



**Microsoft Azure Security Technologies  
Study Guide  
Exam AZ-500**

## Contents at a glance

Chapter 1 **Manage identity and access**

Chapter 2 **Implement platform protection**

Chapter 3 **Manage security operations**

Chapter 4 **Secure data and applications**

## Contents

### Chapter 1 Manage identity and access

#### Skill 1.1: Manage Azure Active Directory identities

- Configure security for service principals

- Manage Azure AD directory groups

- Manage Azure AD users

- Configure password writeback

- Configure authentication methods including password hash and Pass Through Authentication (PTA), OATH, and passwordless authentication

- Transfer Azure subscriptions between Azure AD tenants

#### Skill 1.2: Configure secure access by using Azure AD

- Monitor privileged access for Azure AD Privileged Identity Management (PIM)

- Configure access reviews

- Activate and configure PIM

# ExamLabs

Implement conditional access policies including multifactor authentication

Administer MFA users

Configure Azure AD Identity Protection

## Skill 1.3: Manage application access

Create app registrations

Configure app registration permission scopes

Manage app registration permission consent

Manage API access to Azure subscriptions and resources

## Skill 1.4: Manage access control

Configure subscription and resource permissions

Configure resource group permissions

Identify the appropriate role

Apply the principle of least privilege

Configure custom RBAC roles

Interpret permissions

Check access

Thought experiment answers

Chapter summary

## Chapter 2 Implement platform protection

### Skill 2.1: Implement advanced network security

Overview of Azure network components

Secure the connectivity of virtual networks

Configure network security groups and Application Security Groups

Create and configure Azure Firewall

Configure Azure Front Door service as an application gateway

Configure Web Application Firewall (WAF) on Azure

# ExamLabs

- Application Gateway
- Configure Azure Bastion
- Configure resource firewall
- Implement service endpoint
- Implement DDoS

## Skill 2.2: Configure advanced security for compute

- Configure endpoint security within the VM
- Configure system updates for VMs in Azure
- 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

Thought experiment answers

Chapter summary

## **Chapter 3 Manage security operations**

### Skill 3.1: Configure security services

- Configure Azure Monitor
- Create and customize alerts
- Configure diagnostic logging and log retention
- Monitoring security logs by using Azure Monitor

### Skill 3.2: 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

# ExamLabs

Configure compliance policies and evaluate for compliance by using Azure Security Center

## Skill 3.3: Monitor security by using Azure Sentinel

Introduction to Azure Sentinel's architecture

Configure Data Sources to Azure Sentinel

Create and customize alerts

Configure a Playbook for a security event by using Azure Sentinel

Evaluate results from Azure Sentinel

## Skill 3.4: Configure security policies

Configure security settings by using Azure Policy

Configure security settings by using Azure Blueprint

Thought experiment answers

Chapter summary

## Chapter 4 Secure data and applications

### Skill 4.1: Configure security for storage

Configure access control for storage accounts

Configure key management for storage accounts

Create and manage Shared Access Signatures (SAS)

Create a stored access policy for a blob or blob containers

Configure Azure AD authentication for Azure Storage

Configure Azure AD Domain Services authentication for Azure Files

Configure Storage Service Encryption

Advanced Threat Protection for Azure Storage

### Skill 4.2: Configure security for databases

Enable database authentication

Enable database auditing

Configure Azure SQL Database Advanced Threat

# ExamLabs

Protection

Implement database encryption

Implement Azure SQL Database Always Encrypted

Skill 4.3: Configure and manage Key Vault

Manage access to Key Vault

Key Vault firewalls and virtual networks

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

Thought experiment answers

Chapter summary