Exam Questions MS-500

Microsoft 365 Security Administrator

https://www.2passeasy.com/dumps/MS-500/

NEW QUESTION 1
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 2
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 3
Which user passwords will User2 be prevented from resetting?

A. User6 and User7
B. User4 and User6
C. User4 only
D. User7 and User8
E. User8 only

Answer: C

NEW QUESTION 4
Which role should you assign to User1?

A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator

Answer: D

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim

NEW QUESTION 5
What should User6 use to meet the technical requirements?

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

Answer: B

NEW QUESTION 6
HOTSPOT
Which policies apply to which devices? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

DevicePolicy1:	None
	Device1 only
	Device3 only
	Device2 and Device3 only
	Device1 and Device3 only
	Device1, Device2, and Device3

DevicePolicy2:	None
	Device4 only
	Device2 and Device4 only
	Device2, Device3, and Device 4 only

NEW QUESTION 7
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 User1. Does this meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 8
Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated

goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that is associated to a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.
You use Active Directory Federation Services (AD FS) to federate on-premises Active Directory and the tenant. Azure AD Connect has the following settings:
• Source Anchor: objectGUID
• Password Hash Synchronization: Disabled
• Password writeback: Disabled
• Directory extension attribute sync: Disabled
• Azure AD app and attribute filtering: Disabled
• Exchange hybrid deployment: Disabled
• User writeback: Disabled
You need to ensure that you can use leaked credentials detection in Azure AD Identity Protection. Solution: You modify the Password Hash Synchronization settings.
Does that meet the goal?

A. Yes
B. No

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/azure/security/azure-ad-secure-steps

NEW QUESTION 9
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 10
You have a Microsoft 365 E5 subscription.
You implement Advanced Threat Protection (ATP) safe attachments policies for all users.
User reports that email messages containing attachments take longer than expected to be received. You need to reduce the amount of time it takes to receive email messages that contain attachments. The solution must ensure that all attachments are scanned for malware. Attachments that have malware must be blocked.
What should you do from ATP?

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

Answer: D

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

NEW QUESTION 10
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com. Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

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

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.
You create an app protection policy named ProtectionPolicy1 that has the following settings:
• Protected apps: App1
• Exempt apps: App2
• Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1. For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	○
From Device2, User1 can copy data from App1 to App2.	○	○
From Device2, User1 can copy data from App1 to App3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

	Yes	No
From Device1, User1 can copy data from App1 to App3.	○	●
From Device2, User1 can copy data from App1 to App2.	●	○
From Device2, User1 can copy data from App1 to App3.	●	○

NEW QUESTION 13
HOTSPOT
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

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

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

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

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

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

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	⊙	○
User2 can collect an investigation package from Device2.	⊙	⊙
User3 can isolate Device1.	○	⊙

NEW QUESTION 14
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 16
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 21
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-groupswindows-defender-advanced-threat-protection

NEW QUESTION 23
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 27

Note: This question is part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You add CompanyConfidential to a global policy.

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

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

A. Yes
B. No

Answer: B

NEW QUESTION 32

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.

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
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	Yes	No
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 33
You create a data loss prevention (DLP) policy as shown in the following shown:
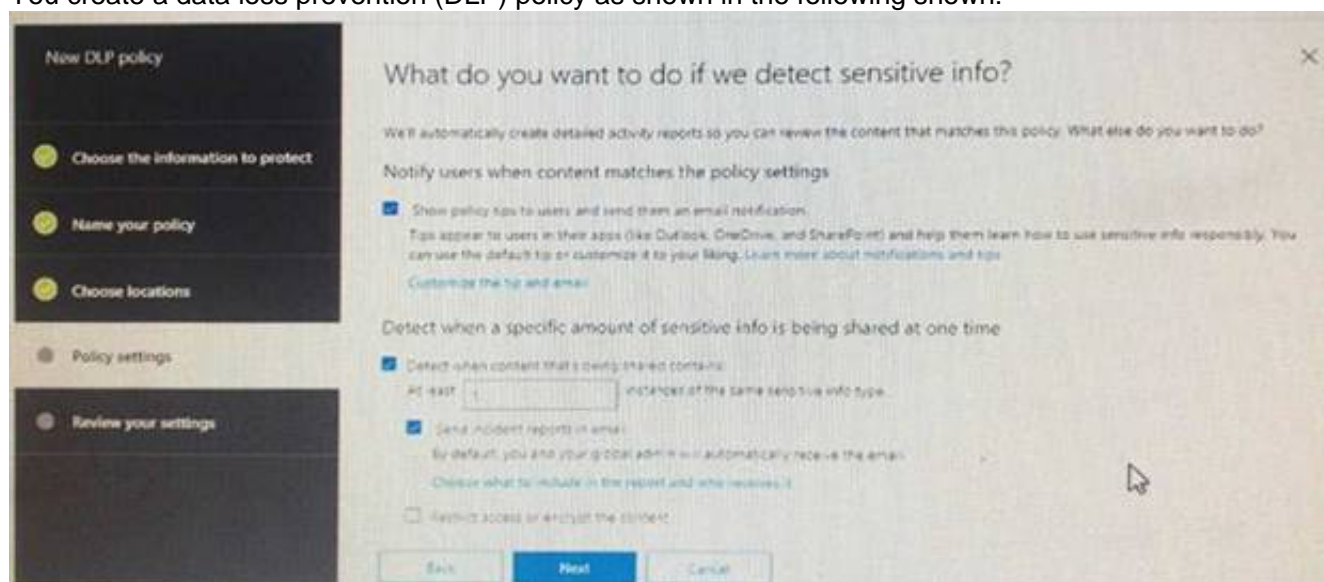
What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?

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 36
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 41
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.

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 Jauary 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 Jauary 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 Jauary 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 Jauary 1,2020
can recover the file until March 1,2020
can recover the file until May 1,2020

NEW QUESTION 44
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 48
You have a Microsoft 365 subscription.
Yesterday, you created retention labels and published the labels to Microsoft Exchange Online mailboxes.
You need to ensure that the labels will be available for manual assignment as soon as possible. What should you do?

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

Answer: C

NEW QUESTION 51
HOTSPOT
You have a Microsoft 365 E5 subscription.
Users and device objects are added and removed daily. Users in the sales department frequently
change their device.
You need to create three following groups:

Group		Requirement
	1	All the devices of users where the Department attributes is set to Sales
	2	All the devices where the Department attribute is set to Sales
	3	All the devices where the deviceOwnership attribute is set to Company

The solution must minimize administrative effort.
What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Groups that have assigned membership:

```
0
1
2
3
```

Groups that have dynamic membership:

```
0
1
2
3
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md

NEW QUESTION 55
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/setadminauditlogconfig?view=exchange-ps

NEW QUESTION 58
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 61
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.

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 66
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 70
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 75
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 79
You have a Microsoft 365 subscription.
You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.
You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.
Which cmdlet should you use?

A. Get-UnifiedGroup
B. Get-MailUser
C. Get-TeanMessagingSettings
D. Get-TeamChannel

Answer: A

NEW QUESTION 80
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 81
Your network contains an on-premises Active Directory domain. The domain contains servers that
run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?

A. Configure Event Forwarding on the domain controllers
B. Configure auditing in the Office 365 Security & Compliance center.
C. Turn on Delayed updates for the Azure ATP sensors.
D. Enable the Audit account management Group Policy setting for the servers.

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION 85
......

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-500 Product From:

https://www.2passeasy.com/dumps/MS-500/

Money Back Guarantee

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