Exam AZ-500: Microsoft Azure Security Technologies – Skills Measured

This exam will be updated on September 29, 2021. Following the current exam guide, we have included a version of the exam guide with Track Changes set to “On,” showing the changes that will be made to the exam on that date.

Audience Profile

Candidates for this exam should have subject matter expertise implementing security controls and threat protection, managing identity and access, and protecting data, applications, and networks.

Responsibilities for an Azure Security Engineer include maintaining the security posture, identifying and remediating vulnerabilities by using a variety of security tools, implementing threat protection, and responding to security incident escalations.

Azure Security Engineers often serve as part of a larger team dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure.

A candidate for this exam should be familiar with scripting and automation, and should have a deep understanding of networking and virtualization. A candidate should also have a strong familiarity with cloud capabilities, Azure products and services, and other Microsoft products and services.

Skills Measured

NOTE: The bullets that follow 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.

Manage identity and access (30-35%)

Manage Azure Active Directory identities

- configure security for service principals
- manage Azure AD directory groups
- manage Azure AD users
- manage administrative units
- configure password writeback
- configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless

- transfer Azure subscriptions between Azure AD tenants

Configure secure access by using Azure AD

- monitor privileged access for Azure AD Privileged Identity Management (PIM)
- configure Access Reviews
- configure PIM
- implement Conditional Access policies including Multi-Factor Authentication (MFA)
- configure Azure AD identity protection

Manage application access

- create App Registration
- configure App Registration permission scopes
- manage App Registration permission consent
- manage API access to Azure subscriptions and resources

Manage access control

- configure subscription and resource permissions
- configure resource group permissions
- configure custom RBAC roles
- identify the appropriate role
- interpret permissions

Implement platform protection (15-20%)

Implement advanced network security

- secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
- configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- create and configure Azure Firewall
- implement Azure Firewall Manager
- configure Azure Front Door service as an Application Gateway
- configure a Web Application Firewall (WAF) on Azure Application Gateway
- configure Azure Bastion
- configure a firewall on a storage account, Azure SQL, Key Vault, or App Service
- implement Service Endpoints
- implement DDoS protection

Configure advanced security for compute

- configure endpoint protection
- configure and monitor system updates for VMs
- configure authentication for Azure Container Registry
- configure security for different types of containers
- implement Azure Disk Encryption
- configure authentication and security for Azure App Service

Manage security operations (25-30%)

Monitor security by using Azure Monitor

- create and customize alerts
- monitor security logs by using Azure Monitor
- configure diagnostic logging and log retention

Monitor security by using Azure Security Center

- evaluate vulnerability scans from Azure Security Center
- configure Just in Time VM access by using Azure Security Center
- configure centralized policy management by using Azure Security Center
- configure compliance policies and evaluate for compliance by using Azure Security Center
- configure workflow automation by using Azure Security Center

Monitor security by using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel
- evaluate results from Azure Sentinel
- configure a playbook

Configure security policies

- configure security settings by using Azure Policy
- configure security settings by using Azure Blueprint

Secure data and applications (20-25%)

Configure security for storage

- configure access control for storage accounts
- configure key management for storage accounts
- configure Azure AD authentication for Azure Storage

- configure Azure AD Domain Services authentication for Azure Files
- create and manage Shared Access Signatures (SAS)
- configure Storage Service Encryption
- configure Azure Defender for Storage

Configure security for databases

- enable database authentication
- enable database auditing
- configure Azure Defender for SQL
- implement database encryption

Configure and manage Key Vault

- manage access to Key Vault
- manage permissions to secrets, certificates, and keys
- manage certificates
- manage secrets
- configure key rotation
- backup and restore of Key Vault items
- configure Azure Defender for Key Vault

The exam guide below shows the changes that will be implemented on September 29, 2021.

Audience Profile

Candidates for this exam should have subject matter expertise implementing Azure security controls that protect identity, access, data, applications, and networks in cloud and hybrid environments as part of an end-to-end infrastructure~~and threat protection, managing identity and access, and protecting data, applications, and networks~~.

Responsibilities for an Azure Security Engineer include ~~maintaining~~ managing the security posture, identifying and remediating vulnerabilities, performing threat modeling~~ by using a variety of security tools~~, implementing threat protection, and responding to security incident escalations.

Azure Security Engineers often serve as part of a larger team to plan and implement cloud-based management and security~~ dedicated to cloud-based management and security and may also secure hybrid environments as part of an end-to-end infrastructure~~.

~~A c~~Candidates for this exam should have practical experience in administration of Azure and hybrid environments. Candidates should have experience with infrastructure as code,~~ and~~

security operations processes, cloud capabilities, and Azure services~~. The Azure Security Engineer should have a strong familiarity withbe familiar with scripting and automation, and should have a deep understanding of networking and virtualization. A candidate should also have a strong familiarity with cloud capabilities, Azure products and services, and other Microsoft products and services~~.

Skills Measured

NOTE: The bullets that follow 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.

Manage identity and access (30-35%)

Manage Azure Active Directory (Azure AD) identities

- create and manage a managed identity for Azure resources~~Configure security for service principals~~
- manage Azure AD ~~directory~~groups
- manage Azure AD users
- manage external identities by using Azure AD
- manage administrative units
- ~~configure password writeback~~
- ~~configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless~~
- ~~transfer Azure subscriptions between Azure AD tenants~~

Manage~~Configure~~ secure access by using Azure AD

- ~~monitor privileged access for Azure AD Privileged Identity Management (PIM)~~
- ~~configure Access Reviews~~
- configure Azure AD Privileged Identity Management (PIM)
- implement Conditional Access policies, including multifactor authentication
- implement~~Configure~~ Azure AD i~~I~~dentity P~~p~~rotection
- implement passwordless authentication
- configure access reviews

Manage application access

- integrate single sign-on (SSO) and ~~multiple~~ identity providers for authentication
- create an a~~A~~pp r~~R~~egistration
- configure a~~A~~pp r~~R~~egistration permission scopes
- manage a~~A~~pp r~~R~~egistration permission consent

- manage API permissions~~access~~ 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
- ~~configure subscription and resource permissions~~
- ~~configure resource group permissions~~
- ~~configure custom RBAC roles~~
- ~~identify the appropriate role~~
- 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 ~~virtual~~ hybrid networks ~~(VPN authentication, Express Route encryption)~~
- secure the connectivity of virtual networks~~Configure Network Security Groups (NSGs) and Application Security Groups (ASGs)~~
- create and configure Azure Firewall
- create and configure ~~Implement~~ Azure Firewall Manager
- create and configure Azure ~~Configure Azure Front Door service as an~~ Application Gateway
- create and configure Azure Front Door
- create and configure ~~a~~ Web Application Firewall (WAF) ~~on Azure Application Gateway~~
- ~~configure Azure Bastion~~
- configure a resource firewall, including ~~on a~~ 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 P~~p~~rotection

Configure advanced security for compute

- configure Azure E~~e~~ndpoint P~~p~~rotection for virtual machines (VMs)
- ~~configure and monitor system~~Implement and manage security updates for VMs
- ~~configure authentication for Azure Container Registry~~
- configure security for ~~different types of~~ 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
- ~~implement Azure Disk Encryption~~
- ~~configure authentication and security for Azure App Service~~
  - ~~configure SSL/TLS certs~~
  - ~~configure authentication for Azure Kubernetes Service~~
  - ~~configure automatic updates~~

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

~~**Monitor security by using Azure Monitor**~~

- ~~create and customize alerts~~
- ~~monitor security logs by using Azure Monitor~~
- ~~configure diagnostic logging and log retention~~

Configure and manage threat protection~~**Monitor security by using Azure Security Center**~~

- configure Azure Defender for Servers (not including Microsoft Defender for Endpoint)
- evaluate vulnerability scans from Azure ~~Security Center~~Defender
- configure Azure Defender for SQL
- use the Microsoft Threat Modeling Tool
- ~~configure centralized policy management by using Azure Security Center~~
- ~~configure compliance policies and evaluate for compliance by using Azure Security Center~~
- ~~configure workflow automation by using Azure Security Center~~

Configure and manage security monitoring solutions~~**Monitor security by using Azure Sentinel**~~

- 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 ~~data sources to~~connectors in Azure Sentinel
- evaluate ~~results from~~alerts and incidents in Azure Sentinel
- ~~configure a playbook~~

~~Configure security policies~~

- ~~configure security settings by using Azure Policy~~
- ~~configure security settings by using Azure Blueprint~~

Secure data and applications (25~~0~~–30~~25~~%)

Configure security for storage

- configure access control for storage accounts
- configure ~~key management for~~ storage account access keys
- configure Azure AD authentication for Azure Storage and Azure Files
- ~~configure Azure AD Domain Services authentication for Azure Files~~
- configure delegated access
- ~~configure Storage Service Encryption~~
- ~~configure Azure Defender for Storage~~

Configure security for databases

- enable database authentication by using Azure AD
- enable database auditing
- configure dynamic masking on SQL workloads
- ~~configure Azure Defender for SQL~~
- 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 ~~Manage~~ access to Key Vault
- ~~manage permissions to secrets, certificates, and keys~~
  - ~~configure RBAC usage in Azure Key Vault~~
- manage certificates, secrets, and keys
- ~~manage secrets~~
- configure key rotation

- configure ~~B~~backup and recovery of certificates, secrets, and keys~~restore of Key Vault items~~
- ~~configure Azure Defender for Key Vault~~