

Microsoft.MS-101.v2023-10-10.q197

Exam Code:	MS-101
Exam Name:	Microsoft 365 Mobility and Security
Certification Provider:	Microsoft
Free Question Number:	197
Version:	v2023-10-10
# of views:	1841
# of Questions views:	1970
https://www.freepdfdumps.com/Microsoft.MS-101.v2023-10-10.q197.html	

NEW QUESTION: 1

You have a Microsoft 365 E5 tenant

You create a data loss prevention (DLP) policy to prevent users from using Microsoft Teams to share internal documents with external users.

To which two locations should you apply the policy? To answer, select the appropriate locations in the answer area.

NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

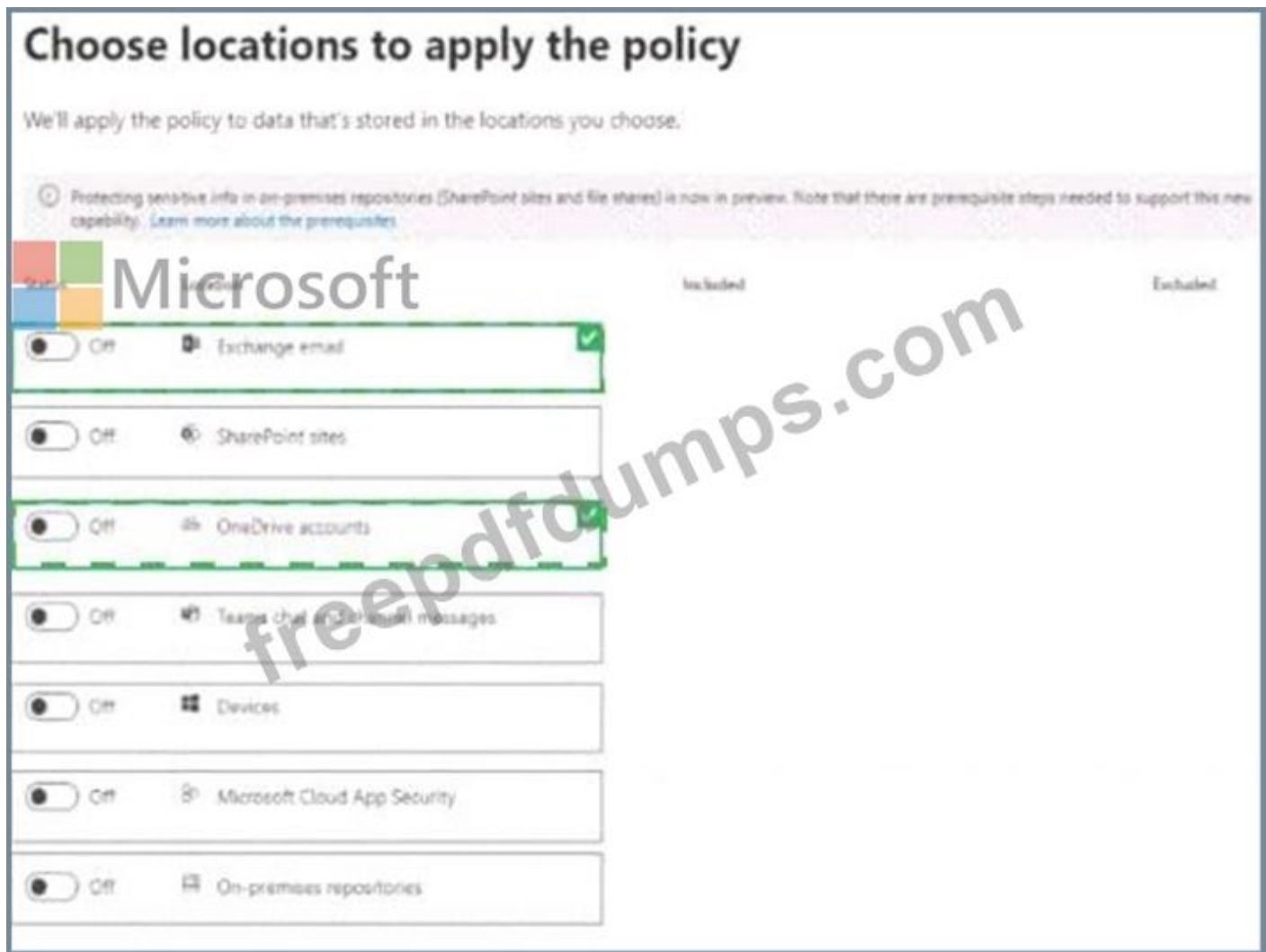
We'll apply the policy to data that's stored in the locations you choose.

Protecting sensitive info in on-premises repositories (SharePoint sites and file shares) is now in preview. Note that there are prerequisite steps needed to support this new capability. [Learn more about the prerequisites](#)

Status	Location	Included	Excluded
☒ On	Exchange email	☒	☐
☐ Off	SharePoint sites	☐	☐
☒ On	OneDrive accounts	☒	☐
☐ Off	Teams chat and channel messages	☐	☐
☐ Off	Devices	☐	☐
☐ Off	Microsoft Cloud App Security	☐	☐
☐ Off	On-premises repositories	☐	☐

Microsoft

Answer:



NEW QUESTION: 2

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

- A. Microsoft Store for Business
- B. Apple Business Manager
- C. Apple iTunes Store
- D. Apple Configurator

Answer: B ([LEAVE A REPLY](#))

Reference:

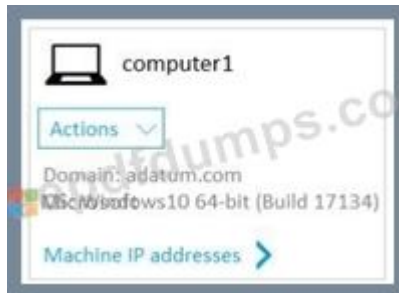
<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

NEW QUESTION: 3

Your company uses Microsoft Defender Advanced Threat Protection (ATP). Microsoft 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 Microsoft Defender ATP as shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement.

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

Answer:

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

Explanation

According to this article

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

- If a machine is also matched to other groups, it is added only to the highest ranked machine group. Part 1 answer should be - computer 1 will be a member of - Group 3 only.

Because its the highest rank and the machine is part of adatum.com Part 2 - if you add the tag demo to computer 1. then the answer should be group 1 only.
Because the machine is tagged "demo" and OS is windows 10.

NEW QUESTION: 4

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

- * Retention period 7 years
- * Start the retention period based on: When items were created

You need to prevent the removal of the label once the label is applied to an item. What should you select in the retention label settings?

- A. Mark items as a regulatory record
- B. Mark items as a record
- C. Retain items even if users delete
- D. Retain items forever

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 5

You have a Microsoft 365 subscription.

From Microsoft 365 Defender, 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 ([LEAVE A REPLY](#))

NEW QUESTION: 6

Your company has a Microsoft 365 subscription that contains the domains shown in the following table.

 Name	Can enroll devices to Microsoft Intune by using auto-discovery
Contoso.com	Yes
Contoso.onmicrosoft.com	Yes

The company plans to add a custom domain named fabrikam.com to the subscription and then to enable enrollment of devices to Intune by using auto discovery for fabrikam.com.

You need to add a DNS record to the fabrikam.com zone.

Which record type should you use for the new record?

- A. SRV
- B. PTR
- C. CNAME
- D. TXT

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 7

You have a Microsoft 365 subscription.

Some users have iPads that are managed by your company.

You plan to prevent the iPad users from copying corporate data in Microsoft Word and pasting the data into other applications.

What should you create?

- A. an app configuration policy
- B. a compliance policy
- C. a Conditional MOMS policy
- D. an app protection policy

Answer: D ([LEAVE A REPLY](#))

Explanation

References:

<https://docs.microsoft.com/en-us/intune/app-protection-policy>

NEW QUESTION: 8

Your company has a Microsoft 365 subscription.

You need to configure Microsoft 365 to meet the following requirements:

- * Malware found in email attachments must be quarantined for 20 days.
- * The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

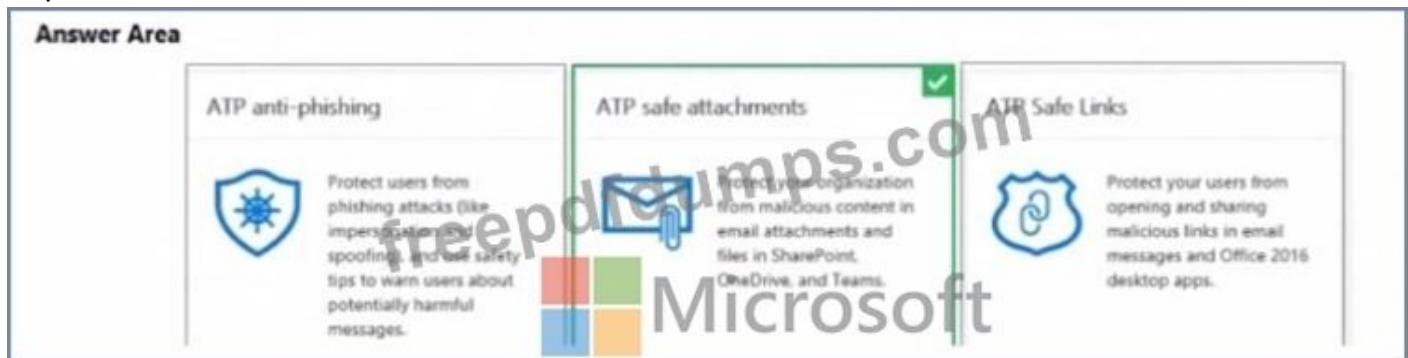
NOTE: Each correct selection is worth one point.



Answer:



Explanation



NEW QUESTION: 9

You need to meet the technical requirement for the EU PII data.

What should you create?

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

Answer: (SHOW ANSWER)

Explanation

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies> EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION: 10

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 ([LEAVE A REPLY](#))

NEW QUESTION: 11

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices. The devices are enrolled in Microsoft intune.

You plan to use Endpoint analytics to identify hardware issues.

You need to enable Window health monitoring on the devices to support Endpoint analytics What should you do?

- A. Create a compliance policy.
- B. Create a Windows 10 Security Baseline profile
- C. Configure the Endpoint analytics baseline regression threshold.
- D. Create a configuration profile.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 12

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

Answer:

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	

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: 13

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 content 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

1year

×

Add ▼

+ Add group



Microsoft

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 will be applied only to documents that have [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 1year label applied
either a credit card number or the 1year label applied
between 85 and 100 credit card numbers

Answer:

DLP1 will be applied only to documents that have [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 1year label applied
either a credit card number or the 1year label applied
between 85 and 100 credit card numbers



Microsoft

Explanation

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

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

Exchange email
SharePoint sites
OneDrive accounts

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

NEW QUESTION: 14

You have a Microsoft 365 subscription.

You plan to connect to Microsoft Exchange Online PowerShell and run the following cmdlets:

- * Search-MailboxAuditLog
- * Test-ClientAccessRule
- * Set-GroupMailbox
- * Get-Mailbox

Which cmdlet will generate an entry in the Microsoft Office 365 audit log?

- A. Search-MailboxAuditLog
- B. Test-ClientAccessRule
- C. Set-GroupMailbox
- D. Get-Mailbox

D18912E1457D5D1DDCBD40AB3BF70D5D

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vie>

NEW QUESTION: 15

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			

Answer:

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

		▼	ActionType startswith 'ASR'
lookup			
project			
render			
where			

Explanation

Graphical user interface, application Description automatically generated

	▼
AlertInfo	
DeviceEvents	
DeviceInfo	

	▼
lookup	
project	
render	
where	

ActionType startswith 'ASR'



Reference:

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

NEW QUESTION: 16

You have a data loss prevention (DLP) 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  Microsoft

Any of these ▼

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min	max
1	any

Match accuracy

min	max
50	100

Add ▼

and ▼

Any of these ▼

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min	max
1	any

Match accuracy

min	max
50	100

Add ▼

Answer:

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 ▼

Explanation

The screenshot shows the Microsoft Azure portal interface for configuring Sensitive Information Types (SITs). It is divided into two main sections: "PII Identifiers" and "Medical Terms".

PII Identifiers Section:

- Sensitive info type:** A dropdown menu currently shows "U.S. Social Security Number (SSN)". Below it is an "Add" button.
- Instance count:** Two buttons are shown: "min" with the value "1" and "max" with the value "any".
- Match accuracy:** Two buttons are shown: "min" with the value "50" and "max" with the value "100".
- Below the instance count and match accuracy buttons are two more dropdown menus, one labeled "and" and another labeled "Any of these".

Medical Terms Section:

- Sensitive info type:** A dropdown menu currently shows "International Classification of Diseases (ICD-9-CM)". Below it is an "Add" button.
- Instance count:** Two buttons are shown: "min" with the value "1" and "max" with the value "any".
- Match accuracy:** Two buttons are shown: "min" with the value "50" and "max" with the value "100".

A large diagonal watermark "freepdfdumps.com" is visible across the center of the image.

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#in>

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 17

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: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 18

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

Answer: B,C ([LEAVE A REPLY](#))

NEW QUESTION: 19

You have a Microsoft 365 E5 tenant.

You configure sensitivity labels.

Users report that the Sensitivity button is unavailable in Microsoft Word for the web. The sensitivity button is available in Word for Microsoft 365.

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

- A. Publish the sensitivity labels.
- B. Create an auto-labeling policy
- C. Enable sensitivity labels for files in Microsoft SharePoint Online and OneDrive.
- D. Copy policies from Azure information Protection to the Microsoft 365 Compliance center

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 20

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 ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 21

You use Microsoft Defender for Endpoint.

You have the Microsoft Defender for Endpoint device groups shown in the following table

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	4	Not applicable

You plan to onboard computers to Microsoft Defender for Endpoint as shown in the following table.

ANSWER AREA

	
Computer1-London:	Group1 Group2 Group3 Ungrouped machines
Server1-London:	Group1 Group2 Group3 Ungrouped machines

Answer:



Explanation

Answer Area

Computer1-London:

Server1-London:

NEW QUESTION: 22

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps. You need to be notified when a single user downloads more than 50 files during any 60-second period.

What should you configure?

- A. a file policy
- B. a session policy
- C. an anomaly detection policy
- D. an activity policy

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 23

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 2,000 computers that run Windows 8.1 and have applications installed as shown in the following table.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You enroll all the computers in Upgrade Readiness.

You need to ensure that App1 and App2 have an UpgradeDecision status of Ready to upgrade.

Solution: You set the importance status of App2 to Low install count.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Explanation

If an app is installed on less than 2% of the targeted devices, it's marked Low install count. Two percent is the default value. You can adjust the threshold in the readiness settings from 0% to 10%. Desktop Analytics automatically marks these apps as Ready to upgrade.

Reference:

<https://docs.microsoft.com/en-us/configmgr/desktop-analytics/about-deployment-plans>

NEW QUESTION: 24

You have Microsoft 365 subscription.

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

Policy1

Edit policy

Delete policy

Status	On
Description	Description
Severity	Low Edit
Category	Threat management
Conditions	Activity is Detected malware in file
Aggregation	Aggregated
Threshold	20 activities Edit
Window	120 minutes
Scope	All users

Email recipients	User1@sk190107outlook.onmicrosoft.com
Daily notification limit	100 Edit

Close

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.

Policy1 will trigger an alert if malware is detected in

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

5
12
20
100

Answer:

Policy1 will trigger an alert if malware is detected in

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

5
12
20
100

Explanation

Policy1 will trigger an alert if malware is detected in

Exchange Online only
SharePoint Online only
SharePoint Online or OneDrive only
Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is

5
12
20
100

Note: The Aggregation settings has a 120 minute window

NEW QUESTION: 25

You have a Microsoft 365 subscription.

You plan to enable Microsoft Azure Information Protection.

You need to ensure that only the members of a group named PilotUsers can protect content.

What should you do?

- A. Run the Add-AadrmRoleBasedAdministrator cmdlet.
- B. Create an Azure Information Protection policy.

C. Configure the protection activation status for Azure Information Protection.

D. Run the Set-AadrmOnboardingControlPolicy cmdlet.

Answer: ([SHOW ANSWER](#))

Reference:

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

NEW QUESTION: 26

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains computers that run Windows 10 Enterprise and are managed by using Microsoft Intune. The computers are configured as shown in the following table.

Name	CPU	Cores	RAM	TPM
Computer1	64-bit	2	12 GB	Enabled
Computer2	64-bit	4	12 GB	Enabled
Computer3	64-bit	8	16 GB	Disabled
Computer4	32-bit	4	4 GB	Disabled

You plan to implement Windows Defender Application Guard for contoso.com.

You need to identify on which two Windows 10 computers Windows Defender Application Guard can be installed.

Which two computers should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Computer1

B. Computer3

C. Computer2

D. Computer4

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-w>

NEW QUESTION: 27

You have Windows 10 devices that are managed by using Microsoft Endpoint Manager.

You need to configure the security settings in Microsoft Edge.

What should you create in Microsoft Endpoint Manager?

A. an app configuration policy

B. an app

C. a device configuration profile

D. a device compliance policy

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune>

NEW QUESTION: 28

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy. You need to identify the following information:

- * The number of email messages quarantined by zero-hour auto purge (ZAP)
 - * The number of times users clicked a malicious link in an email message
- Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

Answer:

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report ▼
Mailflow status report
Spoof detections
Threat protection status
URL threat protection

Explanation

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status ▼

To identify the number of times users clicked a malicious link in an email:

Mailflow status report ▼

NEW QUESTION: 29

You have a Microsoft 365 subscription.

You need to create a data loss prevention (DLP) policy that is configured to use the Set headers action.

To which location can the policy be applied?

- A. Exchange email
- B. Teams chat and channel messages
- C. OneDrive accounts
- D. SharePoint sites

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 30

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 User3 to modify the Defender for identity sensor configuration.

Does this meet the goal?

- A. Yes
- B. No

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 31

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: ([SHOW ANSWER](#)**)**

Explanation

References:

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

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

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101

exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 32

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.	☐	☐
User2 has Cursor movement set to Visual.	☐	☐
User3 has Cursor movement set to Visual.	☐	☐

Answer:

Statements	Yes	No
User1 has their cache cleared on close.	☐	☒
User2 has Cursor movement set to Visual.	☐	☒
User3 has Cursor movement set to Visual.	☐	☒

Explanation

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
User1 has their cache cleared on close.	☐	☐
User2 has Cursor movement set to Visual.	☐	☐
User3 has Cursor movement set to Visual.	☐	☐

Reference:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

NEW QUESTION: 33

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: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 34

On which server should you use the Defender for identity sensor?

- A. Server1
- B. Server2
- C. Server3

- D. Server4
- E. Servers5

Answer: ([SHOW ANSWER](#))

Explanation

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

NEW QUESTION: 35

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The screenshot shows the configuration interface for Azure Active Directory audit logs. It includes two dropdown menus. The first dropdown, labeled 'Save the audit logs to:', is currently empty. The second dropdown, labeled 'Azure Active Directory admin center blade to use to view the saved audit logs:', is also empty. The Microsoft logo is visible in the background.

Answer:

See the answer below

Answer Area

The screenshot shows the configuration interface for Azure Active Directory audit logs with selections. The first dropdown, labeled 'Save the audit logs to:', is set to 'Azure Log Analytics'. The second dropdown, labeled 'Azure Active Directory admin center blade to use to view the saved audit logs:', is set to 'Audit logs'. The Microsoft logo is visible in the background.

NEW QUESTION: 36

You have a Microsoft 365 E5 tenant.

You plan to create a custom Compliance Manager assessment template based on the ISO 27001:2013 template.

You need to export the existing template.

Which file format should you use for the exported template?

- A. CSV
- B. XLSX
- C. JSON
- D. XML

Answer: B ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-templates?view=o365-worldw>

NEW QUESTION: 37

Your network contains an Active Directory domain named contoso.com that uses Microsoft System Center Configuration Manager (Current Branch).

You have Windows 10 and Windows 8.1 devices.

You need to ensure that you can analyze the upgrade readiness of all the Windows 8.1 devices and analyze the update compliance of all the Windows 10 devices.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

First action to perform:

☐	Enroll the devices in Microsoft Intune.
☐	Configure device compliance in Microsoft Intune.
☐	Create a Microsoft Azure Log Analytics workspace.
☐	Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

☐	Configure all the devices to have a commercial ID.
☐	Configure software inventory in Configuration Manager.
☐	Configure all the devices to join the Windows Insider Program.
☐	Configure and restart the Windows Update service on all the devices.

Answer:

First action to perform:	<table border="1"><tr><td>☐</td><td>Enroll the devices in Microsoft Intune.</td></tr><tr><td>☐</td><td>Configure device compliance in Microsoft Intune.</td></tr><tr><td>☒</td><td>Create a Microsoft Azure Log Analytics workspace.</td></tr><tr><td>☐</td><td>Add an alias (CNAME) record to the DNS zone of contoso.com.</td></tr></table>	☐	Enroll the devices in Microsoft Intune.	☐	Configure device compliance in Microsoft Intune.	☒	Create a Microsoft Azure Log Analytics workspace.	☐	Add an alias (CNAME) record to the DNS zone of contoso.com.
☐	Enroll the devices in Microsoft Intune.								
☐	Configure device compliance in Microsoft Intune.								
☒	Create a Microsoft Azure Log Analytics workspace.								
☐	Add an alias (CNAME) record to the DNS zone of contoso.com.								
Second action to perform:	<table border="1"><tr><td>☒</td><td>Configure all the devices to have a commercial ID.</td></tr><tr><td>☐</td><td>Configure software inventory in Configuration Manager.</td></tr><tr><td>☐</td><td>Configure all the devices to join the Windows Insider Program.</td></tr><tr><td>☐</td><td>Configure and restart the Windows Update service on all the devices.</td></tr></table>	☒	Configure all the devices to have a commercial ID.	☐	Configure software inventory in Configuration Manager.	☐	Configure all the devices to join the Windows Insider Program.	☐	Configure and restart the Windows Update service on all the devices.
☒	Configure all the devices to have a commercial ID.								
☐	Configure software inventory in Configuration Manager.								
☐	Configure all the devices to join the Windows Insider Program.								
☐	Configure and restart the Windows Update service on all the devices.								

Explanation

First action to perform:	<table border="1"><tr><td>☐</td><td>Enroll the devices in Microsoft Intune.</td></tr><tr><td>☐</td><td>Configure device compliance in Microsoft Intune.</td></tr><tr><td>☒</td><td>Create a Microsoft Azure Log Analytics workspace.</td></tr><tr><td>☐</td><td>Add an alias (CNAME) record to the DNS zone of contoso.com.</td></tr></table>	☐	Enroll the devices in Microsoft Intune.	☐	Configure device compliance in Microsoft Intune.	☒	Create a Microsoft Azure Log Analytics workspace.	☐	Add an alias (CNAME) record to the DNS zone of contoso.com.
☐	Enroll the devices in Microsoft Intune.								
☐	Configure device compliance in Microsoft Intune.								
☒	Create a Microsoft Azure Log Analytics workspace.								
☐	Add an alias (CNAME) record to the DNS zone of contoso.com.								
Second action to perform:	<table border="1"><tr><td>☒</td><td>Configure all the devices to have a commercial ID.</td></tr><tr><td>☐</td><td>Configure software inventory in Configuration Manager.</td></tr><tr><td>☐</td><td>Configure all the devices to join the Windows Insider Program.</td></tr><tr><td>☐</td><td>Configure and restart the Windows Update service on all the devices.</td></tr></table>	☒	Configure all the devices to have a commercial ID.	☐	Configure software inventory in Configuration Manager.	☐	Configure all the devices to join the Windows Insider Program.	☐	Configure and restart the Windows Update service on all the devices.
☒	Configure all the devices to have a commercial ID.								
☐	Configure software inventory in Configuration Manager.								
☐	Configure all the devices to join the Windows Insider Program.								
☐	Configure and restart the Windows Update service on all the devices.								

References:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started>

<https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started>

NEW QUESTION: 38

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: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 39

Your company has a Microsoft 365 E5 subscription.

Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents. Users in other departments must not be restricted.

What should you do from the Security & Compliance admin center?

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

Answer: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 40

You have a Microsoft 365 tenant named Contoso.com. the tenant contains the users shown in the following table.

Name	Azure AD role	Microsoft Office 365 role group
User1	Application administrator	eDiscovery Administrator
User2	Application administrator	Organization Management
User3	Cloud application administrator	Global Administrator
User4	Compliance administrator	eDiscovery Manager

You have an eDiscovery case shown in the follow table.

Name	Created by
Case1	User1
Case2	User2
Case3	User3
Case4	User4

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 delete Case4.	☐	☐
User3 can add members to Case2.	☐	☐
User4 can close Case3.	☐	☐

Answer:

Statements	Yes	No
User1 can delete Case4.	☐	☒
User3 can add members to Case2.	☐	☒
User4 can close Case3.	☒	☐

NEW QUESTION: 41

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

- A. Microsoft Defender for CloudUse the
- B. Microsoft Purview
- C. Azure Arc
- D. Microsoft Defender for Identity

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

NEW QUESTION: 42

You have a Microsoft 365 E5 subscription. The subscription contains users that have the following types of devices:

- * Windows 10
- * Android
- * OS

On which devices can you configure the Endpoint DLP policies?

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

Answer: C ([LEAVE A REPLY](#))

Explanation

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.

<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

NEW QUESTION: 43

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.

To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group: ▼

Reviewer
Global reader
Data Investigator
Compliance Management

Tool: ▼

Exchange admin center
SharePoint admin center
Microsoft 365 admin center
Microsoft 365 security center

Answer:

Role group: Microsoft ▼

Reviewer
Global reader
Data Investigator
Compliance Management

Tool: ▼

Exchange admin center
SharePoint admin center
Microsoft 365 admin center
Microsoft 365 security center

Explanation

Graphical user interface, text Description automatically generated

Role group:  Microsoft ▼

- Reviewer
- Global reader
- Data Investigator
- Compliance Management

Tool: ▼

- Exchange admin center
- SharePoint admin center
- Microsoft 365 admin center
- Microsoft 365 security center

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vie>

NEW QUESTION: 44

A user named User1 has files in Microsoft OneDrive as shown in the following table.

Name	Date created	Date last modified
File1	January 1, 2019	January 16, 2019
File2	January 15, 2019	January 20, 2019

On February 1, 2019, you apply a retention policy named Policy1 as shown in the following exhibit.

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

Do you want to retain content? ⓘ

☒ Yes, I want to retain it ⓘ

For this long... 1 months

Retain the content based on when it was last modified ⓘ

Do you want us to delete it after this time? ⓘ

☒ Yes ☐ No

☐ No, just delete content that's older than ⓘ

1 years

Need more options?

☐ Use advanced retention settings ⓘ

Back Next Cancel

On February 5, 2019, User1 edits File2.

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
On March 1, 2019, File 1 is deleted automatically.	☐	☐
On February 20, 2019, File 2 is available in OneDrive.	☐	☐
On March 5, 2019, File 2 is deleted automatically.	☐	☐

Answer:

 Statements	Yes	No
On March 1, 2019, File 1 is deleted automatically.	☒	☐
On February 20, 2019, File 2 is available in OneDrive.	☒	☐
On March 5, 2019, File 2 is deleted automatically.	☒	☐

Explanation

 Statements	Yes	No
On March 1, 2019, File 1 is deleted automatically.	☐	☐
On February 20, 2019, File 2 is available in OneDrive.	☐	☐
On March 5, 2019, File 2 is deleted automatically.	☐	☐

NEW QUESTION: 45

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

You need to ensure that user access to Dropbox is authenticated by using a Microsoft 365 identify.

The documents must be protected if the data is downloaded to an untrusted device.

What should you do?

A. From the Azure Active Directory admin center, configure the Organizational relationships settings

B. From the Azure Active Directory admin center, configure the Devices settings.

C. From the Intune admin center, configure the Conditional access settings.

D. From the Azure Active Directory admin center, configure the Application proxy settings.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 46

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 data admin role.

Does this meet the goal?

A. Yes

B. No

Answer: B ([LEAVE A REPLY](#))

Reference:

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

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 47

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 only
- C. Windows 11, Windows 10, and Windows 8.1 only
- D. Windows 11, Windows 10, Windows 8.1, and macOS
- E. Windows 11 and macOS only

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 48

Your company has a Microsoft 365 E5 tenant.

Users access resources in the tenant by using both personal and company-owned Android devices. Company policies requires that the devices have a threat level of medium or lower to access Microsoft Exchange Online mailboxes.

You need to recommend a solution to identify the threat level of the devices and to control access of the devices to the resources.

What should you include in the solution for each device type? To answer, drag the appropriate components to the correct devices. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solutions	Answer Area
An app configuration policy	Company-owned devices: Solution
An app protection policy	Personal devices: Solution
A compliance policy	
A configuration profile	

Microsoft

freepdfdumps.com

Answer:

Solutions	Answer Area
An app configuration policy	Company-owned devices: A compliance policy
An app protection policy	Personal devices: An app protection policy
A compliance policy	
A configuration profile	



Explanation

Graphical user interface, application, Word Description automatically generated

Company-owned devices:

A compliance policy

Personal devices:

An app protection policy



NEW QUESTION: 49

You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.

You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.

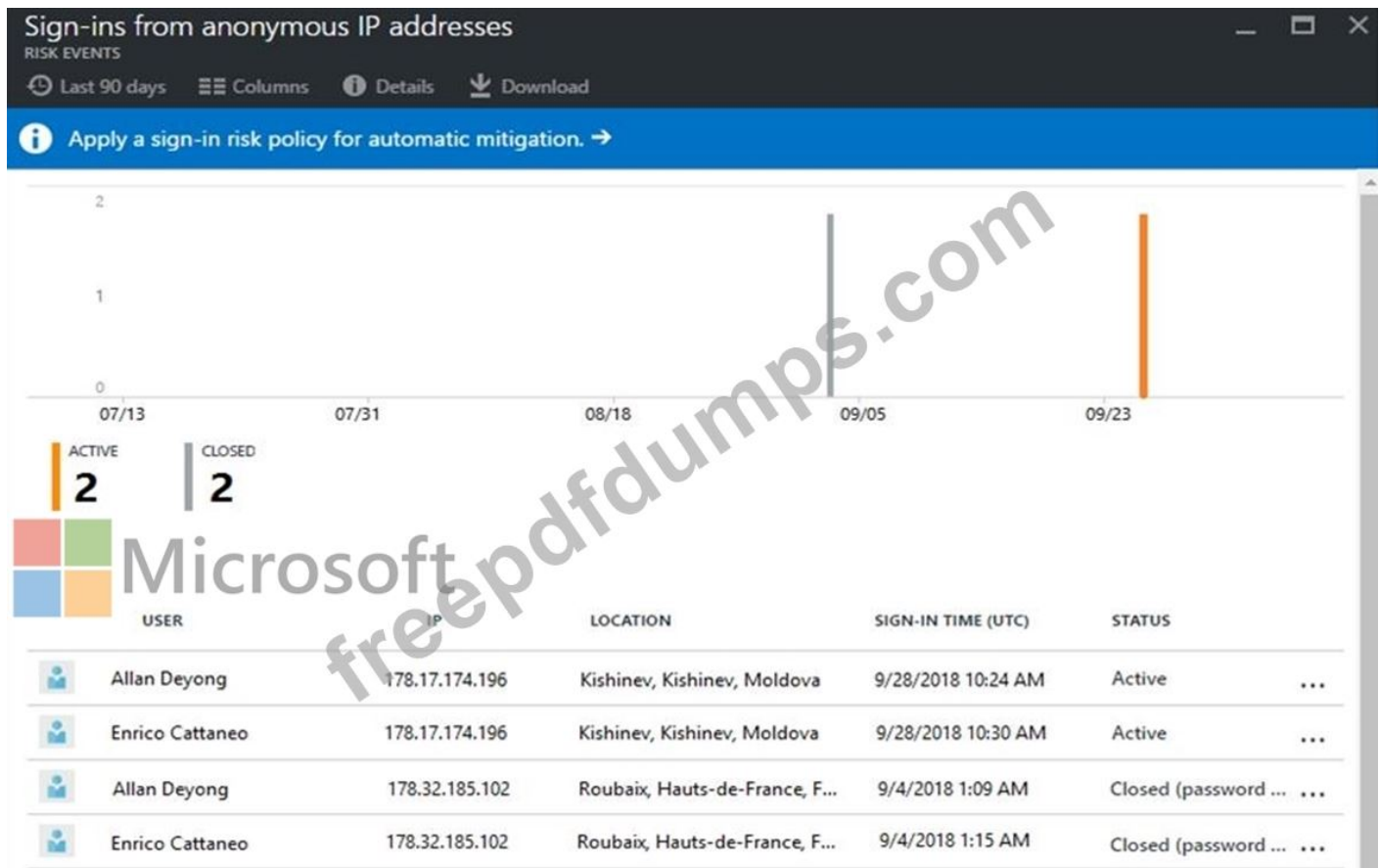
What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 50

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 (LEAVE A REPLY)

Explanation

References:

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

NEW QUESTION: 51

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

Name	Owner	Installed apps	Platform	Microsoft Intune
Device1	User1	None	Windows 10	Enrolled
Device2	User2	App2	Android	Not enrolled
Device3	User3	None	iOS	Not enrolled

You have the apps shown in the following table.

Name	Type
App1	iOS store app
App2	Android store app
App3	Microsoft store app

You plan to use Microsoft Endpoint Manager to manage the apps for the users.

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
App1 can be assigned as a required install for User3.	☐	☐
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	☐	☐
App3 can be installed automatically for UserGroup1.	☐	☐

Answer:

Statements	Yes	No
App1 can be assigned as a required install for User3.	☐	☐
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	☐	☐
App3 can be installed automatically for UserGroup1.	☐	☐

Explanation

Graphical user interface, text, application Description automatically generated

Statements	Yes	No
App1 can be assigned as a required install for User3.	☐	☐
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	☐	☐
App3 can be installed automatically for UserGroup1.	☐	☐

Reference:

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

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>

NEW QUESTION: 52

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records.

You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

- A. Configure custom detection rules.
- B. Create an Exact Data Match (EDM) schema.
- C. Run the Sec-RegulatoryComplianceUI cmdlet.
- D. Run the Sec-LabelPolicy cmdlet.

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/declare-records?view=o365-worldwide>

NEW QUESTION: 53

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
--	--	--	---

Answer:

Set-ComplianceTag Set-HoldCompliancePolicy Set-RetentionCompliancePolicy Set-RetentionPolicy Set-RetentionPolicyTag	-Identity "Policy1"	-enabled -Force -RestrictiveRetention -RetentionPolicyTagLinks -SystemTag	\$true
--	--	--	---

Explanation

Answer Area

▼

- Set-ComplianceTag
- Set-HoldCompliancePolicy
- Set-RetentionCompliancePolicy
- Set-RetentionPolicy
- Set-RetentionPolicyTag

-Identity "Policy1"

▼ \$true

- enabled
- Force
- RestrictiveRetention
- RetentionPolicyTagLinks
- SystemTag

References:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncom>

NEW QUESTION: 54

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 to view information about the system.

Does this meet the goal?

A. Yes

B. No

Answer: A ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 55

You have a new Microsoft 365 subscription.

A user named User1 has a mailbox in Microsoft Exchange Online.

You need to log any changes to the mailbox folder permissions of User1.

Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

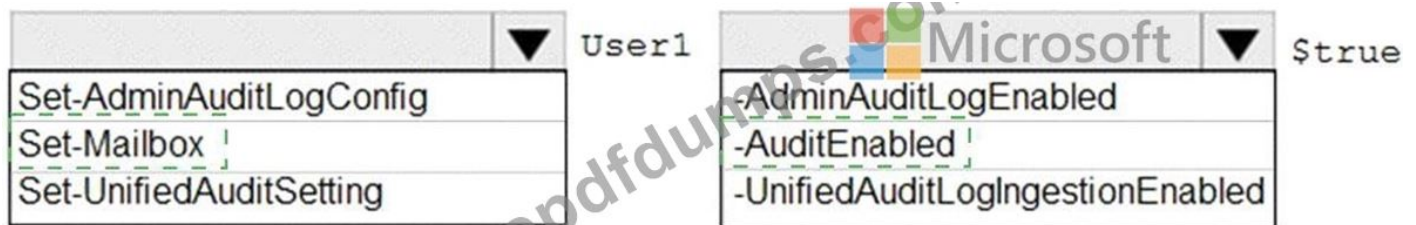
▼ User1

- Set-AdminAuditLogConfig
- Set-Mailbox
- Set-UnifiedAuditSetting

▼ \$true

- AdminAuditLogEnabled
- AuditEnabled
- UnifiedAuditLogIngestionEnabled

Answer:



Explanation



To enable auditing for a single mailbox (in this example, belonging to Holly Sharp), use this PowerShell command: `Set-Mailbox username -AuditEnabled $true` References:

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins>

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

NEW QUESTION: 56

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 copy the Group Policy Administrative Templates from a Windows 10 computer to Server1.

Does this meet the goal?

A. No

B. yes

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 57

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	Role	Member of
User1	Cloud device administrator	GroupA
User2	Intune administrator	GroupB
User3	None	None

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

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

You add user as a device enrollment manager in Endpoint manager

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

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	☐	☐
User2 can enroll a maximum of 10 devices in Endpoint Manager.	☐	☐
User3 can enroll an unlimited number of devices in Endpoint Manager.	☐	☐

Answer:

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	☒	☐
User2 can enroll a maximum of 10 devices in Endpoint Manager.	☐	☒
User3 can enroll an unlimited number of devices in Endpoint Manager.	☒	☐

Explanation

Answer Area

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Endpoint Manager.	☒	☐
User2 can enroll a maximum of 10 devices in Endpoint Manager.	☐	☒
User3 can enroll an unlimited number of devices in Endpoint Manager.	☐	☒

NEW QUESTION: 58

You configure an anti-phishing policy as shown in the following exhibit.

Policy setting	Policy name Description Applied to	Managers If the email is sent to: Irvins@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com	Edit
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off	Edit
Spoof	Enable antispoofting protection Action	On Quarantine the message	Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive	Edit

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

If a message is identified as a domain impersonation, [answer choice].

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

Answer:

If a message is identified as a domain impersonation, [answer choice].

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

Explanation

If a message is identified as a domain impersonation, [answer choice]

the message is delivered to the Inbox folder
the message is moved to the Deleted Items folder
the messages are moved to the Junk Email folder

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].

Advanced phishing thresholds
Domain impersonation
Enable antispooofing protection
Mailbox intelligence

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-ant>

NEW QUESTION: 59

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role	Office 365 role group
User1	None	Compliance data administrator
User2	Global administrator	None

You create a retention label named Label1 that has the following configurations:

Retains content for five years

Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

Applies to content that contains the word Merger

Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention \$true

-Force

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 add Exchange email as a location to Policy1.	☐	☐
User2 can remove SharePoint sites from Policy1.	☐	☐
User2 can add the word Acquisition to Policy1.	☐	☐

Answer:

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☒	☐
User2 can remove SharePoint sites from Policy1.	☐	☒
User2 can add the word Acquisition to Policy1.	☒	☐

Explanation

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☒	☐
User2 can remove SharePoint sites from Policy1.	☐	☒
User2 can add the word Acquisition to Policy1.	☒	☐

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncom>

NEW QUESTION: 60

Your company has a Microsoft 365 subscription.

You need to configure Microsoft 365 to meet the following requirements:

Malware found in email attachments must be quarantined for 20 days.

The email address of senders to your company must be verified.

Which two options should you configure in the Security & Compliance admin center? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Answer:

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

Explanation

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

NEW QUESTION: 61

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

Name	Platform
Device1	MacOS
Device2	Windows 10 Pro
Device3	Windows 10 Enterprise
Device4	Ubuntu 18.04 LTS

You plan to implement attack surface reduction (ASR) rules. Which devices will support the ASR rules?

- A. Device 1, Device2, and Device3 only
- B. Device3 only
- C. Device2 and Device3 only
- D. Device1, Device2, Devices and Device4

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-attack-surface-reduction?view>

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 62

You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP). You need to create a detection exclusion in Azure ATP.

Which tool should you use?

- A. the Security & Compliance admin center
- B. Microsoft Defender Security Center
- C. the Microsoft 365 admin center
- D. the Azure Advanced Threat Protection portal
- E. the Cloud App Security portal

Answer: D ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/defender-for-identity/what-is>

<https://docs.microsoft.com/en-us/defender-for-identity/excluding-entities-from-detections>

NEW QUESTION: 63

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

Name	Role
User1	Exchange administrator
User2	Security administrator
User3	None

You run the following cmdlet.

```
Set-MailboxAuditBypassAssociation -Identity User2
-AuditByPassEnabled $true
```

The users perform the following actions:

User1 accesses an item in the mailbox of User2.

User2 modifies a mailbox item in the mailbox of User3.

User3 signs in to her mailbox.

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
The action performed by User1 is audited.	☐	☐
The action performed by User2 is audited.	☐	☐
The action performed by User3 is audited.	☐	☐

Answer:

Statements	Yes	No
The action performed by User1 is audited.	☒	☐
The action performed by User2 is audited.	☐	☒
The action performed by User3 is audited.	☒	☐

Explanation

Statements	Yes	No
The action performed by User1 is audited.	☒	☐
The action performed by User2 is audited.	☐	☒
The action performed by User3 is audited.	☒	☐

Reference:

<https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailboxauditbypassassociation?view=exchan>

NEW QUESTION: 64

You have a Microsoft 365 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

All the devices in your organization are onboarded to Microsoft Defender ATP.

You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.

What should you do?

- A. From Alerts queue, create a suppression rule and assign an alert
- B. From the Security & Compliance admin center, create an audit log search
- C. From Advanced hunting, create a query and a detection rule
- D. From the Security & Compliance admin center, create a data loss prevention (DLP) policy

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 65

You have a Microsoft 365 subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

You create and assign a data loss prevention (DLP) policy named Policy1. Policy1 is configured to prevent documents that contain Personally Identifiable Information (PII) from being emailed to users outside your organization.

To which users can User1 send documents that contain PII?

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

Answer: B ([LEAVE A REPLY](#))

Explanation

Guest accounts are considered "outside your organization". Users who have non-guest accounts in a host organization's Active Directory or Azure Active Directory tenant are considered as people inside the organization.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide>

NEW QUESTION: 66

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 ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 67

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: ([SHOW ANSWER](#)**)**

Explanation

References:

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

NEW QUESTION: 68

Your company has multiple offices.

You have a Microsoft 365 E5 tenant that uses Microsoft Intune for device management. Each office has a local administrator.

You need to ensure that the local administrators can manage only the devices in their respective office.

What should you use?

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

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/fundamentals/scope-tags>

NEW QUESTION: 69

You have a Microsoft 365 E5 tenant.

You configure a device compliance policy as shown in the following exhibit.

Compliance settings [Edit](#)

Microsoft Defender ATP

Require the device to be at or under the machine risk score: Low

Device Health

Rooted devices Block

Require the device to be at or under the Device Threat Level

System Security

Require a password to unlock mobile devices Require

Required password type Device default

Encryption of data storage on device. Require

Block apps from unknown sources Block

Actions for noncompliance [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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.

When a device reports a medium threat level, the device will



▼

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

▼

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Answer:

When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Explanation

Graphical user interface, text, application, email Description automatically generated

When a device reports a medium threat level, the device will

- be locked remotely
- display a notification
- marked as compliant
- marked as noncompliant
- removed from the database

Rooted devices will be

- allowed to access company resources
- marked as compliant
- prevented from accessing company resources
- reported with a low device threat

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android>

NEW QUESTION: 70

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 the Security & Compliance admin center, you modify the roles of the US eDiscovery Managers role group.

Does this meet the goal?

A. Yes

B. No

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 71

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 ([LEAVE A REPLY](#))

Explanation

References:

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

NEW QUESTION: 72

Your on-premises network contains an Active Directory domain and a Microsoft Endpoint Configuration Manager site.

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

You use Azure AD Connect to sync user objects and group objects to Azure Directory (Azure AD)

Password hash synchronization is disabled.

You plan to implement co-management.

You need to configure Azure AD Connect and the domain to support co-management.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

To configure Azure AD Connect:

- ☐ Configure hybrid Azure AD join.
- ☐ Enable device writeback.
- ☐ Enable password hash synchronization.

To configure the domain:

- ☐ Add an alternative UPN suffix.
- ☐ Register a service connection point.
- ☐ Register a service principal name (SPN).

Answer:

Answer Area

To configure Azure AD Connect:

- Configure hybrid Azure AD join.
- Enable device writeback.
- Enable password hash synchronization.

To configure the domain:

- Add an alternative UPN suffix.
- Register a service connection point.
- Register a service principal name (SPN).

Explanation

Answer Area

To configure Azure AD Connect: Enable password hash synchronization.

To configure the domain: Add an alternative UPN suffix.

NEW QUESTION: 73

From the Microsoft 365 compliance center, you configure a data loss prevention (DLP) policy for a Microsoft SharePoint Online site named Site1. Site1 contains the roles shown in the following table.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi creates the files shown in the exhibit. (Click the

SharePoint

Site1

Search Documents

+ New Upload Quick edit Sync All Documents

Documents

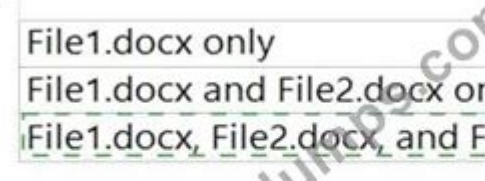
Name	Modified	Modified By	+ Add column
File1.docx	About a minute ago	Prvi	
File2.docx	A few seconds ago	Prvi	
File3.docx	A few seconds ago	Prvi	

Which files can User1 and User2 open? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

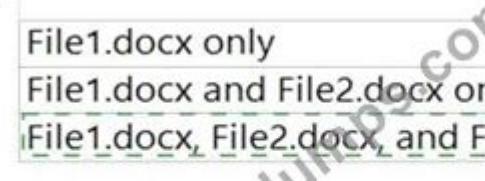
User1:  

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

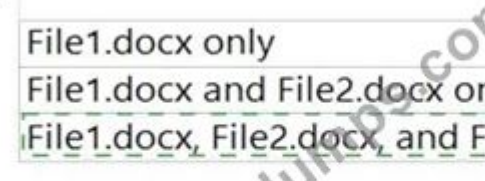
User2:  

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Answer:

User1:  

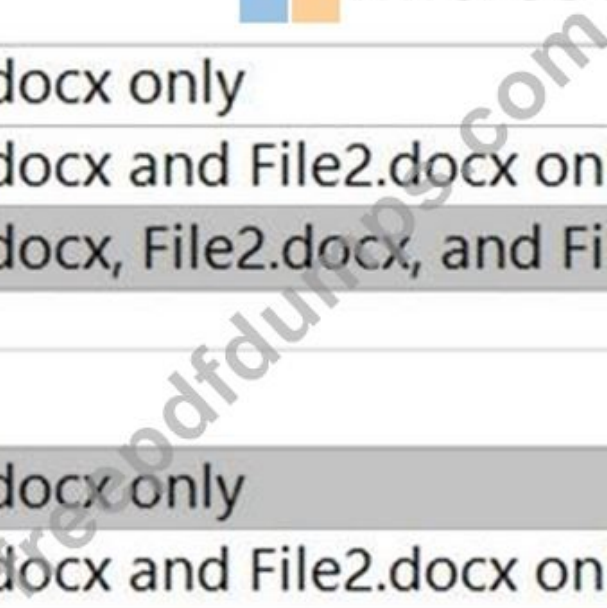
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:  

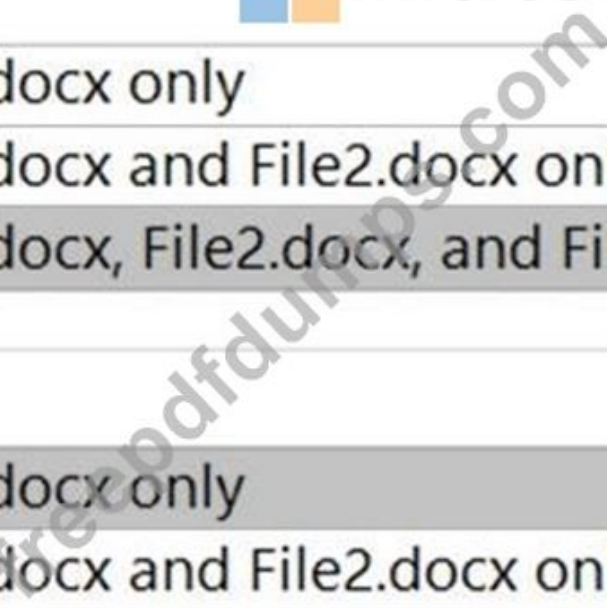
- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Explanation

Graphical user interface, text, application, email Description automatically generated

User1:  

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

User2:  

- File1.docx only
- File1.docx and File2.docx only
- File1.docx, File2.docx, and File3.docx

Reference:

<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/>

<https://gcc.microsoftcrmportals.com/blogs/office365-news/190220SPIcons/>

NEW QUESTION: 74

You have a Microsoft 365 E5 tenant.

You create a retention label named Retention1 as shown in the following exhibit.

The screenshot shows a 'Review your settings' window for a retention label. It contains the following sections and options:

- Name:** Retention1 (with an 'Edit' link)
- Description for admins:** (with an 'Edit' link)
- Description for users:** (with an 'Edit' link)
- File plan descriptors:** (with an 'Edit' link)
 - Reference id: 1
 - Business function/department: Legal
 - Category: Compliance
 - Authority type: Legal
- Retention:** (with an 'Edit' link)
 - 7 years
 - Retain only
 - Based on when it was created

At the bottom are three buttons: 'Back', 'Create this label' (highlighted in blue), and 'Cancel'.

When users attempt to apply Retention1, the label is unavailable.

You need to ensure that Retention1 is available to all the users.

What should you do?

- A. Create a new label policy
- B. Modify the Authority type setting for Retention!
- C. Modify the Business function/department setting for Retention 1.
- D. Use a file plan CSV template to import Retention1.

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-apply-retention-labels?view=o365-worldwide>

NEW QUESTION: 75

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some 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: (SHOW ANSWER)

NEW QUESTION: 76

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

Answer: B (LEAVE A REPLY)

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!
Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 77

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named User1 is a member of a dynamic group named Group1.

User1 reports that he cannot access documents shared to Group1.

You discover that User1 is no longer a member of Group1.

You suspect that an administrator made a change that caused User1 to be removed from Group1.

You need to identify which administrator made the change.

Which audit log activity should you search in the Security & Compliance admin center?

- A. Azure AD group administration activities - Removed member from group
- B. User administration activities - Updated user
- C. Azure AD group administration activities - Updated group

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 78

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

You are planning the auditing strategy.

Which three activities will be audited by default? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

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

Answer: A,B,C ([LEAVE A REPLY](#))

Explanation

References:

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

NEW QUESTION: 79

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

Three files were created on February 1, 2019, as shown in the following table.



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

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

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

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

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

You apply the retention labels to Exchange email, SharePoint sites, and OneDrive accounts. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	☐	☐
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	☐	☐
File3 will be deleted automatically after February 1, 2021.	☐	☐

Answer:

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	☐	☒
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	☐	☒
File3 will be deleted automatically after February 1, 2021.	☐	☒

Explanation

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	☐	☒
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	☐	☒
File3 will be deleted automatically after February 1, 2021.	☐	☒

Box 1: No

Retention overrides deletion.

Box 2: No

Content in a document library will be moved to the first-stage Recycle Bin within 7 days of disposition, and then permanently deleted another 93 days after that. Thus 100 days in total.

Box 3: No

Items in an Exchange mailbox will be permanently deleted within 14 days of disposition.

References:

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

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

NEW QUESTION: 80

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

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.	☐	☐
Label1 applies to File2.docx.	☐	☐
Label1 applies to File3.docx.	☐	☐

Answer:

Statements	Yes	No
Label1 applies to File1.docx.	☐	☐
Label1 applies to File2.docx.	☐	☐
Label1 applies to File3.docx.	☐	☐

Explanation

Statements	Yes	No
Label1 applies to File1.docx.	☐	☐
Label1 applies to File2.docx.	☐	☐
Label1 applies to File3.docx.	☐	☐

The phrase to match is "im" and it is case sensitive. The phrase must also appear at least twice.

Box 1: No

File1.docx contain the word "import" once only

Box 2: Yes

File2.docx contains two occurrences of the word "import" as well as the word "imported" Box 3:

No File3.docx contains "IM" but his is not the correct letter case.

References:

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

NEW QUESTION: 81

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

Answer:

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

Explanation

Text, table Description automatically generated with medium confidence

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view>

NEW QUESTION: 82

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD.

You purchase a Microsoft 365 E3 subscription.

You need to deploy Windows 10 Enterprise to the computers. The solution must minimize administrative effort.

What should you do?

A. Enroll the computers in Microsoft Intune. Create a configuration profile by using the Edition upgrade and mode switch template. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.

B. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile.

Assign the profile to all the computers. Instruct users to restart their computer and perform a network restart.

C. From the Azure Active Directory admin center, create a security group that has dynamic device membership. Assign licenses to the group and instruct users to sign in to their computer.

D. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online site. Instruct users to run the provisioning package from SharePoint Online.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 83

You need to create the DLP policy to meet the technical requirements.

What should you configure first?

A. sensitive info types

B. the Insider risk management settings

C. the event types

D. the sensitivity labels

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

NEW QUESTION: 84

You have a Microsoft 365 tenant.

You plan to enable BitLocker Disk Encryption (BitLocker) automatically for all Windows 10 devices that enroll in Microsoft Intune.

What should you use?

- A. an attack surface reduction (ASR) policy
- B. an app configuration policy
- C. a device compliance policy
- D. a device configuration profile

Answer: ([SHOW ANSWER](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices>

NEW QUESTION: 85

Your company has a Microsoft 365 tenant.

The company sells products online and processes credit card information.

You need to be notified if a file stored in Microsoft SharePoint Online contains credit card information. The file must be removed automatically from its current location until an administrator can review its contents.

What should you use?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 86

You have several devices enrolled in Microsoft Intune.

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

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

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

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

You add User3 as a device enrollment manager in Intune.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Intune.	☐	☐
User2 can enroll a maximum of 10 devices in Intune.	☐	☐
User3 can enroll an unlimited number of devices in Intune.	☐	☐

Answer:

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Intune.	☐	☒
User2 can enroll a maximum of 10 devices in Intune.	☐	☒
User3 can enroll an unlimited number of devices in Intune.	☐	☒

Explanation

Statements	Yes	No
User1 can enroll a maximum of 10 devices in Intune.	☐	☒
User2 can enroll a maximum of 10 devices in Intune.	☐	☒
User3 can enroll an unlimited number of devices in Intune.	☐	☒

References:

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

NEW QUESTION: 87

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 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 88

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 89

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

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices. You enable device clean-up rules. What can you configure as the minimum number of days before a device is removed automatically?

- A. 90
- B. 10
- C. 45
- D. 30

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 90

You have a Microsoft 365 subscription.

You discover that some external users accessed the 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. No
- B. Yes

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 91

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. No

B. Yes

Answer: ([SHOW ANSWER](#))

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: **Freepdfdumps**)

NEW QUESTION: 92

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements.

What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

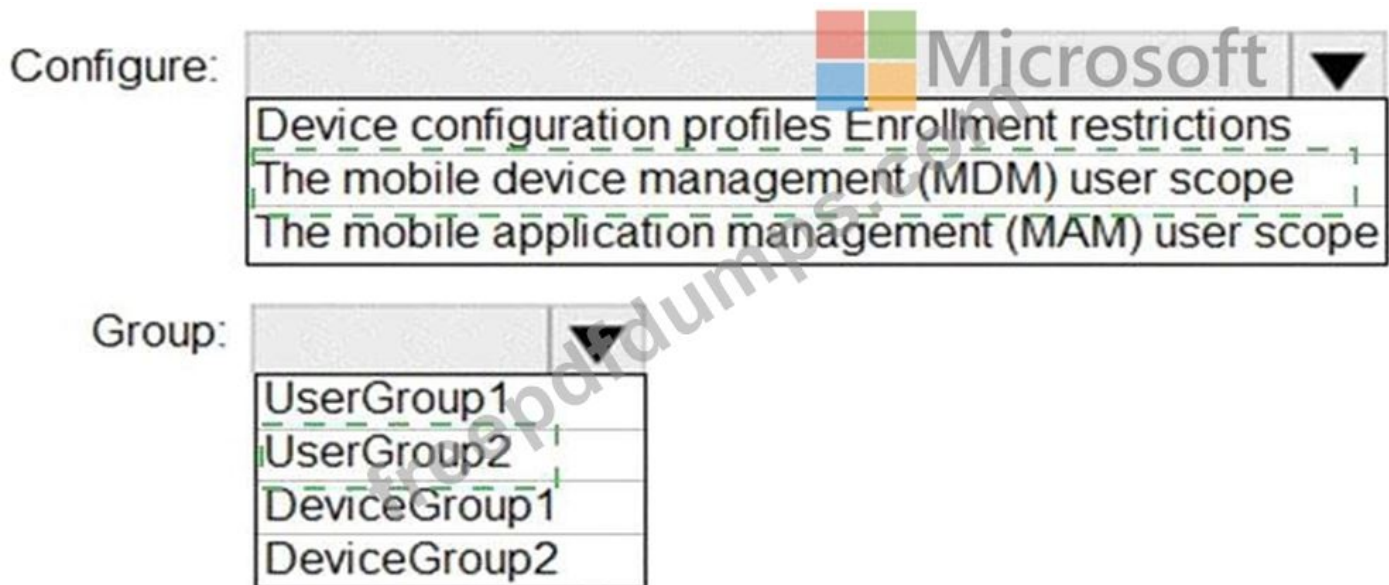
Configure:

Device configuration profiles	Enrollment restrictions
The mobile device management (MDM) user scope	
The mobile application management (MAM) user scope	

Microsoft Group:

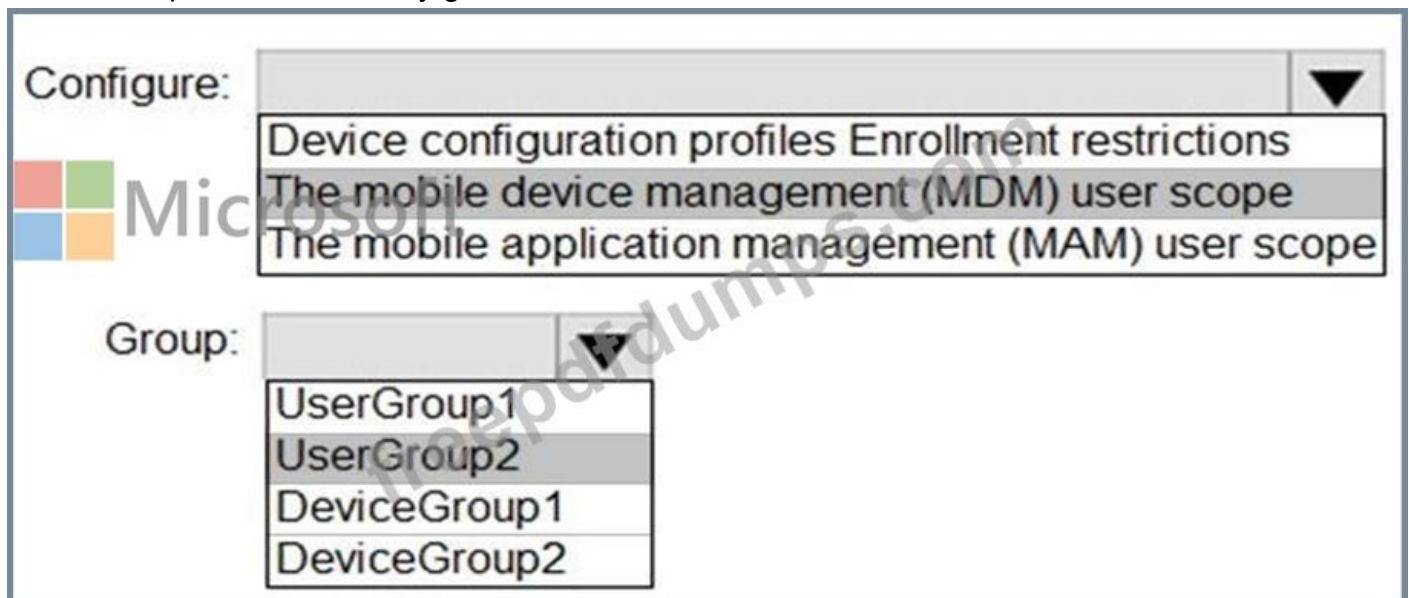
UserGroup1
UserGroup2
DeviceGroup1
DeviceGroup2

Answer:



Explanation

Text Description automatically generated with medium confidence



Reference:

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

NEW QUESTION: 93

Your company has a Microsoft 365 E3 subscription.

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

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

What should you use?

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

Answer: C ([LEAVE A REPLY](#))

Explanation

<https://docs.microsoft.com/en-us/windows/deployment/windows-10-subscription-activation>

NEW QUESTION: 94

Your network contains an on premises Active Directory domain.

Your company has a security policy that prevents additional software from txnrwj installed on domain controllers.

You need to monitor a domain controller by using Microsoft Azure Advanced Threat Protection (ATP).

What should you do? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Deploy an Azure ATP sensor, and then configure port mirroring.
- B. Deploy an Azure ATP sensor, and then configure detections.
- C. Deploy an Azure ATP standalone sensor, and then configure detections.
- D. Deploy an Azure ATP standalone sensor, and then configure port mirroring.

Answer: (SHOW ANSWER)

Explanation

References:

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

NEW QUESTION: 95

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.	☐	☐
User2 can sign in to Windows Defender Security Center.	☐	☐
User3 can view Device1 in Windows Defender Security Center.	☐	☐

Answer:

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	☒	☐
User2 can sign in to Windows Defender Security Center.	☐	☒
User3 can view Device1 in Windows Defender Security Center.	☒	☐

Explanation

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	☒	☐
User2 can sign in to Windows Defender Security Center.	☐	☒
User3 can view Device1 in Windows Defender Security Center.	☒	☐

NEW QUESTION: 96

Your company has digitally signed applications.

You need to ensure that Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) considers the digitally signed applications safe and never analyzes them.

What should you create in the Microsoft Defender Security Center?

- A. a custom detection rule
- B. an allowed/blocked list rule
- C. an alert suppression rule
- D. an indicator

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 97

Your company purchases a cloud app named App1.

You need to ensure that you can use Microsoft Cloud App Security to block downloads in App1.

App1 supports session controls.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Cloud App Security admin center, add an app connector.

Sign in to App1.

Create a conditional access policy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for App1.



Answer:

Actions

Answer Area

Deploy Azure Active Directory (Azure AD) Application Proxy.

From the Cloud App Security admin center, add an app connector.

Sign in to App1.

Create a conditional access policy.

From the Azure Active Directory admin center, configure the Diagnostic settings.

From the Azure Active Directory admin center, add an app registration for App1.

From the Cloud App Security admin center, add an app connector.

Create a conditional access policy.

Sign in to App1.



Explanation

Graphical user interface, text, application Description automatically generated



Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/getting-started-with-cloud-app-security>

NEW QUESTION: 98

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

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

You need to onboard Device1 and Device2 to Microsoft Defender for Endpoint.

What should you use to onboard each device? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Device1:

- A local script
- Group Policy
- Microsoft Endpoint Manager**
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Device2:

- A local script**
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Microsoft

Answer:

Answer Area

Device1: Microsoft Endpoint Manager

- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Device2: A local script

- A local script
- Group Policy
- Microsoft Endpoint Manager
- An app from the Google Play store
- Integration with Microsoft Defender for Cloud

Microsoft

Explanation

Answer Area

Device1: Microsoft Endpoint Manager

Device2: A local script

Microsoft

NEW QUESTION: 99

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

A Built-in protection preset security policy is applied to the subscription.

Which two policy types will be applied by the Built-in protection policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Anti-phishing
- B. Anti-spam
- C. Safe Links
- D. Anti-malware
- E. Safe Attachments

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 100

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: ([SHOW ANSWER](#))

Explanation

References:

[https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?](https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?view=azurermps-6.13.0)
[view=azurermps-6.13.0](https://docs.microsoft.com/en-us/powershell/module/azurerms/resources/new-azurermroleassignment?view=azurermps-6.13.0)

NEW QUESTION: 101

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. The company stores 2 TBs of data in SharePoint Online document libraries.

The tenant has the labels shown in the following table.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

From the Azure portal, you active unified labeling.

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 can now be used as a sensitivity label or an Azure Information Protection label.	☐	☐
Label2 can now be used as a retention label or an Azure Information Protection label.	☐	☐
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	☐	☐

Answer:

Answer Area	
Statements	Yes No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	☒ ☐
Label2 can now be used as a retention label or an Azure Information Protection label.	☐ ☒
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	☒ ☐

Explanation

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	☒	☐
Label2 can now be used as a retention label or an Azure Information Protection label.	☐	☒
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	☒	☐

NEW QUESTION: 102

You have a Microsoft 365 ES subscription that has three auto retention policies as show in the following exhibit.

```

Select Administrator: Windows PowerShell

Name           : Retention1
Priority        : 200
RecordTypes     : {MicrosoftTeams}
Operations      : {}
UserIds        : {}
RetentionDuration : ThreeMonths

Name           : Retention2
Priority        : 150
RecordTypes     : {MicrosoftTeams}
Operations      : {teamcreated}
UserIds        : {User1@sk200628outlook.onmicrosoft.com}
RetentionDuration : SixMonths

Name           : Retention3
Priority        : 100
RecordTypes     : {}
Operations      : {}
UserIds        : {User2@sk200628outlook.onmicrosoft.com}
RetentionDuration : TwelveMonths

PS C:\>

```

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.

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice].

If User2 adds a channel in Microsoft Teams, the event is [answer choice].

Answer:

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice].

If User2 adds a channel in Microsoft Teams, the event is [answer choice].

Explanation

Answer Area

If User1 creates a team in Microsoft Teams, the event is [answer choice] retained for six months

If User2 adds a channel in Microsoft Teams, the event is [answer choice] retained for 90 days

Microsoft

NEW QUESTION: 103

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

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 104

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.

You configure a session control policy to block downloads from SharePoint Online sites.

Users report that they can still download files from SharePoint Online sites.

You need to ensure that file download is blocked while still allowing users to browse SharePoint Online sites.

What should you configure?

- A. an access policy
- B. a Conditional Access policy
- C. a data loss prevention (DLP) policy
- D. an activity policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 105

You have a Microsoft 365 E5 subscription that contains two users named Admin1 and Admin2.

All users are assigned a Microsoft 365 Enterprise E5 license and auditing is turned on.

You create the audit retention policy shown in the exhibit. (Click the Exhibit tab.)

New audit retention policy Microsoft

Name: Policy1

Description:

Record Types: AzureActiveDirectory ▾

Activities: Added user, Deleted user, Reset user password, Changed user password, Changed user license, ... (7) ▾

Users: Admin1 ▾

Duration: ☒ 90 Days ☐ 6 Months ☐ 1 Year

Priority: 100

Save Cancel

After Policy1 is created, the following actions are performed:

Admin1 creates a user named User1.

Admin2 creates a user named User2.

How long will the audit events for the creation of User1 and User2 be retained? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1: ▼

0 days
30 days
90 days
180 days
365 days

User2: ▼

0 days
30 days
90 days
180 days
365 days

Answer:

User1:  ▼

0 days
30 days
90 days
180 days
365 days

User2: ▼

0 days
30 days
90 days
180 days
365 days

Explanation

User1:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	

User2:

	▼
0 days	
30 days	
90 days	
180 days	
365 days	



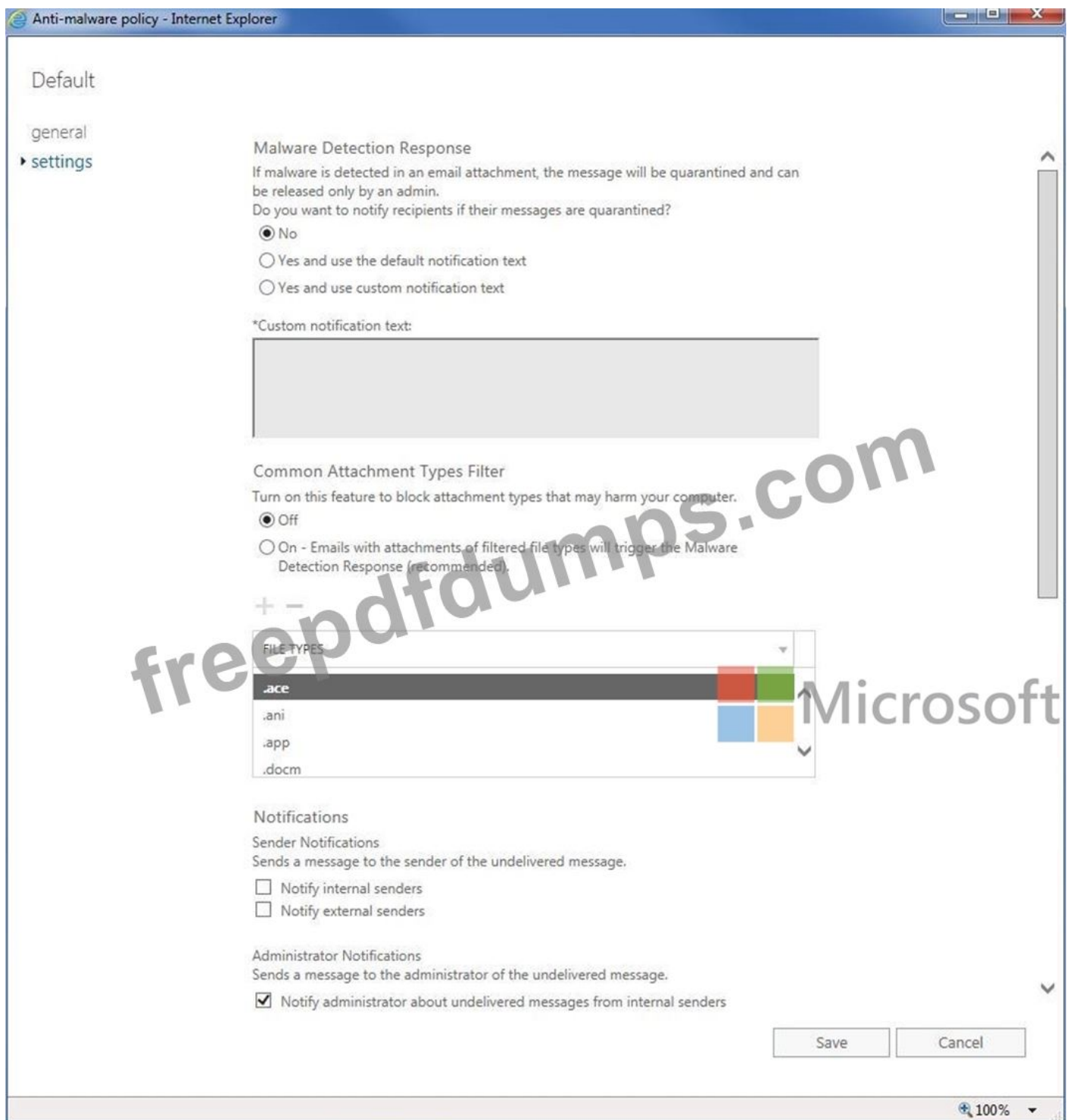
Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide>

NEW QUESTION: 106

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 removed. The email message will be quarantined, and User1 will receive an email message without any attachments and an email message that includes the following text: 'Malware was removed.'
- B.** The email message will be quarantined, and the message will remain undelivered.
- C.** Both attachments will be removed. 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.'

D. The malware-infected attachment will be removed. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-protection?view=o365>

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam! Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 107

Your company uses Microsoft Azure Advanced Threat Protection (ATP) and Windows Defender ATP.

You need to integrate Windows Defender ATP and Azure ATP.

What should you do?

- A.** From Azure ATP, configure the notifications and reports.
- B.** From Azure ATP, configure the data sources.
- C.** From Windows Defender Security Center, configure the Machine management settings.
- D.** From Windows Defender Security Center, configure the General settings.

Answer: ([SHOW ANSWER](#)**)**

Explanation

References:

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

NEW QUESTION: 108

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

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

Use actions to protect content when the conditions are met.



Restrict access or encrypt the content

☒ Block people from sharing and restrict access to shared content

By default, users are blocked from sending email messages to people. You can choose who has access to shared SharePoint and OneDrive content. Block these people from accessing SharePoint and OneDrive content

☐ Everyone. Only the content owner, the last modifier, and the site admin will continue to have access

☒ Only people outside your organization. People inside your organization will continue to have access.

☐ Encrypt email messages (applies only to content in Exchange)

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

What should you configure?

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

Answer: ([SHOW ANSWER](#))

Explanation

Editing Policy settings > +New Rule > Exceptions We won't apply this rule to content that matches any of these exceptions. > +Add an exception > [Dropdownbox] Except if the recipient domain is.

----- Except if recipient domain is Detects when content is sent in an email message to the recipient domains you specify.

NEW QUESTION: 109

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Security & Compliance admin center, you assign the Security Administrator role to User1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B ([LEAVE A REPLY](#))

Explanation

References:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

NEW QUESTION: 110

You have a Microsoft 365 tenant that contains a Windows 10 device named Device1 and the Microsoft Endpoint Manager policies shown in the following table.

Name	Type	Block execution of potentially obfuscated scripts (js/vbs/ps)
Policy1	Attack surface reduction (ASR)	Audit mode
Policy2	Microsoft Defender ATP Baseline	Disable
Policy3	Device configuration profile	Not configured

The policies are assigned to Device1.

Which policy settings will be applied to Device1?

- A. no settings
- B. only the settings of Policy1
- C. only the settings of Policy2
- D. only the settings of Policy3

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 111

Your company has five security information and event management (SIEM) appliances. The traffic logs from each appliance are saved to a file share named Logs.

You need to analyze the traffic logs.

What should you do from Microsoft Cloud App Security?

- A. Click Investigate, and then click Activity log.
- B. Click Control, and then click Policies. Create a file policy.
- C. Click Discover, and then click Create snapshot report.
- D. Click Investigate, and then click Files.

Answer: C ([LEAVE A REPLY](#))

Explanation

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

NEW QUESTION: 112

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 ([LEAVE A REPLY](#))

Explanation

References:

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

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

NEW QUESTION: 113

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: C ([LEAVE A REPLY](#))

Explanation

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-m> In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. In this article we will add a default Windows 10 image to the production deployment share specifically to perform an in-place upgrade.

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/refresh-a-windows-7-computer-wit> To complete a computer refresh you will: Back up data and settings locally, in a backup folder. Wipe the partition, except for the backup folder. Apply the new operating system image. Install other applications.

Restore data and settings.

NEW QUESTION: 114

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

Microsoft

Answer:

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

Microsoft

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

Microsoft

NEW QUESTION: 115

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

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	☐	☐
User1 can access Microsoft Exchange Online from Device2.	☐	☐
User2 can access Microsoft Exchange Online from Device2.	☐	☐

Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	☒	☐
User1 can access Microsoft Exchange Online from Device2.	☐	☒
User2 can access Microsoft Exchange Online from Device2.	☒	☐

Explanation

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	☒	☐
User1 can access Microsoft Exchange Online from Device2.	☐	☒
User2 can access Microsoft Exchange Online from Device2.	☒	☐

NEW QUESTION: 116

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements.

What should you do?

- A. From the Microsoft 365 security center, configure an alert policy.
- B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
- C. From the Microsoft 365 admin center, configure a Briefing email.
- D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365-world>

NEW QUESTION: 117

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

What should you create from the Intune admin center?

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 118

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices.

You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy

Windows 10 and later

Category	Setting	Current Value	Target Value
Encryption	Encryption of data storage on device	Not configured	Require
Device Security	Firewall	Not configured	Require
	Trusted Platform Module (TPM)	Not configured	Require
	Antivirus	Not configured	Require
	Antispyware	Not configured	Require
Defender	Microsoft Defender Antimalware	Not configured	Require
	Microsoft Defender Antimalware minimum version	Not configured	Not configured
	Microsoft Defender Antimalware security intelligence up-to-date	Not configured	Require
	Real-time protection	Not configured	Require

Answer:

Category	Setting	Current Value	Target Value
Encryption	Encryption of data storage on device	Not configured	Require
Device Security	Firewall	Not configured	Require
	Trusted Platform Module (TPM)	Not configured	Require
	Antivirus	Not configured	Require
	Antispyware	Not configured	Require
Defender	Microsoft Defender Antimalware	Not configured	Require
	Microsoft Defender Antimalware minimum version	Not configured	Not configured
	Microsoft Defender Antimalware security intelligence up-to-date	Not configured	Require
	Real-time protection	Not configured	Require

Explanation

Graphical user interface Description automatically generated

Windows 10 compliance policy

Windows 10 and later

Policy	Require	Not configured
Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

NEW QUESTION: 119

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. No

B. yes

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 120

You have a Microsoft 365 E5 subscription.

Several users have iOS devices.

You plan to enroll the iOS devices in Microsoft Endpoint Manager.

You need to ensure that you can create an iOS/iPadOS enrollment profile in Microsoft Endpoint Manager.

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

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area



Answer:

Actions

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer Area

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Create a certificate from the Apple Push Certificates Portal.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager.



Explanation

From the Microsoft Endpoint Manager admin center, download a certificate signing request.
Create a certificate from the Apple Push Certificates Portal.
Upload an Apple MDM push certificate to Microsoft Endpoint Manager.

Reference:

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

NEW QUESTION: 121

You have a Microsoft 365 subscription. You have a user named User1.

You need to ensure that User1 can place a hold on all mailbox content.

Which role should you assign to User1?

- A. e Discovery Manager from the Security & Compliance admin center
- B. compliance management from the Exchange admin center
- C. User management administrator from the Microsoft 365 admin center
- D. Information Protection administrator from the Azure Active Directory admin center

Answer: (SHOW ANSWER)

Explanation

References:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions>

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 122

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

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

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

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

Exempt apps: App2

Protected apps: App1

Windows Information Protection mode: Block

Network boundary: IPv4 range of: 192.168.1.1-192.168.1.255

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can open File1.abc in App1.	☐	☐
You can open File1.abc in App2.	☐	☐
You can open File1.abc in App3.	☐	☐

Answer:

Statements	Yes	No
You can open File1.abc in App1.	☒	☐
You can open File1.abc in App2.	☐	☐
You can open File1.abc in App3.	☐	☒

Explanation

Statements	Yes	No
You can open File1.abc in App1.	☒	☐
You can open File1.abc in App2.	☒	☐
You can open File1.abc in App3.	☐	☒

References:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/creating-a-policy>

NEW QUESTION: 123

Your company uses on-premises Windows Server File Classification Infrastructure (FCI). Some documents on the on-premises file servers are classified as Confidential.

You migrate the files from the on-premises file servers to Microsoft SharePoint Online.

You need to ensure that you can implement data loss prevention (DLP) policies for the uploaded file based on the Confidential classification.

What should you do first?

- A. From the SharePoint admin center, configure hybrid search.
- B. From the SharePoint admin center, create a managed property.
- C. From the Security & Compliance Center PowerShell, run the New-DataClassification cmdlet.
- D. From the Security & Compliance Center PowerShell, run the New-DlpComplianceRule cmdlet.

Answer: (SHOW ANSWER)

Explanation

References:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/protect-documents-that-have-fci-or-other-properties#>

NEW QUESTION: 124

You have a Microsoft 365 tenant.

All users are assigned the Enterprise Mobility + Security license.

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

What should you configure?

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

Answer: D (LEAVE A REPLY)

Explanation

References:

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

NEW QUESTION: 125

Your company has a Microsoft 365 subscription. The subscription contains 500 devices that run Windows 10 and 100 devices that run iOS.

You need to create Microsoft Intune device configuration profiles to meet the following requirements:

- * Configure Wi-Fi connectivity to a secured network named ContosoNet.
- * Require passwords of at least six characters to lock the devices.

What is the minimum number of device configuration profiles that you should create?

- A. 4
- B. 2
- C. 1

Answer: B (LEAVE A REPLY)

NEW QUESTION: 126

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

Platform	Count
Windows 10	50
Android	50
Linux	50

You need to configure an incident email notification rule that will be triggered when an alert occurs only on a Windows 10 device. The solution must minimize administrative effort.

What should you do first?

- A. From the Microsoft 365 admin center, create a mail-enabled security group.
- B. From the Microsoft 365 Defender portal, create a device group.
- C. From the Microsoft Endpoint Manager admin center, create a device category.
- D. From the Azure Active Directory admin center, create a dynamic device group.

Answer: B ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/machine-groups?view=o365-worldw>

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-email-notifications?view=>

NEW QUESTION: 127

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

- A. Policy1 and Policy3 only
- B. Policy1 and Policy2 only
- C. Policy3 and Policy4 only
- D. Policy2 and Policy4 only

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 128

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

Answer:

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

Explanation

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

References:

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

NEW QUESTION: 129

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

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.

You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table.

On Thursday, you review the results of the app deployments.

Name	Shows in Company Portal	Assignment	Microsoft Office app to install	Day of creation
App1	Yes	Group1 - Required	Word	Monday
App2	Yes	Group2 - Required	Excel	Tuesday
App3	Yes	Group1 - Available	PowerPoint	Wednesday

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
Word is installed on Device1.	☒	☐
App3 is displayed in the Company Portal.	☐	☐
Excel is installed on Device1.	☐	☐

Answer:

ANSWER AREA



Microsoft

Statements

Word is installed on Device1.

Yes



No



App3 is displayed in the Company Portal.



Excel is installed on Device1.



Explanation

Answer Area

Statements

Word is installed on Device1.

Yes



No



App3 is displayed in the Company Portal.



Excel is installed on Device1.



NEW QUESTION: 130

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

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

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

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

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

Name	Assigned to
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.	☐	☐
Device2 is compliant.	☐	☐
Device3 is compliant.	☐	☐

Answer:

Answer Area

Statements	Yes	No
Device1 is compliant.	☒	☐
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

Explanation

Answer Area

Statements	Yes	No
Device1 is compliant.	☒	☐
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

NEW QUESTION: 131

You have a Microsoft 365 subscription.

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

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

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To meet the goal for the manager, create:

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

To review the messages, the manager must use:

▼
A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

Answer:

To meet the goal for the manager, create:

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

To review the messages, the manager must use:

▼
A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

Explanation

To meet the goal for the manager, create:

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

To review the messages, the manager must use:

▼
A message trace
An eDiscovery case
MyAnalytics
Outlook Web App

References:

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

NEW QUESTION: 132

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 Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

A. Yes

B. no

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 133

Your company has a Microsoft 365 subscription that uses an Azure Directory (Azure AD0 tenant named Contoso.com. The tenant contains the users shown in the following table.

You create a relation label named Label1 that has the following configurations:

Retains content for five years.

Automatically deletes all content that is older than five years.

You turn on Auto labeling for Label1 b using a policy named Policy1. Policy1 has the following configurations:

* Retains content for five years

* Automatically deletes all content that is older than five years

You turn on Auto labeling for Label 1 by using a policy named Policy1. Policy has the following configurations:

- * Applies to content that contains the word Merger
- * Specifies the OneDrive accounts and SharePoint sites locations

You run the following command

Set RetentionCompliancePolicy Policy1 RestrictiveRetention \$true Force

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 add Exchange email as a location to Policy1.	☐	☐
User2 can remove SharePoint sites from Policy1.	☐	☐
User2 can add the word Acquisition to Policy1.	☐	☐

Answer:

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	☐	☒
User2 can remove SharePoint sites from Policy1.	☒	☐
User2 can add the word Acquisition to Policy1.	☐	☒

NEW QUESTION: 134

You have a Microsoft 365 tenant.

You plan to manage incidents in the tenant by using the Microsoft 365 security center.

Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

- A. Microsoft Cloud App Security
- B. Azure Sentinel
- C. Azure Web Application Firewall
- D. Azure Defender

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-alerts?view=o365-worldwide>

NEW QUESTION: 135

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

SharePoint Content_ExportMicrosoft

↓ 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 10-MB XLSX file
- B. a 5-MB MP3 file
- C. a 5-KB RTF file
- D. an 80-MB PPTX file

Answer: B ([LEAVE A REPLY](#))

Explanation

Unrecognized file formats are excluded from the search.

Certain types of files, such as Bitmap or MP3 files, don't contain content that can be indexed. As a result, the search indexing servers in Exchange and SharePoint don't perform full-text indexing on these types of files.

These types of files are considered to be unsupported file types.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o36>

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

NEW QUESTION: 136

You need to notify the manager of the human resources department when a user in the department shares a file or folder from the department's Microsoft SharePoint Online site. What should you do?

- A. From the SharePoint Online admin center, modify the sharing settings.
- B. From the Microsoft 365 Defender portal, create an alert policy.
- C. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
- D. From the SharePoint Online site, create an alert.

Answer: B ([LEAVE A REPLY](#))

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 137

You have a Microsoft 365 subscription.

All users are assigned Microsoft Azure Active Directory Premium licenses.

From the Device Management admin center, you set Microsoft Intune as the MDM authority.

You need to ensure that when the members of a group named Marketing join a device to Azure Active Directory (Azure AD), the device is enrolled automatically in Intune. The Marketing group members must be limited to five devices enrolled in Intune.

Which two options should you use to perform the configurations? To answer, select the appropriate blades in the answer area.

NOTE: Each correct selection is worth one point.

Device enrollment

Microsoft Intune



 Overview

 Quick start

Manage

 Apple enrollment

 Android enrollment

 Windows enrollment

 Terms and conditions

 Enrollment restrictions

 Device categories

 Corporate device identifiers

 Device enrollment managers

Monitor



 Enrollment failures

 Audit logs

 Incomplete user enrollments

Answer:

Device enrollment

Microsoft Intune

 Search (Ctrl+J)



 Overview

 Quick start

Manage

 Apple enrollment

 Android enrollment

 Windows enrollment

 Terms and conditions

 Enrollment restrictions

 Device categories

 Corporate device identifiers

 Device enrollment managers

Monitor

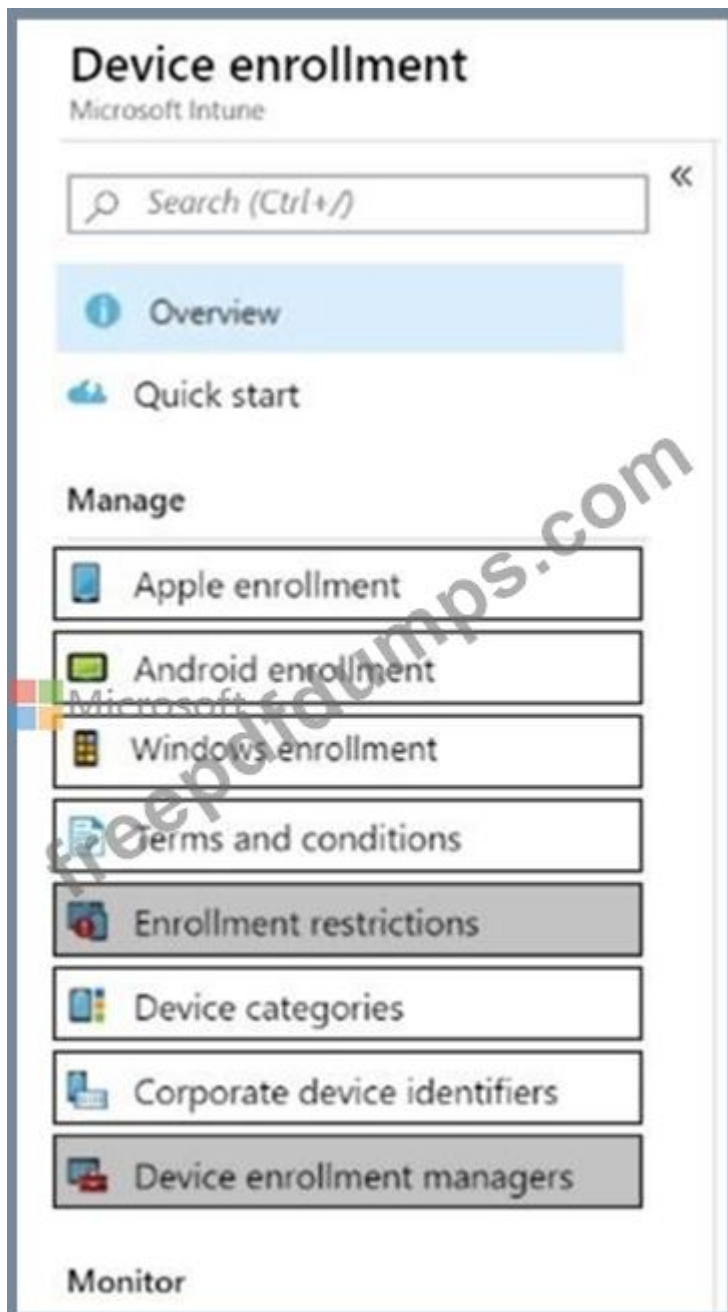
 Enrollment failures

 Audit logs

 Incomplete user enrollments



Explanation



Device enrollment manager (DEM) is an Intune permission that can be applied to an Azure AD user account and lets the user enroll up to 1,000 devices. You can create and manage enrollment restrictions that define what devices can enroll into management with Intune, including the:

- Number of devices.

- Operating systems and versions.

The Marketing group members must be limited to five devices enrolled in Intune. References:

<https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment-manager-enroll>

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

NEW QUESTION: 138

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 ([LEAVE A REPLY](#))

Explanation

References:

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

NEW QUESTION: 139

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 an Azure Active Directory (Azure AD) tenant that contains a user named User1.

Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A ([LEAVE A REPLY](#))

Explanation

References:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

NEW QUESTION: 140

Your company has a Microsoft 365 E5 tenant that contains a user named User1.

You review the company's compliance score.

You need to assign the following improvement action to User1: Enable self-service password reset.

What should you do first?

- A. From Compliance Manager, turn off automated testing.
- B. From the Azure Active Directory admin center, enable self-service password reset (SSPR).
- C. From the Microsoft 365 admin center, modify the self-service password reset (SSPR) settings.
- D. From the Azure Active Directory admin center, add User1 to the Compliance administrator role.

Answer: D (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o3>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-po>

NEW QUESTION: 141

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

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

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

You need to prevent the user from sharing the credit card information by using email and SharePoint.

What should you configure?

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

Answer: A (LEAVE A REPLY)

Explanation

References:

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

NEW QUESTION: 142

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to identify the settings that are below the Standard protection profile settings in the preset security policies.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

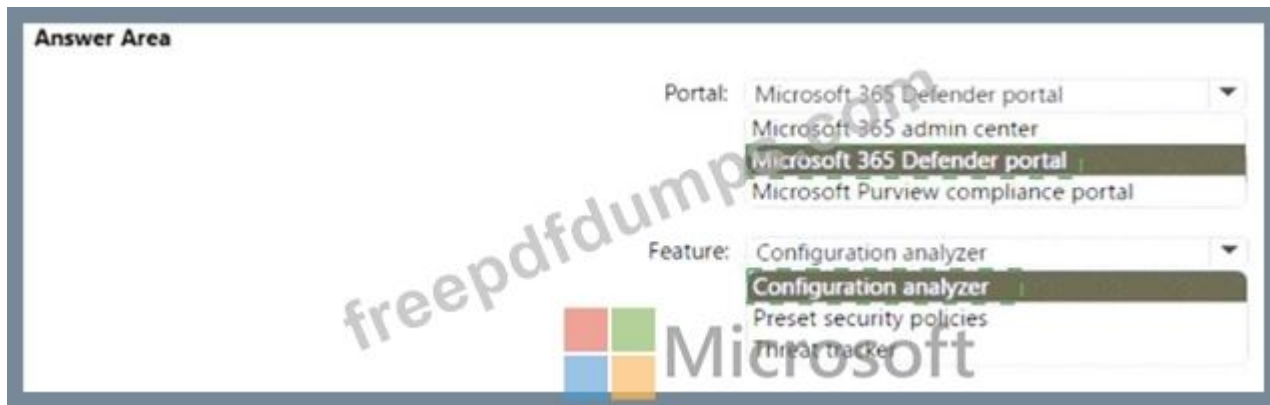
Answer Area

Portal: Microsoft 365 Defender portal
Microsoft 365 admin center
Microsoft 365 Defender portal
Microsoft Purview compliance portal

Feature: Configuration analyzer
Configuration analyzer
Preset security policies
Threat tracker

Microsoft

Answer:



The screenshot shows a web interface with a header 'Answer Area'. Below it, there are two dropdown menus. The first dropdown is labeled 'Portal:' and has four options: 'Microsoft 365 Defender portal', 'Microsoft 365 admin center', 'Microsoft 365 Defender portal' (which is highlighted), and 'Microsoft Purview compliance portal'. The second dropdown is labeled 'Feature:' and has three options: 'Configuration analyzer' (which is highlighted), 'Preset security policies', and 'Threat tracker'. A large, semi-transparent watermark 'freepdfdump.com' is overlaid diagonally across the center of the image. The Microsoft logo is visible in the bottom right corner of the interface area.

Explanation



This screenshot shows the same interface as the previous one, but with the selected options highlighted. The 'Portal:' dropdown now only shows 'Microsoft 365 Defender portal'. The 'Feature:' dropdown now only shows 'Configuration analyzer'. The 'freepdfdump.com' watermark and the Microsoft logo are still present.

NEW QUESTION: 143

Your company has a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

The tenant is configured to use Azure AD Identity Protection.

You plan to use an application named App1 that creates reports of Azure AD Identity Protection usage.

You register App1 in the tenant.

You need to ensure that App1 can read the risk event information of contoso.com.

To which API should you delegate permissions?

- A. Windows Azure Service Management API
- B. Windows Azure Active Directory
- C. Microsoft Graph
- D. Office 365 Management

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/graph/api/resources/identityprotection-root?view=graph-rest-beta>

NEW QUESTION: 144

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Endpoint integrated with Microsoft Endpoint Manager.

Devices are onboarded by using Microsoft Defender for Endpoint.

You plan to block devices based on the results of the machine risk score calculated by Microsoft Defender for Endpoint.

What should you create first?

- A. a device configuration policy
- B. a device compliance policy
- C. a conditional access policy
- D. an endpoint detection and response policy

Answer: ([SHOW ANSWER](#))

Reference:

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

NEW QUESTION: 145

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 admin center, you modify the sharing settings.

Does this meet the goal?

- A. No
- B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 146

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

Name	Platform
Device1	Windows 10 Enterprise
Device2	iOS
Device3	Android
Device4	Windows 10 Pro

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings.

Which devices will support the settings?

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 147

You have a Microsoft 365 subscription that links to an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com.

A user named User1 stores documents in Microsoft OneDrive.

You need to place the contents of User1's OneDrive account on an eDiscovery hold.

Which URL should you use for the eDiscovery hold? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

https://		onedrive.live.com/ contoso.onmicrosoft.com/ contoso.sharepoint.com/ contoso-my.sharepoint.com/	User1 Sites/User1 contoso_onmicrosoft_com/User1 personal/User1_contoso_onmicrosoft_com
----------	---	---	---

Answer:

https://		onedrive.live.com/ contoso.onmicrosoft.com/ contoso.sharepoint.com/ contoso-my.sharepoint.com/	User1 Sites/User1 contoso_onmicrosoft_com/User1 personal/User1_contoso_onmicrosoft_com
----------	---	---	---

Explanation

https://		onedrive.live.com/ contoso.onmicrosoft.com/ contoso.sharepoint.com/ contoso-my.sharepoint.com/	User1 Sites/User1 contoso_onmicrosoft_com/User1 personal/User1_contoso_onmicrosoft_com
----------	---	---	---

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds>

NEW QUESTION: 148

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: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 149

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You are deploying Microsoft Intune.

You successfully enroll Windows 10 devices in Intune.

When you try to enroll an iOS device in Intune, you get an error.

You need to ensure that you can enroll the iOS device in Intune.

Solution: You add your user account as a device enrollment manager.

Does this meet the goal?

- A. No
- B. Yes

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 150

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.	☐	☐
Device2 is marked as noncompliant after 10 days.	☐	☐
Device3 is marked as noncompliant after 15 days.	☐	☐

Answer:

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	☒	☐
Device2 is marked as noncompliant after 10 days.	☒	☐
Device3 is marked as noncompliant after 15 days.	☐	☒

Explanation

Statements	Yes	No
Device1 is marked as noncompliant after 10 days.	☒	☐
Device2 is marked as noncompliant after 10 days.	☒	☐
Device3 is marked as noncompliant after 15 days.	☐	☒

NEW QUESTION: 151

You have a Microsoft 365 E5 subscription.

All users have Mac computers. All the computers are enrolled in Microsoft Endpoint Manager and onboarded to Microsoft Defender for Endpoint.

You need to configure Microsoft Defender for Endpoint on the computers.

What should you create from the Endpoint Management admin center?

- A. a mobile device management (MDM) security baseline profile
- B. a device configuration profile
- C. an update policy for iOS
- D. a Microsoft Defender for Endpoint baseline profile

Answer: ([SHOW ANSWER](#))

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 152

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 153

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Name ↑	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2	1	Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

- A. Label1, Label3, Label2, and Label6 only
- B. Label1, Label2, and Label5 only
- C. Label3, Label4, and Label6 only
- D. Label1, Label2, Label3, Label4, Label5, and Label6

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 154

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

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

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User 3 to modify the Azure ATP sensor configuration- Does this meet the goal?

A. Yes

B. No

Answer: A ([LEAVE A REPLY](#))

Explanation

Access to the Defender for Identity portal is granted only to users within the Defender for Identity security groups, within your Azure Active Directory, as well as global and security admins of the tenant.

NEW QUESTION: 155

You have a Microsoft 365 E5 subscription that uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

D18912E1457D5D1DDCBD40AB3BF70D5D

From Microsoft Defender ATP, you turn on the Allow or block file advanced feature.

You need to block users from downloading a file named File1.exe.

What should you use?

A. a suppression rule

B. an indicator

C. a device configuration profile

Answer: ([SHOW ANSWER](#)**)**

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/respond-filealerts#a>

NEW QUESTION: 156

You use Windows Defender Advanced Threat Protection (Windows Defender ATP).

You have the Windows Defender ATP machine groups shown in the following table.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	Not applicable

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

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

To which machine group will each computer be added? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Computer1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Server1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Answer:

Computer1-London:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Group1</td></tr><tr><td colspan="2">Group2</td></tr><tr><td colspan="2">Group3</td></tr><tr><td colspan="2">Ungrouped machines</td></tr></table>		▼	Group1		Group2		Group3		Ungrouped machines	
	▼										
Group1											
Group2											
Group3											
Ungrouped machines											
Server1-London:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Group1</td></tr><tr><td colspan="2">Group2</td></tr><tr><td colspan="2">Group3</td></tr><tr><td colspan="2">Ungrouped machines</td></tr></table>		▼	Group1		Group2		Group3		Ungrouped machines	
	▼										
Group1											
Group2											
Group3											
Ungrouped machines											

Explanation

Computer1-London:  Microsoft

Server1-London:

Group1
Group2
Group3
Ungrouped machines

Group1
Group2
Group3
Ungrouped machines

NEW QUESTION: 157

You have a Microsoft 365 subscription that uses Security & Compliance retention policies. You implement a preservation lock on a retention policy that is assigned to all executive users. Which two actions can you perform on the retention policy? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point?

- A. Add locations to the policy
- B. Extend the duration of the policy
- C. Disable the policy
- D. Reduce the duration of policy
- E. Remove locations from the policy

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 158

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.	☐	☐
User2 can enroll Android devices in Intune.	☐	☐
User3 can enroll iOS devices in Intune.	☐	☐

Answer:

Statements	Yes	No
User1 can enroll Windows devices in Intune.	☐	☒
User2 can enroll Android devices in Intune.	☒	☐
User3 can enroll iOS devices in Intune.	☐	☒

Explanation

No

Yes

No

NEW QUESTION: 159

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

 Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☐
Device2 is compliant.	☐	☐
Device3 is compliant.	☐	☐

Answer:

Answer Area

 Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☒
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

Explanation

Answer Area

 Microsoft

Statements	Yes	No
Device1 is compliant.	☐	☒
Device2 is compliant.	☐	☒
Device3 is compliant.	☒	☐

NEW QUESTION: 160

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

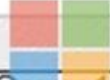
You plan to create a compliance policy named Compliance1.

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:

 Microsoft ▼

<u>Group1</u> 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

Answer:

Can be added to Compliance1 as recipients of noncompliance notifications:



▼

<u>Group1</u> and <u>Group4</u> only
<u>Group3</u> and <u>Group4</u> 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
<u>Group1</u> , <u>Group2</u> and <u>Group3</u> only
<u>Group1</u> , <u>Group3</u> , and <u>Group4</u> only
Group1, Group2, Group3, and Group4

Explanation

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

Can be added to Compliance1 as recipients of noncompliance notifications:

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

Reference:

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

NEW QUESTION: 161

Your company has a Microsoft 365 subscription.

You implement Microsoft Azure Information Protection.

You need to automatically protect email messages that contain the word Confidential in the subject line.

What should you create?

- A. a mail flow rule from the Exchange admin center
- B. a message trace from the Security & Compliance admin center
- C. a supervision policy from the Security & Compliance admin center
- D. a sharing policy from the Exchange admin center

Answer: ([SHOW ANSWER](#))

Explanation

References:

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

NEW QUESTION: 162

Your company uses Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

The devices onboarded to Microsoft Defender ATP are shown in the following table.

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

The alerts visible in the Microsoft Defender ATP alerts queue are shown in the following table.

Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

Triggering IOC: Any IOC

Action: Hide alert

Suppression scope: Alerts on ATP1 machine group

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
After you create the suppression rule, Alert1 is visible in the alerts queue.	☐	☐
After you create the suppression rule, Alert3 is visible in the alerts queue.	☐	☐
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	☐	☐

Answer:

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	☐	☐
After you create the suppression rule, Alert3 is visible in the alerts queue.	☐	☐
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	☐	☐

Explanation

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	☐	☐
After you create the suppression rule, Alert3 is visible in the alerts queue.	☐	☐
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	☐	☐

A suppression rule will not affect alerts that are already in the alerts queue. Only new alerts will be suppressed.

NEW QUESTION: 163

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

Policy type: Activity
App discovery
OAuth app
Session

Filter type: App
App state
App tag
Permission level

These are the selections for Policy type.

These are the selections for Filter type.

Answer:

Answer Area

Policy type: Activity
App discovery
OAuth app
Session

Filter type: App
App state
App tag
Permission level

These are the selections for Policy type.

These are the selections for Filter type.

Explanation

Answer Area

Policy type: App discovery

Filter type: Permission level

NEW QUESTION: 164

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 subscription.

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

Solution: From the Device Management admin center, you create a trusted location and a compliance policy.

Does this meet the goal?

A. Yes

B. No

Answer: B ([LEAVE A REPLY](#))

Explanation

Conditional Access in SharePoint Online can be configured to use an IP Address white list to allow access.

References:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlinean>

NEW QUESTION: 165

You have a Microsoft 365 E5 tenant that contains a Microsoft SharePoint Online site named Site1. Site1 contains the files shown in the following table.

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	2
File3.xlsx	5

You create a sensitivity label named Sensitivity1 and an auto-label policy that has the following configurations:

Name: AutoLabel1

Label to auto-apply: Sensitivity1

Rules for SharePoint Online sites: Rule1-SPO

Choose locations where you want to apply the label: Site1

Rule1-SPO is configured as shown in the following exhibit.

Edit rule Microsoft

Name *

Rule1-SPO

Description

Rule1 description

^ Conditions

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

^ Content contains sensitive info types

Default

All of these 



Sensitive info types

IP Address Accuracy 85 to 100 Instance count 2 to Any 

Add 

Create group

+ Add condition 

Save

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
Sensitivity1 is applied to File1.docx.	☐	☐
Sensitivity1 is applied to File2.txt.	☐	☐
Sensitivity1 is applied to File3.xlsx.	☐	☐

Answer:

Statements



Microsoft

Yes

No

Sensitivity1 is applied to File1.docx.

☐☐

Sensitivity1 is applied to File2.txt.

☐☐

Sensitivity1 is applied to File3.xlsx.

☐☐

Explanation

Graphical user interface, text, application Description automatically generated



Microsoft

Yes

No

Sensitivity1 is applied to File1.docx.

☐☐

Sensitivity1 is applied to File2.txt.

☐☐

Sensitivity1 is applied to File3.xlsx.

☐☐

Reference:

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

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

NEW QUESTION: 166

You have a Microsoft 365 subscription.

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

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

NOTE: Each correct selection is worth one point.

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

Answer:

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

Explanation

Platform:

- Android
- iOS
- Windows 10 and later
- Windows 8.1 and later

Settings:

- Offboard package
- Onboard package
- Windows Defender Application Guard
- Windows Defender Firewall

References:

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

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

Special Discount: **Freepdfdumps**)

NEW QUESTION: 167

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 new Microsoft 365 subscription.

You need to prevent users from sending email messages that contain Personally Identifiable Information (PII).

Solution: From the Azure portal, you create a Microsoft Azure Information Protection label and an Azure Information Protection policy.

Does this meet the goal?

A. No

B. Yes

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 168

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. Android Enterprise

C. macOS

D. Windows 8.1

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 169

You plan to allow users from the engineering department to enroll their mobile device in mobile device management (MDM).

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

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

What is the effective configuration for the members of the Engineering group? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Device limit:



▼

5

10

15

Allowed platform:

▼

Android only

iOS only

All platforms

Answer:

Device limit:

▼

5

10

15

Allowed platform:

▼

Android only

iOS only

All platforms

Explanation

Device limit:

▼
5
10
15

Allowed platform:

▼
Android only
iOS only
All platforms



NEW QUESTION: 170

You have a Microsoft 365 E5 tenant.

You plan to deploy 1,000 new iOS devices to users. The devices will be shipped directly from the supplier to the users.

You need to recommend a Microsoft Intune enrollment option that meets the following requirements:

- * Minimizes user interaction
- * Minimizes administrative effort
- * Automatically installs corporate apps

What should you recommend?

- A. Automated Device Enrollment (ADE)
- B. bring your own device (BYOD) user and device enrollment
- C. Apple Configurator enrollment

Answer: A ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll>

NEW QUESTION: 171

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

Block emails that contain financial data.

Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

Use the following location: Exchange email.

Display the following policy tip text: Message contains sensitive data.

When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

Result

When the user sends an email that contains only financial data:

Result



Microsoft

Answer:

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and the user will receive the policy tip: Message blocked.

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data:

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.



Microsoft

Explanation

When the user sends an email that contains financial data and health records:

The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data:

The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>

NEW QUESTION: 172

You have a Microsoft 365 subscription and an on-premises Active Directory domain named contoso.com. All client computers run Windows 10 Enterprise and are joined to the domain. You need to enable Windows Defender Credential Guard on all the computers. What should you do?

- A. From a domain controller, create a Group Policy object (GPO) that enables the Turn On Virtualization Based Security setting.
- B. domain controller, create a Group Policy object (GPO) that enables the Restrict delegation of credentials to remote servers setting.
- C. From the Security & Compliance admin center, configure the DKIM signatures for the domain
- D. From the Security & Compliance admin center, create a device security policy.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 173

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

Deploy a VPN connection by using a VPN device configuration profile.

Configure security settings by using an Endpoint Protection device configuration profile.

You support the management tasks.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Answer:

VPN device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Explanation

Graphical user interface, application Description automatically generated

VPN device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

▼
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-configure>

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-macos>

NEW QUESTION: 174

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

Name	Platform
Device1	Windows 10
Device2	Android 8.1.0
Device3	Android 10
Device4	iOS 12
Device5	iOS 14

All the devices have an app named App1 installed.

You need to prevent users from copying data from App1 and pasting the data into other apps.

Which policy should you create in Microsoft Endpoint Manager, and what is the minimum number of required policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Policy to create in Microsoft Endpoint Manager:

	▼
An app configuration policy	
An app protection policy	
A conditional access policy	
A device compliance policy	

Minimum number of required policies:

	▼
1	
2	
3	
5	

Answer:

Policy to create in Microsoft Endpoint Manager:

Minimum number of required policies:

An app configuration policy
An app protection policy
A conditional access policy
A device compliance policy

1
2
3
5

Explanation

Graphical user interface, application, table Description automatically generated

Policy to create in Microsoft Endpoint Manager:

Minimum number of required policies:

An app configuration policy
An app protection policy
A conditional access policy
A device compliance policy

1
2
3
5

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy>

NEW QUESTION: 175

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 the Azure Active Directory admin center, you create a conditional access policy.

Does this meet the goal?

A. No

B. Yes

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 176

You have a Microsoft 365 E5 tenant.

You need to evaluate compliance with European Union privacy regulations for customer data.

What should you do in the Microsoft 365 compliance center?

A. Create a Data Subject Request (DSR)

B. Create a data loss prevention (DLP) policy for General Data Protection Regulation (GDPR) data

C. Create an assessment based on the EU GDPR assessment template

D. Create an assessment based on the Data Protection Baseline assessment template

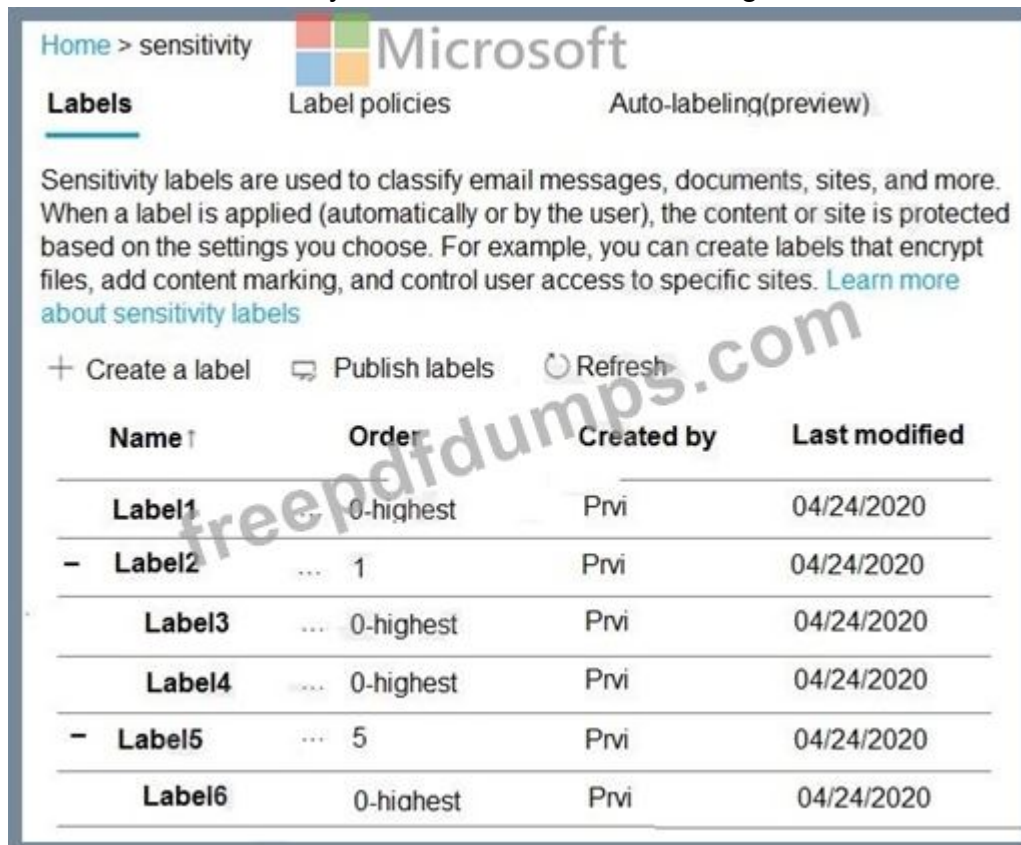
Answer: C ([LEAVE A REPLY](#))

Reference:

<https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan>

NEW QUESTION: 177

You have the sensitivity labels shown in the following exhibit.



Name ↑	Order	Created by	Last modified
Label1	0-highest	Pvi	04/24/2020
- Label2	1	Pvi	04/24/2020
Label3	0-highest	Pvi	04/24/2020
Label4	0-highest	Pvi	04/24/2020
- Label5	5	Pvi	04/24/2020
Label6	0-highest	Pvi	04/24/2020

Which labels can users apply to content?

- A. Label3, Label4, and Label6 only
- B. Label1, Label2, Label3, Label4, Label5, and Label6
- C. Label1, Label2, and Label5 only
- D. Label1, Label3, Label4, and Label6 only

Answer: D ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 178

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

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 179

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

Enable multi-factor authentication (MFA) for all users.

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
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☐
The SP800 assessment score will increase by 54 points.	☐	☐
The Data Protection Baseline score will increase by 9 points.	☐	☐

Answer:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☒
The SP800 assessment score will increase by 54 points.	☐	☒
The Data Protection Baseline score will increase by 9 points.	☒	☐

Explanation

Graphical user interface, text Description automatically generated

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	☐	☒
The SP800 assessment score will increase by 54 points.	☐	☒
The Data Protection Baseline score will increase by 9 points.	☒	☐

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-assessments?view=o365-world>

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-world>

NEW QUESTION: 180

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.

B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.

C. From the Microsoft 365 admin center, modify Organization information.

D. From the Microsoft 365 admin center, modify Help desk information.

Answer: ([SHOW ANSWER](#))

Reference:

<https://systemcenterdudes.com/intune-company-portal-customization/>

NEW QUESTION: 181

You create two device compliance policies for Android devices as shown in the following table.

Name	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 have the Android devices shown in the following table.

Name	User	Configuration
Android1	User1	Not encrypted
Android2	User2	Google Play services not configured
Android3	User3	Not encrypted Google Play services configured

The users belong to the groups shown in the following table.

User	Group
User1	Group1
User2	Group1, Group2
User3	Group2

The users enroll their device in Microsoft 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
The device of User1 is compliant.	☐	☐
The device of User2 is compliant.	☐	☐
The device of User3 is compliant.	☐	☐

Answer:

Statements	Yes	No
The device of User1 is compliant.	☒	☐
The device of User2 is compliant.	☐	☒
The device of User3 is compliant.	☒	☐

Explanation

Statements	Yes	No
The device of User1 is compliant.	☒	☐
The device of User2 is compliant.	☐	☒
The device of User3 is compliant.	☒	☐

References:

<https://docs.microsoft.com/en-us/intune-user-help/enroll-your-device-in-intune-android>

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 182

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.

Answer:

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-MLAgent 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.

Explanation

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-MLAgent 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.

References:

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

NEW QUESTION: 183

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: D (LEAVE A REPLY)

Explanation

References:

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

NEW QUESTION: 184

Which report should the New York office auditors view?

- A. DLP policy matches
- B. DLP false positives and overrides
- C. DLP incidents
- D. Top Senders and Recipients

Answer: C (LEAVE A REPLY)

Explanation

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies> This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

NEW QUESTION: 185

You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel.

What should you do in the Cloud App Security admin center?

- A. From Connected apps, add an app connector.
- B. From Automatic log upload, add a data source.
- C. From Security extension, add a SIEM agent.
- D. From Automatic log upload, add a log collector.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 186

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	 Microsoft	2	Yes

In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.

Users may register their devices with Azure AD

All None

Learn more on how this setting works



Microsoft

Require Multi-Factor Auth to join devices

Yes No

Maximum number of devices per user

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).
For each of the following statement, 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 enroll only five devices in Intune.	☐	☐
User1 can join only five devices to Azure AD.	☐	☐
User2 can enroll all the devices in Intune.	☐	☐

Answer:

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	☐	☒
User1 can join only five devices to Azure AD.	☐	☒
User2 can enroll all the devices in Intune.	☒	☐

Explanation

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	☐	☒
User1 can join only five devices to Azure AD.	☐	☒
User2 can enroll all the devices in Intune.	☒	☐

NEW QUESTION: 187

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

Answer:

Computer1:

	▼
Group1 only	
Group2 only	
Group1 and Group2	
Ungrouped machines	

Computer2:

	▼
Group1 only	
Group3 only	
Group1 and Group3	

Explanation

Computer1:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Group1 only</td></tr><tr><td colspan="2">Group2 only</td></tr><tr><td colspan="2">Group1 and Group2</td></tr><tr><td colspan="2">Ungrouped machines</td></tr></table>		▼	Group1 only		Group2 only		Group1 and Group2		Ungrouped machines	
	▼										
Group1 only											
Group2 only											
Group1 and Group2											
Ungrouped machines											
Computer2:	<table border="1"><tr><td></td><td>▼</td></tr><tr><td colspan="2">Group1 only</td></tr><tr><td colspan="2">Group3 only</td></tr><tr><td colspan="2">Group1 and Group3</td></tr></table>		▼	Group1 only		Group3 only		Group1 and Group3			
	▼										
Group1 only											
Group3 only											
Group1 and Group3											

NEW QUESTION: 188

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 ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 189

You have a Microsoft 365 E5 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that users can enroll devices in Microsoft Endpoint Manager without manually entering the address of Microsoft Endpoint Manager.

Which two DNS records should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a TXT record for EnterpriseRegistration.contoso.com
- B. a TXT record for EnterpriseEnrollment.contoso.com
- C. an SRV record for _SIPfederationTLS.contoso.com
- D. a CNAME record for AutoDiscover.contoso.com
- E. a CNAME record for EnterpriseEnrollment.contoso.com
- F. an SRV record for _SIP._TLS.contoso.com

Answer: E ([LEAVE A REPLY](#))

NEW QUESTION: 190

You plan to implement the endpoint protection device configuration profiles to support the planned changes.

You need to identify which devices will be supported, and how many profiles you should implement.

What should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

The screenshot shows the Microsoft Endpoint Manager console. On the left is the Microsoft logo. The main area has two dropdown menus. The first is labeled 'Supported devices:' and is open, showing a list of device selection options. The second is labeled 'Number of required profiles:' and is also open, showing a list of numbers from 1 to 5. A large, semi-transparent watermark 'reapondit.com' is overlaid diagonally across the center of the image.

Supported devices:
Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:
1
2
3
4
5

Answer:

Supported devices: 

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

1
2
3
4
5

Explanation

Table Description automatically generated

Supported devices: 

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2, and Device3
Device1, Device4, and Device5
Device1, Device2, Device3, Device4, and Device5

Number of required profiles:

1
2
3
4
5

Reference:

<https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create>

NEW QUESTION: 191

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles.

Which platform can you manage by using the profile?

- A. Ubuntu Linux
- B. macOS
- C. iOS
- D. Android

Answer: B ([LEAVE A REPLY](#))

Explanation

Intune device configuration profiles can be applied to Windows 10 devices and macOS devices

Note:

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

- * Windows 10
- * macOS

Other incorrect answer options you may see on the exam include the following:

- * Android Enterprise
- * Windows 8.1

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection-configure>

NEW QUESTION: 192

You have a Microsoft 365 E5 tenant.

Industry regulations require that the tenant comply with the ISO 27001 standard.

You need to evaluate the tenant based on the standard

- A. From the Microsoft 365 admin center enable the Productivity Score.
- B. From Compliance Manager, create an assessment
- C. From the Microsoft J6i compliance center, create an audit retention policy.
- D. From Policy in the Azure portal, select Compliance, and then assign a policy

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 193

You have a Microsoft 365 subscription.

All users have their email stored in Microsoft Exchange Online.

In the mailbox of a user named User1, you need to preserve a copy of all the email messages that contain the word ProjectX.

What should you do first?

- A. From Microsoft Defender for Cloud Apps, create an activity policy.
- B. From Microsoft 365 Defender, start a message trace.
- C. From the Exchange admin center create a mail flow rule.
- D. From the Microsoft Purview compliance portal, create a label and a label policy.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 194

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

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

Answer:

Settings to configure in Azure AD:	<table border="1"><tr><td>Device settings</td></tr><tr><td>Mobility (MDM and MAM)</td></tr><tr><td>Organizational relationships</td></tr><tr><td>User settings</td></tr></table>	Device settings	Mobility (MDM and MAM)	Organizational relationships	User settings
Device settings					
Mobility (MDM and MAM)					
Organizational relationships					
User settings					
Settings to configure in Intune:	<table border="1"><tr><td>Device compliance</td></tr><tr><td>Device configuration</td></tr><tr><td>Device enrollment</td></tr><tr><td>Mobile Device Management Authority</td></tr></table>	Device compliance	Device configuration	Device enrollment	Mobile Device Management Authority
Device compliance					
Device configuration					
Device enrollment					
Mobile Device Management Authority					

Explanation

Settings to configure in Azure AD:

Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority

References:

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

NEW QUESTION: 195

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution. After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You create an Azure Advanced Threat Protection (ATP) workspace named Workspace1.

The tenant contains the users shown in the following table.

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

You need to modify the configuration of the Azure ATP sensors.

Solution: You instruct User4 to modify the Azure ATP sensor configuration.

Does this meet the goal?

A. Yes

B. No

Answer: ([SHOW ANSWER](#))

Explanation

Only Azure ATP administrators can modify the sensors.

Any global administrator or security administrator on the tenant's Azure Active Directory is automatically an Azure ATP administrator.

References:

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

NEW QUESTION: 196

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

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

To which resources can you apply a sensitivity label by using an auto-labeling policy?

- A. Mailbox1 and Site1 only
- B. Mailbox1, Account1, and Site1 only
- C. Account1 and Site1 only
- D. Mailbox1, Account1, Site1, and Channel1
- E. Account1, Site1, and Channel1 only

Answer: E ([LEAVE A REPLY](#))

Reference:

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

Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!
Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: Freepdfdumps)

NEW QUESTION: 197

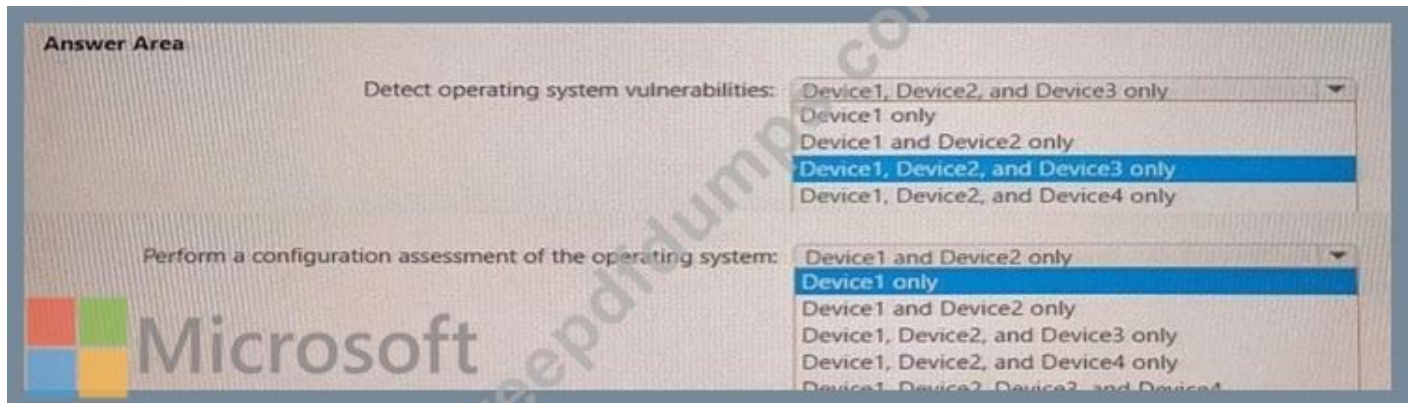
You have a Microsoft 365 E5 subscription that contains the devices shown in the following table.

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	Android
Device4	iOS

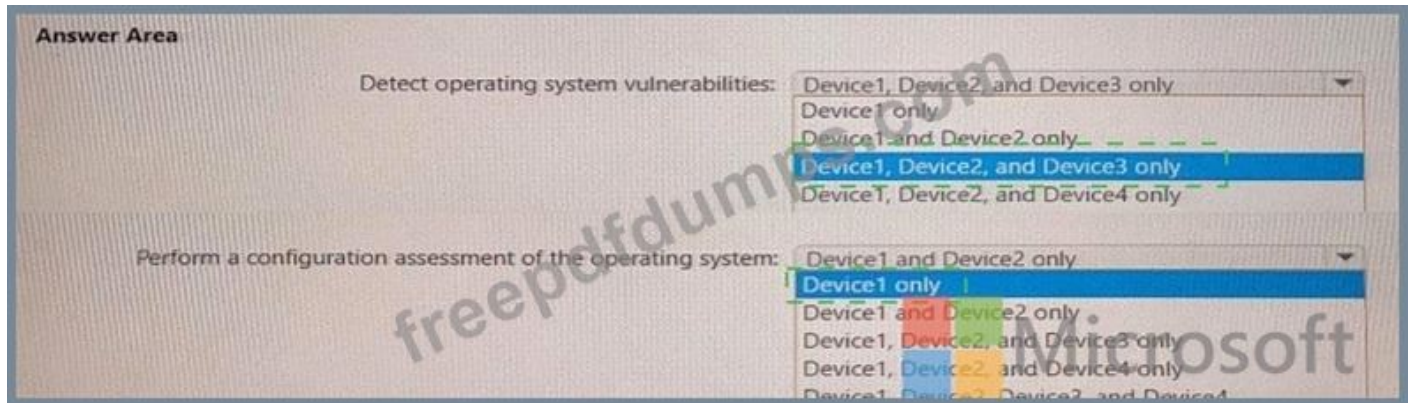
All the devices are onboarded To Microsoft Defender for Endpoint

You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

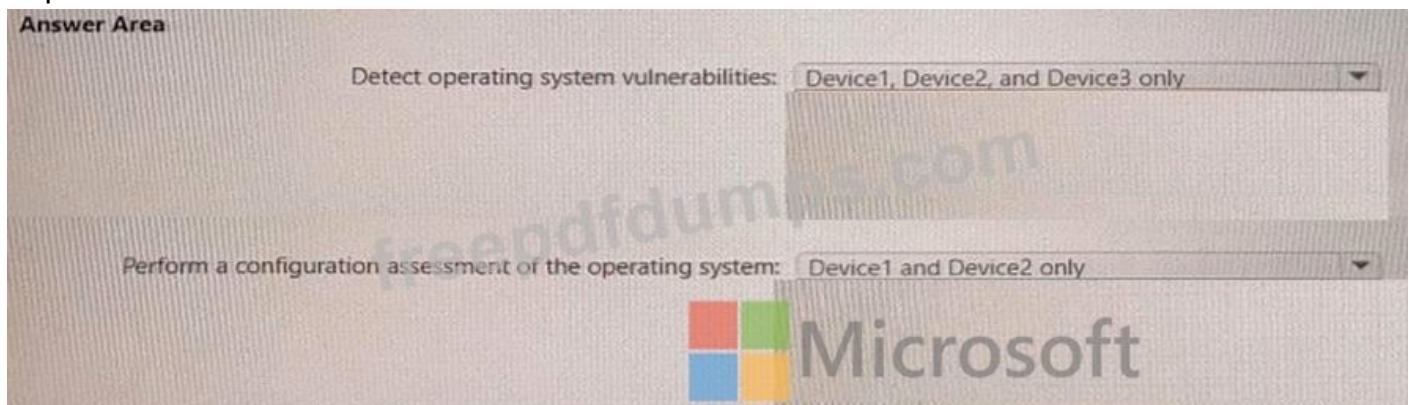
- * Detect operating system vulnerabilities.



Answer:



Explanation



Valid MS-101 Dumps shared by Actual4test.com for Helping Passing MS-101 Exam!

Actual4test.com now offer the **newest MS-101 exam dumps**, the Actual4test.com MS-101 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com MS-101 dumps with Test Engine here:

https://www.actual4test.com/MS-101_examcollection.html (408 Q&As Dumps, **30%OFF**

Special Discount: **Freepdfdumps**)