Microsoft Certified: Azure Security Engineer Associate – Skills Measured

This document contains the skills measured on the exams associated with this certification. It does not include any upcoming or recent changes that have been made to those skills. For more information about upcoming or recent changes, see the associated exam details page(s).

NOTE: The bullets that appear below each of the skills measured are intended to illustrate how we are assessing that skill. This list is NOT definitive or exhaustive.

NOTE: Most questions cover features that are General Availability (GA). The exam may contain questions on Preview features if those features are commonly used.

Exam AZ-500: Microsoft Azure Security Technologies

Manage identity and access (30-35%)

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

- integrate single sign-on (SSO) and identity providers for authentication
- 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 (15-20%)

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 Firewall Manager
- 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 Azure 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 serverless compute
- configure security for an Azure App Service
- configure encryption at rest
- configure encryption in transit

Manage security operations (25-30%)

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 Azure Defender for Servers (not including Microsoft Defender for Endpoint)
- evaluate vulnerability scans from Azure Defender
- configure Azure 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 Azure Sentinel
- configure connectors in Azure Sentinel
- evaluate alerts and incidents in Azure Sentinel

Secure data and applications (25–30%)

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 Cosmos DB

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