

Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator



NEW QUESTION 1

An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.

Exchange Administrator - Members

+ Add member X Remove member v Access reviews ↓ Export ↻ Refresh

Assignment type

Search

Member	Email	ASSIGNMENT TYPE	EXPIRATION
Admin1	Admin1@M365x901434.onmicrosoft.com	Permanent	-
Admin2	Admin2@M365x901434.onmicrosoft.com	Eligible	-

What should you do to meet the security requirements?

- A. Change the Assignment Type for Admin2 to Permanent
- B. From the Azure Active Directory admin center, assign the Exchange administrator role to Admin2
- C. From the Azure Active Directory admin center, remove the Exchange administrator role to Admin1
- D. Change the Assignment Type for Admin1 to Eligible

Answer: D

NEW QUESTION 2

HOTSPOT

You need to recommend an email malware solution that meets the security requirements.

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

NOTE: Each correct selection is worth one point.

Policy to create:

ATP safe attachments	v
ATP Safe Links	
Anti-spam	
Anti-malware	

Option to configure:

Block	v
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policy to create:

ATP safe attachments	v
ATP Safe Links	
Anti-spam	
Anti-malware	

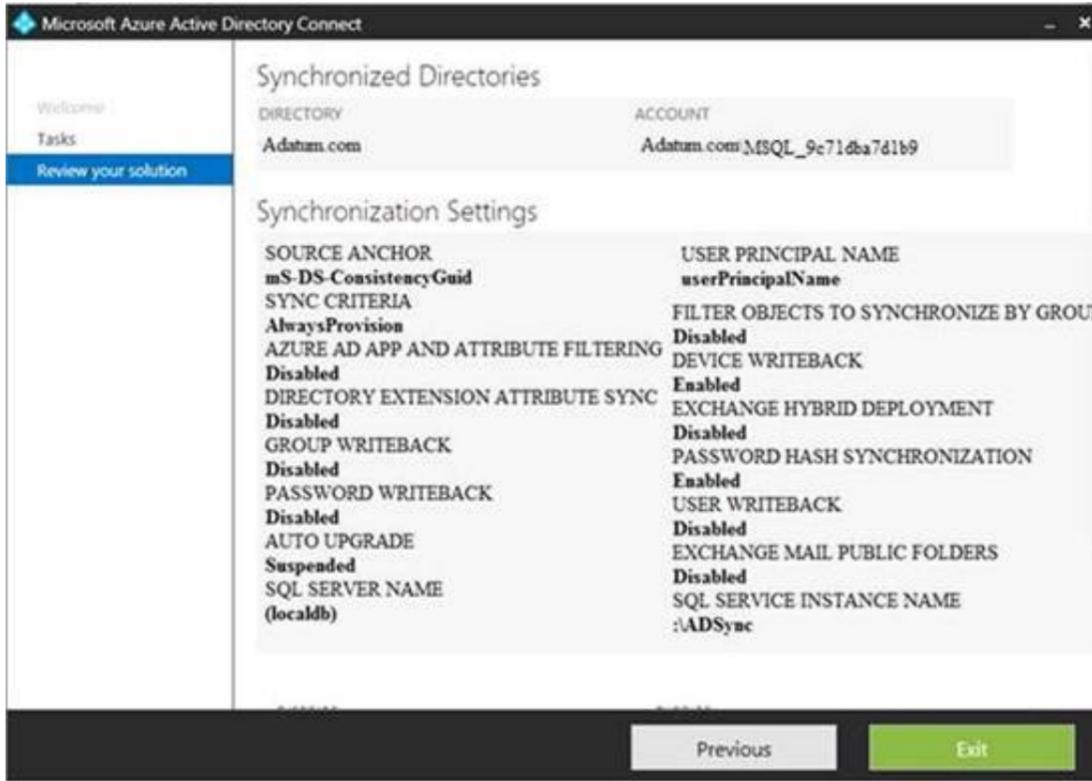
Option to configure:

Block	v
Replace	
Dynamic Delivery	
Monitor	
Quarantine message	

NEW QUESTION 3

HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



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.

If you reset a password in Azure AD, the password will [answer choice].

be overwritten	v
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD, [answer choice].

an object will be provisioned in the Computers container	v
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION 4

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 5

Your company has a Microsoft 365 subscription. The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices. You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant. The users must be prevented from backing up the app's data to iCloud. What should you create?

- A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- B. an app protection policy in Microsoft Intune

- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 6

You have a Microsoft 365 Enterprise E5 subscription.

You use Windows Defender Advanced Threat Protection (Windows Defender ATP). You plan to use Microsoft Office 365 Attack simulator.

What is a prerequisite for running Attack simulator?

- A. Enable multi-factor authentication (MFA)
- B. Configure Advanced Threat Protection (ATP)
- C. Create a Conditional Access App Control policy for accessing Office 365
- D. Integrate Office 365 Threat Intelligence and Windows Defender ATP

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

NEW QUESTION 7

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 8

Your company uses Microsoft Azure Advanced Threat Protection (ATP).

You enable the delayed deployment of updates for an Azure ATP sensor named Sensor1. How long after the Azure ATP cloud service is updated will Sensor1 be updated?

- A. 7 days
- B. 24 hours
- C. 1 hour
- D. 48 hours
- E. 12 hours

Answer: B

Explanation:

Note: The delay period was 24 hours. In ATP release 2.62, the 24 hour delay period has been increased to 72 hours.

NEW QUESTION 9

Your company has 500 computers.

You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.

You need to recommend a remediation solution that meets the following requirements: Windows Defender ATP administrators must manually approve all remediation for the executives

Remediation must occur automatically for all other users

What should you recommend doing from Windows Defender Security Center?

- A. Configure 20 system exclusions on automation allowed/block lists
- B. Configure two alert notification rules
- C. Download an offboarding package for the computers of the 20 executives
- D. Create two machine groups

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groups/windows-defender-advanced-threat-protection>

NEW QUESTION 10

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 10

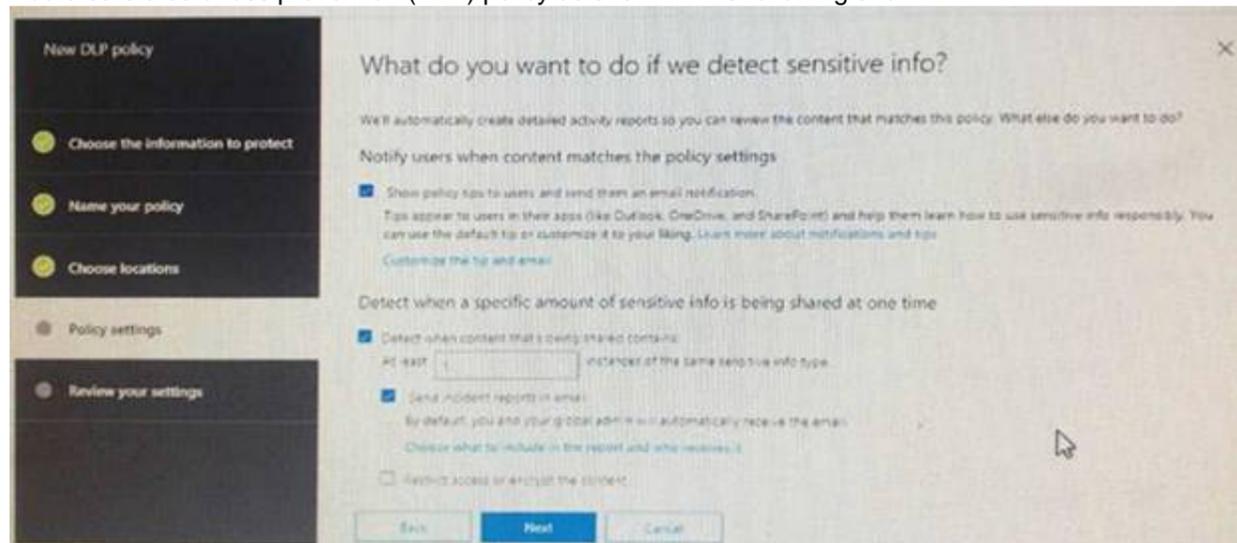
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
 After you answer a 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 encryption settings of the label.
 Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 15

You create a data loss prevention (DLP) policy as shown in the following shown:



What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

- A. The user receives a notification and can send the email message
- B. The user receives a notification and cannot send the email message
- C. The email message is sent without a notification
- D. The email message is blocked silently

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

NEW QUESTION 18

You have a Microsoft 365 subscription.
 You need to create data loss prevention (DLP) queries in Microsoft SharePoint Online to find sensitive data stored in sites.
 Which type of site collection should you create first?

- A. Records Center
- B. Compliance Policy Center
- C. eDiscovery Center
- D. Enterprise Search Center
- E. Document Center

Answer: C

Explanation:

Reference:

<https://support.office.com/en-us/article/overview-of-data-loss-prevention-in-sharepoint-server-2016-80f907bbb944-448d-b83d-8fec4abcc24c>

NEW QUESTION 19

You have a Microsoft 365 subscription.
 A user reports that changes were made to several files in Microsoft OneDrive.
 You need to identify which files were modified by which users in the user's OneDrive. What should you do?

- A. From the Azure Active Directory admin center, open the audit log
- B. From the OneDrive admin center, select Device access
- C. From Security & Compliance, perform an eDiscovery search
- D. From Microsoft Cloud App Security, open the activity log

Answer: D

Explanation:

Reference:
<https://docs.microsoft.com/en-us/cloud-app-security/activity-filters>

NEW QUESTION 24

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

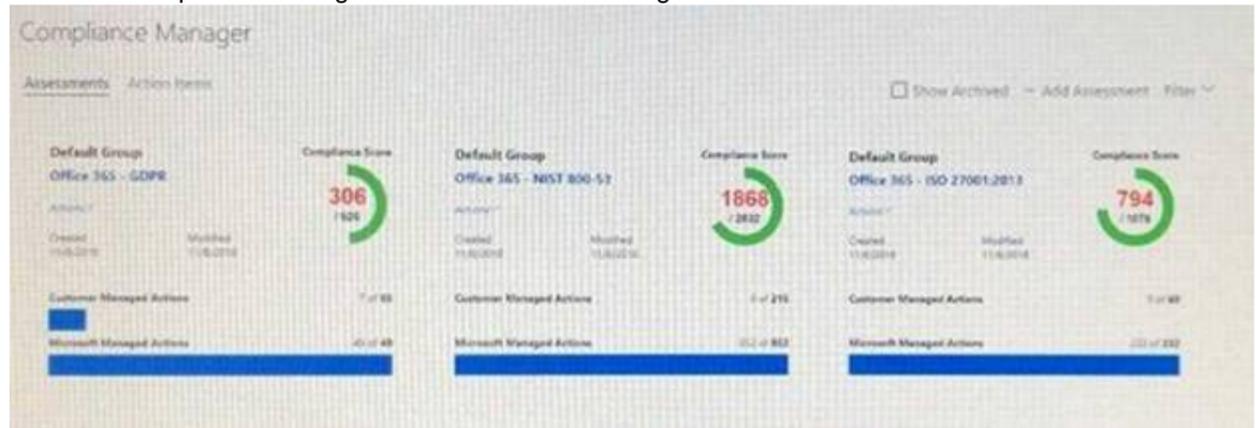
Explanation:

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

NEW QUESTION 29

HOTSPOT

You view Compliance Manager as shown in the following exhibit.



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.

To increase the GDPR Compliance Score for Microsoft Office 365, you must [answer choice].

assign action items	v
review actions	
perform an assessment	
create a service request with Microsoft	

The current GDPR Compliance Score [answer choice].

proves that the organization is non-compliant	v
proves that the organization is compliant	
shows that actions are required to evaluate compliance	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud>

NEW QUESTION 33

Your company has a Microsoft 365 subscription that includes a user named User1.
 You suspect that User1 sent email messages to a competitor detailing company secrets.
 You need to recommend a solution to ensure that you can review any email messages sent by User1 to the competitor, including sent items that were deleted.
 What should you include in the recommendation?

- A. Enable In-Place Archiving for the mailbox of User1
- B. From the Security & Compliance, perform a content search of the mailbox of User1
- C. Place a Litigation Hold on the mailbox of User1
- D. Configure message delivery restrictions for the mailbox of User1

Answer: C

NEW QUESTION 34

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

Direct: Specific people

External sharing

Users can share with:

SharePoint	OneDrive	Anyone
Most permissive	Least permissive	Users can create shareable links that don't require sign-in
Least permissive	Most permissive	New and existing external users External users must sign-in
		Existing external users Only users already in your organization's directory
		Only people in your organization 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 37

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 41

You have a Microsoft 365 subscription.
 A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.
 You need to limit alert notifications to actionable DLP events.
 What should you do?

- A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
- B. From the Cloud App Security admin center, apply a filter to the alerts.
- C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
- D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Answer: D

Explanation:

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

NEW QUESTION 43

You have a Microsoft 365 subscription.
 You create and run a content search from the Security & Compliance admin center. You need to download the results of the content search.
 What should you obtain first?

- A. an export key
- B. a password
- C. a certificate
- D. a pin

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results>

NEW QUESTION 46

HOTSPOT
 You have a Microsoft 365 subscription that include three users named User1, User2, and User3.
 A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.
 You create an alert policy named Policy1 as shown in the following exhibit.

The screenshot shows the configuration for an alert policy named 'Policy1'. At the top, there are two buttons: 'Edit policy' and 'Delete policy'. Below these are several settings:

- Status:** On (indicated by a blue toggle switch).
- Description:** Policy1 description (with an 'Edit' link).
- Severity:** Low (with a blue dot icon and an 'Edit' link).
- Category:** Threat management.
- Conditions:** Activity is Copied file and File name is Like any of File1.docx.
- Aggregation:** Aggregated (with an 'Edit' link).
- Threshold:** 10 activities.
- Window:** 60 minutes.
- Scope:** All users.
- Email recipients:** prvi@sk180920.onmicrosoft.com.
- Daily notifications limit:** Do not send email notifications (with an 'Edit' link).

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.

If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].

▼
Policy1 will not be triggered
Policy1 will be triggered after 45 minutes
Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].

▼
Policy1 will not be triggered
Policy1 will be triggered within 20 minutes
Policy1 will be triggered within 45 minutes
Policy1 will be triggered after 60 minutes

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 51

You have a Microsoft 365 subscription. All users are assigned a Microsoft 365 E5 license. How long will auditing data be retained?

- A. 30 days
- B. 90 days
- C. 365 days
- D. 5 years

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

NEW QUESTION 54

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	Answer Area
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.	⬅

- 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 Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.
From the Azure portal, create an RBAC role.	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-Hso1RoleMember cmdlet.	

NEW QUESTION 56

You have a hybrid Microsoft Exchange Server organization. All users have Microsoft 365 E5 licenses. You plan to implement an Advanced Threat Protection (ATP) anti-phishing policy. You need to enable mailbox intelligence for all users. What should you do first?

- A. Configure attribute filtering in Microsoft Azure Active Directory Connect (Azure AD Connect).
- B. Purchase the ATP add-on.
- C. Select Directory extension attribute sync in Microsoft Azure Active Directory Connect (Azure AD Connect).
- D. Migrate the on-premises mailboxes to Exchange Online.

Answer: B

NEW QUESTION 57

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-MailboxFolderPermission -Identity "User1"

-User User1@contoso.com -AccessRights Owner command. Does that meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

NEW QUESTION 60

.....

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](#)