)
Cost	More cost-effective for large data	Higher cost but familiar interface Optimized for file operations
Performance	Optimized for streaming	Multiple simultaneous connections
Concurrent Access	Limited concurrent connections	
Access Tiers	Hot, Cool, Archive	Premium and Standard

Example:

- Use Blob Storage for storing application logs and media files

- Use File Storage when legacy applications need traditional network file shares

12. What is Azure SQL Database?

Answer:

Azure SQL Database is a fully managed relational database service based on SQL Server technology, delivered as a Platform-as-a-Service (PaaS).

Managed features (no maintenance required):

- Automated backups with point-in-time restore

- Automatic patching and updates

- Database optimization

- High availability and disaster recovery

- Security patches and compliance updates

Deployment options:

- **Single database**: Dedicated resources for one application
- **Elastic Pool**: Shared resources across multiple databases with guaranteed per for mance
- **Managed Instance**: Full SQL Server compatibility in cloud

Service tiers:

- **DTU Model**: Database Transaction Units (simplified pricing)
  - Basic, Standard, Premium
- **vCore Model**: Virtual cores (better control and pricing flexibility)
  - General Purpose, Business Critical, Hyperscale

Key capabilities:

- Advanced threat protection
- Data encryption at rest and in transit
- Transparent data encryption (TDE)
- Row-level security
- Dynamic data masking

---

13. What are the different deployment models in Azure?

Answer:

Azure supports three primary deployment models:

1. Classic Deployment (Legacy)

- Original Azure deployment model
- Limited features and capabilities
- Not recommended for new deployments
- Uses Azure Service Manager (ASM) API

2. Resource Manager (ARM) - Recommended

- Modern deployment model introduced in 2014

- Provides resource grouping and management

- Better access control through RBAC

- Supports templates for Infrastructure-as-Code

- Unified management plane for all services

3. Azure Stack

- Extension of Azure to on-premises environments

- Deploy Azure services in your own data center

- Consistency with Azure cloud services

- Hybrid cloud capabilities

Migration path: Azure strongly recommends moving from Classic to Resource Manager deployment model.

---

14. What is Azure Cosmos DB?

Answer:

Azure Cosmos DB is a globally distributed, multi-model database service designed for applications requiring high availability and low latency at global scale.

Key characteristics:

- **Turnkey global distribution**: Replicate data across multiple regions with a single click
- **Multi-model support**: Document, key-value, graph, and column-family data models

  Guaranteed latency: < 10ms at 99th percentile for reads and writes

- **Elastic scalability**: Scale throughput independently of storage

- **SLA-backed performance**: 99.99% availability

API support:

- SQL (Core) API

- MongoDB API

- Cassandra API

- Table API

- Gremlin API (for graph databases)

Consistency levels (trade-off between consistency and performance):

1. **Strong**: Immediate consistency, highest latency

2. **Bounded Staleness**: Data lag within defined bounds

3. **Session**: Consistent within single session

4. **Consistent Prefix**: Updates maintain order

5. **Eventual**: Lowest latency, eventual consistency

Use cases:

- Real-time personalization at scale

- IoT data storage

- Social media feeds

- Gaming leaderboards

- Content management

15. What are Azure Functions?

Answer:

Azure Functions is a serverless compute service that allows you to run small, event-driven pieces of code in the cloud without managing infrastructure.

Key advantages:

- **No infrastructure management**: Automatic scaling and resource management

- **Event-driven**: Triggered by events (HTTP requests, timer, queue messages, etc.)

- **Pay-per-execution**: Charged only for execution time

- **Quick development**: Focus on business logic, not infrastructure

- **Quick deployment**: Deploy in seconds

Supported languages:

- C#

- JavaScr ipt/TypeScr ipt

- Py thon

- Java

- PowerShell

- Custom handlers

Trigger types:

- HTTP triggers: Direct API calls

- Timer triggers: Scheduled execution (cron expressions)

- Queue triggers: Message-based processing

- Blob triggers: Storage events

- Event Hub triggers: Event stream processing

- Service Bus triggers: Message queue processing

- Cosmos DB triggers: Database change feed

Pricing model:

- Free tier: 1 million free executions

- Premium: Per-second granular pricing

- Consumption plan: Pay only for execution

Use cases:

- Serverless APIs

- Scheduled data processing

- Real-time file processing

- Lightweight microservices

16. What is Azure Kubernetes Service (AKS)?

Answer:

Azure Kubernetes Service is a managed Kubernetes service that simplifies the deployment, management, and scaling of containerized applications.

What AKS manages:

- Kubernetes master nodes (control plane)

- Kubernetes API server

- etcd (cluster state storage)

- Scheduler and controllers

What you manage:

- Worker nodes (agent nodes)

- Application deployments

- Container images

- Application configuration

Key benefits:

- **Reduced operational overhead**: Microsoft manages the control plane

- **Integrated DevOps**: Works seamlessly with Azure DevOps

- **Security**: Built-in RBAC, pod security policies, network policies

- **Monitoring**: Azure Monitor integration for cluster health

- **Scaling**: Automatic node scaling based on demand

Core components:

- **Node**: Virtual machine running containers

- **Pod**: Smallest deployable unit, contains one or more containers

- **Deployment**: Manages pods and ensures desired state

- **Service**: Exposes pods to network traffic

- **Ingress**: Routes external traffic to services

Container registry:

- Integration with Azure Container Registry (ACR)

- Private image repository for enterprise use

Net wor king:

- Multiple network plugins: Azure CNI, Kubenet

- Support for private clusters

- Network policies for traffic control

---

17. What is a Virtual Network in Azure?

Answer:

Azure Virtual Network (VNet) is a private network that enables secure communication between Azure resources and external networks.

Core components:

1. Subnets

- IP address ranges within the VNet

- Resources deployed into subnets

- Enable network segmentation

- Each subnet is associated with a route table

2. Network Interface Cards (NICs)

- Connect resources to subnets

- Assigned private IP addresses

- Can have multiple NICs per VM

3. Network Security Groups (NSGs)

- Firewall-like access control lists

- Inbound and outbound rules

- Can be applied to subnets or individual NICs

- Support allow/deny actions

4. Route Tables

- Define custom routing rules

- Control traffic flow between subnets

- Support user-defined routes (UDRs)

Network configurations:

- **Address space**: Define IP ranges (e.g., 10.0.0.0/16)

- **DNS settings**: Custom DNS servers

- **VNet peering**: Connect multiple VNets

- **VPN gateways**: Connect to on-premises networks

- **ExpressRoute**: Dedicated connections to on-premises

Security best practices:

- Use NSGs to restrict traffic

- Implement network segmentation

- Use VNet service endpoints for PaaS services

- Enable flow logs for monitoring

---

18. What is Azure DevOps?

Answer:

Azure DevOps is a comprehensive suite of development tools and services that help organizations plan, build, test, and deploy applications using agile methodologies.

Core services:

1. Azure Repos

- Git or Team Foundation Version Control (TFVC)

- Source code management

- Branching strategies

- Pull request workflows

2. Azure Pipelines

- Continuous Integration (CI): Automated builds

- Continuous Deployment (CD): Automated releases

- Multi-platform support (Windows, Linux, macOS)

- Integration with GitHub and Bitbucket

3. Azure Boards

- Agile project management

- Work item tracking

- Sprint planning

- Reporting and analytics

4. Azure Test Plans

- Manual and exploratory testing

- Test case management

- Reporting on test coverage

5. Azure Artifacts

- Package management

- NuGet, npm, Maven, and Python packages

- Build artifact storage

Pipeline components:

- **Triggers**: Events that start pipelines (commit, PR)

- **Stages**: Sequential execution phases

- **Jobs**: Collection of tasks

- **Tasks**: Individual steps (build, test, deploy)

- **Agents**: Machines running jobs

Benefits:

- End-to-end DevOps automation

- Visibility across entire development lifecycle

- Security and compliance integration

- Multi-cloud deployment support

19. What is Azure Key Vault?

Answer:

Azure Key Vault is a cloud service for securely managing and storing sensitive information including secrets, encryption keys, and certificates.

Stored objects:

1. Secrets

- Passwords, connection strings, API keys

- Encrypted at rest and in transit

- Access audit trail

2. Keys

- Cryptographic keys (RSA, EC)

- Hardware Security Module (HSM) support

- Automatic key rotation

3. Certificates

- SSL/TLS certificates

- Automatic renewal

- Certificate management

Key capabilities:

- **Encryption**: Data encrypted with customer-managed keys

- **Access control**: RBAC and access policies

- **Audit logging**: Track all access attempts

- **Compliance**: Support for regulatory requirements

- **Integration**: Azure services can authenticate using managed identity

Access methods:

- Azure Portal

- CLI and PowerShell

- REST API

- SDK for applications

Best practices:

- Use managed identities for application access

- Enable soft delete and purge protection

- Rotate secrets regularly

- Use separate key vaults for different environments

- Monitor and audit all access

20. What is Azure Traffic Manager?

Answer:

Azure Traffic Manager is a global DNS-based load balancing service that routes user traffic to the most appropriate endpoint.

Key characteristics:

- **Global scale**: Routes traffic across regions

- **DNS-based**: Works at DNS level (Layer 3)

- **Multiple routing methods**: Different strategies for traffic distribution

- **Health monitoring**: Continuous endpoint health checks

- **Automatic failover**: Routes away from unhealthy endpoints

Routing methods:

1. Priority

- Primary endpoint receives traffic
- Secondary endpoints are standby
- Use case: Active-passive failover

2. Weighted

- Distribute traffic by percentage
- Use case: Gradual rollout of new versions

3. Performance

- Route to geographically closest endpoint
- Minimizes latency
- Use case: Global applications

4. Geographic

- Route based on geographic location
- Use case: Data residency requirements

5. Subnet

- Route based on source IP subnet
- Use case: Internal traffic management

6. Multi-value

- Return multiple healthy endpoints
- Client-side routing decision
- Use case: High availability without load balancer

Health monitoring:

- HTTP/HTTPS probes
- TCP probes
- Custom endpoints
- Configurable probe intervals

ADVANCED LEVEL QUESTIONS

21. What is Azure Service Principal and how is it used?

Answer:

An Azure Service Principal is a security identity used by applications and services to access Azure resources without human intervention.

Types:

1. Application Service Principal

- Associated with an application registered in Azure AD

- Used for app-to-Azure authentication

2. Managed Service Principal

- Automatically created by Azure for specific resources

- Lifecycle managed by Azure

When to use:

- Applications requiring Azure resource access

- CI/CD pipelines deploying to Azure

- Automation and scripting

- Microservices architecture

Authentication methods:

- **Certificates**: X.509 certificates

- **Client secrets**: Username and password (less secure)

- **Federated credentials**: For GitHub Actions and other OIDC providers

Example C# usage:

```
var credential = new ClientSecretCredential(
    tenantId: "your-tenant-id",
    clientId: "your-client-id",
```

```
        clientSecret: "your-client-secret"
    );

    var client = new BlobContainerClient(
        uri: new Uri("https://..."),
        credential: credential
    );
```

Security best practices:

- Use certificates over client secrets

- Implement certificate rotation

- Grant least privilege permissions via RBAC

- Use managed identities when possible

- Monitor service principal activity

22. What is Azure Blob Storage Lifecycle Management?

Answer:

Azure Blob Storage Lifecycle Management automates the movement of blobs between access tiers based on defined rules, optimizing costs.

Access tiers:

Tier	Access Frequency	Cost	Use Case
Hot	Frequent access	Highest storage cost, lowest access cost	Recent data
Cool	Infrequent access	Medium storage cost	30+ days old data
Archive	Rare access	Lowest storage cost, high access cost	90+ days old data

Lifecycle rule example:

```json
{
  "rules": [
    {
      "name": "archive-old-blobs",
      "enabled": true,
      "type": "Lifecycle",
      "definition": {
        "actions": {
          "baseBlob": {
            "tierToCool": {
              "daysAfterModificationGreaterThan": 30
            },
            "tierToArchive": {
              "daysAfterModificationGreaterThan": 90
            },
            "delete": {
              "daysAfterModificationGreaterThan": 365
            }
          }
        },
        "filters": {
          "blobTypes": ["blockBlob"],
          "prefixMatch": ["logs/"]
        }
      }
    }
  ]
}
```

Benefits:

- **Cost optimization**: Automatically move old data to cheaper tiers

- **Compliance**: Automatically delete data per retention policies

- **Efficiency**: No manual intervention required

- **Flexibility**: Define rules per blob prefix or type

23. What is Azure Monitor?

Answer:

Azure Monitor is a comprehensive monitoring platform that collects, analyzes, and acts on telemetry data from Azure and on-premises resources.

Data sources:

- **Metrics**: Numeric values sampled at regular intervals (time-series data)

- **Logs**: Structured text data collected from resources

- **Traces**: Application performance monitoring data

- **Events**: Notifications about resource state changes

Key components:

1. Metrics Explorer

- Visualize time-series data

- Create custom charts

- Export data for analysis

2. Log Analytics

- Kusto Query Language (KQL) for querying logs

- Complex analytics and trending

- Performance analysis

3. Application Insights

- Application performance monitoring

- Exception tracking

- Request tracing

- Dependency monitoring

4. Alerts

- Threshold-based alerts

- Anomaly detection

- Smart groups for alert aggregation

Example alert rule:

- Trigger when VM CPU exceeds 80% for 5 minutes

- Send notification to operations team

- Automatically scale out resources

Advanced features:

- **Log Analytics**: Run complex queries on terabytes of data

- **Dashboards**: Real-time visualization of KPIs

- **Action groups**: Define notification channels (email, SMS, webhook)

- **Workbooks**: Interactive reports and analyses

24. What is the difference between Azure Load Balancer, Application Gateway, and Azure Front Door?

Answer:

Feature	Load Balancer	Application Gateway	Azure Front Door
OSI Layer	Layer 4 (Transport)	Layer 7 (Application)	Layer 7 (Application)
Protocol	TCP/UDP	HTTP/HTTPS	HTTP/HTTPS
Scope	Regional	Regional	Global
Routing	Simple port forwarding	URL/hostname-based	Geographic routing
SSL Termination	No	Yes	Yes
Path-based routing	No	Yes	No
WAF Support	No	Yes	Yes
Use Case	Non-HTTP traffic	Web applications	Global content delivery

Detailed comparison:

Load Balancer:

- Layer 4 (transport) load balancing

- Ideal for non-HTTP protocols or extreme performance

- Lowest latency

- Best for: Database connections, RDP, raw TCP/UDP traffic

Application Gateway:

- Layer 7 (application) load balancing

- URL-based routing (e.g., /api → API backend, /images → image backend)

- SSL termination and re-encryption

- Web Application Firewall (WAF) support

- Best for: Web applications, microservices with complex routing

Azure Front Door:

- Global content delivery network

- Anycast routing for optimal path selection

- Geographic routing capabilities

- DDoS protection

- Best for: Global applications, content delivery, multi-region failover

25. What is Azure VPN Gateway?

Answer:

Azure VPN Gateway connects on-premises networks or individual computers to Azure virtual networks using encrypted VPN connections.

Connection types:

1. Site-to-Site (S2S)

- Connects on-premises network to Azure VNet

- Requires VPN device on-premises

- Enables hybrid cloud scenarios

- Supports Active-Active and Active-Passive configurations

2. Point-to-Site (P2S)

- Connects individual computers to Azure VNet

- Uses SSTP, IKEv2, or OpenVPN protocols

- Suitable for remote workers

- Client VPN software required

3. VNet-to-VNet

- Connects multiple Azure Virtual Networks

- Across regions or subscriptions

- Full mesh topology support

Configuration:

- **Gateway subnet**: /27 or larger subnet in VNet

- **Public IP**: Required for external connectivity

- **Local network gateway**: Defines on-premises network

- **Connection**: Establishes actual VPN connection

Security:

- IPsec/IKE   encryption   Perfect

- Forward   Secrecy   (PFS)   Pre-

- shared   keys   or   certificates

- Firewall requirements

Alternatives:

- **ExpressRoute**: Dedicated, private connections (more expensive, higher per for mance)

- **Azure Virtual WAN**: Simplified hub-and-spoke network architecture

26. What is the difference between Azure Blob and Azure Disk Storage?
Answer:

Aspect	Blob Storage	Disk Storage
Purpose	Unstructured data storage	VM operating system and data disks
Access	HTTP/HTTPS REST API	Block-level access (mounted on VMs)
Data Type	Files, media, backups	Operating systems, databases
Mounting	Cannot mount as drive	Mount as /dev/sda on Linux or D: on Windows
Performance	Lower IOPS, higher throughput	High IOPS for VM operations
Size limit	4.7 TB per blob	Up to 32 TB per disk
Redundancy	LRS, GRS, RA-GRS options	LRS, ZRS options
Snapshots	Point-in-time copies	Managed snapshots for backup
Cost	Cost-effective for large data	Higher cost for performance
Use Case	Archives, media, logs	OS and application data

When to use each:

- **Blob Storage**: Long-term storage, archives, media distribution, backups

- **Disk Storage**: Running VMs, databases, high-performance applications

27. What is Azure Automation?

Answer:

Azure Automation is a cloud-based automation service that allows you to automate repetitive tasks and manage resources at scale.

Core components:

1. Runbooks

- PowerShell Runbooks: PowerShell scripts

- Python Runbooks: Python 2.7 and 3.8+

- Graphical Runbooks: Visual workflow designer

2. Hybrid Runbook Workers

- Execute runbooks on-premises
- Access local resources and services
- Use for secure operations

3. Desired State Configuration (DSC)

- Declarative configuration management
- Define desired state of systems
- Pull-based configuration updates

4. Update Management

- Patch management for Windows and Linux
- Scheduled updates
- Pre and post-update automation

5. Change Tracking

- Monitor configuration changes
- Audit trail for compliance
- Inventory management

Common use cases:

- Infrastructure provisioning
- Patch management
- Cost optimization (stop unused resources)
- Configuration management
- Log analysis and alerting

Example PowerShell Runbook:

```
param(
[Parameter(Mandatory=$true)]
[string]$ResourceGroupName,
[Parameter(Mandatory=$true)]
[string]$VMName )


# Authenticate using managed identity
Connect-AzAccount -Identity

# Start VM
Start-AzVM -ResourceGroupName $ResourceGroupName -Name $VMName -
NoWait

Write-Output "VM startup initiated"
```

28. What is Azure Site Recovery?

Answer:

Azure Site Recovery is a disaster recovery service that replicates workloads from on-premises environments or between Azure regions.

Key capabilities:

- **Continuous replication**: Asynchronous data replication

- **Failover automation**: Automated failover to recovery site

- **Failback capability**: Return to primary site after recovery

- **Compliance**: Helps meet data residency and compliance requirements

Replication scenarios:

1. On-Premises to Azure

- Replicate VMs (Hyper-V, VMware)

- Replicate physical servers

- Enables cloud disaster recovery

2. Azure Region to Azure Region

- Replicate VMs across regions

- Protects against regional failures

- Lower RTO/RPO than on-premises solutions

3. On-Premises to On-Premises

- Replicate between data centers

- Requires Site Recovery provider software

RTO and RPO:

Recovery Point Objective (RPO):

- Maximum acceptable data loss

- Time between last backup and failure

- Measured in minutes

- Affects replication frequency

Recovery Time Objective (RTO):

- Maximum acceptable downtime

- Time to restore and failover

- Measured in hours or minutes

- Affects infrastructure readiness

Configuration:

```
RPO: 5 minutes
RTO: 2 hours
Retention: 24 hours
```

Failover process:

1. Analyze replication consistency

2. Run test failover (non-destructive)

3. Execute planned/unplanned failover

4. Validate on recovery site

5. Commit failover

6. Failback when primary restored

---

29. What are Availability Sets in Azure?

Answer:

Availability Sets are logical groupings of VMs that distribute instances across multiple fault and update domains to improve availability.
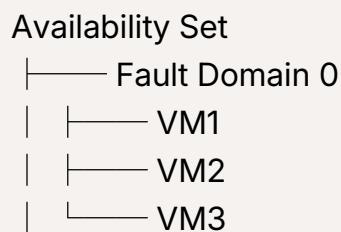
Fault Domains (FDs):
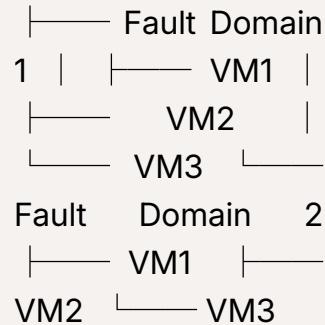
- Physical separation of VMs

- Share common power and network infrastructure

- Default: 3 fault domains (up to 3)

- If one FD fails, others remain operational

Update Domains (UDs):

- VMs rebooted together during updates

- Only one UD rebooted at a time

- 30-minute recovery time between UDs

- Default: 5 update domains (up to 20)

- Ensures application remains available during Azure maintenance

Architecture visualization:

```
Availability Set
├─────── Fault Domain 0
│   ├─────── VM1
│   ├─────── VM2
│   └─────── VM3
```

```
├─── Fault Domain
1 │   ├─── VM1    │
   ├─── VM2      │
   └─── VM3   ───┘
Fault    Domain    2
   ├─── VM1   ──┐
VM2   └──── VM3
```

SLA guarantee:

- 2+ instances in availability set: 99.95% SLA

- Without availability set: No SLA guarantee

Availability Sets vs Availability Zones:

Feature	Availability Set	Availability Zone
Scope	Single data center	Separate physical data centers
Redundancy	Logical grouping	Physical separation
Cost	No additional cost	Potential data transfer charges
Latency	Minimal	Slightly higher latency
Failover	Semi-automatic	Automatic in disaster scenarios

30. What is Azure Container Instances (ACI)?

Answer:

Azure Container Instances allows you to quickly run containers in Azure without managing VMs or orchestrators.

Key features:

- **Simplicity**: Deploy containers in seconds

- **No infrastructure management**: Azure handles VM provisioning

- **Per-second billing**: Pay only for container execution time

- **Linux and Windows containers**: Support for both

- **GPU support**: For compute-intensive workloads

Use cases:

- Quick testing and development

- Short-lived batch jobs

- Simple applications

- Task automation

- CI/CD pipeline agents

Limitations:

- Not suitable for production applications

- Limited scaling capabilities

- No built-in service discovery

- Stateless applications only

Deployment example:

```
az container create \
 --resource-group myResourceGroup \
 --name mycontainer \
 --image myimage:latest \
 --cpu 1 --memory 1.5 \
 --command-line "python app.py"
```

Alternatives for production:

- Azure Kubernetes Service (AKS)

- App Service with containers

- Service Fabric

---

31. What is Azure Firewall?

Answer:

Azure Firewall is a cloud-native, managed network security service that protects Azure Virtual Networks.

Key characteristics:

- **Fully managed**: Microsoft manages updates and infrastructure

- **Stateful firewall**: Maintains connection state

- **Threat intelligence**: Automated threat protection

- **High availability**: Built-in redundancy

- **Scalability**: Automatic scaling up to 30 Gbps

Features:

1. Network rules

- Source and destination filtering

- Protocol-based filtering

- Port-based rules

2. Application rules

- Fully Qualified Domain Name (FQDN) filtering

- HTTP/HTTPS inspection

- URL-based filtering

3. Threat Intelligence

- Real-time threat information

- Automated blocking of malicious IPs

- Alert and deny modes

4. SNAT/DNAT

- Source Network Address Translation

- Destination Network Address Translation

- Port forwarding

Deployment modes:

- **Hub and spoke**: Central firewall for multiple VNets

- **VNet integration**: Deployed within subnet

Comparison with NSG:

Feature	Firewall	NSG
Level	Layer 4-7	Layer 3-4
Scope	VNet	Subnet/NIC
Complexity	Advanced rules	Simple rules
Cost	Higher	Lower
Threat intelligence	Yes	No

32. What are Azure Blob Storage Access Tiers?

Answer:

Azure Blob Storage provides three access tiers optimized for different access patterns and cost profiles.

Tier Details:

Hot Tier:

- **Use case**: Frequently accessed data

- **Access cost**: Low

- **Storage cost**: Highest

- **Availability**: 99.9%

- **Example**: Active websites, ongoing analytics

Cool Tier:

- **Use case**: Infrequently accessed data (30+ days)

- **Access cost**: Higher

- **Storage cost**: Lower than Hot

- **Availability**: 99%

- **Early deletion**: 30-day penalty

- **Example**: Backup archives, less frequent reports

Archive Tier:

- **Use case**: Rarely accessed data (90+ days)

- **Access cost**: Highest

- **Storage cost**: Lowest

- **Availability**: 99%

- **Retrieval time**: Hours (rehydration required)

- **Early deletion**: 180-day penalty

- **Example**: Long-term compliance data, historical records

Cost comparison (approximate):

```
Hot:     $0.024 per GB + $0.00 per 10K operations
Cool:    $0.012 per GB + $0.01 per 10K operations
Archive: $0.004 per GB + $0.05 per 10K operations
```

Rehydration from Archive:

- Standard rehydration: Up to 15 hours

- High priority rehydration: Up to 1 hour

- Rehydration costs apply

Lifecycle management integration:

- Automatic tier transition rules

- Cost optimization

- Compliance enforcement

---

33. What is a Subnet in Azure?

Answer:

A Subnet is a contiguous range of IP addresses within an Azure Virtual Network (VNet), enabling network segmentation and resource organization.

Characteristics:

- **IP addressing**: Defined by CIDR notation (e.g., 10.0.1.0/24)

- **Resource placement**: VMs and other resources deployed into subnets

- **Routing**: Each subnet associated with a route table

- **Access control**: Network Security Groups (NSGs) applied at subnet level

Subnet planning:

```
VNet: 10.0.0.0/16
├──── Subnet 1: 10.0.1.0/24 (Web tier - 254 usable IPs)
├──── Subnet 2: 10.0.2.0/24 (Application tier)
├──── Subnet 3: 10.0.3.0/24 (Database tier)
└──── Subnet 4: 10.0.4.0/24 (Management)
```

Reserved IP addresses (per subnet):

- Network address (x.x.x.0): Not usable

- Gateway address (x.x.x.1): Reserved for VNet gateway

- Azure DNS (x.x.x.2): Reserved

- Azure reserved (x.x.x.3): Reserved

- Broadcast address (x.x.x.255): Not usable

Example /24 subnet:

- Total addresses: 256

- Reserved addresses: 5

- Usable addresses: 251

Subnet delegation:

- Delegate subnets to Azure services

- Services manage resources in delegated subnet

- Example: SQL Managed Instance requires delegated subnet

Best practices:

- Plan IP addressing carefully

- Use consistent naming convention

- Separate by function (web, app, database)

- Reserve space for future growth

- Document all subnets

34. What is Azure Logic Apps?

Answer:

Azure Logic Apps is a cloud service for building automated workflows and integrating apps, data, and services without coding.

Core concepts:

1. Triggers

- Event that starts workflow

- Types: Scheduled, HTTP request, Event-based

- Only one trigger per logic app

2. Actions

- Steps executed after trigger

- Perform operations or transformations

- Sequential or parallel execution

3. Connectors

- Pre-built integrations with services

- Reduce development time

- 500+ connectors available

Supported connectors:

- Microsoft services: Office 365, Dynamics 365, Teams

- Cloud services: Salesforce, ServiceNow, Slack

- Databases: SQL Server, CosmosDB

- APIs: REST, SOAP, custom APIs

Example workflow:

```
Trigger: Email received
  ↓
Action: Parse email
  ↓
Action: Create item in SharePoint
  ↓
Action: Send approval notification
  ↓
Decision: Approved?
  ├── Yes → Workflow A
  └── No → Workflow B
```

Integration patterns:

- B2B (Business-to-Business)

- Data integration across systems

- Process automation

- Event processing

Pricing:

- Pay-as-you-go for executions

- Connector costs

- Integration account fees for enterprise patterns

Advantages:

- No-code/low-code development

- Visual workflow design

- Extensive pre-built connectors

- Scalability and reliability

35. What is Azure ExpressRoute?

Answer:

Azure ExpressRoute establishes private, dedicated connections between on-premises networks and Azure data centers.

Key advantages:

- **Privacy**: Dedicated connection, not internet-based

- **Performance**: Consistent bandwidth and lower latency

- **Compliance**: Data never traverses public internet

- **Reliability**: Redundant connections for high availability

Connection models:

1. Co-location at Cloud Exchange

- Equipment in same facility as exchange

- Virtual cross-connect to Azure

- Fastest provisioning

2. Point-to-Point Ethernet Connection

- Direct fiber connection

- Dedicated line between on-premises and Azure

3. Any-to-Any (IPVPN) Connection

- Through WAN provider

- Flexible scalability

- Works with existing WAN

Bandwidth options:

- 50 Mbps to 100 Gbps

- Can upgrade without circuit replacement

- Symmetrical upload/download

Peering types:

Peering Type	Use Case
Azure Private Peering	Access Azure resources (VMs, databases)
Azure Public Peering	Access public Azure services (Storage, SQL)
Microsoft Peering	Access Microsoft online services (Office 365)

SLA and reliability:

- 99.9% uptime SLA

- 99.99% with dual ExpressRoute circuits

- Automatic failover support

Comparison with VPN Gateway:

Feature	ExpressRoute Private	VPN Gateway
Connection	dedicated Up to 100	Internet-based
Bandwidth	Gbps Consistent low	Up to 10 Gbps
Latency	latency Higher Weeks	Variable
Cost		Lower
Setup time		Minutes

Use cases:

- Hybrid cloud deployments

- High-bandwidth applications

- Sensitive data transfer

- Consistent performance requirements

36. What is Azure Identity Protection?

Answer:

Azure Identity Protection is a security service that helps detect and mitigate identity-based risks.

Risk types:

1. User Risk

- Suspicious user behavior

- Compromised credentials

- Abnormal sign-in patterns

2. Sign-in Risk

- Unusual sign-in properties

- Anonymous IP addresses

- Malware-linked IPs

- Unfamiliar locations

Detection capabilities:

- Machine learning models

- Real-time risk analysis

- Offline processing for historical analysis

- Risk scoring (0-100)

Risk levels:

- **Low**: Typical behavior

- **Medium**: Potential risk detected

- **High**: Confirmed or recent compromise

Response actions:

- **Block**: Deny access

- **Challenge**: Require MFA

- **Require password change**: Force credential reset

- **Require Azure MFA**: Require multi-factor authentication

Policies:

1. User Risk Policy

- Detects compromised credentials

- Forces password reset
- Blocks high-risk users

2. Sign-in Risk Policy

- Detects suspicious sign-ins
- Requires MFA on medium risk
- Blocks high-risk sign-ins

3. MFA Registration Policy

- Enforce MFA registration
- Conditional access requirements

Integration:

- Azure AD conditional access
- Azure AD risk detection API
- SIEM integration
- Third-party security tools

Benefits:

- Proactive threat detection
- Automated response
- Compliance requirements
- Risk-based access control

---

37. What is Azure Synapse Analytics?

Answer:

Azure Synapse Analytics is an enterprise-level analytics service that combines big data and data warehousing capabilities.

Components:

1. SQL Analytics

Enterprise data warehousing

Massive parallel processing (MPP)

Unlimited scale
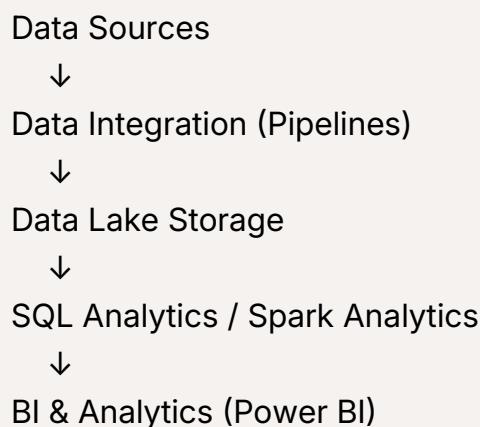
2. Spark Analytics

- Apache Spark for big data processing

- Python, Scala, SQL support

- Machine learning capabilities

3. Data Integration

- ETL/ELT pipelines

- Data flow transformations

- Copy activity for data movement

Architecture:

```
Data Sources
    ↓
Data Integration (Pipelines)
    ↓
Data Lake Storage
    ↓
SQL Analytics / Spark Analytics
    ↓
BI & Analytics (Power BI)
```

Use cases:

- Large-scale data warehousing

- Data lake analytics

- Data preparation and transformation

- Machine learning

- Real-time analytics

Pricing models:

- **Provisioned capacity**: Reserved computing power

- **Pay-as-you-go**: Consumption-based

- **SQL on-demand**: Query data lake without provisioning

Key features:

- **Unified workspace**: Integrated development environment

- **Collaboration**: Shared notebooks and queries

- **Security**: Row-level security, column-level encryption

- **Performance**: Auto-scaling and optimization

38. What is Azure Event Grid?

Answer:

Azure Event Grid is a fully managed event routing service that enables real-time event delivery from various sources to subscribers.

Event sources:

- Azure services (Storage, Key Vault, Event Hub)

- Custom applications

- Third-party services (GitHub, Stripe)

Subscribers:

- Azure Functions

- Logic Apps

- WebHooks

- Event Hub

- Service Bus Queue/Topic

Event flow:

Event Source → Event Grid Topic → Event Subscription → Subscriber

Key concepts:

Topics

- Source for events

- Built-in topics from Azure services

- Custom topics for applications

Event Subscriptions

- Define which events to receive

- Route events to subscribers

- Filter and transform events

Handlers

- Destination for events

- Process and react to events

Event schema:

```
{
  "topic": "/subscriptions/...",
 "eventType": "Microsoft.Storage.BlobCreated",
 "eventTime": "2024-01-15T10:30:00Z",
 "data": {
 "url": "https://example.blob.core.windows.net/images/photo.jpg",
 "contentType": "image/jpeg"
  }
}
```

Use cases:

- Automated image resizing when photos uploaded

- Trigger serverless workflows

- Real-time monitoring

- Application integration

- Event-driven architectures

Features:

- Guaranteed delivery (at least once)

- Advanced filtering

- Dead lettering for failed events

- Event retention

- Custom retries
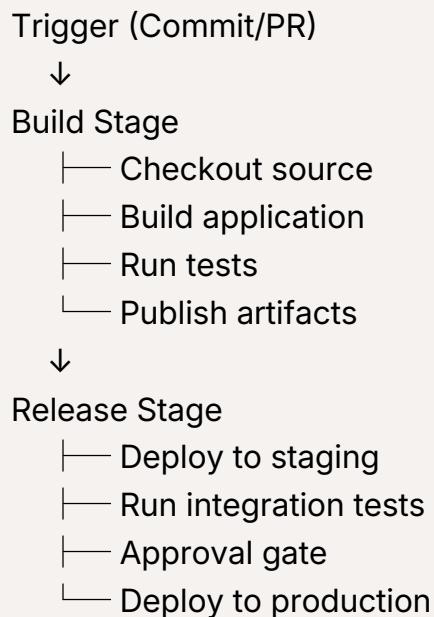
39. What is Azure DevOps Pipeline?

Answer:

Azure DevOps Pipelines is a cloud service for continuous integration (CI) and continuous deployment (CD) of applications.

Pipeline architecture:

```
Trigger (Commit/PR)
     ↓
Build Stage
     ├── Checkout source
     ├── Build application
     ├── Run tests
     └── Publish artifacts
     ↓
Release Stage
     ├── Deploy to staging
     ├── Run integration tests
     ├── Approval gate
     └── Deploy to production
```

Core concepts:

Triggers:

- Continuous Integration: Build on every commit

- Scheduled: Nightly builds

- Pull Request: Validate PRs

Stages:

- Sequential execution phases

- Parallel stages for speed

- Conditional execution

Jobs:

- Collection of steps

- Run on agents (Microsoft-hosted or self-hosted)

- Multiple jobs in parallel

Tasks:

- Individual operations

- Pre-built tasks (NuGet, Docker, deployment)

- Custom scripts (PowerShell, Bash)

Example YAML pipeline:

```
tr igger:
 - main

pool:
 vmImage: 'ubuntu-latest'

stages:
- stage: Build
 jobs:
 - job: BuildApp
    steps:
```

```yaml
        - task: DotNetCoreCLI@2
          inputs:
            command: 'build'
            projects: '**/*.csproj'
        - task: DotNetCoreCLI@2
          inputs:
            command: 'test'
            projects: '**/*Tests.csproj'

    - stage: Deploy
      dependsOn: Build
      condition: succeeded()
      jobs:
      - deployment: DeployWeb
        environment: 'Production'
          strategy:
            runOnce:
              deploy:
                steps:
                - script: echo "Deploying to Azure"
```

Agents:

- **Microsoft-hosted**: Ubuntu, Windows, macOS

- **Self-hosted**: Run on your infrastructure

- **Container jobs**: Execute in containers

Ar tifacts:

- Build outputs

- Stored for release pipelines

- Retention policies

Key features:

- YAML-based configuration

- Integration with GitHub, GitLab, Bitbucket

- Multi-cloud deployment (Azure, AWS, GCP)

- Variable management

- Secrets management

- Status badges

40. What is Azure Application Gateway?

Answer:

Azure Application Gateway is a web traffic load balancer that manages traffic to web applications at Layer 7 (Application layer).

Key capabilities:

1. Request routing

- URL path-based routing: /api → backend pool 1, /images → backend pool 2

- Host-based routing: subdomain-specific backends

- Multi-site hosting

2. SSL/TLS termination

- Decrypt HTTPS traffic

- Offload encryption from backend servers

- Re-encrypt for backend communication

3. Web Application Firewall (WAF)

- Protect against common web exploits

- SQL injection prevention

- Cross-site scripting (XSS) protection

- DDoS mitigation

4. Session persistence (Cookie affinity)

Route sessions to same backend

Maintain session state

Components:

Frontend listeners:

- Listen on ports 80, 443

- Public or private IP

- HTTPS/HTTP protocols

Backend pools:

- Destination servers

- VMs, App Services, on-premises servers

- Health probes monitor availability
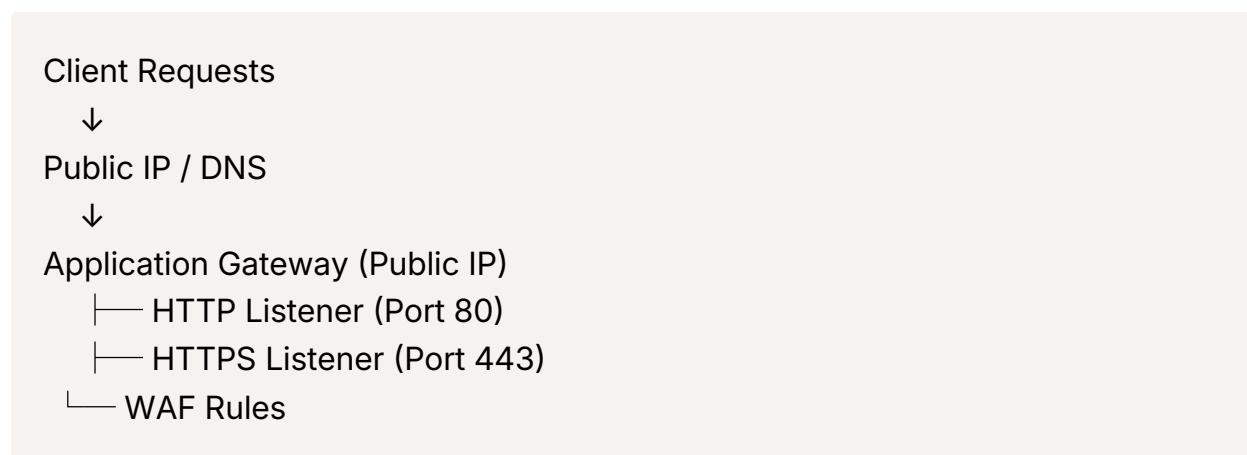
HTTP settings:
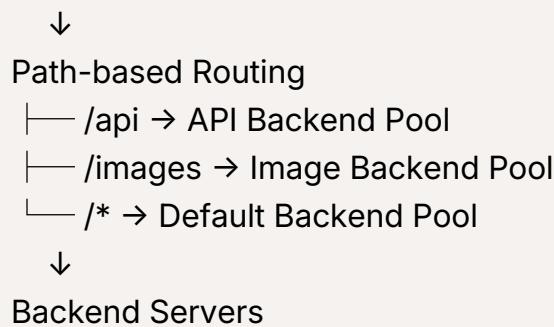
- Protocol (HTTP/HTTPS)

- Port configuration

- Cookie affinity

- Request timeout

Routing rules:

- Connect listeners to backend pools

- Define routing logic

- Path-based rules

**Architecture visualization:**

```
Client Requests
    ↓
Public IP / DNS
    ↓
Application Gateway (Public IP)
    ├── HTTP Listener (Port 80)
    ├── HTTPS Listener (Port 443)
    └── WAF Rules
```

```
        ↓
Path-based Routing
 ├── /api → API Backend Pool
 ├── /images → Image Backend Pool
 └── /* → Default Backend Pool
        ↓
Backend Servers
```

SKUs:

- **Standard**: Basic application delivery

- **Standard v2**: Performance optimization, auto-scaling

- **WAF**: Web Application Firewall

- **WAF v2**: Enhanced WAF with auto-scaling

Use cases:

- Multi-tenant applications

- Microservices routing

- SSL termination

- Web application protection

- Session persistence requirements

---

41. What is Azure Managed Identity?

Answer:

Azure Managed Identity is an Azure AD identity automatically created and managed by Azure for Azure resources.

Two types:

1. System-assigned Managed Identity

- Created automatically with resource

- Lifecycle tied to resource

- Unique identity per resource

- Cannot be shared

Example:

```
var credential = new DefaultAzureCredential();
var client = new BlobContainerClient(
    uri: new Uri("https://..."),
    credential: credential
);
```

2. User-assigned Managed Identity

- Created explicitly in Azure AD

- Lifecycle independent of resources

- Can be assigned to multiple resources

- More control and flexibility

Example:

```
# Create user-assigned identity
az identity create -g myResourceGroup -n myIdentity

# Assign to VM
az vm identity assign -g myResourceGroup -n myVM \
 --identities /subscriptions/.../resourcegroups/.../providers/Microsoft.Manage
dIdentity/userAssignedIdentities/myIdentity
```

Benefits:

- **No credentials to manage**: No passwords or keys

- **Automatic token management**: Tokens refreshed automatically

- **Auditing**: All access logged

- **Least privilege**: Grant specific permissions via RBAC

- **Simplicity**: Eliminates secrets management

Use cases:

- Application to Azure service authentication

- CI/CD pipeline access to Azure resources

- Container access to Azure services

- Microservices inter-service communication

Integration:

- Key Vault secret retrieval

- Storage access

- Database connections

- CosmosDB

- Any Azure resource supporting RBAC

Best practices:

- Use managed identities over service principals with secrets

- Implement minimal RBAC permissions

- Use system-assigned for simple 1:1 mapping

- Use user-assigned for resource sharing

42. What is Azure Data Factory?

Answer:

Azure Data Factory is a cloud-based data integration service for creating data-driven workflows to orchestrate and automate data movement and transformation.

ETL/ELT orchestration:

ETL (Extract-Transform-Load):

- Extract data from source

- Transform in staging area

- Load to destination

ELT (Extract-Load-Transform):

- Extract and load raw data

- Transform in destination (typically data lake)

- More efficient for large data volumes

Core components:

1. Pipelines

- Workflow container

- Execute activities in sequence or parallel

- Scheduled or event-triggered

2. Activities

- Individual operations

- Copy activity: Data movement

- HDInsight: Hadoop processing

- Databricks: Apache Spark processing

- Azure Function: Custom logic

- Stored Procedure: Database operations

- Dynamic range loops
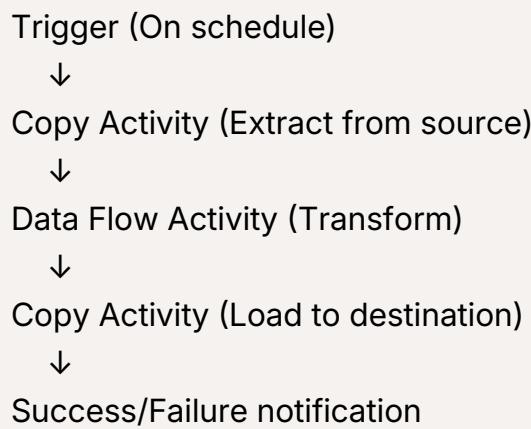
3. Data flows

- Visually designed transformations

- Data transformation without coding

- Auto-generated Spark code

4. Integration runtimes

- **Azure Integration Runtime**: Cloud-based execution

- **Self-hosted Integration Runtime**: On-premises execution

- **Azure-SSIS Integration Runtime**: SSIS package execution

Example pipeline:

```
Trigger (On schedule)
    ↓
Copy Activity (Extract from source)
    ↓
Data Flow Activity (Transform)
    ↓
Copy Activity (Load to destination)
    ↓
Success/Failure notification
```

Supported sources/sinks:

- Azure services (Blob, Data Lake, SQL Database)

- On-premises databases (SQL Server, Oracle)

- SaaS applications (Salesforce, ServiceNow)

- Cloud services (AWS S3, Google Cloud Storage)

Key features:

- Visual pipeline design

- 90+ connectors

- Scheduling and triggers

- Monitoring and alerting

- Parameterization for reusability

- CI/CD integration

Use cases:
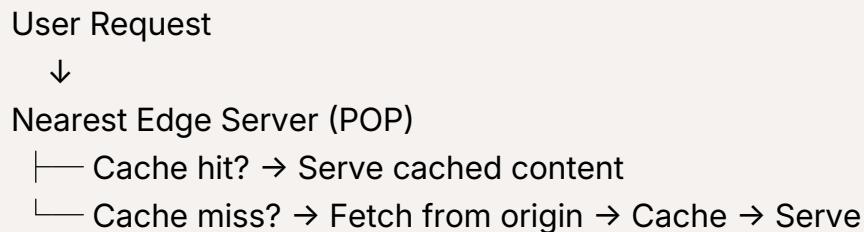
- Data warehouse population

- Data lake ingestion

- Analytics data preparation

- Legacy system migration

- Multi-source data consolidation

43. What is Azure CDN (Content Delivery Network)?

Answer:

Azure CDN is a globally distributed network that caches content closer to users, improving content delivery speed and reliability.

How it works:

```
User Request
    ↓
Nearest Edge Server (POP)
   ├── Cache hit? → Serve cached content
   └── Cache miss? → Fetch from origin → Cache → Serve
```

Performance benefits:

- Reduced latency through geographic proximity

- Lower bandwidth consumption

- Improved user experience

- Reduced load on origin server

Caching behaviors:

Query string handling:

- **Ignore**: Same content for different query strings

- **Bypass**: Different content per query string

- **Cache every unique URL**: Each query string = different cache

Cache rules:

- Expiration times (TTL)

- Specific path rules

- Bypass caching for dynamic content

Purge options:

- Purge single files

- Purge by wildcard paths

- Purge all content

SKUs and providers:

SKU	Standard	CDN Provider	Features	Basic
Microsoft	**Standard**	Microsoft	CDN	service
Akamai	**Standard**	Akamai	Advanced caching	
Verizon	**Premium**	Verizon	Premium features	
Verizon		Verizon	Full rules engine	

Key capabilities:

- Compression: Reduce file sizes

- HTTPS support: Secure content delivery

- Rules engine: Custom routing

- DDoS protection: Basic DDoS mitigation

- Geo-filtering: Content availability by region

- Token authentication: Secure access

Use cases:

- Static content delivery (CSS, JavaScript, images)

- Media streaming

- Software distribution

- API acceleration

- Website acceleration

Integration with storage:

```
Azure Blob Storage
    ↓
Azure CDN origin
    ↓
Global edge servers
```

↓

End users

44. What is Azure Virtual Desktop?

Answer:

Azure Virtual Desktop is a cloud-based service providing virtualized desktop and application experiences delivered from Azure.

Components:

1. Host pools

- Collection of similar VMs

- Shared resources and configuration

- Session or personal desktops

Session pooling:

- Multiple users per VM

- Cost-efficient

- Non-persistent desktop

Persistent:

Single user per VM

Maintains user state

Higher cost

2. Workspaces

- Group of host pools

- User-facing resources

- Applications and desktops

3. Application groups
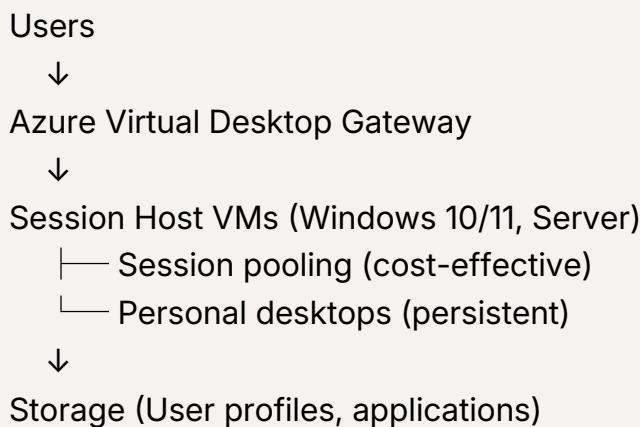
- Desktop or application groups

- Remoteapp applications

- Define what users access

4. User assignments

- Map users to applications/desktops

- Group-based assignment

- RBAC controls

Deployment architecture:

```
Users
   ↓
Azure Virtual Desktop Gateway
   ↓
Session Host VMs (Windows 10/11, Server)
    ├── Session pooling (cost-effective)
    └── Personal desktops (persistent)
   ↓
Storage (User profiles, applications)
```

Key benefits:

- **Multi-user optimization**: Windows 10/11 multi-user capability

- **Simplified management**: Centralized management

- **Security**: Azure AD integration, encryption

- **Flexibility**: Any device, anywhere access

- **Cost savings**: Session pooling reduces infrastructure

Licensing:

- Azure subscription required

- Windows or Microsoft 365 license

- Per-user licensing models

Use cases:

- Remote work desktops

- Application delivery

- Bring Your Own Device (BYOD) support

- Training environments

- Call center agents

Performance considerations:

- Bandwidth: 1.5-2 Mbps minimum

- Latency: <150ms for optimal experience

- Display protocol: RDP optimizations

45. What is Azure Security Center?

Answer:

Azure Security Center (now part of Microsoft Defender for Cloud) is a unified security management system providing threat protection and security posture management.

Key functions:

1. Security recommendations

- Best practice suggestions

- Security controls

- Priority-based recommendations

- Remediation guidance

2. Threat detection

- Advanced threat protection

- Anomaly detection

- Machine learning models

- Real-time alerts

3. Vulnerability management

- Vulnerability assessment

- Patch management

- Configuration management

- Compliance tracking

4. Compliance monitoring

- Regulatory standards (ISO 27001, PCI-DSS, HIPAA)

- Compliance score

- Audit reports

Security controls:

- Access and permissions

- Data protection

- Threat detection

- Vulnerability management

- Incident response

Azure Defender add-ons:

- **Servers**: VM protection

- **App Service**: Web application protection

- **SQL**: Database vulnerability assessment

- **Storage**: Threat detection for storage

- **Containers**: Container image scanning

- **Key Vault**: Suspicious access patterns

Tiers:

Free tier:

- Azure policy recommendations

- Security recommendations

- Limited threat detection

Paid tier (Azure Defender):

- Advanced threat detection
- Vulnerability assessment
- Regulatory compliance
- Just-in-time VM access
- Secure score tracking

Secure Score:

- 0-100 scale
- Percentage of controls implemented
- Tracks improvement over time
- Benchmark against industry

Integration:

- Azure Sentinel for SIEM
- Azure Automation for remediation
- Third-party security tools

---

46. What is Azure Backup?

Answer:

Azure Backup is a cloud-based service providing reliable, scalable, and cost-effective backup and recovery solutions.

Supported sources:

Azure resources:

- Virtual machines
- Databases (SQL Server, PostgreSQL)
- File shares
- Managed disks

- SAP HANA databases

On-premises:

- Files and folders

- System state

- Bare metal recovery

- Windows Server

Backup types:

Full backup:

- Complete copy of all data

- Initial backup

- Larger size

Incremental backup:

- Only changed data

- Reduced storage

- Faster backup

- Dependent on previous backup

Differential backup:

- Changed data since last full backup

- Independent backups

- Medium size

RPO/RTO:

Recovery Point Objective (RPO):

- Time between backups

- 15 minutes minimum for Azure VMs

- Daily for on-premises

Recovery Time Objective (RTO):

- Restore time: Varies from minutes to hours

- Affects infrastructure readiness

Backup vaults:

- **Recovery Services Vault**: Azure resources and on-premises

- **Backup Vault**: Azure database workloads

Retention policies:

Daily backups: 30 days
Weekly backups: 12 weeks
Monthly backups: 60 months

Features:

- Application-consistent backups

- Encryption (customer-managed keys)

- Cross-region restore

- Immutable backups (protection against deletion)

- Long-term retention

Pricing:

- Per VM per day

- Per GB backed up

- Per transaction

Use cases:

- Disaster recovery

- Data protection

- Compliance requirements

- Point-in-time restoration

- Long-term archival

47. What is Azure Advisor?

Answer:

Azure Advisor is a personalized cloud consultant that analyzes your Azure resource configuration and usage patterns, providing recommendations for optimization.

Recommendation categories:

1. Cost optimization

- Eliminate unused resources

- Right-size underutilized VMs

- Reserved Instance recommendations

- Compression for data transfer

2. Reliability

- Improve application availability

- High-availability configurations

- Backup and disaster recovery

- Capacity planning

3. Operational excellence

- Automation opportunities

- Performance monitoring

- Security configuration

- Azure best practices

4. Performance

- Caching recommendations

- Database optimization

- Network configuration

- Throughput improvements

5. Security

Network security groups

MFA recommendations

Encryption requirements

Access control reviews

Recommendation scoring:

- High impact: Immediate attention

- Medium impact: Important but not urgent

- Low impact: Nice to have

Example recommendations:

```
High Impact:
- Enable Azure Security Center standard tier
- Configure Network Security Groups for better security
- Enable encryption on SQL Database

Medium Impact:
- Remove unattached disks to reduce costs
- Configure backup for virtual machines
- Enable monitoring on Azure resources
```

Features:

- Personalized recommendations

- Filters by resource groups

- Trend analysis

- Dismissible recommendations

- Scheduled reports

- Integration with Azure Policy

Benefits:

- Cost   reduction   Improved

- security posture Enhanced

- reliability

- Better performance

- Operational efficiency

48. What are Azure Availability Zones?
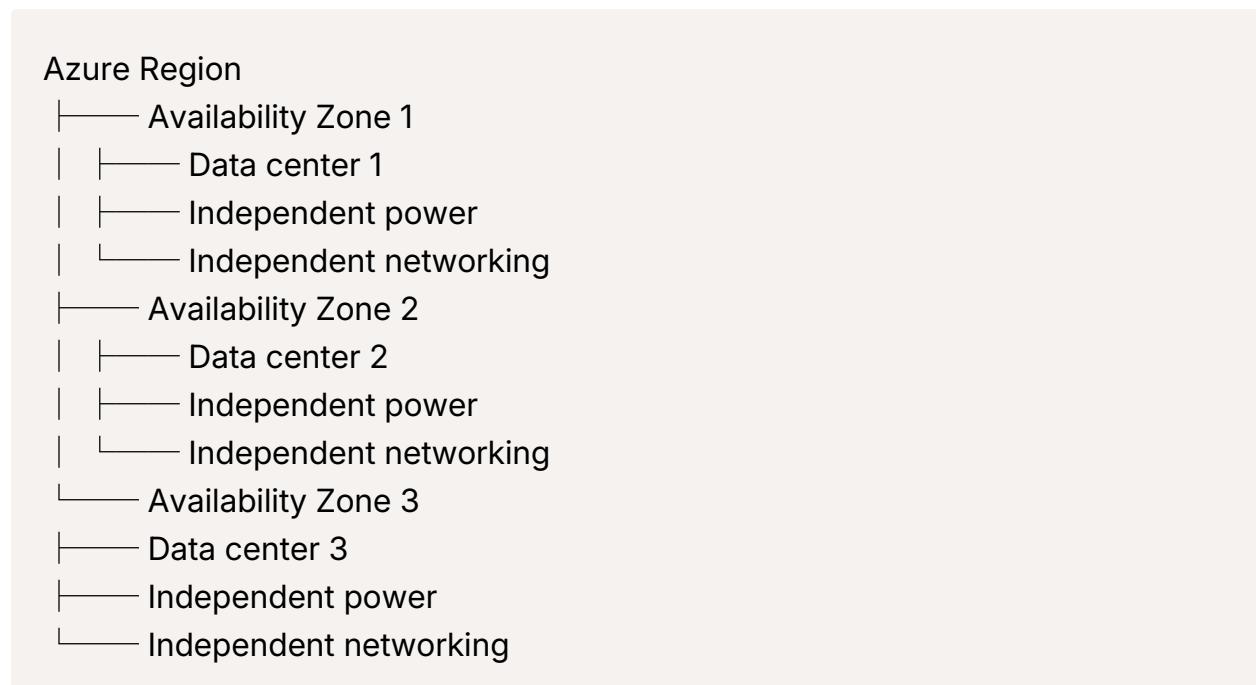
Answer:

Azure Availability Zones are physically separate locations within an Azure region, each with independent power, cooling, and networking infrastructure.

Key characteristics:

- **Physical separation**: Separate data centers

- **Low latency**: Connected via high-speed private fiber

- **Redundancy**: Isolated power and networking

- **Geographic spread**: Within same region (< 3ms latency)

Architecture:

```
Azure Region
    ├────── Availability Zone 1
    │   ├────── Data center 1
    │   ├────── Independent power
    │   └────── Independent networking
    ├────── Availability Zone 2
    │   ├────── Data center 2
    │   ├────── Independent power
    │   └────── Independent networking
    └────── Availability Zone 3
    ├────── Data center 3
    ├────── Independent power
    └────── Independent networking
```

Zone distribution:

- Zone 1, 2, 3 within region

- Not all regions have zones

- Zone-redundant services available

Resource support:

- **Zone redundant**: Replicate across zones

- **Zone resilient**: Deploy in specific zone

- **No zonal**: Standard deployment

SLA guarantees:

Configuration	SLA
Single VM	99.9%
2+ VMs in availability set	99.95%
2+ VMs in availability zones	99.99%

Comparison with Availability Sets:

Feature	Availability Zone Physical data	Availability Set
Scope	centers Complete data center	Logical grouping
Failure isolation	Potential data transfer charges	Partial hardware
Cost	Slightly higher Limited to zones	No additional cost
Latency		Minimal
Scale		More VMs possible

Best practices:

- Deploy critical applications across zones

- Use zone-redundant load balancers

- Implement cross-zone failover

- Test disaster scenarios

- Monitor zone availability

Limitations:

- Not available in all regions

- Limited zone count (typically 3)

- Data transfer between zones incurs charges

- Some services not zone-aware

---

49. What is Azure Service Bus?

Answer:

Azure Service Bus is a fully managed enterprise messaging service for reliable asynchronous communication between applications and services.

Messaging patterns:
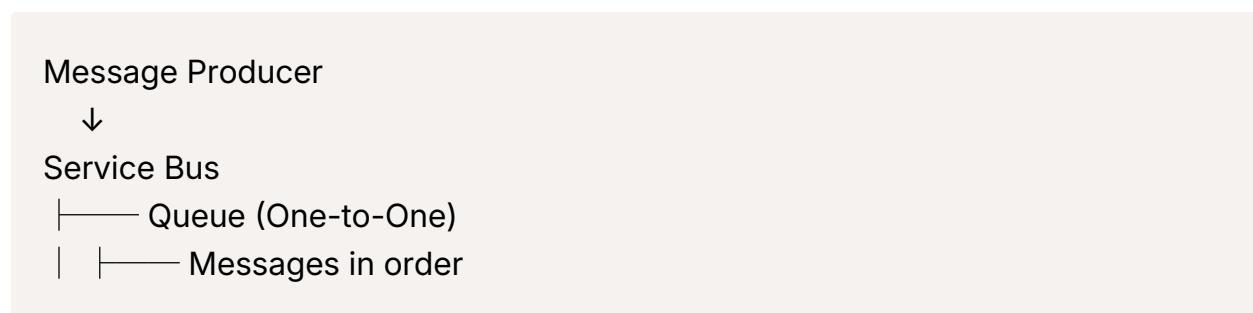
1. Queues
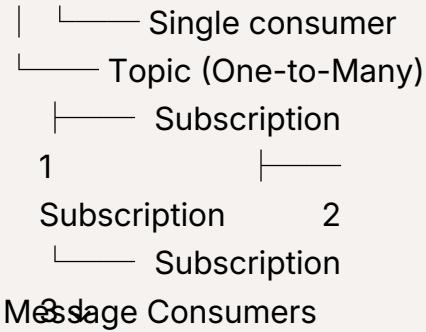
- One-to-one messaging

- FIFO order (First-In-First-Out)

- Single receiver per message

- Asynchronous processing

2. Topics and Subscriptions

- Publish-subscribe pattern

- One-to-many messaging

- Multiple subscribers per topic

- Message filtering

Architecture:

```
Message Producer
    ↓
Service Bus
  ├──── Queue (One-to-One)
  │   ├──── Messages in order
```

```
│      └─────── Single consumer
   └───── Topic (One-to-Many)
     ├────── Subscription
 1                 ├──────
Subscription        2
     └────── Subscription
Message Consumers
```

Key features:

Message properties:

- Time-to-live (TTL)

- Session ID for correlation

- Dead-letter queue for failed messages

- Duplicate detection

- Message deduplication

Delivery guarantees:

- **At least once**: Messages delivered at least one time

- **Exactly once**: Single message delivery

- **Session support**: Ordered message processing

Partitioning:

- Distribute load across multiple brokers

- Improve throughput

- Automatic partitioning

Filtering and actions:

SQL filters:

```
priority > 3 AND status = 'Processing'
```

Correlation filters:

```
CorrelationId = 'OrderId-123'
```

Actions:

- Set properties
- Remove properties
- SQL-like transformations

Message size:

- Standard tier: 256 KB
- Premium tier: 1 MB

SKUs:

SKU	Features
Basic	Queues only, 1GB/day throughput
Standard	Queues, Topics, 12.5GB/day
Premium	Enterprise, 80GB/day, dedicated capacity

Pricing models:

- Basic: Per message
- Standard: Per hour + overage
- Premium: Fixed capacity pricing

Use cases:

- Decoupling services
- Load leveling Order
- processing
- Event notification
- Job scheduling

Example C# usage:

```
// Sender
var client = new ServiceBusClient(connectionString);
var sender = client.CreateSender("queue-name");
await sender.SendMessageAsync(new ServiceBusMessage("Message content"));

// Receiver
var receiver = client.CreateReceiver("queue-name");
var message = await receiver.ReceiveMessageAsync();
await receiver.CompleteMessageAsync(message);
```

50. What is the Azure Marketplace?

Answer:

The Azure Marketplace is an online store providing a curated collection of software solutions, virtual machine images, services, and applications from Microsoft and third-party vendors.

Available resources:

Virtual Machine images:

- Pre-configured operating systems

- Database servers (SQL Server, Oracle, PostgreSQL)

- Web servers (Apache, Nginx)

- Business applications (SAP, Salesforce)

Solutions:

- Industry-specific solutions

- Reference architectures

- Complete deployments

- Multi-tier applications

Ser vices:

- Managed services

- Consulting services

- Professional services

- Support packages

Developer tools:

- IDEs and compilers

- DevOps tools

- Testing frameworks

- Cloud SDKs

Key advantages:

- **Pre-configured**: Reduces setup time

- **Tested**: Microsoft-verified solutions

- **Support**: Vendor support included

- **Deployment**: One-click deployment

- **Licensing**: BYOL or included licensing

Publishing options:

- **Free**: Trial or freemium

- **BYOL (Bring Your Own License)**: Use existing licenses

- **Paid**: Per-hour or subscription pricing

Integration:

- Direct deployment to Azure

- Pre-configured best practices

- Security baseline compliance

- Documentation and support

Finding solutions:

- Category browsing (AI, Databases, DevOps)

- Search functionality

- Vendor filtering

- Rating and reviews

Considerations:

- Verify vendor reputation

- Review support options

- Check licensing terms

- Confirm compatibility

- Test in non-production first

Use cases:

- Quick application deployment

- Vendor evaluation

- Marketplace applications

- Business solutions

- Development environment setup

Summary

These 50 Azure interview questions cover:

- **Foundational concepts**: Cloud computing, Azure services, deployment models
- **Core services**: VMs, storage, databases, networking
- **Intermediate topics**: Load balancing, DevOps, container management
- **Advanced concepts**: Security, disaster recovery, global distribution, automation

Preparation tips for MNC interviews:

1. **Understand the "why"**: Know reasons behind architectural decisions
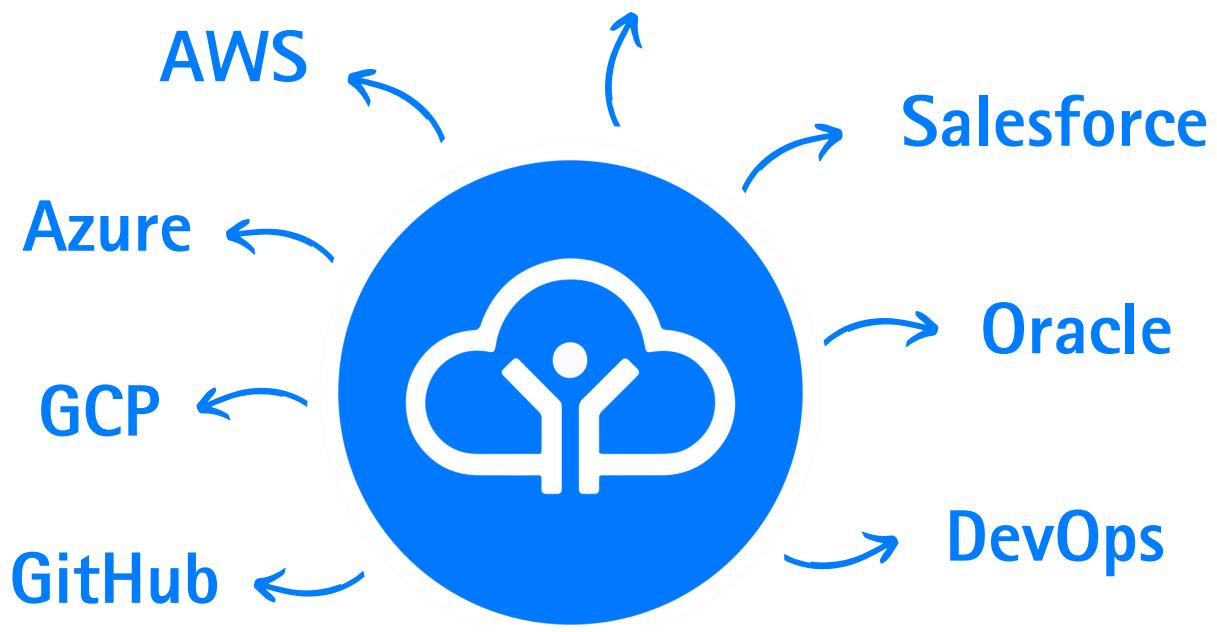
2. **Real-world scenarios**: Be ready to discuss practical implementations

3. **Cost optimization**: Demonstrate knowledge of cost-effective solutions

4. **Security practices**: Emphasize security in all responses

5. **Hands-on experience**: Practice with Azure portal and CLI

6. **Case studies**: Research company-specific Azure usage

7. **Integration patterns**: Understand how services work together

8. **Recent updates**: Stay current with Azure announcements

Key focus areas for interviews:

- Scalability and availability

- Security and compliance

- Cost optimization

- Disaster recovery

- DevOps practices

- Microservices architecture

- Hybrid cloud scenarios

- Performance optimization

Good luck with your Azure interview preparation!

FREE Vouchers

AWS

Azure

GCP

GitHub

Salesforce

Oracle

DevOps

YATRI CLOUD

SUBSCRIBE

Follow me on LinkedIn

to stay updated