AZ-500: Microsoft Certified: Azure Security Engineer Associate

Course Outline

Note

The bullets that follow each of the skills measured are intended to illustrate how we are assessing that skill. Related topics may be covered in the exam

Skills at a glance

- Secure identity and access (15–20%)
- Secure networking (20–25%)
- Secure compute, storage, and databases (20–25%)
- Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel (30–35%)

Secure identity and access (15–20%)

Manage security controls for identity and access

- Manage Azure built-in role assignments
- Manage custom roles, including Azure roles and Microsoft Entra roles
- Implement and manage Microsoft Entra Permissions Management
- Plan and manage Azure resources in Microsoft Entra Privileged Identity Management, including settings and assignments
- Implement multi-factor authentication (MFA) for access to Azure resources
- Implement Conditional Access policies for cloud resources in Azure

Manage Microsoft Entra application access

- Manage access to enterprise applications in Microsoft Entra ID, including OAuth permission grants

- Manage Microsoft Entra app registrations
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage and use service principals
- Manage managed identities

Secure networking (20–25%)

Plan and implement security for virtual networks

- Plan and implement Network Security Groups (NSGs) and Application Security Groups (ASGs)
- Manage virtual networks by using Azure Virtual Network Manager
- Plan and implement user-defined routes (UDRs)
- Plan and implement Virtual Network peering or VPN gateway
- Plan and implement Virtual WAN, including secured virtual hub
- Secure VPN connectivity, including point-to-site and site-to-site
- Implement encryption over ExpressRoute
- Configure firewall settings on Azure resources
- Monitor network security by using Network Watcher

Plan and implement security for private access to Azure resources

- Plan and implement virtual network Service Endpoints
- Plan and implement Private Endpoints
- Plan and implement Private Link services
- Plan and implement network integration for Azure App Service and Azure Functions

- Plan and implement network security configurations for an App Service Environment (ASE)
- Plan and implement network security configurations for an Azure SQL Managed Instance

Plan and implement security for public access to Azure resources

- Plan and implement Transport Layer Security (TLS) to applications, including Azure App Service and API Management
- Plan, implement, and manage an Azure Firewall, including Azure Firewall Manager and firewall policies
- Plan and implement an Azure Application Gateway
- Plan and implement an Azure Front Door, including Content Delivery Network (CDN)
- Plan and implement a Web Application Firewall (WAF)
- Recommend when to use Azure DDoS Protection Standard

Secure compute, storage, and databases (20–25%)

Plan and implement advanced security for compute

- Plan and implement remote access to virtual machines, including Azure Bastion and just-in-time (JIT)
- Configure network isolation for Azure Kubernetes Service (AKS)
- Secure and monitor AKS
- Configure authentication for AKS
- Configure security monitoring for Azure Container Instances (ACIs)
- Configure security monitoring for Azure Container Apps (ACAs)
- Manage access to Azure Container Registry (ACR)

- Configure disk encryption, including Azure Disk Encryption (ADE), encryption at host, and confidential disk encryption
- Recommend security configurations for Azure API Management

Plan and implement security for storage

- Configure access control for storage accounts
- Manage storage account access keys
- Select and configure an appropriate method for access to Azure Files
- Select and configure an appropriate method for access to Azure Blob Storage
- Select and configure appropriate methods for protecting against data security threats, including soft delete, backups, versioning, and immutable storage
- Configure Bring your own key (BYOK)
- Enable double encryption at the Azure Storage infrastructure level

Plan and implement security for Azure SQL Database and Azure SQL Managed Instance

- Enable Microsoft Entra database authentication
- Enable database auditing
- Plan and implement dynamic masking
- Implement Transparent Data Encryption (TDE)
- Recommend when to use Azure SQL Database Always Encrypted

Secure Azure using Microsoft Defender for Cloud and Microsoft Sentinel (30–35%)

Implement and manage enforcement of cloud governance policies

- Create, assign, and interpret policies and initiatives in Azure Policy

- Configure Azure Key Vault network settings
- Configure access to Key Vault, including vault access policies and Azure Role Based Access Control
- Manage certificates, secrets, and keys
- Configure key rotation
- Perform backup and recovery of certificates, secrets, and keys
- Implement security controls to protect backups
- Implement security controls for asset management

Manage security posture by using Microsoft Defender for Cloud

- Identify and remediate security risks by using the Microsoft Defender for Cloud Secure Score and Inventory
- Assess compliance against security frameworks by using Microsoft Defender for Cloud
- Manage compliance standards in Microsoft Defender for Cloud
- Add custom standards to Microsoft Defender for Cloud
- Connect hybrid cloud and multi-cloud environments to Microsoft Defender for Cloud, including Amazon Web Services (AWS) and Google Cloud Platform (GCP)
- Implement and use Microsoft Defender External Attack Surface Management (EASM)

Configure and manage threat protection by using Microsoft Defender for Cloud

- Enable workload protection services in Microsoft Defender for Cloud
- Configure Microsoft Defender for Servers, Microsoft Defender for Databases, and Microsoft Defender for Storage
- Implement and manage agentless scanning for virtual machines in Microsoft Defender for Servers

- Implement and manage Microsoft Defender Vulnerability Management for Azure virtual machines
- Connect to and configure settings in Microsoft Defender for Cloud Devops Security, including GitHub, Azure DevOps, and GitLab

Configure and manage security monitoring and automation solutions

- Manage and respond to security alerts in Microsoft Defender for Cloud
- Configure workflow automation by using Microsoft Defender for Cloud
- Monitor network security events and performance data by configuring data collection rules (DCRs) in Azure Monitor
- Configure data connectors in Microsoft Sentinel
- Enable analytics rules in Microsoft Sentinel
- Configure automation in Microsoft Sentinel