INFOSECTRAIN

Azure Security Combo

Administrator + Security

KEY FEATURES

- 48 hrs of instructor-led training
- 4 hrs/day in Weekend/Weekday
- Certified & Experienced Trainer
- Official Microsoft Curriculum covered

The Azure Combo (AZ-104 Microsoft Azure Administrator Training & Certification + Microsoft AZ-500 Certification: Azure Security Technologies Training & Certification) helps you validate the competencies of candidates in managing cloud services, including computing, networking, storage, security, and other Microsoft Azure Cloud capabilities...

OVERVIEW

The AZ-104 Microsoft Azure Administrator and AZ-500 Microsoft Azure Security courses aim to enhance the latest knowledge and skillset of various Microsoft Azure Cloud levels. Candidates also gain hands-on exposure to optimize cloud performance and scalability, provisioning, reliability, and monitoring.

This extensive training and certification authenticate the capability of aspiring Azure Administrators and Security experts in managing Azure resources and subscriptions, storage implementation and management, VMs deployment and management, configuration and management of virtual networks, identity management, and implement secure infrastructure solutions.

This Azure Security Combo course tends to explain:

- Management of Azure resources and subscriptions
- Implementation and management of Azure cloud storage
- Deployment and management of VMs in Azure
- Configuration and management of Azure virtual networks
- Performance of identity management
- Performance of the deployment of ARM templates
- Implementation of security controls
- Maintenance of the security posture
- Managing identity and access and
- Protection of data, applications, and networks.
- Identification and fixation of vulnerabilities by using a variety of security tools,
- Implementation of threat protection, and
- Response to security incident escalations
- Managing Azure identity and access
- Implementing Azure platform protection
- Managing Azure security operations
- Securing data and applications on Azure

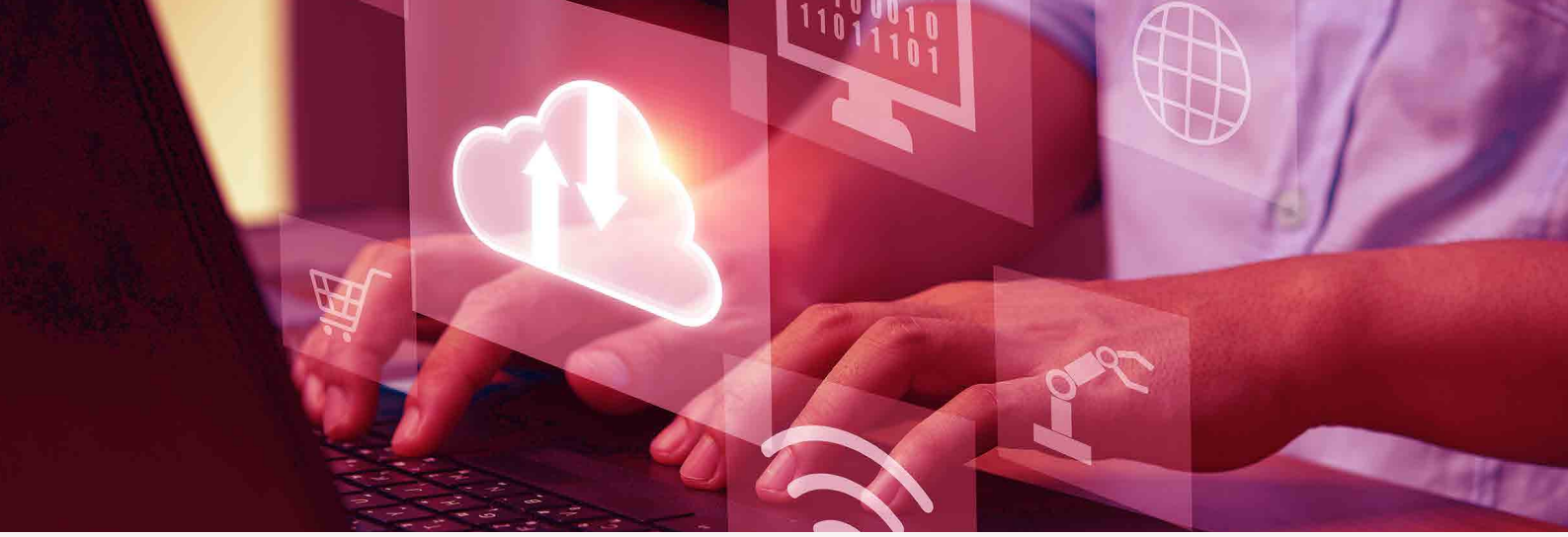
INFOSECTRAIN

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-Requisite

- 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



INFOSECTRAIN

Exam Information

It is a combo course, so there will be two different exams for Microsoft Azure Administrator Exam AZ-104 and Exam AZ-500: Microsoft Azure Security Technologies. Both the exams follow the pattern of Multiple-Choice Questions. The candidates need to pass the following certification exam to get recognized as a certified Azure Administrator and Microsoft Azure Security Engineer:

Certification Name	Microsoft Azure Administrator Exam AZ-104
Number of Questions	40 to 60
Test Duration	180 minutes
Passing score	700 out of 1000

Certification Name	Microsoft Azure Security Technologies Exam AZ-500
Number of Questions	40 to 60
Test Duration	180 minutes
Passing score	700 out of 1000

Why Infosec Train?

INFOSECTRAIN

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

Our Expert Instructors

"

Krish is a senior technical consultant and passionate trainer. He has more than 15 years of experience in various IT domains including Cloud Computing, Security, Linux & Infrastructure Design. He has trained almost 400+ professionals worldwide on various IT domains.

KRISH

CCSP | CCSK | AWS-Sec | AWS CSA-P | MCT | Azure Sec | CEH | MCTS

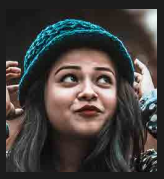
"

Rishabh served as a corporate trainer & Consultant with nearly 8+ years of experience across the diverse industry. Good hands-on experience in vulnerability assessment, Penetration Testing.

RISHABH KOTIYAL

AZ 104 | AZ 500 | AZ 303 | AZ 304 | CEH I ECIH I ECSA I CND I CEI I securitY+ I CSA

HAPPY LEARNERS FROM THE WORLD



Deepthi
AZURE Combo | Norway

I love this course, the explanation is great, the assignments are very good. I learned many things from this course.

Vishnu Dhanavath
AZURE Combo | India

It was my first training module on Azure, I have thoroughly enjoyed the course and learned the basics of Azure, this training surely enhanced my learning experience.

Mohamed Arshad Mubeen
AZURE Combo | India

The course was presented in an enthusiastic way, this has more than met my expectations, A wonderfully practical course.

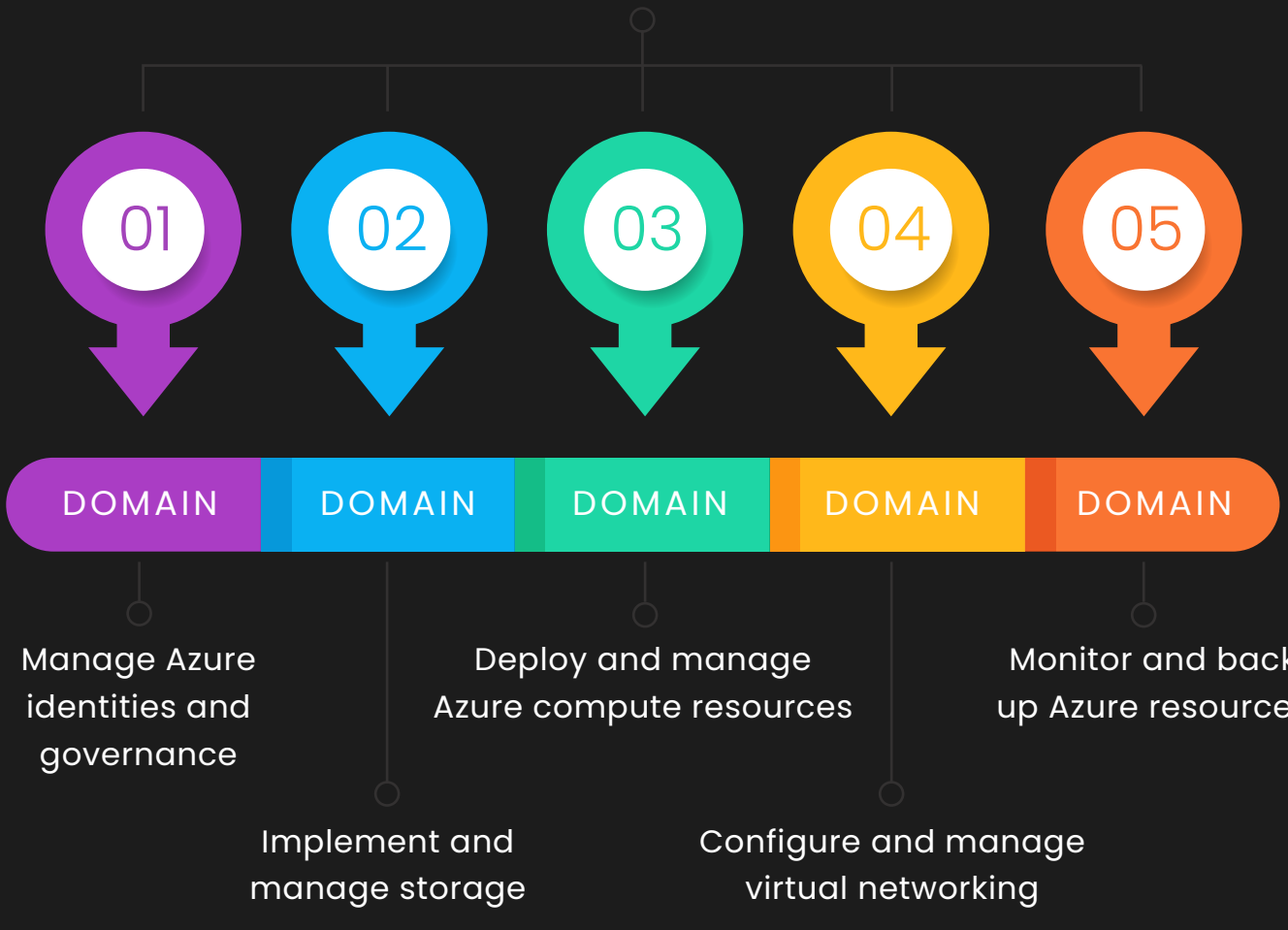
Mohammad Nafees
AZURE Combo | India

This training is very helpful, the trainer did a good job in presenting the ideas in a simplified manner.

INFOSECTRAIN

DOMAIN WISE AGENDA

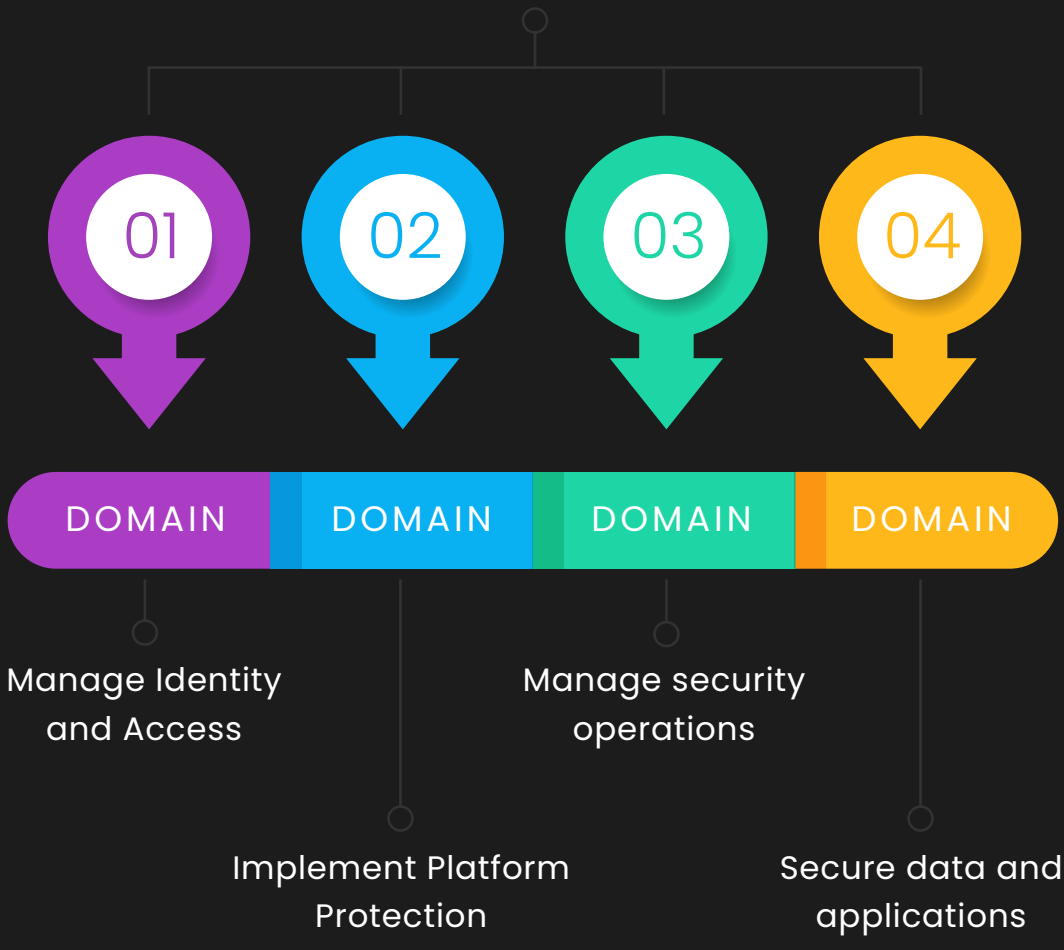
AZ-104: Azure Administrator



INFOSECTRAIN

DOMAIN WISE AGENDA

Azure Security Engineer (AZ-500)



AZ-104: Azure Administrator

Domain 1: Manage Azure identities and governance

Manage Azure AD objects

- Create users and groups
- Manage user and group properties
- Manage device settings
- What is enterprise state roaming?
- Manage users and groups in Azure Active Directory
- Manage guest accounts
- Configure Azure AD join
- Configure self-service password reset
- Plan an Azure Active Directory self-service password reset

Manage role-based access control (RBAC)

- Create a custom role
- Provide access to Azure resources by assigning roles (subscriptions, resource groups. resources)
- Interpret access assignments
- Manage multiple directories

Manage subscriptions and governance

- Configure Azure policies
- Configure resource locks
- Apply tags
- Create and manage resource groups (move and remove)
- Manage subscriptions
- Configure Cost Management
- Configure management groups

Domain 2: Implement and manage storage (15–20%)

Manage storage accounts

- Configure network access to storage accounts
- Create and configure storage accounts
- Generate shared access signature
- Manage access keys
- Implement Azure storage replication
- Configure Azure AD Authentication for a storage account

Manage data in Azure Storage

- Export from Azure job
- Import into Azure job
- Copy data by using AZCopy

Configure Azure files and Azure blob storage

- Create an Azure file share
- Create and configure Azure File Sync service
- Configure Azure blob storage
- Configure storage tiers for Azure blobs

Domain 3: Deploy and manage Azure compute resources

Configure VMs for high availability and scalability

- Configure high availability
- Deploy and configure scale sets

Automate deployment and configuration of VMs

- Modify Azure Resource Manager (ARM) template
- Configure VHD template
- Deploy from template
- Save a deployment as an ARM template
- Automate configuration management by using custom script extensions

Create and configure VMs

- Configure Azure Disk Encryption
- Move VMs from one resource group to another
- Manage VM sizes
- Add data discs
- Configure networking
- Redeploy VMs

Create and configure containers

- Create and configure Azure Kubernetes Service (AKS)
- Create and configure Azure Container Instances (ACI)

Create and configure Web Apps

- Create and configure App Service
- Create and configure App Service Plans

Domain 4: Configure and manage virtual networking

Implement and manage virtual networking

- Create and configure VNET peering
- Configure private and public IP addresses, network routes, network interface, subnets, and virtual network

Configure name resolution

- Configure Azure DNS
- Configure custom DNS settings
- Configure a private or public DNS zone

Secure access to virtual networks

- Create security rules
- Associate an NSG to a subnet or network interface
- Evaluate effective security rules
- Deploy and configure Azure Firewall
- Deploy and configure Azure Bastion Service

Configure load balancing

- Configure Application Gateway
- Configure an internal load balancer
- Configure load balancing rules
- Configure a public load balancer

Monitor and troubleshoot virtual networking

- Monitor on-premises connectivity
- Use Network Performance Monitor
- Use Network Watcher
- Troubleshoot external networking
- Troubleshoot virtual network connectivity

Integrate an on-premises network with an Azure virtual network

- Create and configure Azure VPN Gateway
- Create and configure VPNs
- Configure ExpressRoute
- Configure Azure Virtual WAN

Domain 5: Monitor and back up Azure resources

Monitor resources by using Azure Monitor

- Configure and interpret metrics (Analyze metrics across subscriptions)
- Configure Log Analytics (Implement a Log Analytics workspace, Configure diagnostic settings)
- Query and analyze logs (Create a query, Save a query to the dashboard, Intepret graphs)
- Set up alerts and actions (Create and test alerts, Create action groups, View alerts in Azure Monitor, Analyze alerts across subscriptions)
- Configure Application Insights

Implement backup and recovery

- Configure and review backup reports
- Perform backup and restore operations by using Azure Backup Service
- Create a Recovery Services Vault (Use soft delete to recover Azure VMs)
- Create and configure backup policy
- Perform site-to-site recovery by using Azure Site Recovery

Azure Security Engineer (AZ-500)

Domain 1: 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, 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
- 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 application access

- 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

Domain 2: 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

Configure advanced security for compute

- Configure endpoint protection
- Configure and monitor system updates for VMs
- Configure authentication for Azure Container Registry
- 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 authentication for Azure Kubernetes Service
- Configure automatic updates

Domain 3: Manage security operations

Monitor security by using Azure Monitor

- Create and customize alerts
- Monitor logs by using Azure Monitor
- Configure diagnostic logging and log retention

Monitor security by using Azure Security Center

- Create and customize alerts
- 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 a playbook for a security event by using Azure Sentinel

Configure security policies

- Configure security settings by using Azure Policy
- Configure security settings by using Azure Blueprint

Domain 4: 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

www.infosectrain.com | sales@infosectrain.com