MICROSOFT AZURE ADMINISTRATOR Course (AZ–104T)

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.

آنچه خواهید آموخت

Students will learn to,

- 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 Service
- Configure Azure Container Instances
- Configure file and folder backups

⊕ info@gandotech.com
⦿ Lisbon, Sintra, Mirante St, No3, 2/C
▢ +351 911970800
✉ P.Code: 27 45-039

- Configure virtual machine backups
- Configure Azure Monitor
- Configure Azure alerts
- Configure Log Analytics
- Configure Network Watcher

سرفصل ها

Module 1 : Configure Microsoft Entra ID

- Define Microsoft Entra concepts, including identities, accounts, and tenants.
- Describe Microsoft Entra features to support different configurations.
- Understand differences between Microsoft Entra ID and Active Directory Domain Services (AD DS).
- Choose between supported editions of Microsoft Entra ID.
- Implement the Microsoft Entra join feature.
- Use the Microsoft Entra self–service password reset feature.

Module 2: Configure user and group accounts

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

Module 3: 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.

Module 4: 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.

Module 5: 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 Azure Active Directory roles.
- Manage access to subscriptions with RBAC.
- Review built-in Azure RBAC roles.

Module 6: Configure Azure resources with tools

- Manage resources with the Azure portal.
- Manage resources with Azure Cloud Shell.
- Manage resources with Azure PowerShell.
- Manage resources with Azure CLI.

Module 7: Use Azure Resource Manager

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

Module 8: Configure resources with Azure Resource Manager templates

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

Module 9: 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 and determine which resources require public IP addresses.

- Create and determine which resources require private IP addresses.
- Create virtual networks.

Module 10: Configure network security groups

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

Module 11 : Configure Azure DNS

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

Module 12 : 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.

Module 13 : 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 private links and endpoint services.

Module 14 : 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.

Module 15 : Configure Azure Application Gateway

- Identify features and usage cases for Azure Application Gateway.
- Implement Azure Application Gateway, including selecting a routing method.

- Configure gateway components, such as listeners, health probes, and routing rules.

Module 16: Configure storage accounts

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

Module 17 : Configure Azure Blob Storage

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

Module 18 : 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.

Module 19 : Configure Azure Files and Azure File Sync

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

Module 20 : Configure Azure Storage with tools

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

Module 21 : Configure virtual machines

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

Module 22: Configure virtual machine availability

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

Module 23 : Configure Azure app service plans

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

Module 24 : Configure Azure App Services

- Identify features and usage cases for the 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.

Module 25 : 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.

Module 26 : Configure file and folder backups

- Identify features and usage cases for Azure Backup.
- Configure Azure Recovery Services Vault backup options.

- Implement on-premises file and folder backup.
- Configure the Microsoft Azure Recovery Services (MARS) agent for Azure Backup.

Module 27 : 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.
- Compare the Azure Backup agent to the Azure Backup Server .
- Perform site-to-site recovery by using Azure Site Recovery.

Module 28 : 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.

Module 29 : Configure Azure alerts

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

Module 30 : 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.

Module 31 : 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.

پیش نیازها

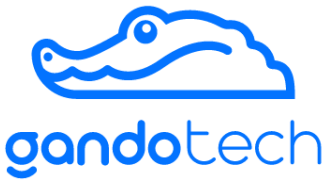Successful Azure Administrators start this role with experience in virtualization, networking, Identity, and storage.

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

- Understanding of network configurations, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of Active Directory concepts, including users, groups, and role–based access control.
- Understanding of resilience and disaster recovery, including backup and restore operations.

مدارک مرتبط

AZ–104: Microsoft Azure Administrator