AZ-103 Microsoft Azure Administrator Training Curriculum

STRUCTURE

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

AZ-103 Microsoft Azure Administrator Training Curriculum

"Become a Microsoft Certified Azure Administrator by joining our comprehensive AZ-103 Microsoft Azure Administrator Training Program"

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 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 103 Certification Training Description:

The AZ-103 Microsoft Azure Administrator certification Training is geared towards those who manage Cloud services that span computes, networking, storage, security, and other Cloud capabilities within Microsoft Azure. Here, are some strong reasons why should take this certification course.

- Validate your technical skills like storage, networking, compute, security, and other Cloud operations on Microsoft Azure.
- 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.

Necessary Details about Certification You must Know

- Certification Name – AZ-103: Microsoft Azure Administrator
- Prerequisites – There are no prerequisites for this certification.
- Exam Duration: 180 minutes
- Number of Questions: 40-60
- Passing score: 700 (Out of 1000)
- Exam Cost: USD 165.00
- Validity: 2 years

Certification Exam Structure:

- Manage Azure subscriptions and resources (15-20%)
- Implement and manage storage (15-20%)
- Deploy and manage virtual machines (VMs) (15-20%)
- Configure and manage virtual networks (30-35%)
- Manage identities (15-20%)

Course Content:

Module 1: Managing Azure Subscriptions and Resource Groups

- 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
- Manage Azure subscriptions
  - Assign administrator permissions
  - Configure cost center quotas and tagging
  - Configure policies at azure subscription level
  - Implement management groups
- Analyze resource utilization and consumption
  - Configure diagnostic settings on resources
  - Create baseline for resources
  - Create and test alerts
  - Analyze alerts across subscription
  - Analyze metrics across subscription
  - Create action groups and action rules
  - Monitor for unused resources
  - Monitoring Spend
  - Report on spend
  - Utilize log queries in azure monitor
  - View alerts in azure monitor
- Manage resource groups
  - Use azure policies for resource groups
  - Configure resource locks
  - Configure resource policies
  - Implement and set tagging on resource groups
  - Move resources across resource groups
  - Remove resource groups
- Managed role-based access control (RBAC)
  - Create a custom role
  - Configure access to azure resources by assigning roles
  - Configure management access to azure
  - Troubleshoot RBAC
  - Implement RBAC policies
  - Assign RBAC roles

Module 2: Implement and Manage Storage

- Introduction
  - Azure Storage
  - Azure Storage Replication
  - Azure Storage Explorer
  - Attach or Detach an External Storage Account
  - Shared Access Signatures (SAS)
  - Attach a Storage Account using SAS
  - Azure Blob Storage
  - Azure File Storage
  - Azure Queue Storage
  - Azure Table Storage
- Create and configure storage accounts
  - configure network access to the storage account
  - create and configure storage account
  - generate shared access signature
  - install and use Azure Storage Explorer
  - manage access keys
  - monitor activity log by using Monitor Logs
  - implement Azure storage replication
  - implement Azure AD Authentication
- Import and export data to Azure
  - create export from Azure job
  - create import into Azure job
  - use Azure Data Box
  - configure and use Azure blob storage
  - configure Azure content delivery network (CDN) endpoints
  - use Azure Data Factory to transfer data to Azure
- Configure Azure files
  - create Azure file share
  - create Azure File Sync service
  - create Azure sync group
  - troubleshoot Azure File Sync
- Implement Azure backup
  - configure and review backup reports
  - perform backup operation
  - create Recovery Services Vault
  - create and configure backup policy
  - perform a restore operation

Module 3: Deploy and Manage Virtual Machines

- Introduction
  - Azure Virtual Machines
  - Azure Resource Manager VM

- Introduction to ARM Templates
- Create a Custom Image of Azure VM
- Create a Managed Image of a Generalized VM
- Create an Image from VM Snapshots
- Creating a Linux Virtual Machine
- Virtual Machine Extensions
- Configuration Management using PowerShell DSC
- Run Custom Scripts using Custom Script Extension

- Create and configure a VM for Windows and Linux
  - configure high availability
  - configure monitoring, networking, storage, and virtual machine size
  - deploy and configure scale sets
- Automate deployment of VMs
  - modify Azure Resource Manager (ARM) template
  - configure location of new VMs
  - configure VHD template
  - deploy from template
  - save a deployment as an ARM template
  - deploy Windows and Linux VMs
- Manage Azure VM
  - add data discs
  - add network interfaces
  - automate configuration management by using PowerShell Desired State Configuration
  - (DSC) and VM Agent by using custom script extensions
  - manage VM sizes
  - move VMs from one resource group to another
  - redeploy VMs
  - soft delete for Azure VMs
- Manage VM backups
  - configure VM backup
  - define backup policies
  - implement backup policies
  - perform VM restore
  - Azure Site Recovery

Module 4: Configure, Manage Virtual Networks & 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

- Create connectivity between virtual networks
  - create and configure VNET peering
  - create and configure VNET to VNET connections
  - verify virtual network connectivity
  - create virtual network gateway
- Implement and manage virtual networking
  - 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 private and public DNS zones
- Create and configure a Network Security Group (NSG)
  - create security rules
  - associate NSG to a subnet or network interface
  - identify required ports
  - evaluate effective security rules
  - implement Application Security Groups
- Implement Azure load balancer
  - configure internal load balancer
  - configure load balancing rules
  - configure public load balancer
  - troubleshoot load balancing
- Monitor and troubleshoot virtual networking
  - monitor on-premises connectivity
  - use Network resource monitoring
  - use Network Watcher
  - troubleshoot external networking
  - troubleshoot virtual network connectivity
- Integrate on premises network with Azure virtual network
  - create and configure Azure VPN Gateway
  - create and configure site to site VPN
  - configure Express Route
  - verify on premises connectivity
  - troubleshoot on premises connectivity with Azure
  - use Azure network adapter

Module 5: 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 6: Placement guide

- What is an Interview?
- Tips to clear an Interview
- Common Interview questions and answers
- AZ 103 Interview Questions and Answers
- Resume Building Guide
- Attempt for AZ 103 Global Certification Exam
- Earn Credentials and Start applying for Jobs