



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.geekcert.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

DRAG DROP

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies.

You need to identify the following:

1.

Rules that are applied without Triggering a policy alert

2.

The top 10 files that have matched DLP policies

3.

Alerts that are miscategorized

Which report should you use for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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.

NOTE: Each correct selection is worth one point.

Select and Place:

	Rule that are applied without triggering a policy alert:	<input type="text"/>
DLP policy matches	The top 10 files that have matched DLP policies:	<input type="text"/>
False positive and override		
Incident reports	Alerts that are miscategorized:	<input type="text"/>

Correct Answer:



	Rule that are applied without triggering a policy alert:
	DLP policy matches
	The top 10 files that have matched DLP policies:
	Incident reports
	Alerts that are miscategorized:
	False positive and override

QUESTION 2

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

Correct Answer: B

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

QUESTION 3

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 System 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 4

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

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

What do you want to do if we detect sensitive info?

We'll automatically create activity reports so you can review the content that matches this policy. What else do you want to do?

Notify users when content matches the policy settings

- Show policy tips to users and send them an email notification.
Tips appear to users in their apps (like Outlook and SharePoint) and help them learn how to use sensitive info responsibly. You can use the default tip or customize it to your liking. [Learn more about notifications and tips](#)
[Customize the tip and email](#)
- Detect when a specific amount of sensitive info is being shared at one time.
 - Detect when content that's being shared contains:
At least instances of the same sensitive info type.
 - Send incident reports in email
By default, you and your global admin will automatically receive the email.
[Choose what to include in the report and who receives it](#)
 - Restrict access or encrypt the content

[Back](#) [Next](#) [Cancel](#)

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

Correct Answer: A

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

QUESTION 5

You have a Microsoft 365 subscription.

You have a Data Subject Request (DSR) case named Case1.

You need to ensure that Case1 includes all the email posted by the data subject to the Microsoft Exchange Online public folders.

Which additional property should you include in the Content Search query?

- A. kind:externaldata
- B. itemclass:ipm.externaldata
- C. itemclass:ipm.post
- D. kind:email

Correct Answer: C

To ensure that the Data Subject Request (DSR) case named Case1 includes all the email posted by the data subject to the Microsoft Exchange Online public folders, you should include the property "itemclass:ipm.post" in the Content Search

query. The "itemclass:ipm.post" property will search for items of the "Post" message class, which are used for messages posted to public folders.

Option A, "kind:externaldata," is not relevant to searching for email messages posted to public folders.

Option B, "itemclass:ipm.externaldata," is not relevant to searching for email messages posted to public folders. The "ipm.externaldata" message class is used for messages that contain links to external data sources.

Option D, "kind:email," would not be sufficient to search for email messages posted to public folders. This property would only search for email messages in the mailbox of the data subject, not in public folders.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsr-case-tool?view=o365-worldwide>