



Microsoft

Exam Questions MS-101

Microsoft 365 Mobility and Security (beta)

NEW QUESTION 1

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

A. Yes

B. No

Answer: B

NEW QUESTION 2

HOTSPOT

You have a Microsoft 365 subscription.

You are configuring permissions for Security & Compliance.

You need to ensure that the users can perform the tasks shown in the following table.

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

The solution must use the principle of least privilege.

To which role should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

Records Management

Security Administrator

Security Reader

Supervisory Review

User2:

Compliance Administrator

Organization Management

Security Administrator

Security Reader

Supervisory Review

A. Mastered

B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles>

"<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles>"o-assigned-roles

NEW QUESTION 3

HOTSPOT

You have a Microsoft 365 subscription.

You need to implement Windows Defender Advanced Threat Protection (ATP) for all the supported devices enrolled in mobile device management (MDM).

What should you include in the device configuration profile? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Platform:

Android

iOS

Windows 10 and later

Windows 8.1 and later

Settings:

Offboard package

Onboard package

Windows Defender Application Guard

Windows Defender Firewall

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

NEW QUESTION 4

DRAG DROP

You create a Microsoft 365 subscription.
You need to create a deployment plan for Microsoft Azure Advanced Threat Protection (ATP).
Which five 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
Download the Azure ATP sensor setup package.	
Create a Security & Compliance threat management policy.	
Create an Azure Active Directory (Azure AD) conditional access policy.	
Install sensors.	
Create a workspace.	
Enter credentials.	
Configure the sensor settings.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/>

NEW QUESTION 5

Your company has a Microsoft 365 E5 subscription.
Users in the research department work with sensitive data.
You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.
Users in other departments must not be restricted.
What should you do from the Security & Compliance admin center?

- A. Create a data loss prevention (DLP) policy that has a Content is shared condition.
- B. Modify the default safe links policy.
- C. Create a data loss prevention (DLP) policy that has a Content contains condition.
- D. Create a new safe links policy.

Answer: D

Explanation:

References:
<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-atp-safe-links-policies#policies-that-apply-to-specific-email-recipients>

NEW QUESTION 6

DRAG DROP

You have a Microsoft 365 subscription.
You have the devices shown in the following table.

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

You need to onboard the devices to Windows Defender Advanced Threat Protection (ATP). The solution must avoid installing software on the devices whenever possible.
Which onboarding method should you use for each operating system? To answer, drag the appropriate methods to the correct operating systems. Each method 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.
NOTE: Each correct selection is worth one point.

Methods	Answer Area	
A Microsoft Azure ATP sensor	Windows 8.1:	<input type="text"/>
A local script	Windows 10:	<input type="text"/>
Microsoft Monitoring Agent	Windows Server 2016:	<input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

hHYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection"tps://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-HYPERLINK "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection"windows-defender-advanced-threat-protection

NEW QUESTION 7

HOTSPOT

You have the Microsoft Azure Active Director (Azure AD) users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings:

- The Assignments settings are configured as follows:
- Users and groups: Group1
- Cloud apps: Microsoft Office 365 Exchange Online
- Conditions: Include All device state, exclude Device marked as compliant
- Access controls is set to Block access.

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

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 8

HOTSPOT

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

The device type restrictions in Intune are configured as shown in the following table.

Priority	Member of	Allowed platform	Assigned to
1	Policy1	Android, iOS, Windows (MDM)	None
2	Policy2	Windows (MDM)	Group2
3	Policy3	Android, iOS	Group1
Default	All users	Android, Windows (MDM)	All users

You add User3 as a device enrollment manager in Intune.

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

Statements	Yes	No
User1 can enroll Windows devices in Intune.	<input type="radio"/>	<input type="radio"/>
User2 can enroll Android devices in Intune.	<input type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Windows devices in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll Android devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can enroll iOS devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 9

The users at your company use Dropbox to store documents. The users access Dropbox by using the MyApps portal.

You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identify. The documents must be protected if the data is downloaded to an untrusted device.

What should you do?

- A. From the Intune admin center, configure the Conditional access settings.
- B. From the Azure Active Directory admin center, configure the Organizational relationships settings
- C. From the Azure Active Directory admin center, configure the Application proxy settings.
- D. From the Azure Active Directory admin center, configure the Devices settings.

Answer: B

NEW QUESTION 10

HOTSPOT

You have several devices enrolled in Microsoft Intune.

You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Role	Member of
User1	Cloud device administrator	Group1
User2	Intune administrator	Group2
User3	None	None

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group2
2	Policy2	10	Group1
Default	All users	5	All users

You add User3 as a device enrollment manager in Intune.

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

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User2 can enroll a maximum of 10 devices in Intune.	<input type="radio"/>	<input type="radio"/>
User3 can enroll an unlimited number of devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

NEW QUESTION 10

You use Microsoft System Center Configuration Manager (Current Branch) to manage devices. Your company uses the following types of devices:

- Windows 10
- Windows 8.1
- Android
- iOS

Which devices can be managed by using co-management?

- A. Windows 10 and Windows 8.1 only
B. Windows 10, Android, and iOS only
C. Windows 10 only
D. Windows 10, Windows 8.1, Android, and iOS

Answer: D

Explanation:

References:

https://docs.microsoft.com/en-us/sccm/core/plan-design/choose-a-device-management-solution#bkmk_intune

NEW QUESTION 11

You have Windows 10 Pro devices that are joined to an Active Directory domain. You plan to create a Microsoft 365 tenant and to upgrade the devices to Windows 10 Enterprise. You are evaluating whether to deploy Windows Hello for Business for SSO to Microsoft 365 services. What are two prerequisites of the deployment? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Microsoft Azure Active Directory (Azure AD)
B. smartcards
C. Microsoft Intune enrollment
D. TPM-enabled devices
E. computers that have biometric hardware features

Answer: AC

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-ss0-base>

NEW QUESTION 12

Your company has a Microsoft 365 E3 subscription.

All devices run Windows 10 Pro and are joined to Microsoft Azure Active Directory (Azure AD).

You need to change the edition of Windows 10 to Enterprise the next time users sign in to their computer. The solution must minimize downtime for the users. What should you use?

- A. Windows Autopilot
B. Windows Update
C. Subscription Activation
D. an in-place upgrade

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot>

NEW QUESTION 15

Your company has a Microsoft 365 subscription.
You need to identify which users performed the following privileged administration tasks:

- Deleted a folder from the second-stage Recycle Bin of Microsoft SharePoint
- Opened a mailbox of which the user was not the owner
- Reset a user password

What should you use?

- A. Microsoft Azure Active Directory (Azure AD) audit logs
- B. Security & Compliance content search
- C. Microsoft Azure Active Directory (Azure AD) sign-ins
- D. Security & Compliance audit tag search

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

NEW QUESTION 17

HOTSPOT

Your network contains an Active Directory domain named contoso.com. The domain contains the file servers shown in the following table.

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

A file named File1.abc is stored on Server1. A file named File2.abc is stored on Server2. Three apps named App1, App2, and App3 all open files that have the .abc file extension.

You implement Windows Information Protection (WIP) by using the following configurations:

Exempt apps: App2

Protected apps: App1

Windows Information Protection mode: Block

Network boundary: IPv4 range of: 192.168.1.1-192.168-1.255

You need to identify the apps from which you can open File1.abc.

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
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

NEW QUESTION 19

HOTSPOT

You have retention policies in Microsoft 365 as shown in the following table.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 is configured as shown in the Policy1 exhibit. (Click the Policy1 tab.)

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... 7 years

☒ No, just delete content that's older than

2 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 Policy2 exhibit. (Click the Policy2 tab.)

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... 4 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

2 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.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or-what-takes-precedence

NEW QUESTION 24

You have a Microsoft 365 subscription.
All users have their email stored in Microsoft Exchange Online.
In the mailbox of a user named User 1. You need to preserve a copy of all the email messages that contain the word Project X.
WDM should you do?

- A. From the Security & Compliance admin center, create an eDiscovery case.
B. From the Exchange admin center, create a mail now rule.

- C. From the Security fit Compliance adman center, start a message trace.
- D. From Microsoft Cloud App Security, create an access policy.

Answer: A

Explanation:

References:

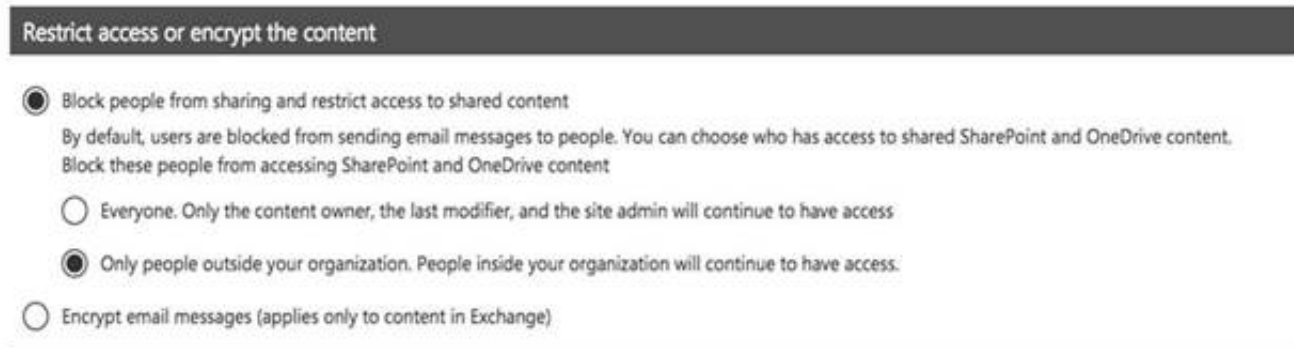
<https://docs.microsoft.com/en-us/office365/securitycompliance/ediscovery-cases#step-2-create-a-new-case>

NEW QUESTION 25

In Microsoft 365, you configure a data loss prevention (DLP) policy named Policy1. Policy1 detects the sharing of United States (US) bank account numbers in email messages and attachments.

Policy1 is configured as shown in the exhibit. (Click the Exhibit tab.)

Use actions to protect content when the conditions are met.



You need to ensure that internal users can email documents that contain US bank account numbers to external users who have an email suffix of contoso.com. What should you configure?

- A. an action
- B. a group
- C. an exception
- D. a condition

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies#how-dlp-policies-work>

NEW QUESTION 27

You have a Microsoft 365 subscription.

From the Security & Compliance admin center, you create a content search of all the mailboxes that contain the word Project X.

You need to export the results of the content search. What do you need to download the report?

- A. a certification authority (CA) certificate
- B. an export key
- C. a password
- D. a user certificate

Answer: B

Explanation:

References:

[https://docs.HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results"microsoft.com/en-us/office365/securitycompliance/export-search-results](https://docs.microsoft.com/en-us/office365/securitycompliance/export-search-results)

NEW QUESTION 32

HOTSPOT

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You have three applications named App1, App2, and App3 that have the same file format.

Your company uses Windows Information Protection (WIP). WIP has the following configurations: Windows Information Protection mode: Silent

Protected apps: App1 Exempt apps: App2

From App1, you create a file named File1.

What is the effect of the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

NEW QUESTION 33

HOTSPOT

You have a Microsoft 365 subscription.

You have a group named Support. Users in the Support group frequently send email messages to external users.

The manager of the Support group wants to randomly review messages that contain attachments. You need to provide the manager with the ability to review messages that contain attachments sent from the Support group users to external users. The manager must have access to only 10 percent of the messages.

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

To meet the goal for the manager, create:

▼
A label policy
A retention policy
A supervisor policy
An alert policy
MyAnalytics

To review the messages, the manager must use:

▼
A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

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 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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 38

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You configure the Apple MDM Push certificate.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/apple-mdm-push-certificate-get>

NEW QUESTION 43

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 are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error. You need to ensure that you can enroll the iOS device in Intune. Solution: You create an Apple Configurator enrollment profile. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 47

You are testing a data loss prevention (DLP) policy to protect the sharing of credit card information with external users.

During testing, you discover that a user can share credit card information with external users by using email.

However, the user is prevented from sharing files that contain credit card information by using Microsoft SharePoint Online.

You need to prevent the user from sharing the credit card information by using email and SharePoint. What should you configure?

- A. the locations of the DLP policy
- B. the user overrides of the DLP policy rule
- C. the status of the DLP policy
- D. the conditions of the DLP policy rule

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

NEW QUESTION 51

HOTSPOT

You have a Microsoft Office 365 subscription.

You need to delegate eDiscovery tasks as shown in the following table.

User	Task
User1	<ul style="list-style-type: none">• Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content.• View the eDiscovery cases created by User1.• Configure case settings.• Place content on hold.
User2	<ul style="list-style-type: none">• View the eDiscovery cases created by User1.• Export data from Advanced eDiscovery.

The solution must follow the principle of the least privilege.

To which role group should you assign each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

eDiscovery Administrator

eDiscovery Manager

Records Management

Reviewer

Security Administrator

User2:

eDiscovery Administrator

eDiscovery Manager

Records Management

Reviewer

Security Administrator

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 53

You plan to use the Security & Compliance admin center to import several PST files into Microsoft 365 mailboxes. Which three actions should you perform before you import the data? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. From the Exchange admin center, create a public folder.
- B. Copy the PST files by using AzCopy.
- C. From the Exchange admin center, assign admin roles.
- D. From the Microsoft Azure portal, create a storage account that has a blob container.
- E. From the Microsoft 365 admin center, deploy an add-in.
- F. Create a mapping file that uses the CSV file format.

Answer: BCF

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/use-network-upload-to-import-pst-files>

NEW QUESTION 58

HOTSPOT

You have a Microsoft 365 tenant. You plan to create a retention policy as shown in the following exhibit.

Create a policy to retain what you want and get rid of what you don't.

✔ Name your policy

✔ Settings

✔ Choose locations

● Review your settings

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Policy name

contoso

Edit

Description

Edit

Applies to content in these locations

Exchange email

OneDrive accounts

SharePoint sites

Office 365 groups

Edit

Settings

Retention period

Don't retain content, but delete it if it's older than 7 years

⚠ Content that's currently older than this will be deleted after you turn on the policy

Edit

Back

Save for later

Create this policy

Cancel

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.

Microsoft SharePoint files that are affected by the policy will be [answer choice].	<div>▼</div> <div>recoverable for up to seven years</div> <div>deleted seven years after they were created</div> <div>retained for only seven years from when they were created</div>
Once the policy is created, [answer choice].	<div>▼</div> <div>some data may be deleted immediately</div> <div>data will be retained for a minimum of seven years</div> <div>users will be prevented from permanently deleting email messages for seven years</div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Microsoft SharePoint files that are affected by the policy will be [answer choice].	<div>▼</div> <div>recoverable for up to seven years</div> <div>deleted seven years after they were created</div> <div>retained for only seven years from when they were created</div>
Once the policy is created, [answer choice].	<div>▼</div> <div>some data may be deleted immediately</div> <div>data will be retained for a minimum of seven years</div> <div>users will be prevented from permanently deleting email messages for seven years</div>

NEW QUESTION 63

You deploy Microsoft Azure Information Protection.

You need to ensure that a security administrator named SecAdmin1 can always read and inspect data protected by Azure Rights Management (Azure RMS). What should you do?

- A. From the Security & Compliance admin center, add User1 to the eDiscovery Manager role group.
B. From the Azure Active Directory admin center, add User1 to the Security Reader role group.
C. From the Security & Compliance admin center, add User1 to the Compliance Administrator role group.
D. From Windows PowerShell, enable the super user feature and assign the role to SecAdmin1.

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-super-users>

NEW QUESTION 68

You create a new Microsoft 365 subscription and assign Microsoft 365 E3 licenses to 100 users. From the Security & Compliance admin center, you enable auditing.

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. An administrator creates a new Microsoft SharePoint site collection.
B. An administrator creates a new mail flow rule.
C. A user shares a Microsoft SharePoint folder with an external user.
D. A user delegates permissions to their mailbox.
E. A user purges messages from their mailbox.

Answer: ABC

Explanation:

References:

[https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c"2farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c](https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%25HYPERLINK%20https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-andcompliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c%2farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c)

NEW QUESTION 72

HOTSPOT

You have a Microsoft 365 tenant.

You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create a policy to retain what you want and get rid of what you don't.

Name your label

Label settings

Review your settings

Review your settings

It will take up to 1 day to apply the retention policy to the locations you chose.

Name

6Months

Edit

Description for admins

Edit

Description for users

Edit

Retention

6 months

Retain and Delete

Based on when it was created

Edit

Back

Create this label

Cancel

You create a label policy as shown in the Label Policy Exhibit. (Click the Label Policy tab.)

Automatically apply a label to content

Choose label to auto-apply

Choose conditions

Name your policy

Locations

Review your settings

Detect content that matches this query:

Conditions

We'll apply this policy to content that matches these conditions.

Keyword query editor

ProjectX

Back

Next

Cancel

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the work ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 76

HOTSPOT

You purchase a new Microsoft 365 subscription.

You create 100 users who are assigned Microsoft 365 E3 licenses. From the Security & Compliance admin center, you enable auditing.

Six months later, a manager sends you an email message asking the following questions: Question1: Who created a team named Team1 14 days ago?

Question2: Who signed in to the mailbox of User1 30 days ago?

Guaranteed success with Our exam guides

visit - <https://www.certshared.com>

Question3: Who changed the site collection administrators of a site 60 days ago?
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
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/office365/securitycomplianceHYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c"nce/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c
https://docs.microsoft.com/HYPERLINK "https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing"en-us/office365/securitycompliance/enable-mailbox-auditing

NEW QUESTION 77

Your company has a Microsoft 365 tenant.
The company sells products online and processes credit card information.
You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.
What should you use?

- A. a Security & Compliance data loss prevention (DLP) policy
B. a Microsoft Cloud App Security access policy
C. a Security & Compliance retention policy
D. a Microsoft Cloud App Security file policy

Answer: A

Explanation:

References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION 80

DRAG DROP
You have the Microsoft Azure Advanced Threat Protection (ATP) workspace shown in the Workspace exhibit. (Click the Workspace tab.)

Workspace ⓘ

Manage Azure ATP user roles ⓘ

Create Workspace

NAME	TYPE	INTEGRATION	GEOLOCATION
testworkspace ⓘ	Primary	Windows Defender ATP	Europe

The sensors settings for the workspace are configured as shown in the Sensors exhibit. (Click the Sensors tab.)

Sensors ⓘ

① Configure Directory Services to install the first Sensor or Standalone Sensor.

NAME	TYPE	DOMAIN CO...	VERSION	SERVICE STATUS	HEALTH
No Sensors registered					

You need to ensure that Azure ATP stores data in Asia.
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
Modify the integration setting for the workspace.	<div></div>
Delete the workspace.	<div></div>
Regenerate the access keys.	<div></div>
Create a new workspace.	
Modify the Azure ATP user roles.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Delete the workspace.

Create a new workspace.

Regenerate the access keys.

NEW QUESTION 83

You have a Microsoft 365 subscription.

You need to be notified if users receive email containing a file that has a virus. What should you do?

- A. From the Exchange admin center, create an in-place eDiscovery & hold.
- B. From the Security & Compliance admin center, create a data governance event.
- C. From the Exchange admin center, create an anti-malware policy.
- D. From the Security & Compliance admin center, create a safe attachments policy.

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/servicedescriptions/exchange-online-service-description/anti-spamand-anti-malware-protection>

NEW QUESTION 85

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

You need to ensure that when users join their device to Microsoft Azure Active Directory (Azure AD), the device is enrolled in Microsoft Intune automatically.

What should you configure?

- A. Enrollment restrictions from the Intune admin center
- B. device enrollment managers from the Intune admin center
- C. MAM User scope from the Azure Active Directory admin center
- D. MDM User scope from the Azure Active Directory admin center

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/windows-enroll>

NEW QUESTION 89

HOTSPOT

Your network contains an Active Directory domain named contoso.com. All client devices run Windows 10 and are joined to the domain.

You update the Windows 10 devices by using Windows Update for Business.

What is the maximum amount of time you can defer Windows 10 updates? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Quality updates:

▼
14 days
30 days
60 days
120 days

Feature updates:

▼
60 days
180 days
365 days
540 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb>

NEW QUESTION 94

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. You have a Microsoft 365 subscription. You need to ensure that users can manage the configuration settings for all the Windows 10 devices in your organization. What should you configure?

- A. the Enrollment restrictions
- B. the mobile device management (MDM) authority
- C. the Exchange on-premises access settings
- D. the Windows enrollment settings

Answer: B

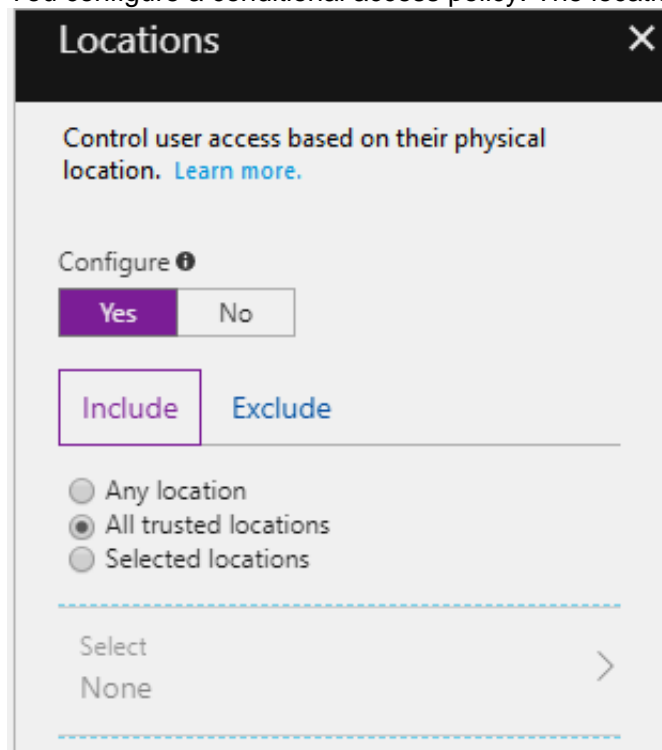
Explanation:

References:

<https://docs.microsoft.com/en-us/intune/mdm-authority-set>

NEW QUESTION 98

You configure a conditional access policy. The locations settings are configured as shown in the Locations exhibit. (Click the Locations tab.)



The users and groups settings are configured as shown in the Users and Groups exhibit. (Click Users and Groups tab.)



Members of the Security reader group report that they cannot sign in to Microsoft Active Directory (Azure AD) on their device while they are in the office. You need to ensure that the members of the Security reader group can sign in to Azure AD on their device while they are in the office. The solution must use the principle of least privilege. What should you do?

- A. From the conditional access policy, configure the device state.
- B. From the Azure Active Directory admin center, create a custom control.
- C. From the Intune admin center, create a device compliance policy.
- D. From the Azure Active Directory admin center, create a named location.

Answer: D

Explanation:

References:

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

NEW QUESTION 101

You have computers that run Windows 10 Enterprise and are joined to the domain.

You plan to delay the installation of new Windows builds so that the IT department can test application

compatibility.

You need to prevent Windows from being updated for the next 30 days.

Which two Group Policy settings should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Select when Quality Updates are received
- B. Select when Preview Builds and Feature Updates are received
- C. Turn off auto-restart for updates during active hours
- D. Manage preview builds
- E. Automatic updates detection frequency

Answer: BD

NEW QUESTION 105

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

You need to provide a user with the ability to sign up for Microsoft Store for Business for contoso.com. The solution must use the principle of least privilege.

Which role should you assign to the user?

- A. Cloud application administrator
- B. Application administrator
- C. Global administrator
- D. Service administrator

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business>

NEW QUESTION 106

HOTSPOT

You have the Microsoft Azure Active Directory (Azure AD) users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

You create a conditional access policy that has the following settings: The Assignments settings are configured as follows:

Users and groups: Group1

Cloud apps: Microsoft Office 365 Exchange Online

Conditions: Include All device state, exclude Device marked as compliant Access controls is set to Block access.

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

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 108

HOTSPOT

You have three devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group2

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

Name	Platform	Require BitLocker	Assigned
Policy1	Windows 10 and later	Require	Yes
Policy2	Windows 10 and later	Not configured	Yes
Policy3	Windows 10 and later	Require	No

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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
Device1 is compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device2 is compliant.	<input type="radio"/>	<input checked="" type="radio"/>
Device3 is compliant.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 111

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Device Management admin center, you create a trusted location and a compliance policy Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678>

NEW QUESTION 113

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.

You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.

Solution: From the Microsoft 365 admin center, you configure the Organization profile settings. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678A>

NEW QUESTION 118

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.

From the Security & Compliance admin center, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-ComplianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search>

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/newcompliancesecurityfilter?view=exchange-ps>

NEW QUESTION 123

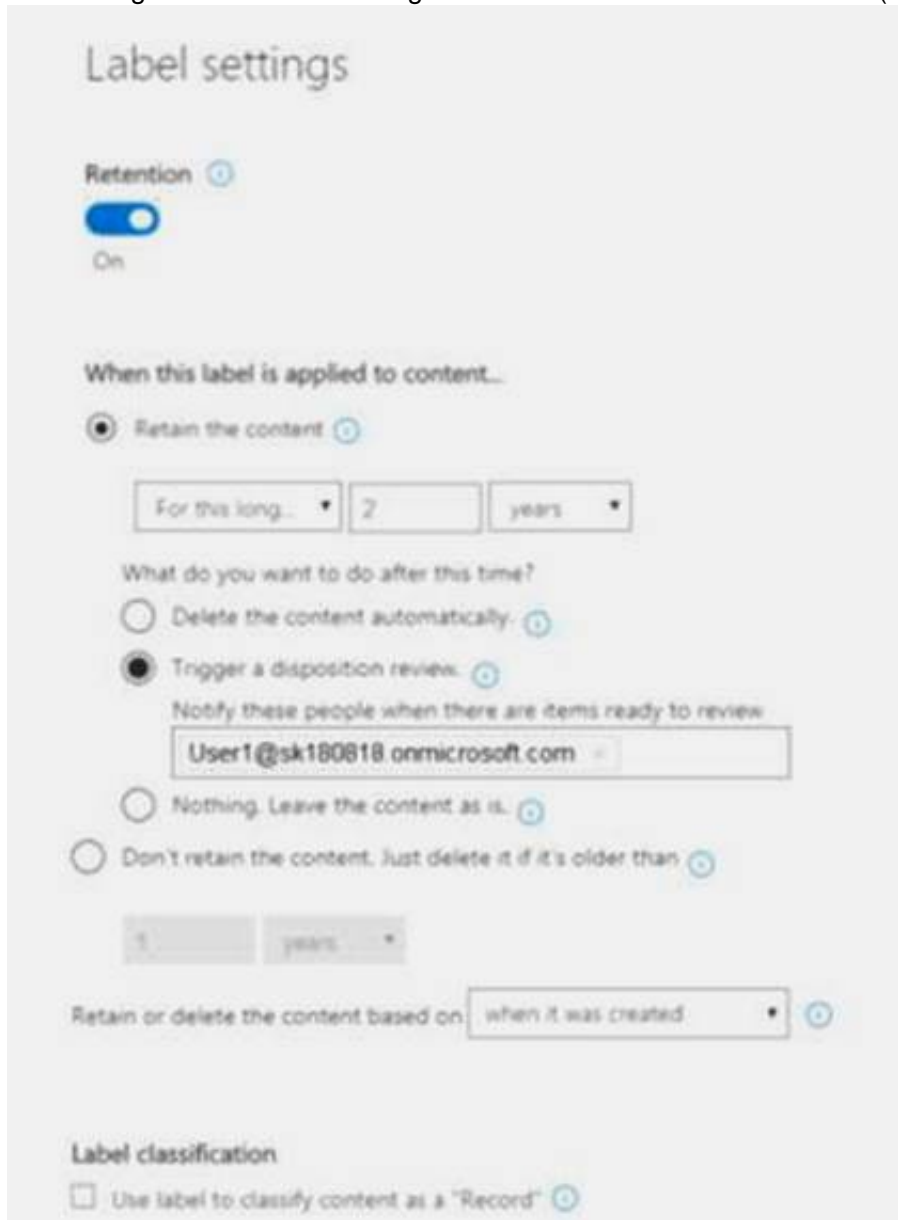
HOTSPOT

You have a Microsoft 365 subscription that uses a default domain named contoso.com. Three files were created on February 1, 2019, as shown in the following table.

Name	Stored in
File1	Microsoft OneDrive
File2	A Microsoft SharePoint library
File3	Microsoft Exchange Online email

On March 1, 2019, you create two retention labels named Label1 and Label2.

The settings for Label1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)



The settings for Label2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)



You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts.
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
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 127

You have a Microsoft 365 subscription.
You plan to enable Microsoft Azure Information Protection.
You need to ensure that only the members of a group named PilotUsers can protect content. What should you do?

- A. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- B. Create an Azure Information Protection policy.
- C. Configure the protection activation status for Azure Information Protection.
- D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Answer: D

Explanation:

References:
<https://docs.microsoft.com/en-us/azure/information-protection/activate-service>

NEW QUESTION 129

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 Azure Active Directory (Azure AD) tenant named contoso.com. You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1. The tenant contains users shown in the following table.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

You need to modify the configuration of the Azure ATP sensors.
Solution: You instruct User1 to modify the Azure ATP sensor configuration. Does this meet the goal?

- A. Yes
- B. No

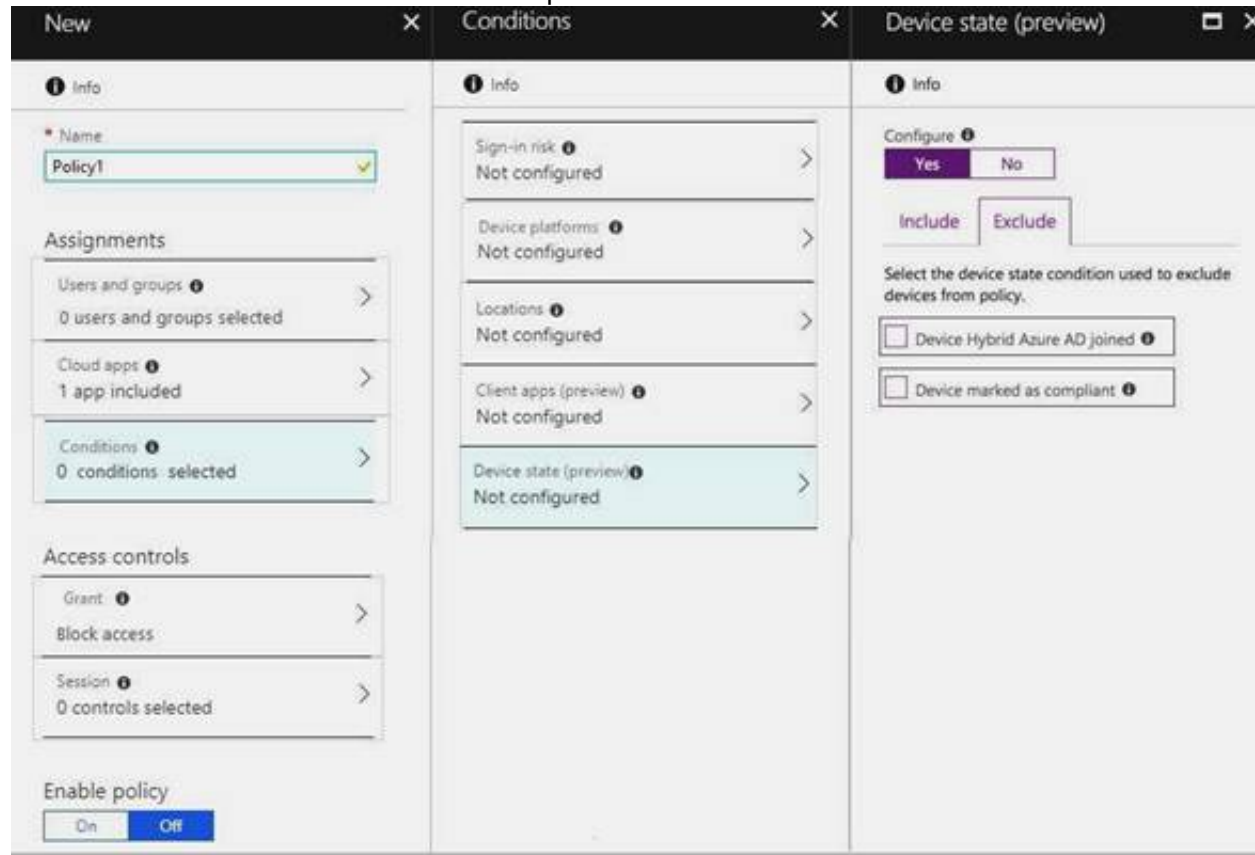
Answer: A

NEW QUESTION 132

HOTSPOT

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app. Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

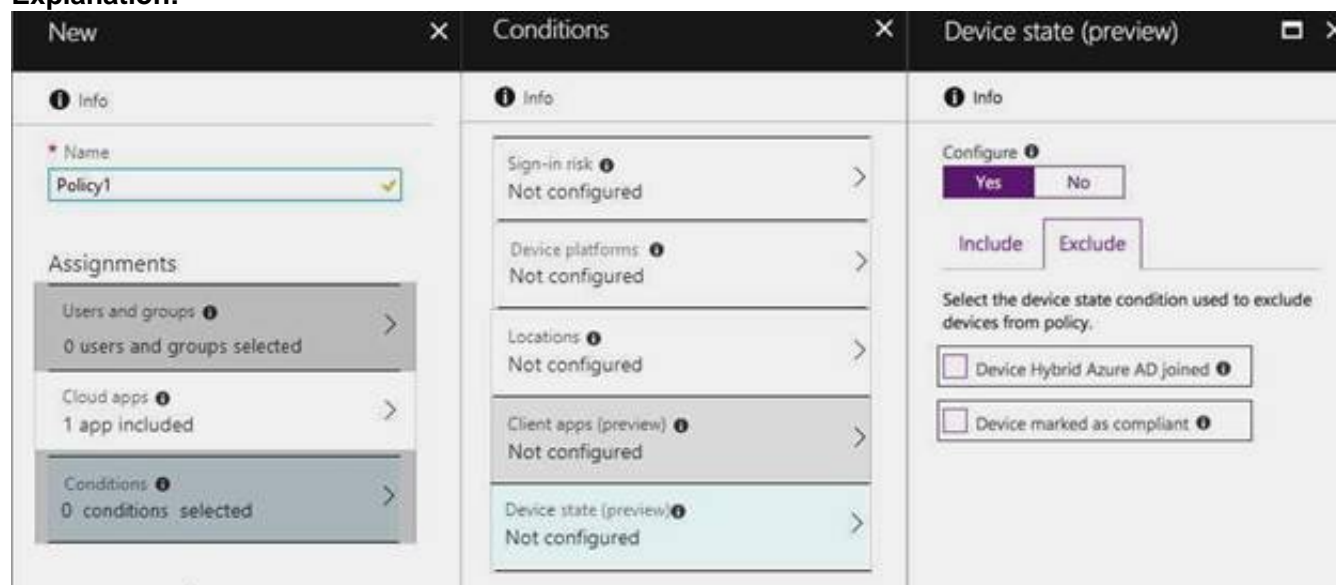
NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 136

You need to meet the compliance requirements for the Windows 10 devices. What should you create from the Intune admin center?

- A. a device compliance policy
- B. a device configuration profile
- C. an application policy
- D. an app configuration policy

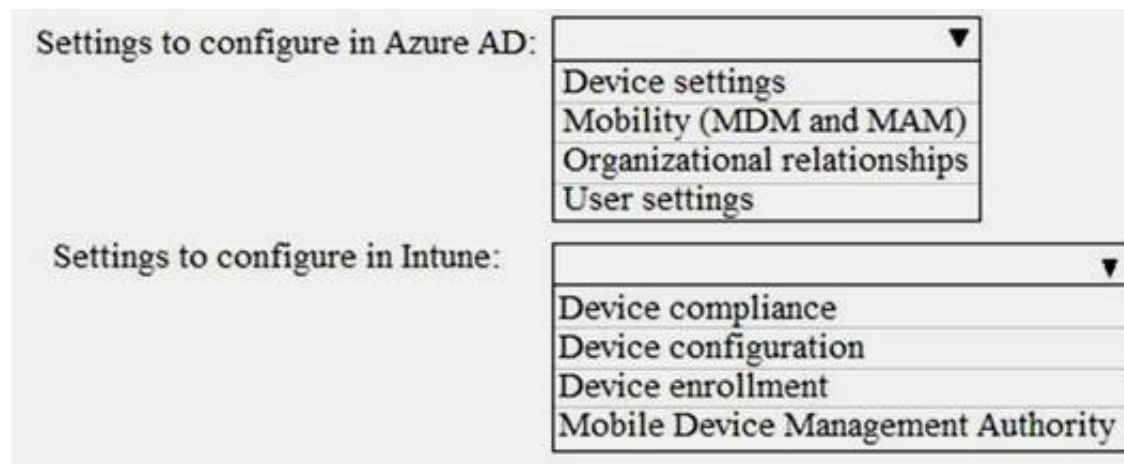
Answer: D

NEW QUESTION 141

HOTSPOT

You need to meet the Intune requirements for the Windows 10 devices.

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/intune/windows-enroll>

NEW QUESTION 142

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices. What is the minimum of dedicated support technicians required?

- A. 1
- B. 4
- C. 7
- D. 31

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

NEW QUESTION 143

You need to create the Microsoft Store for Business. Which user can create the store?

- A. User2
- B. User3
- C. User4
- D. User5

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business>

Case Study: 2

A. Datum Case Study: Overview

Existing Environment

This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question. Current Infrastructure

A. Datum recently purchased a Microsoft 365 subscription. All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

A. Datum uses and processes Personally Identifiable Information (PII).

Problem Statements Requirements

A. Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365. Business Goals

A. Datum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A. Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A. Datum identifies the following technical requirements:

- Centrally perform log analysis for all offices.

- Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
- Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
- Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.
- Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
- If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user's user account.
- A security administrator requires a report that shows which Microsoft 365 users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
- Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION 147

You need to meet the technical requirement for the EU PII data. What should you create?

- A. a retention policy from the Security & Compliance admin center.
- B. a retention policy from the Exchange admin center
- C. a data loss prevention (DLP) policy from the Exchange admin center
- D. a data loss prevention (DLP) policy from the Security & Compliance admin center

Answer: A

Explanation:

References:

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

NEW QUESTION 150

You need to meet the technical requirement for large-volume document retrieval. What should you create?

- A. a data loss prevention (DLP) policy from the Security & Compliance admin center
- B. an alert policy from the Security & Compliance admin center
- C. a file policy from Microsoft Cloud App Security
- D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts>

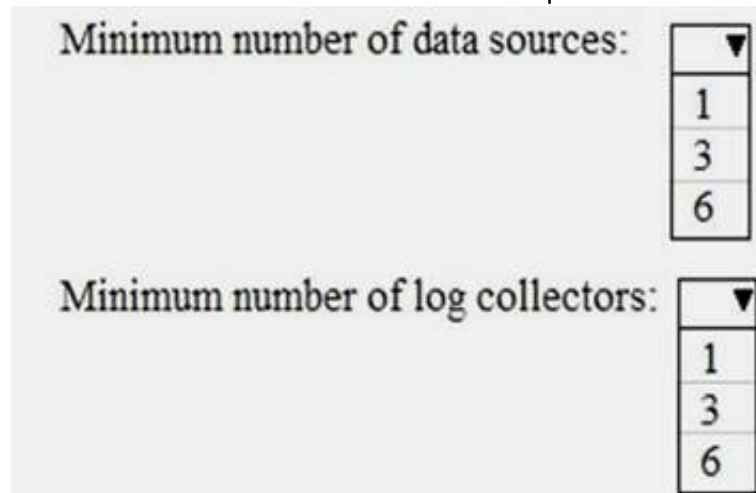
NEW QUESTION 151

HOTSPOT

You need to meet the technical requirement for log analysis.

What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Minimum number of data sources:

Minimum number of log collectors:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

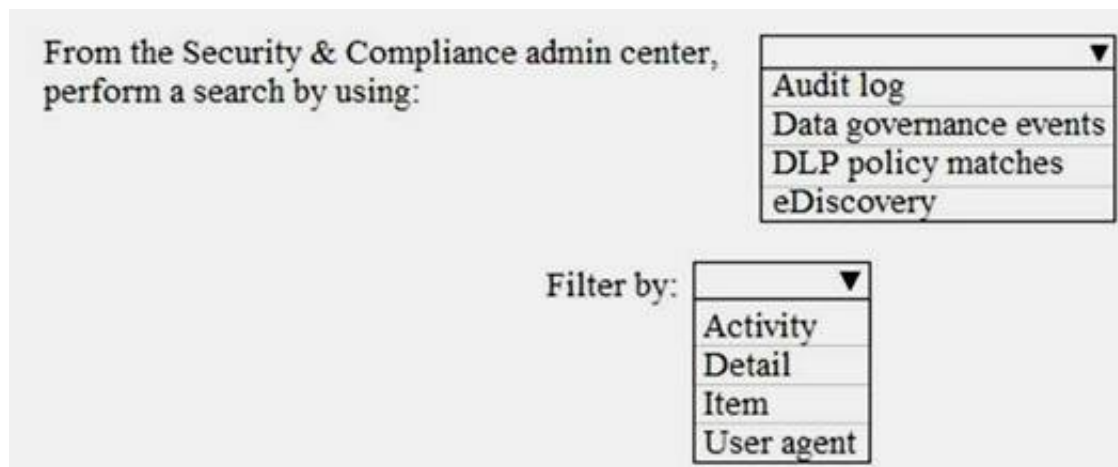
<https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker>

NEW QUESTION 152

HOTSPOT

You need to meet the technical requirement for the SharePoint administrator. What should you do?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results>

NEW QUESTION 155

.....

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-101 Practice Exam Features:

- * MS-101 Questions and Answers Updated Frequently
- * MS-101 Practice Questions Verified by Expert Senior Certified Staff
- * MS-101 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MS-101 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MS-101 Practice Test Here](#)