PhoenixTS

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

MICROSOFT

Microsoft Certified: Azure Security Engineer Associate

Validate your technical skills and grow your career.

This certification demonstrates that the recipient can maintain the security posture, identify and provide solutions for any weak spots by using a library of security tools, implementing threat protection and taking care of any security breaches.

Why Take The Microsoft Certified: Azure Security Engineer Associate AZ-500 Exam?

The need AI tech professionals is going to increase dramatically in the near future and passing the exam will help you secure an excellent position in the industry as a Security Engineer.

Increase Your Salary:

- The average salary for someone who holds a Microsoft Certified: Azure Security Engineer Associate certification is around $136,000

Be Part Of The Team

- As a security engineer, you become part of a team that is dedicated to managing cloud-based or hybrid environments security and sometimes as part of an end-to-end infrastructure.

Abilities Validated By The Certification:

- Manage identity and access
- Implement platform protection

- Manage security operations
- Secure data and applications

Recommended Knowledge & Experience:

- Strong skills in scripting and automation
- Deep understanding of networking, visualization and cloud N-tier architecture
- Strong familiarity with cloud capabilities and products and services for Azure plus other Microsoft products and services.

Exam Topics & Scoring:

AZ-500 Exam: Microsoft Azure SEurity Engineer Associate

MANAGE IDENTITY AND ACCESS (30-35%)

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

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

Manage application access

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

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 (15-20%)

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 protection

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 (25-30%)

Monitor security by using Azure Monitor

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

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

Monitor security by using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel
- evaluate results from Azure Sentinel
- configure workflow automation by using Azure Sentinel

Configure security policies

- configure security settings by using Azure Policy
- configure security settings by using Azure Blueprint
- configure a playbook by using Azure Sentinel

SECURE DATA AND APPLICATIONS (20-25%)

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

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

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

Prepare for your exam:

The best way to prepare is with first-hand experience. Taking advantage of the opportunities that Phoenix TS provides will assist you with gathering all the knowledge and skills you'll need for certification.

Phoenix TS Microsoft Certified: Azure Security Engineer Associate – Learning Pathways

- **AZ-500T00: Microsoft Azure Security Technologies**

  Course Overview Phoenix TS' 4-day instructor-led Microsoft Azure Security Technologies training and certification boot camp in Washington, DC Metro, Tysons Corner, VA, Columbia, MD or Live Online will proved the knowledge and skills needed to implement security controls, maintain the security posture, and identify and remediate vulnerabilities by using a variety of security tools. The […]

  Click To Read More

1 –

https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/?utm_source=Sales-Enablement&utm_medium=White-Paper&utm_campaign=&utm_content=Top-Paying-Certs

301-258-8200 | Sales@PhoenixTS.com | www.PhoenixTS.com

Price Match Guarantee

We'll match any competitor's price quote. Call us at 240-667-7757.

Exam Details

- Multiple choice, multiple answers
- Testing in person or online proctored exam
- 130 Min to take the test
- $150 test fee
- Available in English, Japanese, Korean, and Simplified Chinese

10420 Little Patuxent Parkway Suite 500 Columbia, MD 21044