TechyEdz Solutions

Training | Consulting | Developement | Outsourcing

Azure Security (AZ-500)

☎ 9032803832

9032803832

contact@techyedz.com

www.techyedz.com

Azure - Microsoft Azure Security Technologies (AZ-500)

Course Overview:

This learning path is designed to help you and your team prepare for the AZ-500 Microsoft Azure Security Technologies exam. Even if you aren’t planning to take the exam, these courses and hands-on labs will help you get started on your way to deploying and managing Microsoft Azure security technologies.

The AZ-500 exam is part of Microsoft’s new role-based certification program. Candidates who pass the AZ-500 exam will earn the Microsoft Certified: Azure Security Engineer Associate certification.

The AZ-500 exam tests your knowledge in four different subject areas, and that’s how this learning path is structured. We’ll start with managing identities and access. Next, we’ll get into implementing platform protection, which will include topics like Network Security Groups, Azure Firewalls, Container Security, and much more. You will then learn about managing security options using tools like Azure Monitor, the Azure Security Center, and Log Analytics. Rounding out the learning path, you’ll learn how to secure data and applications by configuring security policies, enabling auditing, leveraging Key Vault, and many other topics.

Course Outline:

Manage identity and access

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), OAuth, and passwordless
- transfer Azure subscriptions between Azure AD tenants

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
- implement Conditional Access policies including Multi-Factor Authentication (MFA)
- configure Azure AD identity protection

3. Manage application access

- create App Registration
- configure App Registration permission scopes
- manage App Registration permission consent
- manage API access to Azure subscriptions and resources

4. Manage access control

- configure subscription and resource permissions
- configure resource group permissions
- configure custom RBAC roles
- identify the appropriate role
- apply principle of least privilege
- interpret permissions
- check access

Implement platform protection

1. Implement advanced network security

- secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
- 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, KeyVault, or App Service
- implement Service Endpoints
- implement DDoS

2. Configure advanced security for compute

- configure endpoint protection

- configure and monitor system updates for VMs
- configure authentication for Azure Container Registry
- configure security for different types of containers
- implement vulnerability management
- configure isolation for AKS
- configure security for container registry
- implement Azure Disk Encryption
- configure authentication and security for Azure App Service
- configure SSL/TLS certs
- configure authentication for Azure Kubernetes Service
- configure automatic updates

Manage security operations

1. Monitor security by using Azure Monitor

- create and customize alerts
- monitor security logs by using Azure Monitor
- configure diagnostic logging and log retention

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
- configure compliance policies and evaluate for compliance by using Azure Security Center

3. Monitor security by using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel
- evaluate results from Azure Sentinel
- configure a playbook for a security event by using Azure Sentinel

4. Configure security policies

- configure security settings by using Azure Policy
- configure security settings by using Azure Blueprint

Secure data and applications

1. Configure security for storage

- 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

2. Configure security for databases

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

3. 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
- backup and restore of Key Vault items

Prerequisites:

- Microsoft Azure Administrator Associate.
- A candidate for this exam should be familiar with scripting and automation, should have a deep understanding of networking and virtualization. A candidate should also have a strong familiarity with cloud capabilities, Azure products and services, and other Microsoft products and services.
- 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.

Who Should Attend:

- Students should have at least one year of hands-on experience securing Azure workloads and experience with security controls for workloads on

Azure.

- **Number of Hours: 40hrs**

- **Certification: AZ-500**

- **Key Features:**

- One to One Training
- Online Training
- Fastrack & Normal Track
- Resume Modification
- Mock Interviews
- Video Tutorials
- Materials
- Real Time Projects
- Virtual Live Experience
- Preparing for Certification