

Exam Questions MS-500

Microsoft 365 Security Administrator

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



NEW QUESTION 1

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

Exchange Administrator - Members

+ Add member
X Remove member

✓

✗

Access reviews

↓

Export

↻

Refresh

Assignment type

All

Search

🔍

Search by members name

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

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

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

Answer: C

Explanation:

References:

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

NEW QUESTION 4

You need to recommend a solution that meets the technical and security requirements for sharing data with the partners.

What should you include in the recommendation? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Create an access review.
- B. Assign the Global administrator role to User1.
- C. Assign the Guest inviter role to User1.
- D. Modify the External collaboration settings in the Azure Active Directory admin center.

Answer: AC

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

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 7

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 Azure AD app and attribute filtering settings.

Does that 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 Source Anchor settings.

Does that meet the goal?

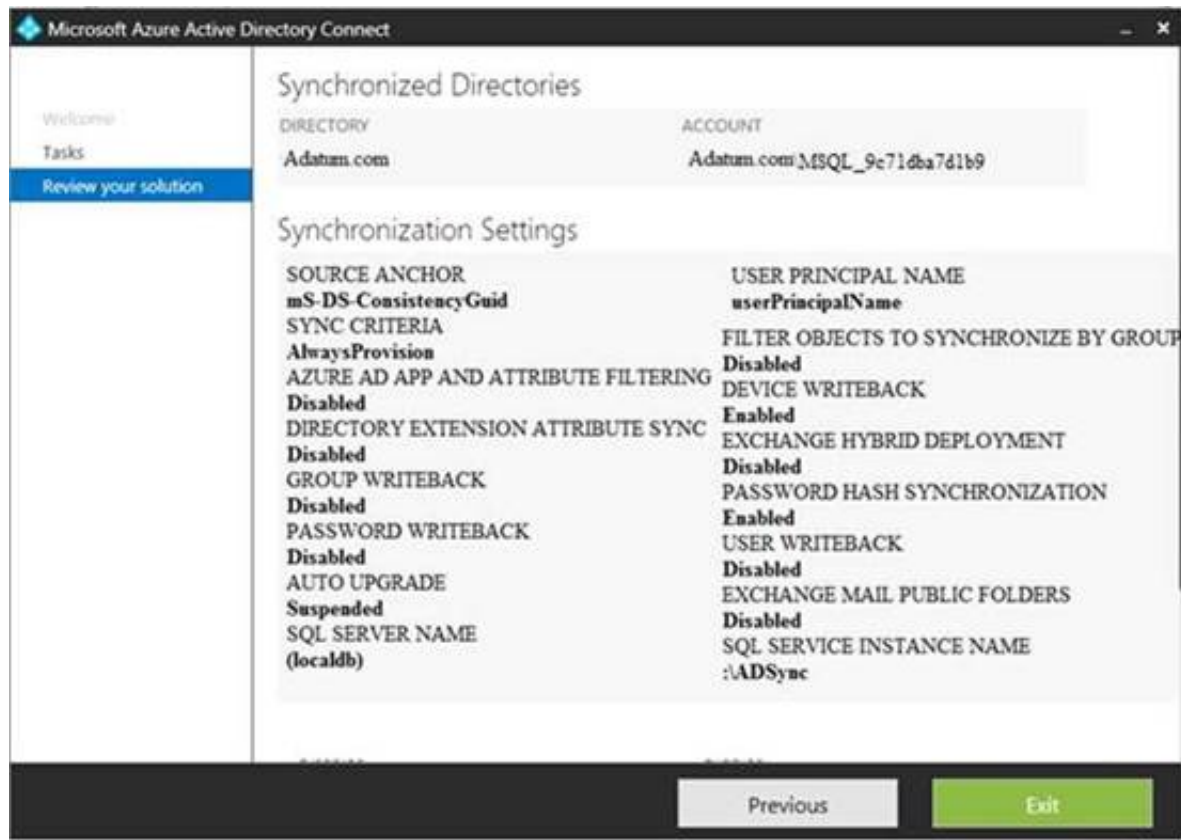
- A. Yes
- B. No

Answer: B

NEW QUESTION 9

HOTSPOT

You configure Microsoft Azure Active Directory (Azure AD) Connect as shown in the following exhibit.



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

If you reset a password in Azure AD, the password will [answer choice] .

be overwritten	V
be synced to Active Directory	
be subject to the Active Directory password policy	

If you join a computer to Azure AD,[answer choice].

an object will be provisioned in the Computers container	V
an object will be provisioned in the RegisteredDevices container	
the device object in Azure will be deleted during synchronization	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-device-writeback>

NEW QUESTION 10

You have a hybrid Microsoft 365 environment. All computers run Windows 10 and are managed by using Microsoft Intune. You need to create a Microsoft Azure Active Directory (Azure AD) conditional access policy that will allow only Windows 10 computers marked as compliant to establish a VPN connection to the on- premises network. What should you do first?

- A. From the Azure Active Directory admin center, create a new certificate
- B. Enable Application Proxy in Azure AD
- C. From Active Directory Administrative Center, create a Dynamic Access Control policy
- D. From the Azure Active Directory admin center, configure authentication methods

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn- connectivitywindows10>

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 12

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	<i>Not applicable</i>	<i>None</i>	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.	<input type="radio"/>	<input type="radio"/>
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.	<input type="radio"/>	<input type="radio"/>
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input type="radio"/>

- 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.	<input type="radio"/>	<input checked="" type="radio"/>
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.	<input checked="" type="radio"/>	<input type="radio"/>
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 17

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 18

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 22

Your company has a main office and a Microsoft 365 subscription.
 You need to enforce Microsoft Azure Multi-Factor Authentication (MFA) by using conditional access for all users who are NOT physically present in the office.
 What should you include in the configuration?

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

Answer: C

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

NEW QUESTION 23

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 25

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

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

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, Exclude Group2
- Conditions: Sign in risk of Low and above

Passing Certification Exams Made Easy

visit - <https://www.2PassEasy.com>

•Access: Allow access, Require password multi-factor authentication You need to identify how the policy affects User1 and User2.
What occurs when each user signs in from an anonymous IP address? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

User1:	<div><div></div><div>▼</div></div>
<div>Blocked</div> <div>Can sign in without MFA</div> <div>Prompted for MFA</div>	

User2:	<div><div></div><div>▼</div></div>
<div>Blocked</div> <div>Can sign in without MFA</div> <div>Prompted for MFA</div>	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1:	<div><div></div><div>▼</div></div>
<div>Blocked</div> <div>Can sign in without MFA</div> <div>Prompted for MFA</div>	

User2:	<div><div></div><div>▼</div></div>
<div>Blocked</div> <div>Can sign in without MFA</div> <div>Prompted for MFA</div>	

NEW QUESTION 26

You have a Microsoft 365 subscription that uses a default domain name of fabrikam.com. You create a safe links policy, as shown in the following exhibit.

Safe links policy for your organization

Settings that apply to content across Office 365

When users click a blocked URL, they're redirected to a web page that explains why the URL is blocked.
 Block the following URLs:

-

Enter a valid URL

+

.phishing..*

malware.*com

*.contoso.com

Settings that apply to content except email

These settings don't apply to email messages. If you want to apply them for email, create a safe links policy for email recipients.

Use safe links in:

- ☒ Office 356 ProPlus, Office for iOS and Android
☒ Office Online of above applications

For the locations selected above:

- ☒ Do not track when users click safe links:
☒ Do not let users click through safe links to original URL:

Which URL can a user safely access from Microsoft Word Online?

- A. fabrikam.phishing.fabrikam.com
 B. malware.fabrikam.com
 C. fabrikam.contoso.com
 D. www.malware.fabrikam.com

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list- wti h-atp>

NEW QUESTION 31

HOTSPOT

You have a Microsoft 365 subscription that uses a default name of litwareinc.com.

You configure the Sharing settings in Microsoft OneDrive as shown in the following exhibit.

Links

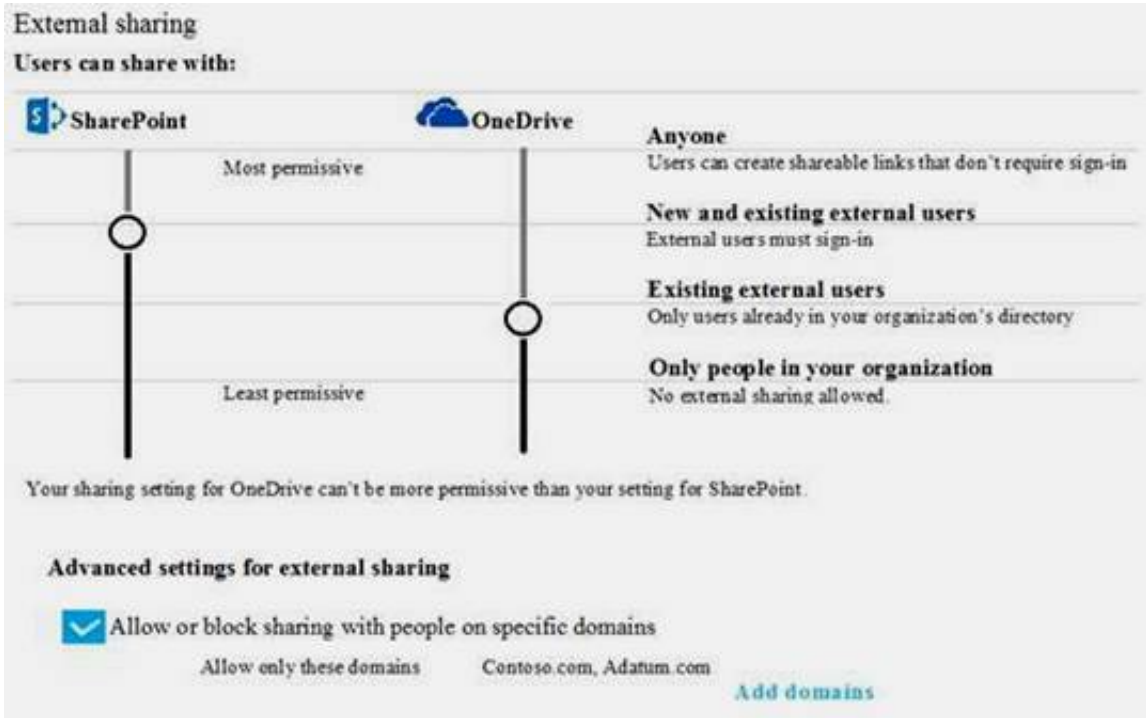
Choose the kind of link that's selected by default when users share items.

Default link type

Shareable: Anyone with the link

Internal: Only people in your organization

Direct: Specific people



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.

A user who has an email address of user1@fabrikam.com [answer choice]

cannot access OneDrive content

can access OneDrive content after a link is created

must be added to be a group before the user can access shared files

If a new guest user is created for user2@contoso.com [answer choice]

the user cannot access OneDrive content

the user can access OneDrive content after a link is created

must be added to a group before the user can access shared files

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

https://docs.microsoft.com/en-us/onedrive/manage-sharing

NEW QUESTION 32

You have a Microsoft 365 subscription that includes a user named User1.
You have a conditional access policy that applies to Microsoft Exchange Online. The conditional access policy is configured to use Conditional Access App Control.
You need to create a Microsoft Cloud App Security policy that blocks User1 from printing from Exchange Online.
Which type of Cloud App Security policy should you create?

- A. an app permission policy
- B. an activity policy
- C. a Cloud Discovery anomaly detection policy
- D. a session policy

Answer: D

NEW QUESTION 35

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

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps>

You have a Microsoft 365 subscription.

You need to be notified by email whenever an administrator starts an eDiscovery search. What should you do from the Security & Compliance admin center?

- A. From Search & investigation, create a guided search.
- B. From Events, create an event.
- C. From Alerts, create an alert policy.
- D. From Search & Investigation, create an eDiscovery case.

Answer: C

References:

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

You have a Microsoft 365 subscription.

A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.

You need to limit alert notifications to actionable DLP events.

What should you do?

- A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
- B. From the Cloud App Security admin center, apply a filter to the alerts.
- C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
- D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.

Answer: D

References:

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

HOTSPOT

You have a Microsoft 365 subscription. Auditing is enabled.

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

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

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

NOTE: Each correct selection is worth one point.

Search

Clear

Results

Activities

Show results for all activities

x Clear all to show results for all activities

Search

Date ▼	IP address	User	Activity	Item
User administration activities				
<div>Added user</div>	<div>Deleted user</div>	<div>Set license properties</div>		
<div>Reset user password</div>	<div>Changed user password</div>	<div>Changed user license</div>		
<div>Updated user</div>	<div>Set property that forces user to change password</div>			
Azure AD group administration activities				
<div>Added group</div>	<div>Updated group</div>	<div>Deleted group</div>		
<div>Added member to group</div>	<div>Removed member from group</div>			
Application administration activities				
<div>Added service principal</div>	<div>Removed a service principal from the directory</div>	<div>Set delegation entry</div>		
<div>Removed credentials from a service principal</div>	<div>Added delegation entity</div>	<div>Added credentials to a service principal</div>		

- A. Mastered
B. Not Mastered

Answer: A

References:

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

NEW QUESTION 50

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 53

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 54

HOTSPOT

You have a Microsoft 365 subscription.

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

The screenshot shows the 'Review your settings' page for a retention label named 'Label1'. On the left, there are three steps: 'Name your label' (completed), 'Label settings' (completed), and 'Review your settings' (active). The main area displays the following settings:

- Name:** Label1 (with an 'Edit' link)
- Descriptions for admins:** (with an 'Edit' link)
- Description for users:** (with an 'Edit' link)
- Retention:**
 - 2 years
 - Retain and Delete
 - Based on when it was created
 - Use Label to classify content as a "Record"

At the bottom, there are three buttons: 'Back', 'Create this label', and 'Cancel'.

You publish Label1 to SharePoint sites.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

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

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

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 58

HOTSPOT

You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:

- Rule1:
- Conditions: Label 1, Detect content that's shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 0
- Rule2:
- Conditions: Label 1 or Label2
- Actions: Restrict access to the content
- Priority: 1
- Rule3:
- Conditions: Label2, Detect content that's shared with people outside my organization
- Actions: Restrict access to the content for external users
- User notifications: Notify the user who last modified the content
- User overrides: On
- Priority: 2

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

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

Statements	Yes	No
External users can access File1.	<input type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input type="radio"/>	<input type="radio"/>
External users can access File3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
External users can access File1.	<input checked="" type="radio"/>	<input type="radio"/>
The users in contoso.com can access File2.	<input checked="" type="radio"/>	<input type="radio"/>
External users can access File3.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 60

DRAG DROP

You have a Microsoft 365 E5 subscription.

All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

You create a Windows Defender machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-HsolRoleMember cmdlet.

Answer Area

>

<

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Actions

From Windows Defender Security Center, create a role.

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Azure portal, create an RBAC role.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From Azure Cloud Shell, run the Add-HsolRoleMember cmdlet.

Answer Area

From Windows Defender Security Center, configure the permissions for MachineGroup1.

From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) group.

From the Azure portal, create an RBAC role.

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 an on-premises Active Directory domain named contoso.com. You install and run Azure AD Connect on a server named Server1 that runs Windows Server. You need to view Azure AD Connect events. You use the Security event log on Server1. Does that meet the goal?

- A. Yes
B. No

Answer: B

Explanation:

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

NEW QUESTION 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 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 67

.....

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