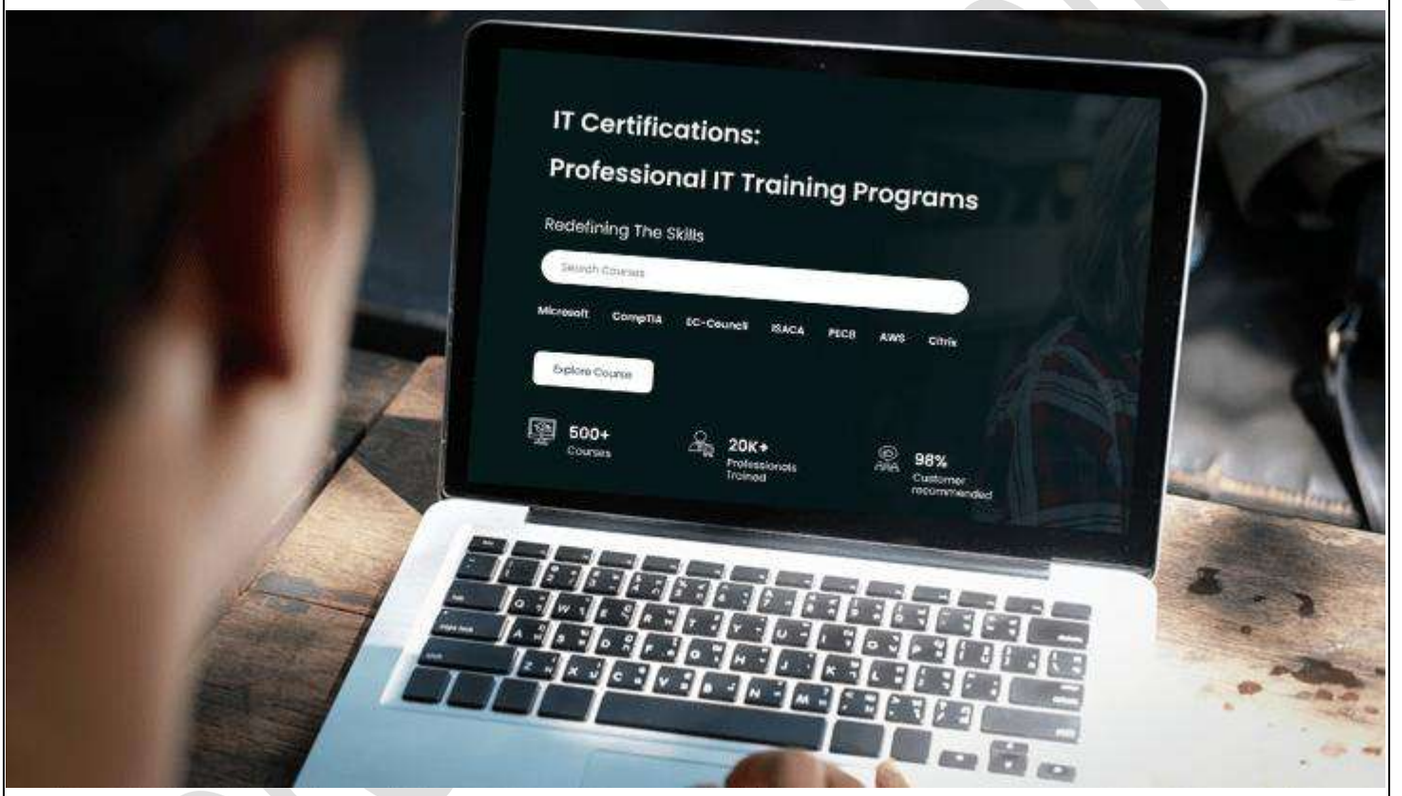
MICROTEK LEARNING | Redefining The Skills



AZ-104T00: MICROSOFT AZURE ADMINISTRATOR TRAINING

Duration: 4 Days

Course Description

AZ-104T00: Microsoft Azure Administrator is focused on teaching the right methodologies to manage Azure subscriptions, configure digital networking, implement storage and scale digital machines. This technical course is for IT professionals specifically for Azure administrators who are responsible for managing, governance, and monitoring computation in a cloud network.

AZ-104T00 certification helps professionals to:

- Connect Azure and on-site premises
- Apply Azure active directory
- Monitor solutions
- Secure identities
- Manage network traffic

Thus, by the end of this program, you will know how to manage your accounts, use role-based access control, and implement Azure policies successfully.

This training is designed based on the objectives of the course variant AZ-104T00-A.

Who should attend this course?

- Microsoft Azure Administrator Training is focused on Azure administrators.
- Azure administrators will implement, monitor, and manage various cloud services.
- Azure administrators will also communicate with vendors to provide optimal solutions to end-users for cloud applications.
- Azure administrators will give strategic recommendations to ensure the provision, monitor, size, and adjust resources as needed.
- Given below are professionals who can use Microsoft Azure Administrator to upskill their current positions:
    - System administrators
    - IT professionals with Azure experience
    - Network Engineers
    - Security Engineers
    - DevOps Engineers

What you will learn

- Learning about basic storage features
- Learning about network traffic strategies
- Learning about Azure virtual machines
- Understanding basic virtual networking concepts
- Learning administers serverless computing features
- Learning how to monitor your Azure infrastructure
- Learning about backing up files and folders including virtual machine backups
- Learning how to manage infrastructure with tools an Azure Administrator uses
- Learning how to use Azure Active Directory to secure identities and implement users and groups
- Exploring inter-site connectivity features such as Virtual Network Gateways, Site-to-Site Connections, and VNet Peering
- Learning how to manage your subscriptions and accounts by implementing Azure policies and using Role-Based Access Control

Prerequisites

- A basic understanding of on-premises virtualization technologies, including VMs, Virtual networking, and virtual hard disks is recommended.
- Understanding network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies is beneficial.
- Understanding of Active Directory concepts, including domains, forests, domain controllers, replication, Kerberos protocol, and Lightweight Directory Access Protocol (LDAP).
- Understanding of resilience and disaster recovery, including backup and restore operations.

Curriculum

Module 1: Manage identities and governance in Azure

- Understand Microsoft Entra ID
  - Describe Microsoft Entra ID.
  - Compare Microsoft Entra ID to Active Directory Domain Services (AD DS).
  - Describe how Microsoft Entra ID is used as a directory for cloud apps.
  - Describe Microsoft Entra ID P1 and P2.
  - Describe Microsoft Entra Domain Services.
- Configure user and group accounts
  - Configure user's accounts and user account properties
  - Create new user accounts
  - Import bulk user accounts with a template
  - Configure group accounts and assignment types
- Configure subscriptions
  - Determine the correct region to locate Azure services
  - Review features and use cases for Azure subscriptions
  - Obtain an Azure subscription
  - Understand billing and features for different Azure subscriptions
  - Use Microsoft Cost Management for cost analysis
  - Discover when to use Azure resource tagging
  - Identify ways to reduce costs
- Configure Azure Policy
  - Create management groups to target policies and spending budgets.
  - Implement Azure Policy with policy and initiative definitions.
  - Scope Azure policies and determine compliance.
- Configure role-based access control
  - Identify features and use cases for role-based access control.
  - List and create role definitions.
  - Create role assignments.
  - Identify differences between Azure RBAC and Microsoft Entra roles.
  - Manage access to subscriptions with RBAC.
  - Review built-in Azure RBAC roles.
- Create Azure users and groups in Microsoft Entra ID
  - Add users to Microsoft Entra ID
  - Manage app and resource access by using Microsoft Entra groups
  - Give guest users access in Microsoft Entra business-to-business (B2B)
- Secure your Azure resources with Azure role-based access control (Azure RBAC)
  - Verify access to resources for yourself and others.
  - Grant access to resources.
  - View activity logs of Azure RBAC changes.

- Allow users to reset their password with Microsoft Entra self-service password reset
    - Decide whether to implement a self-service password reset.
    - Implement self-service password reset to meet your requirements.
    - Configure self-service password reset to customize the experience.

Module 2: Configure and manage virtual networks for Azure administrators

- Configure virtual networks
    - Describe Azure virtual network features and components.
    - Identify features and usage cases for subnets and subnetting.
    - Identify usage cases for private and public IP addresses.
    - Create a virtual network and assign IP address.
- Configure network security groups
    - Determine when to use network security groups.
    - Create network security groups.
    - Implement and evaluate network security group rules.
    - Describe the function of application security groups.
- Configure Azure Virtual Network peering
    - Identify usage cases and product features of Azure Virtual Network peering.
    - Configure your network to implement Azure VPN Gateway for transit connectivity.
    - Extend peering by using a hub and spoke network with user-defined routes and service chaining.
- Configure network routing and endpoints
    - Implement system routes and user-defined routes.
    - Configure a custom route.
    - Implement service endpoints.
    - Identify features and usage cases for Azure Private Link and endpoint services.
- Configure Azure Load Balancer
    - Identify features and usage cases for Azure Load Balancer.
    - Implement public and internal Azure load balancers.
    - Compare features of load balancer SKUs and configuration differences.
    - Configure back-end pools, load-balancing rules, session persistence, and health probes.
- Configure Azure Application Gateway
    - Identify features and usage cases for Azure Application Gateway.
    - Implement an Azure application gateway, including selecting a routing method.
    - Configure gateway components, such as listeners, health probes, and routing rules.
- Design an IP addressing schema for your Azure deployment
    - Identify the private IP addressing capabilities of Azure virtual networks.
    - Identify the public IP addressing capabilities of Azure.
    - Identify the requirements for IP addressing when integrating with on-premises networks.
- Distribute your services across Azure virtual networks and integrate them by using virtual network peering
    - Identify use cases for virtual network peering.
    - Identify the features and limitations of virtual network peering.
    - Configure peering connections between virtual networks.
- Host your domain on Azure DNS
    - Configure Azure DNS to host your domain.
- Manage and control traffic flow in your Azure deployment with routes
    - Identify the routing capabilities of an Azure virtual network
    - Configure routing within a virtual network
    - Deploy a basic network virtual appliance
    - Configure routing to send traffic through a network virtual appliance

- Improve application scalability and resiliency by using Azure Load Balancer
    - Identify the features and capabilities of Azure Load Balancer.
    - Deploy and configure an Azure Load Balancer.

Module 3: Implement and manage storage in Azure

- Configure storage accounts
    - Identify features and usage cases for Azure storage accounts.
    - Select between different types of Azure Storage and create storage accounts.
    - Select a storage replication strategy.
    - Configure secure network access to storage endpoints.
- Configure Azure Blob Storage
    - Understand the purpose and benefits of Azure Blob Storage.
    - Create and configure Azure Blob Storage accounts.
    - Manage containers and blobs within Azure Blob Storage.
    - Optimize blob storage performance and scalability.
    - Implement lifecycle management policies to automate data movement and deletion.
    - Determine the best pricing plans for your Azure Blob Storage.
- Configure Azure Storage security
    - Configure a shared access signature (SAS), including the uniform resource identifier (URI) and SAS parameters.
    - Configure Azure Storage encryption.
    - Implement customer-managed keys.
    - Recommend opportunities to improve Azure Storage security.
- Configure Azure Files and Azure File Sync
    - Identify storage for file shares versus blob data.
    - Configure Azure file shares and file share snapshots.
    - Identify features and use cases of Azure File Sync.
    - Identify Azure File Sync components and configuration steps.
- Create an Azure Storage account
    - Decide how many storage accounts you need for your project
    - Determine the appropriate settings for each storage account
    - Create a storage account using the Azure portal
- Control access to Azure Storage with shared access signatures
    - Identify the features of a shared access signature for Azure Storage.
    - Identify the features of stored access policies.
    - Programmatically generate and use a shared access signature to access storage.
- Upload, download, and manage data with Azure Storage Explorer
    - Describe the features of Azure Storage Explorer.
    - Install Storage Explorer.
    - Use Storage Explorer to connect to Azure Storage services and manipulate stored data.

Module 4: Deploy and manage Azure compute resources

- Configure virtual machines
    - Determine the responsibilities of cloud service providers and customers in a cloud computing environment.
    - Identify the key considerations and factors involved in planning for virtual machines. Considerations include workload requirements, resource allocation, and secure access.
    - Configure virtual machine storage and virtual machine sizing.
    - Create a virtual machine in the Azure portal.
    - Practice deploying an Azure virtual machine and verify the configuration.

- Configure virtual machine availability
    - Implement availability sets and availability zones.
    - Implement update and fault domains.
    - Implement Azure Virtual Machine Scale Sets.
    - Autoscale virtual machines.
- Configure Azure App Service plans
    - Identify features and usage cases for Azure App Service.
    - Select an appropriate Azure App Service plan pricing tier.
    - Scale an Azure App Service plan.
- Configure Azure App Service
    - Identify features and usage cases for Azure App Service.
    - Create an app with Azure App Service.
    - Configure deployment settings, specifically deployment slots.
    - Secure your Azure App Service app.
    - Configure custom domain names.
    - Back up and restore your Azure App Service app.
    - Configure Azure Application Insights.
- Configure Azure Container Instances
    - Identify when to use containers versus virtual machines.
    - Identify the features and usage cases of Azure Container Instances.
    - Implement Azure container groups.
- Manage virtual machines with the Azure CLI
    - Create a virtual machine with the Azure CLI.
    - Resize virtual machines with the Azure CLI.
    - Perform basic management tasks using the Azure CLI.
    - Connect to a running VM with SSH and the Azure CLI.
- Create a Windows virtual machine in Azure
    - Create a Windows virtual machine using the Azure portal.
    - Connect to a running Windows virtual machine using Remote Desktop.
    - Install software and change the network configuration on a VM using the Azure portal.
- Host a web application with Azure App Service
    - Use the Azure portal to create an Azure App Service web app.
    - Use developer tools to create the code for a starter web application.
    - Deploy your code to Azure App Service.

Module 5: Monitor and back up Azure resources

- Introduction to Azure Backup
    - Evaluate whether Azure Backup is appropriate to use for your backup needs.
    - Describe how the features of Azure Backup work to provide backup solutions for your needs.
- Configure virtual machine backups
    - Identify features and usage cases for different Azure backup methods.
    - Configure virtual machine snapshots and backup options.
    - Implement virtual machine backup and restore, including soft delete.
    - Perform site-to-site recovery by using Azure Site Recovery.
- Configure Azure Monitor
    - Identify the features and usage cases for Azure Monitor.
    - Configure and interpret metrics and logs.
    - Identify the Azure Monitor components and data types.
    - Configure the Azure Monitor activity log.

- Configure Log Analytics
    - Identify the features and usage cases for Log Analytics.
    - Create a Log Analytics workspace.
    - Structure a Log Analytics query and review results.
- Configure Network Watcher
    - Identify the features and usage cases for Azure Network Watcher.
    - Configure diagnostic capabilities like IP Flow Verify, Next Hop, and Network Topology.
- Improve incident response with Azure Monitor alerts
    - Configure alerts on events in your Azure resources based on metrics, log events, and activity log events.
    - Learn how to use action groups in response to an alert, and how to use alert processing rules to override action groups when necessary.
- Analyze your Azure infrastructure by using Azure Monitor logs
    - Identify the features and capabilities of Azure Monitor logs.
    - Create basic Azure Monitor log queries to extract information from log data.
- Monitor your Azure virtual machines with Azure Monitor
    - Understand which monitoring data you need to collect from your VM.
    - Enable and view recommended alerts and diagnostics.
    - Use Azure Monitor to collect and analyze VM host metrics data.
    - Use Azure Monitor Agent to collect VM client performance metrics and event logs.

For any query Contact Us – Microtek Learning