MS-500 Q&As

Microsoft 365 Security Administration

Pass Microsoft MS-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.certbus.com/ms-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

HOTSPOT

You create device groups in Microsoft Defender for Endpoint as shown in the following table.

Name	Rank
Group1	1
Group2	2
Group3	3

Membership rule
Name Starts with Device
Tag Equals Tag1
Name Starts with Computer and OS is Windows 10

You onboard three devices to Microsoft Defender for Endpoint as shown in the following table.

Name	Operating system
Device1	Windows 10
Device2	MacOS
Computer3	Windows 10

After the devices are onboarded, you perform the following actions:

1.

Add a tag named Tag1 to Device1.

2.

Rename Computer3 as Device3.

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

Hot Area:

Answer Area

Correct Answer:

Answer Area

Box 1: No

The Group1 membership rule \\'Name Start with Device\\' applies to Device1.

However, the higher ranked Group2 membership rule \\'Tag Equals Tag1\\' also applies to Device1, and overrules the lower ranked rule.

Note: Specify the matching rule that determines which device group belongs to the group based on the device name, domain, tags, and OS platform. If a device is also matched to other groups, it\\'s added only to the highest ranked device

group.

Box 2: No

The Group1 membership rule \\'Name Start with Device\\' applies Device2.

No other rule applies.

Box 3: Yes

The Group3 rule applies for Computer3.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups

QUESTION 2

You have a hybrid Azure Active Directory (Azure AD) tenant that has pass- through authentication enabled.

You plan to implement Azure AD identity Protection and enable the user risk policy.

You need to configure the environment to support the user risk policy.

What should you do first?

A. Enable password hash synchronization.

B. Configure a conditional access policy.

C. Enforce the multi-factor authentication (MFA) registration policy.

D. Enable the sign-in risk policy.

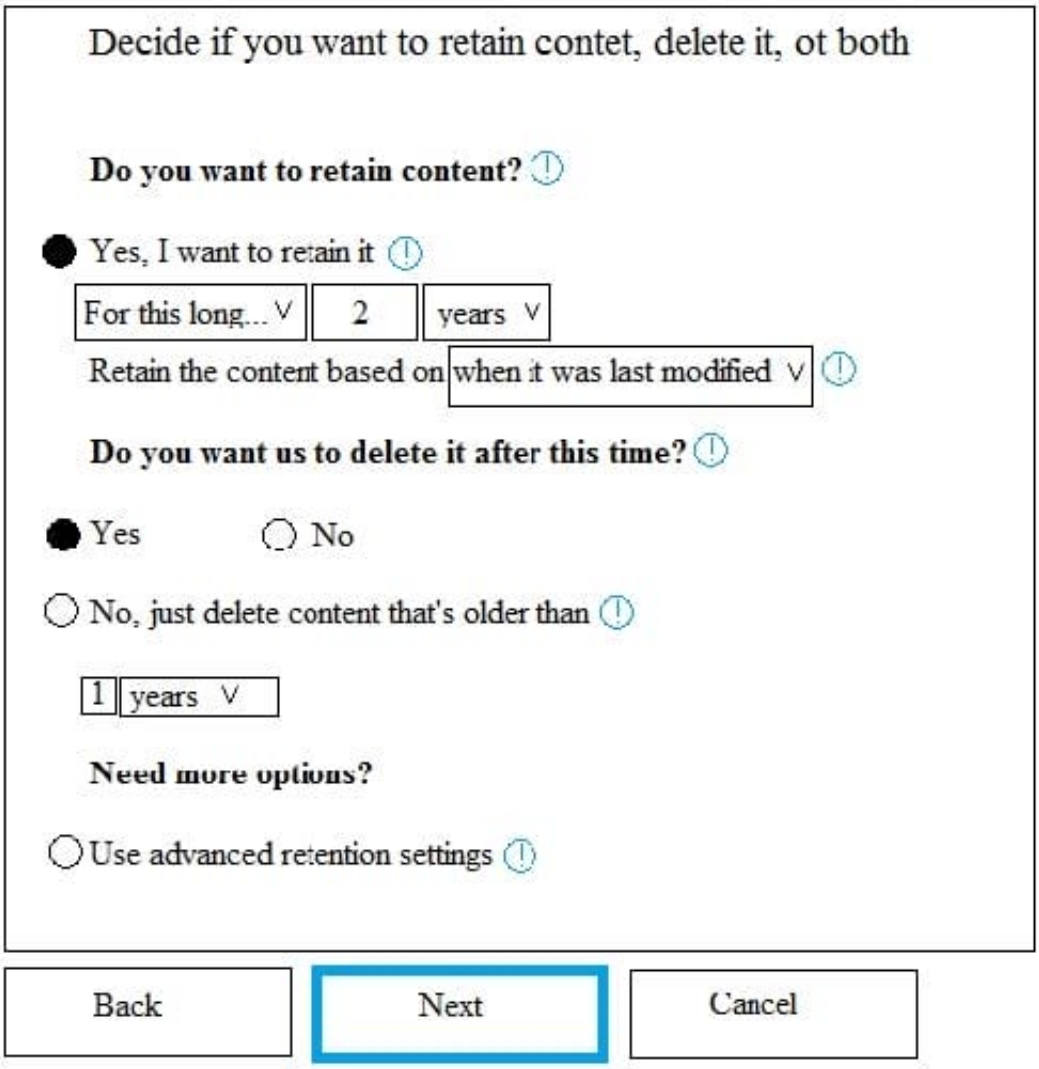
Correct Answer: A

QUESTION 3

HOTSPOT

You have a Microsoft 365 subscription.

You are creating a retention policy named Retention1 as shown in the following exhibit.



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.

Hot Area:

Answer Area

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 a 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]**.

can recover the file until the Recycle Bin retention period expires
can recover the file until January 1, 2021
can recover the file until March 1, 2021
can recover the file until May 1, 2021

Correct Answer:

Answer Area

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 a 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]**.

can recover the file until the Recycle Bin retention period expires
can recover the file until January 1, 2021
can recover the file until March 1, 2021
can recover the file until May 1, 2021

1.- Retained

2.- Can recover the file until the Recycle Bin retention period expired (93 days). Because the question says "the user", so the user can\\'t recover a file from the "Preservation hold library". "If the content is modified or deleted during the retention period, a copy of the original content as it existed when the retention policy was assigned is created in the Preservation Hold library. There, the timer job identifies items whose retention period has expired. Those items are moved to the second-stage Recycle Bin, where they\\'re permanently deleted at the end of 93 days. The second-stage Recycle Bin is not visible to end users (only the first-stage Recycle Bin is), but site collection admins can view and restore content from there." https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-sharepoint?view=o365-worldwide

QUESTION 4

You have a Microsoft 365 E5 subscription.

Some users are required to use an authenticator app to access Microsoft SharePoint Online.

You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.

What should you do?

A. From the Azure Active Directory admin center, view the sign-ins.

B. From the Microsoft 365 Security admin center, download a report.

C. From the Enterprise applications blade of the Azure Active Directory admin center, view the audit logs.

D. From the Azure Active Directory admin center, view the authentication methods.

Correct Answer: A

The user sign-ins report provides information on the sign-in pattern of a user, the number of users that have signed in over a week, and the status of these sign- ins.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

1.

From the Enterprise applications blade of the Azure Active Directory admin center, view the sign-ins.

2.

From the Azure Active Directory admin center, view the sign-ins. Other incorrect answer options you may see on the exam include the following:

1.

From Azure Log Analytics, query the logs.

2.

From the Microsoft 365 Compliance center, perform an audit log search.

3.

From the Microsoft 365 Defender portal, download a report.

Reference:

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

QUESTION 5

You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD).

To complete this task, sign in to the Microsoft Office 365 admin center.

Correct Answer: See explanation below.

1.

After signing into the Microsoft 365 admin center, click Admin centers > Azure Active Directory > Devices.

2.

Navigate to Device Settings.

3.

Set the Users may join devices to Azure AD setting to All.

4.

Set the Additional local administrators on Azure AD joined devices setting to None.

5.

Set the Users may register their devices with Azure AD setting to All.

6.

Leave the Require Multi-Factor Auth to join devices setting on it default setting.

7.

Set the Maximum number of devices setting to 5.

8.

Set the Users may sync settings and app data across devices setting to All.

9.

Click the Save button at the top left of the screen.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?view=o365-worldwide

---

QUESTION 6

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 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 User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Compliance Manager uses a role-based access control (RBAC) permission model. Only users who are assigned a role may access Compliance Manager, and the actions allowed by each user are restricted by role type. https://learn.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide#set-user-permissions-and-assign-roles

QUESTION 7

HOTSPOT

You have a Microsoft 365 sensitivity label that is published to all the users in your Azure Active Directory (Azure AD) tenant as shown in the following exhibit.

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

Hot Area:

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Correct Answer:

Statements	Yes	No
All the documents stored on each user's computer will include a watermark automatically.	○	○
If the sensitivity label is applied to a document, the document will have a header that contains the word "INTERNAL".	○	○
The sensitivity label can be applied only to documents that contain the word rebranding.	○	○

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide#when-office-apps-apply-content-marking-and-encryption

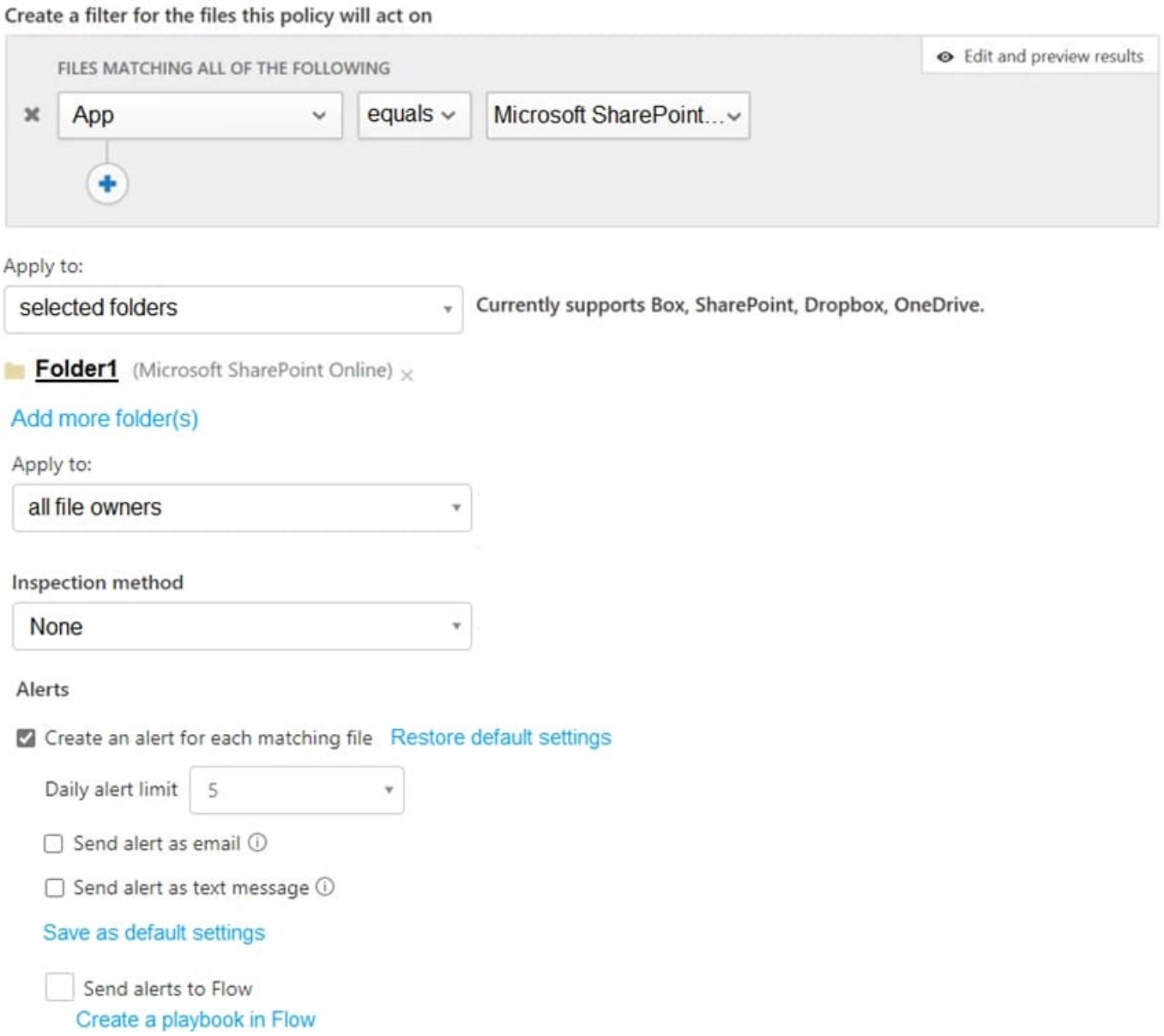
QUESTION 8

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 contains the folders shown in the following table.

Name	File in folder
Folder1	File1
Folder2	File2

At 09:00, you create a Microsoft Cloud App Security policy named Policy1 as shown in the following exhibit.



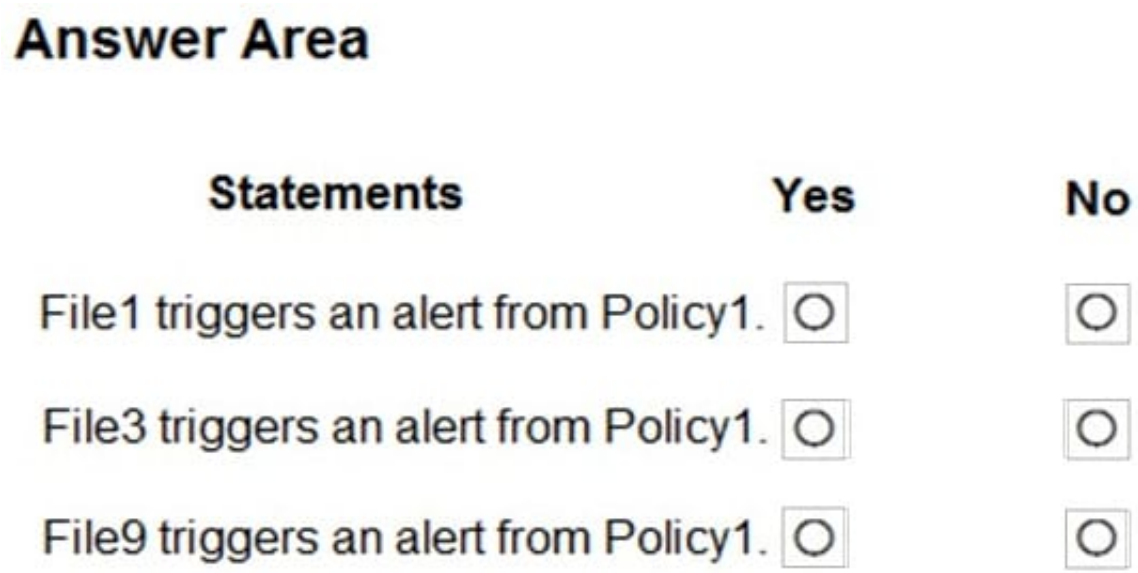
After you create Policy1, you upload files to Site1 as shown in the following table.

Time	Name	Uploaded to
09:05	File3	Folder2
09:10	File4	Folder1
09:15	File5	Folder2
09:20	File6	Folder1
09:25	File7	Folder1
09:30	File8	Folder1
09:33	File9	Folder1

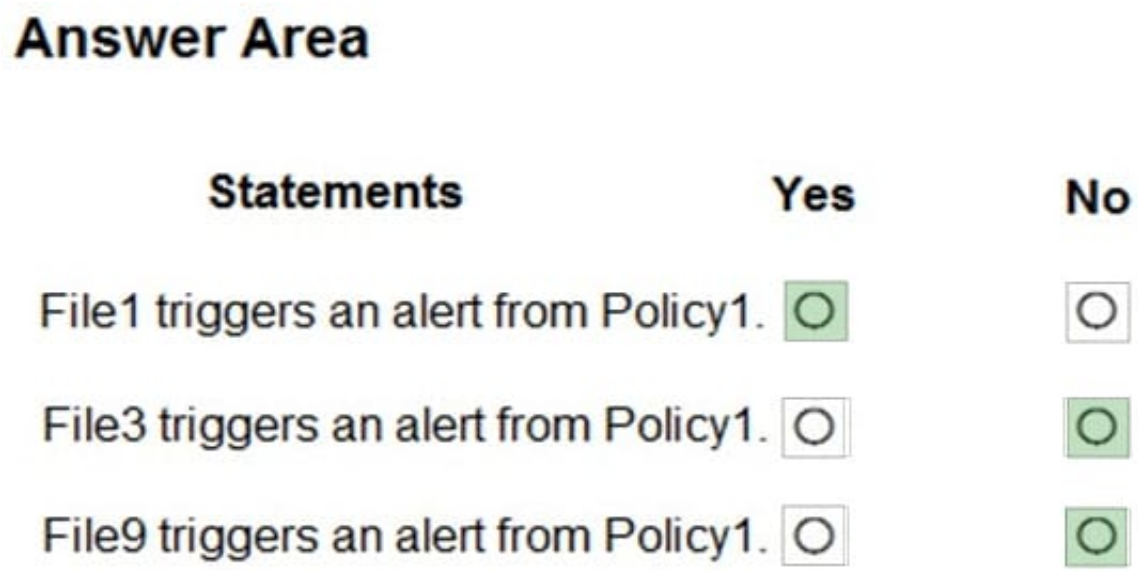
For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/cloud-app-security/data-protection-policies

QUESTION 9

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.

Solution: You use the Security event log on Server1.

Does that meet the goal?

A. Yes

B. No

Correct Answer: B

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

QUESTION 10

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Office 365 enabled.

You need to review the zero-hour auto purge (ZAP) configuration for the subscription.

Which two threat policies should you review? Each correct answer presents part of the solution NOTE: Each correct selection is worth one point,

A. Safe attachments Built-in protection (Microsoft)

B. Anti-malware (Default) Default

C. Safe links Built-in protection (Microsoft)

D. Anti-spam outbound policy (Default)

E. Office365 AntiPhish Default (Default)

F. Anti-spam inbound policy (Default)

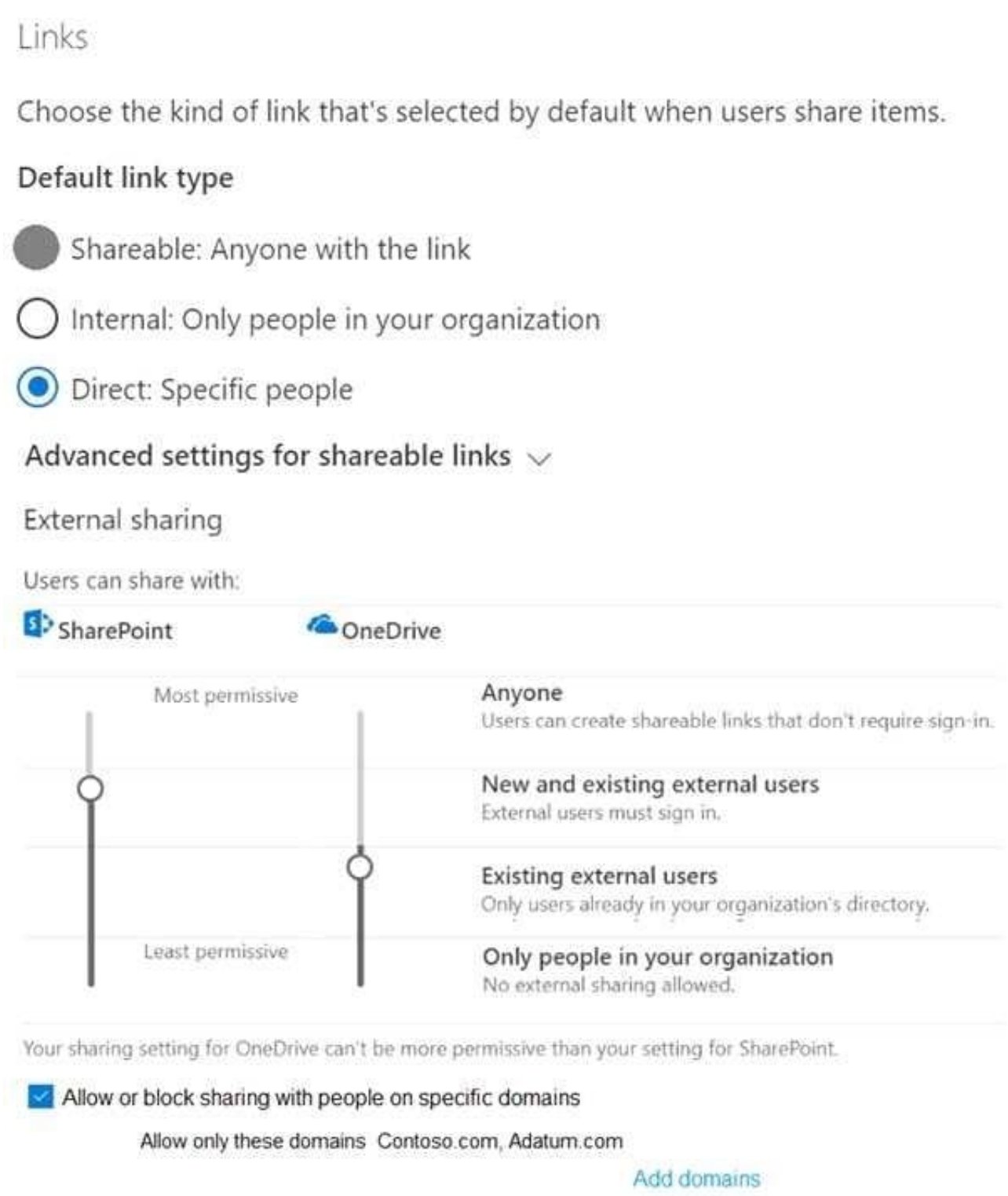
Correct Answer: BE

1) "ZAP for malware is enabled by default in anti-malware policies." https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#zero-hour-auto-purge-zap-for-malware 2) "By default, ZAP for phishing is enabled in anti-spam policies[...]" https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/zero-hour-auto-purge?view=o365-worldwide#zero-hour-auto-purge-zap-for-phishing

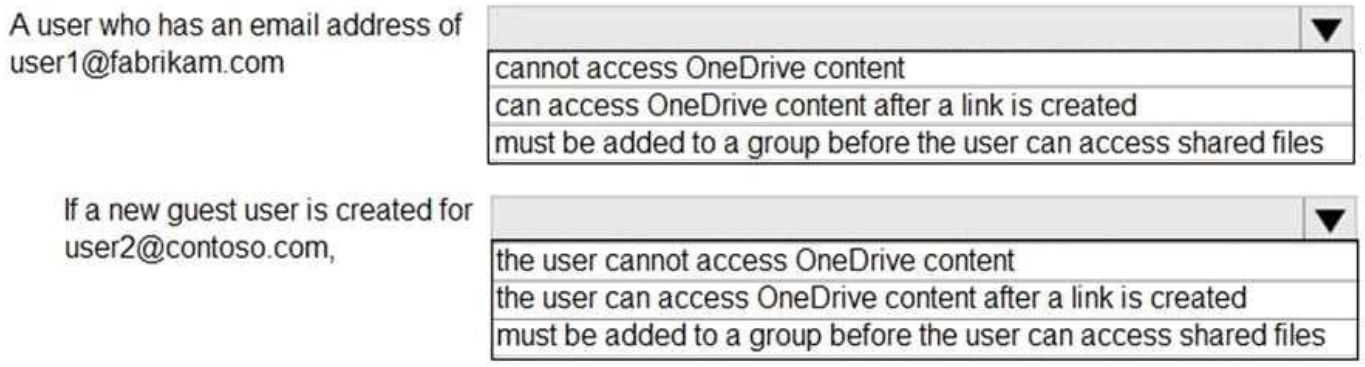
QUESTION 11

HOTSPOT

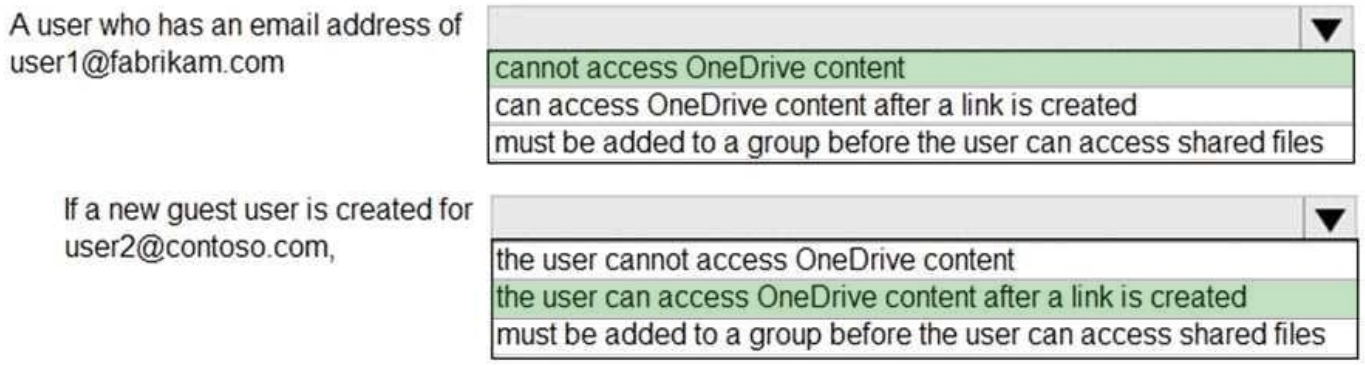
You have a Microsoft 365 subscription that uses a default domain name of litwareinc.com. You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.


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
Advanced settings for shareable links
External sharing
Users can share with:
SharePoint
OneDrive
Most permissive
Least permissive
Anyone
Users can create shareable links that don't require sign-in.
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.
Allow or block sharing with people on specific domains
Allow only these domains Contoso.com, Adatum.com
Add domains

Hot Area:



Correct Answer:



Reference: https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

QUESTION 12

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Email address	Role
Admin1	admin1@contoso.com	Global Administrator
Admin2	admin2@contoso.com	Security Administrator
Admin3	admin3@contoso.com	Security Reader
Admin4	admin4@contoso.com	User Administrator
User1	user1@contoso.com	*None*

Azure AD Identity Protection detects that the account of User1 is at risk and generates an alert. How many users will receive the alert?

A. 1

B. 2

C. 3

D. 4

Correct Answer: C

https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-notifications

QUESTION 13

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.

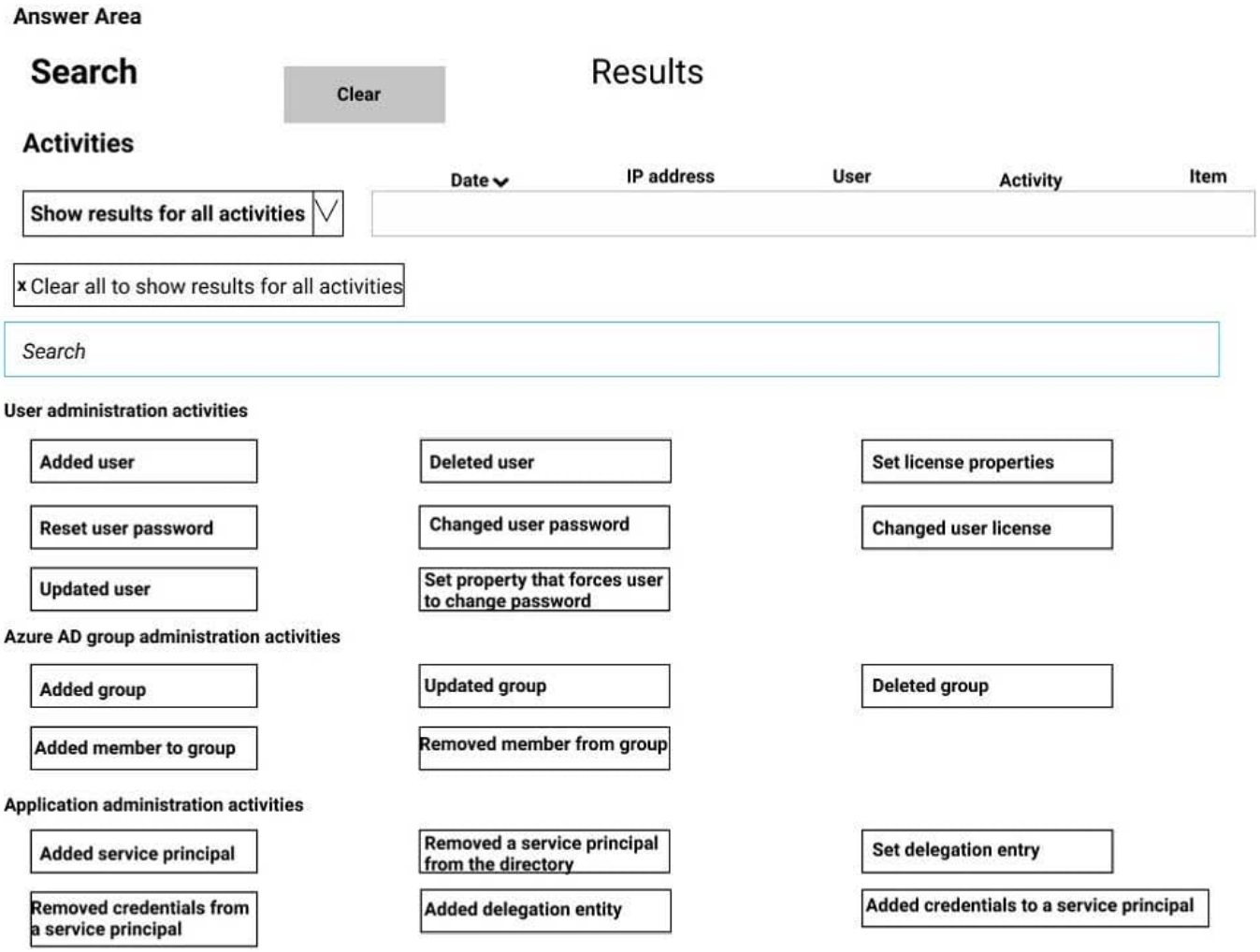
You need to search the audit log to identify why User1 was removed from Group1.

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.

Hot Area:

Answer Area



Correct Answer:

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

QUESTION 14

HOTSPOT

You have a Microsoft 365 subscription that uses Microsoft Teams and contains the users shown in the following table.

Name	Team membership
User1	Team1, Team2
User2	Team2

You have the retention policies shown in the following table.

Name	Location	Included	Retain items for	Start retention period	At the end of retention period
Policy1	Microsoft Teams channel messages	All teams	7 years	When items are created	Delete items automatically
	Microsoft Teams chats	User1			
Policy2	Microsoft Teams channel messages	Team1	5 years	When items are created	Delete items automatically
	Microsoft Teams chats	User2			

The users perform the actions shown in the following table.

User	Location	Action
User1	Team1 channel	Edits a message
User2	Private 1:1 chat with User1	Sends a message to User1
User1	Team2 channel	Deletes a message

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

Hot Area:

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	○	○
User1 can see the message sent by User2 for up to seven years.	○	○
The message deleted by User1 will be moved to the SubstrateHolds folder.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
The message edited by User1 will be deleted after five years.	○	○
User1 can see the message sent by User2 for up to seven years.	○	○
The message deleted by User1 will be moved to the SubstrateHolds folder.	○	○

Box 1: No

It will be retained for seven years.

Both Policy1 and Policy2 apply.

If there is a conflict in how long to retain the same content, it is retained in the secured location for the longest retention period.

Note: If you configure a Teams retention policy to retain chats or channel messages, users

Box 2: No

User2 creates the message in chat. Policy2 applies. The message will be retained for 5 years.

Box 3: Yes

After a retention policy is configured for chat and channel messages, a timer job from the Exchange service periodically evaluates items in the hidden mailbox folder where these Teams messages are stored. The timer job typically takes 1-7

Messages remain in the SubstrateHolds folder for at least 1 day, and then if they\\'re eligible for deletion, the timer job permanently deletes them the next time it runs.

Reference:

https://docs.microsoft.com/en-us/microsoftteams/retention-policies https://docs.microsoft.com/en-us/microsoft-365/compliance/retention-policies-teams

QUESTION 15

You have a Microsoft 365 E5 subscription that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to implement privileged access in Microsoft 365, Which groups can you specify as the default approval group?

A. Group4 only

B. Group3 or Group4 only

C. Group1, Group2, or Grcup3

D. Group1, Group3, or Group4 only

E. Group1, Group2. Group3, or Group4

Correct Answer: C

If the security group does not have an email address associated with it, you can still use it as the default approval group for privileged access in Microsoft 365.

When you select a security group as the default approval group, Azure AD Privileged Identity Management will send approval notifications to the members of the security group using their individual email addresses. The email notifications will contain a link to the approval request in the Azure portal, where the members can review the request and approve or deny it.

So even if the security group itself does not have an email address, the members of the group will still receive email notifications for any access requests that require approval. However, it\\'s important to ensure that the members of the security group have valid email addresses associated with their user accounts in Azure AD, so that they can receive the approval notifications.