AZ 500 Microsoft Azure Security Technologies Training Curriculum

STRUCTURE

www.cromacampus.com | helpdesk@cromacampus.com | +91-120-4155255

AZ 500 Microsoft Azure Security Technologies Training Curriculum

"Learn building, managing, and securing Microsoft Azure solutions with our detailed curriculum plan."

Course Objectives:

- Prepare yourself for the certification exam and clear your certification exam in the first attempt
- Add an attractive credential in your resume that is really appreciated by Companies.
- Improve your overall Cloud management skills, azure development and security skills, and explore more job prospects with better salary packages.
- Boost your social media profiles especially LinkedIn by adding this certification and become one of the top persons to be chosen by industries.

AZ 500 Certification Training Description:

Our AZ-500 "Microsoft Azure Security Technologies" certification Training will help you to gain 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.

The job responsibilities for an Azure Security Engineer include maintaining the security posture, identifying and remediating vulnerabilities by using a variety of security tools, implementing threat protection, and responding to security incident escalations.

Azure Security Engineers often serve as part of a larger team dedicated to cloud-based management and security or hybrid environments as part of an end-to-end infrastructure.

Here are some strong reasons why should you consider this certification course.

- Validate your technical skills like storage, networking, compute, security, and other Cloud operations on Microsoft Azure.
- Validate your development skills and showcase your expertize in building cloud solutions, apps, and services.
- Top-paying info-tech certification in the world.
- It provides you with global recognition for your knowledge, skills, and experience.
- The organization looks for those who know Oracle Cloud, AWS, Azure, etc.

Prerequisites for the Certification Exam:

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.

Necessary Details About Certification You Must Know

- Certification Name – AZ-500 "Microsoft Azure Security Technologies"
- Exam Duration: 150 minutes
- Number of Questions: 40-60
- Passing score: 700 (Out of 1000)
- Exam Cost: USD 165.00
- Validity: 2 years

Certification Exam Structure:

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

Course Content:

Module 1: Overview

- Introduction to Cloud Computing
- Overview of Microsoft Azure
- Microsoft Azure Services
- Azure Subscriptions
- Management Groups
- Azure Resource Manager
- Azure Portal and PowerShell
- Azure Resource Manager Policies
- Azure Policy Definition Structure
- Resource Management Locks
- Organizing Azure Resources

Module 2: Virtual Networks and Network Security

- Introduction
- Azure Virtual Networks
- IP Addresses – Public & Private
- Classless Inter-domain Routing (CIDR)
- Subnets
- Network Interface Cards (NICs)
- Network Security Groups (NSGs)
- Network Security Group Rules
- Virtual Network Service Endpoints
- Service Endpoint Policies
- Azure Load Balancer
- Azure DNS
- Plan and Design Azure Virtual Networks

Module 3: Manage Identities

- Introduction
- Manage Azure Active Directory (AD)
    - add custom domains
    - Azure AD Join
    - configure self-service password reset
    - manage multiple directories
- Manage Azure AD objects (users, groups, and devices)

- create users and groups
- manage user and group properties
- manage device settings
- perform bulk user updates
- manage guest accounts

- Implement and manage hybrid identities
  - install Azure AD Connect, including password hash and pass-through synchronization
  - use Azure AD Connect to configure federation with on-premises Active Directory Domain Services (AD DS)
  - manage Azure AD Connect
  - manage password sync and password writeback
- Implement multi-factor authentication (MFA)
  - configure user accounts for MFA
  - enable MFA by using bulk update
  - configure fraud alerts
  - configure bypass options
  - configure Trusted IPs
  - configure verification methods

Module 4: Manage Access Control

- Configure secure access by using Azure AD
  - monitor privileged access for Azure AD Privileged Identity Management (PIM)
  - configure Access Reviews
  - activate and configure PIM
  - 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

Module 5: 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

Module 6: 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

Module 7: Manage security operations

- 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
- 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

Module 8: Secure data and applications

- 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

Module 7: Placement Guide

- What is an Interview?
- Tips to clear an Interview
- Common Interview questions and answers
- AZ 500 Interview Questions and Answers
- Resume Building Guide
- Attempt for AZ 500 Global Certification Exam
- Start applying for Jobs