Microsoft Azure Security

Description

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 in cloud and hybrid environments as part of an end-to-end infrastructure.

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 or hybrid environments as part of an end-to-end infrastructure.

A candidate for this exam should have strong skills in scripting and automation; a deep understanding of networking, virtualization, and cloud N-tier architecture; and a strong familiarity with cloud capabilities and products and services for Azure, plus other Microsoft products and services.

Skills Measured

- Manage identity and access (20-25%)
- Implement platform protection (35-40%)
- Manage security operations (15-20%)
- Secure data and applications (30-35%)

Course Content

Manage identity and access (20-25%)

Configure Azure Active Directory for workloads

- create App Registration
- configure App Registration permission scopes
- manage App Registration permission consent

- configure Multi-Factor Authenticationsettings
- manage Azure AD directorygroups
- manage Azure AD users
- install and configure Azure AD Connect
- configure authentication methods
- implement Conditional Accesspolicies
- configure Azure AD identityprotection

Configure Azure AD Privileged Identity Management

- monitor privileged access
- configure Access Reviews
- activate Privileged IdentityManagement

Configure Azure tenant security

- transfer Azure subscriptions between Azure AD tenants
- manage API access to Azure subscriptions and resources

Implement platform protection (35-40%)

Implement network security

- configure virtual networkconnectivity
- configure Network Security Groups (NSGs)
- create and configure AzureFirewall
- create and configure Azure Front Door service
- create and configure application security groups
- configure remote accessmanagement
- configure baseline
- configure resource firewall

Implement host security

- configure endpoint security within the VM
- configure VM security
- harden VMs in Azure
- configure system updates for VMs in Azure
- configure baseline

Configure container security

- configure network
- configure authentication
- configure container isolation
- configure AKS security
- configure container registry
- implement vulnerability management

Implement Azure Resource management security

- create Azure resource locks
- manage resource group security
- configure Azure policies
- configure custom RBAC roles
- configure subscription and resource permissions

Manage security operations (15-20%)

Configure security services

- configure Azure Monitor
- configure diagnostic logging and log retention
- configure vulnerability scanning

Configure security policies

- configure centralized policy management by using Azure Security Center
- configure Just in Time VM access by using Azure Security Center

Manage security alerts

- create and customize alerts
- review and respond to alerts and recommendations
- configure a playbook for a security event by using Azure Sentinel
- investigate escalated security incidents

Secure data and applications (25-30%)

Configure security policies to manage data

- configure data classification
- configure data retention

- configure data sovereignty

Configure security for data infrastructure

- enable database authentication
- enable database auditing
- configure Azure SQL Database Advanced Threat Protection
- 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 security for HDInsight
- configure security for CosmosDB
- configure security for Azure Data Lake

Configure encryption for data at rest

- implement Azure SQL Database Always Encrypted
- implement database encryption
- implement Storage Service Encryption
- implement disk encryption

Configure application security

- configure SSL/TLS certs
- configure Azure services to protect web apps
- create an application securitybaseline

Configure and manage Key Vault

- manage access to KeyVault
- manage permissions to secrets, certificates, and keys
- configure RBAC usage in Azure Key Vault
- manage certificates
- manage secrets
- configure key rotation

Manage identity and access (30-35%)

Manage Azure Active Directory identities

- configure security for serviceprincipals
- manage Azure AD directorygroups
- manage Azure AD users
- configure password writeback
- configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless (not ADFS)
- transfer Azure subscriptions between Azure AD tenants

Configure secure access by using Azure AD ~~Privileged Identity Management~~

- monitorprivilegedaccessforAzureADPrivilegedIdentityManagement(PIM)
- configure Access Reviews
- activate and configure PIM
- implementConditionalAccesspoliciesincludingMulti-FactorAuthentication(MFA)
- configure Azure AD identityprotection

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 grouppermissions
- configure custom RBACroles
- identify the appropriate role
- apply principle of leastprivilege
- interpret permissions
- check access

Implement platform protection (15-20%)

Implement advanced network security

- Secure the connectivity of virtual networks
    - VPN authentication

- BYO Key for Express Route encryption
- Point to site
- Site to site

- configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- create and configure Azure Firewall
- 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

Configure advanced security for compute

- configure endpoint protection
- configure and monitor system updates for VMs
- configure authentication for containers
- configure security for different types of containers
- implement vulnerability management
- configure isolation for AKS
- configure security for container registry
- implement Azure Disk Encryption
- configure security for Azure App Service
- configure SSL/TLS certs
- configure authentication
- configure automatic updates
- configure subscription and resource permissions

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

Monitor security by using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel ~~to parse logs~~
- evaluate results from AzureSentinel
- configure a playbook for a security event 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 data classification
- 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 security for databases

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

Configure and manage Key Vault

- manage access to KeyVault
- 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

Comparison between original guide and new study guide

Old Objective	New Objective(s)
1.1. Configure Azure Active Directory for workloads	**1.1** Manage Azure Active Directory identities **1.2** Configure secure access by using Azure AD **1.3** Manage application access
1.2. Configure Azure AD Privileged Identity Management	1.2 Configure secure access by using Azure AD
1.3. Configure Azure tenant security	1.1 Manage Azure Active Directory identities 1.3 Manage application access
2.1. Implement network security	2.1 Implement advanced network security
2.2. Implement host security	2.2 Configure advanced security for compute
2.3. Configure container security	2.2 Configure advanced security for compute
2.4. Implement Azure Resource management security	1.4 Manage access control
3.1. Configure security services	**3.1** Monitor security by using Azure Monitor **3.2** Monitor security by using Azure Security Center
3.2. Configure security policies	3.2 Monitor security by using Azure Security Center
3.3. Manage security alerts	**3.2** Monitor security by using Azure Security Center **3.3** Monitor security by using Azure Sentinel
~~4.1 Configure security policies to manage data~~	no match
4.2. Configure security for data infrastructure	**4.1** Configure security for storage **4.2** Configure security for databases
4.3. Configure encryption for data at rest	2.2 Configure advanced security for compute
	4.1 Configure security for storage 4.3 Configure and manage Key Vault

4.4. Implement security for application delivery	1.3 Manage application access
4.5. Configure application security	2.2 Configure advanced security for compute
4.6. Configure and manage Key Vault	4.3 Configure and manage Key Vault

Follow On Courses

Microsoft Certified: Azure DevOps Engineer Expert