

Microsoft

Exam Questions MS-500

Microsoft 365 Security Administrator



NEW QUESTION 1

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 2

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

NEW QUESTION 3

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 4

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 5

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	v
User1 and User2 only	
User2 and User4 only	
User3 and User4 only	
User1, User2, User3, and User4	

ADGroup2:

None	v
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 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 Source Anchor settings.
 Does that meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 8

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)

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	

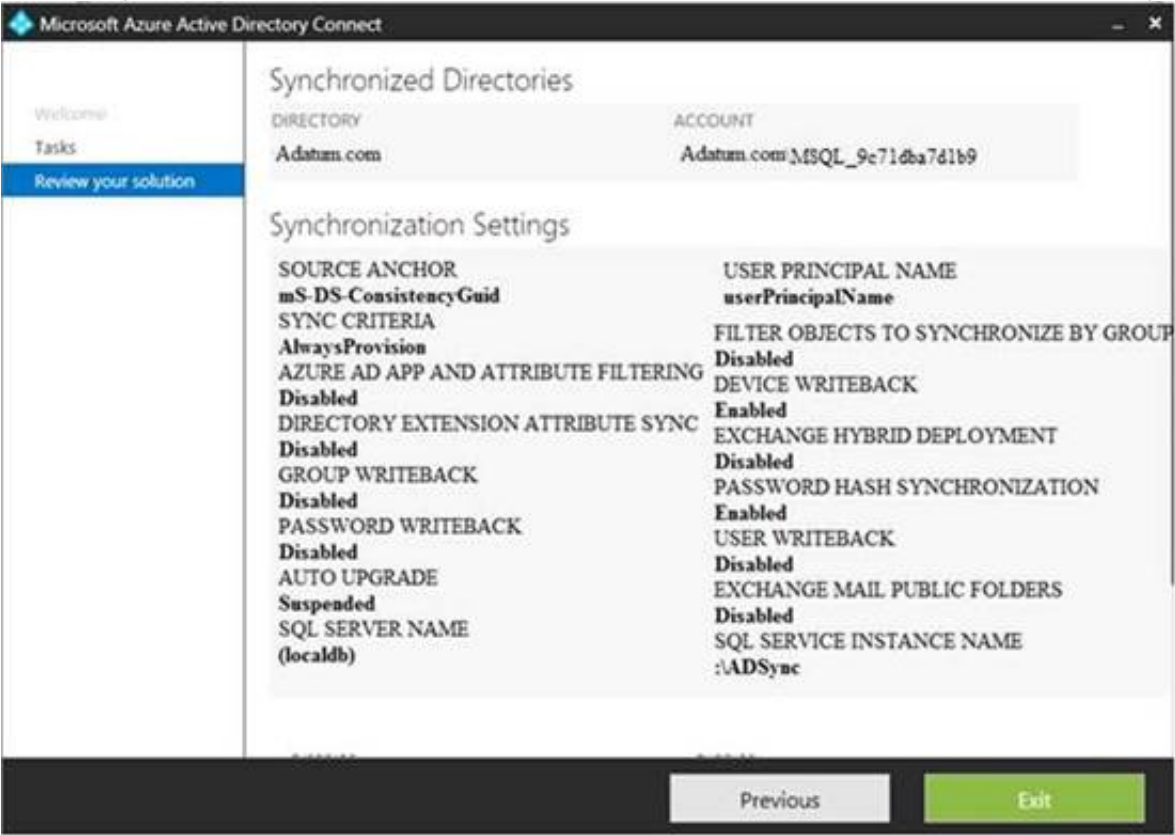
User2:

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 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

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 13

Your company has a Microsoft 365 subscription.

The company forbids users to enroll personal devices in mobile device management (MDM). Users in the sales department have personal iOS devices.

You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant.

The users must be prevented from backing up the app's data to iCloud. What should you create?

- A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
- B. an app protection policy in Microsoft Intune
- C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
- D. a device compliance policy in Microsoft Intune

Answer: B

NEW QUESTION 15

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 16

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 17

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed. You have a Microsoft Azure subscription.

You are deploying Azure Advanced Threat Protection (ATP)

You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.

You need to integrate the VPN and Azure ATP.

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

On VPN1:

Configure an authentication provider.	v
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	v
1723	
1813	
8080	
8531	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn>

NEW QUESTION 18

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 22

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 24

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 encryption settings of the label.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 25

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 28

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 29

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 Jauary 1,2021	
deleted on July 1,2021	

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until Jauary 1,2020	
can recover the file until March 1,2020	
can recover the file until May 1,2020	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

If a user creates a file in a Microsoft SharePoint library on January 1,2019, and modifies the file every six months, the file will be [answer choice].

retained	▼
deleted on Jauary 1,2021	
deleted on July 1,2021	

If a user creates a file in Microsoft OneDrive on January 1,2019, modifies the file on March 1, 2019, and deletes the file on May 1, 2019, the user [answer choice].

cannot recover the file	▼
can recover the file until Jauary 1,2020	
can recover the file until March 1,2020	
can recover the file until May 1,2020	

NEW QUESTION 34

DRAG DROP

You have a Microsoft 365 subscription.
A customer requests that you provide her with all documents that reference her by name. You need to provide the customer with a copy of the content.
Which four 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
Close the case.	
Regenerate a report.	
View the results.	
Export the results.	
Create a Data Subject Request (DSR) case.	
Save the search.	
Download the results.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365>

NEW QUESTION 36

HOTSPOT

You have a Microsoft 365 subscription. From the Security & Compliance admin center, you create the retention policies shown in the following table.

Name	Location
Policy1	OneDrive accounts
Polciy2	Exchange email, SharePoint sites, OneDrive accounts, Office 365 groups

Policy1 if configured as showing 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... 1 years

☐ No, just delete content that's older than

1 years

Delete the content based on when it was created

Need more options?

☐ Use advanced retention settings

Back

Next

Cancel

Policy2 is configured as shown in the following exhibit.

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

Do you want to retain content?

☒ Yes, I want to retain it

For this long... 3 years

Retain the content based on when it was created

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

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

Answer Area

- If a user creates a file in Microsoft OneDrive on January 1, 2018, users can access the file on January 15, 2019
- If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2019
- If a user deletes a Microsoft OneDrive file created on January 1, 2018, an administrator can recover the file on April 15, 2022

Yes	No
<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:

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies?redirectSourcePath=%252fen-us%252farticle%252fOverview-of-retention-policies-5e377752-700d-4870-9b6d-12bfc12d2423#the-principles-of-retention-or-what-takes-precedence>

NEW QUESTION 37

You have a Microsoft 365 subscription.
All computers run Windows 10 Enterprise and are managed by using Microsoft Intune. You plan to view only security-related Windows telemetry data.
You need to ensure that only Windows security data is sent to Microsoft. What should you create from the Intune admin center?

- A. a device configuration profile that has device restrictions configured
- B. a device configuration profile that has the Endpoint Protection settings configured
- C. a device configuration policy that has the System Security settings configured
- D. a device compliance policy that has the Device Health settings configured

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry>

NEW QUESTION 42

You have a Microsoft 365 subscription that includes a user named Admin1.
You need to ensure that Admin1 can preserve all the mailbox content of users, including their deleted items.
The solution must use the principle of least privilege. What should you do?

- A. From the Microsoft 365 admin center, assign the Exchange administrator role to Admin1.
- B. From the Exchange admin center, assign the Discovery Management admin role to Admin1.
- C. From the Azure Active Directory admin center, assign the Service administrator role to Admin1.
- D. From the Exchange admin center, assign the Recipient Management admin role to Admin1.

Answer: B

NEW QUESTION 47

DRAG DROP

You have a Microsoft 365 subscription.
You have a site collection named SiteCollection1 that contains a site named Site2. Site2 contains a document library named Customers.
Customers contains a document named Litware.docx. You need to remove Litware.docx permanently.
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
From PowerShell, run Remove-SPOUserProfile	
Delete Litware.docx from the Recycle Bin of Site2.	
From PowerShell, run Set-SPOSite.	
Delete Litware.docx from the Recycle Bin of SiteCollection1.	
From Powershell, run Remove-SPOUserInfo	
Delete Litware.docx from Customers.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Delete Litware.docx from Customers.
Delete Litware.docx from the Recycle Bin of Site2.
Delete Litware.docx from the Recycle Bin of SiteCollection1.

NEW QUESTION 50

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 52

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:

 -

+

.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 55

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

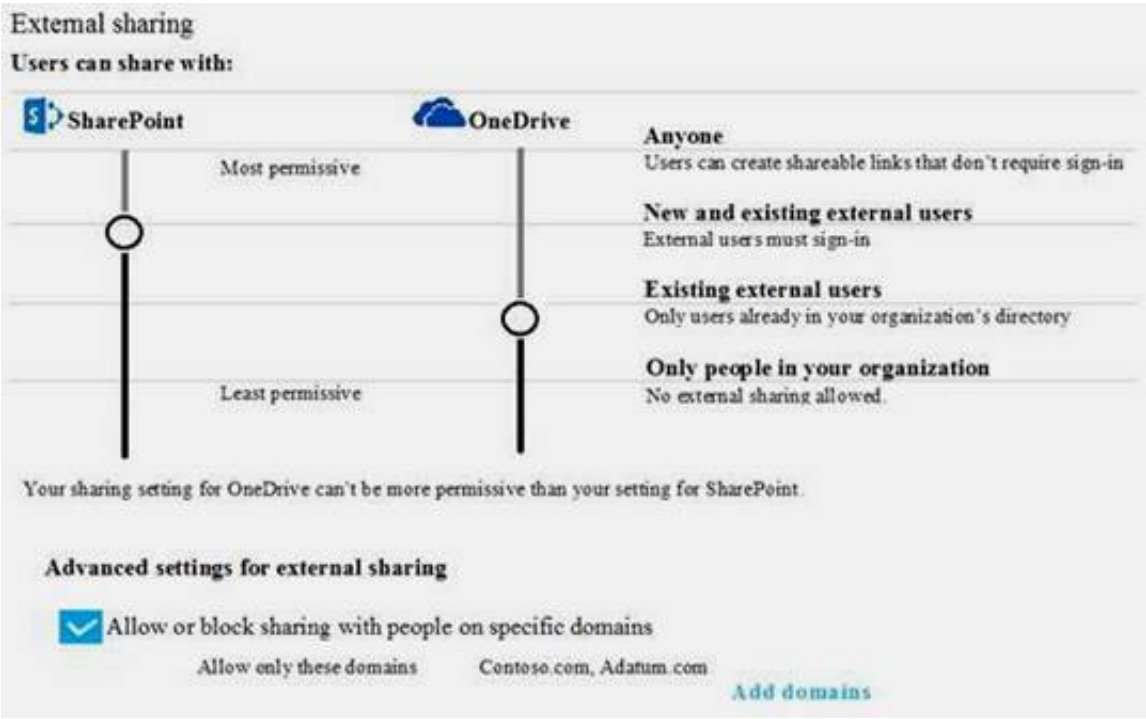
Choose the kind of link that's selected by default when users share items.

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 58

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 61

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	<div><div></div>On</div>	
Description	Policy1 description	
Severity	<div><div></div>Low</div>	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 64
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 66
You have a Microsoft 365 subscription.
You have a team named Team1 in Microsoft Teams. You plan to place all the content in Team1 on hold.
You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.
Which cmdlet should you use?

- A. Get-UnifiedGroup
- B. Get-MailUser

- C. Get-TeanMessagingSettings
- D. Get-TeamChannel

Answer: A

NEW QUESTION 67

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 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 72

You have a Microsoft 365 subscription.

You create an Advanced Threat Protection (ATP) safe attachments policy.

You need to configure the retention duration for the attachments in quarantine. Which type of threat management policy should you create?

- A. Anti-malware
- B. DKIM
- C. Anti-spam
- D. ATP anti-phishing

Answer: A

NEW QUESTION 73

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 75

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

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 79

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 84

.....

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](#)