Azure Scenarios - Medium

Scenario 11: Highly Available Web Application

A retail company’s e-commerce site gets 5,000 visitors/day with spikes during sales. The current single VM crashed during a flash sale. They need HA within a single region. The checkout process cannot go down. Budget is moderate.

Keywords to google: Availability Sets, Azure Load Balancer, VMSS, health probes, Application Gateway

---

Scenario 12: Three-Tier Application with Network Segmentation

A financial services company is deploying a 3-tier application (IIS frontend, Java app tier, SQL Server database). Security policy requires: no direct internet access to app or database tiers, all management via Bastion, micro-segmentation between tiers.

Keywords to google: VNet subnets, NSG rules, Application Security Groups, Azure Bastion, Private Endpoints

---

Scenario 13: Hub-Spoke Network for Multi-Department Organization

A company has 4 departments (Finance, HR, Engineering, Marketing), each with their own subscription. They share: Azure Firewall, ExpressRoute to on-prem, and DNS servers. Each department must be isolated from others but all must reach shared services and on-prem network.

Keywords to google: Hub-spoke topology, VNet peering, Azure Firewall, gateway transit, UDR

Scenario 14: Hybrid Identity Setup

A manufacturing company with 2,000 on-prem AD users is moving to Azure. Users must use the same credentials for on-prem and cloud. They need self-service password reset. Some users only need M365 access (no on-prem resources).

Keywords to google: Entra Connect, Password Hash Sync, self-service password reset, hybrid identity, Entra Connect Health

---

Scenario 15: Secure Internet Egress for All VMs

A company has 150 VMs across 5 VNets. Currently every VM has a public IP and connects to the internet directly. Security team mandates: no VM should have a public IP. All internet-bound traffic must go through a centralized firewall for inspection.

Keywords to google: Azure Firewall, forced tunneling, UDR, NAT Gateway, AzureFirewallSubnet

---

Scenario 16: Application Migration from On-Prem VMware to Azure

A retail company has 20 VMware VMs running their ERP system on-premises. They want to lift-and-shift to Azure IaaS. The VMs run a mix of Windows and Linux. Network connectivity to on-prem AD is required during and after migration.

Keywords to google: Azure Migrate, agentless VMware migration, replication, cutover, ExpressRoute

---

Scenario 17: Database Migration from On-Prem SQL Server to Azure SQL

A healthcare company runs SQL Server 2016 on-premises (2TB database). They want to migrate to Azure SQL Managed Instance. The database must remain available during migration with minimal downtime. HIPAA compliance required.

Keywords to google: Azure SQL Managed Instance, DMA Data Migration Assistant, DMS, online migration, Managed Instance networking

---

Scenario 18: Private Endpoints for All PaaS Services

A company uses Azure Storage, Azure SQL Database, Azure Key Vault, and Azure App Service. Currently all have public endpoints. Security policy requires all PaaS services to be accessible only from within the VNets — no public internet exposure.

Keywords to google: Azure Private Endpoint, Private Link, Private DNS zones, disable public access

---

Scenario 19: Multi-Region Web Application with Front Door

A SaaS company has users in US, Europe, and Asia. Their application is currently hosted only in East US. European users experience 200ms+ latency. They want global routing to nearest healthy region with automatic failover.

Keywords to google: Azure Front Door, multi-region deployment, geo-replication, health probes, WAF

Scenario 20: Centralized Logging and Monitoring

A company has 40 VMs across 3 subscriptions. Each team logs into individual VMs to check event logs. They need: all Windows Event Logs and Linux syslog centralized in one place, 90-day retention for ops, 7-year retention for compliance (cheap), single search interface.

Keywords to google: Azure Monitor, Log Analytics workspace, diagnostic settings, KQL, data collection rules, archive tier

---

Scenario 21: RBAC Implementation for Large Organization

A company with 3 Azure subscriptions needs: 2 admins with full access, 10 developers with VM access in dev and read-only in staging, 5 QA engineers with restart access in staging, nobody except admins can access prod. Use built-in roles where possible.

Keywords to google: Azure RBAC, built-in roles, custom roles, role assignments, scope hierarchy

---

Scenario 22: Conditional Access and Zero Trust

A company wants to enforce: MFA for all admin portal access, managed devices only for M365, MFA + manager approval for sign-ins from new countries, block legacy authentication, contractors can only access specific apps from specific IPs.

Keywords to google: Conditional Access, named locations, device compliance, legacy auth block, Entra ID P1

Scenario 23: Azure Policy for Governance

A company needs to enforce across all subscriptions: resources only in East US/Central US/West US, all storage accounts must enforce HTTPS, all resources must have CostCenter and Environment tags, no public Load Balancers, all SQL servers must have auditing enabled.

Keywords to google: Azure Policy, policy definitions, policy initiative, DeployIfNotExists, remediation tasks

---

Scenario 24: VM Backup Strategy with Compliance

A healthcare company has 20 production VMs. Requirements: RPO 4 hours for app VMs, 1 hour for database VMs, retention: 30 days daily + 12 months monthly + 7 years yearly, backups must be encrypted, database VMs must have application-consistent backups.

Keywords to google: Azure Backup, Recovery Services vault, backup policy, application-consistent backup, backup encryption, long-term retention

---

Scenario 25: IIS to App Service Migration

A company runs 3 .NET web applications on IIS VMs (Windows Server 2019). Each app has its own VM. The team spends hours weekly patching and managing VMs. Move to PaaS with zero code changes. Need: custom domain with HTTPS, auto-scale, deployment slots, VNet integration for backend database.

Keywords to google: Azure App Service, App Service plan, deployment slots, VNet integration, managed certificate, custom domain

---

Scenario 26: SQL Server VM to Azure SQL Managed Instance

A company runs SQL Server 2019 on an Azure VM. Problems: 8 hours/month on patching/backups/maintenance, CPU hits 100% during month-end reporting, they want read replicas without managing replication. Migrate to Azure SQL MI.

Keywords to google: Azure SQL Managed Instance, vCore purchasing model, General Purpose tier, read replicas, DMA, DMS

Scenario 27: ETL VMs to Data Factory and Functions

A company runs nightly ETL jobs on 2 VMs: SSIS packages extracting from 3 on-prem SQL databases, and Python scripts processing CSV files from FTP. Both VMs run 3 hours nightly, idle 21 hours. Replace with serverless/PaaS.

Keywords to google: Azure Data Factory, SSIS Integration Runtime, Azure Functions, blob trigger, self-hosted integration runtime

---

Scenario 28: Containerize Java App on Azure

A company has a Java Spring Boot application on 3 Tomcat VMs. They want to containerize and run on Azure without managing Kubernetes. Need: blue/green deployments, auto-scale, internal only (no public endpoint), logs to Log Analytics.

Keywords to google: Azure Container Apps, container registry, ingress internal, KEDA autoscaling, revision management

---

Scenario 29: Cross-Region DR with Azure Site Recovery

A company’s primary region is East US. They need DR in Central US: RTO 2 hours / RPO 1 hour for 8 critical VMs, RTO 24 hours / RPO 4 hours for 12 non-critical VMs, must be able to test DR without affecting production, failback must be supported.

Keywords to google: Azure Site Recovery, recovery plan, test failover, multi-VM consistency, reprotect

---

Scenario 30: Sentinel SIEM Implementation

A company with 300 Azure resources needs centralized SIEM: collect security logs from Entra ID, Defender for Cloud, Azure Firewall, and VMs, detect brute force attacks and impossible travel, auto-block source IPs and create incident tickets, build CISO dashboards.

Keywords to google: Microsoft Sentinel, data connectors, analytics rules, KQL, playbooks, workbooks, SOAR

Azure Architecture Scenarios — Complex (31-50)
