AZ-500T00: Microsoft Azure Security Technologies Associate Training

Duration: 4 Days

Course Content:

AZ-500T00: Microsoft Azure Security Technologies Associate (Security Engineer) Training is aimed at professionals to help them gain skills and knowledge required to maintain the security posture, implement security control, and recognize and remediate vulnerabilities with the help of various security tools. This technical course contains different essential topics, including virtualization, automation, and cloud N-tier architecture. Our enterprise training program is best for organizations and companies. It helps individuals enhance their skills and prepare for the AZ-500: Microsoft Azure Security Technologies exam. This program teaches the right techniques to recognize Azure data mechanisms and demonstrate specialized data classifications. You will also learn the leading methodologies to protect internet protocols and the main steps to implement them on Azure.

This training is designed based on the objectives of the course variant AZ-500T00-A.

Prerequisites for this training

The candidates preparing and appearing AZ-500 exam must understand networking, skills in scripting and automation, understanding of virtualization, familiarity with cloud N-tier architecture etc. The candidates are also required to have knowledge and experience in using cloud capabilities and Microsoft products / services including those of Azure.

Who should attend this course?

The Microsoft Azure Security Technologies Training is suited for professionals who have at least one year of hands-on experience with security controls for workloads on Azure.

What you will learn

- Understanding specialized Azure data classifications
- Understanding Azure security features and services
- Learning about the implementation of Secure Internet protocols on Azure
- Identifying data protection methods in Azure
- Implementing data encryption mechanisms in Azure

Curriculum

Module 1: Manage Identity and Access

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

Lesson

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

- Enterprise Governance

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.

Lesson

- 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.

Lesson

- 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 Center, and Azure Sentinel.

Lesson

- Azure Monitor
- Azure Security Center
- Azure Sentinel

Lab: Azure Monitor

Lab: Azure Security Center

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 Center including policies, recommendations, and just in time virtual machine access.
- Implement Azure Sentinel including workbooks, incidents, and playbooks.

For any query ***Contact Us - MicrotekLearning***