

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

## **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 Authentication settings
- manage Azure AD directory groups
- manage Azure AD users
- install and configure Azure AD Connect
- configure authentication methods
- implement Conditional Access policies
- configure Azure AD identity protection

### **Configure Azure AD Privileged Identity Management**

- monitor privileged access
- configure Access Reviews
- activate Privileged Identity Management

### **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 network connectivity
- configure Network Security Groups (NSGs)
- create and configure Azure Firewall
- create and configure Azure Front Door service
- create and configure application security groups
- configure remote access management
- 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 Security Center
- 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 Cosmos DB
- 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 security baseline

### **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