



AZ-104^{Q&As}

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.passapply.com/az-104.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

You have an Azure virtual machine named VM1.

You use Azure Backup to create a backup of VM1 named Backup1.

After creating Backup1, you perform the following changes to VM1:

1.

Modify the size of VM1.

2.

Copy a file named Budget.xls to a folder named Data.

3.

Reset the password for the built-in administrator account.

4.

Add a data disk to VM1.

An administrator uses the Replace existing option to restore VM1 from Backup1.

You need to ensure that all the changes to VM1 are restored.

Which change should you perform again?

A. Modify the size of VM1.

B. Reset the password for the built-in administrator account.

C. Add a data disk.

D. Copy Budget.xls to Data.

Correct Answer: D

Reference: <https://docs.microsoft.com/en-us/azure/backup/about-azure-vm-restore>

QUESTION 2

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has an Azure subscription with two storage accounts. Each of these storage accounts includes a queue service, a table service, and a blob service.

You have created two apps that must be configured to store various types of data to all the storage services on the two storage accounts.



You need to configure the required amount of endpoints for the apps.

Solution: You configure two endpoints per app.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: A

Each app needs a service endpoint in each Storage Account.

Reference: <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You need to ensure that an Azure Active Directory (Azure AD) user named Admin1 is assigned the required role to enable Traffic Analytics for an Azure subscription.

Solution: You assign the Network Contributor role at the subscription level to Admin1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Your account must meet one of the following to enable traffic analytics:

Your account must have any one of the following Azure roles at the subscription scope: owner, contributor, reader, or network contributor.

Reference: <https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics-faq>

QUESTION 4

You have an Azure App Service plan named AdatumASP1 that uses the P2v2 pricing tier. AdatumASP1 hosts MI Azure web app named adatumwebapp1. You need to delegate the management of adatumwebapp1 to a group named Devs. Devs must be able to perform the following tasks:

1.



Add deployment slots.

2.

View the configuration of AdatumASP1.

3.

Modify the role assignment for adatumwebapp1.

Which role should you assign to the Devs group?

A. Owner

B. Contributor

C. Web Plan Contributor

D. Website Contributor

Correct Answer: A

Owner : Correct Choice

The Owner role lets you manage everything, including access to resources.

Contributor : Incorrect Choice

With contributor role you can Add deployment slots and View the configuration of App service plan but you can't Modify the role assignment. For this you need User Access Administrator or Owner role. So this is incorrect.

Web Plan Contributor : Incorrect Choice

The Web Plan Contributor role lets you manage the web plans for websites, but not access to them.

So this option is incorrect.

Website Contributor : Incorrect Choice

The Website Contributor role lets you manage websites (not web plans), but not access to them. So this is incorrect option.

Note:

As per least privilege principle it is not advisable to provide owner role to any group, rather you should create custom RBAC role with custom policy and use that role for this operation. However as this option is not available here so only option

to go with owner role.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>



QUESTION 5

You create an Azure Storage account named contosostorage.

You plan to create a file share named data.

Users need to map a drive to the data file share from home computers that run Windows 10. Which port should be open between the home computers and the data file share?

- A. 80
- B. 443
- C. 445
- D. 3389

Correct Answer: C

Ensure port 445 is open: The SMB protocol requires TCP port 445 to be open; connections will fail if port 445 is blocked.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

QUESTION 6

You have an Azure subscription that contains a storage account named account1.

You plan to upload the disk files of a virtual machine to account1 from your on-premises network. The on-premises network uses a public IP address space of 131.107.1.0/24.

You plan to use the disk files to provision an Azure virtual machine named VM1. VM1 will be attached to a virtual network named VNet1. VNet1 uses an IP address space of 192.168.0.0/24.

You need to configure account1 to meet the following requirements:

1.
Ensure that you can upload the disk files to account1.
2.
Ensure that you can attach the disks to VM1.
3.
Prevent all other access to account1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. From the Networking blade of account1, select Selected networks.



- B. From the Networking blade of account1, select Allow trusted Microsoft services to access this storage account.
- C. From the Networking blade of account1, add the 131.107.1.0/24 IP address range.
- D. From the Networking blade of account1, add VNet1.
- E. From the Service endpoints blade of VNet1, add a service endpoint.

Correct Answer: AC

QUESTION 7

Your on-premises network contains an SMB share named Share1. You have an Azure subscription that contains the following resources:

1.

A web app named webapp1

2.

A virtual network named VNET1

You need to ensure that webapp1 can connect to Share1.

What should you deploy?

- A. an Azure Application Gateway
- B. an Azure Active Directory (Azure AD) Application Proxy
- C. an Azure Virtual Network Gateway

Correct Answer: C

A Site-to-Site VPN gateway connection can be used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device, a VPN gateway, located on-premises that has an externally facing public IP address assigned to it.

Incorrect Answers:

B: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client.

Reference: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

QUESTION 8

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while



others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an app named App1 that is installed on two Azure virtual machines named VM1 and VM2. Connections to App1 are managed by using an Azure Load Balancer.

The effective network security configurations for VM2 are shown in the following exhibit.

Home > VM2 - Networking

VM2 - Networking
Virtual machine

Search (Ctrl+/) Attach network interface Detach network interface

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Networking Disks Size Security Extensions

Network Interface: VM2-NIC1 Effective security rules Topology

Virtual network/subnet: Vnet1/Subnet11 NIC Public IP: - NIC Private IP: 10.240.11.5 Accelerated networking: Disabled

Inbound port rules Outbound port rules Application security groups Load balancing

Network security group NSG2 (attached to network interface: Subnet11)
Impacts 1 subnets, 0 network interfaces

Add inbound port rule

Priority	Name	Port	Protocol	Source	Destination	Action
100	Allow_131.107.100.50	443	TCP	131.107.100.50	VirtualNetwork	Allow
200	BlockAllOther441	443	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

You discover that connections to App1 from 131.107.100.50 over TCP port 443 fail.

You verify that the Load Balancer rules are configured correctly.

You need to ensure that connections to App1 can be established successfully from 131.107.100.50 over TCP port 443.

Solution: You modify the priority of the Allow_131.107.100.50 inbound security rule.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

llow_131.107.100.50 rule has a higher priority (100). The issue is not related with the priority of the rule.

QUESTION 9

You have an Azure AD tenant named adatum.com that contains the groups shown in the following table.



Name	Type	Member of
Group1	Security	None
Group2	Security	Group1

Adatum.com contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You assign an Azure Active Directory Premium P2 license to Group1 as shown in the following exhibit.



Assign license ...



Got feedback?

Users and groups

Assignment options

Review + assign

Azure Active Directory Premium P2

Azure Active Directory Premium P1

Off

On

Azure Active Directory Premium P2

Off

On

Microsoft Azure Multi-Factor Authentication

Off

On

Microsoft Defender for Cloud Apps Discovery

Off

On

Group2 is NOT directly assigned a license.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point

Hot Area:

Statements

You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.

Yes

☐

No

☐

You can remove the Azure Active Directory Premium P2 license from User1.

☐☐

User2 is assigned the Azure Active Directory Premium P2.

☐☐

Correct Answer:



Statements

You can assign User1 the Microsoft Defender for Cloud Apps Discovery license.

Yes

☐

No

☒

You can remove the Azure Active Directory Premium P2 license from User1.

☐☒

User2 is assigned the Azure Active Directory Premium P2.

☐☒

QUESTION 10

You have an Azure virtual machine named VMV

The network interface for VM1 is configured as shown in the exhibit(Click the Exhibit tab.)

Network interface: vm1175 Effective security rules Topology ⓘ
Virtual network/subnet: RGS-vnet/default Public IP: 40.127.109.108 Private IP: 172.16.1.4 Accelerated networking: Disabled

APPLICATION SECURITY GROUPS ⓘ

Configure the application security groups

INBOUND PORT RULES ⓘ

Network security group VM1-nsg (attached to network interface: vm1175)
Impacts 0 subnets, 1 network interfaces

Add inbound port rule

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
300	RDP	3389	TCP	Any	Any	Allow	...
400	Rule1	80	TCP	Any	Any	Deny	...
500	Rule2	80,443	TCP	Any	Any	Deny	...
1000	Rule4	50-100,400-500	UDP	Any	Any	Allow	...
2000	Rule5	50-5000	Any	Any	VirtualNetwork	Deny	...
3000	Rule6	150-300	Any	Any	Any	Allow	...
4000	Rule3	60-500	Any	Any	VirtualNetwork	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBala...	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

You deploy a web server on VM1. and then create a secure website that is accessible by using the HTTPS protocol. VM1 is used as a web server only.

You need to ensure that users can connect to the website from the internet.



What should you do?

- A. For Rule4. change the protocol from UDP to Any
- B. Modify the protocol of Rule4.
- C. Modify the action of Rule1.
- D. Change the priority of Rule3 to 450

Correct Answer: D

Rule 2 is blocking HTTPS access (port 443) and has a priority of 500. Changing Rule 3 (ports 60-500) and giving it a lower priority number will allow access on port 443. Note: Rules are processed in priority order, with lower numbers

processed before higher numbers, because lower numbers have higher priority. Once traffic matches a rule, processing stops.

Incorrect Answers:

A: HTTPS uses port 443. Rule6 only applies to ports 150 to 300. C, D: Rule 1 blocks access to port 80, which is used for HTTP, not HTTPS.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

QUESTION 11

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You have a CSV file that contains the names and email addresses of 500 external users.

You need to create a guest user account in contoso.com for each of the 500 external users.

Solution: You create a PowerShell script that runs the New-AzureADUser cmdlet for each user.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

The New-AzureADUser cmdlet creates a user in Azure Active Directory (Azure AD).

Instead use the New-AzureADMSInvitation cmdlet which is used to invite a new external user to your directory.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation>



QUESTION 12

HOTSPOT

You have a sync group that has the endpoints shown in the following table.

Name	Type
Endpoint1	Cloud endpoint
Endpoint2	Server endpoint
Endpoint3	Server endpoint

Cloud tiering is enabled for Endpoint3.

You add a file named File1 to Endpoint1 and a file named File2 to Endpoint2.

You need to identify on which endpoints File1 and File2 will be available within 24 hours of adding the files.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

File1:

	▼
Endpoint1only	
Endpoint3 only	
Endpoint2 and Endpoint3 only	
Endpoint1, Endpoint2, and Endpoint3	

File2:

	▼
Endpoint1only	
Endpoint3 only	
Endpoint2 and Endpoint3 only	
Endpoint1, Endpoint2, and Endpoint3	

Correct Answer:



File1:

Endpoint1only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

File2:

Endpoint1only
Endpoint3 only
Endpoint2 and Endpoint3 only
Endpoint1, Endpoint2, and Endpoint3

File1: Endpoint3 only Cloud Tiering: A switch to enable or disable cloud tiering. When enabled, cloud tiering will tier files to your Azure file shares. This converts on-premises file shares into a cache, rather than a complete copy of the dataset, to help you manage space efficiency on your server. With cloud tiering, infrequently used or accessed files can be tiered to Azure Files. File2: Endpoint1, Endpoint2, and Endpoint3 References: <https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-cloud-tiering>

QUESTION 13

You need to create an Azure virtual machine named VM1 that requires a static private IP address configured inside the IP address space for the VNet in which the VM resides. How do you configure a static IP address for this Azure VM?

- A. After the VM has been created, create a new network interface and configure a static IP address for that network interface
- B. When creating a VM in the portal, select New next to private ip address and choose static after assigning the correct IP address
- C. When creating the VM in the portal, change the setting from dynamic to static on the networking tab under private IP address
- D. After the VM has been created, go to the network interface attached to the VM and change the IP configuration to static assignment

Correct Answer: D

Changing the IP configuration on the network interface will achieve the requirement.

QUESTION 14

This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others



might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Location	Resource group
RG1	Resource group	East US	<i>Not applicable</i>
RG2	Resource group	West Europe	<i>Not applicable</i>
RG3	Resource group	North Europe	<i>Not applicable</i>
VNET1	Virtual network	Central US	RG1
VM1	Virtual machine	West US	RG2

VM1 connects to a virtual network named VNET2 by using a network interface named NIC1. You need to create a new network interface named NIC2 for VM1.

Solution: You create NIC2 in RG1 and Central US. Does this meet the goal?

A. Yes

B. No

Correct Answer: B

The virtual machine you attach a network interface to and the virtual network you connect it to must exist in the same location, here West US, also referred to as a region.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

QUESTION 15

You create an Azure Storage account.

You plan to add 10 blob containers to the storage account.

For one of the containers, you need to use a different key to encrypt data at rest.

What should you do before you create the container?

A. Generate a shared access signature (SAS).

B. Modify the minimum TLS version.

C. Rotate the access keys.

D. Create an encryption scope.



Correct Answer: D

Encryption scopes enable you to manage encryption with a key that is scoped to a container or an individual blob. You can use encryption scopes to create secure boundaries between data that resides in the same storage account but

belongs to different customers.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/encryption-scope-overview>

[AZ-104 VCE Dumps](#)

[AZ-104 Practice Test](#)

[AZ-104 Braindumps](#)