

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 create an Apple Configurator enrollment profile. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 2

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 discover that some external users accessed content on a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing outside your organization.

You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 3

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management

You add a new device named Device 1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You unjoin Device1 from the Active Directory domain. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 4

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management

You add a new device named Device 1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You create a device configuration profile from the Intune admin center. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 5

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 6

HOTSPOT

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	None

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 view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

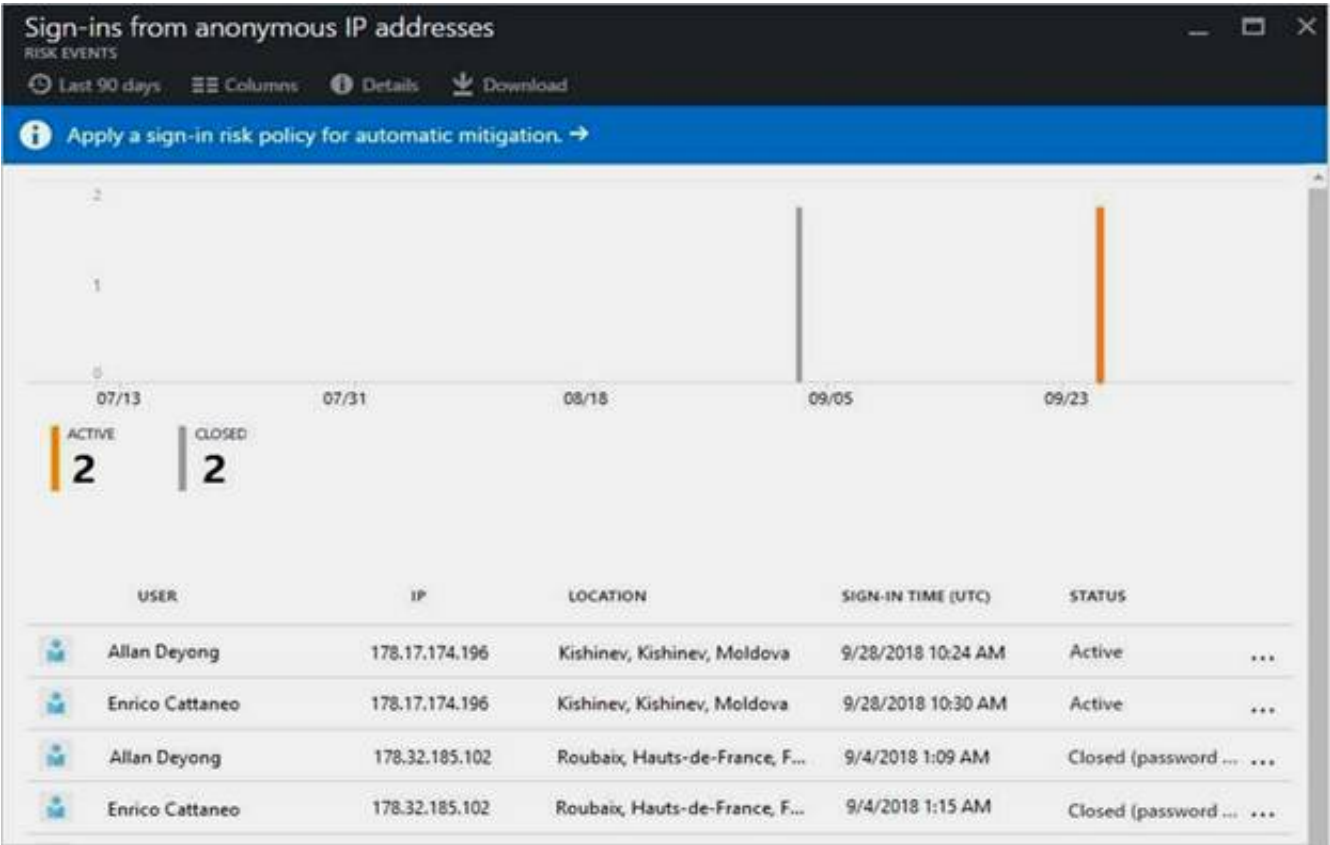
Answer: A

Explanation:

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 7

From the Microsoft Azure Active Directory (Azure AD) Identity Protection dashboard, you view the risk events shown in the exhibit. (Click the Exhibit tab.)



You need to reduce the likelihood that the sign-ins are identified at risky. What should you do?

- A. From the Security & Compliance admin center, create a classification label.
- B. From the Security & Compliance admin center, add the users to the Security Readers role group.
- C. From the Azure Active Directory admin center, configure the trusted IPs for multi-factor authentication.
- D. From the Conditional access blade in the Azure Active Directory admin center, create named locations.

Answer: D

Explanation:

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

NEW QUESTION 8

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	Not applicable

You onboard computers to Windows Defender ATP as shown in the following table.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Of which groups are Computer1 and Computer2 members? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Computer1:

Group1 only

Group2 only

Group1 and Group2

Ungrouped machines

Computer2:

Group1 only

Group3 only

Group1 and Group3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Computer1:

▼
Group1 only
Group2 only
Group1 and Group2
Ungrouped machines

Computer2:

▼
Group1 only
Group3 only
Group1 and Group3

NEW QUESTION 9

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.

Answer Area

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:

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 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	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 10

Your network contains an Active Directory domain named contoso.com. The domain contains 100 Windows 8.1 devices. You plan to deploy a custom Windows 10 Enterprise image to the Windows 8.1 devices. You need to recommend a Windows 10 deployment method. What should you recommend?

- A. a provisioning package
- B. an in place upgrade
- C. wipe and load refresh
- D. Windows Autopilot

Answer: B

Explanation:

References:
<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windHYPERLINK> "https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure"ows10- infrastructure

NEW QUESTION 12

HOTSPOT
 You have three devices enrolled .n Microsoft Intune as shown .n 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
Policy1	Group3
Policy2	Group2

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

NEW QUESTION 17

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-sso-base>

NEW QUESTION 21

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. From the AADRM PowerShell module, run the set-AadmonboardingControlPolicy cmdlet.
 B. From Azure Information Protection, create a policy.
 C. From the AAORM PowerShell module, run the Add-AadrmRoleBasedAdministrator cmdlet.
 D. From Azure Information Protection, configure the protection activation status.

Answer: B

Explanation:

References:

<https://blogs.technet.microsoft.com/kemckinn/2018/05/17/creating-labels-for-azure-information- protection/>

NEW QUESTION 24

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>docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview

NEW QUESTION 27

You have a Microsoft 365 subscription

All users are assigned a Microsoft 365 E3 License. You enable auditing for your organization.

What is the maximum amount of time data will be retained in the Microsoft 365 audit log?

- A. 2 years
- B. 1 year
- C. 30 days
- D. 90 days

Answer: D

Explanation:

References:

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

NEW QUESTION 32

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>

NEW QUESTION 34

HOTSPOT

You have a document in Microsoft OneDrive that is encrypted by using Microsoft Azure Information Protection as shown in the following exhibit.

Protection settings ⓘ

Azure (cloud key)

HYOK (AD RMS)

Select the protection action type ⓘ

☒ Set permissions

☐ Set user-defined permissions (Preview)

USERS	PERMISSIONS
M365x901434.onmicrosoft.com	Co-Owner

+ Add permissions

Content expiration

Always

Never

By days

Number of days the content is valid

30

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always

Never

By days

Number of days the content is available without an Internet connection

7

Protection template ID - template id is automatically generated after template is saved

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 copy the file to your local computer, you [answer choice].

cannot open the document

can open the document indefinitely

can open the document for up to 7 days

can open the document for up to 30 days

If you email the document to a user outside your organization, the user [answer choice].

cannot open the document

can open the document indefinitely

can open the document for up to 7 days

can open the document for up to 30 days

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 35

You have a Microsoft 365 subscription.
You configure a data loss prevention (DLP) policy.
You discover that users are incorrectly marking content as false positive and bypassing the OLP policy.
You need to prevent the users from bypassing the DLP policy. What should you configure?

- A. incident reports
- B. actions
- C. exceptions
- D. user overrides

Answer: D

Explanation:

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

NEW QUESTION 40

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 45

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:

<input type="checkbox"/>	A label policy
<input type="checkbox"/>	A retention policy
<input type="checkbox"/>	A supervisor policy
<input type="checkbox"/>	An alert policy
<input type="checkbox"/>	MyAnalytics

To review the messages, the manager must use:

<input type="checkbox"/>	A message trace
<input type="checkbox"/>	An eDiscovery case
<input type="checkbox"/>	MyAnalytics
<input type="checkbox"/>	Outlook Web App

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 47

HOTSPOT

You have a data loss prevention (DIP) policy.
You need to increase the likelihood that the DLP policy will apply to data that contains medical terms from the International Classification of Diseases (ICD-9-CM).
The solution must minimize the number of false positives.
Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.

Content contains

Any of these ▾

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min

1

max

any

Match accuracy

min

50

max

100

Add ▾

and ▾

Any of these ▾

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min

1

max

any

Match accuracy

min

50

max

100

Add ▾

A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies> <https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

NEW QUESTION 51

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 52

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.

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure pilot co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager.

Solution: You add Device1 to an Active Directory group. Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

References:

<https://www.sccconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/>

NEW QUESTION 56

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.

Passing Certification Exams Made Easy

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

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 57

You have a Microsoft 365 subscription.

You need to view the IP address from which a user synced a Microsoft SharePoint library.

What should you do?

- A. From the SharePoint admin center, view the usage reports.
- B. From the Security & Compliance admin center, perform an audit log search.
- C. From the Microsoft 365 admin center, view the usage reports.
- D. From the Microsoft 365 admin center, view the properties of the user's user account.

Answer: B

Explanation:

References:

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

NEW QUESTION 62

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:	<div><div></div><div>eDiscovery Administrator</div><div>eDiscovery Manager</div><div>Records Management</div><div>Reviewer</div><div>Security Administrator</div></div>
User2:	<div><div></div><div>eDiscovery Administrator</div><div>eDiscovery Manager</div><div>Records Management</div><div>Reviewer</div><div>Security Administrator</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 67

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 72

HOTSPOT

From the Security & Compliance admin center, you create a retention policy named Policy1. You need to prevent all users from disabling the policy or reducing the retention period.

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

Answer Area

Set-ComplianceTag

Set-HoldCompliancePolicy

Set-RetentionCompliancePolicy

Set-RetentionPolicy

Set-RetentionPolicyTag

-Identity "Policy1"

-enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-SystemTag

\$true

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:
<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-pHYPERLINK>
"https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps"s

NEW QUESTION 77

From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)

SharePoint Content_Export

Restart report

Download report

Delete

Status:
The export has completed. You can start downloading the results.

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

Close

Feedback

What will be excluded from the export?

- A. a 60-MB DOCX file
- B. a 5-MB MP3 file
- C. a 10-MB XLSX file
- D. a 5-KB RTF file

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

NEW QUESTION 78

Your company has 5,000 Windows 10 devices. All the devices are protected by using Windows Defender

Advanced Threat Protection (ATP).

You need to view which Windows Defender ATP alert events have a high severity and occurred during the last seven days.

What should you use in Windows Defender ATP?

- A. the threat intelligence API
- B. Automated investigations
- C. Threat analytics
- D. Advanced hunting

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/investigate-alertswindows-defender-advanced-threat-protection>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/automatedinvestigations-windows-defender-advanced-threat-protection>

NEW QUESTION 81

HOTSPOT

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP includes the machine groups shown in the following table.

Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	Not applicable

You onboard a computer named computer1 to Windows Defender ATP 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.

Computer1 will be a member of [answer choice].

▼

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped machines

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Computer1 will be a member of [answer choice].

▼

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped machines

If you add the tag demo to Computer1, the computer will be a member of [answer choice].

▼

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped machines

NEW QUESTION 83

DRAG DROP

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



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



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

Modify the integration setting for the workspace.

Delete the workspace.

Regenerate the access keys.

Create a new workspace.

Modify the Azure ATP user roles.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Delete the workspace.

Create a new workspace.

Regenerate the access keys.

NEW QUESTION 84

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains 1,000 Windows 10 devices. You perform a proof of concept (PoC) deployment of Windows Defender Advanced Threat Protection (ATP) for 10 test devices. During the onboarding process, you configure Windows Defender ATP- related data to be stored in the United States. You plan to onboard all the devices to Windows Defender ATP. You need to store the Windows Defender ATP data in Europe. What should you first?

- A. Create a workspace.
- B. Onboard a new device.
- C. Delete the workspace.
- D. Offboard the test devices.

Answer: D

NEW QUESTION 87

HOTSPOT

Your company uses Microsoft Cloud App Security.

You plan to integrate Cloud App Security and security information and event management (SIEM). You need to deploy a SIEM agent on a server that runs Windows Server 2016.

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

First action to perform:

▼
Install Java 8.
Install Microsoft .NET Framework 3.5.
Add the Windows Internal Database feature.
Add the Setup and Boot Event Collection feature.

Second action to perform:

▼
Run the Set-MMagent cmdlet.
Add the Setup and Boot Event Collection feature.
Run the java command and specify the -jar parameter.
Run the Install-WindowsFeature cmdlet and specify the -source parameter.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas>

NEW QUESTION 92

Your company uses Microsoft System Center Configuration Manager (Current Branch) and Microsoft Intune to co-manage devices.

Which two actions can be performed only from Intune? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Deploy applications to Windows 10 devices.
- B. Deploy VPN profiles to iOS devices.
- C. Deploy VPN profiles to Windows 10 devices.
- D. Publish applications to Android devices.

Answer: BD

Explanation:

References:

<https://docs.microsoft.com/en-us/sccm/comanage/overview>

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles>

NEW QUESTION 97

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 102

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 103

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	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Non configured	15	Yes

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 marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 is marked as noncompliant after 10 days.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 is marked as noncompliant after 15 days.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 108

HOTSPOT

You have a Microsoft Azure Activity Directory (Azure AD) tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 is a member of Group1.

Your company uses Windows Defender Advanced Threat Protection (ATP). Windows Defender ATP contains the roles shown in the following table.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP contains the device groups shown in the following table.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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 run an antivirus scan on Device2.	<input type="radio"/>	<input type="radio"/>
User2 can collect an investigation package from Device2.	<input type="radio"/>	<input type="radio"/>
User3 can isolate Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-HYPERLINK> "https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/user-roles-windows-defender-advanced-threat-protection"defender-atp/user-roles-windows-defender-advanced-threat-protection

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 Azure Active Directory admin center, you create a trusted location and a conditional access policy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition> <https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678>

NEW QUESTION 114

You have a Microsoft 365 subscription.

You recently configured a Microsoft SharePoint Online tenant in the subscription. You plan to create an alert policy.

You need to ensure that an alert is generated only when malware is detected in more than five documents stored in SharePoint Online during a period of 10 minutes.

What should you do first?

- A. Enable Microsoft Office 365 Cloud App Security.
- B. Deploy Windows Defender Advanced Threat Protection (Windows Defender ATP)
- C. Enable Microsoft Office 365 Analytics.

Answer: B

NEW QUESTION 117

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 118

HOTSPOT

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

A user named User1 has files on a Windows 10 device as shown in the following table.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

In Azure Information Protection, you create a label named Label1 that is configured to apply automatically. Label1 is configured as shown in the following exhibit.

Condition: Condition1

Default Directory – Azure Information Protection

Save

Discard

Delete

Choose the type of condition

Information Types

Custom

Name

Condition1

Match exact phrase or pattern

im

Match as a regular expression

Off

On

Match with case sensitivity

Off

On

Minimum number of occurrences

2

Count occurrences with unique values only

Off

On

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
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
References:
<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION 122

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 Lable1 are configured as shown in the Label1 exhibit. (Click the Label1 tab.)

Label settings

Retention ⓘ

On

When this label is applied to content...

●

Retain the content ⓘ

For this long... 2 years

What do you want to do after this time?

Delete the content automatically. ⓘ

●

Trigger a disposition review. ⓘ

Notify these people when there are items ready to review

User1@sk180818.onmicrosoft.com

Nothing. Leave the content as is. ⓘ

Don't retain the content. Just delete it if it's older than ⓘ

1 years

Retain or delete the content based on when it was created ⓘ

Label classification

Use label to classify content as a "Record" ⓘ

The settings for Lable2 are configured as shown in the Label2 exhibit. (Click the Label2 tab.)

Label settings

Retention ⓘ

On

When this label is applied to content...

Retain the content ⓘ

For this long... 2 years

●

Don't retain the content. Just delete it if it's older than ⓘ

1 years

Retain or delete the content based on when it was created ⓘ

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.	<div><div></div></div>	<div><div></div></div>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<div><div></div></div>	<div><div></div></div>
File3 will be deleted automatically after February 1, 2021.	<div><div></div></div>	<div><div></div></div>

- 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 125

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-AzureRmRoleAssignment cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?view=azurermps-6.13.0>

NEW QUESTION 129

Your company has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. You sign for Microsoft Store for Business.
The tenant contains the users shown in the following table.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator
User5	None	None

Microsoft Store for Business has the following Shopping behavior settings: Allow users to shop is set to On
Make everyone a Basic Purchaser is set to Off

You need to identify which users can install apps from the Microsoft for Business private store.

Which users should you identify?

- A. User1, User2, User3, User4, and User5
- B. User1 only
- C. User1 and User2 only
- D. User3 and User4 only
- E. User1, User2, User3, and User4 only

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/microsoft-store/acquire-apps-microsoft-store-for-business>

NEW QUESTION 131

You have a Microsoft 365 subscription that contains a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

In the tenant, you create a user named User1.

You need to ensure that User1 can publish retention labels from the Security & Compliance admin center. The solution must use the principle of least privilege.

To which role group should you add User1?

- A. Security Administrator
- B. Records Management
- C. Compliance Administrator
- D. eDiscovery Manager

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/file-plan-manager>

NEW QUESTION 135

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 139

On which server should you install the Azure ATP sensor?

- A. Server 1
- B. Server 2
- C. Server 3
- D. Server 4
- E. Server 5

Answer: A

Explanation:

References:

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

NEW QUESTION 142

HOTSPOT

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Seattle:

▼
6 months
18 months
24 months
30 months
5 years

New York:

▼
6 months
18 months
24 months
30 months
5 years

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

References:

[https://www.windowscentral.com/whats-difference-HYPERLINK \"https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10\"between-quality-updates-and-feature-updates-windows-10](https://www.windowscentral.com/whats-difference-HYPERLINK \)

NEW QUESTION 145

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 36S 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 148

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:

1

3

6

Minimum number of log collectors:

1

3

6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 149

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.

From the Security & Compliance admin center, perform a search by using:

Audit log

Data governance events

DLP policy matches

eDiscovery

Filter by:

Activity

Detail

Item

User agent

- 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 150

.....

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 First Try
- * MS-101 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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