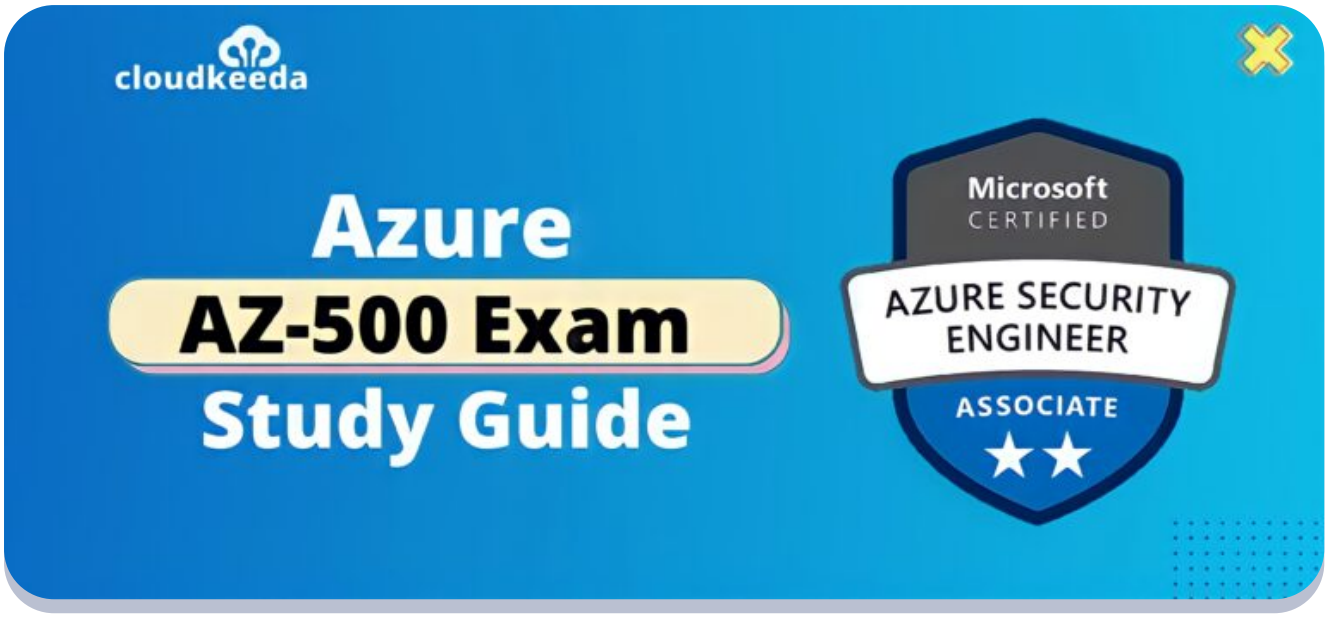


AZ-500: Microsoft Azure Security Engineer Exam Study Guide

April 6, 2022 by manish

Rate this post

In this post, we will discuss with you how to prepare and pass the **Microsoft Azure AZ-500 Exam** (Microsoft Azure Security Engineer Technologies) successfully.

The topics covered in this blog are:

AZ-500 Exam Overview

The Azure Security Technologies exam (AZ-500) is an associate-level exam that is highly focused on the Security aspect of Azure services. The exam is designed to confirm that you can manage and deploy identity and access controls, threat prevention and security controls, and data and application protection in the cloud and hybrid environments as part of end-to-end security enablement.

The AZ-500 exam requires fundamental knowledge of IT security concepts and a decent awareness of most Azure solutions as it focuses on the candidate's ability to identify and patch vulnerabilities using numerous security tools on the cloud.

Are you new to Azure Cloud? Do check out our blog post on the Microsoft Azure Certification Path and choose the best certification for you.

Why Take Up AZ-500 Exam?

If you are already working under security profiles, you might be seeking to gain a chance to enhance your standards. So, this certification is for you. As a student you will master skills like:

1. Develop and improve the skills needed to use security controls.
2. Investigate and identify solutions enforcing different security techniques accessible in the event of a vulnerability.
3. Execute and carry out the security posture and control for the things under your control.
4. Understand how to use numerous security technologies accessible for each application.
5. Exercise the threat protection and execute them.
6. Finally, you will be able to manage and react to security escalation.

Who Can Do This Certification?

1. If you want to understand more about Security, Identity, and Encryption in Azure cloud services.
2. If you want to improve your security expertise and learn more about cloud workload security effectively.
3. If you work in administration or software development and want to move into the security domain.

Benefits of AZ-500 Certification

Learning numerous security tools, particularly within a single exam track, is quite advantageous to gain knowledge as well as experience. The security engineer certified by Microsoft Azure will be distinct from most of the other common pros who haven't taken up the exam. They will be able to appraise

more of the security tools available and apply it to regular security risks and flaws compared to non-exam takers.

Furthermore, professionals that pursue Microsoft Azure security certification have a greater probability of obtaining and retaining better work prospects than non-certified professionals who fall into the AZ-500 exam takers class. Candidates who pass the AZ-500 exam have a greater influence and brunt in the workplace, putting them in a better position to take on more challenging security responsibilities.

A candidate who has been certified in Microsoft Azure security technologies can avail a variety of specific features like:

1. Gain comprehensive knowledge and grasp of networking and controls.
2. Deep-rooted understanding of the different Microsoft Azure and its numerous services offered.
3. Inherent knowledge about virtualization and cloud N-tier architecture appear to be significant in various modern-day apps.
4. Access Azure and other Microsoft products with ease and implement safeguards.

Check Out: ADF Interview Questions

AZ-500 Exam Details

Exam Name Exam AZ-500: Microsoft Azure Security Technologies	**Exam Duration** 150 Minutes
Exam Type Multiple Choice Examination	**Number of Questions** 40 - 60
Exam Fee $165	**Eligibility/Pre-Requisite** None

Exam validity 2 Years	**Exam Languages** English, Japanese, Korean, and Simplified Chinese

AZ-500 Exam Skills Measured

Manage identity and access	**30-35%**
Implement platform protection	**15-20%**
Manage security operations	**25-30%**
Secure data and applications	**20-25%**

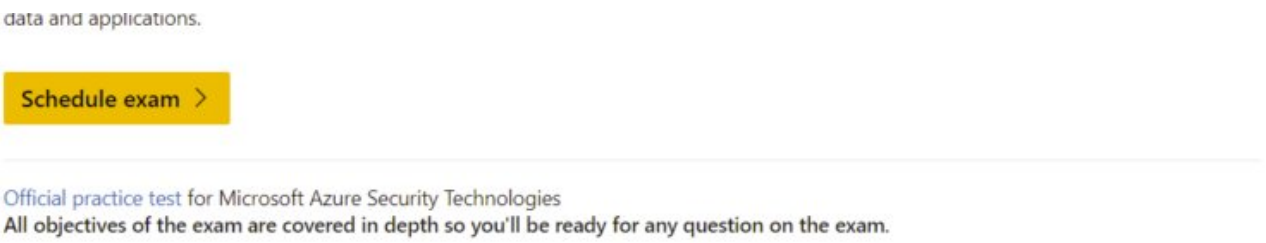
AZ-500 Sample Question Types

Some of the types of questions that might be asked are listed below:

1. Single choice scenario-based questions.
2. Multiple-choice questions.
3. Case studies with many questions
4. Arrange in proper order type questions
5. Single choice questions (without scenario)

How to Register for Azure AZ 500 Exam

You can register for the Microsoft Azure Security Technologies Exam (AZ-500) by going to the official Microsoft page.



Pre-requisites for AZ-500 Certification

If you're thinking of taking this Azure Security Technologies certification, make certain to pass one of these tests before you start, as it will give you sufficient exposure to Azure services and offerings:

- Azure Administrator Associate: AZ-104
- Azure Developer Associate: AZ-204

AZ 500 Study Guide

Manage Identity and Access (30-35%)

Manage Azure Active Directory Identities

- Configure security for service principals
  - Application and service principal objects in Azure Active Directory
  - Create an Azure AD application and service principal to access resources
- Manage Azure Active Directory groups
  - Create a basic group and add members using Azure Active Directory
  - Access with Azure Active Directory groups
- Manage Azure Active Directory users
  - Add or delete users using Azure Active Directory
  - Create and manage users
- Manage administrative units

    - Administrative units in Azure Active Directory
- Configure password writeback
    - Enable Azure Active Directory self-service password reset writeback
- Configure authentication methods including password hash and Pass-Through Authentication (PTA), OAuth, and passwordless
    - What is password hash synchronization with Azure AD?
    - Implement password hash synchronization with Azure AD Connect sync
    - User Sign-in with Azure Active Directory Pass-through Authentication
    - Azure Active Directory Pass-through Authentication: Quickstart
    - Configure an OpenID Connect OAuth application from the Azure AD app gallery
    - Passwordless authentication options for Azure Active Directory
    - Enable passwordless sign-in with the Microsoft Authenticator app
- Transfer Azure subscriptions between Azure Active Directory tenants
    - Transfer an Azure subscription to a different Azure AD directory
    - Associate a subscription to a directory

Configure Secure Access by Using Azure AD

- Monitor privileged access for Azure AD Privileged Identity Management (PIM)
    - Monitor privileged access for Azure AD PIM
- Configure Access Reviews
    - What are Azure AD access reviews?
    - Manage user access with Azure AD access reviews
- Configure Azure AD Privileged Identity Management (PIM)
    - Start using Privileged Identity Management
    - Activate an Azure AD role in PIM
- Implement Conditional Access policies including Multi-Factor Authentication (MFA)

    - What is Conditional Access?
    - Conditional Access: Require MFA for all users
    - Secure user sign-in events with Azure AD Multi-Factor Authentication
- Configure Azure Azure Active Directory identity protection
    - What is Identity Protection?
    - Configure the Azure AD Multi-Factor Authentication registration policy
    - How To: Configure and enable risk policies

Manage Application Access

- Create an App Registration
    - Quickstart: Register an application with the Microsoft identity platform
    - Register an application with the Microsoft identity platform
- Configure App Registration permission scopes
    - Permissions and consent in the Microsoft identity platform
    - Quickstart: Configure an application to expose a web API
- Manage App Registration permission consent
    - Microsoft identity platform consent framework
    - Permissions and consent in the Microsoft identity platform
    - Manage consent to applications and evaluate consent requests
- Manage API access to Azure subscriptions and resources
    - How to use Role-Based Access Control in Azure API Management

Manage Access Control

- Configure subscription and resource permissions
    - How to use Add or change Azure subscription administrators in Azure API Management
    - Assign Azure roles using the Azure portal
- Configure resource group permissions

    - Grant group access to Azure resources using Azure PowerShell
- Configure custom Role-Based Access Control roles
    - Azure custom roles
    - Create and assign a custom role in Azure Active Directory
    - Create or update Azure custom roles using the Azure portal
- Identify the appropriate role
    - Identify the appropriate role
    - Apply the principle of least privilege
        - Principle of least privilege
        - Assign permissions to groups, using the principle of least privilege
- Interpret permissions
    - List Azure role assignments using the Azure portal
    - Check access
        - Check access for a user to Azure resources

Implement Platform Protection (15-20%)

Implement Advanced Network Security

- Secure the connectivity of virtual networks (VPN authentication, Express Route encryption)
    - Azure network security overview
    - Create a site-to-site VPN connection in the Azure portal
    - Configure a Point-to-Site VPN connection using Azure certificate authentication
    - ExpressRoute encryption
    - ExpressRoute encryption: IPsec over ExpressRoute for Virtual WAN
- Configure NSGs and ASGs
    - Create, change, or delete a network security group
    - Create application security groups
    - Associate network interfaces to an ASG
- Create and configure Azure Firewall

    - What is Azure Firewall?
    - Deploy and configure Azure Firewall using the Azure portal
- Implement Azure Firewall Manager
    - What is Azure Firewall Manager?
    - Secure your virtual hub using Azure Firewall Manager
- Configure Azure Front Door service as an Application Gateway
    - Create and configure Azure Front Door service as an application gateway
    - Load-balancing options
- Configure a WAF on Azure Application Gateway
    - Create an application gateway with a WAF using the Azure portal
    - Create an Azure WAF v2 on Application Gateway using an ARM template
    - FAQs for Azure Web Application Firewall on Application Gateway
- Configure Azure Bastion
    - Deploy Bastion using the Azure portal
- Configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
    - Configure Azure Storage firewalls and virtual networks
    - Create a server-level firewall rule using the Azure portal
    - Configure Azure Key Vault firewalls and virtual networks
    - Configuring Azure Firewall with your ASE
- Implement Service Endpoints
    - Virtual Network service endpoints
    - Restrict network access with service endpoints
- Implement DDoS protection
    - Azure DDoS Protection Standard overview
    - Create and configure Azure DDoS Protection Standard

Configure Advanced Security for Compute

- Configure endpoint protection
    - Defender for Containers feature availability

    - Endpoint protection in Microsoft Azure
- Configure and monitor system updates for VMs
    - Manage updates and patches for your VMs
    - Managing updates for your Azure VM
- Configure authentication for Azure Container Registry
    - Authenticate with an Azure container registry
    - Use an Azure managed identity to authenticate to an Azure container registry
    - Authenticate with ACR from AKS
- Configure security for different types of containers
    - Container security in Azure Security Center
    - Implement vulnerability management
        - Security Control: Vulnerability Management
    - Configure isolation for AKS
        - Compute isolation in Azure Kubernetes Service
        - Best practices for cluster isolation in AKS
    - Configure security for container registry
        - Azure security baseline for Container Registry
        - Azure Container Registry image scanning by Security Center
        - Azure Container Registry updates for security and reliability
- Implement Azure Disk Encryption
    - Azure Disk Encryption for Windows VMs
    - Azure Disk Encryption for Linux VMs
    - Azure Disk Encryption for Windows virtual machines FAQ
- Configure authentication and security for Azure App Service
    - Authentication and authorization in Azure App Service
    - Configure your App Service or Azure Functions app to use Azure AD login
    - Authenticate and authorize users end-to-end in Azure App Service
    - Configure SSL/TLS certs
        - Add a TLS/SSL certificate in Azure App Service
        - Configuring TLS for an application in Azure
    - Configure authentication for Azure Kubernetes Service

        - Access and identity options for AKS
        - Use managed identities in AKS
        - Best practices for authentication and authorization in AKS
    - Configure automatic updates
        - Update Management overview
        - Enable Update Management for an Azure VM

Manage Security Operations (25-30%)

Monitor Security by Using Azure Monitor

- Create and customize alerts
    - Create, view, and manage metric alerts using Azure Monitor
    - Create custom alerts
- Monitor security logs by using Azure Monitor
    - Analyze and review Logs for anomalous behavior
- Configure diagnostic logging and log retention
    - Enable diagnostics logging for apps in Azure App Service
    - Change the data retention period

Monitor Security by Using Azure Security Center

- Evaluate vulnerability scans from Azure Security Center
    - Integrated vulnerability assessment solution for Azure VMs
- Configure Just in Time VM access by using Azure Security Center
    - Understanding just-in-time (JIT) VM access
    - Azure Security Center – Just-in-Time Network Access
    - Secure your management ports with just-in-time access
- Configure centralized policy management by using Azure Security Center
    - Manage security policies
    - Create custom security initiatives and policies
- Configure compliance policies and evaluate for compliance by using

Azure Security Center
    - Working with security policies
    - Assess your regulatory compliance
- Configure workflow automation by using Azure Security Center
    - Automate responses to Microsoft Defender for Cloud triggers

Monitor Security by Using Azure Sentinel

- Create and customize alerts
    - Create custom analytics rules to detect threats
- Configure data sources to Azure Sentinel
    - Microsoft Sentinel data connectors
    - Connect data sources
- Evaluate results from Azure Sentinel
    - Investigate incidents with Microsoft Sentinel
    - Use Azure Monitor workbooks to visualize and monitor your data
- Configure a playbook
    - Use playbooks with automation rules in Microsoft Sentinel

Configure Security Policies

- Configure security settings by using Azure Policy
    - Manage security policies
- Configure security settings by using Azure Blueprint
    - Configure your environment for a Blueprint Operator

Secure Data and Applications (20-25%)

Configure Security for Storage

- Configure access control for storage accounts
    - Assign an Azure role for access to blob data
    - Authorize access to blobs using Azure Active Directory

- Configure key management for storage accounts
  - Manage storage account access keys
  - Manage storage account keys with Key Vault and the Azure CLI
- Configure Azure AD authentication for Azure Storage
  - Azure AD Authentication for Azure Blobs and Queues
  - Authorize access to blobs using Azure Active Directory
- Configure Azure AD Domain Services authentication for Azure Files
  - Enable Azure AD Domain Services authentication on Azure Files
- Create and Manage Shared Access Signatures (SAS)
  - Getting Started with Shared Access Signatures (SAS)
  - Grant limited access to Storage with Shared Access Signatures
  - Create a shared access policy for a blob or blob container
    - Define a stored access policy
    - Create a stored access policy with .NET
- Configure Storage Service Encryption
  - Azure Storage Service Encryption (SSE) support for Managed Disks
  - Azure Storage Encryption for data at rest
- Configure Azure Defender for Storage
  - Configure Microsoft Defender for Storage

Configure Security for Databases

- Enable database authentication
  - Use Azure Active Directory authentication
- Enable database auditing
  - Auditing for Azure SQL Database and Azure Synapse Analytics
- Configure Azure Defender for SQL
  - Microsoft Defender for SQL
  - Enable Microsoft Defender for SQL servers on machines
- Implement database encryption
  - Transparent data encryption for SQL Database
  - Implement Azure SQL Database Always Encrypted

        - Always Encrypted is now generally available in Azure SQL Database
        - Configure Always Encrypted by using Azure Key Vault
        - Configure Always Encrypted by using the Windows certificate store

Configure and Manage Key Vault

- Manage access to Key Vault
    - Azure Key Vault security
- Manage permissions to secrets, certificates, and keys
    - Azure Key Vault keys, secrets, and certificates overview
    - Azure RBAC secret, key, & certificate permissions with Key Vault
    - Configure RBAC usage in Azure Key Vault
        - Provide access to Key Vault with Azure RBAC
        - Azure Key Vault security
- Manage certificates
    - Manage certificates via Azure Key Vault
- Manage secrets
    - Configure and manage secrets in Azure Key Vault
    - Manage keys and secrets
- Configure key rotation
    - Automate the rotation of a secrets
- Backup and restore of Key Vault items
    - Azure Key Vault backup and restore
- Configure Azure Defender for Key Vault
    - Introduction to Microsoft Defender for Key Vault

AZ-500 Exam Retake Policy

The AZ-500 exam retake policy is as follows:

1. If a candidate fails on the first attempt, they must wait for 24 hours

before retaking the exam.
2. If a candidate again fails on the second attempt, then the candidate will have to wait for 14 days.
3. A candidate will be given a maximum of five attempts to retake an exam in a year.

AZ 500 Exam Day Tips

Below are some of my suggestions for the exam and some pointers that might be useful.

1. Learn the basics of Azure using the Exams AZ-104 as well as AZ-900 to gain a better understanding of the Azure services offered and Azure products.
2. If this is your first time taking the Virtual Exam, be sure to review the PearsonVUE exam guidelines to make sure that your workspace and desk are tidy prior to taking the exam.
3. There is a whiteboard where you can think of ideas for the exam. It's been the least utilized option of the exam for me personally.
4. Make use of this Exam Outline to write down the dates you want to complete each section and module to ensure you stay on the right track. For instance, I typically choose a date for my final exam and then work backward to figure out the time I've spent on each section or module.

Conclusion

In this Azure tutorial, we discussed **AZ-500 Exam Overview**, **Who Can Do This Certification**, **benefits, Exam Details, Study Guide,** and much more.

I hope you enjoyed this article!!!

Related/References

- DP-300: Azure Database Administrator Exam Study Guide
- SC-900: Azure Security Fundamentals Exam Study Guide
- AZ-900: Azure Fundamentals Exam Study Guide
- AI-900: Azure AI Fundamentals Exam Study Guide
- DP-900: Azure Data Fundamentals Exam Study Guide

Leave a Comment

Name *

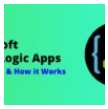
Email *

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Recent Posts

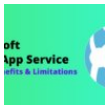
Azure Storage Explorer: Download, Install, and Setup Overview



What are Azure Logic Apps: Components, Advantages and How it Works

Microsoft Azure Application Insights: A Complete Beginners Guide

Microsoft Azure Service Bus: A Complete Beginners Guide



Azure App Service: Types, Benefits and Limitations