



Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator

NEW QUESTION 1

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 2

HOTSPOT

You install Azure ATP sensors on domain controllers.

You add a member to the Domain Admins group. You view the timeline in Azure ATP and discover that information regarding the membership change is missing.

You need to meet the security requirements for Azure ATP reporting.

What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Policy to edit:

	▼
Default Domain Controllers Policy	
Default Domain Policy	
A local policy on one domain controller	

Audit setting to configure:

	▼
Audit User Account Management	
Audit Computer Account Management	
Audit Other Account Management Events	
Audit Security Group Management	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-advanced-audit-policy>

NEW QUESTION 3

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 4

You need to resolve the issue that targets the automated email messages to the IT team. Which tool should you run first?

- A. Synchronization Service Manager
- B. Azure AD Connect wizard
- C. Synchronization Rules Editor
- D. IdFix

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization>

Case Study: 2 Litware, Inc Overview

Litware, Inc. is a financial company that has 1,000 users in its main office in Chicago and 100 users in a branch office in San Francisco.

Existing Environment

Internal Network Infrastructure

The network contains a single domain forest. The forest functional level is Windows Server 2016. Users are subject to sign-in hour restrictions as defined in Active Directory.

The network has the IP address range shown in the following table.

Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

The offices connect by using Multiprotocol Label Switching (MPLS).

The following operating systems are used on the network:

- Windows Server 2016
- Windows 10 Enterprise
- Windows 8.1 Enterprise

The internal network contains the systems shown in the following table.

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litware uses a third-party email system.

Cloud Infrastructure

Litware recently purchased Microsoft 365 subscription licenses for all users.

Microsoft Azure Active Directory (Azure AD) Connect is installed and uses the default authentication settings. User accounts are not yet synced to Azure AD.

You have the Microsoft 365 users and groups shown in the following table.

Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

Planned Changes

Litware plans to implement the following changes: Migrate the email system to Microsoft Exchange Online Implement Azure AD Privileged Identity Management

Security Requirements

Litware identifies the following security requirements:

- Create a group named Group2 that will include all the Azure AD user accounts. Group2 will be used to provide limited access to Windows Analytics
- Create a group named Group3 that will be used to apply Azure Information Protection policies to pilot users. Group3 must only contain user accounts
- Use Azure Advanced Threat Protection (ATP) to detect any security threats that target the forest
- Prevent users locked out of Active Directory from signing in to Azure AD and Active Directory
- Implement a permanent eligible assignment of the Compliance administrator role for User1
- Integrate Windows Defender and Windows Defender ATP on domain-joined servers
- Prevent access to Azure resources for the guest user accounts by default
- Ensure that all domain-joined computers are registered to Azure AD

Multi-factor authentication (MFA) Requirements

Security features of Microsoft Office 365 and Azure will be tested by using pilot Azure user accounts. You identify the following requirements for testing MFA.

Pilot users must use MFA unless they are signing in from the internal network of the Chicago office. MFA must NOT be used on the Chicago office internal network.

If an authentication attempt is suspicious, MFA must be used, regardless of the user location Any disruption of legitimate authentication attempts must be minimized

General Requirements

Litware wants to minimize the deployment of additional servers and services in the Active Directory forest.

NEW QUESTION 5

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 6

Which IP address space should you include in the MFA configuration?

- A. 131.107.83.0/28
- B. 192.168.16.0/20
- C. 172.16.0.0/24
- D. 192.168.0.0/20

Answer: B

NEW QUESTION 7

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 8

HOTSPOT

You are evaluating which finance department users will be prompted for Azure MFA credentials. 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
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
A finance department user who has an IP address from the Montreal office will be prompted for Azure MFA credentials.	<input type="radio"/>	<input checked="" type="radio"/>
A finance department user who works from home and who has an IP address of 193.77.140.140 will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>
A finance department user who has an IP address from the New York office will be prompted for Azure MFA credentials.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 9

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 10

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 10

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 12

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 16

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. (Click 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	V
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	V
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	V
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	V
Must use app passwords for legacy apps	
Must use an app password to sign in to the My-Apps portal	

NEW QUESTION 17

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 22

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 25

You have a Microsoft 365 subscription. You need to ensure that all users who are assigned the Exchange administrator role have multi-factor authentication (MFA) enabled by default. What should you use to achieve the goal?

- A. Security & Compliance permissions
- B. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- C. Microsoft Azure AD group management
- D. Microsoft Office 365 user management

Answer: B

NEW QUESTION 28

You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization. Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online. You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members. The email address that you intend to spoof belongs to the Executive group members. What should you do first?

- A. From Azure ATP admin center, configure the primary workspace settings
- B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
- C. Enable MFA for the Research group members
- D. Migrate the Executive group members to Exchange Online

Answer: C

Explanation:

Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator>

NEW QUESTION 31

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.

<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>
<input type="radio"/>	<input type="radio"/>

- 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.

<input type="radio"/>	<input checked="" type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>
<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 32

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 36

DRAG DROP

You have a Microsoft 365 subscription. All users use Microsoft Exchange Online. Microsoft 365 is configured to use the default policy settings without any custom rules. You manage message hygiene.
Where are suspicious email messages placed by default? To answer, drag the appropriate location to the correct message types. Each location may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Locations

ATP quarantine

The Junk Email folder of a user's mailbox

The Clutter folder a user's mailbox

Answer Area

Messages that contain word-filtered content:

Location

Messages that are classified as phishing:

Location

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Messages that contain word-filtered content:

The Junk Email folder of a user's mailbox

Messages that are classified as phishing:

The Junk Email folder of a user's mailbox

NEW QUESTION 38

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 41

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 46

HOTSPOT
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the groups shown in the following table.

Name	Type	Email address
Group1	Security Group – Domain Local	<u>Group1@contoso.com</u>
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	<u>Group4@contoso.com</u>

The domain is synced to a Microsoft Azure Active Directory (Azure AD) tenant that contains the groups shown in the following table.

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

You create an Azure Information Protection policy named Policy1. You need to apply Policy1.
To which groups can you apply Policy1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

On-premises Active Directory groups:

Group4 only	V
Group1 and Group4 only	
Group3 and Group4 only	
Group1, Group3, and Group4 only	
Group1, Group2, Group3, and Group4	

Azure AD groups:

Group13 only	V
Group13 and Group14 only	
Group11 and Group12 only	
Group11, Group13, and Group14 only	
Group11, Group12,Group13,and Group14 only	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/information-protection/prepare>

NEW QUESTION 49

HOTSPOT

You have a Microsoft 365 subscription.

You identify the following data loss prevention (DLP) requirements:

- Send notifications to users if they attempt to send attachments that contain EU social security numbers
- Prevent any email messages that contain credit card numbers from being sent outside your organization
- Block the external sharing of Microsoft OneDrive content that contains EU passport numbers
- Send administrators email alerts if any rule matches occur.

What is the minimum number of DLP policies and rules you must create to meet the requirements? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policies:

1	V
2	
3	

Rules:

1	V
2	
3	
4	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Policies:

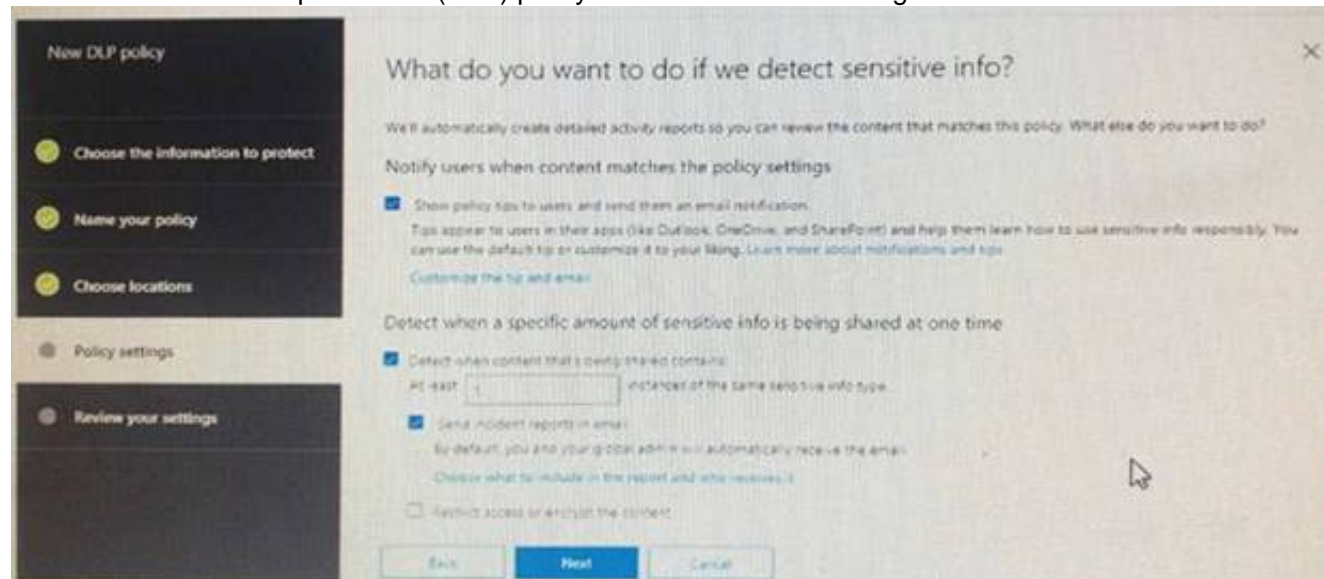
1	V
2	
3	

Rules:

1	V
2	
3	
4	

NEW QUESTION 54

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 58

HOTSPOT

You have a Microsoft 365 subscription.

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

Decide if you want to retain content, delete it, or both

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 2 years

Retain the content based on when it was last modified

Do you want us to delete it after this time?

☒ Yes ☐ No

☐ No, just delete content that's older than

1 years

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

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

NEW QUESTION 59

You have a Microsoft 365 subscription. You need to ensure that users can apply retention labels to individual documents in their Microsoft SharePoint libraries. Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the Cloud App Security admin center, create a file policy.
- B. From the SharePoint admin center, modify the Site Settings.
- C. From the SharePoint & Compliance admin center, create a label.
- D. From the SharePoint admin center, modify the records management settings.
- E. From the Security & Compliance admin center, publish a label.

Answer: CE

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/protect-sharepoint-online-files-with-office-365-labels-and-dlp>

NEW QUESTION 62

You have a Microsoft 365 subscription.

The Global administrator role is assigned to your user account. You have a user named Admin1. You create an eDiscovery case named Case1.

You need to ensure that Admin1 can view the results of Case1. What should you do first?

- A. From the Azure Active Directory admin center, assign a role group to Admin1.
- B. From the Microsoft 365 admin center, assign a role to Admin1.
- C. From Security & Compliance admin center, assign a role group to Admin1.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION 67

You create a label that encrypts email data. Users report that they cannot use the label in Outlook on the web to protect the email messages they send.

You need to ensure that the users can use the new label to protect their email. What should you do?

- A. Modify the priority order of label policies
- B. Wait six hours and ask the users to try again
- C. Create a label policy
- D. Create a new sensitive information type

Answer: B

NEW QUESTION 69

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 74

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 auditing in the Office 365 Security & Compliance center.
- B. Turn off Delayed updates for the Azure ATP sensors.
- C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
- D. Integrate SIEM and Azure ATP.

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

NEW QUESTION 76

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 80

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-Mailbox -Identity "User1" -AuditEnabled \$true command. Does that meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

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

NEW QUESTION 81

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 85

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

Explanation:

References:

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

NEW QUESTION 86

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

× Clear all to show results for all activities

Search

User administration activities

Added user

Deleted user

Set license properties

Reset user password

Changed user password

Changed user license

Updated user

Set property that forces user to change password

Azure AD group administration activities

Added group

Updated group

Deleted group

Added member to group

Removed member from group

Application administration activities

Added service principal

Removed a service principal from the directory

Set delegation entry

Removed credentials from a service principal

Added delegation entity

Added credentials to a service principal

- 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 87

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 88

HOTSPOT

You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

You create an alert policy named Policy1 as shown in the following exhibit.

Policy1

Edit policy

Delete policy

Status	<input checked="" type="checkbox"/> On	
Description	Policy1 description	
Severity	<input checked="" type="radio"/> Low	Edit
Category	Threat management	

Conditions	Activity is Copied file and File name is Like any of File1.docx	
Aggregation	Aggregated	
Threshold	10 activities	Edit
Window	60 minutes	
Scope	All users	

Email recipients	prvi@sk180920.onmicrosoft.com	
Daily notifications limit	Do not send email notifications	Edit

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 User1 runs a scheduled task that copies File1.docx to a local folder every five minutes.
 [answer choice].

Policy1 will not be triggered
 Policy1 will be triggered after 45 minutes
 Policy1 will be triggered after 60 minutes

If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes.
 [answer choice].

Policy1 will not be triggered
 Policy1 will be triggered within 20 minutes
 Policy1 will be triggered within 45 minutes
 Policy1 will be triggered after 60 minutes

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 90

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:

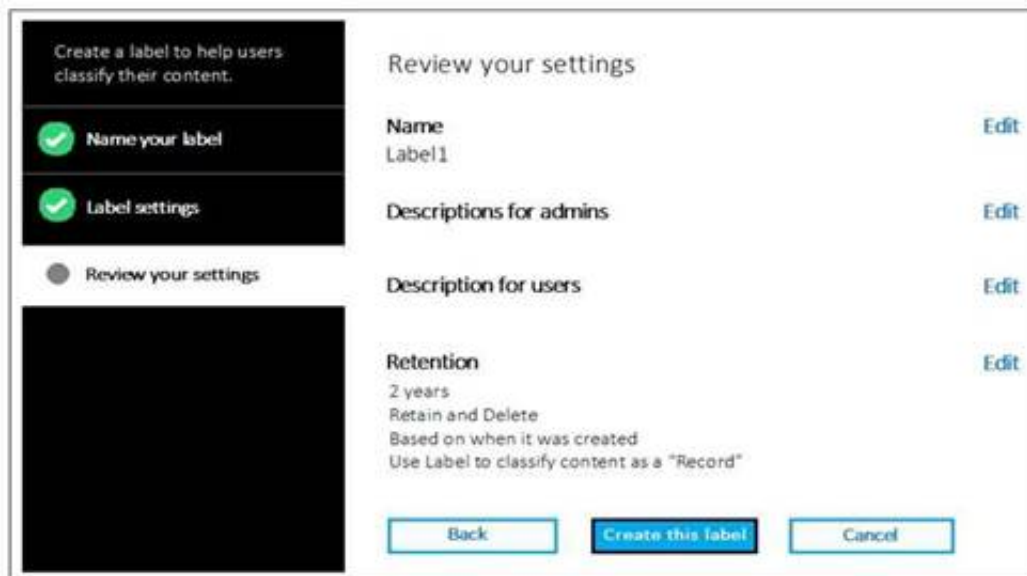
<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance>

NEW QUESTION 95

HOTSPOT

You have a Microsoft 365 subscription.

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



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 100

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-TeamMessagingSettings
- D. Get-TeamChannel

Answer: A

NEW QUESTION 102

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 104

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 108

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 Directory Service 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 111

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 116

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 121

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

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

100% Actual & Verified — Instant Download, Please Click
[Order The MS-500 Practice Test Here](#)