Exam AZ-101: Microsoft Azure Integration and Security – Skills Measured

Evaluate and perform server migration to Azure (15-20%)

Evaluate migration scenarios by using Azure Migrate

- discover and assess environment
- identify workloads that can and cannot be deployed
- identify ports to open
- identify changes to network
- identify if target environment is supported
- setup domain accounts and credentials

Migrate servers to Azure

- migrate by using Azure Site Recovery (ASR)
- migate using P2V
- configure storage
- create a recovery services vault
- prepare source and target environments
- backup and restore data
- deploy Azure Site Recovery (ASR) agent
- prepare virtual network

Implement and manage application services (20-25%)

Configure serverless computing

- create and manage objects
- manage a Logic App resource
- manage Azure Function app settings
- manage Event Grid
- manage Service Bus

Manage App Service Plans

- configure application for scaling
- enable monitoring and diagnostics
- configure App Service plans

Manage App services

- assign SSL Certificates
- configure application settings
- configure deployment slots
- configure Azure content delivery network (CDN) integration
- manage App service protection
- manage roles for an App service
- create and manage App Service environment

Implement advanced virtual networking (30-35%)

Implement application load balancing

- configure application gateway and load balancing rules
- implement front end IP configurations
- manage application load balancing

Implement Azure load balancer

- configure internal load balancer, load balancing rules, and public load balancer
- manage Azure load balancing

Monitor and manage networking

- monitor on-premises connectivity
- use network resource monitoring and Network Watcher
- manage external networking and virtual network connectivity

Integrate on-premises network with Azure virtual network

- create and configure Azure VPN Gateway
- create and configure site to site VPN
- configure Express Route
- verify on-premises connectivity
- manage on-premises connectivity with Azure

Secure identities (25-30%)

Implement Multi-Factor Authentication (MFA)

- enable MFA for an Azure AD tenant
- configure user accounts for MFA
- configure fraud alerts

- configure bypass options
- configure trusted IPs
- configure verification methods
- manage role-based access control (RBAC)
- implement RBAC policies
- assign RBAC Roles
- create a custom role
- configure access to Azure resources by assigning roles
- configure management access to Azure

Manage role-based access control (RBAC)

- create a custom role
- configure access to Azure resources by assigning roles
- configure management access to Azure
- troubleshoot RBAC
- implement RBAC policies
- assign RBAC roles

Implement Azure AD Privileged Identity Management (PIM)

- activate a PIM role
- configure just-in-time access, permanent access, PIM management access, and time-bound access
- create a Delegated Approver account
- enable PIM
- process pending approval requests