

AZ-104T00-A: Microsoft Azure Administrator

Course Summary

Description

This course teaches IT Professionals how to manage their Azure subscriptions, secure identities, administer the infrastructure, configure virtual networking, connect Azure and on-premises sites, manage network traffic, implement storage solutions, create and scale virtual machines, implement web apps and containers, back up and share data, and monitor your solution.

Topics

- Configure Microsoft Entra ID
- Configure user and group accounts
- Configure subscriptions
- Configure Azure Policy
- Configure role-based access control
- Configure Azure resources with tools
- Use Azure Resource Manager
- Configure resources with Azure Resource Manager templates
- Configure virtual networks
- Configure network security groups
- Configure Azure DNS
- Configure Azure virtual network peering
- Configure network routing and endpoints
- Configure Azure Load Balancer
- Configure Azure Application Gateway
- Configure storage accounts
- Configure Azure Blob Storage
- Configure Azure Storage security
- Configure Azure Files and Azure File Sync
- Configure Azure Storage with tools
- Configure virtual machines
- Configure virtual machine availability
- Configure Azure app service plans
- Configure Azure App Services
- Configure Azure Container Instances
- Configure file and folder backups
- Configure virtual machine backups
- Configure Azure Monitor
- Configure Azure alerts
- Configure Log Analytics
- Configure Network Watcher

Audience

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

Before attending this course, students must have:

- Successful Azure Administrators start this role with experience on operating systems, virtualization, cloud infrastructure, storage structures, and networking.
- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- 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.

Duration

Four days

AZ-104T00-A: Microsoft Azure Administrator

Course Outline

I. Configure Microsoft Entra ID

- A. Define Microsoft Entra concepts, including identities, accounts, and tenants.
- B. Describe Microsoft entra features to support different configurations.
- C. Understand differences between Microsoft Entra ID and Active Directory Domain Services (AD DS)
- D. Choose between supported editions of Microsoft Entra ID.
- E. Use the Microsoft Entra self-service password reset feature.
- B. List and create role definitions.
- C. Create role assignments.
- D. Identify differences between Azure RBAC and Azure Active Directory roles.
- E. Manage access to subscriptions with RBAC.
- F. Review built-in Azure RBAC roles.

II. Configure user and group accounts

- A. Configure users accounts and user account properties.
- B. Create new user accounts.
- C. Import bulk user accounts with a template.
- D. Configure group accounts and assignment types.

III. Configure subscriptions

- A. Determine the correct region to locate Azure services.
- B. Review features and use cases for Azure subscriptions.
- C. Obtain an Azure subscription.
- D. Understand billing and features for different Azure subscriptions.
- E. Use Microsoft Cost Management for cost analysis.
- F. Discover when to use Azure resource tagging.
- G. Identify ways to reduce costs.

IV. Configure Azure Policy

- A. Create management groups to target policies and spending budgets.
- B. Implement Azure Policy with policy and initiative definitions.
- C. Scope Azure policies and determine compliance.

V. Configure role-based access control

- A. Identify features and use cases for role-based access control.

VI. Configure Azure resources with tools

- A. Manage resources with the Azure portal.
- B. Manage resources with Azure Cloud Shell.
- C. Manage resources with Azure PowerShell.
- D. Manage resources with Azure CLI.

VII. Use Azure Resource Manager

- A. Identify the features and usage cases for Azure Resource Manager.
- B. Describe each Azure Resource Manager component and its usage.
- C. Organize your Azure resources with resource groups.
- D. Apply Azure Resource Manager locks.
- E. Move Azure resources between groups, subscriptions, and regions.
- F. Remove resources and resource groups.
- G. Apply and track resource limits.

AZ-104T00-A: Microsoft Azure Administrator

Course Outline (summary)

VIII. Configure resources with Azure Resource Manager templates

- A. List the advantages of Azure templates.
- B. Identify the Azure template schema components.
- C. Specify Azure template parameters.
- D. Locate and use Azure Quickstart Templates.

IX. Configure virtual networks

- A. Describe Azure virtual network features and components.
- B. Identify features and usage cases for subnets and subnetting.
- C. Identify usage cases for private and public IP addresses.
- D. Create and determine which resources require public IP addresses.
- E. Create and determine which resources require private IP addresses.
- F. Create virtual networks.

X. Configure network security groups

- A. Determine when to use network security groups.
- B. Implement network security group rules.
- C. Evaluate network security group effective rules.
- D. Examine advantages of application security groups.

XI. Configure Azure DNS

- A. Identify features and usage cases for domains, custom domains, and private zones.
- B. Verify custom domain names using DNS records.
- C. Implement DNS zones, DNS delegation, and DNS record sets.

XII. Configure Azure virtual network peering

- A. Identify usage cases and product features of Azure virtual network peering.
- B. Configure your network to implement Azure VPN Gateway for transit connectivity.

- C. Extend peering by using a hub and spoke network with user-defined routes and service chaining.

XIII. Configure network routing and endpoints

- A. Implement system routes and user-defined routes.
- B. Configure a custom route.
- C. Implement service endpoints.
- D. Identify features and usage cases for private links and endpoint services.

XIV. Configure Azure Load Balancer

- A. Identify features and usage cases for Azure load balancer.
- B. Implement public and internal Azure load balancers.
- C. Configure load balancer SKUs, backend pools, session persistence, and health probes.
- D. Configure back-end pools, load-balancing rules, session persistence, and health probes.

XV. Configure Azure Application Gateway

- A. Identify features and usage cases for Azure Application Gateway.
- B. Implement Azure Application Gateway, including selecting a routing method.
- C. Configure gateway components, such as listeners, health probes, and routing rules.

XVI. Configure storage accounts

- A. Identify features and usage cases for Azure storage accounts.
- B. Select between different types of Azure Storage and storage accounts.
- C. Select a storage replication strategy.
- D. Configure network access to storage accounts.
- E. Secure storage endpoints.

AZ-104T00-A: Microsoft Azure Administrator

Course Outline (summary)

XVII. Configure Azure Blob Storage

- A. Identify features and usage cases for Azure Blob Storage.
- B. Configure Blob Storage and Blob access tiers.
- C. Configure Blob lifecycle management rules.
- D. Configure Blob object replication.
- E. Upload and price Blob Storage

XVIII. Configure Azure Storage security

- A. Configure a shared access signature (SAS), including the uniform resource identifier (URI) and SAS parameters.
- B. Configure Azure Storage encryption.
- C. Implement customer-managed keys.
- D. Recommend opportunities to improve Azure Storage security.

XIX. Configure Azure Files and Azure File Sync

- A. Identify storage for file shares and blob data.
- B. Configure Azure Files shares and file share snapshots.
- C. Identify features and usage cases of Azure File Sync.
- D. Identify Azure File Sync components and configuration steps.

XX. Configure Azure Storage with tools

- A. Configure and use Azure Storage Explorer.
- B. Configure the Azure Import/Export service.
- C. Use the WAImportExport tool with the Azure Import/Export service.
- D. Configure and use AZCopy.

XXI. Configure virtual machines

- A. Create a virtual machine planning checklist.
- B. Determine virtual machine locations and pricing models.
- C. Determine the correct virtual machine size.
- D. Configure virtual machine storage.

XXII. Configure virtual machine availability

- A. Implement availability sets and availability zones.
- B. Implement update and fault domains.
- C. Implement Virtual Machine Scale Sets.
- D. Autoscale virtual machines.

XXIII. Configure Azure app service plans

- A. Identify features and usage cases of the Azure App Service.
- B. Select an appropriate Azure App Service plan pricing tier.
- C. Scale the App Service Plan.
- D. Scale out the App Service Plan.

XXIV. Configure Azure App Services

- A. Identify features and usage cases for the Azure App Service.
- B. Create an app with Azure App Service.
- C. Configure deployment settings, specifically deployment slots.
- D. Secure your Azure App Service app.
- E. Configure custom domain names.
- F. Back up and restore your Azure App Service app.
- G. Configure Azure Application Insights.

XXV. Configure Azure Container Instances

- A. Identify when to use containers versus virtual machines.
- B. Identify the features and usage cases of Azure Container Instances.
- C. Implement Azure Container Groups.

AZ-104T00-A: Microsoft Azure Administrator

Course Outline (summary)

XXVI. *Configure file and folder backups*

- A. Identify features and usage cases for Azure Backup.
- B. Configure Azure Recovery Services Vault backup options.
- C. Implement on-premises file and folder backup.
- D. Configure the Microsoft Azure Recovery Services (MARS) agent for Azure Backup.

- B. Configure diagnostic capabilities like IP Flow Verify, Next Hop, and Network Topology.

XXVII. *Configure virtual machine backups*

- A. Identify features and usage cases for different Azure backup methods.
- B. Configure virtual machine snapshots and backup options.
- C. Implement virtual machine backup and restore, including soft delete.
- D. Compare the Azure Backup agent to the Azure Backup Server.
- E. Perform site-to-site recovery by using Azure Site Recovery.

XXVIII. *Configure Azure Monitor*

- A. Identify the features and usage cases for Azure Monitor.
- B. Configure and interpret metrics and logs.
- C. Identify the Azure Monitor components and data types.
- D. Configure the Azure Monitor Activity Log.

XXIX. *Configure Azure alerts*

- A. Identify Azure Monitor alerts, including alert types and alert states.
- B. Configure Azure Monitor alerts.
- C. Create alert rules and action groups

XXX. *Configure Log Analytics*

- A. Identify the features and usage cases for Log Analytics.
- B. Create a Log Analytics workspace.
- C. Structure a Log Analytics query and review results.

XXXI. *Configure Azure Network Watcher*

- A. Identify the features and usage cases for Azure Network Watcher.