AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

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

https://www.pass4itsure.com/az-500.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

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.

You are in the process of creating an Azure Kubernetes Service (AKS) cluster. The Azure Kubernetes Service (AKS) cluster must be able to connect to an Azure Container Registry.

You want to make sure that Azure Kubernetes Service (AKS) cluster authenticates to the Azure Container Registry by making use of the auto-generated service principal.

Solution: You create a secret in Azure Key Vault.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

QUESTION 2

DRAG DROP

Your company has an Azure SQL database that has Always Encrypted enabled.

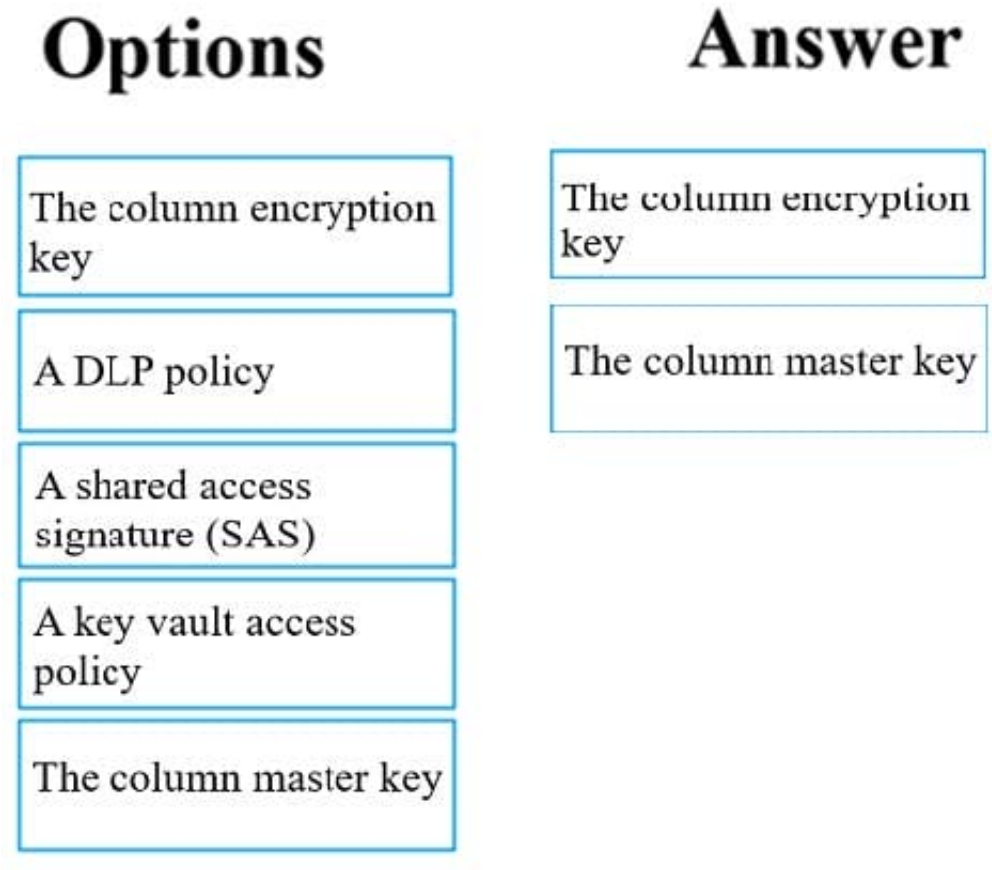
You are required to make the relevant information available to application developers to allow them to access data in the database.

Which two of the following options should be made available? Answer by dragging the correct options from the list to the answer area.

Select and Place:

Options	Answer
The column encryption key	
A DLP policy	
A shared access signature (SAS)	
A key vault access policy	
The column master key	

Correct Answer:



Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

Reference: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine

QUESTION 3

HOTSPOT

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	Table

User1 is assigned the following roles for storage1:

1.

Storage Blob Data Reader

2.

Storage Table Data Contributor

3.

Storage File Data SMB Share Reader

Hot Area:

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	○
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	○	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	○

Correct Answer:

Statements	Yes	No
On October 1, 2022, if User1 accesses folder1 by using SAS1, he can delete the files in folder1.	○	●
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	●	○
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	○	●

QUESTION 4

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

A. the Security and Compliance admin center

B. SQL query editor in Azure

C. File Explorer in Windows

D. AzCopy

Correct Answer: D

https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json

QUESTION 5

You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.

Name	Type	Azure AD roles can be assigned to the group
User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1. Which identities can you add to Group4 as members?

A. User1 only

B. User1 and Group3 only

C. User1, Group1, and Group3 only

D. User1, Group2, and Group3 only

E. User1, Group1, Group2, and Group3

Correct Answer: B

Limitation of using managed identities for authorization Using Azure AD groups for granting access to services is a great way to simplify the authorization process. The idea is simple – grant permissions to a group and add identities to the group so that they inherit the same permissions. This is a well-established pattern from various on-premises systems and works well when the identities represent users.

Reference: https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations

QUESTION 6

SIMULATION

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account.

To complete this task, sign in to the Azure portal.

This task might take several minutes to complete You can perform other tasks while the task completes.

A. See the explanation below.

Correct Answer: A

Step 1: Create a workspace

Azure Monitor can collect data directly from your Azure virtual machines into a Log Analytics workspace for detailed analysis and correlation.

1.

In the Azure portal, select All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.

2.

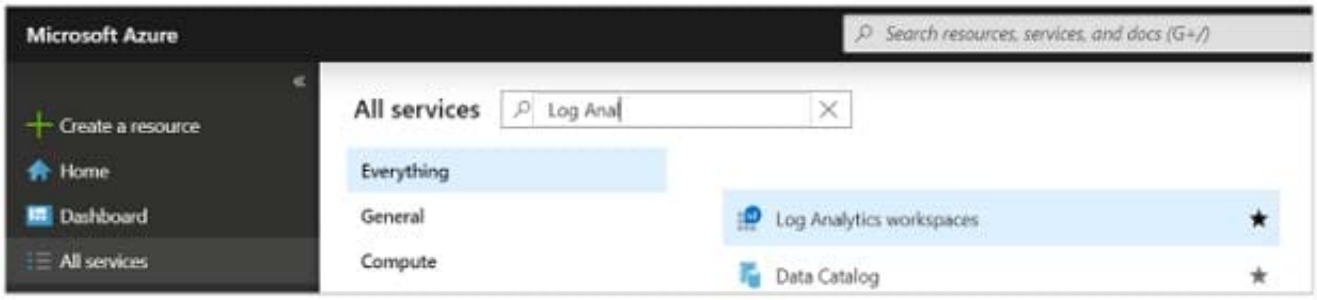
Select Create, and then select choices for the following items:

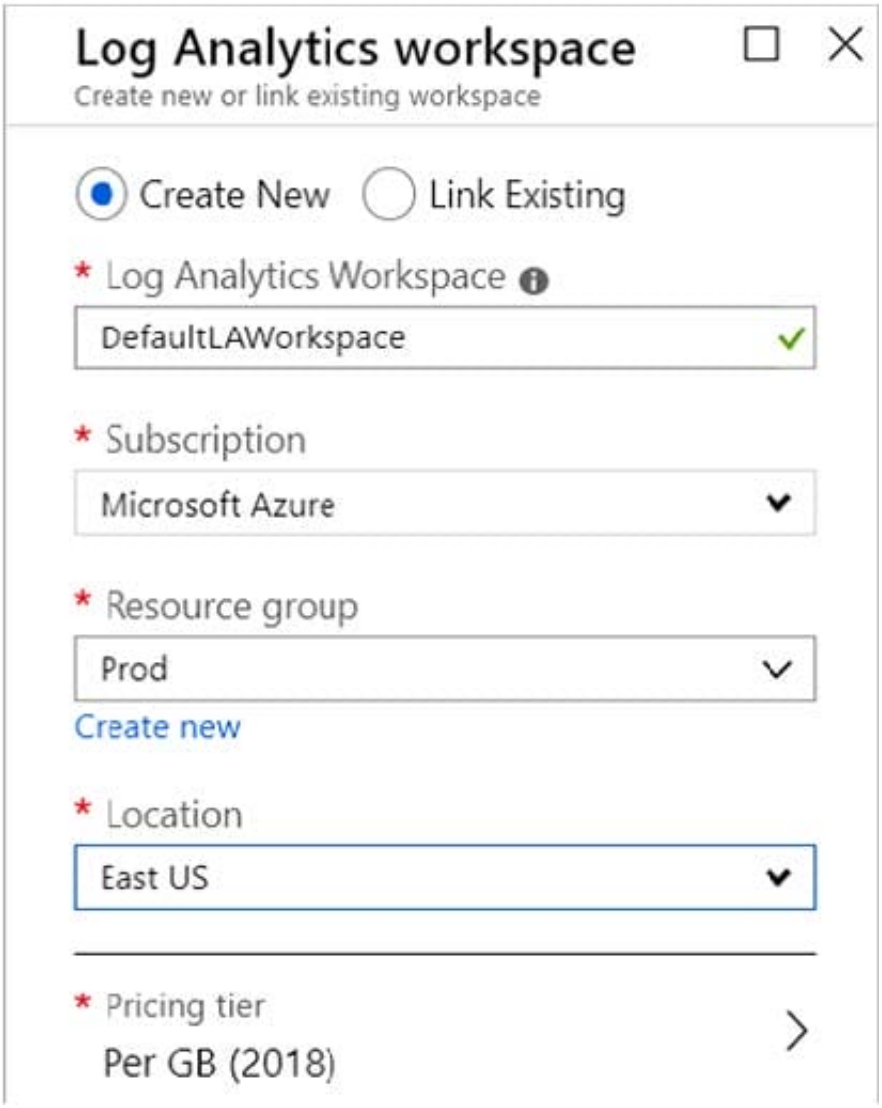
3.

After providing the required information on the Log Analytics workspace pane, select OK.

While the information is verified and the workspace is created, you can track its progress under Notifications from the menu.

Step 2: Enable the Log Analytics VM Extension





Installing the Log Analytics VM extension for Windows and Linux allows Azure Monitor to collect data from your Azure VMs.

1.

In the Azure portal, select All services found in the upper left-hand corner. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics workspaces.

2.

In your list of Log Analytics workspaces, select DefaultWorkspace (the name you created in step 1).

3.

On the left-hand menu, under Workspace Data Sources, select Virtual machines.

4.

In the list of Virtual machines, select a virtual machine you want to install the agent on. Notice that the Log Analytics connection status for the VM indicates that it is Not connected.

5.

In the details for your virtual machine, select Connect. The agent is automatically installed and configured for your Log Analytics workspace. This process takes a few minutes, during which time the Status shows Connecting.

After you install and connect the agent, the Log Analytics connection status will be updated with This workspace.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-azurevm

QUESTION 7

DRAG DROP

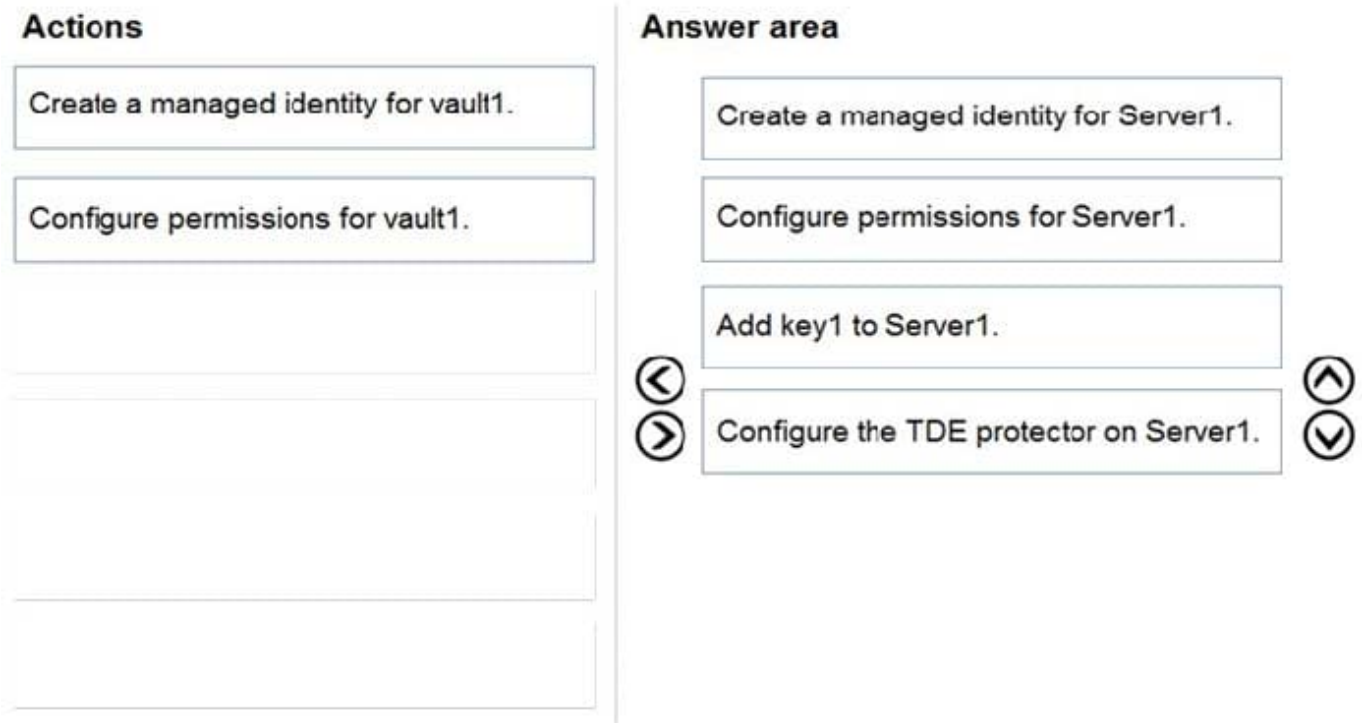
You have an Azure subscription that contains a Microsoft SQL server named Server1 and an Azure key vault named vault1. Server1 hosts a database named DB1. Vault1 contains an encryption key named key1.

You need to ensure that you can enable Transparent Data Encryption (TDE) on DB1 by using key1.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

Correct Answer:



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 Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

1.

Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issused before

2.

Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates the SASs liked to the Stored Access Policy.

QUESTION 9

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

References: https://docs.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 10

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 Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to sa1.

Solution: You regenerate the Azure storage account access keys.

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Generating new storage account keys will invalidate all SAS\\'s that were based on the previous keys.

QUESTION 11

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

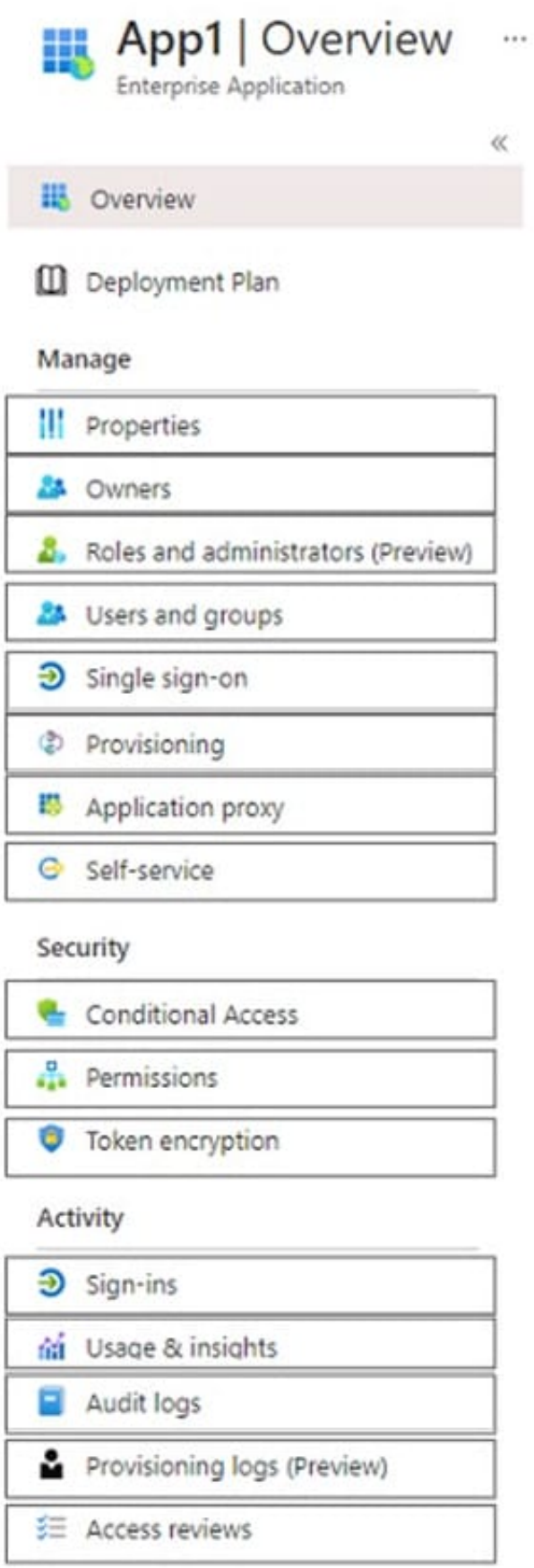
You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:


App1 | Overview
Enterprise Application
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Preview)
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-ins
Usage & insights
Audit logs
Provisioning logs (Preview)
Access reviews

Correct Answer:

Box 1: Roles and administrators

Here you will find Role1 and be able to assign User1 to the role.

Box 2: Self Service

Under Self Service, there is an option to “Allow users to request access to this application”.

QUESTION 12

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

A. Security administrator

B. Global administrator

C. User administrator

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions

QUESTION 13

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\\'s Azure subscription includes a virtual network that has a single subnet configured.

You have created a service endpoint for the subnet, which includes an Azure virtual machine that has Ubuntu Server 18.04 installed.

You are preparing to deploy Docker containers to the virtual machine. You need to make sure that the containers can access Azure Storage resources and Azure SQL databases via the service endpoint.

You need to perform a task on the virtual machine prior to deploying containers.

Solution: You create an AKS Ingress controller.

Does the solution meet the goal?

A. Yes

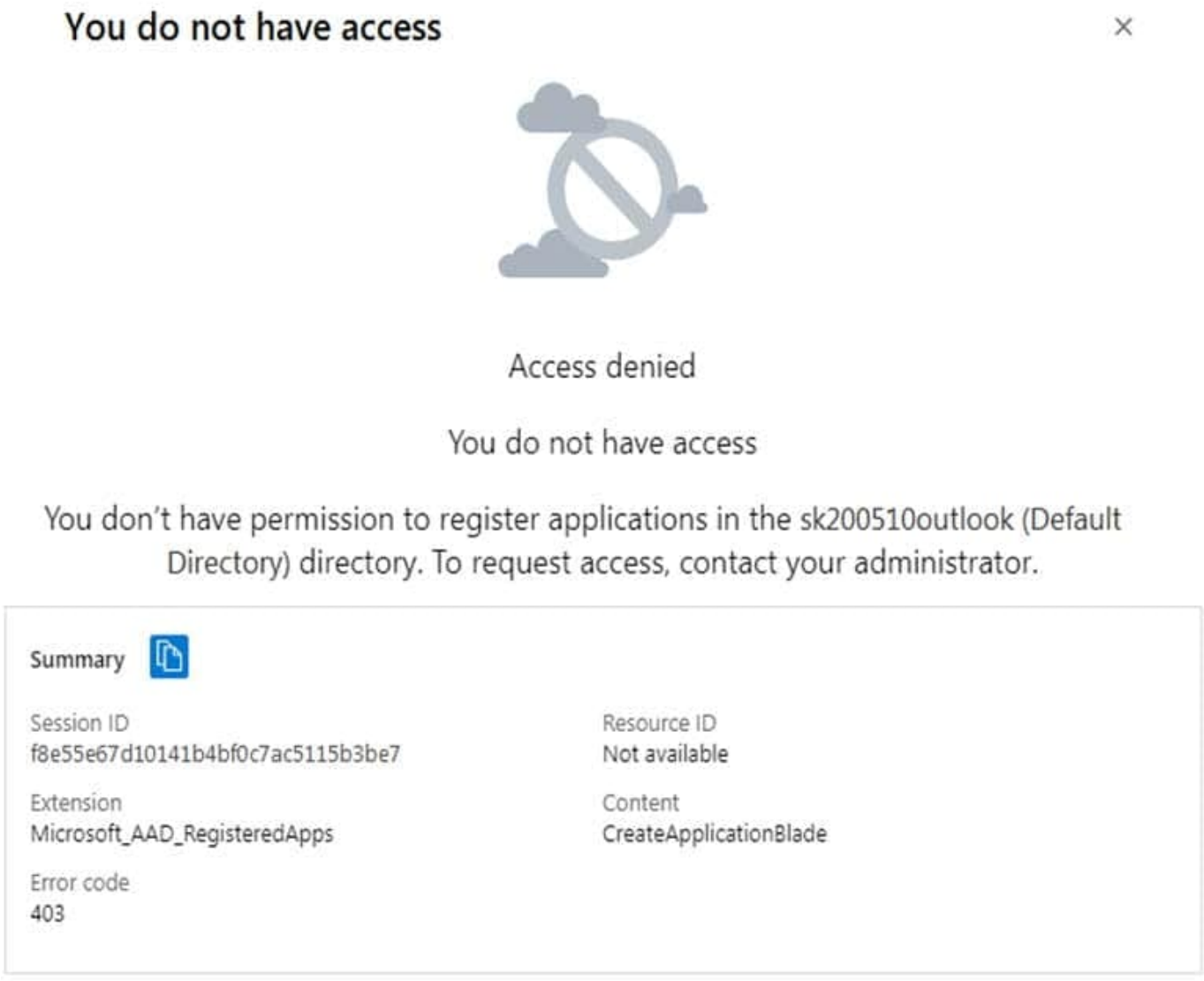
B. No

Correct Answer: B

QUESTION 14

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.



You need to ensure that the developer can register App1 in the tenant. What should you do for the tenant?

A. Modify the User settings

B. Set Enable Security default to Yes.

C. Modify the Directory properties.

D. Configure the Consent and permissions settings for enterprise applications.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

QUESTION 15

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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously. However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.

References: https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/