



# Microsoft Azure Security Technologies (AZ-500)

## About DevOpsSchool

DevOpsSchool is a unit of "Cotocus PVT Ltd" and a leading platform which helps IT organizations and professionals to learn all the emerging technologies and trend which helps them to learn and embrace all the skills, intelligence, innovation and transformation which requires to achieve the end result, quickly and efficiently. We provide over 40 specialized programs on DevOps, Cloud, Containers, Security, AI, ML and on Big data that are focused on industry requirement and each curriculum is developed and delivered by leading experts in each domain and aligned with the industry standards.

## About Course

This "Microsoft Azure Security Technologies" Program is the only course in the WORLD which can make you an expert and proficient in Azure Platform. Our curriculum has been determined by comprehensive research on 10000+ job descriptions across the globe and epitome of 20+ years of industry experience.

"Microsoft Azure Security Technologies AZ-500" program is structured in a way, whether you are an experienced IT professional or a college graduate, this course will help you to integrate all the real-world experience, specialization, and job-ready skills. DevOpsSchool offers Master in Microsoft Azure DevOps Online and classroom Training and Certification course by Expert. Microsoft Azure Security Technologies AZ-500 course is specially designed by IT industries expert for beginners who will offer you an in-depth understanding of numerous Azure DevOps equipment.



Co-coordinator - Akanksha Kumari

Call/WhatsApp: - +91 1800 889 7977

Mail Address: -

[contact@DevOpsSchool.com](mailto:contact@DevOpsSchool.com)

Secondary contact - Patrick

Call/WhatsApp: - +91 7004 215 841

Mail Address: - [contact@DevOpsSchool.com](mailto:contact@DevOpsSchool.com)

Duration	35 Hours
Mode	Online (Instructor-led, live & Interactive)
Projects (Real time scenario based)	1

FEATURES	DEVOPSSCHOOL	OTHERS
Faculty Profile Check	✓	✗
Lifetime Technical Support	✓	✗
Lifetime LMS access	✓	✗
Top 25 Tools	✓	✗
Interviews Kit	✓	✗
Training Notes	✓	✗
Step by Step Web Based Tutorials	✓	✗
Training Slides	✓	✗
Training + Additional Videos	✓	✗



## Projects

---

In Microsoft Azure Security Technologies AZ-500 training & Certification Course a Participant will get total 100+ Lab Assignment, real-time scenario-based projects to work on, and 250+ real-time interview questions, as part of these projects, we would help our participant to have first-hand experience of the real-time scenario-based project from scratch to end. We would also help our participants to visualize a real Azure environment.

## Interview

---

As part of this, You would be given complete interview preparations kit, set to be ready for the DevOps hotseat. This kit has been crafted by 200+ years industry experience and the experiences of nearly 10000 DevOpsSchool DevOps learners worldwide.

# AGENDA OF THE MICROSOFT AZURE SECURITY TECHNOLOGIES (AZ-500)

## Manage identity and access

### 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.
- 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

---

### 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

### 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

### 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
- manage certificates
- manage secrets
- configure key rotation
- backup and restore of Key Vault items





# Thank you!

Connect with us for more info

Call/WhatsApp: - +91 968 682 9970

Mail: - [contact@DevOpsSchool.com](mailto:contact@DevOpsSchool.com)

[www.DevOpsSchool.com](http://www.DevOpsSchool.com)