

Microsoft Azure Administrator

Microsoft Azure Administrator Training is one of the widely-acknowledged credentials from Microsoft for professionals worldwide.

Participants who take up this 4-day Microsoft Azure Administrator (AZ-104) course will gain a proper understanding of managing Azure subscriptions, securing identities, configuring virtual networking, managing network traffic, and more.

Microsoft Azure Administrator training will help participants to gain a fundamental understanding of implementing and managing identities, governance, cloud storage, creating virtual networks, and managing resources as and when needed.



Audience Profile:

This course is for Azure Administrators. The Azure Administrator implements, manages, and monitors identity, governance, storage, compute, and virtual networks in a cloud environment.

The Azure Administrator will provision, size, monitor, and adjust resources as appropriate.

Prerequisites:

Required

Understanding of Active Directory concepts, including users, groups, and role-based access control.

Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.

Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.

Understanding of resilience and disaster recovery, including backup and restore operations.

After completing this learning path, you'll be able to:

Learn how to secure identities with Azure Active Directory, and implement users and groups

Learn how to manage your subscriptions and accounts, implementing Azure policies, and using Role-Based Access Control

Learn about the tools an Azure Administrator uses to manage their infrastructure

Learn about basic virtual networking concepts

Learn about inter-site connectivity features including VNet Peering, Virtual Network Gateways, and Site-to-Site Connections

Learn about network traffic strategies

Learn about basic storage features

Learn about Azure virtual machines

Learn administer serverless computing features

Learn about backing up files and folders, and virtual machine backups

Learn how to monitor your Azure infrastructure

Here are the learning paths in this series:

Manage Azure Active Directory (Azure AD) objects

- create users and groups
- create administrative units
- manage user and group properties
- manage device settings
- perform bulk user updates
- manage guest accounts
- configure Azure AD join
- configure self-service password reset

Manage role-based access control (RBAC)

- create a custom role
- provide access to Azure resources by assigning roles at different scopes
- interpret access assignments

Manage subscriptions and governance

- configure Azure policies
- configure resource locks
- apply and manage tags on resources
- manage resource groups
- manage subscriptions
- manage costs
- configure management groups

Secure storage

- configure network access to storage accounts
- create and configure storage accounts
- generate shared access signature (SAS) tokens
- manage access keys
- configure Azure AD authentication for a storage account
- configure access to Azure Files

Manage storage

- export from Azure job
- import into Azure job
- install and use Azure Storage Explorer
- copy data by using AZ Copy
- implement Azure Storage replication
- configure blob object replication

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
- configure blob lifecycle management

Automate deployment of virtual machines (VMs) by using Azure Resource Manager templates

- modify an Azure Resource Manager template
- configure a virtual hard disk (VHD) template
- deploy from a template
- save a deployment as an Azure Resource Manager template
- deploy virtual machine extensions

Configure VMs

- configure Azure Disk Encryption
- move VMs from one resource group to another
- manage VM sizes
- add data disks
- configure networking
- redeploy VMs
- configure high availability

- deploy and configure virtual machine scale sets

Create and configure containers

- configure sizing and scaling for Azure Container Instances
- configure container groups for Azure Container Instances
- configure storage for Azure Kubernetes Service (AKS)
- configure scaling for AKS
- configure network connections for AKS
- upgrade an AKS cluster

Create and configure Azure App Service

- create an App Service plan
- configure scaling settings in an App Service plan
- create an App Service
- secure an App Service
- configure custom domain names
- configure backup for an App Service
- configure networking settings
- configure deployment settings

Implement and manage virtual networking

- create and configure virtual networks, including peering
- configure private and public IP addresses
- configure user-defined network routes
- implement subnets
- configure endpoints on subnets
- configure private endpoints
- configure Azure DNS, including custom DNS settings and private or public DNS zones

Secure access to virtual networks

- create security rules
- associate a network security group (NSG) to a subnet or network interface
- evaluate effective security rules
- implement Azure Firewall
- implement Azure Bastion

Configure load balancing

- configure Azure Application Gateway
- configure an internal or public load balancer

- troubleshoot load balancing

Monitor and troubleshoot virtual networking

- monitor on-premises connectivity
- configure and use Azure Monitor for Networks
- use Azure 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 Azure ExpressRoute
- configure Azure Virtual WAN

Monitor resources by using Azure Monitor

- configure and interpret metrics
- configure Azure Monitor logs
- query and analyze logs
- set up alerts and actions
- configure Application Insights

Implement backup and recovery

- create a Recovery Services vault
- create a Backup vault
- create and configure backup policy
- perform backup and restore operations by using Azure Backup
- perform site-to-site recovery by using Azure Site Recovery
- configure and review backup reports

COST

Course Duration	4 days
Training Fees	¥ 400,000