Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam

NEW QUESTION 1
- (Exam Topic 1)
On which server should you use the Defender for identity sensor?

A. Server1
B. Server2
C. Server3
D. Server4
E. Servers5

Answer: A

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 2
- (Exam Topic 1)
As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date
References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

NEW QUESTION 3
- (Exam Topic 1)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).
You configure a pilot for co-management.
You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.
You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the
collection.
Does this meet the goal?

A. Yes
B. NO

Answer: A

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

NEW QUESTION 4

- (Exam Topic 2)
You need to meet the technical requirement for the EU PII data. What should you create?

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

Answer: A

Explanation:
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies
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.

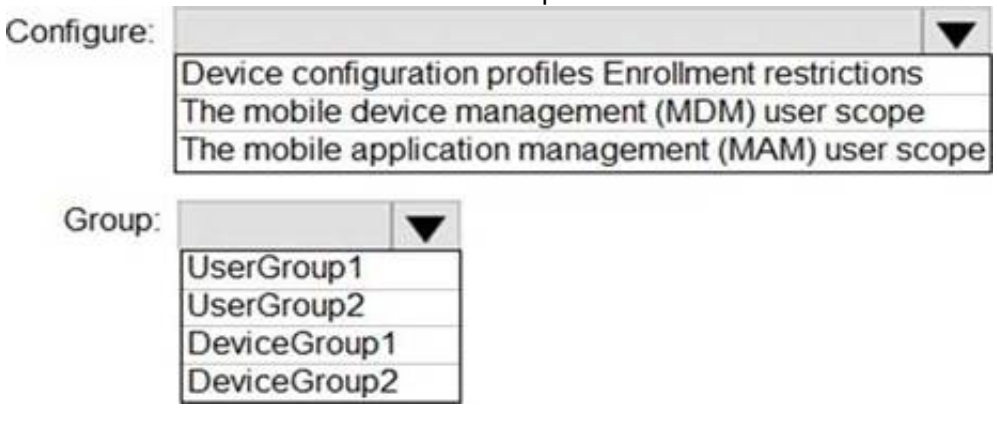
NEW QUESTION 5
- (Exam Topic 2)
Which report should the New York office auditors view?

A. DLP policy matches
B. DLP false positives and overrides
C. DLP incidents
D. Top Senders and Recipients

Answer: C

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 6
- (Exam Topic 3)
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.

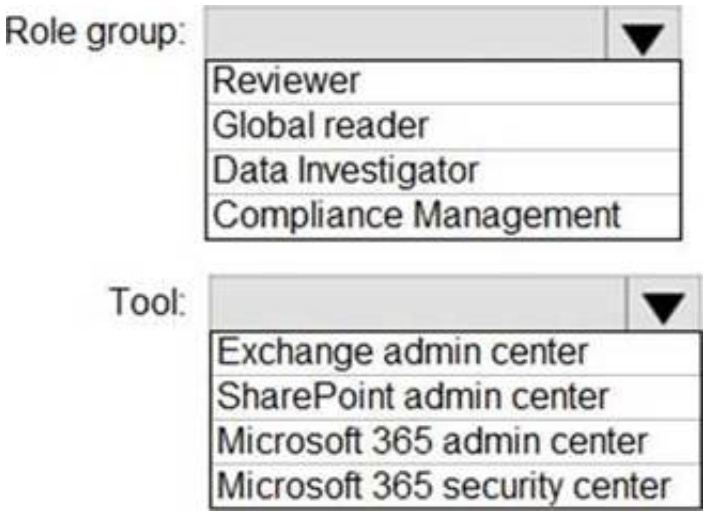


A. Mastered
B. Not Mastered

Answer: A

Explanation:
Text Description automatically generated with medium confidence
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

NEW QUESTION 7
- (Exam Topic 3)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?vi

NEW QUESTION 8
- (Exam Topic 4)
Which role should you assign to User1?
Available Choices (select all choices that are correct)

A. Hygiene Management
B. Security Reader
C. Security Administrator
D. Records Management

Answer: B

Explanation:
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management, as well as the ability to read Azure Active Directory sign-in reports and audit logs, and in Office 365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

NEW QUESTION 9
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains the users in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

In Microsoft Endpoint Manager, you create two device type restrictions that have the settings shown in the following table.

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

In Microsoft Endpoint Manager, you create three device limit restrictions that have the settings shown in the following table.

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	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
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	○	○
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	○	○
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	○	○

NEW QUESTION 10
- (Exam Topic 5)
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/	User1
contoso.onmicrosoft.com/	Sites/User1
contoso.sharepoint.com/	contoso_onmicrosoft_com/User1
contoso-my.sharepoint.com/	personal/User1_contoso_onmicrosoft_com

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-ediscovery-holds

NEW QUESTION 10
- (Exam Topic 5)
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

NEW QUESTION 13

- (Exam Topic 5)
You have a hybrid Azure Active Directory (Azure AD) tenant and a Microsoft Endpoint Configuration Manager deployment.
You have the devices shown in the following table.

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

You plan to enable co-management.
You need to identify which devices support co-management without requiring the installation of additional software.
Which devices should you identify?

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

Answer: D

NEW QUESTION 15
- (Exam Topic 5)
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. Configure the Endpoint analytics baseline regression threshold.
B. Create a configuration profile.
C. Create a Windows 10 Security Baseline profile
D. Create a compliance policy.

Answer: B

NEW QUESTION 20
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You register two applications named App1 and App2 to Azure AD.
You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

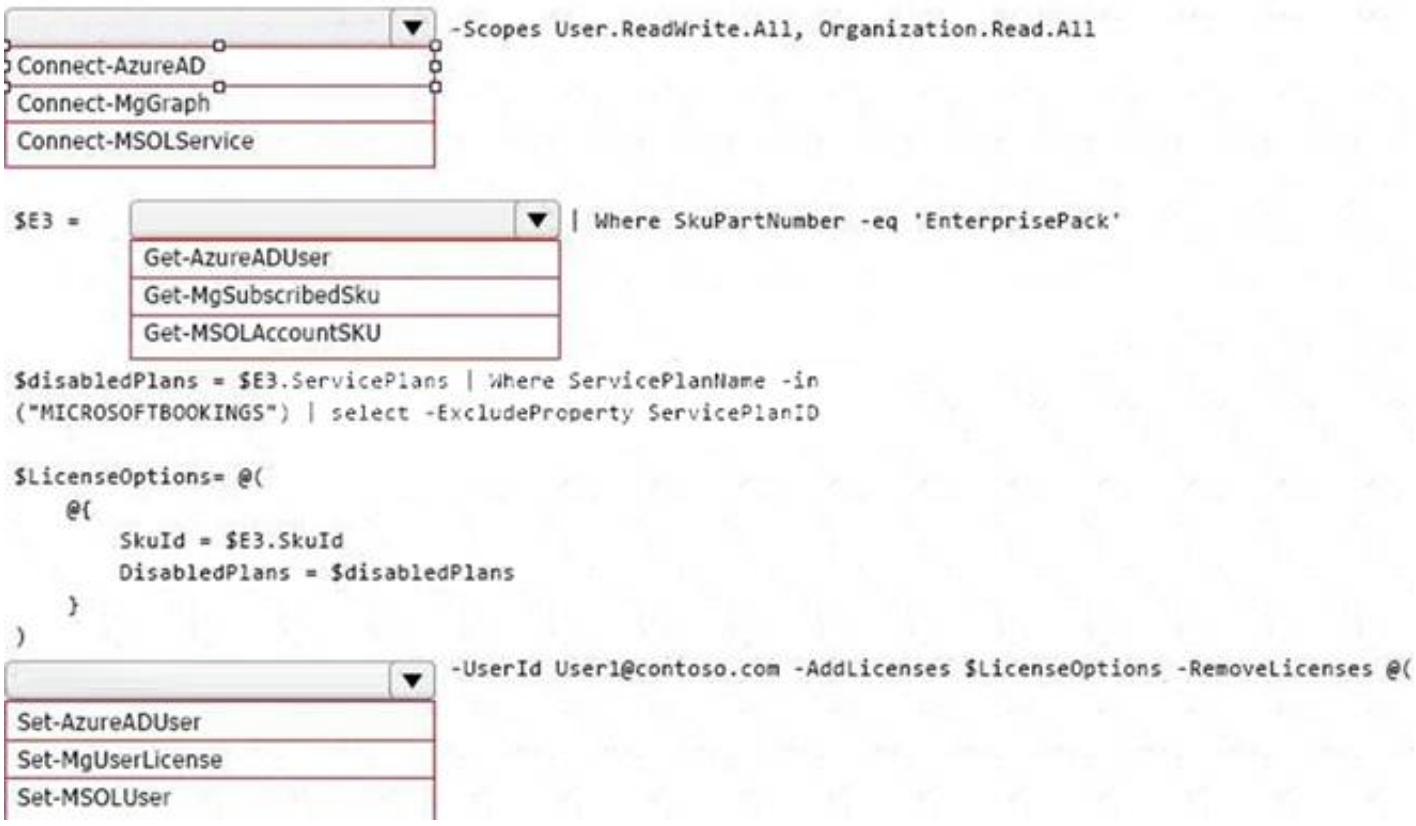
A. From the Microsoft Entra admin center, create a conditional access policy
B. From the Microsoft 365 admin center, configure the Modem authentication settings.
C. From the Enterprise applications blade of the Microsoft Entra admin center, configure the Users settings.
D. From Multi-Factor Authentication, configure the service settings.

Answer: A

Explanation:
Use Conditional Access policies
If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati

NEW QUESTION 24
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription.
A user named user1@contoso.com was recently provisioned.
You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Connect-MgGraph
Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK
First, connect to your Microsoft 365 tenant.
Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.
The Organization.Read.All permission scope is required to read the licenses available in the tenant. Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All
Box 2: Get-MgSubscribedSku
Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.
Box 3: Set-MgUserLicense
Assigning licenses to user accounts
To assign a license to a user, use the following command in PowerShell.
Set-MgUserLicense -UserId $userUPN -AddLicenses @{SkuId = "<SkuId>"} -RemoveLicenses @() This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user
belindan@litwareinc.com:
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{SkuId = $e5Sku.SkuId}
-RemoveLicenses @()
Reference:
https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365

NEW QUESTION 28
- (Exam Topic 5)
Your company has a Microsoft 365 subscription.
You need to identify all the users in the subscription who are licensed for Office 365 through a group membership. The solution must include the name of the group used to assign the license.
What should you use?

A. Active users in the Microsoft 365 admin center
B. Reports in Microsoft Purview compliance portal
C. the Licenses blade in the Microsoft Entra admin center
D. Reports in the Microsoft 365 admin center

Answer: D

Explanation:
Microsoft 365 Reports in the admin center
You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.
Which activity reports are available in the admin center
Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	N/A[1]	N/A[1]	N/A[1]	N/A[1]
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/activity-reports

NEW QUESTION 29
- (Exam Topic 5)
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: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION 31
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You create an auto-labeling policy to encrypt emails that contain a sensitive info type. You specify the locations where the policy will be applied.
You need to deploy the policy. What should you do first?

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

Answer: C

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

NEW QUESTION 35
- (Exam Topic 5)
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

Explanation:
Reference:
https://docs.microsoft.com/en-us/compliance/regulatory/gdpr-action-plan

NEW QUESTION 38
- (Exam Topic 5)
Your network contains an on-premises Active Directory domain named contoso.local. The domain contains five domain controllers.
Your company purchases Microsoft 365 and creates an Azure AD tenant named contoso.onmicrosoft.com. You plan to install Azure AD Connect on a member server and implement pass-through authentication. You need to prepare the environment for the planned implementation of pass-through authentication. Which three actions should you perform? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. From a domain controller install an Authentication Agent
B. From the Microsoft Entra admin center, confiqure an authentication method.
C. From Active Director,' Domains and Trusts add a UPN suffix
D. Modify the email address attribute for each user account.

E. From the Microsoft Entra admin center, add a custom domain name.
F. Modify the User logon name for each user account.

Answer: ABE

Explanation:
Deploy Azure AD Pass-through Authentication Step 1: Check the prerequisites
Ensure that the following prerequisites are in place. In the Entra admin center
* 1. Create a cloud-only Hybrid Identity Administrator account or a Hybrid Identity administrator account on your Azure AD tenant. This way, you can manage the configuration of your tenant should your on-premises services fail or become unavailable.
(E) 2. Add one or more custom domain names to your Azure AD tenant. Your users can sign in with one of these domain names.
(A) In your on-premises environment
* 1. Identify a server running Windows Server 2016 or later to run Azure AD Connect. If not enabled already, enable TLS 1.2 on the server. Add the server to the same Active Directory forest as the users whose passwords you need to validate. It should be noted that installation of Pass-Through Authentication agent on Windows Server Core versions is not supported.
* 2. Install the latest version of Azure AD Connect on the server identified in the preceding step. If you already have Azure AD Connect running, ensure that the version is supported.
* 3. Identify one or more additional servers (running Windows Server 2016 or later, with TLS 1.2 enabled) where you can run standalone Authentication Agents. These additional servers are needed to ensure the high availability of requests to sign in. Add the servers to the same Active Directory forest as the users whose passwords you need to validate.
* 4. Etc.
(B) Step 2: Enable the feature
Enable Pass-through Authentication through Azure AD Connect.
If you're installing Azure AD Connect for the first time, choose the custom installation path. At the User
sign-in page, choose Pass-through Authentication as the Sign On method. On successful completion, a Pass-through Authentication Agent is installed on the same server as Azure AD Connect. In addition, the Pass-through Authentication feature is enabled on your tenant.
Incorrect:
Not C: From Active Directory Domains and Trusts, add a UPN suffix Not D. Modify the email address attribute for each user account.
Not F. Modify the User logon name for each user account. Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/how-to-connect-pta-quick-start

NEW QUESTION 43
- (Exam Topic 5)
You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.
You need to centrally monitor System log events from the computers.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

In Azure:
- Add and configure the Diagnostics settings for the Azure Activity Log.
- Add and configure an Azure Log Analytics workspace.
- Add an Azure Storage account and Azure Cognitive Search
- Add an Azure Storage account and a file share.

On the computers:
- Create an event subscription.
- Modify the membership of the Event Log Readers group.
- Enroll in Microsoft Endpoint Manager.
- Install the Microsoft Monitoring Agent.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer

NEW QUESTION 45
- (Exam Topic 5)
HOTSPOT
You have an Azure AD tenant named contoso.com that contains the users shown in the following table.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1	Enforced

Multi-factor authentication (MFA) is configured to use 131.107.5.0/24 as trusted IPs. The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Location1	131.107.20.0/24	Yes
Location2	131.107.50.0/24	Yes

You create a conditional access policy that has the following configurations:
- Users or workload identities assignments: All users
- Cloud apps or actions assignment: App1
- Conditions: Include all trusted locations
- Grant access: Require multi-factor authentication

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
When User1 connects to App1 from a device that has an IP address of 131.107.50.10, User1 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	○	○
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
* 131.107.50.10 is in a Trusted Location so the conditional access policy applies. The policy requires MFA. However, User1's MFA status is disabled. The MFA requirement in the conditional access policy will override the user's MFA status of disabled. Therefore, User1 must use MFA.
Box 2: Yes.
* 131.107.20.15 is in a Trusted Location so the conditional access policy applies. The policy requires MFA so User2 must use MFA.
Box 3: No.
IP not from Trusted Location so Policy does not apply, Subnet 131.107.5.5 is not in the range of 131.107.50.0/24
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

NEW QUESTION 50
- (Exam Topic 5)
DRAG DROP
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

A. Mastered
B. Not Mastered

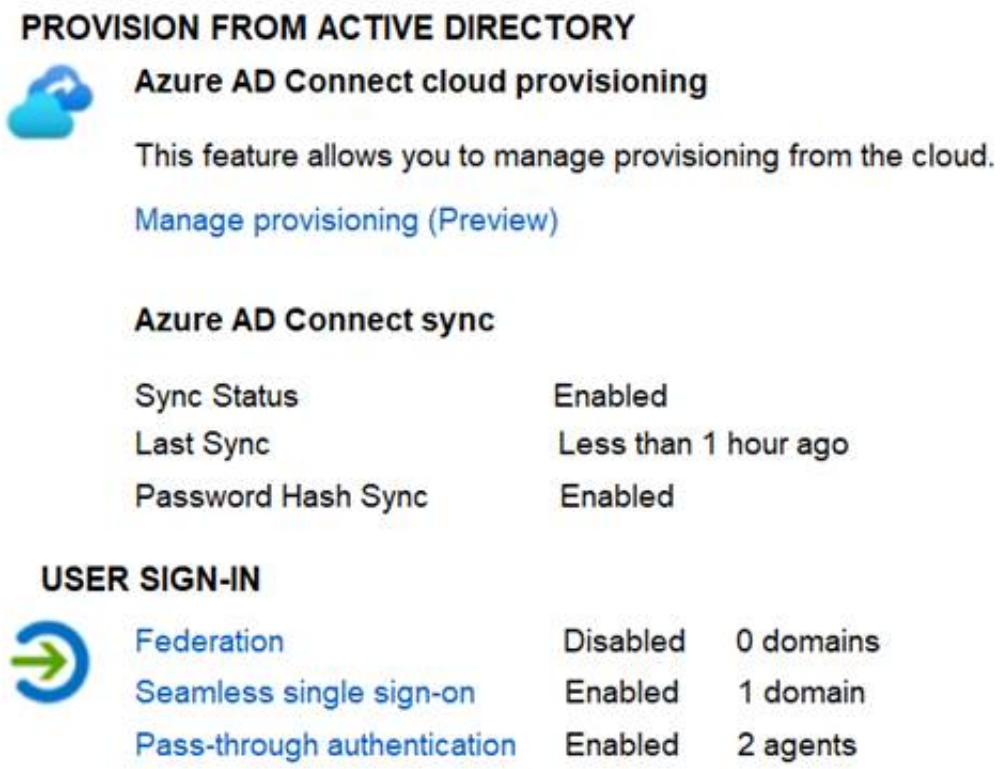
Answer: A

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

NEW QUESTION 55
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

The domain syncs to an Azure AD tenant named contoso.com as shown in the exhibit. (Click the Exhibit tab.)



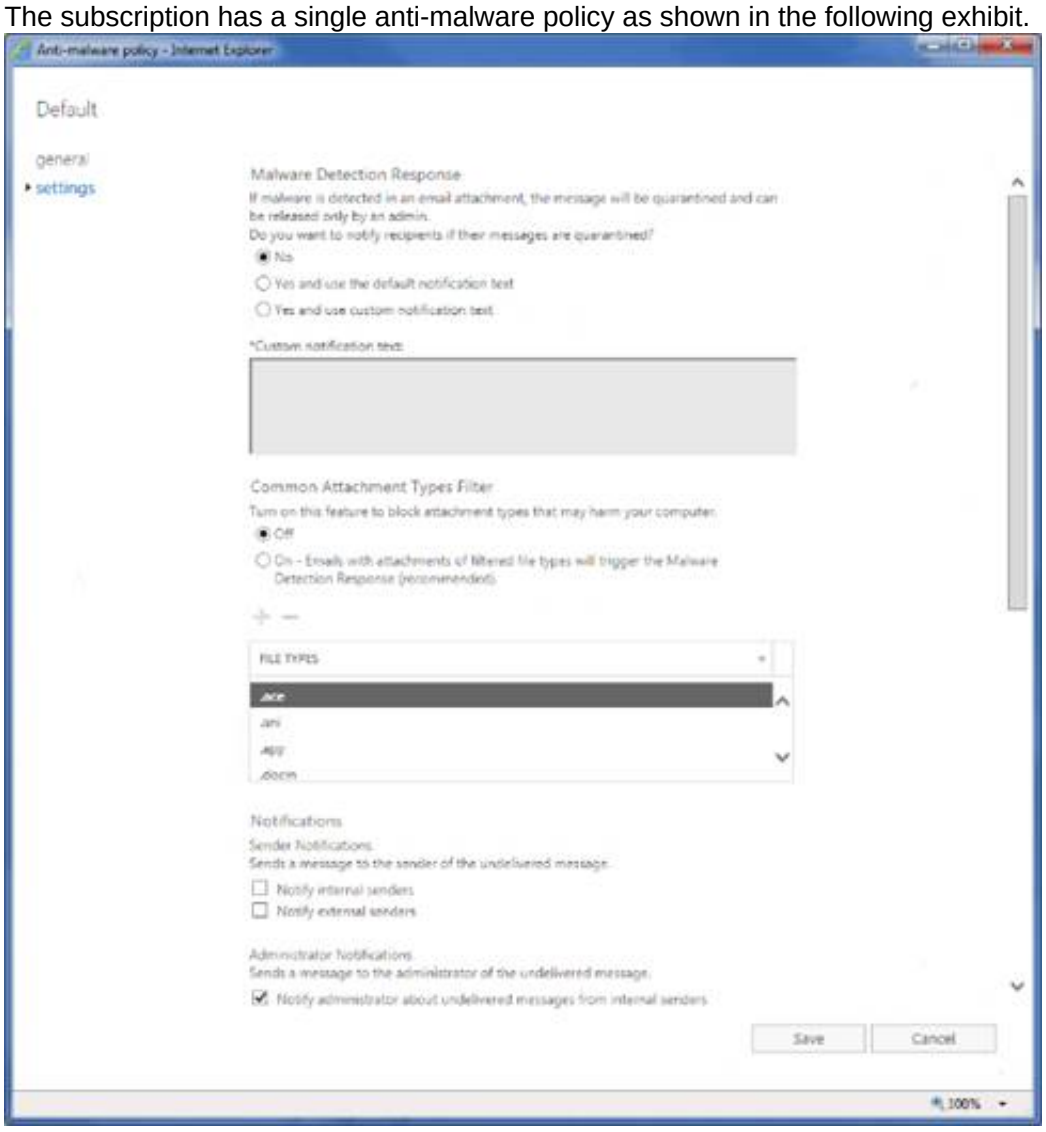
User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD.
Solution: From the on-premises Active Directory domain, you set the UPN suffix for User2 to @contoso.com. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:
The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

NEW QUESTION 56
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains a user named User1.
The subscription has a single anti-malware policy as shown in the following exhibit.



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

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

D. Both attachments will be remove
E. The email message will be quarantined, and User1 will receive a copy of the message containing the original text and a new attachment that includes the following text: 'Malware was removed."
F. The malware-infected attachment will be remove
G. The email message will be quarantined, and User1 will receive a copy of the message containing only the uninfected attachment.

Answer: C

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

NEW QUESTION 61
- (Exam Topic 5)
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

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/ios-enroll

NEW QUESTION 62
- (Exam Topic 5)
You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

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

Which users will receive the weekly digest email automatically?

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

Answer: E

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

NEW QUESTION 64
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You need to ensure that administrators are notified when a user receives an email message that contains malware. The solution must use the principle of least privilege.
Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 65

- (Exam Topic 5)

DRAG DROP

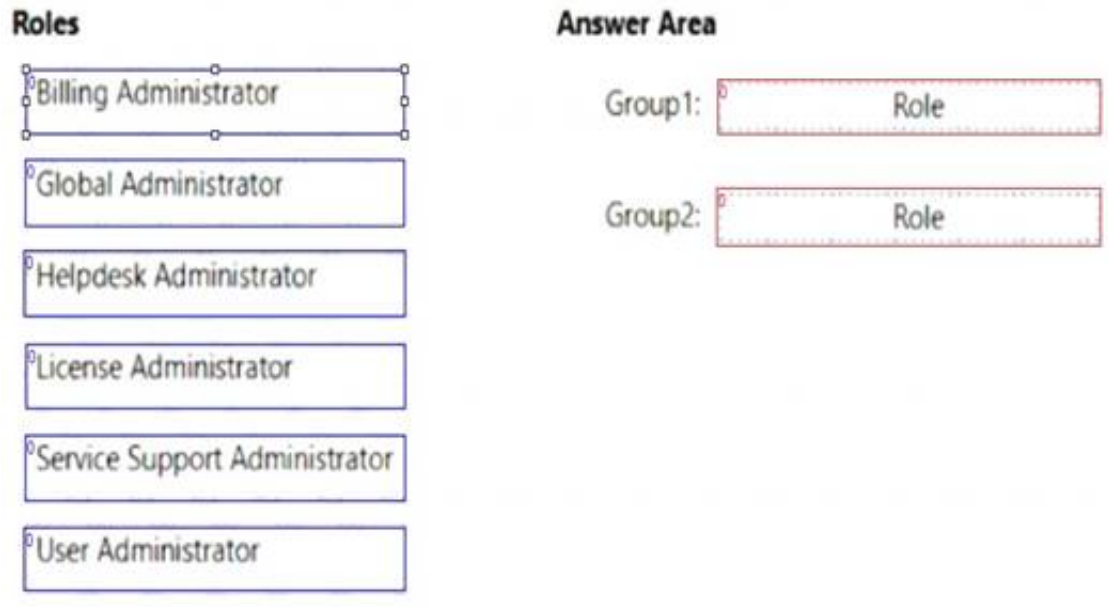
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2. You need to ensure that each group can perform the tasks shown in the following table.

Group	Task
Group1	• Manage service requests. • Purchase new services. • Manage subscriptions. • Monitor service health.
Group2	• Assign licenses. • Add users and groups. • Create and manage user views. • Update password expiration policies.

The solution must use the principle of least privilege.

Which role should you assign to each group? To answer, drag the appropriate roles to the correct groups. Each role 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.



A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Billing admin manage service request

Purchase new services Etc.

Assign the Billing admin role to users who make purchases, manage subscriptions and service requests, and monitor service health.

Box 2: User admin User admin

Assign the User admin role to users who need to do the following for all users:

- Add users and groups
- Assign licenses
- Manage most users properties
- Create and manage user views
- Update password expiration policies
- Manage service requests
- Monitor service health Reference:

https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles

NEW QUESTION 68

- (Exam Topic 5)

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

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

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

Devices that can onboarded to Microsoft Defender for Endpoint:
- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:
- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 71
- (Exam Topic 5)
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)	Last	*Not applicable*

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

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

Answer Area

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

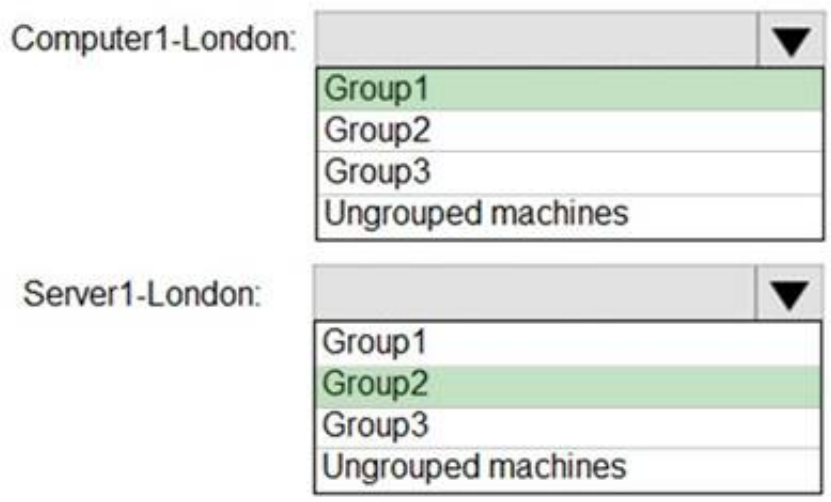
Server1-London:
- Group1
- Group2
- Group3
- Ungrouped machines

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area



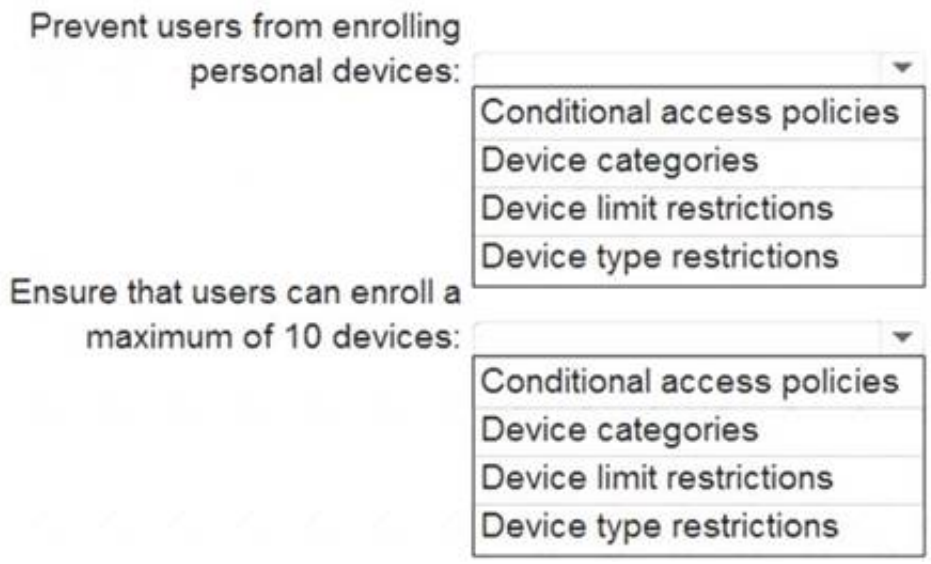
NEW QUESTION 73
- (Exam Topic 5)
You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that Used can place a hold on all mailbox content. What permission should you assign to User1?

A. the Information Protection administrator ide from the Azure Active Directory admin center.
B. the eDiscovery Manager tote from the Microsoft 365 compliance center.
C. the Compliance Management role from the Exchange admin center.
D. the User management administrator role from the Microsoft 365 admin center.

Answer: B

NEW QUESTION 74
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune. You need to configure Intune to meet the following requirements:
- Prevent users from enrolling personal devices.
- Ensure that users can enroll a maximum of 10 devices.

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



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 79
- (Exam Topic 5)
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

Explanation:
Reference:
https://docs.microsoft.com/en-us/deployedge/configure-edge-with-intune

NEW QUESTION 83
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant.
You plan to deploy a monitoring solution that meets the following requirements:
- Captures Microsoft Teams channel messages that contain threatening or violent language.
- Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

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

Answer: C

NEW QUESTION 86
- (Exam Topic 5)
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: D

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

NEW QUESTION 87
- (Exam Topic 5)
Your network contains an Active Directory domain named adatum.com that is synced to Azure AD. The domain contains 100 user accounts.
The city attribute for all the users is set to the city where the user resides.
You need to modify the value of the city attribute to the three-letter airport code of each city. What should you do?

A. From Windows PowerShell on a domain controller, run the Gec-ADUser and Sec-ADUser cmdlets.
B. From Azure Cloud Shell, run the Gec-ADUser and Sec-ADUser cmdlets.
C. From Windows PowerShell on a domain controller, run the Gec-MgUser and Updace-MgUser cmdlets.
D. From Azure Cloud Shell, run the Gec-MgUser and Update-MgUser cmdlets.

Answer: A

Explanation:
The user accounts are synced from the on-premise Active Directory to the Microsoft Azure Active Directory (Azure AD). Therefore, the city attribute must be changed in the on-premise Active Directory.
You can use Windows PowerShell on a domain controller and run the Get-ADUser cmdlet to get the required users and pipe the results into Set-ADUser cmdlet to modify the city attribute.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
* 1. From Windows PowerShell on a domain controller, run the Get-ADUser and Set-ADUser cmdlets.
* 2. From Active Directory Administrative Center, select the Active Directory users, and then modify the Properties settings.
Other incorrect answer options you may see on the exam include the following:
* 1. From the Azure portal, select all the Azure AD users, and then use the User settings blade.
* 2. From Windows PowerShell on a domain controller, run the Get-AzureADUser and Set-AzureADUser cmdlets.
* 3. From the Microsoft 365 admin center, select the users, and then use the Bulk actions option.
* 4. From Azure Cloud Shell, run the Get-ADUser and Set-ADUser cmdlets. Reference:
https://docs.microsoft.com/en-us/powershell/module/addsadministration/set-aduser

NEW QUESTION 88
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant. Users store data in the following locations:
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Exchange Online
- Microsoft SharePoint Online

You need to retain Microsoft 365 data for two years.
What is the minimum number of retention policies that you should create?

A. 1
B. 2

C. 3
D. 4

Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-retention-policies?view=o365-worldwide

NEW QUESTION 90
- (Exam Topic 5)
You are reviewing alerts in the Microsoft 365 Defender portal.
How long are the alerts retained in the portal?

A. 30 days
B. 60 days
C. 3 months
D. 6 months
E. 12 months

Answer: C

Explanation:
Data retention information for Microsoft Defender for Office 365
By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.
Defender for Office 365 Plan 1
* Alert metadata details (Microsoft Defender for Office alerts) 90 days.
Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention

NEW QUESTION 93
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

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

Site1 contains the files shown in the following table.

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

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

Answer Area

File1.docx:
- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:
- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 96
- (Exam Topic 5)
You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.

How long after the Azure ATP cloud service is updated will the sensor update?

A. 20 hours
B. 12 hours
C. 7 hours
D. 48 hours

Answer: B

NEW QUESTION 100
- (Exam Topic 5)
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. OneDrive accounts
B. Exchange email
C. Teams chat and channel messages
D. SharePoint sites

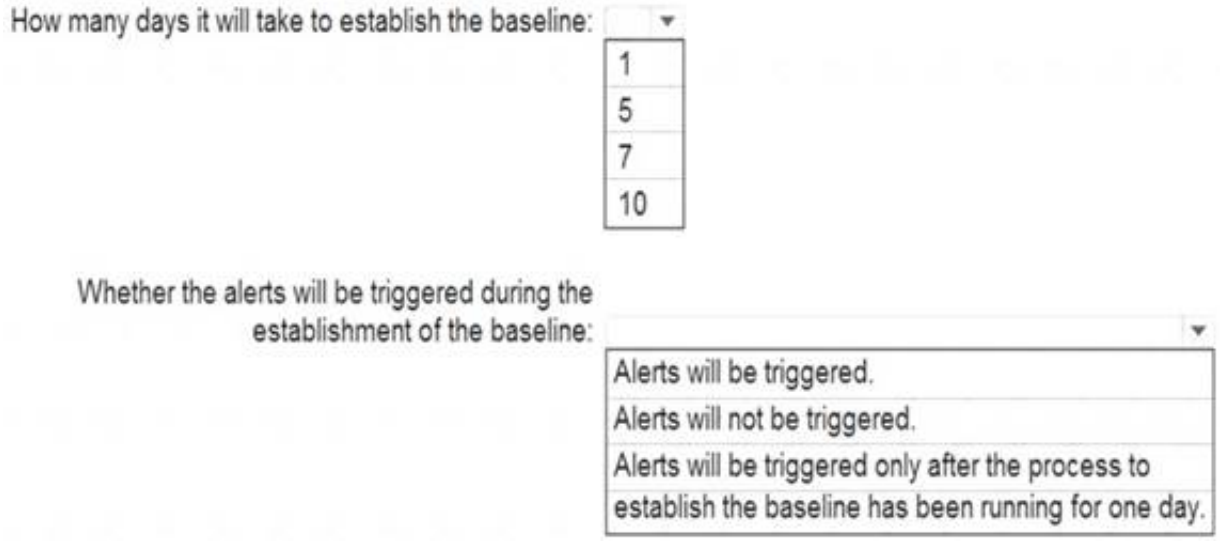
Answer: B

NEW QUESTION 101
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.

You configure a new alert policy as shown in the following exhibit.

You need to identify the following:
- How many days it will take to establish a baseline for unusual activity.
- Whether alerts will be triggered during the establishment of the baseline.

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/alert-policies?view=o365-worldwide

NEW QUESTION 102
- (Exam Topic 5)
Your network contains an on-premises Active Directory domain named contoso.com.
For all user accounts, the Logon Hours settings are configured to prevent sign-ins outside of business hours. You plan to sync contoso.com to an Azure AD tenant.
You need to recommend a solution to ensure that the logon hour restrictions apply when synced users sign in to Azure AD.
What should you include in the recommendation?

A. pass-through authentication
B. conditional access policies
C. password synchronization
D. Azure AD Identity Protection policies

Answer: A

Explanation:
Reference:
https://nickblog.azurewebsites.net/2016/10/17/azure-ad-pass-through-authentication/

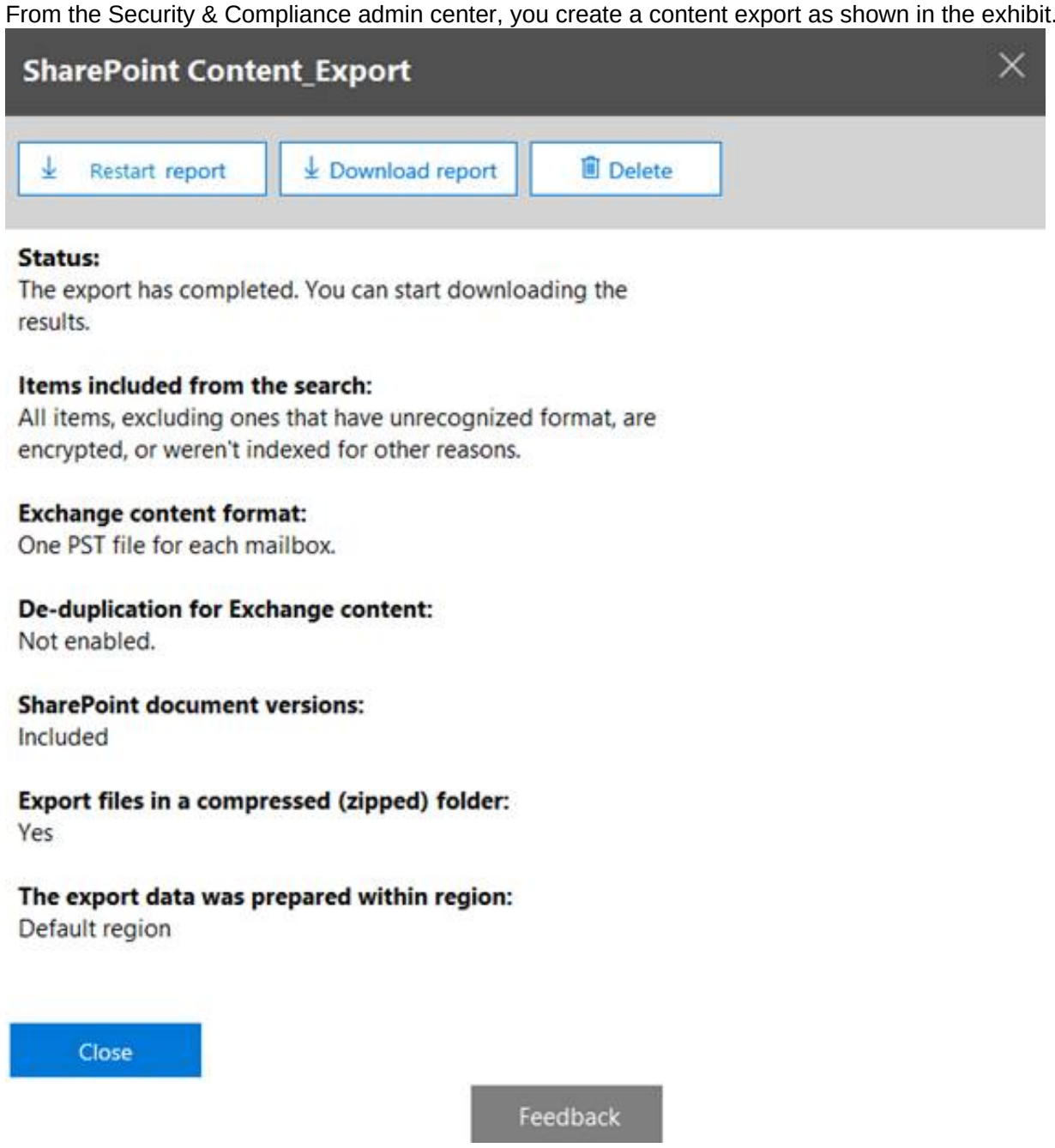
NEW QUESTION 106
- (Exam Topic 5)
Your company has 10,000 users who access all applications from an on-premises data center. You plan to create a Microsoft 365 subscription and to migrate data to the cloud.
You plan to implement directory synchronization.
User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.
You need to resolve the issue as quickly as possible. What should you do?

A. From Active Directory Administrative Center, search for all the users, and then modify the properties of the user accounts.
B. Run idfix.exe, and then click Edit.
C. From Windows PowerShell, run the start-AdSyncSyncCycle -PolicyType Delta command.
D. Run idfix.exe, and then click Complete.

Answer: B

Explanation:
IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix

NEW QUESTION 108
- (Exam Topic 5)
From the Security & Compliance admin center, you create a content export as shown in the exhibit. (Click the Exhibit tab.)



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

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=o3 https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION 112
- (Exam Topic 5)
Your on-premises network contains an Active Directory domain. You have a Microsoft 365 subscription.
You need to sync the domain with the subscription. The solution must meet the following requirements: On-premises Active Directory password complexity policies must be enforced.
Users must be able to use self-service password reset (SSPR) in Azure AD.
What should you use?

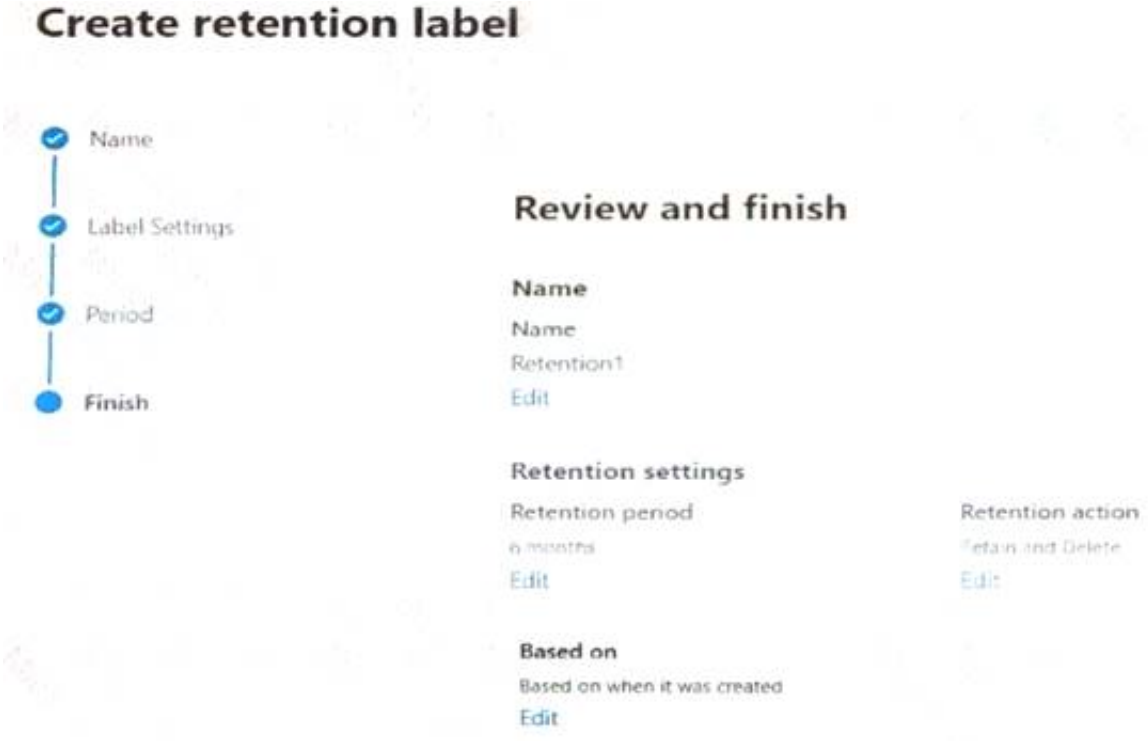
A. password hash synchronization
B. Azure AD Identity Protection

C. Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
D. pass-through authentication

Answer: D

Explanation:
Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign in to both on-premises and cloud-based applications using the same passwords.
This feature is an alternative to Azure AD Password Hash Synchronization, which provides the same benefit of cloud authentication to organizations. However, certain organizations wanting to enforce their on-premises Active Directory security and password policies, can choose to use Pass-through Authentication instead.
Note: Azure Active Directory (Azure AD) self-service password reset (SSPR) lets users reset their passwords in the cloud, but most companies also have an on-premises Active Directory Domain Services (AD DS) environment for users. Password writeback allows password changes in the cloud to be written back to an on-premises directory in real time by using either Azure AD Connect or Azure AD Connect cloud sync. When users change or reset their passwords using SSPR in the cloud, the updated passwords also written back to the on-premises AD DS environment.
Password writeback is supported in environments that use the following hybrid identity models: Password hash synchronization
Pass-through authentication
Active Directory Federation Services Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback

NEW QUESTION 116
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You create a retention label named Retention1 as shown in the following exhibit.



You apply Retention! to all the Microsoft OneDrive content.
On January 1, 2020, a user stores a file named File1 in OneDrive. On January 10, 2020, the user modifies File1.
On February 1, 2020, the user deletes File1.
When will File1 be removed permanently and unrecoverable from OneDrive?

A. February 1, 2020
B. July 1.2020
C. July 10, 2020
D. August 1, 2020

Answer: B

NEW QUESTION 119
- (Exam Topic 5)
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

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 124
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users. What is the longest time range that can be included in the report?

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

Answer: C

Explanation:
View email security reports in the Microsoft 365 Defender portal
The aggregate view shows data for the last 90 days and the detail view shows data for the last 30 days Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/reports-email-security

NEW QUESTION 125
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
Al users have Mac computers. ATI 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 Microsoft Defender for Endpoint baseline profile
B. an update policy for iOS
C. a device configuration profile
D. a mobile device management (MDM) security baseline profile

Answer: D

NEW QUESTION 130
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.
Solution: From the Microsoft 365 admin center, you assign User1 the Compliance admin role. Does this meet the goal?

A. Yes
B. No

Answer: B

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

NEW QUESTION 132
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create an account for a new security administrator named SecAdmin1.
You need to ensure that SecAdmin1 can manage Office 365 Advanced Threat Protection (ATP) settings and policies for Microsoft Teams, SharePoint, and OneDrive.
Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Security administrator role.
Does this meet the goal?

A. Yes
B. No

Answer: A

NEW QUESTION 134
- (Exam Topic 5)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com.
You create a Microsoft Defender for identity instance Contoso. The tenant contains the users shown in the following table.

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

You need to modify the configuration of the Defender for identify sensors.
Solutions: You instruct User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

A. Yes

B. No

Answer: A

NEW QUESTION 138
- (Exam Topic 5)
HOTSPOT
Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.
You plan to implement directory synchronization.
You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.
What should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: IdFix
Query and fix invalid object attributes with the IdFix tool
Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.
The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Window's Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.
Incorrect:
* AccessChk
Box 2: Enterprise Admins IdFix permissions requirements
The user account that you use to run IdFix must have read and write access to the AD DS domain.
If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.
* Enterprise Admins
The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.
Incorrect:
* Domain Admins
Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.
* Server Operator
Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.
* Domain Users - too few permissions
The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.
Reference: https://microsoft.github.io/idfix/
https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups

NEW QUESTION 143
- (Exam Topic 5)
Your network contains three Active Directory forests. There are forests trust relationships between the forests. You create an Azure AD tenant.
You plan to sync the on-premises Active Directory to Azure AD.
You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.
What should you include in the recommendation?

A. one Azure AD Connect sync server and one Azure AD Connect sync server in staging mode
B. three Azure AD Connect sync servers and one Azure AD Connect sync server in staging mode
C. six Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode
D. three Azure AD Connect sync servers and three Azure AD Connect sync servers in staging mode

Answer: A

Explanation:
Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION 146
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant. The tenant contains a group named Group1 and the users shown in the following table:

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

The tenant has a conditional access policy that has the following configurations: Name: Policy1
Assignments:
- Users and groups: Group1
- Cloud aps or actions: All cloud apps
- Access controls:
- Grant, require multi-factor authentication
- Enable policy: Report-only

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

Statements	Yes	No
Admin1 can set Enable policy for Policy1 to **On**.	○	○
Admin2 can set Enable policy for Policy1 to **Off**.	○	○
Admin3 can set Users and groups for Policy1 to **All users**.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Report-only mode is a new Conditional Access policy state that allows administrators to evaluate the impact of Conditional Access policies before enabling them in their environment. With the release of report-only mode:
- Conditional Access policies can be enabled in report-only mode.
- During sign-in, policies in report-only mode are evaluated but not enforced.
- Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.
- Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

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

NEW QUESTION 151
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

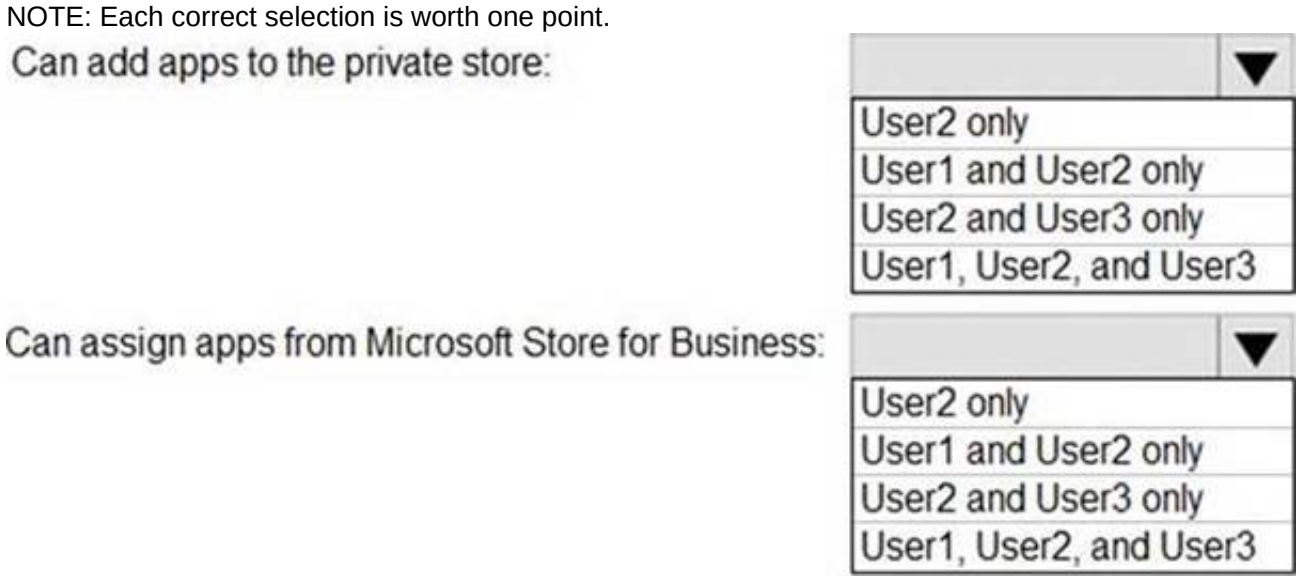
Name	Role
User1	Global admin
User2	*None*
User3	*None*

You provision the private store in Microsoft Store for Business.
You assign Microsoft Store for Business roles to the users as shown in the following table.

Name	Role
User1	*None*
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.

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



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-rol

NEW QUESTION 152
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains a user named User1.
User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list. You need to remove User1 from the Restricted entities list.
What should you use?

A. the Exchange admin center
B. the Microsoft Purview compliance portal
C. the Microsoft 365 admin center
D. the Microsoft 365 Defender portal
E. the Microsoft Entra admin center

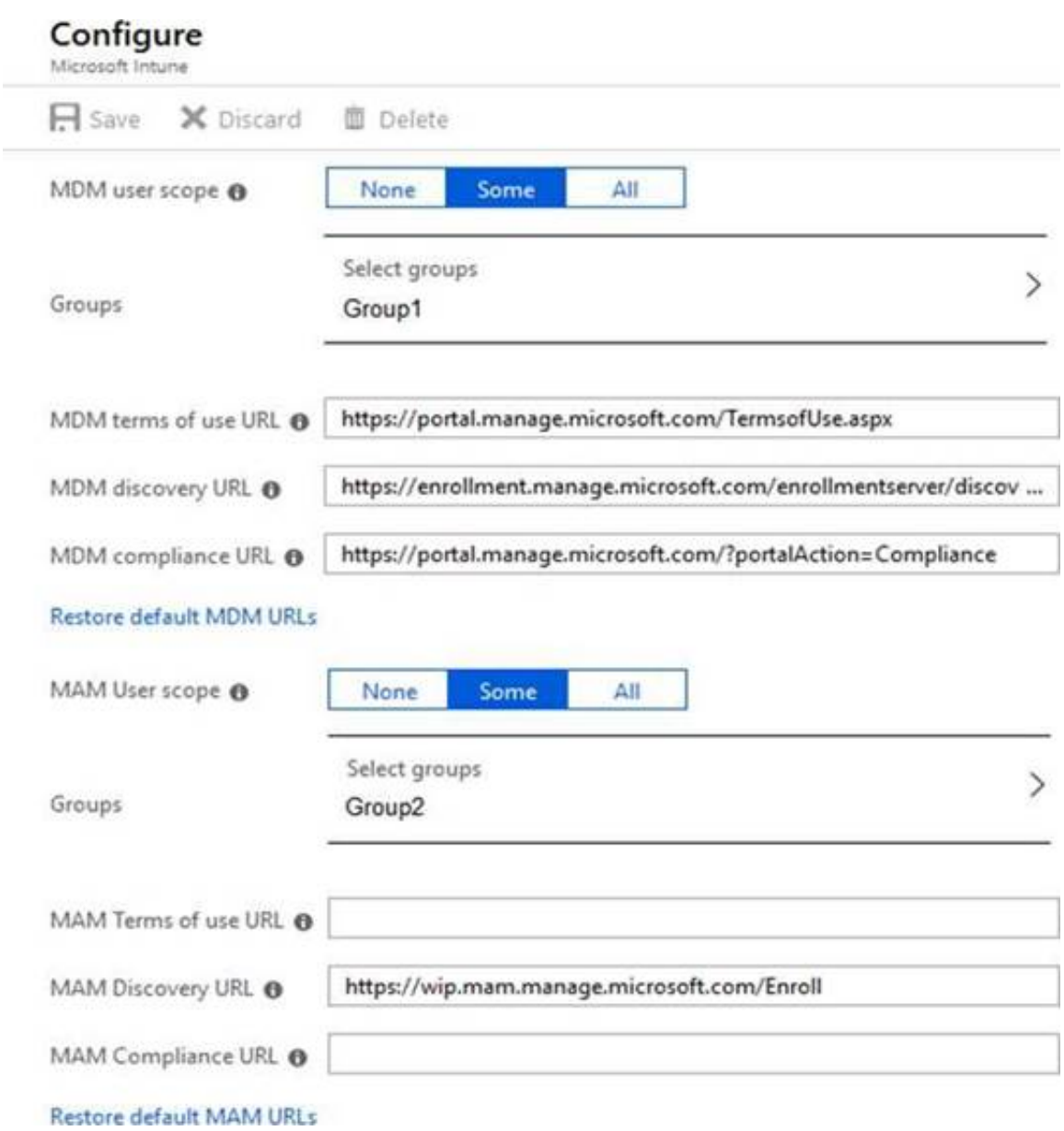
Answer: D

Explanation:
Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.
Remove a user from the Restricted entities page in the Microsoft 365 Defender portal
In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email & collaboration > Review
> Restricted entities. Or, to go directly to the Restricted entities page, use https://security.microsoft.com/restrictedentities.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-user

NEW QUESTION 156
- (Exam Topic 5)
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You integrate Microsoft Intune and contoso.com as shown in the following exhibit.



You purchase a Windows 10 device named Device1.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically.	○	○
If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically.	○	○

A. Mastered
B. Not Mastered

Answer: A

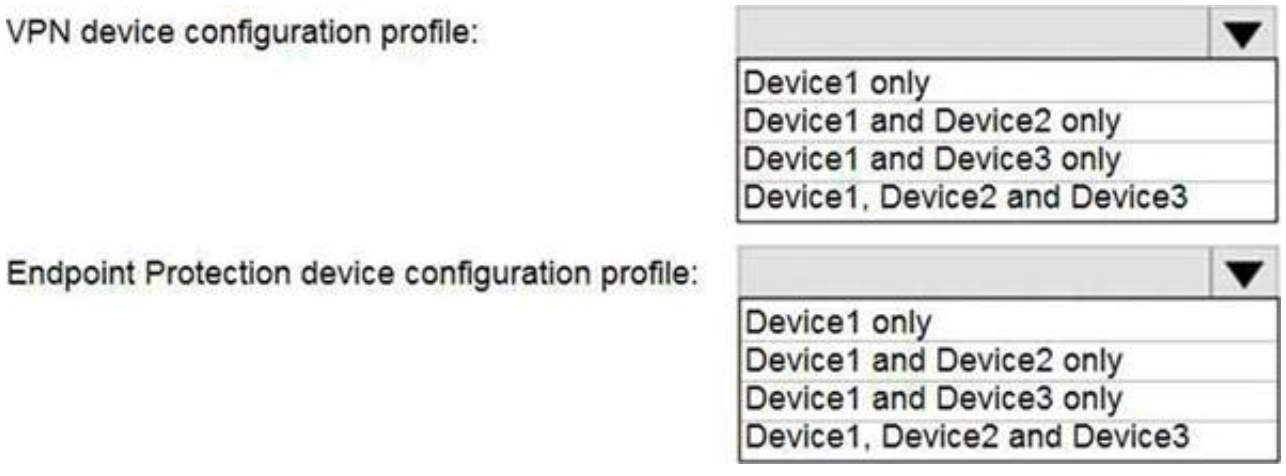
Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

NEW QUESTION 160
- (Exam Topic 5)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application Description automatically generated
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 165
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that uses Microsoft Intune.
You need to ensure that users can select a department when they enroll their device in Intune. What should you create?

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

Answer: C

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

NEW QUESTION 168
- (Exam Topic 5)
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. only the settings of Policy1
B. only the settings of Policy2
C. only the settings of Policy3
D. no settings

Answer: D

NEW QUESTION 172
- (Exam Topic 5)
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a computer that runs Windows 10.
You need to verify which version of Windows 10 is installed.
Solution: From the Settings app, you select System, and then you select About to view information about the system.
Does this meet the goal?

A. Yes
B. No

Answer: A

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

NEW QUESTION 176
- (Exam Topic 5)
You need to notify the manager of the human resources department when a user in the department shares a file or folder from the departments Microsoft SharePoint Online site. What should you do?

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

Answer: C

NEW QUESTION 177
- (Exam Topic 5)
You have a Microsoft Azure Active Directory (Azure AD) tenant named Contoso.com. You create a Microsoft Defender for identity instance Contoso.
The tenant contains the users shown in the following table.

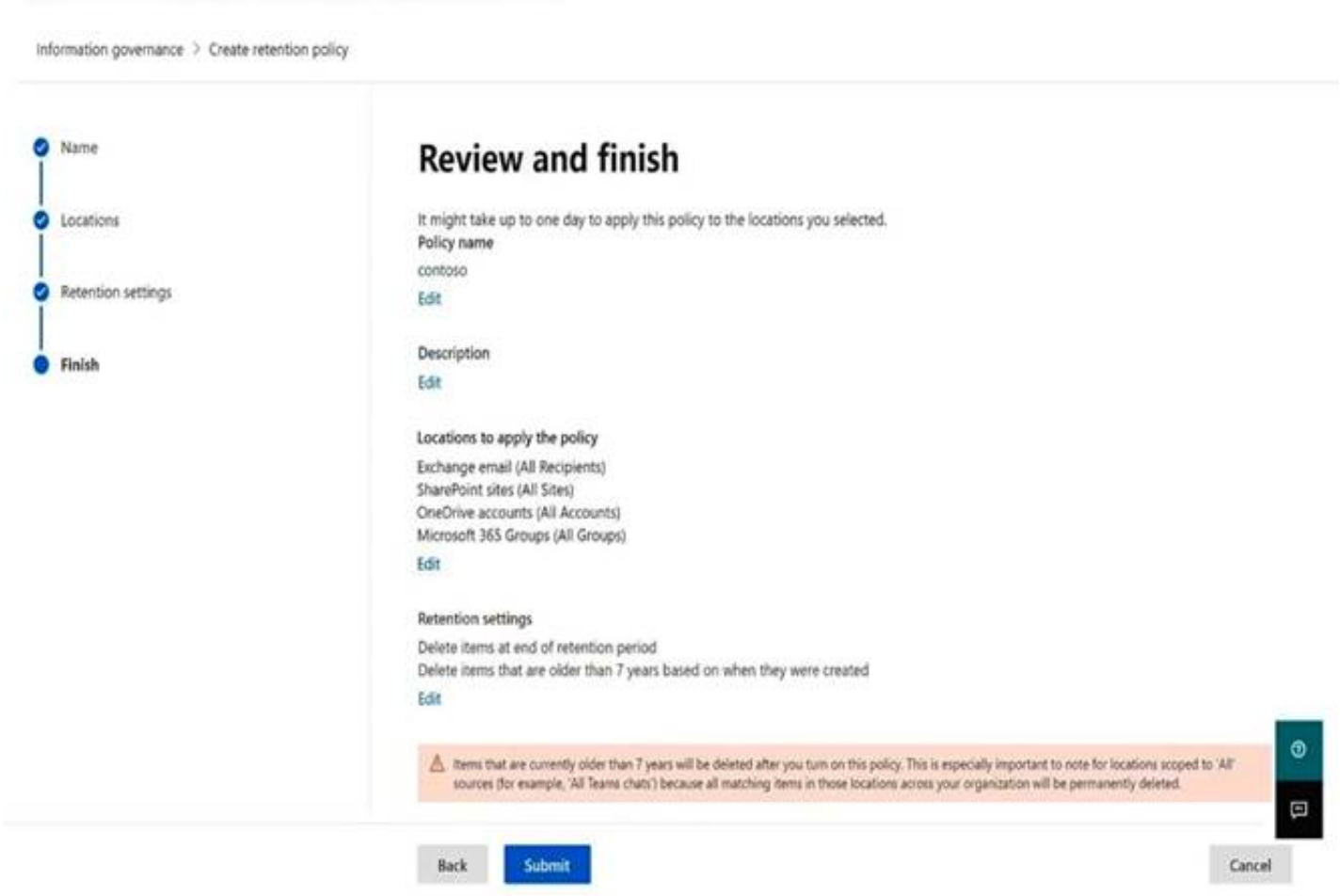
Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Users	Global administrator

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

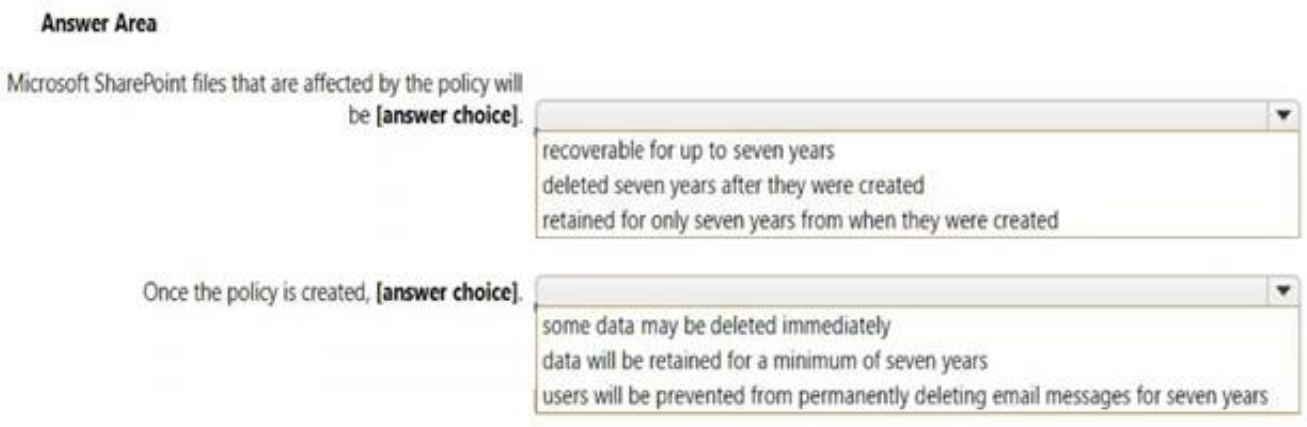
A. Yes
B. No

Answer: A

NEW QUESTION 181
- (Exam Topic 5)
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.

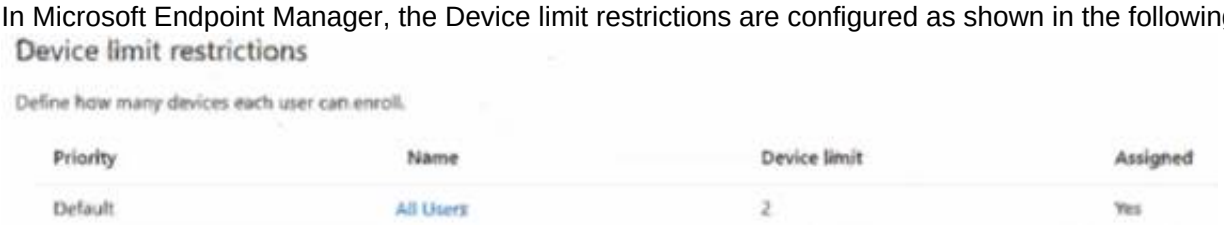


A. Mastered
B. Not Mastered

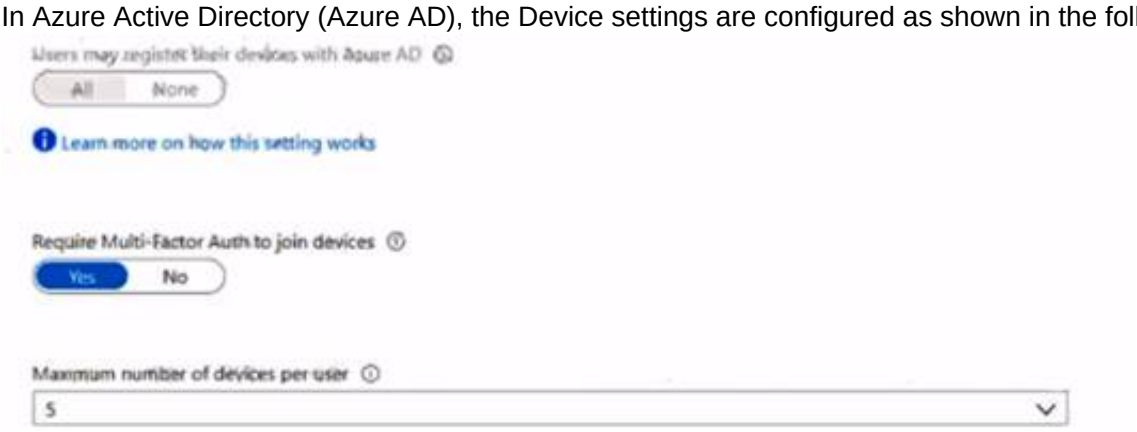
Answer: A

Explanation:
Box 1: Deleted seven years after they were created. From the exhibit:
The retention policy applies to SharePoint sites.
Delete items that are older than 7 years based on when they were created. Box 2: data will retained for a minimum of seven years
The longest retention period wins. If content is subject to multiple retention settings that retain content for different periods of time, the content will be retained until the end of the longest retention period for the item.
Note: Use a retention policy to assign the same retention settings for content at a site or mailbox level, and use a retention label to assign retention settings at an item level (folder, document, email).
For example, if all documents in a SharePoint site should be retained for 5 years, it's more efficient to do this with a retention policy than apply the same retention label to all documents in that site. However, if some documents in that site should be retained for 5 years and others retained for 10 years, a retention policy wouldn't be able to do this. When you need to specify retention settings at the item level, use retention labels.
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/retention

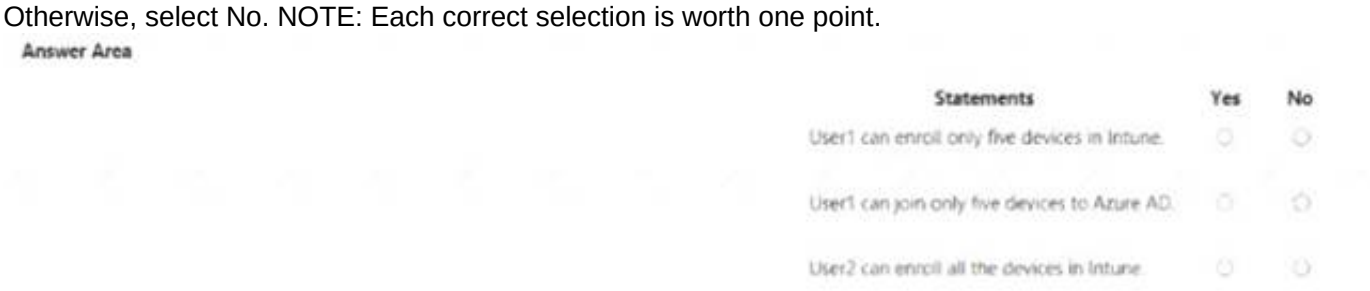
NEW QUESTION 184
- (Exam Topic 5)
You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.
In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.



In Azure Active Directory (Azure AD), the Device settings are configured as shown in the following exhibit.



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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

NEW QUESTION 188
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains four devices enrolled in Microsoft Intune as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	macOS
Device4	iOS

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

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

Answer: B

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

NEW QUESTION 190
- (Exam Topic 5)
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. From the Microsoft Endpoinf Manager admin center, create a Windows Autopilot deployment profile.Assign the profile to all the computer
B. Instruct users to restart their computer and perform a network restart.
C. Enroll the computers in Microsoft Intun
D. Create a configuration profile by using the Edition upgrade and mode switch templat
E. From the Microsoft Endpoint Manager admin center, assign the profile to all the computers and instruct users to restart their computer.
F. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
G. Instruct users to run the provisioning package from SharePoint Online.
H. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
I. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

NEW QUESTION 192
- (Exam Topic 5)
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

Explanation:
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 197
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You need to create Conditional Access policies to meet the following requirements:
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network.
Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must be blocked from signing in from outside the United States and Canada.
Only users in the R&D department must be blocked from signing in from both Android and iOS devices. Only users in the finance department must be able to sign in to an Azure AD enterprise application named
App1. All other users must be blocked from signing in to App1.
What is the minimum number of Conditional Access policies you should create?

A. 3
B. 4
C. 5
D. 6
E. 7
F. 8

Answer: B

Explanation:
* Only users in the finance department must be able to sign in to an Azure AD enterprise application named App1. All other users must be blocked from signing in to App1.
One Policy.
* Only users in the R&D department must be blocked from signing in from both Android and iOS devices. One Policy.
* Users must only be able to sign in from outside the corporate network if the sign-in originates from a compliant device.
All users must use multi-factor authentication (MFA) when they sign in from outside the corporate network. One policy
* All users must be blocked from signing in from outside the United States and Canada. Only users in the R&D department must be blocked from signing in from both Android One Policy
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access

NEW QUESTION 200
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription. You need to meet the following requirements:
Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Information protection

Automatically encrypt documents stored in Microsoft OneDrive and SharePoint.
How to integrate Microsoft Purview Information Protection with Defender for Cloud Apps Enable Microsoft Purview Information Protection
All you have to do to integrate Microsoft Purview Information Protection with Defender for Cloud Apps is
select a single checkbox. By enabling automatic scan, you enable searching for sensitivity labels from Microsoft Purview Information Protection on your Office 365 files without the need to create a policy. After you enable it, if you have files in your cloud environment that are labeled with sensitivity labels from Microsoft Purview Information Protection, you'll see them in Defender for Cloud Apps.
To enable Defender for Cloud Apps to scan files with content inspection enabled for sensitivity labels: In the Microsoft 365 Defender portal, select Settings. Then choose Cloud Apps. Then go to Information
Protection -> Microsoft Information Protection.
Note: Encryption of data at rest
Encryption at rest includes two components: BitLocker disk-level encryption and per-file encryption of customer content.
BitLocker is deployed for OneDrive for Business and SharePoint Online across the service. Per-file encryption is also in OneDrive for Business and SharePoint Online in Microsoft 365 multi-tenant and new dedicated environments that are built on multi-tenant technology.
Box 2: Settings
Enable co-authoring for Microsoft Office documents encrypted by using a sensitivity label.
* 1. Sign in to the Microsoft Purview compliance portal as a global admin for your tenant.
* 2. From the navigation pane, select Settings > Co-authoring for files with sensitivity files.
* 3. On the Co-authoring for files with sensitivity labels page, read the summary description, prerequisites, and what to expect.
* 4. Then select Turn on co-authoring for files with sensitivity labels, and Apply.
* 5. Wait 24 hours for this setting to replicate across your environment before you use this new feature for co-authoring.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/azip-integration https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-coauthoring

NEW QUESTION 204
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:
- MDM user scope: Some
- Groups: Group1
- MAM user scope: Some
- Groups: Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	○	○
User1 can enroll Device2 in Intune by using automatic enrollment	○	○
User2 can enroll Device2 in Intune by using automatic enrollment	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 209
- (Exam Topic 5)
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

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

NEW QUESTION 212
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

A. Microsoft Exchange Online only
B. Microsoft Teams only
C. Microsoft Exchanqe Online and SharePoint Online only
D. Microsoft Teams and SharePoint Online only
E. Microsoft Teams, Exchanqe Online, and SharePoint Online

Answer: A

Explanation:
Privileged access management
Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.
Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon. Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management

NEW QUESTION 216
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples
Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages
Which two components should you configure? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

A. a trainable classifier
B. a sensitive info type
C. an insider risk policy
D. an adaptive policy scope
E. a data loss prevention (DLP) policy

Answer: AE

Explanation:
A: Classifiers
This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.
Where you can use classifiers
Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels
Auto-apply retention label policy based on a condition Communication compliance
Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically. Data loss prevention
E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).
Reference:
https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp

NEW QUESTION 219
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

Name	Member of	Device
User1	Group1	Device1
User2	Group1	Device2, Device3

The devices are configured as shown in the following table.

Name	Platform	Azure AD join type
Device1	Windows 11	None
Device2	Windows 10	Joined
Device3	Android	Registered

You have a Conditional Access policy named CAPolicy1 that has the following settings:
* 1. Assignments
- Users or workload identities: Group1
- Cloud apps or actions: Office 365 SharePoint Online
- Conditions
- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith "Device"
* 2. Access controls
- Grant
- Grant: Block access
- Session: 0 controls selected
* 3. Enable policy: 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.

Answer Area

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User2 can access Site1 from Device3.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: No
User1 is member of Group1 and has Device1. Device1 is not Azure AD joined.
Note: Requiring a hybrid Azure AD joined device is dependent on your devices already being hybrid Azure AD joined.
Box 2: Yes
User2 is member of Group1 and has devices Device2 and Device3. Device2 is Azure AD joined.
Device2 is excluded from CAPolicy1 (which would block access to Site1). Box 3: Yes
User2 is member of Group1 and has devices Device2 and Device3. Device3 is Android and is Azure AD registered.
Device3 is excluded from CAPolicy1 (which would block access to Site1).
Note: On Windows 7, iOS, Android, macOS, and some third-party web browsers, Azure AD identifies the device using a client certificate that is provisioned when the device is registered with Azure AD. When a user first signs in through the browser the user is prompted to select the certificate. The end user must select this certificate before they can continue to use the browser.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-hybrid-azure-ad-join
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-com

NEW QUESTION 220
- (Exam Topic 5)
DRAG DROP
You have a Microsoft 365 E5 tenant.
You need to implement compliance solutions that meet the following requirements:
• Use a file plan to manage retention labels.
• Identify, monitor, and automatically protect sensitive information.
• Capture employee communications for examination by designated reviewers.
Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bat between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

lutions

- Data loss prevention
- Information governance
- Insider risk management
- Records management

Answer Area

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

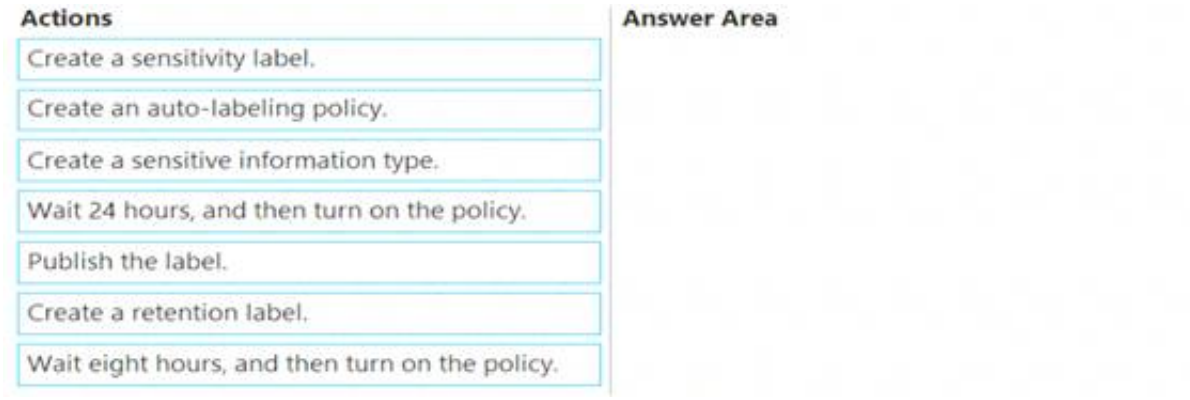
A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 223

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1. You need to automatically label the documents on Site1 that contain credit card numbers.
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, email Description automatically generated
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide#what-labe https://docs.microsoft.com/en-us/microsoft-365/compliance/apply-sensitivity-label-automatically?view=o365-w

NEW QUESTION 228
- (Exam Topic 5)
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

NEW QUESTION 231
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription.
You are planning a threat management solution for your organization.
You need to minimize the likelihood that users will be affected by the following threats:
- Opening files in Microsoft SharePoint that contain malicious content
- Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content:
- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

Impersonation and spoofing attacks in email messages:
- Anti-spam
- Anti-Phishing
- Safe Attachments
- Safe Links

NEW QUESTION 233
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Department
User1	Human resources
User2	Research
User3	Human resources
User4	Marketing

You need to configure group-based licensing to meet the following requirements:
- To all users, deploy an Office 365 E3 license without the Power Automate license option.
- To all users, deploy an Enterprise Mobility + Security E5 license.
- To the users in the research department only, deploy a Power BI Pro license.
- To the users in the marketing department only, deploy a Visio Plan 2 license.

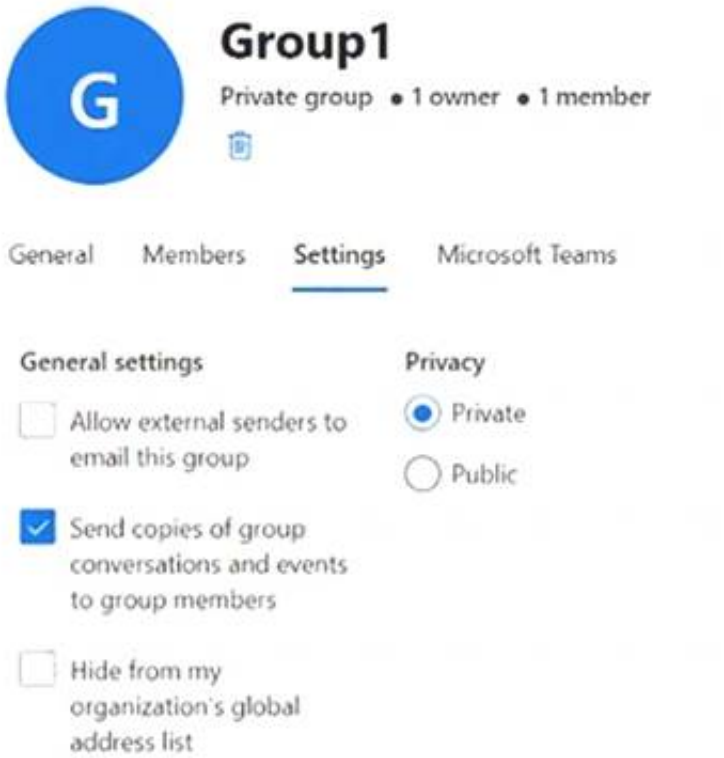
What is the minimum number of deployment groups required?

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

Answer: C

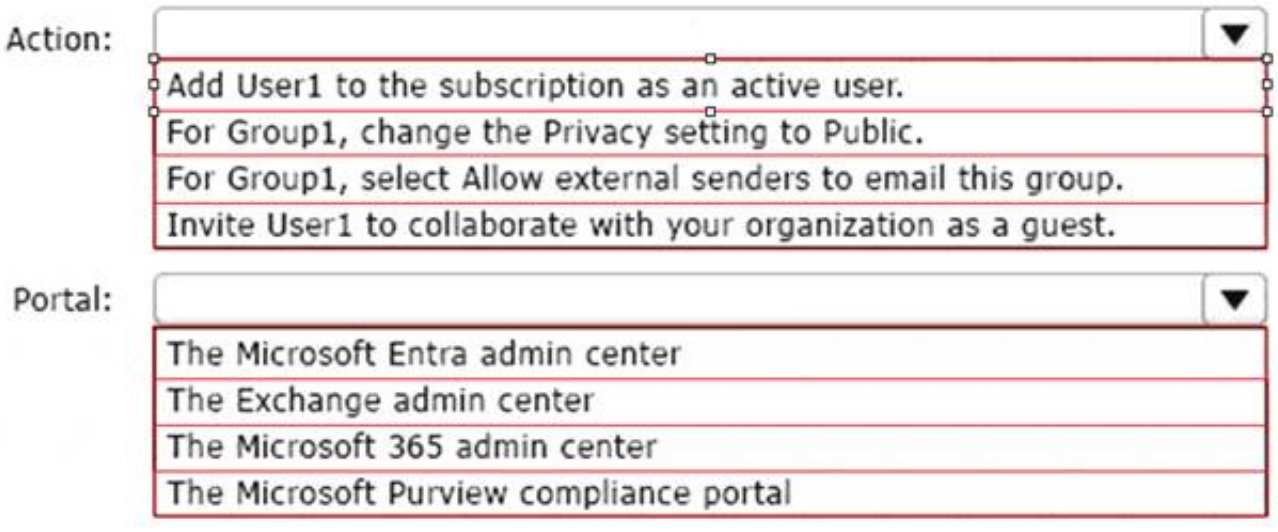
Explanation:
One for all users, one for the research department, and one for the marketing department. Note: What are Deployment Groups?
With Deployment Groups, you can orchestrate deployments across multiple servers and perform rolling updates, while ensuring high availability of your application throughout. You can also deploy to servers
on-premises or virtual machines on Azure or any cloud, plus have end-to-end traceability of deployed artifact versions down to the server level.
Reference:
https://devblogs.microsoft.com/devops/deployment-groups-is-now-generally-available-sharing-of-targets-and-m

NEW QUESTION 235
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains a Microsoft 365 group named Group1. Group1 is configured as shown in the following exhibit.



An external user named User1 has an email address of user1@outlook.com. You need to add User1 to Group1.
What should you do first, and which portal should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Invite User1 to collaborate with your organization as a guest.
To manage guest users of a Microsoft 365 tenant via the Admin Center portal, go through the following steps. Navigate with your Web browser to https://admin.microsoft.com.
On the left pane, click on “Users”, then click “Guest Users”.
On the “Guest Users” page, to create a new guest user, click on either the “Add a guest user” link on the top of the page or click on “Go to Azure Active Directory to add guest users” link at the bottom of the page. Both of these links will take you to the Azure Active Directory portal, which is located at https://aad.portal.azure.com.
On the “New user” page in the Microsoft Azure portal, you must choose to either “Create user” or “Invite user”. If you choose the “Create user” option, this will create a new user in your organization, which will have a login address with format username@tenantdomain,dot,com. If you choose the “Invite user” option, this will invite a new guest user to collaborate with your organization. The user will be emailed an email invitation which they can accept in order to begin collaborating. For the purpose of creating a guest user, you must choose the “Invite user” option.
Box 2: The Microsoft Entra admin center
Microsoft Entra admin center unites Azure AD with family of identity and access products
Microsoft Entra admin center gives customers an entire toolset to secure access for everyone and everything in multicloud and multiplatform environments. The entire Microsoft Entra product family is available at this new admin center, including Azure Active Directory (Azure AD) and Microsoft Entra Permissions Management, formerly known as CloudKnox.
Starting this month, waves of customers will begin to be automatically directed to entra.microsoft.com from Microsoft 365 in place of the Azure AD admin center (aad.portal.azure.com).
Reference:
https://stefanos.cloud/kb/how-to-manage-microsoft-365-guest-users https://m365admin.handsontek.net/microsoft-entra-admin-center-unites-azure-ad-with-family-of-identity-and-ac

NEW QUESTION 237
- (Exam Topic 5)
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 Purview compliance portal
C. the Microsoft Defender for Cloud Apps portal
D. the Microsoft Apps admin center

Answer: C

NEW QUESTION 238
- (Exam Topic 5)
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

NEW QUESTION 242
- (Exam Topic 5)
You have device compliance policies shown in the following table.

Name	Platform	Assignment
Policy1	Windows 10 and later	Device1
Policy2	Windows 10 and later	Device1
Policy3	Windows 10 and later	Device2
Policy4	Windows 10 and later	Device2
Policy5	iOS/iPadOS	Device3
Policy6	iOS/iPadOS	Device3

The device compliance state for each policy is shown in the following table.

Policy	State
Policy1	Compliant
Policy2	In grace period
Policy3	Compliant
Policy4	Not compliant
Policy5	In grace period
Policy6	Compliant

NOTE: Each correct selection is worth one point.

Answer 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.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer 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.	○	○

NEW QUESTION 243
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 subscription that contains the users shown in the following table.

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

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

```
(user.userType [ -eq "Guest" | -in "Guest" | -ne "Guest" | -notmatch "Member" ]) and (user.department [ -contains "Support" | -in "Support" | -match "Support" | -startsWith "Sup" ])
```

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: -eq "Guest"
Dynamic membership rules for groups in Azure Active Directory Supported expression operators
The following table lists all the supported operators and their syntax for a single expression. Operators can be used with or without the hyphen (-) prefix. The Contains operator does partial string matches but not item in a collection matches.
* Equals
-eq
* Contains
-contains
* Etc.
Box 2: -contains "Support" Incorrect:
* -in
If you want to compare the value of a user attribute against multiple values, you can use the -in or -notIn operators.

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

NEW QUESTION 245
- (Exam Topic 5)
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 DLP policy. You need to prevent the users from bypassing the DLP policy.
What should you configure?

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

Answer: D

Explanation:
A DLP policy can be configured to allow users to override a policy tip and report a false positive.
You can educate your users about DLP policies and help them remain compliant without blocking their work. For example, if a user tries to share a document containing sensitive information, a DLP policy can both send them an email notification and show them a policy tip in the context of the document library that allows them to override the policy if they have a business justification. The same policy tips also appear in Outlook on the web, Outlook, Excel, PowerPoint, and Word.
If you find that users are incorrectly marking content as false positive and bypassing the DLP policy, you can configure the policy to not allow user overrides.
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION 247
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains the groups shown in the following table.

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

You plan to create a compliance policy named Compliance1.
You need to identify the groups that meet the following requirements:
- Can be added to Compliance1 as recipients of noncompliance notifications
- Can be assigned to Compliance1

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

Can be added to Compliance1 as recipients of noncompliance notifications:
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:
- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application, chat or text message Description automatically generated
Reference:
https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manage

NEW QUESTION 249
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

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

Answer: D

NEW QUESTION 251
- (Exam Topic 5)
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?

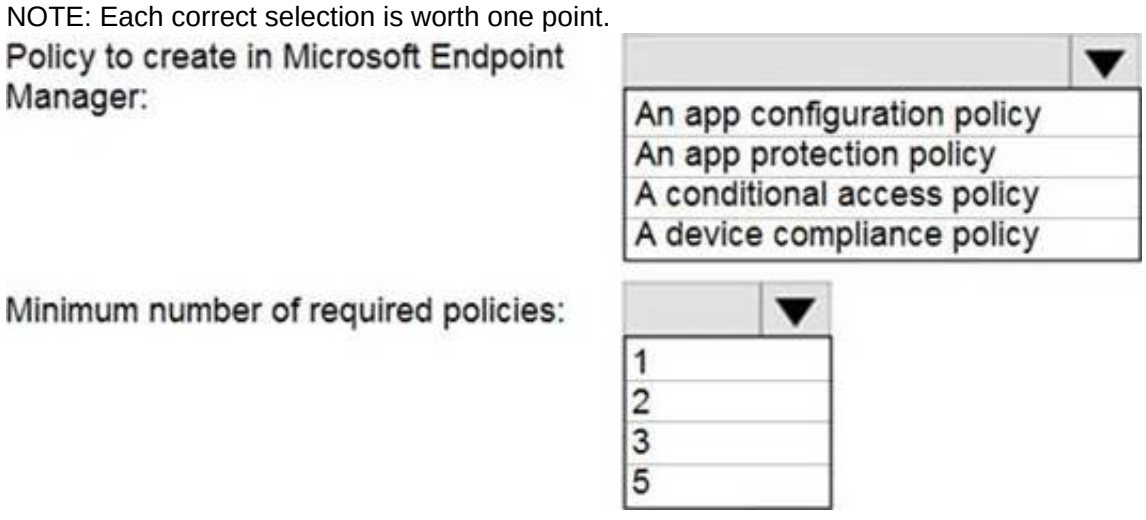
A. a session policy
B. a file policy
C. an activity policy
D. an anomaly detection policy

Answer: D

NEW QUESTION 256
- (Exam Topic 5)
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.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
Graphical user interface, application, table Description automatically generated
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/app-protection-policy

NEW QUESTION 259
- (Exam Topic 5)
You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.
From Microsoft Defender Security Center, you perform a security investigation.
You need to run a PowerShell script on the device to collect forensic information. Which action should you select on the device page?

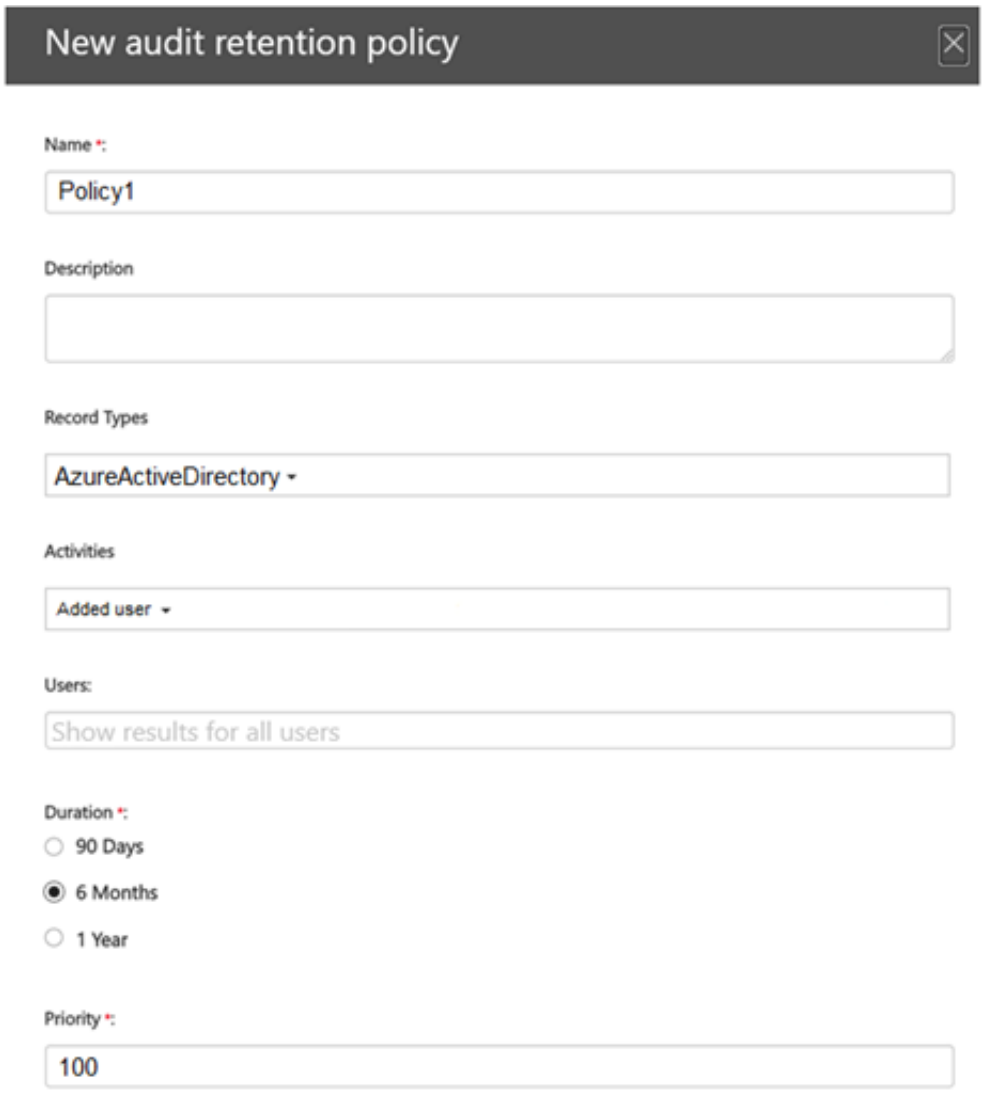
A. Initiate Live Response Session
B. Initiate Automated Investigation
C. Collect investigation package
D. Go hunt

Answer: A

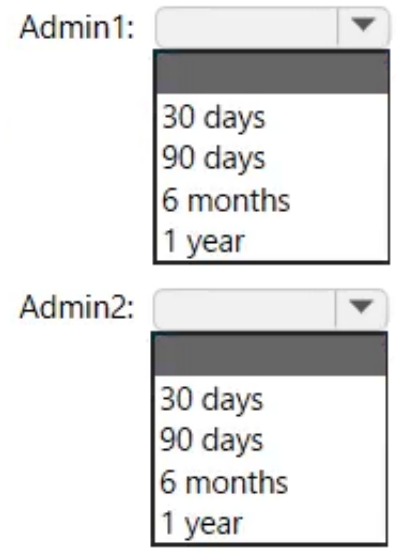
Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/live-response?view=o365-worldwid

NEW QUESTION 263
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	*None*



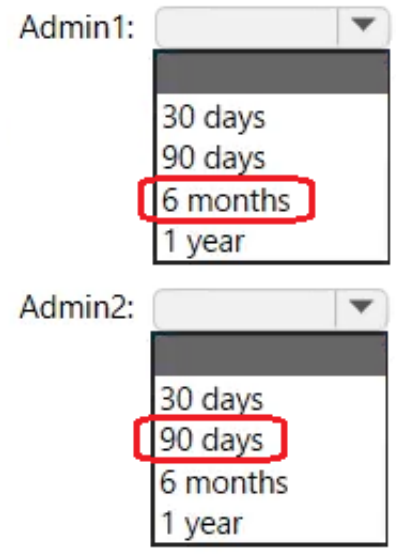
You plan to create a new user named User1.
How long will the user creation audit event be available if Admin1 or Admin2 creates User1? To answer, select the appropriate options in the answer area.
Each correct selection is worth one point.



A. Mastered
B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 268
- (Exam Topic 5)
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

Explanation:
Reference:
https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios

NEW QUESTION 272
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains a user named User1. You plan to implement insider risk management.
You need to ensure that User1 can perform the following tasks:
- Review alerts.
- Manage cases.
- Create notice templates.
- Review user emails by using Content explorer. The solution must use the principle of least privilege. To which role group should you add User1?

A. Insider Risk Management
B. Insider Risk Management Analysts
C. Insider Risk Management Investigators
D. Insider Risk Management Admin

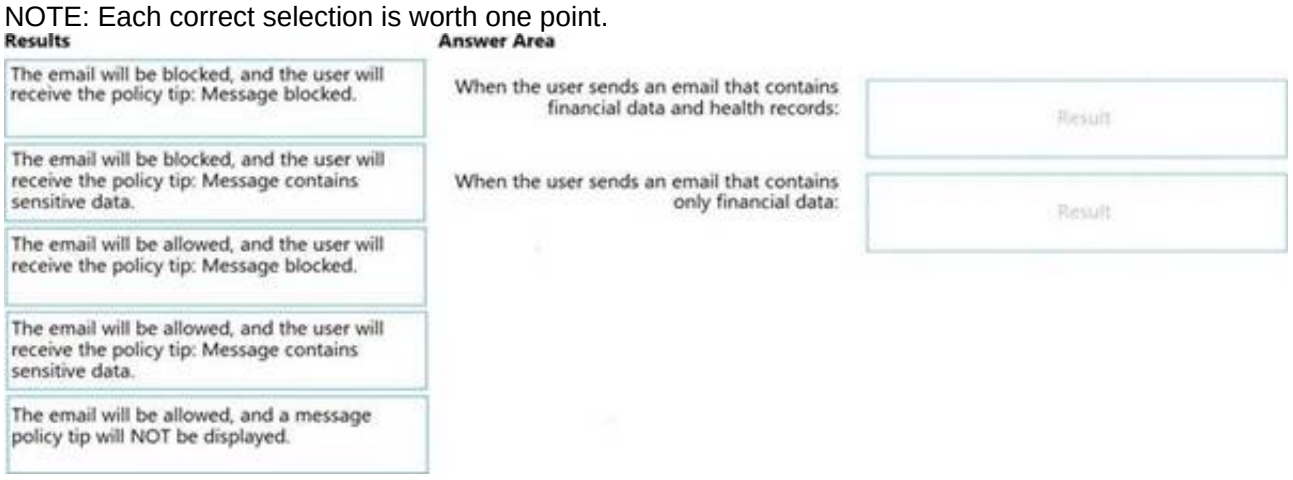
Answer: C

Explanation:
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-wo

NEW QUESTION 275
- (Exam Topic 5)
DRAG DROP
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.



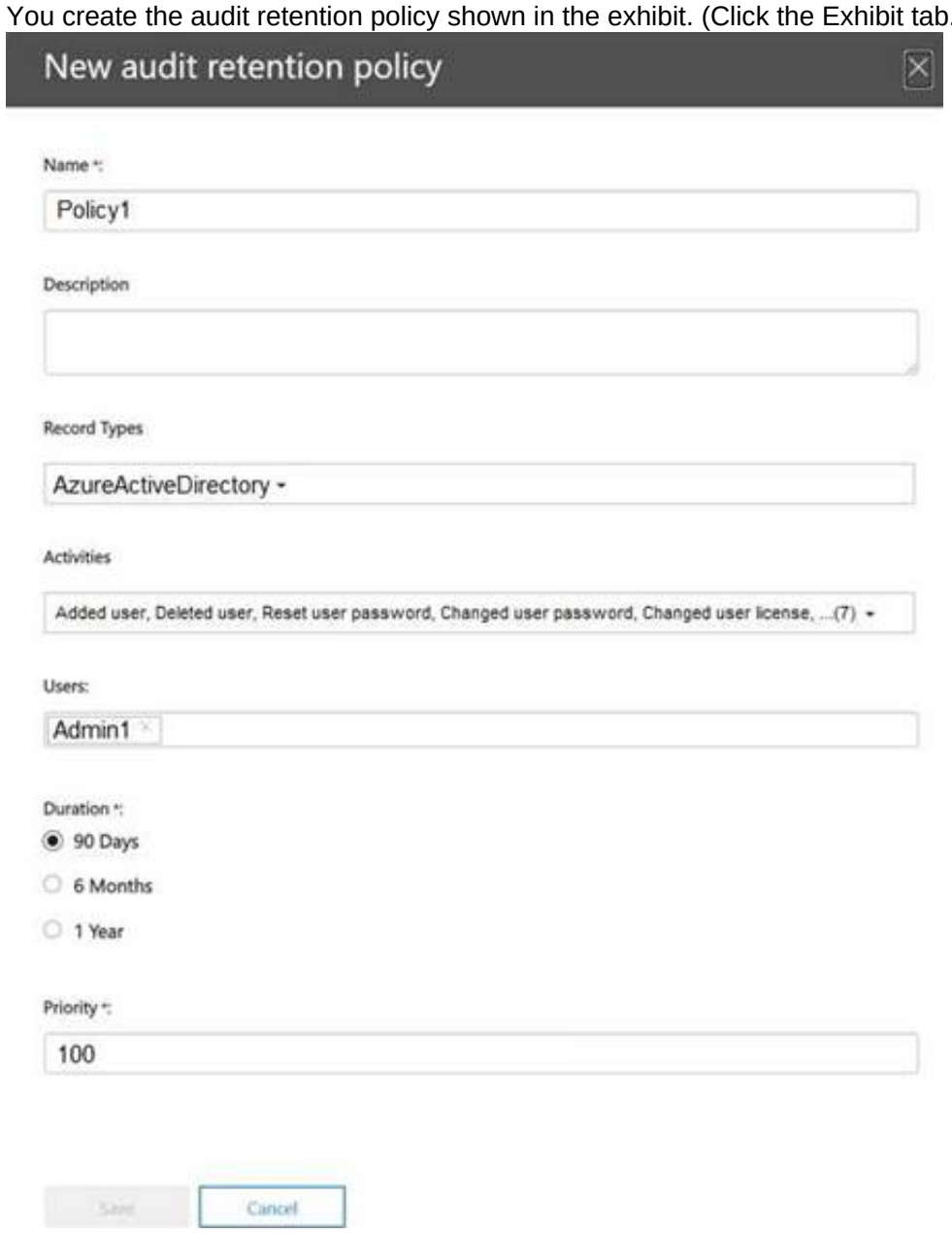
A. Mastered
B. Not Mastered

Answer: A

Explanation:
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

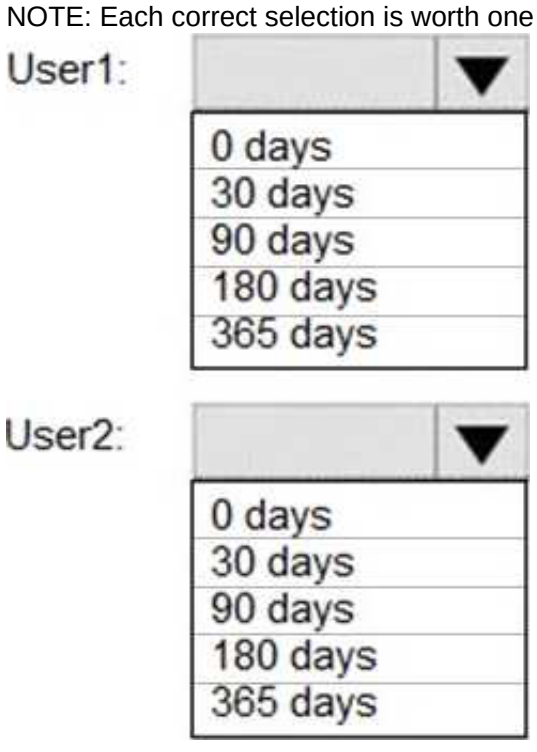
NEW QUESTION 276

- (Exam Topic 5)
HOTSPOT
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.)



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.



A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 279
- (Exam Topic 5)
You have a Microsoft 365 E5 tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:
- Show app and profile configuration progress: Yes
- Allow users to collect logs about installation errors: Yes
- Assignments: Group2

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

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	○	○

A. Mastered
B. Not Mastered

Answer: A

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

NEW QUESTION 282
- (Exam Topic 5)
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

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

Azure AD Connect has the following settings:
- Password Hash Sync: Enabled
- Pass-through authentication: Enabled

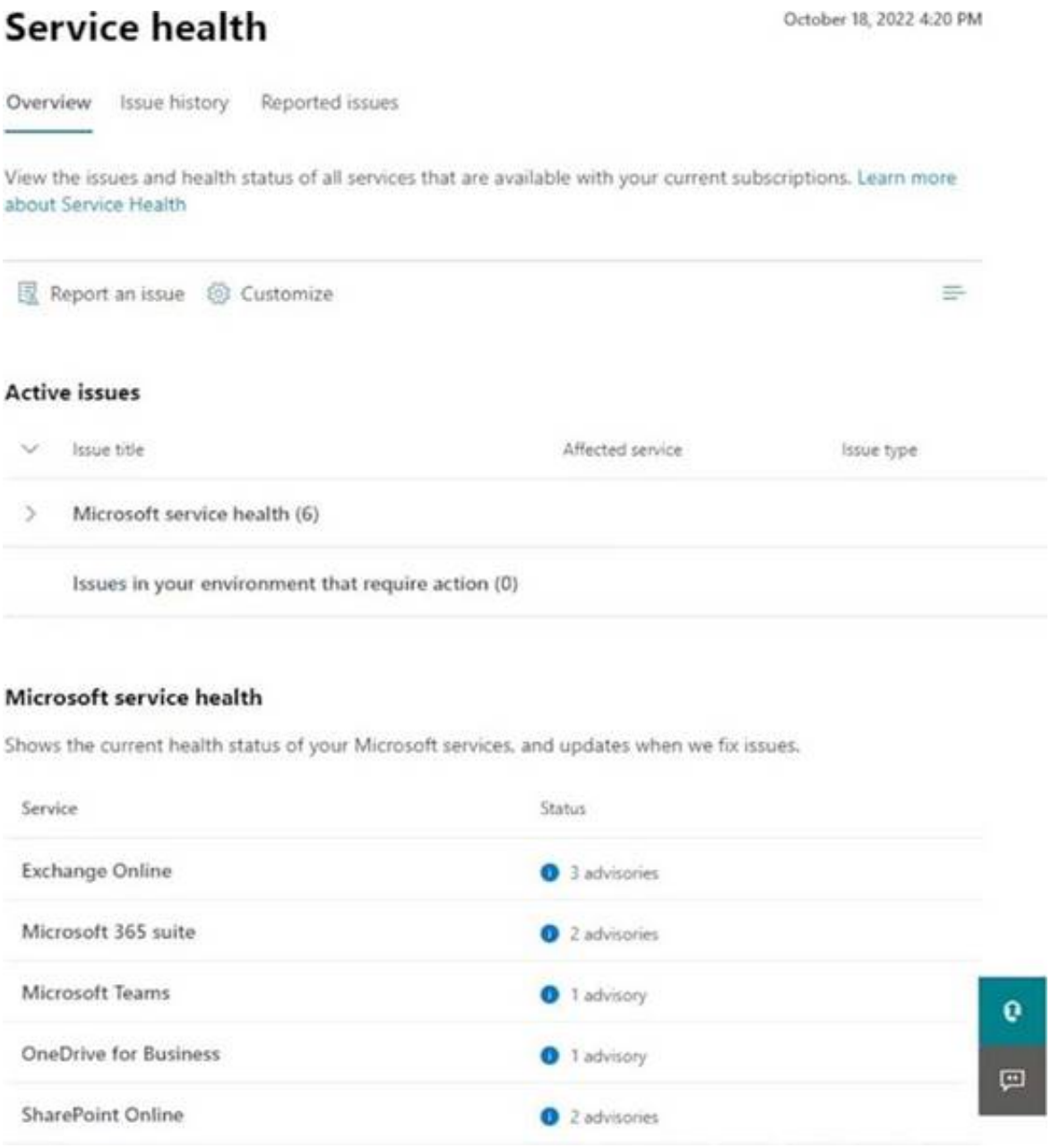
You need to identify which users will be able to authenticate by using Azure AD if connectivity between on-premises Active Directory and the internet is lost.
Which users should you identify?

A. none
B. Used only1
C. User1 and User2 only
D. User1. User2, and User3

Answer: D

Explanation:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn¨

NEW QUESTION 283
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You view the Service health Overview as shown in the following exhibit.



You need to ensure that a user named User1 can view the advisories to investigate service health issues. Which role should you assign to User1?

A. Message Center Reader
B. Reports Reader
C. Service Support Administrator
D. Compliance Administrator

Answer: C

Explanation:

Service Support admin
Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:
- Open and manage service requests
- View and share message center posts
- Monitor service health Incorrect:
* Message center reader
Assign the Message center reader role to users who need to do the following:
- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups
* Reports reader
Assign the Reports reader role to users who need to do the following:
- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API Reference:
https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

NEW QUESTION 287
- (Exam Topic 5)
You have a Microsoft E5 subscription.
You need to ensure that administrators who need to manage Microsoft Exchange Online are assigned the Exchange Administrator role for five hours at a time.
What should you implement?

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

Answer: A

Explanation:

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

NEW QUESTION 290
- (Exam Topic 5)
You have a Microsoft 365 subscription.
You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.
Which type of group should you use to assign the Reports Reader role and to access App1?

A. a Microsoft 365 group that has assigned membership
B. a Microsoft 365 group that has dynamic user membership
C. a security group that has assigned membership
D. a security group that has dynamic user membership

Answer: C

Explanation:
To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.
Note: You can add the following types of groups:
Assigned groups - Manually add users or devices into a static group.
Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.
Note:
Security groups
Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.
Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.
Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.
Security groups can be added to a team.
Microsoft 365 Groups can't be members of security groups. Microsoft 365 Groups
Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups? https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy

NEW QUESTION 292
- (Exam Topic 5)
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

Explanation:

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

NEW QUESTION 294
- (Exam Topic 5)
HOTSPOT
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:
- Scope type: Directory
- Selected members: Group1
- Assignment type: Active

- Assignment starts: Mar 15, 2023
- Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

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

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

Answer Area

Statements	Yes	No
On July 15, 2023, Admin1 can reset the password of a user.	○	○
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	○	○
On May 1, 2023, Admin3 can reset the password of a user.	○	○

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: Yes
Admin1 is member of Group1.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
July 15, 2023 is with the assignment period.
A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.
Box 2: No
Admin2 is member of Group2.
The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible
June 20, 2023 is with the assignment period. The assignment must be approved.
Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member.
The assignment type: Active
May 1, 2023 is with the assignment period. Reference:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/groups-assign-member

NEW QUESTION 297
- (Exam Topic 5)
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 Microsoft Defender for Endpoint for 10 test devices. During the onboarding process, you configure Microsoft Defender for Endpoint-related data to be stored in the United States.
You plan to onboard all the devices to Microsoft Defender for Endpoint. You need to store the Microsoft Defender for Endpoint data in Europe. What should you do first?

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

Answer: B

Explanation:
Storage locations
Understand where Defender for Cloud stores data and how you can work with your data:
* Machine information
- Stored in a Log Analytics workspace.
- You can use either the default Defender for Cloud workspace or a custom workspace. Data is stored in accordance with the workspace location.
Reference:
https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers-data-workspace

NEW QUESTION 298
- (Exam Topic 5)
You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Security Operator
User3	Security Reader
User4	Compliance Administrator

You plan to implement Microsoft Defender for Endpoint.
You verify that role-based access control (RBAC) is turned on in Microsoft Defender for Endpoint. You need to identify which user can view security incidents from the Microsoft 365 Defender portal. Which user should you identify?

A. User1
B. User2
C. User3
D. User4

Answer: A

NEW QUESTION 299
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

MS-102 Practice Exam Features:

* MS-102 Questions and Answers Updated Frequently

* MS-102 Practice Questions Verified by Expert Senior Certified Staff

* MS-102 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* MS-102 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year