Microsoft Certified: Azure Security Engineer Associate

(Exam AZ-500: Microsoft Azure Security Technology)

(Microsoft Certification Mapped Curriculum)

Manage identity and access
Manage Azure Active Directory (Azure AD) identities

- Create and manage a managed identity for Azure resources
- Manage Azure AD groups
- Manage Azure AD users
- Manage external identities by using Azure AD
- Manage administrative units

Manage secure access by using Azure AD

- Configure Azure AD Privileged Identity Management (PIM)
- Implement Conditional Access policies, including multifactor authentication
- Implement Azure AD Identity Protection
- Implement passwordless authentication
- Configure access reviews

Manage application access

- Create an app registration
- Configure app registration permission scopes
- Manage app registration permission consent
- Manage API permissions to Azure subscriptions and resources
- Configure an authentication method for a service principal

Manage access control

- Configure Azure role permissions for management groups, subscriptions, resource groups, and resources
- Interpret role and resource permissions

Assign built-in Azure AD roles

- Create and assign custom roles, including Azure roles and Azure AD roles

Implement platform protection
Implement advanced network security

- Secure the connectivity of hybrid networks
- Secure the connectivity of virtual networks
- Create and configure Azure Firewall
- Create and configure Azure Application Gateway
- Create and configure Azure Front Door
- Create and configure Web Application Firewall (WAF)
- Configure a resource firewall, including storage account, Azure SQL, Azure Key Vault, or Azure

App Service

- Configure network isolation for Web Apps and Azure Functions
- Implement Azure Service Endpoints
- Implement Azure Private Endpoints, including integrating with other services
- Implement Azure Private Links
- Implement Azure DDoS Protection

Configure advanced security for compute

- Configure Endpoint Protection for virtual machines (VMs)
- Implement and manage security updates for VMs
- Configure security for container services
- Manage access to Azure Container Registry
- Configure security for an Azure App Service
- Configure encryption at rest
- Configure encryption in transit

Manage security operations
Configure centralized policy management

- Configure a custom security policy
- Create a policy initiative
- Configure security settings and auditing by using Azure Policy

Configure and manage threat protection

- Configure Microsoft Defender for Servers (not including Microsoft Defender for Endpoint)
- Evaluate vulnerability scans from Microsoft Defender for Servers

Configure Microsoft Defender for SQL

- Use the Microsoft Threat Modeling Tool

Configure and manage security monitoring solutions

- Create and customize alert rules by using Azure Monitor
- Configure diagnostic logging and log retention by using Azure Monitor
- Monitor security logs by using Azure Monitor
- Create and customize alert rules in Microsoft Sentinel
- Configure connectors in Microsoft Sentinel
- Evaluate alerts and incidents in Microsoft Sentinel

Secure data and applications
Configure security for storage

- Configure access control for storage accounts
- Configure storage account access keys
- Configure Azure AD authentication for Azure Storage and Azure Files
- Configure delegated access

Configure security for data

- Enable database authentication by using Azure AD
- Enable database auditing
- Configure dynamic masking on SQL workloads
- Implement database encryption for Azure SQL Database
- Implement network isolation for data solutions, including Azure Synapse Analytics and Azure

Configure and manage Azure Key Vault

- Create and configure Key Vault
- Configure access to Key Vault
- Manage certificates, secrets, and keys
- Configure key rotation
- Configure backup and recovery of certificates, secrets, and keys