

Syllabus

Microsoft Certified: Azure Administrator Associate

Exam AZ-104: Microsoft Azure Administrator

1. Manage Azure identities and governance (15–20%)

1.1 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

1.2 Manage role-based access control (RBAC)

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

1.3 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

2. Implement and manage storage (15–20%)

2.1 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

2.2 Manage storage

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

2.3 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

3. Deploy and manage Azure compute resources (20–25%)

3.1 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

3.2 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

3.3 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

3.4 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

4. Configure and manage virtual networking (25–30%)

4.1 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

4.2 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

4.3 Configure load balancing

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

4.4 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

4.5 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

5. Monitor and back up Azure resources (10–15%)

5.1 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

5.2 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