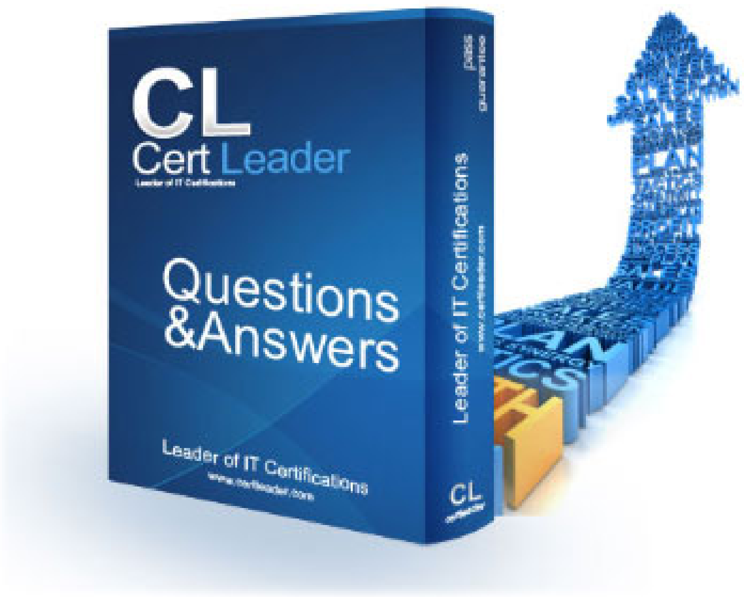
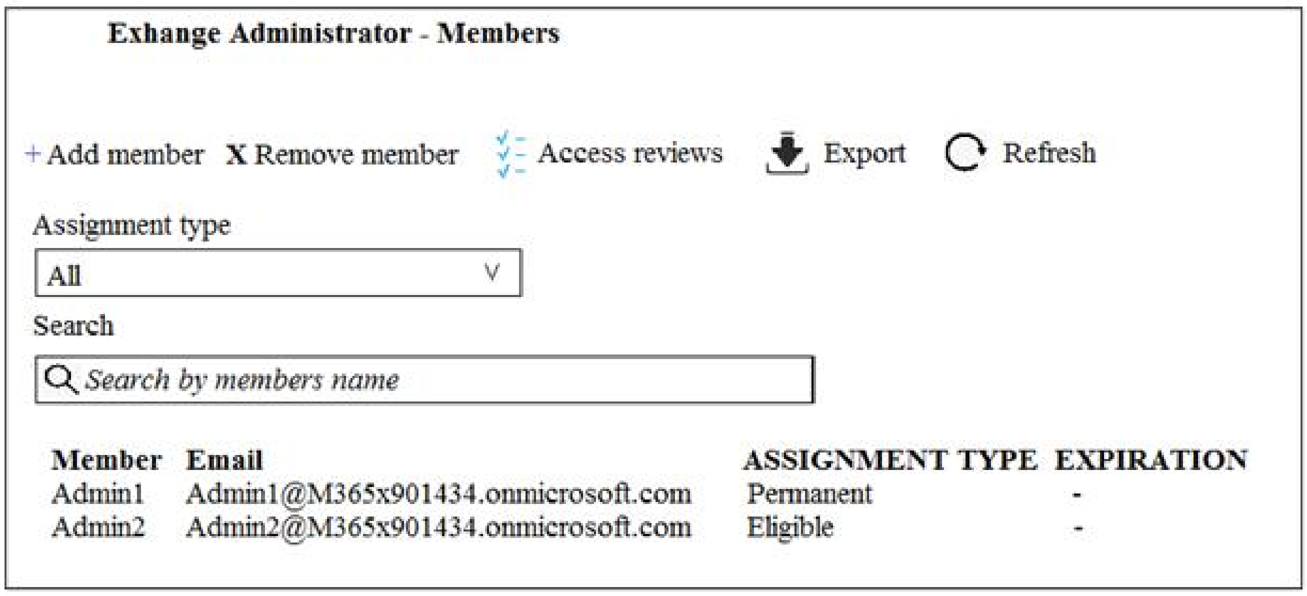
MS-500 Dumps

Microsoft 365 Security Administrator

https://www.certleader.com/MS-500-dumps.html



NEW QUESTION 1
An administrator configures Azure AD Privileged Identity Management as shown in the following exhibit.



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

What should you do to meet the security requirements?

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

Answer: D

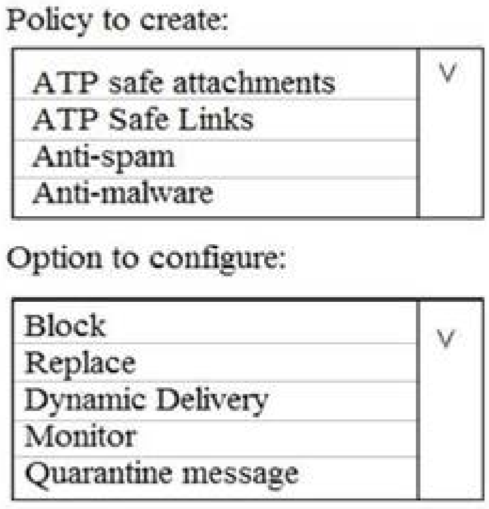
NEW QUESTION 2
You need to recommend a solution for the user administrators that meets the security requirements for auditing.
Which blade should you recommend using from the Azure Active Directory admin center?

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

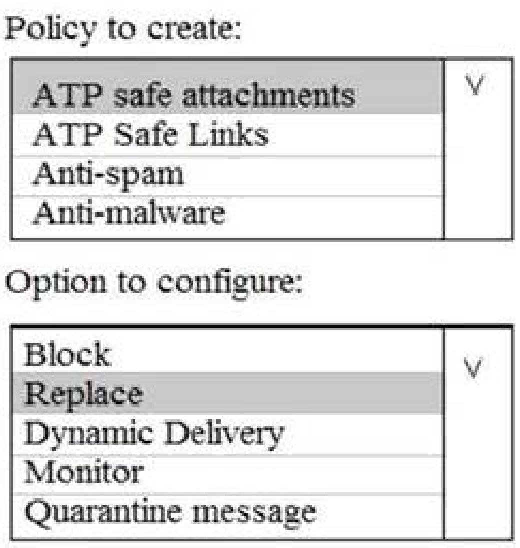
NEW QUESTION 3
HOTSPOT
You need to recommend an email malware solution that meets the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



Policy to create:

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

Option to configure:

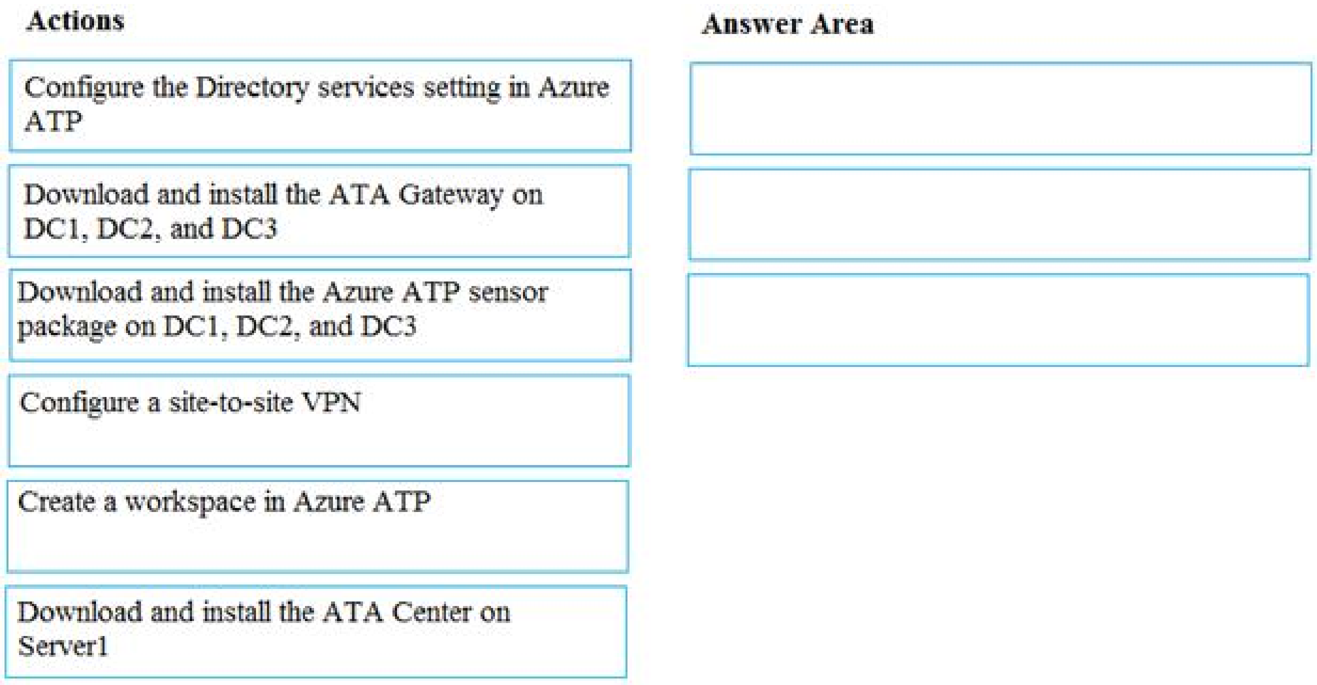
Block
Replace
Dynamic Delivery
Monitor
Quarantine message

NEW QUESTION 4

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

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

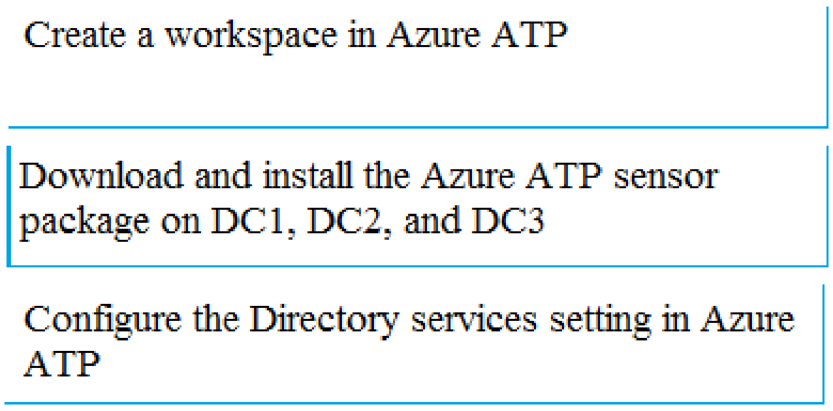
Download and install the ATA Center on Server1

Answer Area

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 5

You need to implement Windows Defender ATP to meet the security requirements. What should you do?

A. Configure port mirroring
B. Create the ForceDefenderPassiveMode registry setting
C. Download and install the Microsoft Monitoring Agent
D. Run WindowsDefenderATPOnboardingScript.cmd

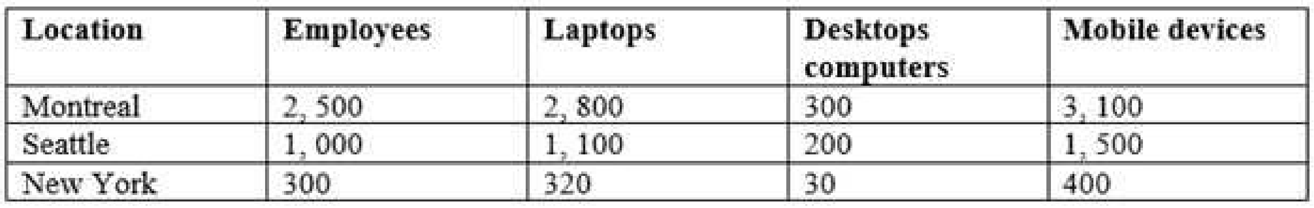
Answer: C

Explanation:

Case Study: 3 Contoso, Ltd Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and three branch offices in Seattle, and New York.

The company has the offices shown in the following table.



Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

Contoso has IT, human resources (HR), legal, marketing, and finance departments. Contoso uses Microsoft 365.

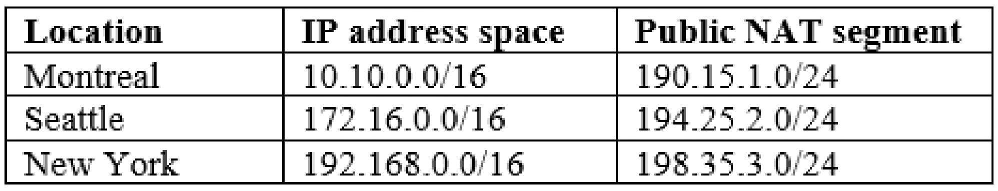
Existing Environment Infrastructure

The network contains an Active Directory domain named contoso.com that is synced to a Microsoft Azure Active Directory (Azure AD) tenant. Password writeback is enabled.

The domain contains servers that run Windows Server 2016. The domain contains laptops and desktop computers that run Windows 10 Enterprise.

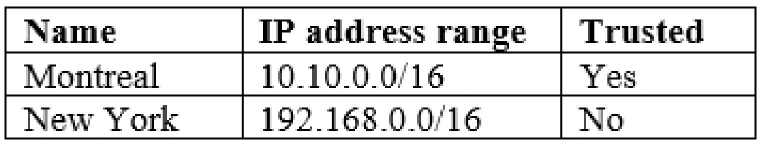
Each client computer has a single volume.

Each office connects to the Internet by using a NAT device. The offices have the IP addresses 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

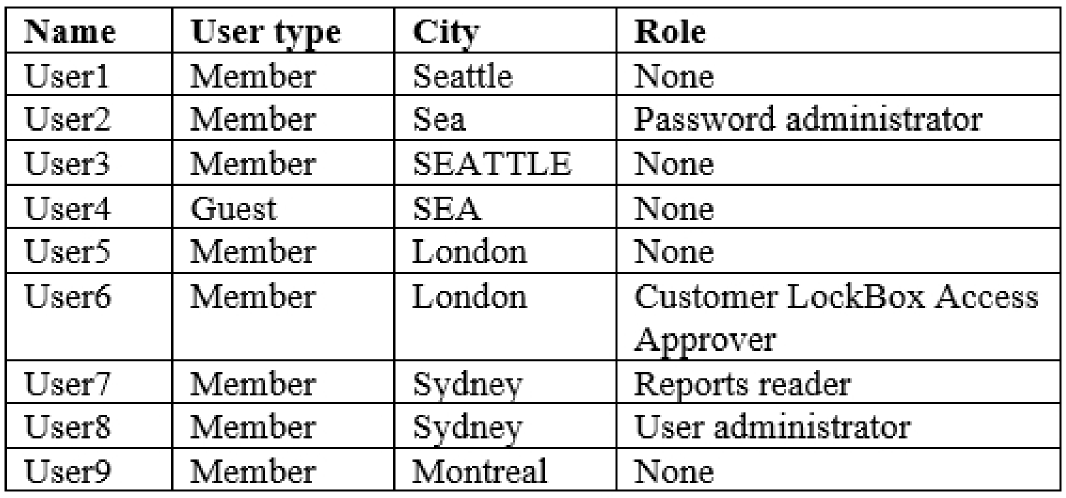
Named locations are defined in Azure AD as shown in the following table.



Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

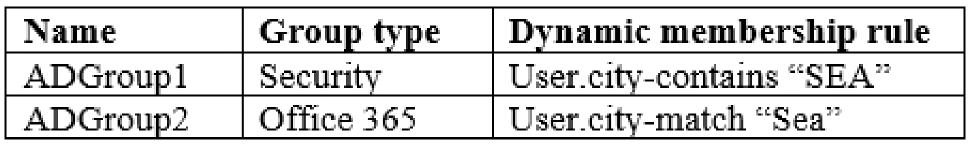
From the Multi-Factor Authentication page, an address space of 198.35.3.0/24 is defined in the trusted IPs list.

Azure Multi-Factor Authentication (MFA) is enabled for the users in the finance department. The tenant contains the users shown in the following table.



Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

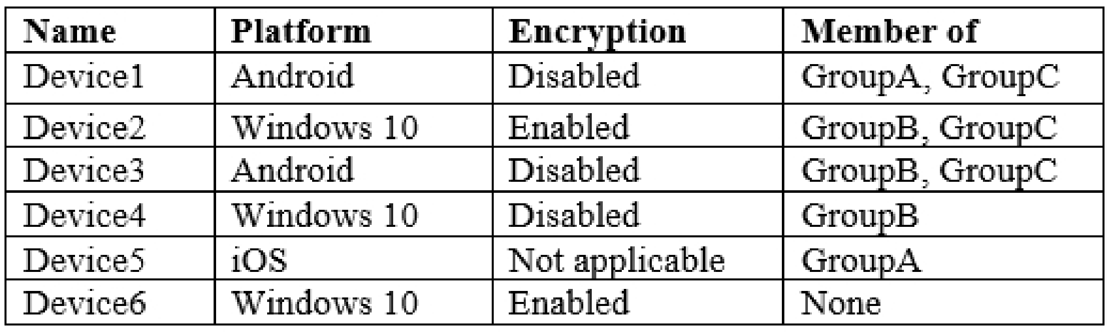
The tenant contains the groups shown in the following table.



Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains “SEA”
ADGroup2	Office 365	User.city-match “Sea”

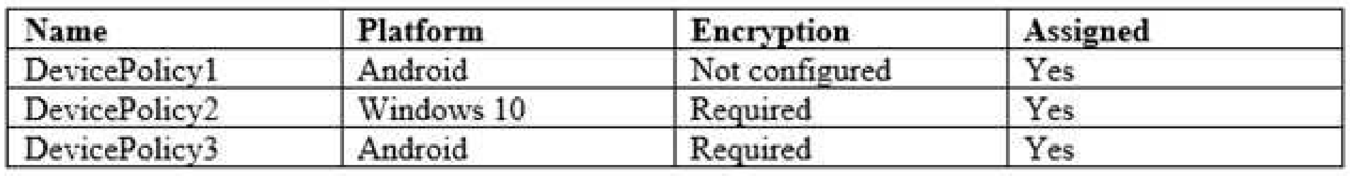
Customer Lockbox is enabled in Microsoft 365. Microsoft Intune Configuration

The devices enrolled in Intune are configured as shown in the following table.



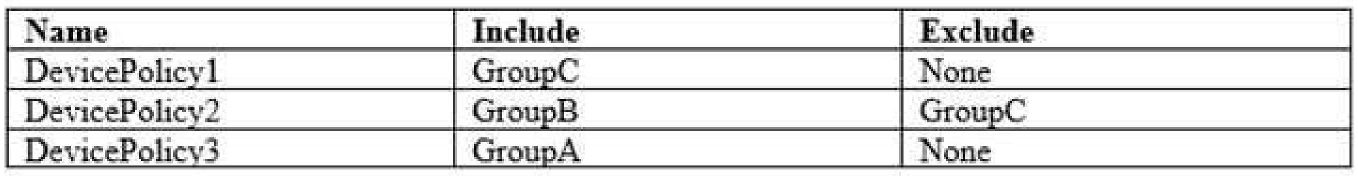
Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

The device compliance policies in Intune are configured as shown in the following table.



Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

The device compliance policies have the assignments shown in the following table.



Name	Include	Exclude
DevicePolicy1	GroupC	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

The Mark devices with no compliance policy assigned as setting is set to Compliant.

Requirements

Technical Requirements

Contoso identifies the following technical requirements:

•Use the principle of least privilege

•Enable User1 to assign the Reports reader role to users

•Ensure that User6 approves Customer Lockbox requests as quickly as possible

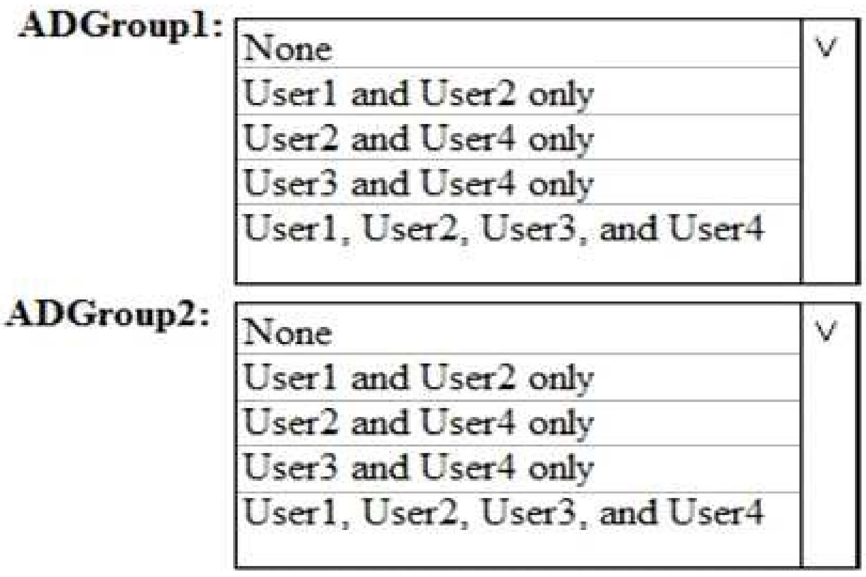
•Ensure that User9 can implement Azure AD Privileged Identity Management

NEW QUESTION 6

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.



ADGroup1:

None
User1 and User2 only
User2 and User4 only
User3 and User4 only
User1, User2, User3, and User4

ADGroup2:

None
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 7

You need to meet the technical requirements for User9. What should you do?

A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9

B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9

C. Assign the Security administrator role to User9

D. Assign the Global administrator role to User9

Answer: A

Explanation:

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

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

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

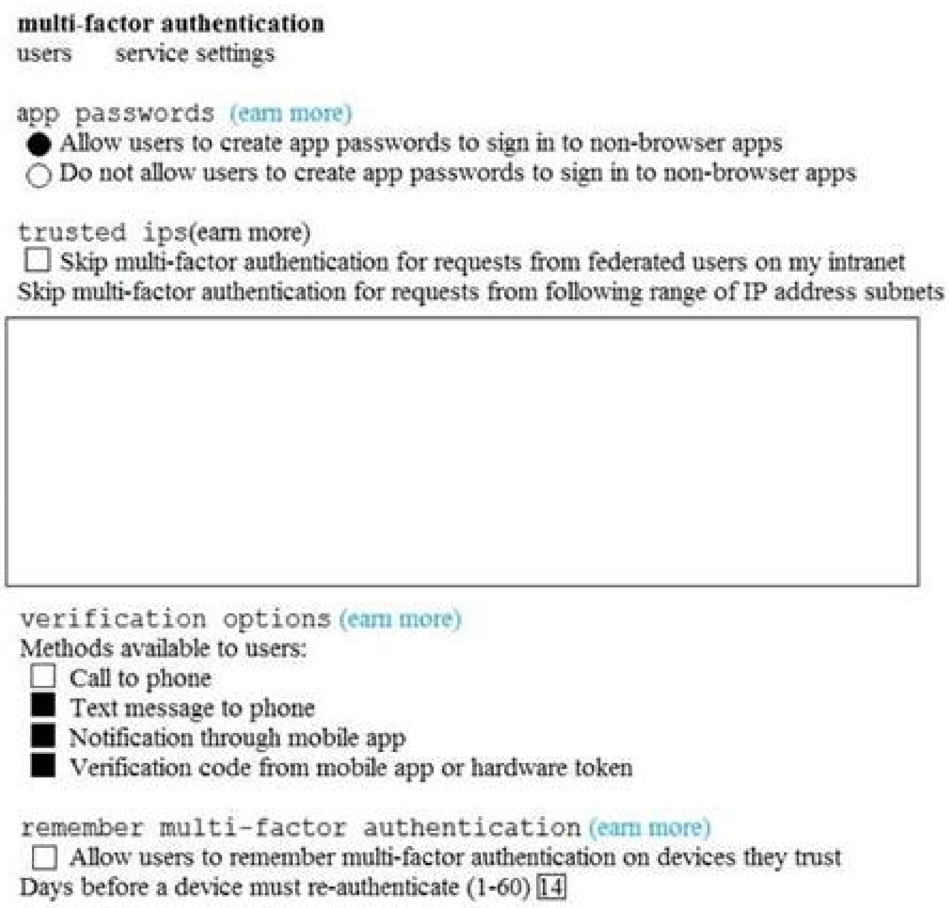
•Password Hash Synchronization: Disabled

•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 Source Anchor settings.
Does that meet the goal?

A. Yes
B. No

Answer: B

NEW QUESTION 10
HOTSPOT
You have a Microsoft 365 subscription that uses a default domain name of contoso.com.
The multi-factor authentication (MFA) service settings are configured as shown in the exhibit. (Clock the Exhibit tab.)



multi-factor authentication
users service settings

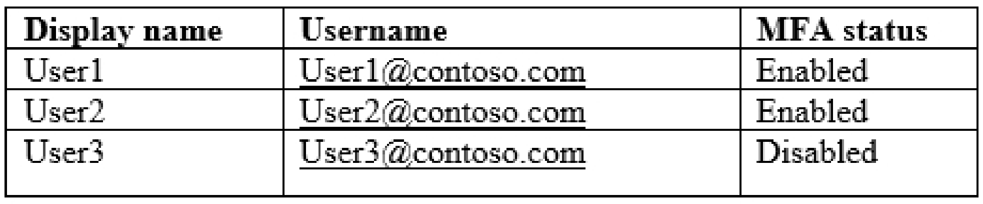
app passwords (earn more)
● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

trusted ips(earn more)
□ Skip multi-factor authentication for requests from federated users on my intranet
Skip multi-factor authentication for requests from following range of IP address subnets

verification options (earn more)
Methods available to users:
□ Call to phone
■ Text message to phone
■ Notification through mobile app
■ Verification code from mobile app or hardware token

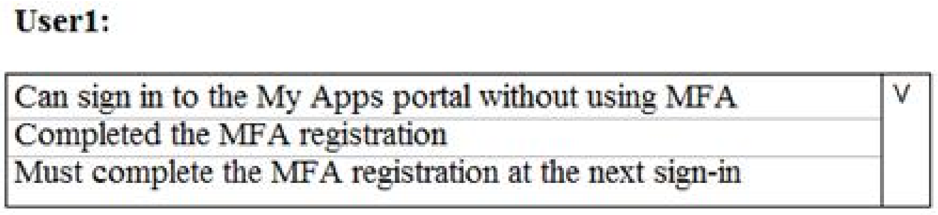
remember multi-factor authentication (earn more)
□ Allow users to remember multi-factor authentication on devices they trust
Days before a device must re-authenticate (1-60) 14

In contoso.com, you create the users shown in the following table.



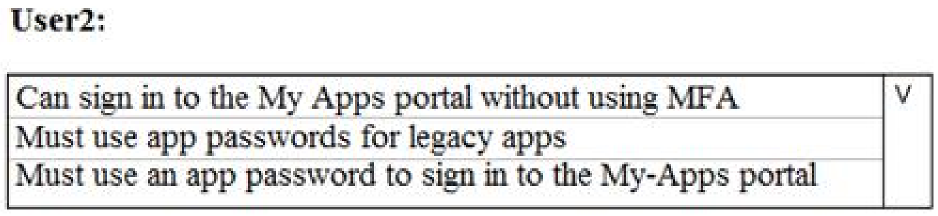
Display name	Username	MFA status
User1	User1@contoso.com	Enabled
User2	User2@contoso.com	Enabled
User3	User3@contoso.com	Disabled

What is the effect of the configuration? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



User1:

Can sign in to the My Apps portal without using MFA
Completed the MFA registration
Must complete the MFA registration at the next sign-in



User2:

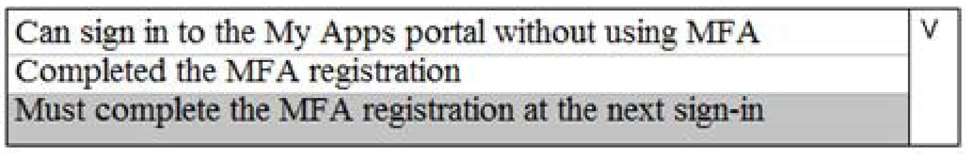
Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My-Apps portal

A. Mastered
B. Not Mastered

Answer: A

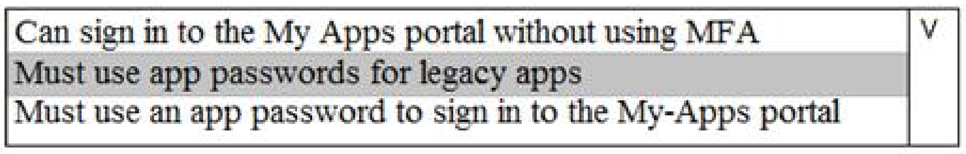
Explanation:

User1:



Can sign in to the My Apps portal without using MFA
Completed the MFA registration
Must complete the MFA registration at the next sign-in

User2:



Can sign in to the My Apps portal without using MFA
Must use app passwords for legacy apps
Must use an app password to sign in to the My-Apps portal

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 13
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 User1with 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 18
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 20
You have a Microsoft 365 tenant.
You have 500 computers that run Windows 10.
You plan to monitor the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP) after the computers are enrolled in Microsoft Intune.
You need to ensure that the computers connect to Windows Defender ATP. How should you prepare Intune for Windows Defender ATP?

A. Configure an enrollment restriction
B. Create a device configuration profile
C. Create a conditional access policy
D. Create a Windows Autopilot deployment profile

Answer: B

Explanation:
Reference:
https://docs.microsoft.com/en-us/intune/advanced-threat-protection

NEW QUESTION 23

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 26

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 30

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?

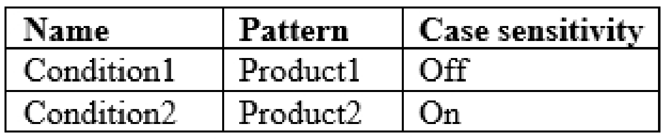
A. Yes
B. No

Answer: B

NEW QUESTION 35

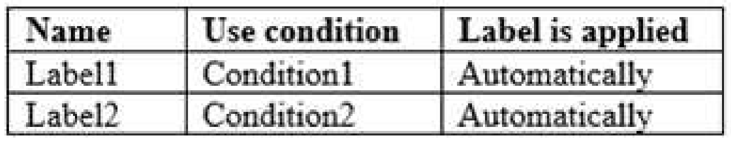
HOTSPOT

You have the Microsoft conditions shown in the following table.



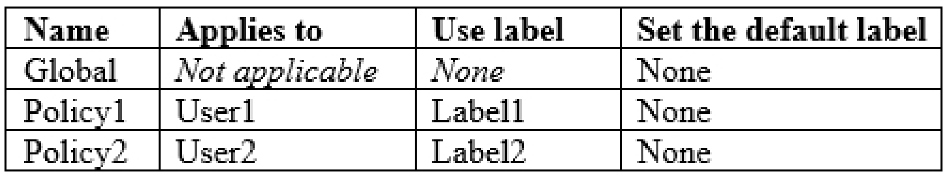
Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

You have the Azure Information Protection labels shown in the following table.



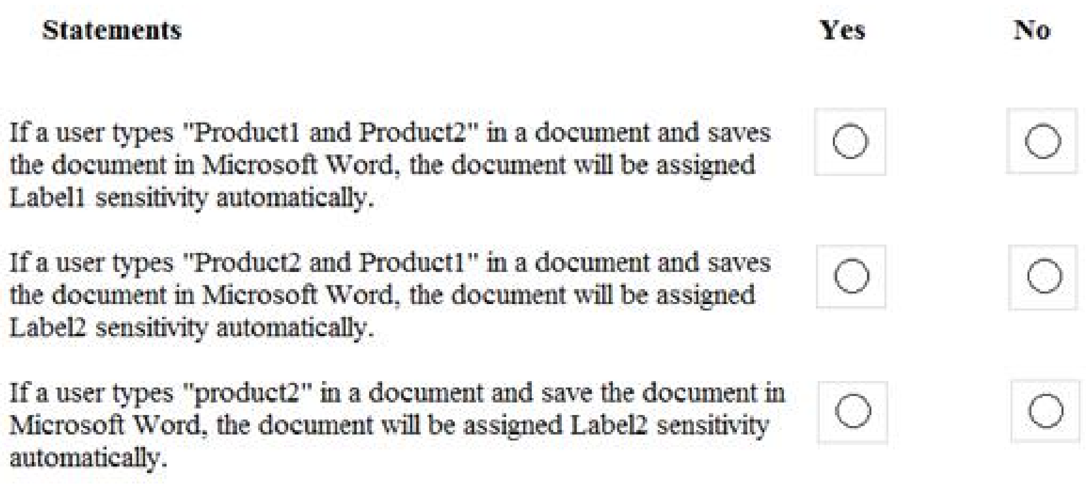
Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

You have the Azure Information Protection policies shown in the following table.



Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

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

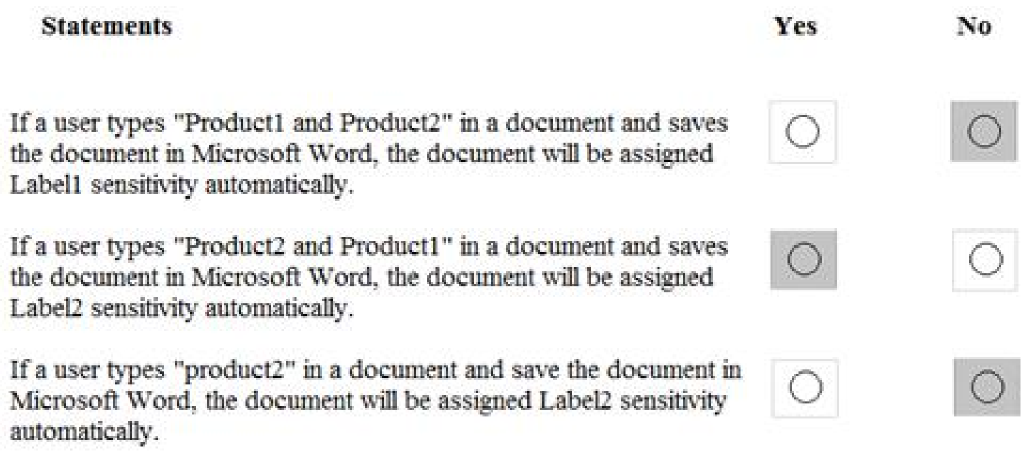


Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	○
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	○

A. Mastered
B. Not Mastered

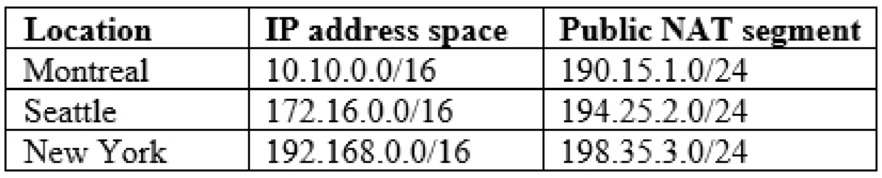
Answer: A

Explanation:



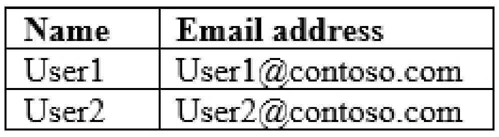
Statements	Yes	No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.	○	●
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	●	○
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	○	●

NEW QUESTION 40
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.



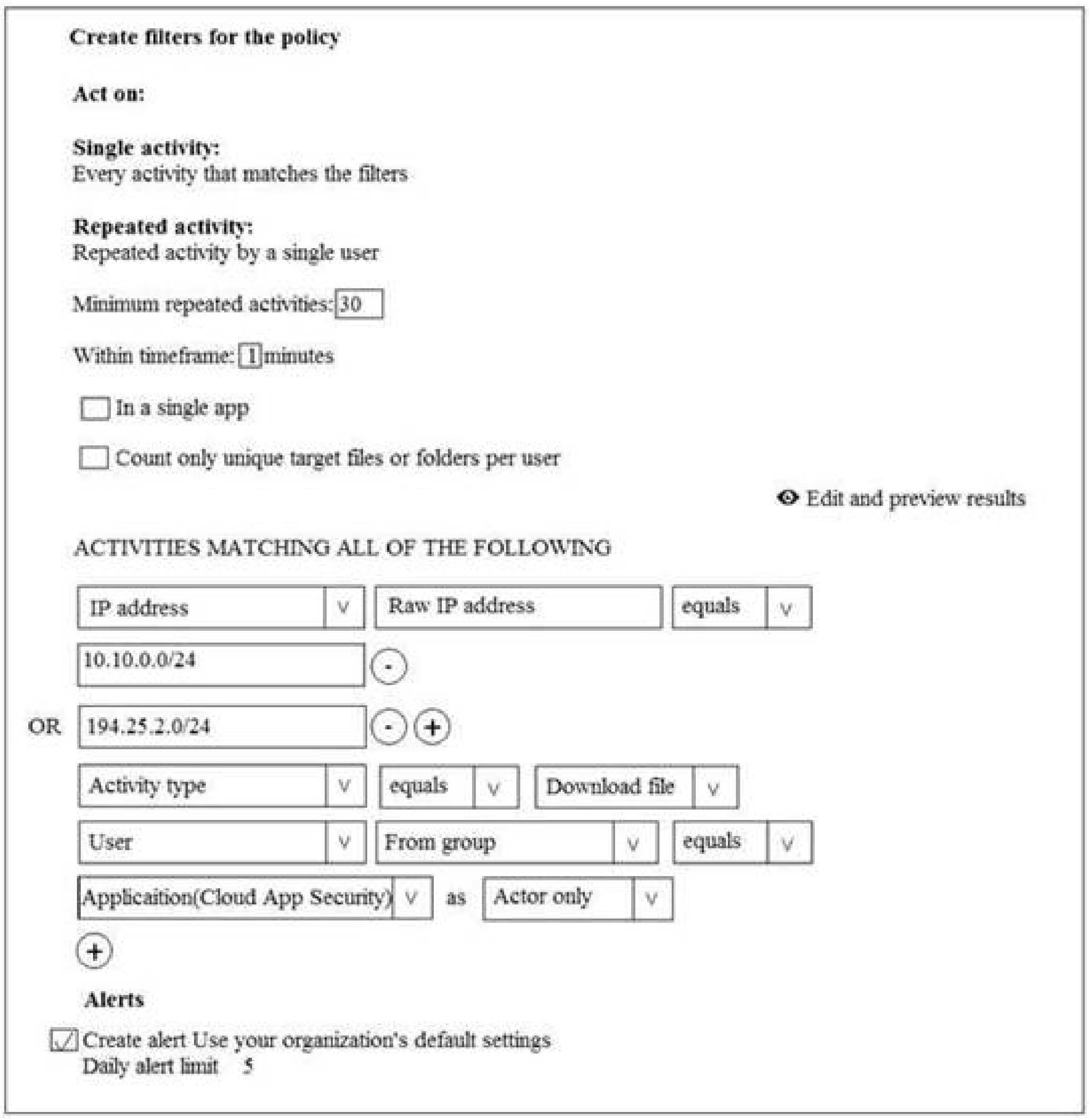
Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

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: 30

Within timeframe: 1 minutes

□ In a single app

□ Count only unique target files or folders per user

Edit and preview results

ACTIVITIES MATCHING ALL OF THE FOLLOWING

IP address | Raw IP address | equals
10.10.0.0/24
OR 194.25.2.0/24

Activity type | equals | Download file

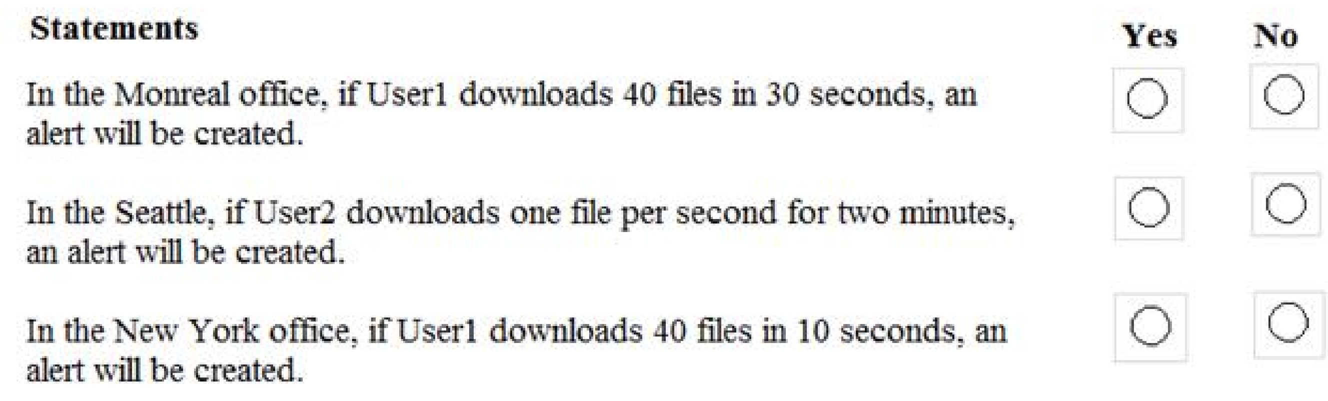
User | From group | equals

Application(Cloud App Security) as Actor only

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.

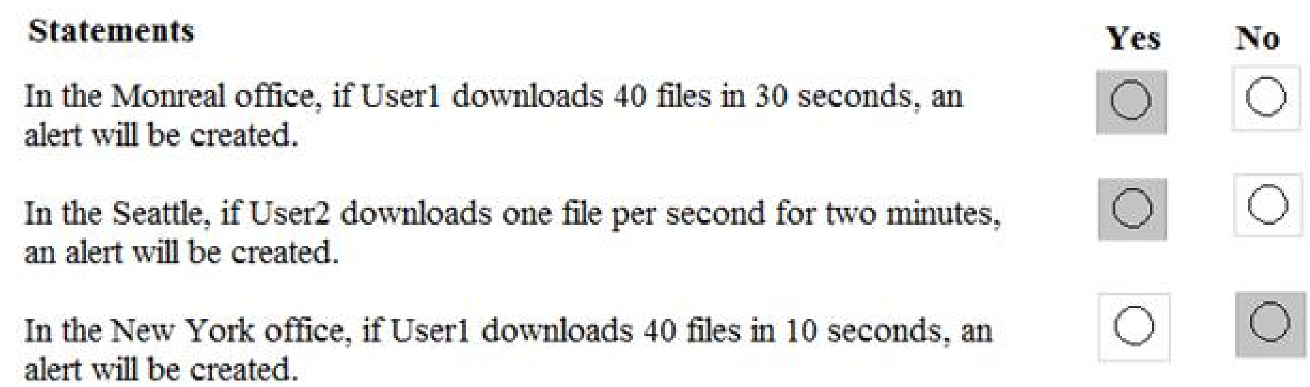


Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

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.	○	●

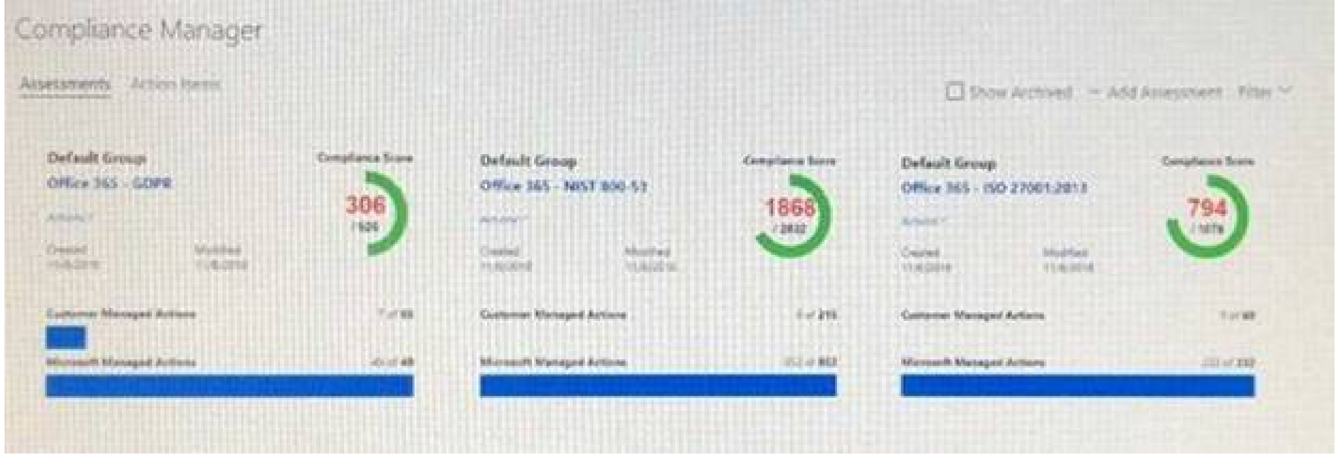
NEW QUESTION 43
You have a Microsoft 365 subscription.
You need to enable auditing for all Microsoft Exchange Online users. What should you do?

A. From the Exchange admin center, create a journal rule
B. Run the Set-MailboxDatabase cmdlet
C. Run the Set-Mailbox cmdlet
D. From the Exchange admin center, create a mail flow message trace rule.

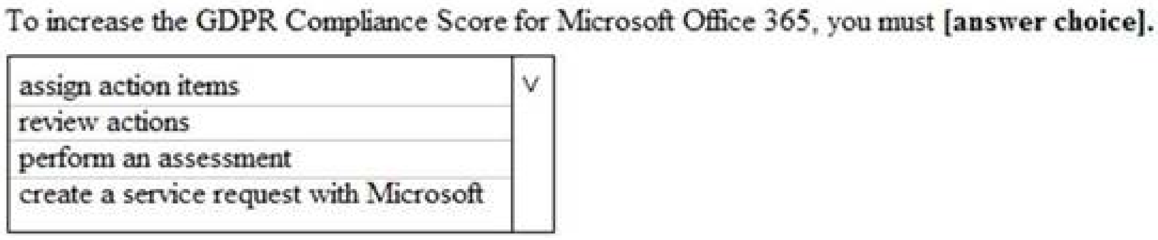
Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

NEW QUESTION 48
HOTSPOT
You view Compliance Manager as shown in the following exhibit.

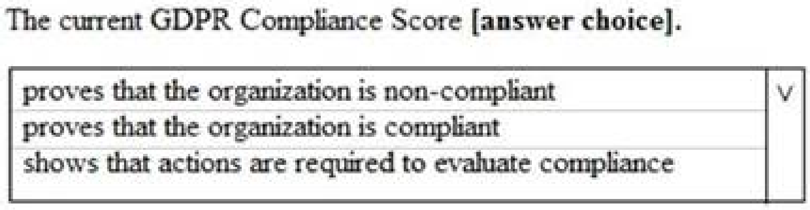


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.



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

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



The current GDPR Compliance Score **[answer choice]**.

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

A. Mastered
B. Not Mastered

Answer: A

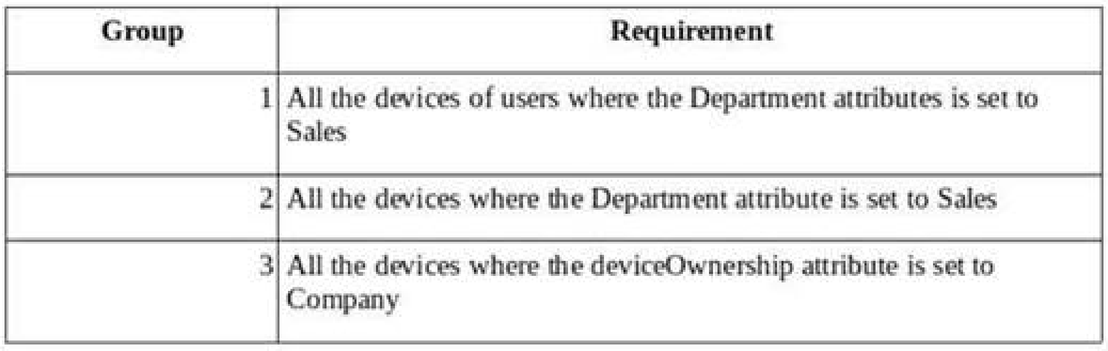
Explanation:
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/meet-data-protection-and-regulatory-reqs-using-microsoft-cloud

NEW QUESTION 50
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

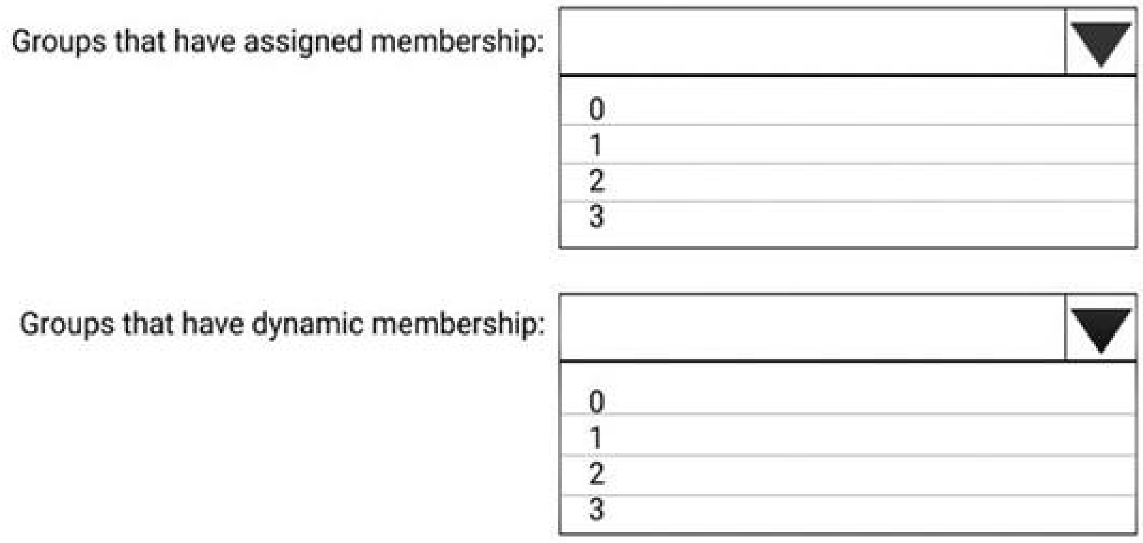
Answer: C

NEW QUESTION 54
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:

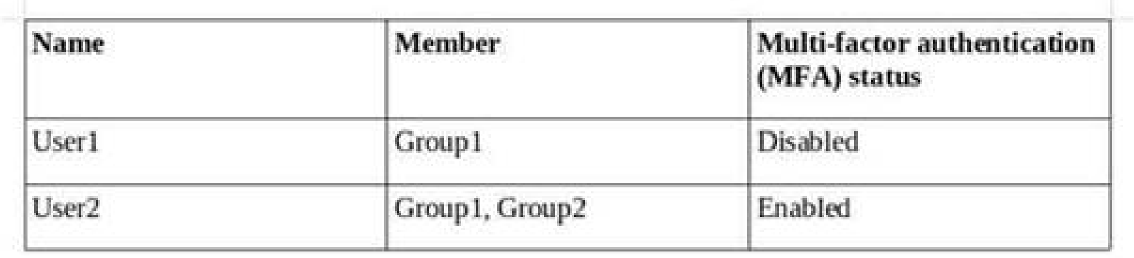
- 0
- 1
- 2
- 3

A. Mastered
B. Not Mastered

Answer: A

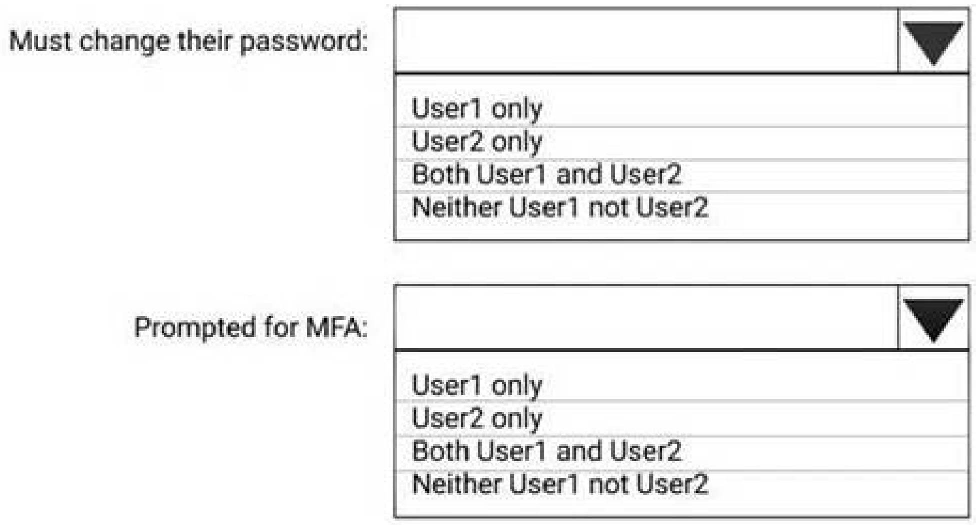
Explanation:
References:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md

NEW QUESTION 58
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

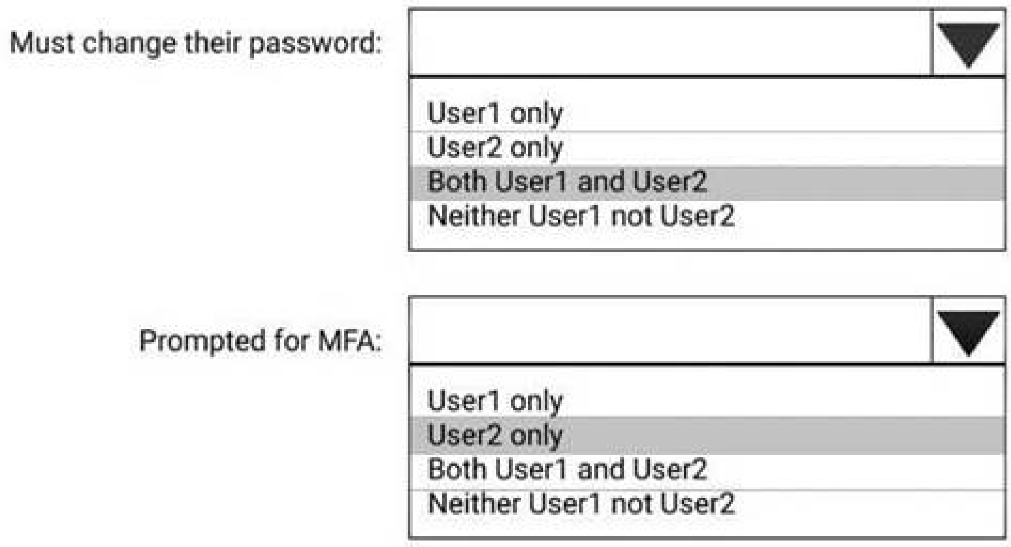
Prompted for MFA:

- 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 61
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 64
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 66
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 68
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 69
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 73
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 74
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 78
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some questions sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 subscription.
You have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1. You run the Set-MailboxFolderPermission –Identity "User1"
-User User1@contoso.com –AccessRights Owner command. Does that meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 80

……