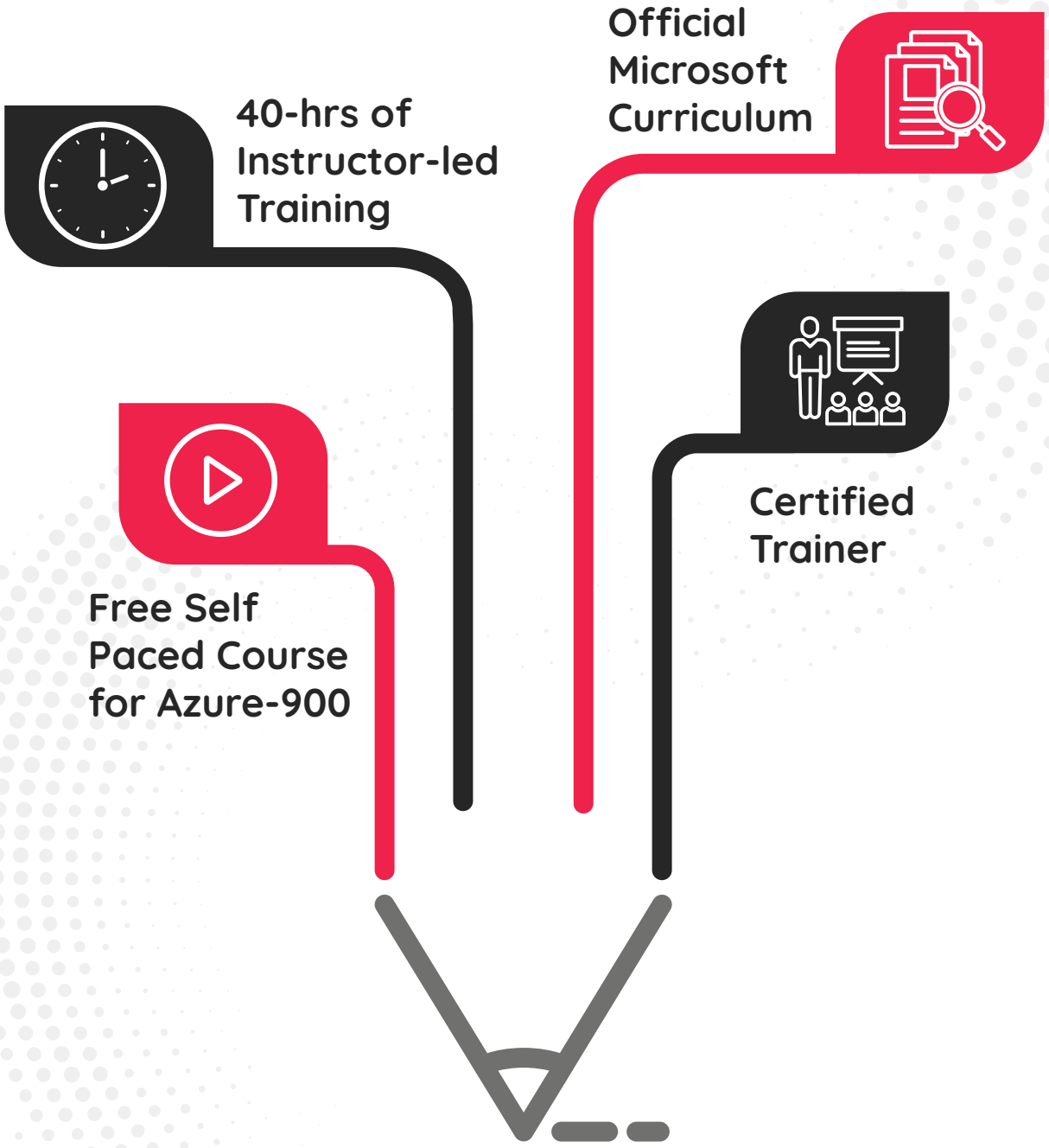
INFOSECTRAIN

Microsoft

AZURE ADMINISTRATOR & SECURITY

(AZ-104 + AZ-500) COMBO TRAINING

COURSE
HIGHLIGHTS



COURSE OVERVIEW

The Azure Administrator & Security training course from InfosecTrain is designed to equip aspiring Azure Administrators and Security experts with an integrated skill set for effectively managing and securing Azure environments. This comprehensive course covers a broad spectrum of topics, including Azure governance, compliance, subscription management, resource grouping, virtual networking, and Azure Virtual Machines. It delves into hands-on practices for implementing Azure policies, managing identities with Azure Active Directory, and applying Role-Based Access Control (RBAC) for enhanced security.

Participants will learn to optimize cloud performance, ensure data protection, and deploy secure infrastructure solutions. Additionally, the course addresses implementing perimeter security, managing host security, securing data and applications with Azure Key Vault, and safeguarding Azure Storage. It concludes with advanced security operations techniques, including using Azure Monitor, Microsoft Defender for Cloud, and Microsoft Sentinel to maintain a robust security posture.

WHY AZURE COMBO AZ-104T00 AND AZ-500T00A TRAINING COURSE WITH INFOSECTRAIN?

InfosecTrain is a leading IT security training and consulting organization offering best-in-class yet cost-effective customized training programs to enterprises and individuals across the globe. We offer role-specific certification training programs and prepare professionals for the future. Our Azure Administrator & Security training course is designed to equip participants with both areas of expertise within the Microsoft Azure ecosystem.

Here's what you get when you choose InfosecTrain as your learning partner:

- **Flexible Schedule:** Training sessions to match your schedule and accommodate your needs.
- **Post Training Support with No Expiry Date:** Ongoing assistance and support until the learners achieve their certification goals.
- **Recorded Sessions:** Access to LMS and recorded sessions for post-training reference.
- **Customized Training:** A training program that caters to your specific learning needs.
- **Knowledge Sharing Community:** Collaborative group discussions to facilitate knowledge sharing and learning.
- **Certificate:** Each candidate receives a certificate of participation as a testament to their accomplishment.
- **Expert Career Guidance:** Free career guidance and support from industry experts.

TARGET AUDIENCE

- Azure Administrators
- Azure Cloud Engineers
- Systems Administrators intending to advance their Azure skills
- IT professionals looking forward to becoming Azure Security Engineers
- IT professionals preparing for Microsoft's AZ-500 exam

PRE-REQUISITES

- Basic understanding of networking
- Basic understanding of Windows/Linux OS
- Exposure to working with PowerShell Client on Windows or macOS
- Suggested to have knowledge of Microsoft Azure administrator associate
- Understanding of basic IT security principles

EXAM INFORMATION

Certification Name	AZ-104T00	AZ-500T00
Number of Questions	40 to 60	40 to 60
Exam Duration	180 minutes	180 minutes
Passing Score	700 out of 1000	700 out of 1000

COURSE OBJECTIVES

- Provides hands-on expertise in services and technologies to improve your capabilities to address tasks in professional roles easily
- Enhances your knowledge of Identity and Security, Hybrid Cloud, Monitoring, Encryption, Database Security, and Securing apps and services for the cloud.
- Showcases your commitment to skill development
- Provides knowledge about Microsoft Azure Administrator and Microsoft Azure Security
- Offers you an initiative to pursue comprehensive administrator and security expertise on a notable public cloud platform

COURSE CONTENT

AZ-104T00 MICROSOFT AZURE ADMINISTRATOR

Module 01 - Administer Governance and Compliance

- Introduction
- Identify regions
- Implement Azure subscriptions
- Obtain a subscription
- Create resource groups
- Determine resource limits
- Create an Azure resource hierarchy
- Apply resource tagging
- Manage costs

Module 02 - Configure Azure Policy

- Introduction
- Implement Azure policy
- Create Azure policies
- Create policy definitions
- Create initiative definitions
- Scope the initiative definition
- Determine compliance

Module 03 - Configure Role Based Access Control

- Introduction
- Compare Azure RBAC roles to Azure AD roles
- Create a role definition
- Create a role assignment
- Apply RBAC authentication
- Determine Azure RBAC roles

Module 04 - Configure Azure Resources with Tools

- Introduction
- Use the Azure portal
- Demonstration Azure portal
- Use Azure cloud shell
- Demonstration cloud shell
- Use Azure powerShell
- Deploy template

Module 05 - Administer Virtual Networking

- Introduction
- Plan virtual networks
- Create subnets
- Create virtual network
- Plan IP addressing
- Create public IP addresses
- Associate public IP addresses
- Associate private IP addresses

Module 06 - Configure Azure DNS

- Introduction
- Identify domains and custom domains
- Verify custom domain names (optional)
- Create Azure DNS zones
- Delegate DNS domain
- Add DNS record sets
- Plan for private DNS zones
- Determine private zones scenarios

Module 07 - Administer Azure Virtual Machines Configure Virtual Machines Configure

- Introduction
- Review cloud services-responsibilities
- Plan virtual machines
- Determine virtual machine sizing
- Determine virtual machine storage
- Demonstration –create virtual machines
- Connect to virtual machines

Module 08 - Virtual Machine Availability

- Introduction
- Plan for maintenance and downtime
- Setup availability sets
- Review update and fault domains
- Review availability zones
- Compare vertical and horizontal scaling
- Create scale sets
- Configure auto scale

Module 09 - Administer PaaS Compute Options Configure App Service Plans

- Introduction
- Implement Azure app service plans
- Determine app service plan pricing
- Scale up and scale out the app service
- Configure app service plan scaling

Module 10 - Administer Data Protection Configure File and Folder Backups

- Introduction
- Describe Azure backup benefits
- Implement azure backup center
- Setup recovery service vault backup options
- Demonstration – backup Azure file shares
- Configure on-premises file and folder backups
- Manage the Azure recovery services agent

AZ-500T00A: MICROSOFT AZURE SECURITY TECHNOLOGIES

Learning Path 1: Manage Identity and Access

Module 1 - Secure Azure Solution with Azure Active Directory

- Configure Azure AD and Azure AD domain services for security
- Create users and groups that enable secure usage of your tenant
- Use MFA to protect user's identities
- Configure password less security options

Module 2 - Implement Hybrid Identity

- Deploy Azure AD connect
- Pick and configure that best authentication option for your security needs
- Configure password writeback

Module 3 - Deploy Azure AD Identity Protection

- Deploy and configure identity protection
- Configure MFA for users, groups, and applications
- Create conditional access policies to ensure your security
- Create and follow an access review process

Module 4 - Configure Azure AD Privileged Identity Management

- Describe zero trust and how it impacts security
- Configure and deploy roles using privileged identity management (PIM)
- Evaluate the usefulness of each PIM setting as it relates to your security goals

Module 5 - Design an Enterprise Governance Strategy

- Explain the shared responsibility model and how it impacts your security configuration
- Create Azure policies to protect your solutions
- Configure and deploy access to services using RBAC

Learning Path 2: Implement Platform Protection

Module 1 - Implement Perimeter Security

- Define defense in depth
- Protect your environment from denial-of-service attacks
- Secure your solutions using firewalls and VPNs
- Explore your end-to-end perimeter security configuration based on your security posture

Module 2 - Configure Network Security

- Deploy and configure network security groups to protect your Azure solutions
- Configure and lockdown service endpoints and private links
- Secure your applications with application gateway, web app firewall, and front door
- Configure expressroute to help protect your network traffic

Module 3 - Configure and Manage Host Security

- Configure and deploy endpoint protection
- Deploy a privileged access strategy for devices and privileged workstations
- Secure your virtual machines and access to them
- Deploy Windows Defender
- Practice layered security by reviewing and implementing security center and security benchmarks

Module 4 - Enable Containers Security

- Define the available security tools for containers in azure
- Configure security settings for containers and kubernetes services
- Lock down network, storage, and identity resources connected to your containers
- Deploy RBAC to control access to containers

Learning Path 3: Secure your Data and Applications

Module 1 - Deploy and Secure Azure Key Vault

- Define what a key vault is and how it protects certificates and secrets
- Deploy and configure Azure Key Vault
- Secure access and administration of your key vault
- Store keys and secrets in your key vault
- Explore key security considers like key rotation and backup / recovery

Module 2 - Configure Application Security Features

- Register an application in Azure using app registration
- Select and configure which Azure AD users can access each application
- Configure and deploy web app certificates

Module 3 - Implement storage security

- Define data sovereignty and how that is achieved in Azure
- Configure Azure Storage access in a secure and managed way
- Encrypt your data while it is at rest and in transit
- Apply rules for data retention

Module 4 - Configure and Manage SQL Database Security

- Configure which users and applications have access to your SQL databases
- Block access to your servers using firewalls
- Discover, classify, and audit the use of your data
- Encrypt and protect your data while is it stored in the database.

Learning Path 4: Manage Security Operation

Module 1 - Configure and manage Azure Monitor

- Configure and monitor Azure Monitor
- Define metrics and logs you want to track for your Azure applications
- Connect data sources to and configure Log Analytics
- Create and monitor alerts associated with your solutions security

Module 2 - Enable and Manage Microsoft Defender for Cloud

- Define the most common types of cyber-attacks
- Configure Azure Security Center based on your security posture
- Review Secure Score and raise it
- Lock down your solutions using Security Center and Defender
- Enable Just-in-Time access and other security features

Module 3 - Configure and Monitor Microsoft Sentinel

- Explain what Azure Sentinel is and how it is used
- Deploy Azure Sentinel
- Connect data to Azure Sentinel, like Azure Logs, Azure AD, and others
- Track incidents using workbooks, playbooks, and hunting techniques

COURSE

BENEFITS

HIRING COMPANIES

Deloitte. KPMG pwc

Source: Payscale, Glassdoor


INFOSECTRAIN