MS-101 Q&As

Microsoft 365 Mobility and Security

Pass Microsoft MS-101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ms-101.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

QUESTION 1

HOTSPOT

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

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

Answer Area

User1:

- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

User2:

- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

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

Answer Area

User1:

- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

User2:

- October 5, 2019
- October 10, 2019
- November 5, 2019
- November 10, 2019

You create a suppression rule that has the following settings:

1.

Triggering IOC: Any IOC

2.

Action: Hide alert

3.

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.

Hot Area:

Name	Machine group
Device1	ATP1
Device2	ATP1
Device3	ATP2

Correct Answer:

Name	Machine
Alert1	Device1
Alert2	Device2
Alert3	Device3

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

QUESTION 2

Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company has a Microsoft Azure Active Directory (Azure AD) tenant.

You have been tasked with assigning a user the minimum required role to allow him to sign up for Microsoft Store for Business.

Solution: You assign the user the Purchasing role.

Does the solution meet the goal?

A. Yes

B. No

Correct Answer: B

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

QUESTION 3

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

Name	Windows 10 edition	Azure Active Directory (Azure AD)	Mobile device management (MDM) enrollment
Device1	Windows 10 Pro	Registered	Microsoft Intune
Device2	Windows 10 Enterprise	Joined	Microsoft Intune
Device3	Windows 10 Pro	Joined	Not enrolled
Device4	Windows 10 Enterprise	Registered	Microsoft Intune
Device5	Windows 10 Enterprise	Joined	Not enrolled

You add custom apps to the private store in Microsoft Store Business.

You plan to create a policy to show only the private store in Microsoft Store for Business.

To which devices can the policy be applied?

A. Device2 only

B. Device1 and Device3 only

C. Device1 and Device3 only

D. Device2, Device3, and Device5 only

E. Device1, Device2, Device3, Device4, and Device5

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-store/manage-access-to-private-store#show-private-store-only-using-mdm-policy

QUESTION 4

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 and 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

Correct Answer: D

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

QUESTION 5

HOTSPOT

You need to meet the technical requirement for log analysis.

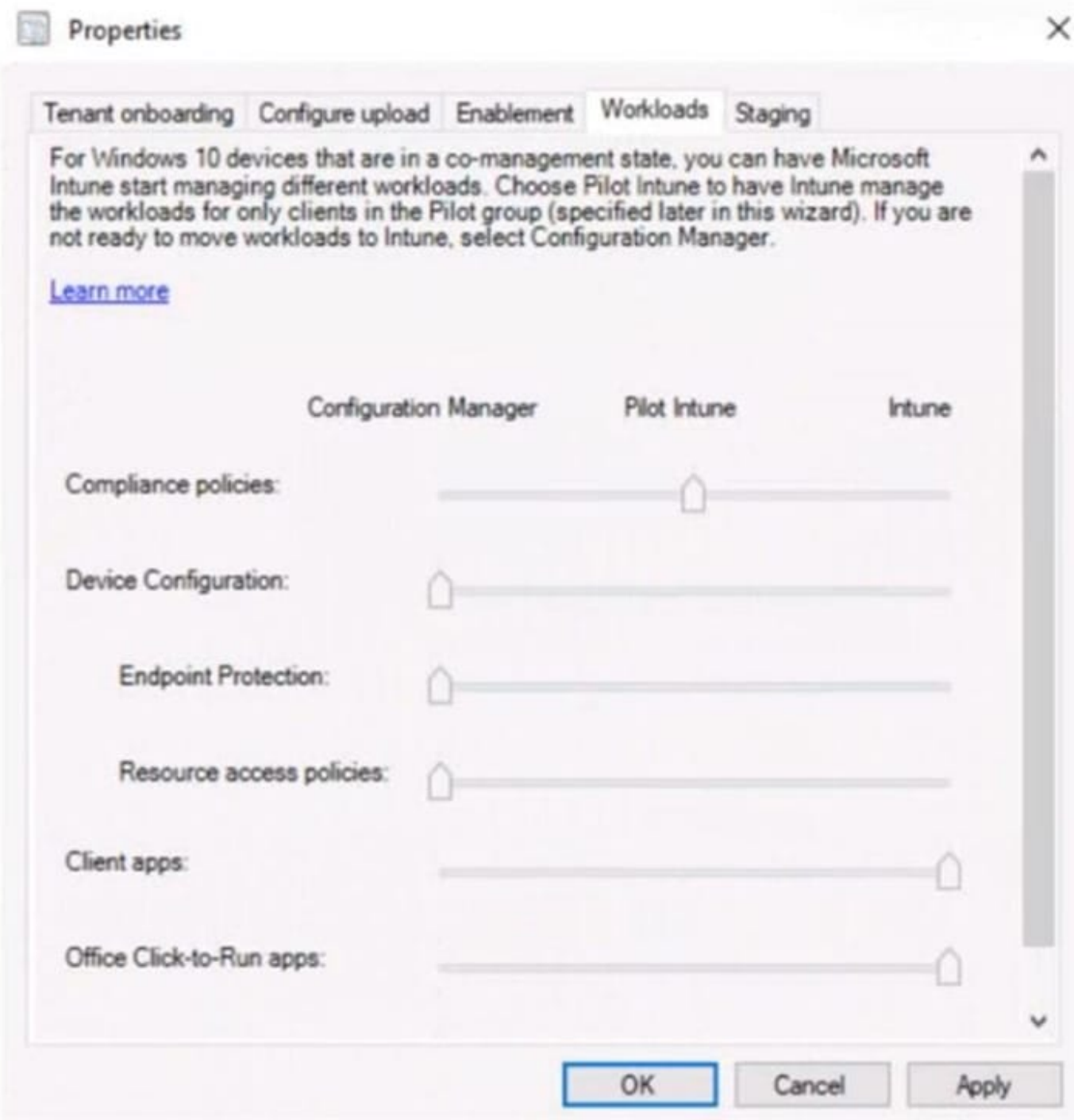
What is the minimum number of data sources and log collectors you should create from Microsoft Cloud App Security? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	○	○
Device2 has an overall compliance state of Not compliant.	○	○
Device3 has an overall compliance state of In grace period.	○	○

Correct Answer:



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

QUESTION 6

You have a Microsoft 365 E5 tenant.

You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.

What should you use to create the policy?

A. the Microsoft 365 admin center

B. the Microsoft 365 compliance center

C. the Microsoft Defender for Cloud Apps portal

D. the Microsoft Apps admin center

Correct Answer: B

Explanation:

Real-Time Alerting with Microsoft 365 Alert Policies

Microsoft 365 suite comes with a large set of apps and services, with most of them having a user-friendly interface. However, Microsoft 365 suite is very vast and includes an extensive list of audit logs of all actions performed in an

organization. Thus, it has become difficult and time-consuming for the administrators to monitor the suspicious activities and unauthorized actions that are taking place. This is where Microsoft 365 Alert Policies come in.

Using the Alert Policies feature available in the Compliance Center and Microsoft 365 Defender/Security admin center, you can combat this problem. With the help of alert policies, you can monitor user activities and security incidents, such as

phishing, unusual external user activities, suspicious massive file or folder deletions, and more.

Reference: https://o365reports.com/2022/03/10/real-time-alerting-with-microsoft-365-alert-policies/

QUESTION 7

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 and 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.

Correct Answer: D

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

---

QUESTION 8

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 the Security and Compliance admin center, create a data loss prevention (DLP) policy.

B. From the Security and Compliance admin center, create a label and label policy.

C. From the Security and Compliance admin center, create, create a label and a label policy.

D. From the Security and Compliance admin center, start a message trace.

E. From the Exchange admin center, start a mail flow message trace

Correct Answer: A

A DLP policy contains a few basic things:

Where to protect the content: locations such as Exchange Online, SharePoint Online, and OneDrive for Business sites, as well as Microsoft Teams chat and channel messages.

When and how to protect the content by enforcing rules comprised of:

Conditions the content must match before the rule is enforced. For example, a rule might be configured to look only for content containing Social Security numbers that\\'s been shared with people outside your organization.

Actions that you want the rule to take automatically when content matching the conditions is found. For example, a rule might be configured to block access to a document and send both the user and compliance officer an email notification.

References:

https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies

QUESTION 9

HOTSPOT

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

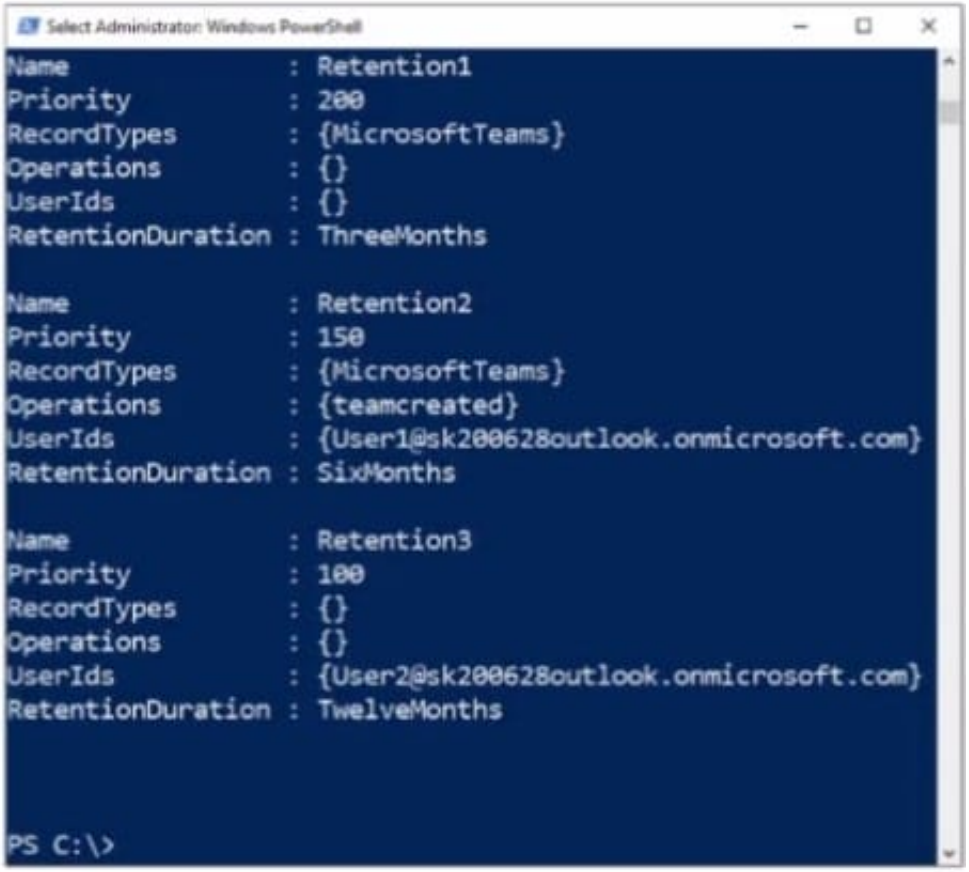
Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

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.

Hot Area:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	○	○
Sensitivity1 is applied to File2.txt.	○	○
Sensitivity1 is applied to File3.xlsx.	○	○

Correct Answer:

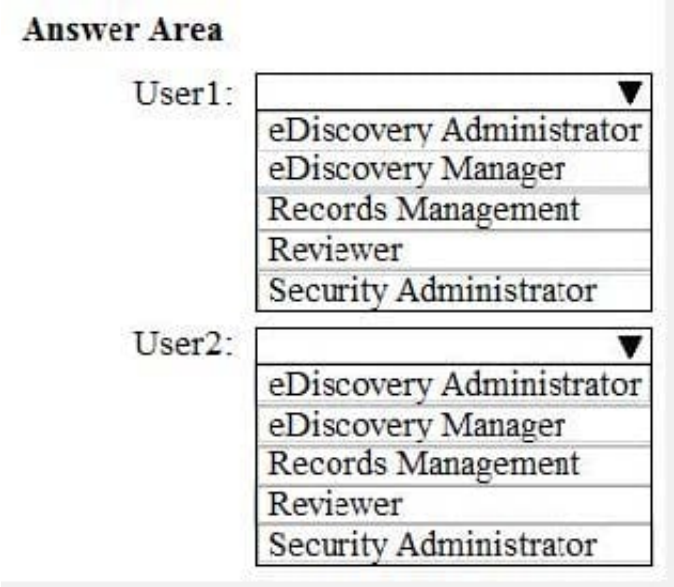


QUESTION 10

HOTSPOT

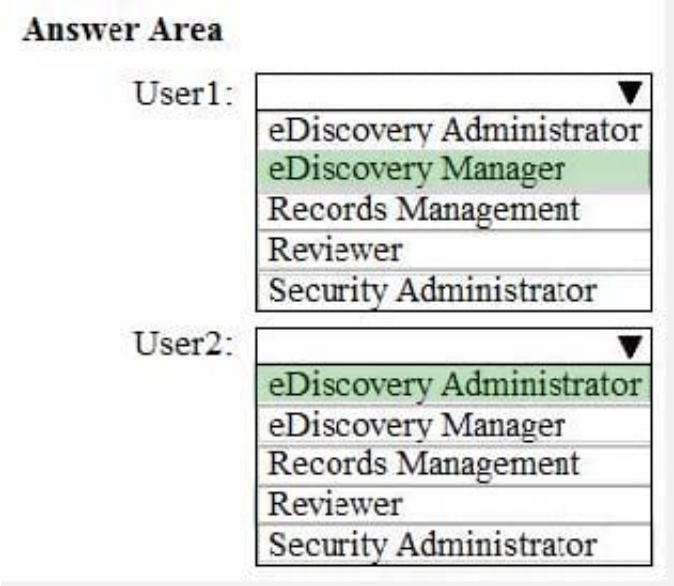
You have a Microsoft 365 tenant.

You plan to create a retention policy as shown in the following exhibit.

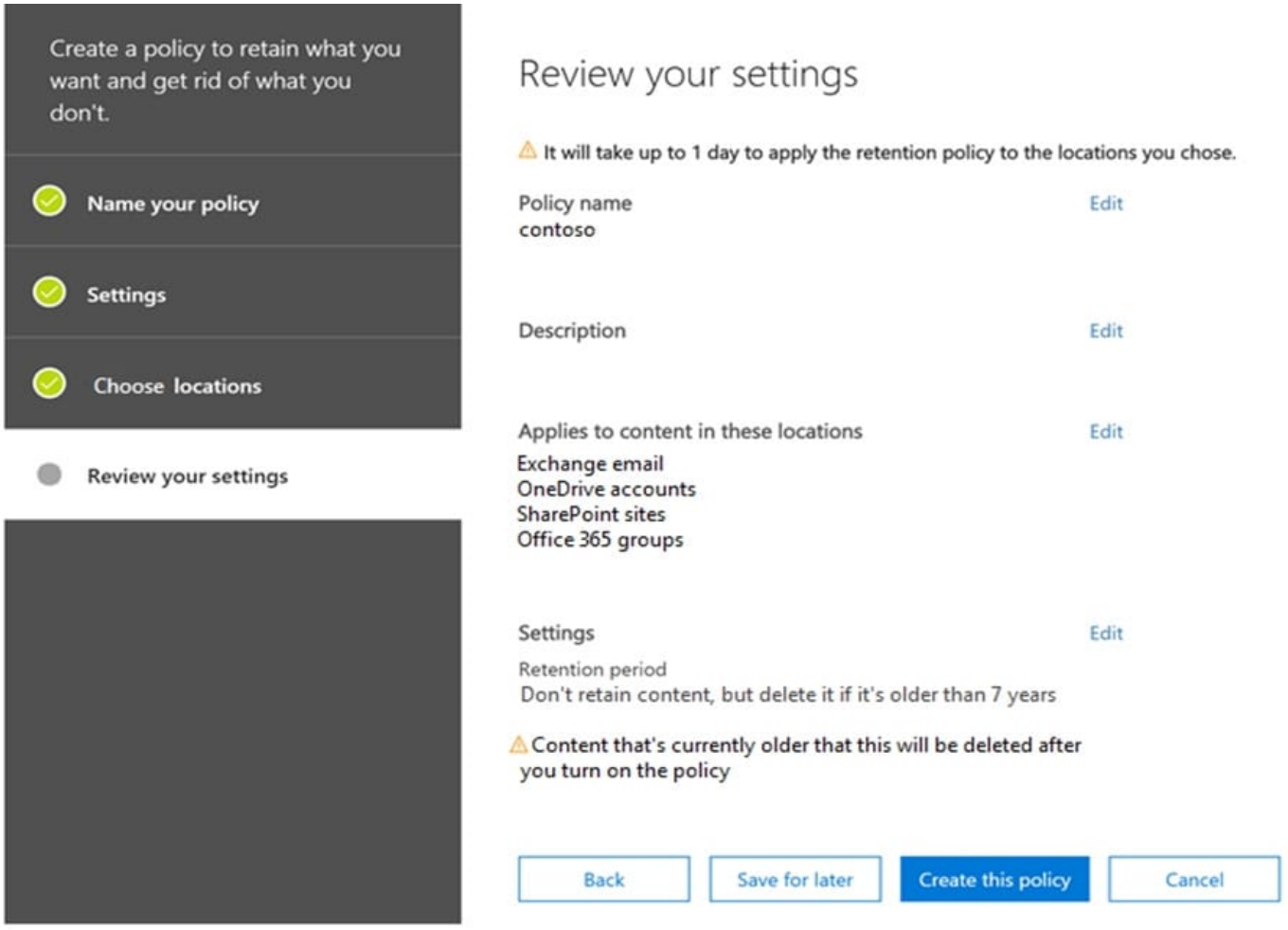


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 11

HOTSPOT

You have several devices enrolled in Microsoft Intune.

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

You can open File1 from:

- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

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

- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

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

You can open File1 from:

- App1 only
- **App1 and App2 only**
- App1 and App3 only
- App1, App2 and App3

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

- App1 only
- **App3 only**
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

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.

Hot Area:

Name	Role	Member of
User1	Cloud device administrator	Group A
User2	Intune administrator	Group B
User3	*None*	*None*

Correct Answer:

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group A
2	Policy2	10	Group B
Default	All users	5	All users

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

QUESTION 12

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

Correct Answer: A

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

QUESTION 13

You have a Microsoft 365 E5 subscription.

You plan to deploy 100 new Windows 10 devices.

You need to identify the appropriate version of Windows 10 for the new devices. The version must meet the following requirements:

1.

Be serviced for a minimum of 24 months.

2.

Support Microsoft Application Virtualization (App-V). Which version should you identify?

A. Windows 10 Pro, version 1909

B. Windows 10 Pro, version 2004

C. Windows 10 Enterprise, version 1909

D. Windows 10 Enterprise, version 2004

Correct Answer: D

Reference: https://docs.microsoft.com/en-us/windows/release-health/release-information

https://docs.microsoft.com/en-us/windows/application-management/app-v/appv-supported-configurations

QUESTION 14

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

Correct Answer: A

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

QUESTION 15

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

You have a Microsoft 365 subscription.

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

You need to be notified if the SharePoint sharing policy is modified in the future.

Solution: From the SharePoint site, you create an alert.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Latest MS-101 Dumps MS-101 Study Guide MS-101 Exam Questions