

Question #40

Topic 2

Note: This question is part of 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.

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

Question #41

Topic 2

HOTSPOT -

You are building an application that will run in a virtual machine (VM). The application will use Managed Service Identity (MSI).

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authorization methods should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Functionality	Authorization method
Azure Key Vault	Hash-based message authentication code (HMAC)
	Managed Service Identity (MSI)
	Role-Based Access Controls (RBAC)
	HTTPS encryption
Azure SQL	Hash-based message authentication code (HMAC)
	Managed Service Identity (MSI)
	Role-Based Access Controls (RBAC)
	HTTPS encryption
Cosmos DB	Hash-based message authentication code (HMAC)
	Managed Service Identity (MSI)
	Role-Based Access Controls (RBAC)
	HTTPS encryption

Correct Answer:

Answer Area

Functionality	Authorization method
Azure Key Vault	<div>Hash-based message authentication code (HMAC)</div> <div>Managed Service Identity (MSI)</div> <div>Role-Based Access Controls (RBAC)</div> <div>HTTPS encryption</div>
Azure SQL	<div>Hash-based message authentication code (HMAC)</div> <div>Managed Service Identity (MSI)</div> <div>Role-Based Access Controls (RBAC)</div> <div>HTTPS encryption</div>
Cosmos DB	<div>Hash-based message authentication code (HMAC)</div> <div>Managed Service Identity (MSI)</div> <div>Role-Based Access Controls (RBAC)</div> <div>HTTPS encryption</div>

Question #42

Topic 2

You are designing a security solution for a company's Azure Active Directory (Azure AD). The company currently uses Azure AD Premium for all employees.

Contractors will periodically access the corporate network based on demand.

You must ensure that all employees and contractors are required to log on by using two-factor authentication. The solution must minimize costs.

You need to recommend a solution.

What should you recommend?

- A. Purchase Azure Multi-Factor Authentication licenses for the employees and the contractors
- B. Use the Multi-Factor Authentication provider in Azure and configure the usage model for each authentication type
- C. Use the Multi-Factor Authentication provider in Azure and configure the usage model for each enabled user
- D. Purchase Azure Multi-Factor Authentication licenses for the contractors only

Correct Answer: C

Question #43

Topic 2

Note: This question is part of 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 Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

- A. Yes
- B. No

Correct Answer: B

Question #44

Topic 2

Note: This question is part of 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 Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do NOT work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: You implement an access package.

Does this solution meet the goal?

A. Yes

B. No

Correct Answer: *B*

← Previous Questions

Next Questions →

