KPMG Learning Academy

Microsoft Azure Security Technologies Training (AZ-500) Course Outline

Module 1: Manage Identity and Access –

This module covers Azure Active Directory, Azure Identity Protection, Enterprise Governance, Azure AD PIM, and Hybrid Identity.

Lessons

- Azure Active Directory
- Azure Identity Protection
- Enterprise Governance
- Azure AD Privileged Identity Management
- Hybrid Identity

Lab : Role-Based Access Control

Lab : Azure Policy

Lab : Resource Manager Locks

Lab : MFA, Conditional Access and AAD Identity Protection

Lab : Azure AD Privileged Identity Management

Lab : Implement Directory Synchronization

After completing this module, students will be able to:

- Implement enterprise governance strategies including role-based access control, Azure policies, and resource locks.
- Implement an Azure AD infrastructure including users, groups, and multi-factor authentication.
- Implement Azure AD Identity Protection including risk policies, conditional access, and access reviews.
- Implement Azure AD Privileged Identity Management including Azure AD roles and Azure resources.
- Implement Azure AD Connect including authentication methods and on-premises directory synchronization.

Module 2: Implement Platform Protection –

This module covers perimeter, network, host, and container security.

Lessons

- Perimeter Security
- Network Security
- Host Security
- Container Security

Lab : Network Security Groups and Application Security Groups

Lab : Azure Firewall Lab : Configuring and Securing ACR and AKS

After completing this module, students will be able to:

- Implement perimeter security strategies including Azure Firewall.
- Implement network security strategies including Network Security Groups and Application Security Groups.
- Implement host security strategies including endpoint protection, remote access management, update management, and disk encryption.
- Implement container security strategies including Azure Container Instances, Azure Container Registry, and Azure Kubernetes.

Module 3: Secure Data and Applications –

This module covers Azure Key Vault, application security, storage security, and SQL database security.

Lessons

- Azure Key Vault
- Application Security
- Storage Security
- SQL Database Security

Lab : Key Vault (Implementing Secure Data by setting up Always Encrypted)

Lab : Securing Azure SQL Database

Lab : Service Endpoints and Securing Storage

After completing this module, students will be able to:

- Implement Azure Key Vault including certificates, keys, and secretes.
- Implement application security strategies including app registration, managed identities, and service endpoints.
- Implement storage security strategies including shared access signatures, blob retention policies, and Azure Files authentication.
- Implement database security strategies including authentication, data classification, dynamic data masking, and always encrypted.

Module 4: Manage Security Operations –

This module covers Azure Monitor, Azure Security Centre, and Azure Sentinel.

Lessons

- Azure Monitor
- Azure Security Centre
- Azure Sentinel

Lab : Azure Monitor

Lab : Azure Security Centre

Lab : Azure Sentinel

After completing this module, students will be able to:

- Implement Azure Monitor including connected sources, log analytics, and alerts.
- Implement Azure Security Centre including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.