Exam AZ-103: Microsoft Azure Administrator – Skills Measured

A NEW VERSION OF THIS EXAM, AZ-104, WILL BE AVAILABLE IN LATE MARCH/EARLY APRIL. You will still be able to take this exam for ~90 days after the release of AZ-104. Specific dates related to the availability of AZ-104 and the retirement of AZ-103 will be posted to the website when they are known. The objective domain for AZ-104 is appended below.

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

Manage Azure subscriptions and resources (15-20%)

Manage Azure subscriptions

May include but not limited to:

- assign administrator permissions
- configure cost center quotas and tagging
- configure policies at Azure subscription level
- implement Management Groups

Analyze resource utilization and consumption

May include but not limited to:

- configure diagnostic settings on resources
- create baseline for resources
- create and test alerts
- analyze alerts across subscription
- analyze metrics across subscription

- create action groups and action rules
- monitor for unused resources
- monitor spend
- report on spend
- utilize log queries in Azure Monitor
- view alerts in Azure Monitor

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

Managed role based access control (RBAC)

May include but 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

Implement and manage storage (15-20%)

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 Monitor Logs
- implement Azure storage replication
- implement Azure AD Authentication

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
- use Azure Data Factory to transfer data to Azure

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

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

Deploy and manage virtual machines (VMs) (15-20%)

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

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

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
- soft delete for Azure VMs

Manage VM backups

May include but not limited to:

- configure VM backup
- define backup policies
- implement backup policies
- perform VM restore
- Azure Site Recovery

Configure and manage virtual networks (30-35%)

Create connectivity between virtual networks

May include but not limited to:

- create and configure VNET peering
- create and configure VNET to VNET connections
- verify virtual network connectivity
- create virtual network gateway

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

Configure name resolution

May include but not limited to:

- configure Azure DNS
- configure custom DNS settings
- configure private and public DNS zones

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
- implement Application Security Groups

Implement Azure load balancer

May include but not limited to:

- configure internal load balancer
- configure load balancing rules
- configure public load balancer
- troubleshoot load balancing

Monitor and troubleshoot virtual networking

May include but not limited to:

- monitor on-premises connectivity
- use Network resource monitoring
- use Network Watcher
- troubleshoot external networking
- troubleshoot virtual network connectivity

Integrate on premises network with Azure virtual network

May include but 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
- use Azure network adapter

Manage identities (15-20%)

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

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

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

Implement multi-factor authentication (MFA)

May include but 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

AZ-103/104 Comparison

Microsoft Azure Administrator

Current Skills Measured as of January 15, 2020	Updated Skills Measured List (ignore the numbering below)
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.	**Audience Profile** The Azure Administrator implements, manages, and monitors identity, governance, storage, compute~~virtual machines~~, and virtual networks in a cloud environment. ~~This role focuses primarily on enabling Infrastructure as a Service (IaaS)~~. The Azure Administrator will provision, size, monitor, and adjust resources as appropriate. **Candidates should have a minimum of six months of hands-on experience administering Azure. Candidates should have a strong understanding of core Azure services, Azure workloads, security, and governance. Candidates for this exam should have experience in using PowerShell, the Command Line Interface, Azure Portal, and ARM templates.**
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 policies at Azure subscription level **1.2 Analyze resource utilization and consumption**	**6. Manage Azure Identities and Governance (15-20%)** **6.1 Manage Azure AD objects** *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 • configure Azure AD Join

May include but not limited to: Configure diagnostic settings on resources; create baseline for resources; create and test alerts; analyze alerts across subscription; analyze metrics across subscription; create action groups and action rules; monitor for unused resources; monitor spend; report on spend; utilize log queries in Azure Monitor; view alerts in Azure Monitor
 	
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
	• configure self-service password reset
	• NOT: Azure AD Connect; PIM
	
	6.2 Manage role-based access control (RBAC)
	
	May include but not limited to:
	
	• create a custom role
	• provide access to Azure resources by assigning roles
	  ○ subscriptions
	  ○ resource groups
	  ○ resources (VM, disk, etc.)
	• interpret access assignments
	• manage multiple directories
	
	6.3 Manage subscriptions and governance
	
	May include but not limited to:
	
	• configure Azure policies
	• configure resource locks
	• apply tags
	• create and manage resource groups
	  ○ move resources
	  ○ remove RGs
	• manage subscriptions
	• configure Cost Management
	• configure management groups

<u>2. Implement and manage storage</u> (15-20%) **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	**<u>7. Implement and Manage Storage</u> (10-15%)** **7.1 Manage storage accounts** *May include but not limited to:* • configure network access to storage accounts • create and configure storage accounts • generate shared access signature

access keys; monitor activity log by using Monitor Logs; implement Azure storage replication; Implement Azure AD Authentication, manage blob storage lifecycle management **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	• manage access keys • implement Azure storage replication • configure Azure AD Authentication for a storage account **7.2 Manage data in Azure Storage** *May include but not limited to:* • export from Azure job • import into Azure job • install and use Azure Storage Explorer • copy data by using AZCopy **7.3 Configure Azure files and Azure blob storage** *May include but not limited to:* • create an Azure file share • create and configure Azure File Sync service • configure Azure blob storage • configure storage tiers for Azure blobs
<u>3. Deploy and manage virtual machines (VMs)</u> (15-20%) **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	**<u>8. Deploy and Manage Azure Compute Resources</u> (25-30%)** **8.1 Configure VMs for high availability and scalability** *May include but not limited to:* • configure high availability • deploy and configure scale sets **8.2 Automate deployment and configuration of VMs** *May include but not limited to:*

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; soft delete for Azure VMs; Azure Site Recovery	• modify Azure Resource Manager (ARM) template • configure VHD template • deploy from template • save a deployment as an ARM template • automate configuration management by using custom script extensions **8.3 Create and configure VMs** *May include but not limited to:* • configure Azure Disk Encryption • move VMs from one resource group to another • manage VM sizes • add data discs • configure networking • redeploy VMs **8.4 Create and configure containers** • create and configure Azure Kubernetes Service (AKS) • create and configure Azure Container Instances (ACI) • NOT: selecting an container solution architecture or product; container registry settings **8.5 Create and configure Web Apps** • create and configure App Service • create and configure App Service Plans • NOT: Azure Functions; Logic Apps; Event Grid
4. Configure and manage virtual networks (30-35%) **4.1 Create connectivity between virtual**	**9. Configure and Manage Virtual Networking (30-35%)** **9.1 Implement and manage virtual**

networks *May include but not limited to*: Create and configure VNET peering; create and configure VNET to VNET connections; 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,	**networking** *May include but not limited to:* • create and configure VNET peering • configure private and public IP addresses, network routes, network interface, subnets, and virtual network **9.2 Configure name resolution** *May include but not limited to:* • configure Azure DNS • configure custom DNS settings • configure a private or public DNS zone **9.3 Secure access to virtual networks** *May include but not limited to:* • create security rules • associate an NSG to a subnet or network interface • evaluate effective security rules • deploy and configure Azure Firewall • deploy and configure Azure Bastion Service • NOT: Implement Application Security Groups; DDoS **9.4 Configure load balancing** *May include but not limited to:* • configure Application Gateway • configure an internal load balancer • configure load balancing rules • configure a public load balancer • troubleshoot load balancing • NOT: Traffic Manager and FrontDoor and PrivateLink **9.5 Monitor and troubleshoot virtual**

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	**networking** *May include but not limited to:* • monitor on-premises connectivity • use Network resource monitoring • use Network Watcher • troubleshoot external networking • troubleshoot virtual network connectivity **9.6 Integrate an on-premises network with an Azure virtual network** *May include but not limited to:* • create and configure Azure VPN Gateway • create and configure VPNs • configure ExpressRoute • verify on premises connectivity • configure Azure Virtual WAN
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**	[NO EQUIVALENT --- SEE NEW FG 5 BELOW]

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	

	<u>10. Monitor and back up Azure resources</u> (10-15%)
	
	10.1 Monitor resources by using Azure Monitor
	
	May include but not limited to:
	
	• configure and interpret metrics
	  ○ analyze metrics across subscriptions
	• configure Log Analytics
	  ○ implement a Log Analytics workspace
	  ○ configure diagnostic settings
	• query and analyze logs
	  ○ create a query
	  ○ save a query to the dashboard
	  ○ interpret graphs
	• set up alerts and actions
	  ○ create and test alerts
	  ○ create action groups
	  ○ view alerts in Azure Monitor
	  ○ analyze alerts across subscriptions
	• configure Application Insights

	• NOT: Network monitoring **10.2 Implement backup and recovery** *May include but not limited to:* • configure and review backup reports • perform backup and restore operations by using Azure Backup Service • create a Recovery Services Vault ○ use soft delete to recover Azure VMs • create and configure backup policy • perform site-to-site recovery by using Azure Site Recovery • NOT: SQL or HANA