

[Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

Traffic destined for an Azure Storage account is [answer choice].

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

	▼
allowed	
dropped	
forwarded	

Correct Answer:

Traffic destined for an Azure Storage account is [answer choice].

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

	▼
allowed	
dropped	
forwarded	

QUESTION 72

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 access keys.

Does this meet the goal?

- A. Yes
- B. No

[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)

<https://www.ensurepass.com/AZ-500.html>

[Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

Correct Answer: B

Explanation:

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

QUESTION 73

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: A

Explanation:

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

QUESTION 74

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)

<https://www.ensurepass.com/AZ-500.html>

[Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Medium and above
- Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

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

NOTE: Each correct selection is worth one point.

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

Correct Answer:

When User1 signs in from an anonymous IP address, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User2 signs in from an unfamiliar location, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

When User3 signs in from an infected device, the user will:

	▼
Be blocked	
Be prompted for MFA	
Sign in by using a username and password only	

[Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

QUESTION 75

HOTSPOT

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips [\(learn more\)](#)

☒ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16
194.25.2.0/24

verification options [\(learn more\)](#)

Methods available to users:

☒ Call to phone

☒ Text message to phone

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

NOTE: Each correct selection is worth one point.

[AZ-500 Exam Dumps](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#) [AZ-500 Q&As](#)
<https://www.ensurepass.com/AZ-500.html>

[Download Full Version AZ-500 Exam Dumps\(Updated in Feb/2023\)](#)

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

Correct Answer:

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 76

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Azure Username: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168