



## 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 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**

You need to recommend a solution to protect the sign-ins of Admin1 and Admin2. What should you include in the recommendation?

- A. a device compliance policy
- B. an access review
- C. a user risk policy
- D. a sign-in risk policy

**Answer:** C

**Explanation:**

References:  
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy>

**NEW QUESTION 4**

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

- A. Synchronization Service Manager
- B. Azure AD Connect wizard
- C. Synchronization Rules Editor
- D. IdFix

**Answer: B**

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization>

Case Study: 2 Litware, Inc Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes

Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management Security Requirements

Litware identifies the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA.

Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.

If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized

General Requirements

Litware want to minimize the deployment of additional servers and services in the Active Directory forest.

**NEW QUESTION 5**

You need to create Group2.

What are two possible ways to create the group?

- A. an Office 365 group in the Microsoft 365 admin center
- B. a mail-enabled security group in the Microsoft 365 admin center
- C. a security group in the Microsoft 365 admin center

- D. a distribution list in the Microsoft 365 admin center
- E. a security group in the Azure AD admin center

**Answer:** CE

**NEW QUESTION 6**

DRAG DROP

You need to configure threat detection for Active Directory. The solution must meet the security requirements.

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
Configure the Directory services setting in Azure ATP	
Download and install the ATA Gateway on DC1, DC2, and DC3	
Download and install the Azure ATP sensor package on DC1, DC2, and DC3	
Configure a site-to-site VPN	
Create a workspace in Azure ATP	
Download and install the ATA Center on Server1	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Create a workspace in Azure ATP
Download and install the Azure ATP sensor package on DC1, DC2, and DC3
Configure the Directory services setting in Azure ATP

**NEW QUESTION 7**

HOTSPOT

Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

<b>ADGroup1:</b>	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	
<b>ADGroup2:</b>	None	v
	User1 and User2 only	
	User2 and User4 only	
	User3 and User4 only	
	User1, User2, User3, and User4	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values>

**NEW 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 a Microsoft 365 subscription that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports. The Compliance Manager Reader role is not assigned to any users. You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

Solution: You recommend assigning the Compliance Manager Reader role to User5. Does this meet the goal?

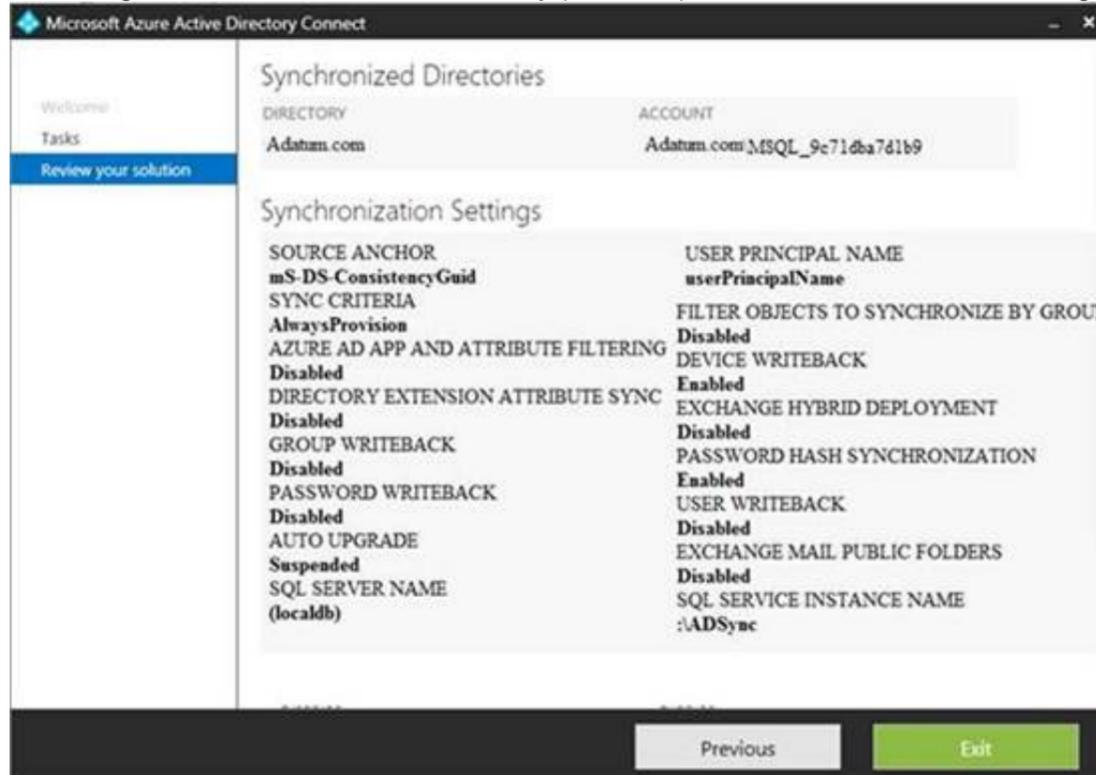
- A. Yes
- B. No

**Answer: B**

**NEW QUESTION 9**

**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 10**

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 10**

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 15**

You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription. You need to allow a user named User1 to view ATP reports in the Threat management dashboard. Which role provides User1 with the required role permissions?

- A. Security reader
- B. Message center reader
- C. Compliance administrator
- D. Information Protection administrator

**Answer: A**

**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded-to-view-the-atp-reports>

**NEW QUESTION 16**

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.

Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.

You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.

The email address that you intend to spoof belongs to the Executive group members. What should you do first?

- A. From Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
- C. Enable MFA for the Research group members
- D. Migrate the Executive group members to Exchange Online

**Answer: C**

**Explanation:**

Reference:

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

**NEW QUESTION 21**

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 25**

**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 30**

**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.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- 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 33**

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 38**

DRAG DROP

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.

Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Locations		Answer Area
ATP quarantine	Messages that contain word-filtered content:	Location
The Junk Email folder of a user's mailbox	Messages that are classified as phishing:	Location
The Chatter folder a user's mailbox		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area	
Messages that contain word-filtered content:	The Junk Email folder of a user's mailbox
Messages that are classified as phishing:	The Junk Email folder of a user's mailbox

**NEW QUESTION 39**

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 42**

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	<input checked="" type="checkbox"/>
Group1 and Group4 only	<input type="checkbox"/>
Group3 and Group4 only	<input type="checkbox"/>
Group1, Group3, and Group4 only	<input type="checkbox"/>
Group1, Group2, Group3, and Group4	<input type="checkbox"/>

Azure AD groups:

Group13 only	<input checked="" type="checkbox"/>
Group13 and Group14 only	<input type="checkbox"/>
Group11 and Group12 only	<input type="checkbox"/>
Group11, Group13, and Group14 only	<input type="checkbox"/>
Group11, Group12, Group13, and Group14 only	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

**NEW QUESTION 46**

HOTSPOT

Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com. The company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.

**Create filters for the policy**

**Act on:**

**Single activity:**  
Every activity that matches the filters

**Repeated activity:**  
Repeated activity by a single user

Minimum repeated activities:

Within timeframe:  minutes

In a single app

Count only unique target files or folders per user

[Edit and preview results](#)

ACTIVITIES MATCHING ALL OF THE FOLLOWING

equals

OR

equals

From group  equals

as

**Alerts**

Create alert Use your organization's default settings  
Daily alert limit 5

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**

<b>Yes</b>	<b>No</b>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Statements**

<b>Yes</b>	<b>No</b>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input checked="" type="radio"/>

In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.

In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.

In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.

**NEW QUESTION 49**

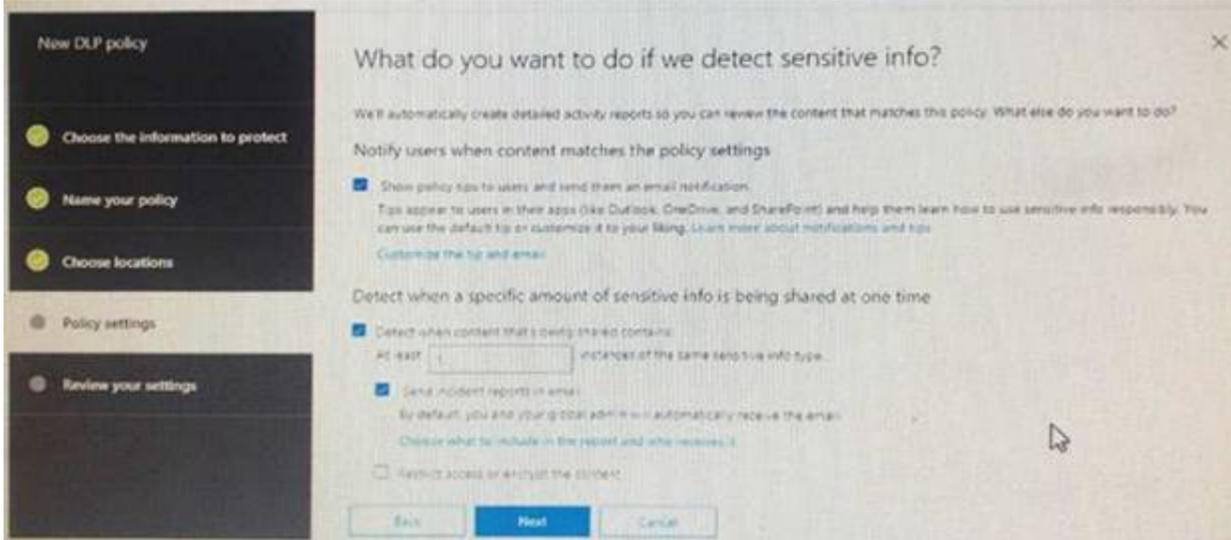
You have a Microsoft 365 subscription.  
 Some users access Microsoft SharePoint Online from unmanaged devices.  
 You need to prevent the users from downloading, printing, and synching files. What should you do?

- A. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
- B. From the SharePoint admin center, configure the Access control settings
- C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
- D. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy

Answer: B

**NEW QUESTION 53**

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 57**

**HOTSPOT**

You have a Microsoft 365 E5 subscription.

From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.

You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	V
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	V
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

- A. Mastered
- B. Not Mastered

Answer: A

**Explanation:**

From the Azure portal, create a conditional access policy and configure:

Users and groups, Cloud apps, and Session settings	V
Users and groups, Cloud apps, and Conditions settings	
Users and groups, Conditions, and Session settings	

From an Exchange Online Remote PowerShell session, run:

New-OwaMailbox Policy and Set-OwaMailboxPolicy	V
New-ClientAccessRule and Test-ClientAccessRule	
Get-CASMailbox and Set-CASMailbox	

**NEW QUESTION 59**

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 60**

**HOTSPOT**

You have a Microsoft 365 subscription.  
 You are creating a retention policy named Retention1 as shown in the following exhibit.

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

**Do you want to retain content?** ⓘ

Yes, I want to retain it ⓘ

For this long... v  years v

Retain the content based on  ⓘ

**Do you want us to delete it after this time?** ⓘ

Yes  No

No, just delete content that's older than ⓘ

years v

**Need more options?**

Use advanced retention settings ⓘ

Back Next Cancel

You apply Retention1 to SharePoint sites and OneDrive accounts.  
 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 a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	v
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	v
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

If a user creates a file in a Microsoft SharePoint library on January 1, 2019, and modifies the file every six months, the file will be [answer choice].

retained	▼
deleted on January 1, 2021	
deleted on July 1, 2021	

If a user creates a file in Microsoft OneDrive on January 1, 2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until January 1, 2020	
can recover the file until March 1, 2020	
can recover the file until May 1, 2020	

**NEW QUESTION 62**

You recently created and published several labels policies in a Microsoft 365 subscription. You need to view which labels were applied by users manually and which labels were applied automatically. What should you do from the Security & Compliance admin center?

- A. From Search & investigation, select Content search
- B. From Data governance, select Events
- C. From Search & investigation, select eDiscovery
- D. From Reports, select Dashboard

Answer: B

**NEW QUESTION 64**

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

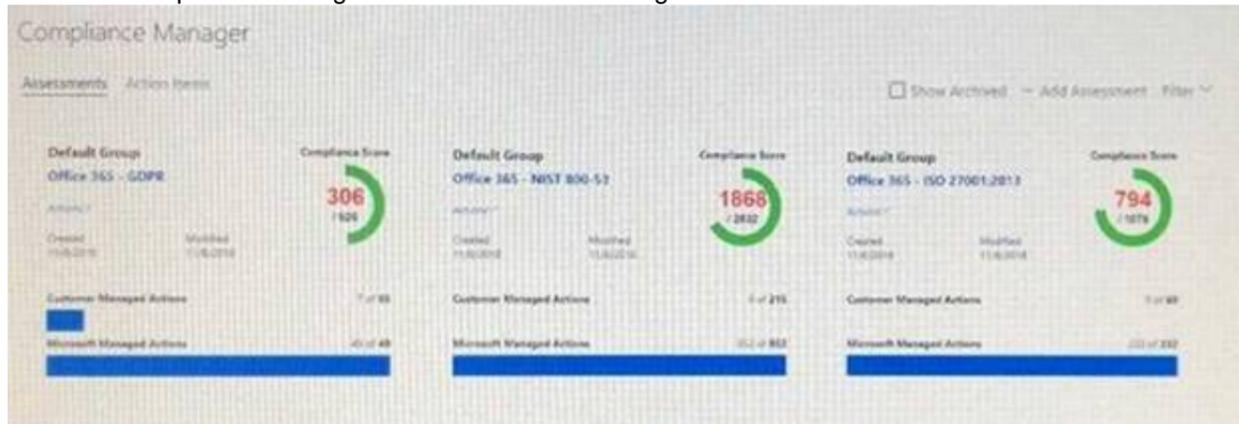
**Explanation:**

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

**NEW QUESTION 65**

**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	▼
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	▼
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 70**

DRAG DROP

You have a Microsoft 365 subscription.

You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.

Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.

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 PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.
Delete Litware.docx from the Recycle Bin of SiteCollection1.

**NEW QUESTION 71**

Your company has a main office and a Microsoft 365 subscription.

You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.

What should you include in the configuration?

- A. a user risk policy
- B. a sign-in risk policy
- C. a named location in Azure Active Directory (Azure AD)
- D. an Azure MFA Server

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

**NEW QUESTION 75**

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:

	▼
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	

- 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 79**

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 of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group1	Disabled

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 of Low and above
  - Access: Allow access, Require password multi-factor authentication
- You need to identify how the policy affects User1 and User2.

What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

User2:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

User1:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

User2:  ▼

Blocked
Can sign in without MFA
Prompted for MFA

**NEW QUESTION 84**

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 86**

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 91**

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-AdminAuditLogConfig -AdminAuditLogEnabled $true-AdminAuditLogCmdlets *Mailbox*` 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/setadmindlogconfig?view=exchange-ps>

**NEW QUESTION 93**

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 96**

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 99**

**HOTSPOT**

You have a Microsoft 365 subscription. Auditing is enabled.

A user named User1 is a member of a dynamic security group named Group1. You discover that User1 is no longer a member of Group1.

You need to search the audit log to identify why User1 was removed from Group1.

Which two actions should you use in the search? To answer, select the appropriate activities in the answer area.

NOTE: Each correct selection is worth one point.

**Search** Clear **Results**

**Activities**

Show results for all activities  Date IP address User Activity Item

**User administration activities**

- Added user
- Deleted user
- Set license properties
- Reset user password
- Changed user password
- Changed user license
- Updated user
- Set property that forces user to change password

**Azure AD group administration activities**

- Added group
- Updated group
- Deleted group
- Added member to group
- Removed member from group

**Application administration activities**

- Added service principal
- Removed a service principal from the directory
- Set delegation entry
- Removed credentials from a service principal
- Added delegation entity
- Added credentials to a service principal

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 102**

**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.

**Policy1**

Status	<input checked="" type="checkbox"/> On	
Description	Policy1 description	<input type="button" value="Edit"/>
Severity	<input checked="" type="radio"/> Low	<input type="button" value="Edit"/>
Category	Threat management	
Conditions	Activity is Copied file and File name is Like any of File1.docx	
Aggregation	Aggregated	<input type="button" value="Edit"/>
Threshold	10 activities	
Window	60 minutes	
Scope	All users	
Email recipients	prvi@sk180920.onmicrosoft.com	
Daily notifications limit	Do not send email notifications	<input type="button" value="Edit"/>

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:

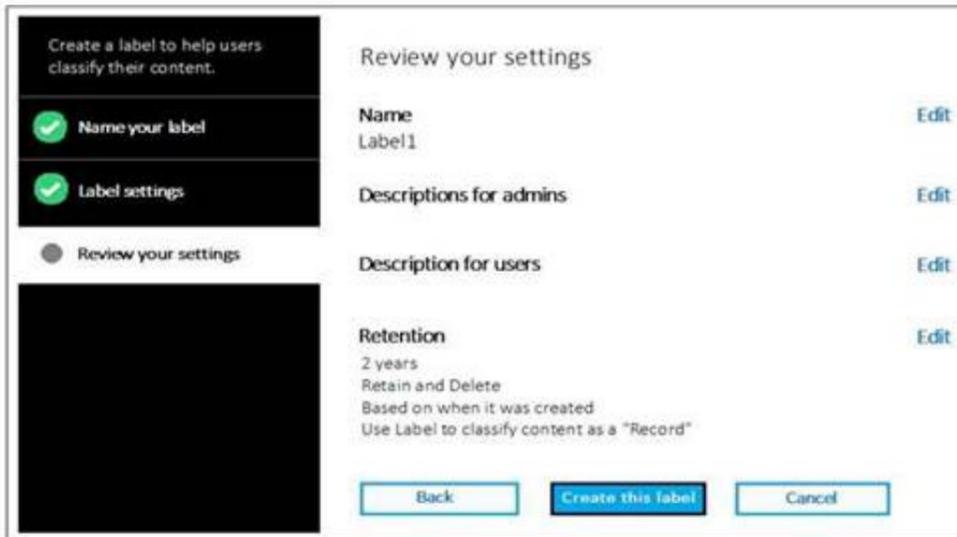
<https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies>

**NEW QUESTION 106**

**HOTSPOT**

You have a Microsoft 365 subscription.

You create a retention label named Label1 as shown in the following exhibit.



You publish Label1 to SharePoint sites.

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 create a file in a Microsoft SharePoint library on January 1, 2019, you can [answer choice].

▼
never delete the file.
delete the file before January 1, 2021.
delete the file after January 1, 2021.

If you create a file in a Microsoft SharePoint library on March 15, 2019, the file will [answer choice].

▼
always remain in the library.
remain in the library until you delete the file.
be deleted automatically on March 15, 2021.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

References:

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

**NEW QUESTION 111**

You have a Microsoft 365 subscription.

You create a retention policy and apply the policy to Exchange Online mailboxes.

You need to ensure that the retention policy tags can be assigned to mailbox items as soon as possible.

What should you do?

- A. From Exchange Online PowerShell, run Start-RetentionAutoTagLearning
- B. From Exchange Online PowerShell, run Start-ManagedFolderAssistant
- C. From the Security & Compliance admin center, create a data loss prevention (DLP) policy
- D. From the Security & Compliance admin center, create a label policy

**Answer:** D

**Explanation:**

References:

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

**NEW QUESTION 112**

You have a Microsoft 365 subscription.

You need to ensure that users can manually designate which content will be subject to data loss prevention (DLP) policies.

What should you create first?

- A. A retention label in Microsoft Office 365
- B. A custom sensitive information type
- C. A Data Subject Request (DSR)
- D. A safe attachments policy in Microsoft Office 365

**Answer:** C

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-thedsr-case-tool#more-information-about-using-the-dsr-case-tool>

**NEW QUESTION 113**

Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. the Exchange admin center
- B. the Azure ATP admin center
- C. Microsoft Azure Security Center
- D. the Security & Compliance admin center
- E. Outlook on the web

**Answer:** AD

**Explanation:**

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files>

**NEW QUESTION 118**

You have a Microsoft 365 subscription. You enable auditing for the subscription.

You plan to provide a user named Auditor with the ability to review audit logs. You add Auditor to the Global administrator role group.

Several days later, you discover that Auditor disabled auditing.

You remove Auditor from the Global administrator role group and enable auditing.

- A. Security operator
- B. Security reader
- C. Security administrator
- D. Compliance administrator

**Answer:** D

**NEW QUESTION 123**

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine. Which type of threat management policy should you create?

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

**Answer:** A

**NEW QUESTION 124**

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 127**

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 Security 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 129**

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 133**

.....

## 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](#)