

Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam



NEW QUESTION 1

- (Exam Topic 1)

You need to ensure that User1 can enroll the devices to meet the technical requirements. What should you do?

- A. From the Azure Active Directory admin center, assign User1 the Cloud device administrator role.
- B. From the Azure Active Directory admin center, configure the Maximum number of devices per user setting.
- C. From the Intune admin center, add User1 as a device enrollment manager.
- D. From the Intune admin center, configure the Enrollment restrictions.

Answer: C

Explanation:

References:

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

NEW QUESTION 2

- (Exam Topic 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.

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 a pilot for 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: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

- A. Yes
- B. NO

Answer: A

Explanation:

Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrolls in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: <https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable>

NEW QUESTION 3

- (Exam Topic 1)

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 4

- (Exam Topic 3)

You need to configure the information governance settings to meet the technical requirements.

Which type of policy should you configure, and how many policies should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type: 

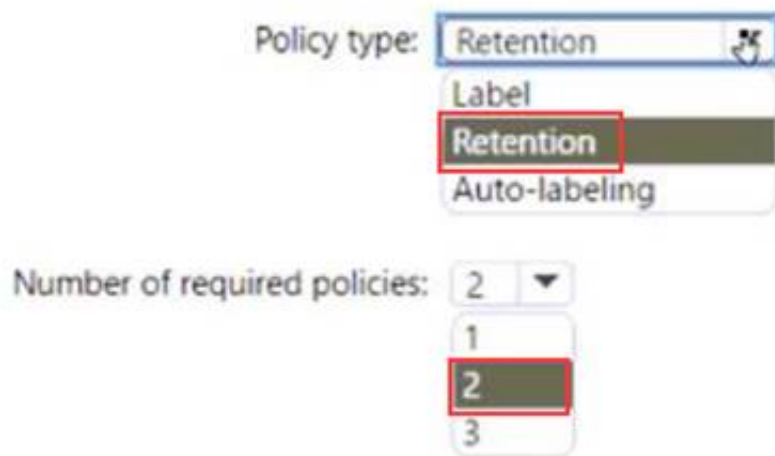
Number of required policies: 

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 5

- (Exam Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project. Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. pointer (PTR)

Answer: A

Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

There are several versions of this question in the exam. The question has two possible correct answers: Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting>

NEW QUESTION 6

- (Exam Topic 5)

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.

What should you do first?

- A. Enable auditing.
- B. Enable Microsoft 365 usage analytics.
- C. Create an Insider risk management policy.
- D. Create a communication compliance policy.

Answer: A

Explanation:

Microsoft Purview auditing solutions provide an integrated solution to help organizations effectively respond to security events, forensic investigations, internal investigations, and compliance obligations. Thousands of user and admin operations performed in dozens of Microsoft 365 services and solutions are captured, recorded, and retained in your organization's unified audit log. Audit records for these events are searchable by security ops, IT admins, insider risk teams, and compliance and legal investigators in your organization. This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

Generates an alert when someone is assigned administrative permissions in your Exchange Online organization. For example, when a user is added to the Organization Management role group in Exchange Online.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/audit-solutions-overview> <https://learn.microsoft.com/en-us/microsoft-365/compliance/alert-policies>

NEW QUESTION 7

- (Exam Topic 5)

You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.

You have the devices shown in the following table.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

You plan to enable co-management.

You need to identify which devices support co-management without requiring the installation of additional software.

Which devices should you identify?

- A. Device1 only
- B. Device2 only
- C. Device3 only
- D. Device2 and Device3 only
- E. Device1, Device2, and Device3

Answer: D

NEW QUESTION 8

- (Exam Topic 5)

Your company has a Microsoft 365 tenant

You plan to allow users that are members of a group named Engineering to enroll their mobile device in mobile device management (MDM)

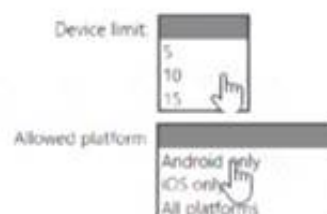
The device type restriction are configured as shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

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

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	West Region	5	Engineering
Default	All users	10	All users

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#change-enrollment-restricti>

NEW QUESTION 9

- (Exam Topic 5)

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. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.

You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to Azure AD.

Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The question states that “all the user account synchronizations completed successfully”. Therefore, the synchronization rule is configured correctly. It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

NEW QUESTION 10

- (Exam Topic 5)
Your company has a Microsoft E5 tenant.
The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.
What should you use?

- A. eDiscovery
- B. Information governance
- C. Compliance Manager
- D. Data Subject Requests (DSRs)

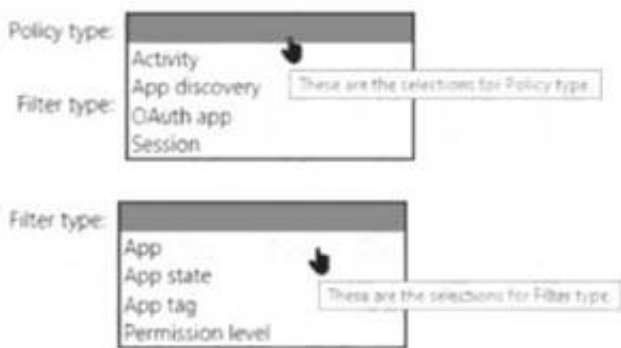
Answer: C

Explanation:
Reference:
<https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001>

NEW QUESTION 10

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to create a policy that will generate an email alert when a banned app is detected requesting permission to access user information or data in the subscription.
What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

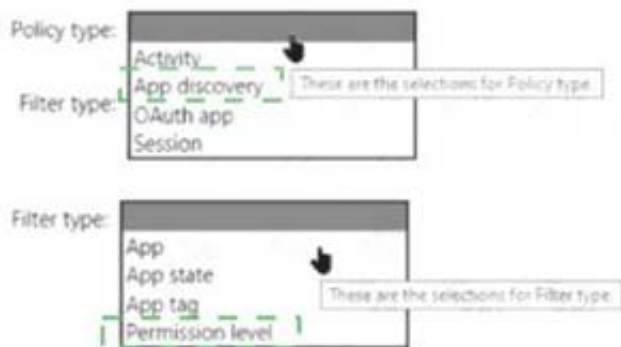
Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

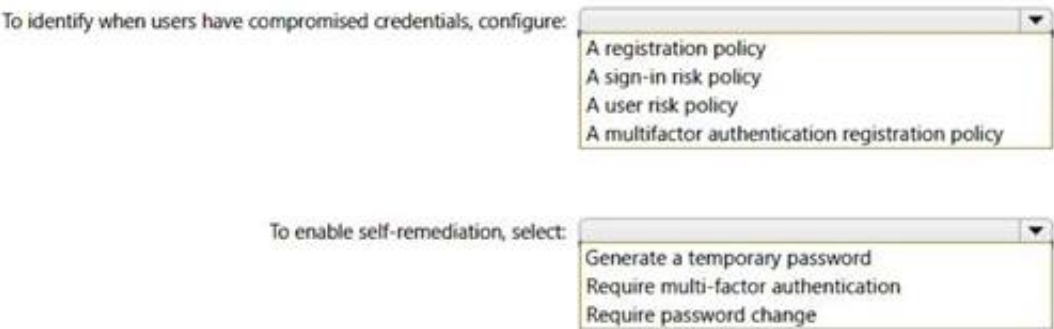
Explanation:
Answer Area



NEW QUESTION 15

- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription.
You need to implement identity protection. The solution must meet the following requirements:
➤ Identify when a user's credentials are compromised and shared on the dark web.
➤ Provide users that have compromised credentials with the ability to self-remediate. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A user risk policy

Identify when a user's credentials are compromised and shared on the dark web. User risk-based Conditional Access policy

Identity Protection analyzes signals about user accounts and calculates a risk score based on the probability that the user has been compromised. If a user has risky sign-in behavior, or their credentials have been leaked, Identity Protection will use these signals to calculate the user risk level. Administrators can configure user risk-based Conditional Access policies to enforce access controls based on user risk, including requirements such as:

Block access

Allow access but require a secure password change.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators.

Box 2: Require password change

Provide users that have compromised credentials with the ability to self-remediate.

A secure password change will remediate the user risk and close the risky user event to prevent unnecessary noise for administrators

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies#>

NEW QUESTION 19

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains the resources shown in the following table.

Name	Type
Group1	Microsoft 365 group
Group2	Distribution group
Site1	Microsoft SharePoint site

You create a sensitivity label named Label1. To which resource can you apply Label1?

- A. Group1 only
- B. Group2 only
- C. Site1 only
- D. Group1 and Group2 only
- E. Group1, Group2, and Site1

Answer: E

Explanation:

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.

In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.

When you configure a label policy, you can:

Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

NEW QUESTION 21

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.

You need to deploy the policy. What should you do first?

- A. Review the sensitive information in Activity explorer
- B. Turn on the policy
- C. Run the policy in simulation mode
- D. Configure Azure Information Protection analytics

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w>

NEW QUESTION 25

- (Exam Topic 5)

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select Update & Security to view the update history.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 28

- (Exam Topic 5)

You have three devices enrolled in Microsoft Endpoint Manager 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 Endpoint Manager 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.

Answer Area

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:

Answer Area





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 31

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

Domains

+ Add domain Buy domain Refresh		
Domain name ↑	Status	Choose columns
<input type="checkbox"/> Sub1.contoso221018.onmicrosoft.com (D...	 Possible service issues	
<input type="checkbox"/> contoso.com	 Incomplete setup	
<input type="checkbox"/> contoso221018.onmicrosoft.com	 Healthy	
<input type="checkbox"/> Sub2.contoso221018.onmicrosoft.com	 Incomplete setup	

Which domain name suffixes can you use when you create users?

- A. only Sub1.contoso221018.onmicrosoft.com
- B. onlycontoso.com and Sub2.contoso221018.onmicrosoft.com
- C. onlvcontoso221018.onmicrosoft.com, Sub.contoso221018.onmicrosoft.com, and Sub2.contoso221018.onmicrosoft.com
- D. all the domains in the subscription

Answer: B

NEW QUESTION 32

- (Exam Topic 5)

You have several devices enrolled in Microsoft Endpoint Manager.

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 Endpoint Manager are configured as shown in the following table.

Priority	Name	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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 37

- (Exam Topic 5)

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the SharePoint admin role. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

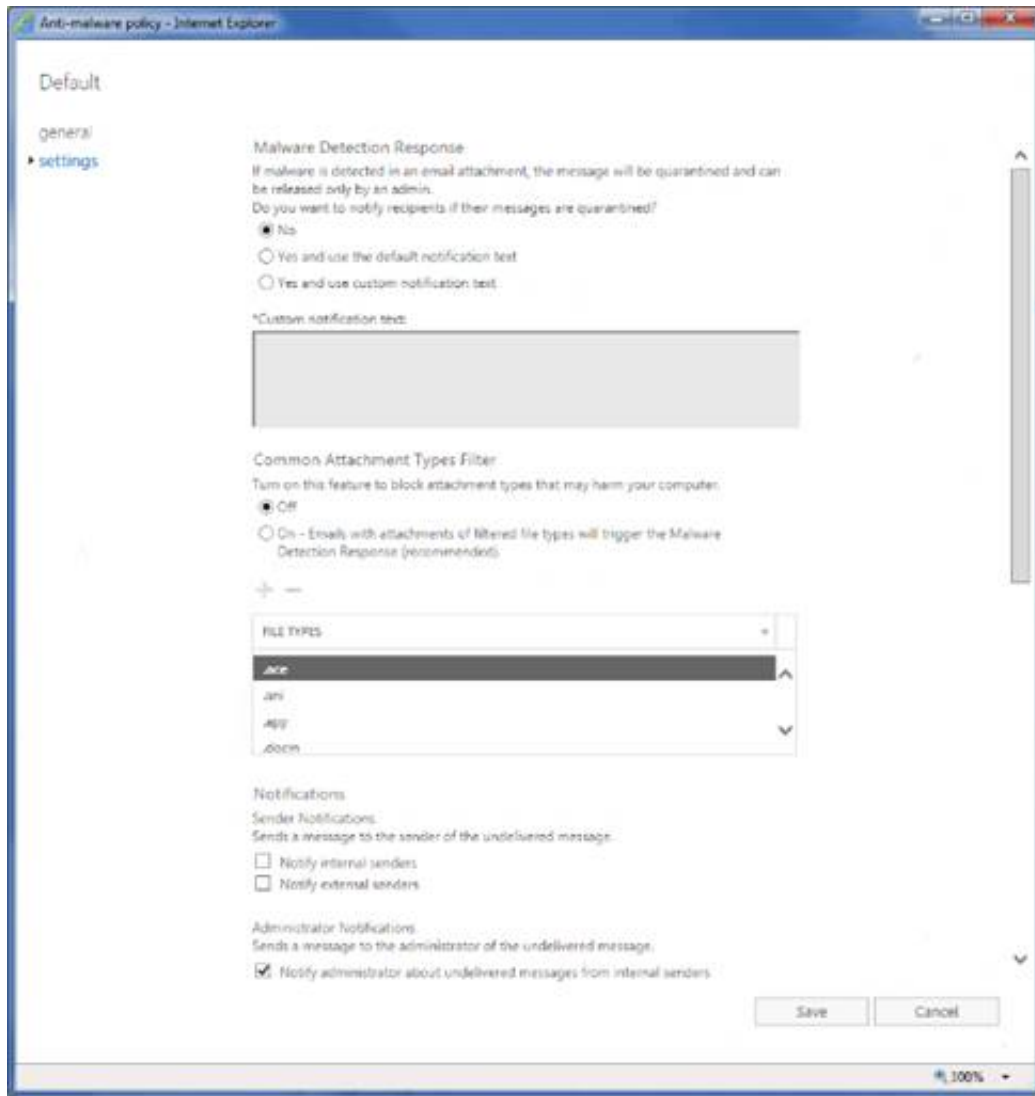
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi>

NEW QUESTION 38

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains a user named User1.

The subscription has a single anti-malware policy as shown in the following exhibit.



An email message that contains text and two attachments is sent to User1. One attachment is infected with malware. How will the email message and the attachments be processed?

- A. Both attachments will be remove
- B. The email message will be quarantined, and Used will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
- C. The email message will be quarantined, and the message will remain undelivered.
- D. Both attachments will be remove
- E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed.'
- F. The malware-infected attachment will be remove
- G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o36>

NEW QUESTION 40

- (Exam Topic 5)

You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

Name	Role
Admin1	Security reader
Admin2	User administrator
Admin3	Security administrator
Admin4	Compliance administrator

Which users will receive the weekly digest email automatically?

- A. Admin2, Admin3, and Admin4 only
- B. Admin1, Admin2, Admin3, and Admin4
- C. Admin2 and Admin3 only
- D. Admin3 only
- E. Admin1 and Admin3 only

Answer: E

Explanation:

By default, all Global Admins receive the email. Any newly created Global Admins, Security Readers or Security Administrators will automatically be added to the recipients list.

NEW QUESTION 43

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least

privilege.
Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Alert

Threat

Compliance

Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Alert

Threat

Compliance

Role:

Quarantine

Security Administrator

Organization Configuration

Communication Compliance Admin

NEW QUESTION 47

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that connects to Microsoft Defender for Endpoint. You have devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

You plan to use risk levels in Microsoft Defender for Endpoint to identify whether a device is compliant. Noncompliant devices must be blocked from accessing corporate resources.
You need to identify which devices can be onboarded to Microsoft Defender for Endpoint, and which Endpoint security policies must be configured.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Devices that can onboarded to Microsoft Defender for Endpoint:

Device 1 only

Device 1 and Device 2 only

Device 1 and Device 3 only

Device 1 and Device 4 only

Device 1, Device 2, and Device 4 only

Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

A conditional access policy only

A device compliance policy only

A device configuration profile only

A device configuration profile and a conditional access policy only

Device configuration profile, device compliance policy, and conditional access policy

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?vie>

NEW QUESTION 48

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:

- > Prevent users from enrolling personal devices.
- > Ensure that users can enroll a maximum of 10 devices.

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

Prevent users from enrolling personal devices:

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

Ensure that users can enroll a maximum of 10 devices:

Conditional access policies

Device categories

Device limit restrictions

Device type restrictions

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/mem/intune/enrollment/enrollment-restrictions-set#blocking-personal-window>

NEW QUESTION 49


- (Exam Topic 5)
HOTSPOT

Your company uses Microsoft Defender for Endpoint. Microsoft Defender for Endpoint includes the device groups shown in the following table.

Rank	Device 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 devices (default)	Not applicable

You onboard a computer named computer1 to Microsoft Defender for Endpoint as shown in the following exhibit.

Settings > Endpoints > computer1



computer1

Device summary

Risk level ⓘ

None

Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

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

Answer Area

Computer1 will be a member of [answer choice].

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

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 devices

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Group3 and Group4 only Computer1 has no Demo Tag.
Computer1 is in the adatum domain and OS is Windows 10. Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION 52

- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:
> Captures Microsoft Teams channel messages that contain threatening or violent language.
> Alerts a reviewer when a threatening or violent message is identified.
What should you include in the solution?

- A. Data Subject Requests (DSRs)
- B. Insider risk management policies
- C. Communication compliance policies
- D. Audit log retention policies

Answer: C

NEW QUESTION 56

- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	2
File4.bmp	3
File5.doc	5

The Site1 users are assigned the roles shown in the following table.

Name	Role
User1	Owner
User2	Visitor

You create a data less prevention (DLP) policy names Policy1 as shown in the following exhibit.

New DLP policy

Choose the information to protect

Name your policy

Choose locations

Policy settings

Review your settings

Review your settings

Template name

Custom policy

Edit

Policy name

Policy1

Edit

Description

Edit

Applies to content in these locations

SharePoint sites

Edit

Policy settings

If the content contains these types of sensitive info: IP Address then notify people with a policy tip and email message.

If there are at least 2 instances of the same type of sensitive info, block access to the content.

Edit

Turn policy on after it's created?

Yes

Edit

How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Passing Certification Exams Made Easy

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

Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5

NEW QUESTION 60

- (Exam Topic 5)
HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only
File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.
Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.
Box 2: Rule1 tip only
Note: User Override support
The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).
It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.
If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched. Reference:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp> <https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips>

NEW QUESTION 61

- (Exam Topic 5)
Your company has a Microsoft 365 E5 tenant.
Users at the company use the following versions of Microsoft Office:

- Microsoft 365 Apps for enterprise
- Office for the web
- Office 2016
- Office 2019

The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- xls

You plan to use sensitivity labels. You need to identify the following:

- Which versions of Office require an add-in to support the sensitivity labels.
- Which file types support the sensitivity labels.

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

Answer Area

Office versions that require an add-in to support the sensitivity labels:

Microsoft 365 Apps for enterprise and Office for the web only
Office 2016 only
Office 2019 only
Office for the web only
Office 2016 and Office 2019 only
Microsoft 365 Apps for enterprise only
Microsoft 365 Apps for enterprise and Office for the web only

Office file types that support the sensitivity labels:

.docx and .xlsx
.doc only
.docx only
.xls only
.xlsx only
.doc and .xls
.docx and .xlsx

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Office versions that require an add-in to support the sensitivity labels:

- Microsoft 365 Apps for enterprise and Office for the web only
- Office 2016 only
- Office 2019 only
- Office for the web only
- Office 2016 and Office 2019 only
- Microsoft 365 Apps for enterprise only
- Microsoft 365 Apps for enterprise and Office for the web only**

Office file types that support the sensitivity labels:

- .docx and .xlsx
- .doc only
- .docx only
- .xls only
- .xlsx only
- .doc and .xls
- .docx and .xlsx**

NEW QUESTION 63

- (Exam Topic 5)

You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

Name	Retention period	During the retention period
Retention1	5 years	Retain items even if users delete
Retention2	5 years	Mark items as a record
Retention3	5 years	Mark items as a regulatory record

Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Rename:

- File1 only
- File1 and File2 only
- File1, File2, and File3 only**
- File1, File2, File3, and File4

Delete:

- File1 only
- File1 and File2 only**
- File1, File2, and File3 only
- File1, File2, File3, and File4

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Rename:

- File1 only
- File1 and File2 only
- File1, File2, and File3 only**
- File1, File2, File3, and File4

Delete:

- File1 only
- File1 and File2 only**
- File1, File2, and File3 only
- File1, File2, File3, and File4

NEW QUESTION 64

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain. You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements: On-premises Active Directory password complexity policies must be enforced.

Users must be able to use self-service password reset (SSPR) in Azure AD.

What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection
- C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- D. pass-through authentication

Answer: D

Explanation:

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.

This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.

Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.

Password writeback is supported in environments that use the following hybrid identity models: Password hash synchronization

Pass-through authentication

Active Directory Federation Services Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

NEW QUESTION 69

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users. What is the longest time range that can be included in the report?

- A. 1 day
- B. 7 days
- C. 30 days
- D. 90 days

Answer: C

Explanation:

View email security reports in the Microsoft 365 Defender portal

The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security>

NEW QUESTION 70

- (Exam Topic 5)

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 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/pe>

NEW QUESTION 72

- (Exam Topic 5)

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

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.

Answer Area

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 word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No
 Box 2: Yes
 Box 3: No Reference:
<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies>

NEW QUESTION 74

- (Exam Topic 5)
 You have a Microsoft 365 tenant and a LinkedIn company page.
 You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector. Where can you store data from the LinkedIn connector?

- A. a Microsoft OneDrive for Business folder
- B. a Microsoft SharePoint Online document library
- C. a Microsoft 365 mailbox
- D. Azure Files

Answer: C

Explanation:

Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/archive-linkedin-data?view=o365-worldwide

NEW QUESTION 79

- (Exam Topic 5)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

Choose the types of content to protect

This policy will protect that matches these requirements. You can choose sensitive info types and existing labels

Content contains

Any of these ▾

Sensitive info type	Match accuracy		✕
	min	max	
Credit Card Number	85	100	

Retention labels

1 year ✕

Add ▾

+ Add group

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.

DLP1 cannot be applied to [answer choice].

▼

Exchange email
SharePoint sites
OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

▼

both a credit card number and the 1 year label applied
either a credit card number or the 1 year label applied
between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwid

NEW QUESTION 83

- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:

- Users and groups: Group1
- Cloud aps or actions: All cloud apps
- > Access controls:
- > Grant, require multi-factor authentication
- > Enable policy: Report-only

You set Enabled Security defaults to Yes for the tenant.
For each of the following settings select Yes, if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to On .	<input type="radio"/>	<input type="radio"/>
Admin2 can set Enable policy for Policy1 to Off .	<input type="radio"/>	<input type="radio"/>
Admin3 can set Users and groups for Policy1 to All users .	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:

- Conditional Access policies can be enabled in report-only mode.
- During sign-in, policies in report-only mode are evaluated but not enforced.
- Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-on>

NEW QUESTION 87

- (Exam Topic 5)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User1 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 88

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

Users access Microsoft 365 from both their laptop and a corporate Virtual Desktop Infrastructure (VDI) solution.

From Azure AD Identity Protection, you enable a sign-in risk policy.

Users report that when they use the VDI solution, they are regularly blocked when they attempt to access Microsoft 365.

What should you configure?

- A. the Tenant restrictions settings in Azure AD
- B. a trusted location
- C. a Conditional Access policy exclusion
- D. the Microsoft 365 network connectivity settings

Answer: B

Explanation:

There are two types of risk policies in Azure Active Directory (Azure AD) Conditional Access you can set up to automate the response to risks and allow users to self-remediate when risk is detected:

Sign-in risk policy User risk policy

Configured trusted network locations are used by Identity Protection in some risk detections to reduce false positives.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-> <https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

NEW QUESTION 92

- (Exam Topic 5)

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 E5 subscription.

You create an account for a new security administrator named SecAdmin1.

You need to ensure that SecAdmin1 can manage Microsoft Defender for Office 365 settings and policies for Microsoft Teams, SharePoint, and OneDrive.

Solution: From the Microsoft Entra admin center, you assign SecAdmin1 the Security Administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You need to assign the Security Administrator role. Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp>

NEW QUESTION 95

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Identity Protection on August 1, you configure a Multifactor authentication registration policy that has the following settings:

- > Assignments: All users
- > Controls: Require Azure AD multifactor authentication registration
- > Enforce Policy: On
- > On August 3, you create two users named User1 and User2.

Users authenticate by using Azure Multi-Factor Authentication (MFA) for the first time on the dates shown in the following table.

User	Date
User1	August 5
User2	August 7

By which dates will User1 and User2 be forced to complete their Azure MFA registration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1: ▼

- August 6
- August 17
- August 19
- September 3
- September 5

User2: ▼

- August 8
- August 17
- August 19
- August 21
- September 7

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: August 19

Note: Security defaults will trigger a 14 day grace period for registration after a user's first login and security defaults being enabled. After 14 days users will be required to register for MFA and will not be able to skip.

Conditional Access by itself without Azure Identity Protection does not allow for the 14 day grace period. Identity Protection includes the registration policy that allows registration on its own with no apps assigned to the policy. If a Conditional Access policy requires Multi-Factor Authentication, then the user must be able to pass that MFA request.

Box 2: August 21 Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

NEW QUESTION 97

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your company has a customer ID associated to each customer. The customer IDs contain 10 numbers followed by 10 characters. The following is a sample customer ID: 12-456-7890-abc-de-fghij.

You plan to create a data loss prevention (DLP) policy that will detect messages containing customer IDs. D18912E1457D5D1DDCBD40AB3BF70D5D

What should you create to ensure that the DLP policy can detect the customer IDs?

- A. a sensitive information type
- B. a sensitivity label
- C. a supervision policy
- D. a retention label

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

NEW QUESTION 99

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement device configuration profiles in Microsoft Intune. Which platform can you manage by using the profiles?

- A. Ubuntu Linux
- B. macOS
- C. Android Enterprise
- D. Windows 8.1

Answer: D

NEW QUESTION 104

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that uses Microsoft Intune.

You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

- A. scope tags
- B. device configuration profiles
- C. device categories
- D. device compliance policies

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/device-group-mapping>

NEW QUESTION 105

- (Exam Topic 5)

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 computer that runs Windows 10.

You need to verify which version of Windows 10 is installed.

Solution: From the Settings app, you select System, and then you select About to view information about the system.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628be>

NEW QUESTION 110

- (Exam Topic 5)

You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.

The tenant contains the users shown in the following table.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

You need to modify the configuration of the Defender for identify sensors.

Solutions: You instruct User4 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 115

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains devices registered for mobile device management. The devices are configured as shown in the following table.

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro for Workstations
Device3	Windows 10 Enterprise
Device4	iOS
Device5	Android

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

- A. 3
- B. 5
- C. 4
- D. 1

Answer: D

NEW QUESTION 116

- (Exam Topic 5)
 You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1, Group2
User2	Group2, Group3
User3	Group1, Group3

In Microsoft Endpoint Manager, you have the Policies for Office apps settings shown in the following table.

Name	Priority	Applies to
Policy1	0	Group1
Policy2	1	Group2
Policy3	2	Group3

The policies use the settings shown in the following table.

Name	Cursor movement	Clear cache on close
Policy1	Logical	Disabled
Policy2	Not configured	Enabled
Policy3	Visual	Enabled

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 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Graphical user interface, text, application Description automatically generated
 Reference:
<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

NEW QUESTION 117

- (Exam Topic 5)
 You have a Microsoft 365 subscription.
 Your network uses an IP address space of 51.40.15.0/24.
 An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.
 For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Activities to search for:

Exchange mailbox activities
 Site administration activities
 Show results for all activities
 Role administration activities

Field to filter by:

Item
 User
 Detail
 IP address

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Activities to search for:

▼

Exchange mailbox activities
Site administration activities
Show results for all activities
Role administration activities

Field to filter by:

▼

Item
User
Detail
IP address

NEW QUESTION 118

- (Exam Topic 5)
 You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

You plan to deploy Microsoft 365 Apps for enterprise by using Microsoft Endpoint Manager. To which devices can you deploy Microsoft 365 Apps for enterprise?

- A. Device1 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device1, Device2, and Device3 only
- E. Device1, Device2, Device3, and Device4

Answer: B

Explanation:

Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/apps-add>

NEW QUESTION 121

- (Exam Topic 5)
HOTSPOT
 You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
 Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
 Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
 Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Solutions

 Catalog

 Audit

 Content search

 Communication compliance

 Data loss prevention

 eDiscovery 

 Data lifecycle management

 Information protection

 Information barriers 

 Insider risk management

 Records management

 Privacy Risk Managem... 

 Privacy Subject Rights Requests

 Settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.

How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection

All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is

select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.

To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels: In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information Protection -> Microsoft Information Protection.

Note: Encryption of data at rest

Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.

BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology.

Box 2: Settings

Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.

- * 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
- * 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
- * 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
- * 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
- * 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.

Reference:

<https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration> <https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring>

NEW QUESTION 125

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

- > MDM user scope: Some
- > Groups: Group1
- > MAM user scope: Some
- > Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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 Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll-device-administrator

NEW QUESTION 130

- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:

- Use a file plan to manage retention labels.
- Identify, monitor, and automatically protect sensitive information.
- Capture employee communications for examination by designated reviewers.

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Capture employee communications for examination by designated reviewers:

Use a file plan to manage retention labels:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated

NEW QUESTION 131

- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Type	Department
User1	Guest	IT support
User2	Guest	SupportCore
User3	Member	IT support

You need to configure a dynamic user group that will include the guest users in any department that contains the word Support.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

(user.userType

-eq "Guest"

-in "Guest"

-ne "Guest"

-notmatch "Member"

) and (user.department

-contains "Support"

-in "Support"

-match "Support"

-startsWith "Sup"

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: -eq "Guest"

Dynamic membership rules for groups in Azure Active Directory Supported expression operators

The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.

* Equals

-eq

* Contains

-contains

* Etc.

Box 2: -contains "Support" Incorrect:

* -in

If you want to compare the value of a user attribute against multiple values, you can use the -in or -notIn operators.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

NEW QUESTION 133

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains the groups shown in the following table.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

You plan to create a compliance policy named Compliance1.

You need to identify the groups that meet the following requirements:

> Can be added to Compliance1 as recipients of noncompliance notifications

> Can be assigned to Compliance1

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Can be assigned to Compliance1:

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated

Reference:

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manage>

NEW QUESTION 136

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains the devices shown in the following table.

Name	Operating system	Tag
Device1	Windows 10	Inventory1
Computer1	Windows 10	Inventory2
Device3	Android	Inventory3

Defender for Endpoint has the device groups shown in the following table.

Rank	Name	Matching rule
1	Group1	Tag Contains Inventory And OS in Android
2	Group2	Name Starts with Device And Tag Contains Inventory
Last	Ungrouped devices (default)	Not applicable

You create an incident email notification rule configured as shown in the following table.

Setting	Value
Name	Rule1
Alert severity	Low
Device group scope	Group1, Group2
Recipient email address	User1@contoso.com

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
If a high-severity incident is triggered for Device1, an incident email notification will be sent.	<input checked="" type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Computer1, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>
If a low-severity incident is triggered for Device3, an incident notification email will be sent.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No
Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.
Box 2: No
Computer1 does not belong to either Group1 or Group2
Box 3: Yes
Device3 belongs to both Group1 and Group2. Note: Understanding alert severity
Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.
The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.
Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue>

NEW QUESTION 140

- (Exam Topic 5)
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

A. Perform a content search
B. Create a supervision policy
C. Create an eDiscovery case
D. Perform an audit log search

Answer: D

NEW QUESTION 142

- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices. You plan to attack surface reduction (ASR) rules for the Windows 10 devices. You configure the ASR rules in audit mode and collect audit data in a Log Analytics workspace. You need to find the ASR rules that match the activities on the devices.
How should you complete the Kusto query? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

AlertInfo
DeviceEvents
DeviceInfo

| ActionType startswith 'ASR'

lookup
project
render
where

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application Description automatically generated

Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction>

NEW QUESTION 145

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation.

You need to run a PowerShell script on the device to collect forensic information. Which action should you select on the device page?

- A. Initiate Live Response Session
- B. Initiate Automated Investigation
- C. Collect investigation package
- D. Go hunt

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwid>

NEW QUESTION 149

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains 1,000 Windows 10 devices. The devices are enrolled in Microsoft Intune.

Company policy requires that the devices have the following configurations:

- > Require complex passwords.
- > Require the encryption of removable data storage devices.
- > Have Microsoft Defender Antivirus real-time protection enabled.

You need to configure the devices to meet the requirements. What should you use?

- A. an app configuration policy
- B. a compliance policy
- C a security baseline profile
- D a conditional access policy

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started>

NEW QUESTION 151

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You discover that some external users accessed center for 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 Security & Compliance admin center you create a threat management policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 152

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None

New audit retention policy
✕

Name *:

Description

Record Types

Activities

Users:

Duration *:

☐ 90 Days
☒ 6 Months
☐ 1 Year

Priority *:

You plan to create a new user named User1.
 How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.
 Each correct selection is worth one point.

Admin1:

▾

30 days

90 days

6 months

1 year

Admin2:

▾

30 days

90 days

6 months

1 year

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Admin1:

▾

30 days

90 days

6 months

1 year

Admin2:

▾

30 days

90 days

6 months

1 year

NEW QUESTION 154

- (Exam Topic 5)

Your company has a Microsoft 365 subscription. you implement sensitivity Doris for your company.

You need to automatically protect email messages that contain the word Confidential m the subject line. What should you create?

- A. a sharing policy from the Exchange admin center
- B. a mail flow rule from the Exchange admin center
- C. a message Dace from the Microsoft 365 security center
- D. a data loss prevention (DLP) policy from the Microsoft 365 compliance center

Answer: B

NEW QUESTION 157

- (Exam Topic 5)

You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	Source	Last sign in
User1	Azure AD	Yesterday
User2	Active Directory Domain Services (AD DS)	Two days ago
User3	Active Directory Domain Services (AD DS)	Never

Azure AD Connect has the following settings:

- > Password Hash Sync: Enabled
- > Pass-through authentication: Enabled

You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost. Which users should you identify?

- A. none
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION 160

- (Exam Topic 5)

You have a Microsoft E5 subscription.

You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time. What should you implement?

- A. Azure AD Privileged Identity Management (PIM)
- B. a conditional access policy
- C. a communication compliance policy)
- D. Azure AD Identity Protection
- E. groups that have dynamic membership

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-def>

NEW QUESTION 161

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

- > Scope type: Directory
- > Selected members: Group1
- > Assignment type: Active
- > Assignment starts: Mar 15, 2023
- > Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

- > Scope type: Directory
- > Selected members: Group2
- > Assignment type: Eligible
- > Assignment starts: Jun 15, 2023
- > Assignment ends: Oct 15, 2023

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
On July 15, 2023, Admin1 can reset the password of a user.	<input type="radio"/>	<input type="radio"/>
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	<input type="radio"/>	<input type="radio"/>
On May 1, 2023, Admin3 can reset the password of a user.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member. The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible

June 20, 2023 is with the assignment period. The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

Admin3 is member of Group1 and Group2.

The User Administrator role assignment has Group1 as a member.

The assignment type: Active

May 1, 2023 is with the assignment period. Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference> <https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member>

NEW QUESTION 165

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Microsoft 365 role
User1	Cloud application administrator
User2	Application administrator
User3	Application developer
User4	None

Users are assigned Microsoft Store for Business roles as shown in the following table.

User	Role
User1	None
User2	Basic Purchaser
User3	Purchaser
User4	Device Guard signer

Which users can add apps to the private store in Microsoft Store for Business, and which users can install apps from the private store? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Add apps to the private store:

Install apps from the private store:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text Description automatically generated

Reference:

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

NEW QUESTION 170

- (Exam Topic 5)

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 on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings. You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You upgrade Server1 to Windows Server 2019.

Does this meet the goal?

- A. yes
- B. No

Answer: A

NEW QUESTION 175

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that contains the devices shown in the following table.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

You plan to review device startup performance issues by using Endpoint analytics. Which devices can you monitor by using Endpoint analytics?

- A. Device1 only
- B. Device1 and Device2 only
- C. Device1, Device2, and Device3 only
- D. Device1, Device2, and Device4 only
- E. Device1, Device2, Device3, and Device4

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION 178

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to ensure that when a document containing a credit card number is added to the tenant, the document is encrypted.

Which policy should you use?

- A. a retention policy
- B. a retention label policy
- C. an auto-labeling policy
- D. an insider risk policy

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w>

NEW QUESTION 180

- (Exam Topic 5)

Your on-premises network contains an Active Directory domain named Contoso.com and 500 devices that run either macOS, Windows 8.1. Windows 10, or Windows 11. All the devices are managed by using Microsoft Endpoint Configuration Manager. The domain syncs with Azure Active Directory (Azure AD).

You plan to implement a Microsoft 365 E5 subscription and enable co-management. Which devices can be co-managed after the implementation?

- A. Windows 11 and Windows 10 only
- B. Windows 11, Windows 10-Windows8.1.andmacOS

- C. Windows 11 and macOS only
- D. Windows 11 only
- E. Windows 11. Windows 10, and Windows8.1 only

Answer: C

NEW QUESTION 185

.....

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-102 Practice Exam Features:

- * MS-102 Questions and Answers Updated Frequently
- * MS-102 Practice Questions Verified by Expert Senior Certified Staff
- * MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The MS-102 Practice Test Here](#)