



Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1

You need to recommend a solution for the user administrators that meets the security requirements for auditing. Which blade should you recommend using from the Azure Active Directory admin center?

- A. Sign-ins
- B. Azure AD Identity Protection
- C. Authentication methods
- D. Access review

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins>

NEW QUESTION 2

HOTSPOT

You plan to configure an access review to meet the security requirements for the workload administrators. You create an access review policy and specify the scope and a group.

Which other settings should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Set the frequency to:

One time	v
Weekly	
Monthly	

To ensure that access is removed if an administrator fails to respond, configure the:

Upon completion settings	v
Advanced settings	
Programs	
Reviewers	

NEW QUESTION 3

Which IP address space should you include in the MFA configuration?

- A. 131.107.83.0/28
- B. 192.168.16.0/20
- C. 172.16.0.0/24
- D. 192.168.0.0/20

Answer: B

NEW QUESTION 4

What should User6 use to meet the technical requirements?

- A. Supervision in the Security & Compliance admin center
- B. Service requests in the Microsoft 365 admin center
- C. Security & privacy in the Microsoft 365 admin center
- D. Data subject requests in the Security & Compliance admin center

Answer: B

NEW QUESTION 5

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 a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.

Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps>

NEW QUESTION 6

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 a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:

- Source Anchor: objectGUID
- Password Hash Synchronization: Disabled
- Password writeback: Disabled
- Directory extension attribute sync: Disabled
- Azure AD app and attribute filtering: Disabled
- Exchange hybrid deployment: Disabled
- User writeback: Disabled

You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection.

Solution: You modify the Source Anchor settings.

Does that meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 7

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune.

You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network.

What should you do first?

- A. From the Azure Active Directory admin center, create a new certificate
- B. Enable Application Proxy in Azure AD
- C. From Active Directory Administrative Center, create a Dynamic Access Control policy
- D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10>

NEW QUESTION 8

You have a Microsoft 365 subscription.

From the Microsoft 365 admin center, you create a new user. You plan to assign the Reports reader role to the user.

You need to see the permissions of the Reports reader role. Which admin center should you use?

- A. Azure Active Directory
- B. Cloud App Security
- C. Security & Compliance
- D. Microsoft 365

Answer: A

NEW QUESTION 9

You have a Microsoft 365 subscription.
 You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default.
 What should you use to achieve the goal?

- A. Security & Compliance permissions
- B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- C. Microsoft Azure AD group management
- D. Microsoft Office 365 user management

Answer: B

NEW QUESTION 10

You have a Microsoft 365 E5 subscription.
 You implement Advanced Threat Protection (ATP) safe attachments policies for all users.
 User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.
 What should you do from ATP?

- A. Set the action to Block
- B. Add an exception
- C. Add a condition
- D. Set the action to Dynamic Delivery

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing>

NEW QUESTION 10

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.
 You are deploying Azure Advanced Threat Protection (ATP)
 You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.
 You need to integrate the VPN and Azure ATP.
 What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On VPN1:

Configure an authentication provider.	v
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	v
1723	
1813	
8080	
8531	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

NEW QUESTION 15

HOTSPOT

You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

- Protected apps: App1
- Exempt apps: App2
- Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.

☐
☐

From Device2, User1 can copy data from App1 to App2.

☐
☐

From Device2, User1 can copy data from App1 to App3.

☐
☐

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Yes No

From Device1, User1 can copy data from App1 to App3.

☐
☒

From Device2, User1 can copy data from App1 to App2.

☒
☐

From Device2, User1 can copy data from App1 to App3.

☒
☐

NEW QUESTION 17

HOTSPOT

Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements

Yes

No

User1 can run an antivirus scan on Device1.

☐
☐

User2 can collect an investigation package from Device2.

☐
☐

User3 can isolate Device1.

☐
☐

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 22

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy to quarantine malware. You need to configure the retention duration for the attachments in quarantine.

Which type of threat management policy should you create from the Security&Compliance admin center?

- A. ATP anti-phishing
 B. DKIM
 C. Anti-spam
 D. Anti-malware

Answer: D

NEW QUESTION 25

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 a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You create a new label in the global policy and instruct the user to resend the email message.

Does this meet the goal?

- A. Yes
 B. No

Answer: A

NEW QUESTION 30

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 a Microsoft 365 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.

You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.

You need to ensure that the external recipients can open protected email messages sent to them. Solution: You modify the content expiration settings of the label.

Does this meet the goal?

- A. Yes
 B. No

Answer: B

NEW QUESTION 35

HOTSPOT

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.
To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12,Group13,and Group14 only	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/information-protection/prepare>

NEW QUESTION 40

DRAG DROP

You have a Microsoft 365 subscription.
A customer requests that you provide her with all documents that reference her by name. You need to provide the customer with a copy of the content.
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.

Actions

Close the case.

Regenerate a report.

View the results.

Export the results.

Create a Data Subject Request (DSR) case.

Save the search.

Download the results.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365>

NEW QUESTION 45

You have a Microsoft 365 subscription.
The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1. What should you do first?

- A. From the Azure Active Directory admin center, assign a role group to Admin1.
- B. From the Microsoft 365 admin center, assign a role to Admin1.
- C. From Security & Compliance admin center, assign a role group to Admin1.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION 48

HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing in the following exhibit.

Decide if you want to retain content, delete it, ot both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 1 years ▾

☐ No, just delete content that's older than ⓘ

1 years ▾

Delete the content based on when it was created ▾ ⓘ

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

Policy2 is configured as shown in the following exhibit.

Decide if you want to retain contet, delete it, ot both

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... ▾ 3 years ▾

Retain the content based on when it was created ▾ ⓘ

Do you want us to delete it after this time?

☐ Yes ☒ No

☐ No, just delete content that's older than ⓘ

1 years ▾

Need more options?

☐ Use advanced retention settings ⓘ

Back

Next

Cancel

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

Answer Area	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1,2018, an administrator can recover the file on April 15, 2019	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence

NEW QUESTION 50

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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

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

- Assignments: Include Group1, Exclude Group2
- Conditions: Sign in risk of Low and above
- Access: Allow access, Require password change

You need to identify how the policy affects User1 and User2.

What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Must change their password:	<div><div></div><div>User1 only</div><div>User2 only</div><div>Both User1 and User2</div><div>Neither User1 not User2</div></div>
Prompted for MFA:	<div><div></div><div>User1 only</div><div>User2 only</div><div>Both User1 and User2</div><div>Neither User1 not User2</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Must change their password:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	

Prompted for MFA:

	▼
User1 only	
User2 only	
Both User1 and User2	
Neither User1 not User2	


NEW QUESTION 53

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
Block the following URLs:

 -

Enter a valid URL +

.phishing..*
malware.*com
*.contoso.com

Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 356 ProPlus, Office for iOS and Android
- ☒ Office Online of above applications

For the locations selected above:

- ☒ Do not track when users click safe links:
- ☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- A. fabrikam.phishing.fabrikam.com
- B. malware.fabrikam.com
- C. fabrikam.contoso.com
- D. www.malware.fabrikam.com

Answer: D

Explanation:

References:

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list- wtih-atp

NEW QUESTION 55

HOTSPOT

You have a Microsoft 365 subscription that uses a default name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.

Links

Choose the kind of link that's selected by default when users share items.

Default link type

☒

Shareable: Anyone with the link

☐

Internal: Only people in your organization☐

External sharing

Users can share with:

SharePoint

OneDrive

Most permissive

Least permissive

Anyone

New and existing external users

Existing external users

Only people in your organization

Users can create shareable links that don't require sign-in

External users must sign-in

Only users already in your organization's directory

No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Advanced settings for external sharing

☒

Allow or block sharing with people on specific domains

Allow only these domains

Contoso.com, Adatum.com

Add domains

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

A user who has an email address of user1@fabrikam.com [answer choice]

cannot access OneDrive content

can access OneDrive content after a link is created

must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

the user cannot access OneDrive content

the user can access OneDrive content after a link is created

must be added to a group before the user can access shared files

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/onedrive/manage-sharing>

NEW QUESTION 57

You have a Microsoft 365 subscription that includes a user named User1.
You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.
You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.
Which type of Cloud App Security policy should you create?

- A. an app permission policy
B. an activity policy
C. a Cloud Discovery anomaly detection policy
D. a session policy

Answer: D

NEW QUESTION 61

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 questions 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 a Microsoft 365 subscription. You have a user named User1. Several users have full access to the mailbox of User1. Some email messages sent to User1 appear to have been read and deleted before the user viewed them. When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank. You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-AuditConfig -Workload Exchange command. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

NEW QUESTION 64

You have a Microsoft 365 subscription. You have a Microsoft SharePoint Online site named Site1. The files in Site1 are protected by using Microsoft Azure Information Protection. From the Security & Compliance admin center, you create a label that designates personal data. You need to auto-apply the new label to all the content in Site1. What should you do first?

- A. From PowerShell, run Set-ManagedContentSettings.
- B. From PowerShell, run Set-ComplianceTag.
- C. From the Security & Compliance admin center, create a Data Subject Request (DSR).
- D. Remove Azure Information Protection from the Site1 files.

Answer: D

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/apply-labels-to-personal-data-in-office-365>

NEW QUESTION 69

You have a Microsoft 365 subscription. You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

- A. From Search & investigation, create a guided search.
- B. From Events, create an event.
- C. From Alerts, create an alert policy.
- D. From Search & Investigation, create an eDiscovery case.

Answer: C

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

NEW QUESTION 72

DRAG DROP

You have a Microsoft 365 E5 subscription. All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP). You create a Windows Defender machine group named MachineGroup1. You need to enable delegation for the security settings of the computers in MachineGroup1. Which three 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.

Actions

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-HsolRoleMember cmdlet.

Answer Area

>

<

^

v

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
From Windows Defender Security Center, create a role.	From Windows Defender Security Center, configure the permissions for MachineGroup1.
From Windows Defender Security Center, configure the permissions for MachineGroup1.	
From the Azure portal, create an RBAC role.	From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.	
From Azure Cloud Shell, run the Add-HsolRoleMember cmdlet.	From the Azure portal, create an RBAC role.

NEW QUESTION 74

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 questions 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 on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the Directory Service event log on Server1. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

NEW QUESTION 75

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 questions 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 on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events.

You use the System event log on Server1. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:
<https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance>

NEW QUESTION 77

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

MS-500 Practice Exam Features:

- * MS-500 Questions and Answers Updated Frequently
- * MS-500 Practice Questions Verified by Expert Senior Certified Staff
- * MS-500 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MS-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MS-500 Practice Test Here](#)