# Microsoft Azure Administrator

**Exam number:** AZ-103

**Exam title:** Microsoft Azure Administrator

## Exam Design

**Audience Profile**

Candidates for this exam are Azure Administrators who manage cloud services that span storage, security, networking, and compute cloud capabilities. Candidates have a deep understanding of each service across the full IT lifecycle, and take requests for infrastructure services, applications, and environments. They make recommendations on services to use for optimal performance and scale, as well as provision, size, monitor, and adjust resources as appropriate.

Candidates for this exam should have proficiency in using PowerShell, the Command Line Interface, Azure Portal, ARM templates, operating systems, virtualization, cloud infrastructure, storage structures, and networking.

## Skills measured

### 1. Manage Azure subscriptions and resources (15-20%)

**1.1 Manage Azure subscriptions**
*May include but not limited to:* Assign administrator permissions; configure cost center quotas and tagging; configure Azure subscription policies at Azure subscription level

**1.2 Analyze resource utilization and consumption**
*May include but not limited to:* Configure diagnostic settings on resources; create baseline for resources; create and rest alerts; analyze alerts across subscription; analyze metrics across subscription; create action groups; monitor for unused resources; monitor spend; report on spend; utilize Log Search query functions; view alerts in Log Analytics

**1.3 Manage resource groups**
*May include but not limited to:* Use Azure policies for resource groups; configure resource locks; configure resource policies; implement and set tagging on resource groups; move resources across resource groups; remove resource groups

**1.4 Managed role based access control (RBAC)**
*May include but is not limited to*: Create a custom role, configure access to Azure resources by assigning roles, configure management access to Azure, troubleshoot RBAC, implement RBAC policies, assign RBAC Roles

## 2. Implement and manage storage (20-25%)

### 2.1 Create and configure storage accounts
*May include but not limited to:* Configure network access to the storage account; create and configure storage account; generate shared access signature; install and use Azure Storage Explorer; manage access keys; monitor activity log by using Log Analytics; implement Azure storage replication

### 2.2 Import and export data to Azure
*May include but not limited to:* Create export from Azure job; create import into Azure job; Use Azure Data Box; configure and use Azure blob storage; configure Azure content delivery network (CDN) endpoints

### 2.3 Configure Azure files
*May include but not limited to:* Create Azure file share; create Azure File Sync service; create Azure sync group; troubleshoot Azure File Sync

### 2.4 Implement Azure backup
*May include but not limited to:* Configure and review backup reports; perform backup operation; create Recovery Services Vault; create and configure backup policy; perform a restore operation

## 3. Deploy and manage virtual machines (VMs) (20-25%)

### 3.1 Create and configure a VM for Windows and Linux
*May include but not limited to:* Configure high availability; configure monitoring, networking, storage, and virtual machine size; deploy and configure scale sets

### 3.2 Automate deployment of VMs
*May include but not limited to:* Modify Azure Resource Manager (ARM) template; configure location of new VMs; configure VHD template; deploy from template; save a deployment as an ARM template; deploy Windows and Linux VMs

### 3.3 Manage Azure VM
*May include but not limited to:* Add data discs; add network interfaces; automate configuration management by using PowerShell Desired State Configuration (DSC) and VM Agent by using custom script extensions; manage VM sizes; move VMs from one resource group to another; redeploy VMs

### 3.4 Manage VM backups
*May include but not limited to:* Configure VM backup; define backup policies; implement backup policies; perform VM restore; Azure Site Recovery

## 4. Configure and manage virtual networks (20-25%)

### 4.1 Create connectivity between virtual networks
*May include but not limited to:* Create and configure VNET peering; create and configure VNET to VNET; verify virtual network connectivity; create virtual network gateway

**4.2 Implement and manage virtual networking**

*May include but not limited to:* Configure private and public IP addresses, network routes, network interface, subnets, and virtual network

**4.3 Configure name resolution**

*May include but not limited to:* Configure Azure DNS; configure custom DNS settings; configure private and public DNS zones

**4.4 Create and configure a Network Security Group (NSG)**

*May include but not limited to:* Create security rules; associate NSG to a subnet or network interface; identify required ports; evaluate effective security rules

**4.5 Implement Azure load balancer**

May include but is not limited to: Configure internal load balancer, configure load balancing rules, configure public load balancer, troubleshoot load balancing

**4.6 Monitor and troubleshoot virtual networking**

May include but is not limited to: Monitor on-premises connectivity, use Network resource monitoring, use Network Watcher, troubleshoot external networking, troubleshoot virtual network connectivity

**4.7 Integrate on premises network with Azure virtual network**

May include but is not limited to: Create and configure Azure VPN Gateway, create and configure site to site VPN, configure Express Route, verify on premises connectivity, troubleshoot on premises connectivity with Azure

## 5. Manage identities (15-20%)

**5.1 Manage Azure Active Directory (AD)**

*May include but not limited to*: Add custom domains; Azure AD Join; configure self-service password reset; manage multiple directories;

**5.2 Manage Azure AD objects (users, groups, and devices)**

*May include but not limited to:* Create users and groups; manage user and group properties; manage device settings; perform bulk user updates; manage guest accounts

**5.3 Implement and manage hybrid identities**

*May include but not limited to:* Install Azure AD Connect, including password hash and pass-through synchronization; use Azure AD Connect to configure federation with on-premises Active Directory Domain Services (AD DS); manage Azure AD Connect; manage password sync and password writeback

**5.4 Implement multi-factor authentication (MFA)**

*May include but is not limited to*: Configure user accounts for MFA, enable MFA by using bulk update, configure fraud alerts, configure bypass options, configure Trusted IPs, configure verification methods

---

**Commented [SJ2]:** Formerly AZ101 3.2

**Commented [SJ3]:** Objective renamed, formerly "Monitor and manage networking" (AZ101 3.3)

**Commented [SJ4]:** Formerly AZ101 3.3

**Commented [SJ5]:** Formerly AZ101 3.4

**Commented [SJ6]:** Formerly AZ 101 4.1