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

This exam will be updated on June 2, 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 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.

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
- activate and 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
    - apply principle of least privilege
- interpret permissions
    - check access

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, KeyVault, 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 vulnerability management
    - configure isolation for AKS
    - configure security for container registry
- 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%)

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 by using Azure Sentinel

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)
    - create a shared access policy for a blob or blob container
- configure Storage Service Encryption
- configure Azure Defender for Storage

Configure security for databases

- enable database authentication
- enable database auditing
- configure Azure Defender for SQL
    - configure Azure SQL Database Advanced Threat Protection
- implement database encryption
    - implement Azure SQL Database Always Encrypted

Configure and manage Key Vault

- manage access to Key Vault
- manage permissions to secrets, certificates, and keys
    - configure RBAC usage in Azure Key Vault
- 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 June 2, 2021.

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 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.

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
- ~~Activate and c~~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
    - apply principle of least privilege
- interpret permissions
    - check access

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, KeyVault, 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 vulnerability management
    - configure isolation for AKS
    - configure security for container registry
- 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%)

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 by using Azure Sentinel

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)
    - create a shared access policy for a blob or blob container
- configure Storage Service Encryption
- configure Azure Defender for Storage

Configure security for databases

- enable database authentication

- enable database auditing
- configure Azure Defender for SQL
    - configure Azure SQL Database Advanced Threat Protection
- implement database encryption
    - implement Azure SQL Database Always Encrypted

Configure and manage Key Vault

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