

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)

On which server should you install the Azure ATP sensor?

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

Answer: A

Explanation:

References:

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

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 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: You create a device configuration profile from the Device Management admin center.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

It looks like the given answer is correct. There is an on-premises Active Directory synced to Azure Active Directory (Azure AD) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Azure AD 2. Client agent setting for hybrid Azure AD-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager

<https://docs.microsoft.com/en-us/mem/configmgr/comanage/tutorial-co-manage-client>

NEW QUESTION 4

- (Exam Topic 1)

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices.

What is the minimum of dedicated support technicians required?

- A. 1
- B. 4
- C. 7
- D. 31

Answer: B

Explanation:

References:

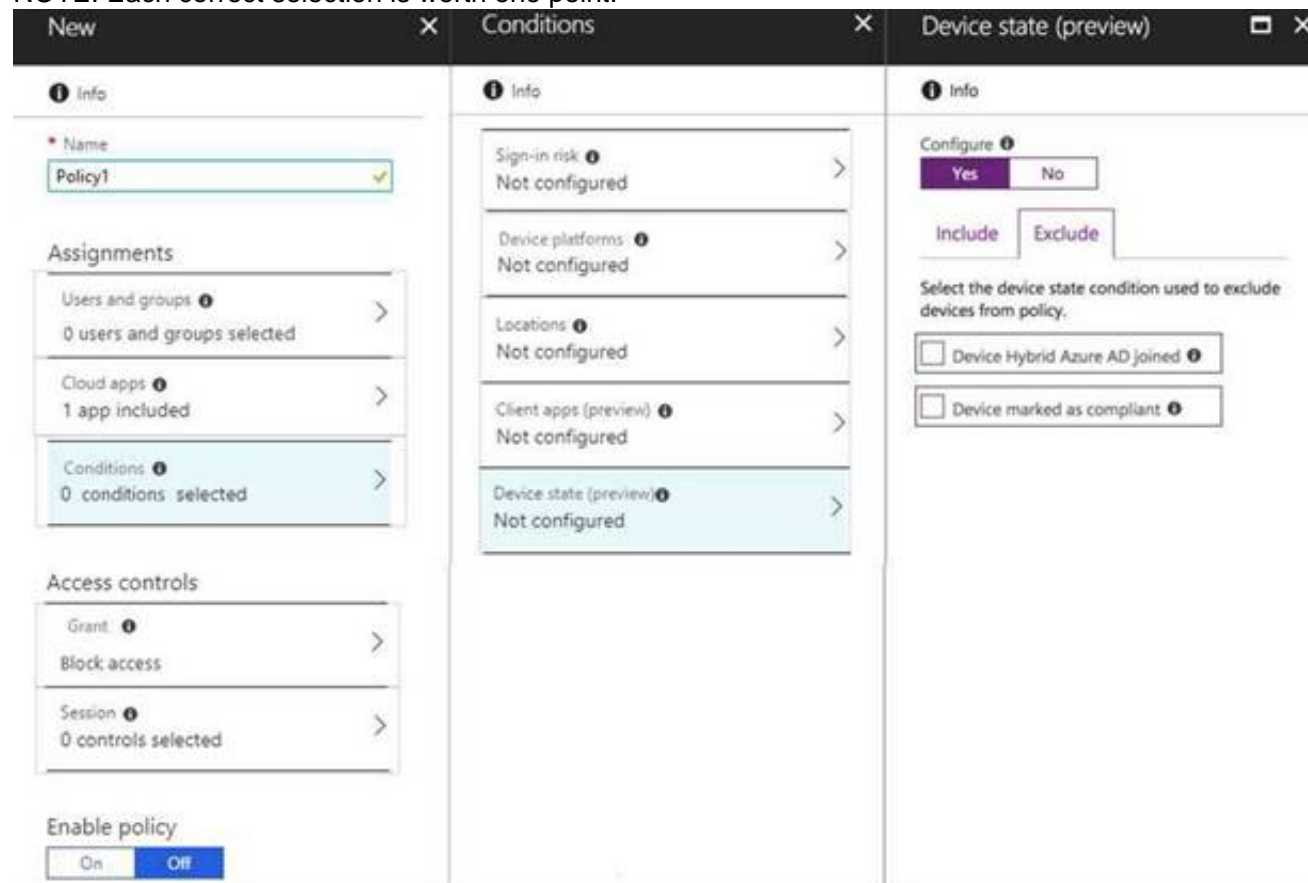
<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager>

NEW QUESTION 5

- (Exam Topic 1)

You need to configure a conditional access policy to meet the compliance requirements. You add Exchange Online as a cloud app. Which two additional settings should you configure in Policy1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Suggested Answer

References: <https://docs.microsoft.com/en-us/intune/create-conditional-access-intune>

NEW QUESTION 6

- (Exam Topic 1)

You need to create the Microsoft Store for Business. Which user can create the store?

- A. User2
- B. User3
- C. User4
- D. User5

Answer: C

Explanation:

References:

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

NEW QUESTION 7

- (Exam Topic 1)

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

What should you create from the Intune admin center?

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

Answer: C

NEW QUESTION 8

- (Exam Topic 2)

You need to meet the technical requirement for log analysis.

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

NOTE: Each correct selection is worth one point.

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 9

- (Exam Topic 2)

You need to protect the U.S. PII data to meet the technical requirements.
What should you create?

- A. a data loss prevention (DLP) policy that contains a domain exception
- B. a Security & Compliance retention policy that detects content containing sensitive data
- C. a Security & Compliance alert policy that contains an activity
- D. a data loss prevention (DLP) policy that contains a user override

Answer: A

NEW QUESTION 10

- (Exam Topic 2)

You need to recommend a solution for the security administrator. The solution must meet the technical requirements.
What should you include in the recommendation?

- A. Microsoft Azure Active Directory (Azure AD) Privileged Identity Management
- B. Microsoft Azure Active Directory (Azure AD) Identity Protection
- C. Microsoft Azure Active Directory (Azure AD) conditional access policies
- D. Microsoft Azure Active Directory (Azure AD) authentication methods

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-condition> states clearly that Sign-in risk

NEW QUESTION 10

- (Exam Topic 3)

You need to create the Safe Attachments policy to meet the technical requirements. Which option should you select?

- A. Replace
- B. Enable redirect
- C. Block
- D. Dynamic Delivery

Answer: D

Explanation:

Reference:

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

NEW QUESTION 14

- (Exam Topic 3)

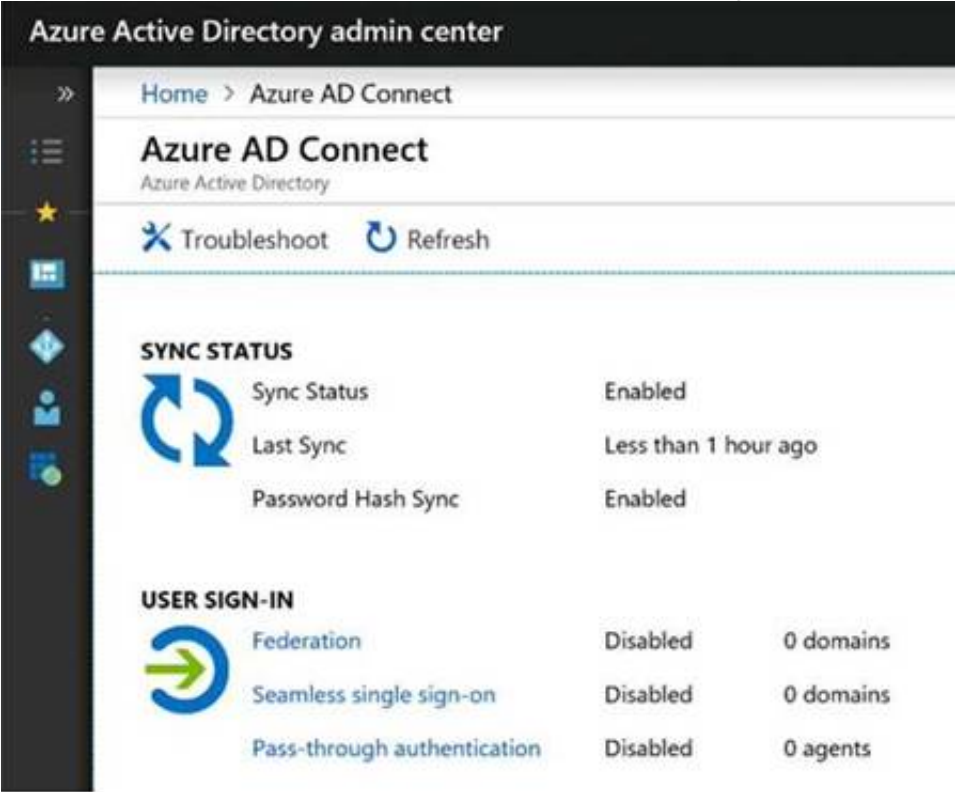
You need to configure Office on the web to meet the technical requirements. What should you do?

- A. Assign the Global reader role to User1.
- B. Enable sensitivity labels for Office files in SharePoint Online and OneDrive.
- C. Configure an auto-labeling policy to apply the sensitivity labels.
- D. Assign the Office apps admin role to User1.

Answer: B

Explanation:
Reference:
<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?view=o>

NEW QUESTION 19
- (Exam Topic 4)
HOTSPOT
You create the Microsoft 365 tenant.
You implement Azure AD Connect 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.

Answer Area

During Project1, sales department users can access [answer choice] applications by using SSO.

both on-premises and cloud-based
only cloud-based
only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources [answer choice].

both on-premises and in the cloud
in the cloud only
on-premises only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Box 1: only on-premises
In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.
In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Azure Active Directory user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Azure Active Directory. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.
Box 2: in the cloud only

NEW QUESTION 23
- (Exam Topic 4)
You are evaluating the required processes for Project1.
You need to recommend which DNS record must be created while adding a domain name for the project. Which DNS record should you recommend?

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

Answer: A

Explanation:
When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers: Text (TXT)

Mail exchanger (MX)
incorrect answer options you may see on the exam include the following: alias (CNAME)
Host (A) host (AAA)
Pointer (PTR) Name Server (NS)
host information (HINFO) pointer (PTR)
Reference:
<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting>

NEW QUESTION 24

- (Exam Topic 4)

You need to ensure that all the sales department users can authenticate successfully during Project1 and Project2.
Which authentication strategy should you implement for the pilot projects?

- A. pass-through authentication
- B. pass-through authentication and seamless SSO
- C. password hash synchronization and seamless SSO
- D. password hash synchronization

Answer: C

Explanation:

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365. Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.

After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.

Fabrikam does NOT plan to implement identity federation.

After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.

You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

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

NEW QUESTION 26

- (Exam Topic 5)

You have a new Microsoft 365 E5 tenant.

You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected.
What should you do first?

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

Answer: A

Explanation:

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

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

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

Reference:

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

NEW QUESTION 27

- (Exam Topic 5)

Your network contains an Active Directory forest named contoso.local.

You purchase a Microsoft 365 subscription.

You plan to move to Microsoft 365 and to implement a hybrid deployment solution for the next 12 months. You need to prepare for the planned move to Microsoft 365.

What is the best action to perform before you implement directory synchronization? More than one answer choice may achieve the goal. Select the BEST answer.

- A. Purchase a third-party X.509 certificate.
- B. Create an external forest trust.
- C. Rename the Active Directory forest.
- D. Purchase a custom domain name.

Answer: D

Explanation:

The first thing you need to do before you implement directory synchronization is to purchase a custom domain name. This could be the domain name that you use in your on-premise Active Directory if it's a routable domain name, for example, contoso.com.

If you use a non-routable domain name in your Active Directory, for example contoso.local, you'll need to add the routable domain name as a UPN suffix in Active Directory.

Incorrect:

Not C: No need to rename the Active Directory forest. As we use a non-routable domain name contoso.local, we just need to add the routable domain name as a UPN suffix in Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/set-up-directory-synchronization>

NEW QUESTION 31

- (Exam Topic 5)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
 After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
 Your network contains an Active Directory domain. You deploy an Azure AD tenant.
 Another administrator configures the domain to synchronize to Azure AD.
 You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully.
 You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully.
 You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: You run idfix.exe and export the 10 user accounts.
 Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The question states that “all the user account synchronizations completed successfully”. If there were problems with the 10 accounts that needed fixing with idfix.exe, there would have been synchronization errors in Azure AD Connect Health.
 It is likely that the 10 user accounts are being excluded from the synchronization cycle by a filtering rule. Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering>

NEW QUESTION 35

- (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 36

- (Exam Topic 5)

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

Name	Type	Member of
User1	User	Group1
Device1	Device	Group2

User1 is the owner of Device1.
 You add Microsoft 365 Apps Windows 10 and later app types to Intune as shown in the following table. On Thursday, you review the results of the app deployments.

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

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

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="radio"/>	<input type="radio"/>
App3 is displayed in the Company Portal.	<input type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Word is installed on Device1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
App3 is displayed in the Company Portal.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Excel is installed on Device1.	<input type="checkbox"/>	<input type="checkbox"/>

NEW QUESTION 40

- (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 43

- (Exam Topic 5)

You have a Microsoft 365 tenant. You plan to manage incidents in the tenant by using the Microsoft 365 security center. Which Microsoft service source will appear on the Incidents page of the Microsoft 365 security center?

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

Answer: D

Explanation:

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

NEW QUESTION 46

- (Exam Topic 5)

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

Name	TPM version	Operating system	BIOS/UEFI	BitLocker Drive Encryption (BitLocker)
Device1	TPM 1.2	Windows 10 Pro	BIOS	Enabled
Device2	TPM 2	Windows 10 Home	BIOS	Not applicable
Device3	TPM 2	Windows 8.1 Pro	UEFI	Enabled

You plan to join the devices to Azure Active Directory (Azure AD) What should you do on each device to support Azure AU join? To answer, drag the appropriate actions to the collect devices, Each action may be used once, more than once, of 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.

Actions	Answer Area
Disable BitLocker.	Device1: Action
Disable TPM.	Device2: Action
Switch to UEFI.	Device3: Action
Upgrade to Windows 10 Enterprise.	

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
Disable BitLocker.	Device1: Disable BitLocker.
Disable TPM.	Device2: Switch to UEFI.
Switch to UEFI.	Device3: Upgrade to Windows 10 Enterprise.
Upgrade to Windows 10 Enterprise.	

NEW QUESTION 47

- (Exam Topic 5)

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

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

Your network contains an Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

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

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

- A. Yes
 B. No

Answer: B

Explanation:

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

Reference:

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

NEW QUESTION 50

- (Exam Topic 5)

Your company has a Microsoft E5 tenant.

The company must meet the requirements of the ISO/IEC 27001:2013 standard. You need to assess the company's current state of compliance.

What should you use?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 55

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E3 subscription.

You plan to launch Attack simulation training for all users.

Which social engineering technique and training experience will be available? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Social engineering technique:

▼

Credential harvest

Link to malware

Malware attachment

Training experience:

▼

Identity Theft

Mass Market Phishing

Web Phishing

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Credential Harvest

Attack simulation training offers a subset of capabilities to E3 customers as a trial. The trial offering contains the ability to use a Credential Harvest payload and the ability to select 'ISA Phishing' or 'Mass Market Phishing' training experiences. No other capabilities are part of the E3 trial offering.

Note: In Attack simulation training, multiple types of social engineering techniques are available: Credential Harvest

Malware Attachment Link to Malware Etc.

Box 2: Mass Market Phishing Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulation-training-get-start>

NEW QUESTION 57

- (Exam Topic 5)

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

- Windows 10
- Android
- OS

On which devices can you configure the Endpoint DLP policies?

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

Answer: C

Explanation:

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

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

NEW QUESTION 58

- (Exam Topic 5)

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

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

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

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

Answer: E

Explanation:

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory

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

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

When you configure a label policy, you can:

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

Reference:

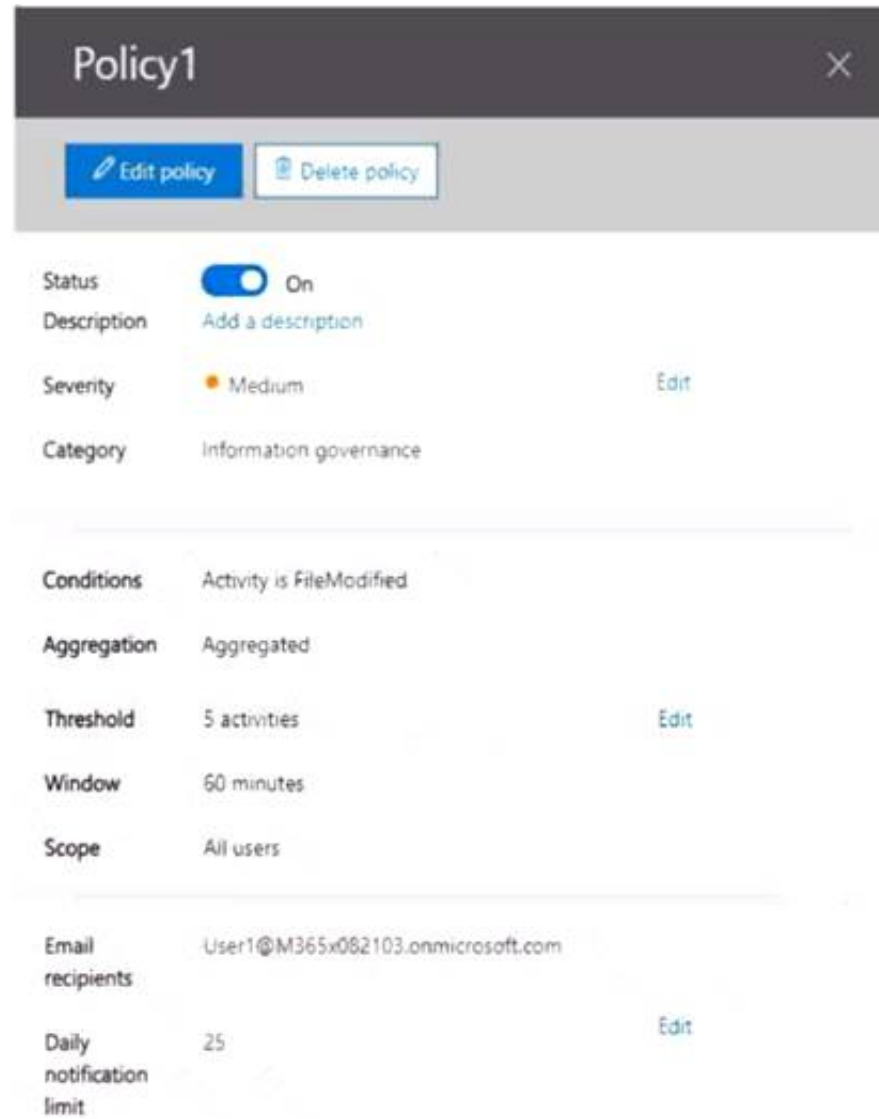
<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>

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

NEW QUESTION 63

- (Exam Topic 5)

You have a Microsoft 365 tenant that contains two users named User1 and User2. You create the alert policy shown in the following exhibit.



The screenshot shows the configuration for an alert policy named 'Policy1'. The policy is currently 'On'. The description is 'Add a description'. The severity is set to 'Medium' with an 'Edit' link. The category is 'Information governance'. The conditions are 'Activity is FileModified'. The aggregation is 'Aggregated'. The threshold is '5 activities' with an 'Edit' link. The window is '60 minutes'. The scope is 'All users'. The email recipients are 'User1@M365x082103.onmicrosoft.com'. The daily notification limit is '25' with an 'Edit' link.

User2 runs a script that modifies a file in a Microsoft SharePoint Online library once every four minutes and runs for a period of two hours. How many alerts will User1 receive?

- A. 2
- B. 5
- C. 10
- D. 25

Answer: D

NEW QUESTION 67

- (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, configure 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 70

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 tenant.

You need to create a custom Compliance Manager assessment template.

Which application should you use to create the template, and in which file format should the template be saved? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Application:

Microsoft Excel
Microsoft Forms
Microsoft Word
Visual Studio Code

File format:

csv
dbx
docx
dotx
json
xlsx
xltx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 71

- (Exam Topic 5)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

- A. Yes
- B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 73

- (Exam Topic 5)

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

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

You have a computer that runs Windows 10.

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 76

- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the domains shown in the following exhibit.

Domains

+ Add domain

Buy domain

Refresh

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

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

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

Answer: B

NEW QUESTION 78

- (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.	<input checked="" type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.20.15, User2 must use MFA.	<input type="radio"/>	<input type="radio"/>
When User2 connects to App1 from a device that has an IP address of 131.107.5.5, User2 must use MFA.	<input type="radio"/>	<input type="radio"/>

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 80

- (Exam Topic 5)

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

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

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

You plan to create a policy to show only the private store in Microsoft Store for Business. To which devices can the policy be applied?

- A. Device2 only
- B. Device1 and Device3 only
- C. Device2 and Device4 only
- D. Device2, Device3, and Device5 only
- E. Device1, Device2, Device3, Device4, and Device5

Answer: C

NEW QUESTION 81

- (Exam Topic 5)

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

Devices are onboarded by using Microsoft Defender for Endpoint.

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

What should you create first?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 86

- (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.)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

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 88

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You need to retain Azure Active Directory (Azure AD) audit logs for two years. Administrators must be able to query the audit log information by using the Azure Active Directory admin center.

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

Answer Area

Save the audit logs to:

Azure Active Directory admin center blade to use to view the saved audit logs:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to:

Azure Active Directory admin center blade to use to view the saved audit logs:

NEW QUESTION 92

- (Exam Topic 5)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

- A. Yes
- B. No

Answer:

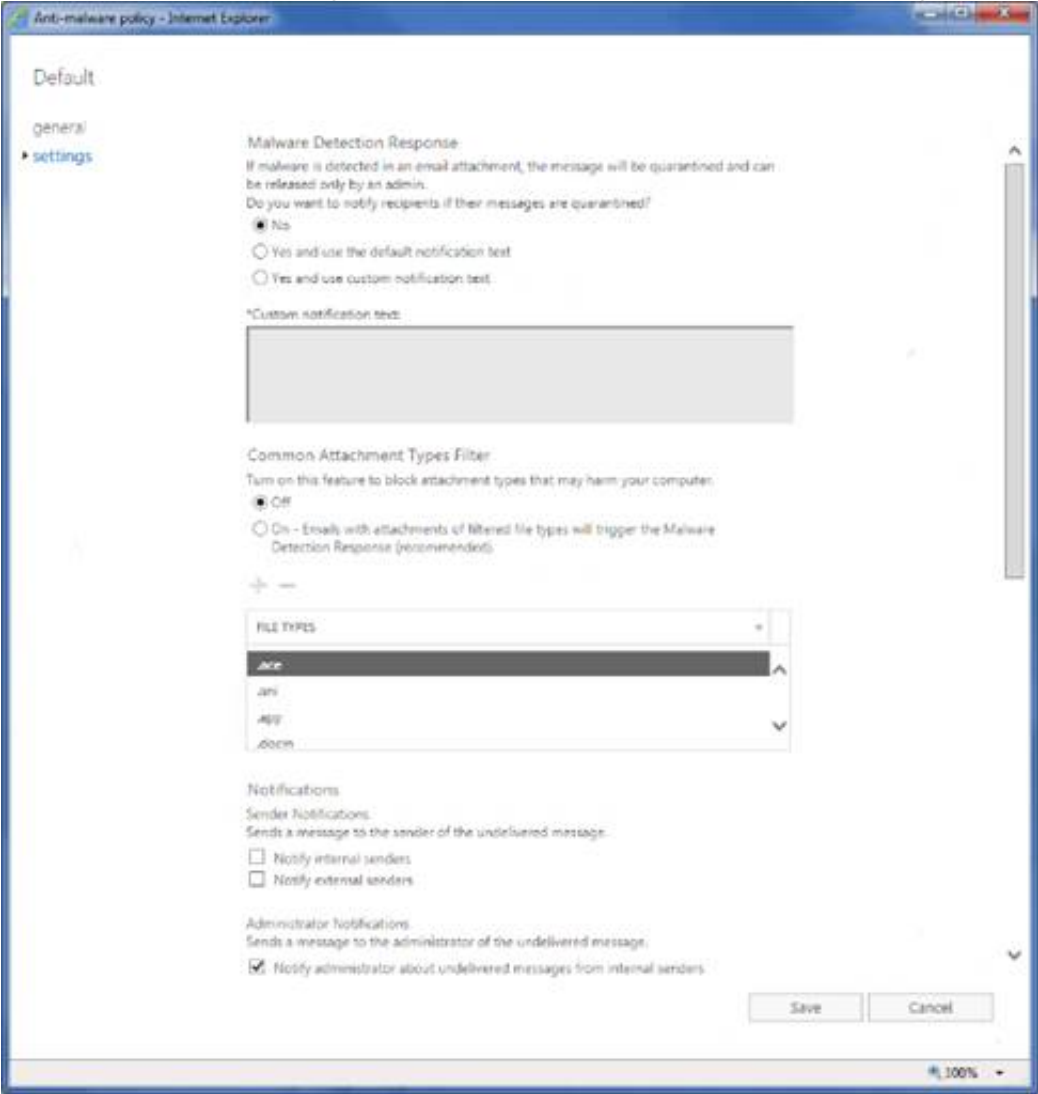
B

Explanation:

You need to assign the Security Administrator role. Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwi>

NEW QUESTION 96

- (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 99

- (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 100

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

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

Which type of policy should you create and which Microsoft 365 compliance center role is required to create the pokey? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Policy type:

Alert
Threat
Compliance

Role:

Quarantine
Security Administrator
Organization Configuration
Communication Compliance Admin

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy type:

Alert
Threat
Compliance

Role:

Quarantine
Security Administrator
Organization Configuration
Communication Compliance Admin

NEW QUESTION 103

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that contains 200 Android devices enrolled in Microsoft Intune. You create an Android app protection policy named Policy! that is targeted to all Microsoft apps and assigned to all users. Policy! has the Data protection settings shown in the following exhibit.

Select apps to exempt Select

Save copies of org data ⓘ Allow Block

Allow user to save copies to selected services ⓘ SharePoint

Transfer telecommunication data to ⓘ Any Dialer App

Dialer App Package ID

Dialer App Name

Received data from other apps ⓘ All Apps

Open data into Org documents ⓘ Allow Block

Allow users to open data from services ⓘ 3 selected

Restrict cut, copy, and paste between other apps ⓘ Policy managed apps with paste in

Cut and copy character limit for any app 0

Screen capture and Google Assistant ⓘ Allow Block

Approved keyboards ⓘ Require Not required

Select keyboards to approve Select

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

Answer Area

A user can copy files from Microsoft OneDrive to [answer choice] only.

▼

OneDrive
local storage
Microsoft SharePoint Online
Microsoft SharePoint Online and OneDrive

A user can copy and paste text from [answer choice] to Microsoft Word document stored in Microsoft OneDrive.

▼

any app
only managed apps
only unmanaged apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

A user can copy files from Microsoft OneDrive to [answer choice] only.

▼

OneDrive
~~local storage~~
Microsoft SharePoint Online
Microsoft SharePoint Online and OneDrive

A user can copy and paste text from [answer choice] to Microsoft Word document stored in Microsoft OneDrive.

▼

any app
only managed apps
only unmanaged apps

NEW QUESTION 105

- (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	<ul style="list-style-type: none">• Manage service requests.• Purchase new services.• Manage subscriptions.• Monitor service health.
Group2	<ul style="list-style-type: none">• 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.

Roles

Billing Administrator

Global Administrator

Helpdesk Administrator

License Administrator

Service Support Administrator

User Administrator

Answer Area

Group1:

Role

Group2:

Role

- A. Mastered
- B. Not Mastered

Answer: A

Passing Certification Exams Made Easy

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

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 110

- (Exam Topic 5)

You have a Microsoft 365 subscription. You have a user named User1. You need to ensure that User1 can place a hold on all mailbox content. What permission should you assign to User1?

- A. the Information Protection administrator role from the Azure Active Directory admin center.
- B. the eDiscovery Manager role 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 112

- (Exam Topic 5)

HOTSPOT

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

Name	Member of	Multi-factor authentication (MFA) method registered
User1	Group1	Microsoft Authenticator app (push notification)
User2	Group2	Microsoft Authenticator app (push notification)
User3	Group1	None

You configure the Microsoft Authenticator authentication method policy to enable passwordless authentication as shown in the following exhibit.



Name	Type	Registration	Authentication mode
Group1	Group	Optional	Any

Both User1 and User2 report that they are NOT prompted for passwordless sign-in in the Microsoft Authenticator app.

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

User1 will be prompted for passwordless authentication once User1 sets up phone sign-in in the Microsoft Authenticator app.

Yes	No
<input type="radio"/>	<input type="radio"/>

User2 will be prompted for passwordless authentication once User2 sets up phone sign-in in the Microsoft Authenticator app.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

User3 can use passwordless authentication without further action.

<input type="radio"/>	<input type="radio"/>
-----------------------	-----------------------

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

User1 is member of Group1.

User1 has MFA registered method of Microsoft Authenticator app (push notification)

The Microsoft Authenticator authentication method policy is configured for Group1, registration is optional, authentication method is any.

Note: Microsoft Authenticator can be used to sign in to any Azure AD account without using a password. Microsoft Authenticator uses key-based authentication to enable a user credential that is tied to a device, where the device uses a PIN or biometric. Windows Hello for Business uses a similar technology.

This authentication technology can be used on any device platform, including mobile. This technology can also be used with any app or website that integrates with Microsoft Authentication Libraries.

Box 2: No

User2 is member of Group2.
The Microsoft Authenticator authentication method policy is configured for Group1, not for Group2. Box 3: No
User3 is member of Group1.
User3 has no MFA method registered.
User3 must choose an authentication method.
Note: Enable passwordless phone sign-in authentication methods
Azure AD lets you choose which authentication methods can be used during the sign-in process. Users then register for the methods they'd like to use.
Reference:
<https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-phon>

NEW QUESTION 114


- (Exam Topic 5)
HOTSPOT

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

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

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

Settings > Endpoints > computer1

 **computer1**

Device summary

Risk level ⓘ
None

Device details

Domain
adatum.com

OS
Windows 10 64-bit
Version 21H2
Build 19044.2130

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

Answer Area

Computer1 will be a member of [answer choice].

Group3 only

Group4 only

Group3 and Group4 only

Ungrouped devices

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

Group1 only

Group1 and Group2 only

Group1, Group2, Group3, and Group4

Ungrouped devices

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 115

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

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 120

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has he files in the following table.

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

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

Name	Role
User1	Owner
User2	Visitor

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

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings
- Review your settings

Review your settings

Template name
Custom policy [Edit](#)

Policy name
Policy1 [Edit](#)

Description [Edit](#)

Applies to content in these locations
SharePoint sites [Edit](#)

Policy settings [Edit](#)
 If the content contains these types of sensitive info: IP Address
 then notify people with a policy tip and email message.
 If there are at least 2 instances of the same type of sensitive info,
 block access to the content.

Turn policy on after it's created? [Edit](#)
 Yes

How many files will be visible to user1 and User2 after Policy' is applied to answer, selected select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

User1:

1

2

3

4

5

User2:

1

2

3

4

5

NEW QUESTION 122

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
Conditional Access is configured to block high-risk sign-ins for all users.
All users are in France and are registered for multi-factor authentication (MFA). Users in the media department will travel to various countries during the next month.
You need to ensure that if the media department users are blocked from signing in while traveling, the users can remediate the issue without administrator intervention. What should you configure?

- A. an exclusion group
- B. the MFA registration policy
- C. named locations
- D. self-service password reset (SSPR)

Answer: D

Explanation:
Self-remediation with self-service password reset
If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.
Reference:
<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate>

NEW QUESTION 123

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

Name	Role
Admin1	Global Administrator
Admin2	Security Administrator
Admin3	Security Operator
Admin4	Security Reader
Admin5	Application Administrator

You are implementing Microsoft Defender for Endpoint. You need to enable role-based access control (RBAC) to restrict access to the Microsoft 365 Defender portal. Which users can enable RBAC, and which users will no longer have access to the Microsoft 365 Defender portal after RBAC is enabled? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Users that can enable RBAC:

Admin1 and Admin2 only

Admin1 only

Admin1 and Admin2 only

Admin1, Admin2, and Admin5 only

Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

Admin3, Admin4, and Admin5 only

Admin5 only

Admin3 and Admin4 only

Admin4 and Admin5 only

Admin3, Admin4, and Admin5 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users that can enable RBAC:

Admin1 and Admin2 only

Admin1 only

Admin1 and Admin2 only

Admin1, Admin2, and Admin5 only

Admin1, Admin2, Admin3, and Admin5 only

Users that will no longer have access to the Microsoft 365 Defender portal:

Admin3, Admin4, and Admin5 only

Admin5 only

Admin3 and Admin4 only

Admin4 and Admin5 only

Admin3, Admin4, and Admin5 only

NEW QUESTION 127

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant.

Users at the company use the following versions of Microsoft Office:

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

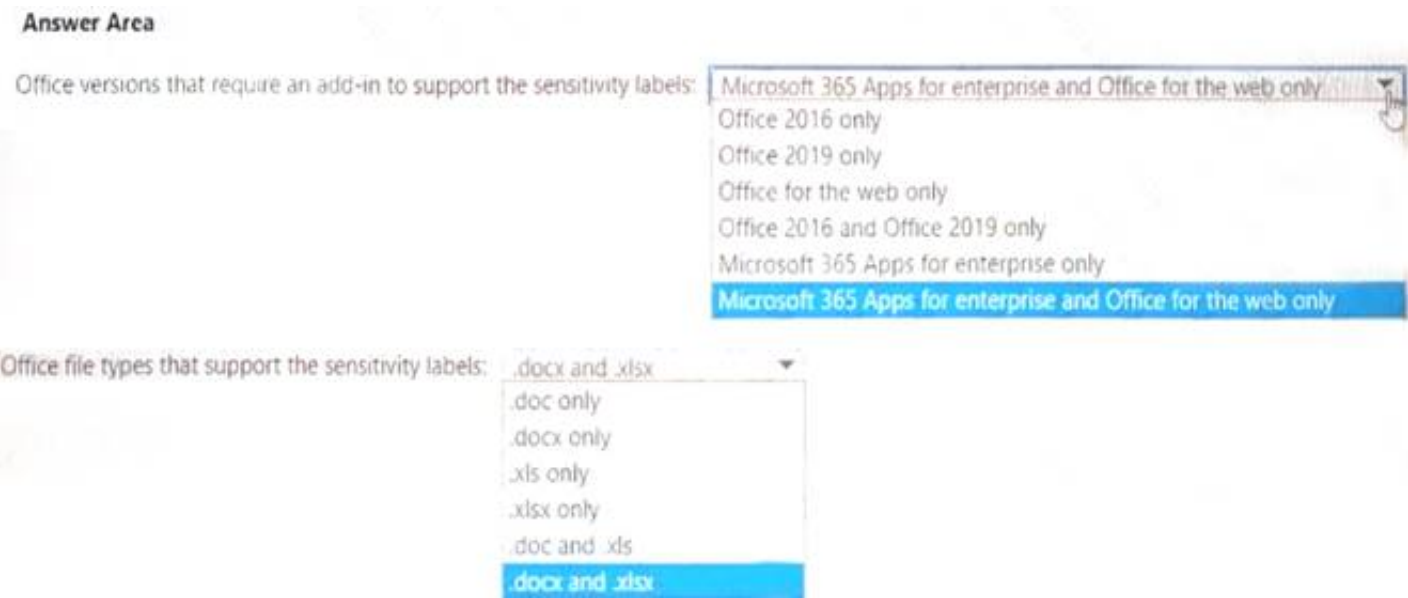
The company currently uses the following Office file types:

- .docx
- .xlsx
- .doc
- .xls

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

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

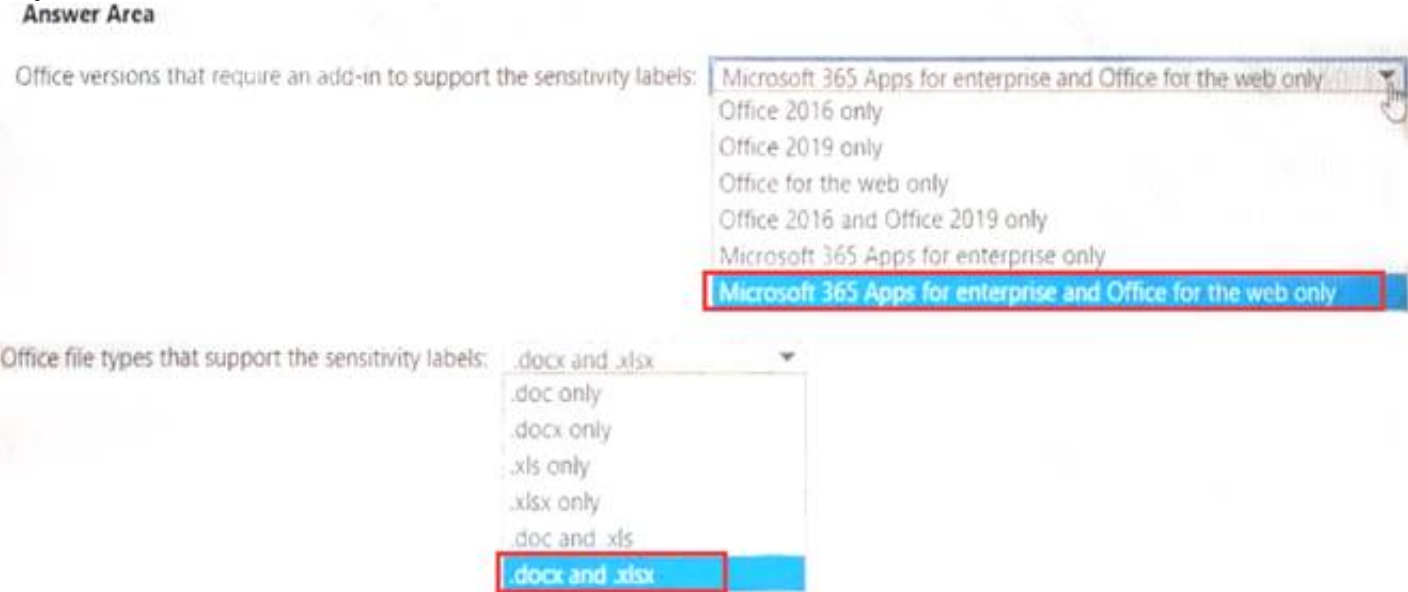
What should you identify? To answer, select the appropriate options in the answer area, NOTE: Each correct selection is worth one point.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 128

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

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

You plan to create a new Windows 10 Security Baseline profile. To which groups can you assign to the profile?

- A. Group3 only
- B. Group1 and Group3 only
- C. Group2 and Group3 only
- D. Group1. Group2. and Group3

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile> <https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

NEW QUESTION 130

- (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 133

- (Exam Topic 5)
 You have a Microsoft 365 tenant that contains 100 Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager. You plan to create two attack surface reduction (ASR) policies named ASR1 and ASR2. ASR1 will be used to configure Microsoft Defender Application Guard. ASR2 will be used to configure Microsoft Defender SmartScreen. Which ASR profile type should you use for each policy? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

ASR1:

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

ASR2:

Device control
Exploit protection
Application control
App and browser isolation
Attack surface reduction rules

- 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/protect/endpoint-security-asr-policy>

NEW QUESTION 135

- (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 139

- (Exam Topic 5)
 You have a Microsoft 365 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. User1 is assigned the Owner role for Site1. To Site1, you publish the file plan retention labels shown in the following table.

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

Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3

Which files can User1 rename, and which files can User1 delete? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Answer Area

Rename:

File1, File2, and File3 only

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

Delete:

File1 and File2 only

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Rename:

File1, File2, and File3 only

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

Delete:

File1 and File2 only

File1 only

File1 and File2 only

File1, File2, and File3 only

File1, File2, File3, and File4

NEW QUESTION 143

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

Create retention label

Name

Label Settings

Period

Finish

Review and finish

Name

Retention1

Edit

Retention settings

Retention period

6 months

Edit

Retention action

Retain and Delete

Edit

Based on

Based on when it was created

Edit

You apply Retention1 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 148

- (Exam Topic 5)

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

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group1, Group2
Device2	Windows 10	Disabled	Group2, Group3
Device3	Windows 10	Disabled	Group3

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

Name	Require BitLocker	Mark noncompliant after (days)	Assigned
Policy1	Require	5	No
Policy2	Require	10	Yes
Policy3	Not configured	15	Yes

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 151

- (Exam Topic 5)

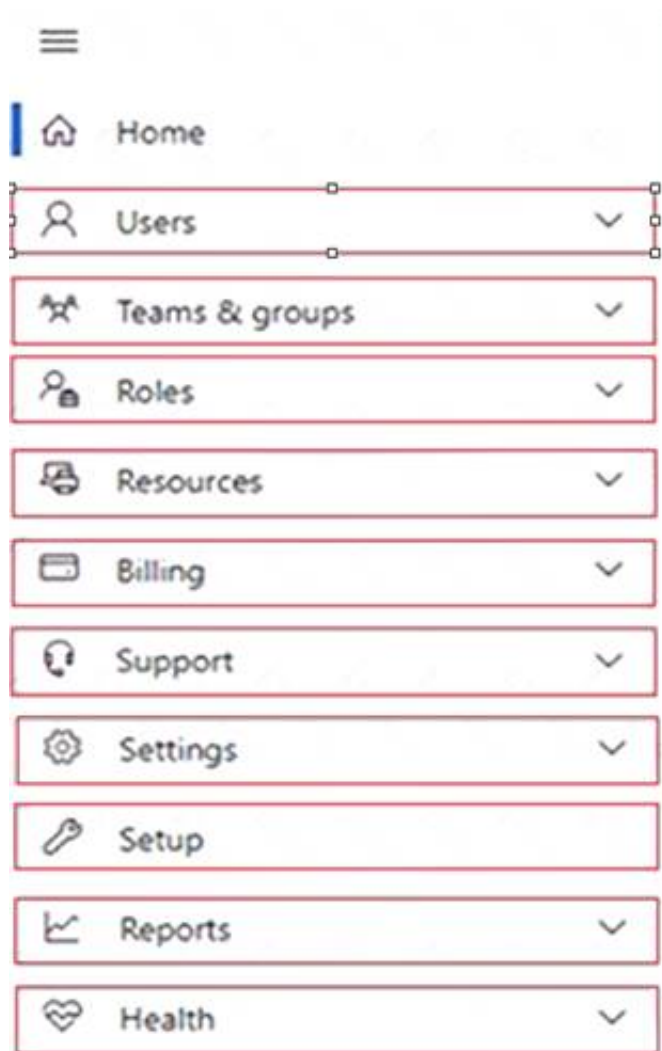
HOTSPOT

Your company has a Microsoft 365 E5 subscription. You need to perform the following tasks:

View the Adoption Score of the company. Create a new service request to Microsoft.

Which two options should you use in the Microsoft 365 admin center? 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:

Box 1: Reports

View the Adoption Score of the company. How to enable Adoption Score

To enable Adoption Score:

- > Sign in to the Microsoft 365 admin center as a Global Administrator and go to Reports > Adoption Score
- > Select enable Adoption Score. It can take up to 24 hours for insights to become available.

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request. If you're in the admin center, select Support > New service request.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score> <https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9-c13d1085>

NEW QUESTION 153

- (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 154

- (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 157
- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling(preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

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

- Which labels can users apply to content?
- A. Label1, Label2, and Label5 only
 - B. Label3, Label4, and Label6 only
 - C. Label1, Label3, Label2, and Label6 only
 - D. Label1, Label2, Label3, Label4, Label5, and Label6

Answer: C

NEW QUESTION 160
- (Exam Topic 5)
You have a Microsoft 365 ES tenant.
You have the alerts shown in the following exhibit.

View alerts

Export Filter

Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
Medium	Alert1	Active	-	Threat management	2	3 minutes ago
High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

Answer Area

For Alert1, you can change Status to

For Alert5, you can

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

For Alert1, you can change Status to

Investigating only

Investigating or Resolved only

Investigating or Dismissed only

Investigating, Resolved, or Dismissed

For Alert5, you can

not change Status

change Status to Dismissed only

change Status to Dismissed or Active only

change Status to Dismissed or Investigating only

change Status to Dismissed, Investigating, or Active

NEW QUESTION 164
- (Exam Topic 5)
You have a Microsoft 365 subscription that contains the devices shown in the following table.

Name	Operating system	Microsoft Intune
Device1	Windows 11 Enterprise	Enrolled
Device2	iOS	Enrolled
Device3	Android	Not enrolled

You install Microsoft Word on all the devices.
You plan to configure policies to meet the following requirements:

- Word files created by using Windows devices must be encrypted automatically.
- If an Android device becomes jailbroken, access to corporate data must be blocked from Word.
- For iOS devices, users must be prevented from using native or third-party mail clients to connect to Microsoft 365.

Which type of policy should you configure for each device? To answer, drag the appropriate policy types to the correct devices. Each policy type 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.

Policy Types

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1:

Device2:

Device3:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Policy Types

App configuration policy

App protection policy

Compliance policy

Conditional Access policy

Answer Area

Device1: App protection policy

Device2: Conditional Access policy

Device3: Compliance policy

NEW QUESTION 167
- (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

Tool:

AccessChk
Azure AD Connect
Active Directory Explorer
IdFix

Required group membership:

Domain Admins
Domain Users
Server Operators
Enterprise Admins

- 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 Windows 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/ldfix/>

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-groups>

NEW QUESTION 169

- (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 170

- (Exam Topic 5)

You have a Microsoft 365 tenant and a LinkedIn company page.

You plan to archive data from the LinkedIn page to Microsoft 365 by using the LinkedIn connector. Where can you store data from the LinkedIn connector?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 173

- (Exam Topic 5)

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

Choose the types of content to protect

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

Content contains

Any of these

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

Retention labels

1 year	
--------	--

Add

+ Add group

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

NOTE: Each correct selection is worth one point.

DLP1 cannot be applied to [answer choice].

Exchange email

SharePoint sites

OneDrive accounts

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

both a credit card number and the 1 year label applied

either a credit card number or the 1 year label applied

between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Using a retention label in a policy is only supported for items in SharePoint Online and OneDrive for Business.

Reference:

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

NEW QUESTION 176

- (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.)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Enabled	2 agents

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 Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

The on-premises Active Directory domain is named contoso.com. To enable users to sign on using a different UPN (different domain), you need to add the domain to Microsoft 365 as a custom domain.

NEW QUESTION 177

- (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 apps or actions: All cloud apps
- > Access controls:
- > Grant, require multi-factor authentication
- > Enable policy: Report-only

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

Reference:

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

NEW QUESTION 179

- (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 identity sensors.

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

- A. Yes
- B. No

Answer: A

NEW QUESTION 182

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

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

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

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

Answer: B

NEW QUESTION 183

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

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

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

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

What should you configure?

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

Answer: B

Explanation:

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

Sign-in risk policy User risk policy

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

Reference:

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

NEW QUESTION 185

- (Exam Topic 5)

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

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

You have a Microsoft 365 E5 subscription.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 190

- (Exam Topic 5)

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

Name	Require BitLocker	Require the device to be at or under the machine risk score
Policy1	Required	High
Policy2	Not configured	Medium
Policy3	Required	Low

The tenant contains the devices shown in the following table.

Name	BitLocker Drive Encryption (BitLocker)	Microsoft Defender for Endpoint risk status	Policies applied
Device1	Configured	High	Policy1, Policy3
Device2	Not configured	Medium	Policy2, Policy3
Device3	Not configured	Low	Policy1, Policy2

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

Statements	Yes	No
Device1 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device2 is marked as compliant.	<input type="radio"/>	<input type="radio"/>
Device3 is marked as compliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 191

- (Exam Topic 5)

You plan to use Azure Sentinel and Microsoft Cloud App Security. You need to connect Cloud App Security to Azure Sentinel.

What should you do in the Cloud App Security admin center?

- A. From Automatic log upload, add a log collector.
B. From Automatic log upload, add a data source.
C. From Connected apps, add an app connector.
D. From Security extension, add a SIEM agent.

Answer: D

NEW QUESTION 196

- (Exam Topic 5)

HOTSPOT

			progress	actions	status			
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Answer Area	Statements	Yes	No
	Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
	The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
	The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input checked="" type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input checked="" type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 197

- (Exam Topic 5)

You have a Microsoft 365 tenant that has Enable Security defaults set to No in Azure Active Directory (Azure AD). The tenant has two Compliance Manager assessments as shown in the following table.

Name	Score	Status	Assessment progress	Your improvement actions	Microsoft actions	Group	Product	Regulation
SP800	15444	Incomplete	72%	3 of 450 completed	887 of 887 completed	Group1	Microsoft 365	NIST 800-53
Data Protection Baseline	14370	Incomplete	70%	3 of 489 completed	835 of 835 completed	Group2	Microsoft 365	Data Protection Baseline

The SP800 assessment has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Regulations
Establish a threat intelligence program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline
Establish and document a configuration management program	None	+9 points	0/9	NIST 800-53, Data Protection Baseline

You perform the following actions:

- > For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.
- > Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in the SP800 assessment.	<input type="radio"/>	<input type="radio"/>
The SP800 assessment score will increase by 54 points.	<input type="radio"/>	<input type="radio"/>
The Data Protection Baseline score will increase by 9 points.	<input type="radio"/>	<input type="radio"/>

- 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/compliance-manager-assessments?view=o365-world> <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-world>

NEW QUESTION 199

- (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 204

- (Exam Topic 5)

HOTSPOT

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

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The tenant contains the devices shown in the following table.

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

You have the apps shown in the following table.

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

You plan to use Microsoft Endpoint Manager to manage the apps for the users.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
App1 can be assigned as a required install for User3.	<input type="radio"/>	<input type="radio"/>
App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
App3 can be installed automatically for UserGroup1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/mem/intune/apps/apps-deploy> <https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>

NEW QUESTION 207

- (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 211

- (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 213

- (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 215

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint.

When users attempt to access the portal of a partner company, they receive the message shown in the following exhibit.



You need to enable user access to the partner company's portal. Which Microsoft Defender for Endpoint setting should you modify?

- A. Alert notifications
- B. Alert suppression
- C. Custom detections
- D. Advanced hunting
- E. Indicators

Answer: E

Explanation:

This Website Is Blocked By Your Organization

Custom indicators will block malicious IPs, URLs, and domains. Then, they will display the above message for the user.

Reference:

<https://jadexstrategic.com/web-protection/>

NEW QUESTION 218

- (Exam Topic 5)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 has their cache cleared on close.	<input type="radio"/>	<input type="radio"/>
User2 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>
User3 has Cursor movement set to Visual.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 221

- (Exam Topic 5)

You have a Microsoft 365 subscription.

Your network uses an IP address space of 51.40.15.0/24.

An Exchange Online administrator recently created a role named Role1 from a computer on the network. You need to identify the name of the administrator by using an audit log search.

For which activities should you search and by which field should you filter in the audit log search? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Activities to search for:

▼

Exchange mailbox activities

Site administration activities

Show results for all activities

Role administration activities

Field to filter by:

▼

Item

User

Detail

IP address

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Activities to search for:

▼

Exchange mailbox activities

Site administration activities

Show results for all activities

Role administration activities

Field to filter by:

▼

Item

User

Detail

IP address

NEW QUESTION 224

- (Exam Topic 5)

You have a Microsoft 365 subscription.

From Microsoft 365 Defender, you create a role group named US eDiscovery Managers by copying the eDiscovery Manager role group.

You need to ensure that the users in the new role group can only perform content searches of mailbox content for users in the United States.

Solution: From Windows PowerShell, you run the New-complianceSecurityFilter cmdlet with the appropriate parameters.

Does this meet the goal?

- A. Yes

B. No

Answer: A

NEW QUESTION 227

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 tenant.

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

Information governance > Create retention policy

Name

Locations

Retention settings

Finish

Review and finish

It might take up to one day to apply this policy to the locations you selected.

Policy name
contoso
[Edit](#)

Description
[Edit](#)

Locations to apply the policy
Exchange email (All Recipients)
SharePoint sites (All Sites)
OneDrive accounts (All Accounts)
Microsoft 365 Groups (All Groups)
[Edit](#)

Retention settings
Delete items at end of retention period
Delete items that are older than 7 years based on when they were created
[Edit](#)

⚠ Items that are currently older than 7 years will be deleted after you turn on this policy. This is especially important to note for locations scoped to 'All' sources (for example, 'All Teams chats') because all matching items in those locations across your organization will be permanently deleted.

[Back](#)[Submit](#)[Cancel](#)

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

recoverable for up to seven years
deleted seven years after they were created
retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.

some data may be deleted immediately
data will be retained for a minimum of seven years
users will be prevented from permanently deleting email messages for seven years

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 231

- (Exam Topic 5)

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

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

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

Answer Area

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

Feature: Configuration analyzer
Configuration analyzer
Preset security policies
Threat tracker

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
Answer Area

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

Feature: Configuration analyzer
Configuration analyzer
Preset security policies
Threat tracker

NEW QUESTION 232

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant that has sensitivity label support enabled for Microsoft and SharePoint Online. You need to enable unified labeling for Microsoft 365 groups. Which cmdlet should you run?

- A. set-unifiedGroup
B. Set-Labelpolicy
C. Execute-AzureAdLabelSync
D. Add-UnifiedGroupLinks

Answer: C

NEW QUESTION 234

- (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 238

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

NEW QUESTION 239

- (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 subscription.

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

Solution: From the Endpoint Management admin center, you create a device configuration profile. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to create a trusted location and a conditional access policy.

NEW QUESTION 240

- (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 243

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You need to compare the current Safe Links configuration to the Microsoft recommended configurations. What should you use?

- A. Microsoft Purview
- B. Azure AD Identity Protection
- C. Microsoft Secure Score
- D. the configuration analyzer

Answer: C

NEW QUESTION 248

- (Exam Topic 5) You have a Microsoft 365 E5 tenant. You configure sensitivity labels.

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

You need to ensure that the users can apply the sensitivity labels when they use Word for the web. What should you do?

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

Answer: B

NEW QUESTION 252

- (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 254

- (Exam Topic 5)

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

Name	Role
User1	Exchange Administrator
User2	User Administrator
User3	Global Administrator
User4	None

You add another user named User5 to the User Administrator role. You need to identify which two management tasks User5 can perform.

Which two tasks should you identify? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Delete User2 and User4 only.
- B. Reset the password of User4 only
- C. Reset the password of any user in Azure AD.
- D. Delete User1, User2, and User4 only.
- E. Reset the password of User2 and User4 only.
- F. Delete any user in Azure AD.

Answer: AE

Explanation:

Users with the User Administrator role can create users and manage all aspects of users with some restrictions (see below).

Only on users who are non-admins or in any of the following limited admin roles:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Reports Reader
- User Administrator Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles#availab>

NEW QUESTION 258

- (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.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Site1 from Device3.	<input type="radio"/>	<input type="radio"/>

- 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 260

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

Solutions	Answer Area
Data loss prevention	Identify, monitor, and automatically protect sensitive information: <input type="text"/>
Information governance	Capture employee communications for examination by designated reviewers: <input type="text"/>
Insider risk management	Use a file plan to manage retention labels: <input type="text"/>
Records management	

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 262

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?
A. From the Cloud App Security admin center, select Users and accounts.
B. From the Microsoft 365 security center, view the Threat tracker.
C. From the Microsoft 365 admin center, view the Security & compliance report.

D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

NEW QUESTION 263

- (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 268

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

industry regulations require that the tenant comply with the ISO 27001 standard. You need to evaluate the tenant based on the standard

A. From Policy in the Azure portal, select Compliance, and then assign a pokey

B. From Compliance Manager, create an assessment

C. From the Microsoft J6i compliance center, create an audit retention policy.

D. From the Microsoft 365 admin center enable the Productivity Score.

Answer: B

NEW QUESTION 273

- (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 278

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You have the retention policies shown in the following table.

Name	Location	Retain items for a specific period	Start the retention period based on	At the end of the retention period
Policy1	SharePoint sites	1 years	When items were created	Delete items automatically
Policy2	SharePoint sites	2 years	When items were last modified	Do nothing

Both policies are applied to a Microsoft SharePoint site named Site1 that contains a file named File1.docx. File1.docx was created on January 1, 2022 and last modified on January 31,2022. The file was NOT modified again.

When will File1.docx be deleted automatically?

- A. January 1,2023
- B. January 1,2024
- C. January 31, 2023
- D. January 31, 2024
- E. never

Answer: D

Explanation:

for the four different principles:
* 1. Retention wins over deletion. Content won't be permanently deleted when it also has retention settings to retain it. While this principle ensures that content is preserved for compliance reasons, the delete process can still be initiated (user-initiated or system-initiated) and consequently, might remove the content from users' main view. However, permanent deletion is suspended.
* 2. Etc. Reference:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention>

NEW QUESTION 281

- (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.	<input type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Device1 has an overall compliance state of Compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device2 has an overall compliance state of Not compliant.	<input checked="" type="radio"/>	<input type="radio"/>
Device3 has an overall compliance state of In grace period.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 283

- (Exam Topic 5)
You have a Microsoft 365 E5 subscription that uses Azure Advanced Threat Protection (ATP). You need to create a detection exclusion in Azure ATP. Which tool should you use?

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

Answer: D

Explanation:

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

NEW QUESTION 286

- (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 291

- (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 294

- (Exam Topic 5)

You purchase a new computer that has Windows 10, version 2004 preinstalled.

You need to ensure that the computer is up-to-date. The solution must minimize the number of updates installed.

What should you do on the computer?

- A. Install all the feature updates released since version 2004 and all the quality updates released since version 2004 only.
- B. install the West feature update and the latest quality update only.
- C. install all the feature updates released since version 2004 and the latest quality update only.
- D. install the latest feature update and all the quality updates released since version 2004.

Answer: B

NEW QUESTION 298

- (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.

Policy to create in Microsoft Endpoint Manager:

An app configuration policy

An app protection policy

A conditional access policy

A device compliance policy

Minimum number of required policies:

1

2

3

5

- 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 303

- (Exam Topic 5)
HOTSPOT

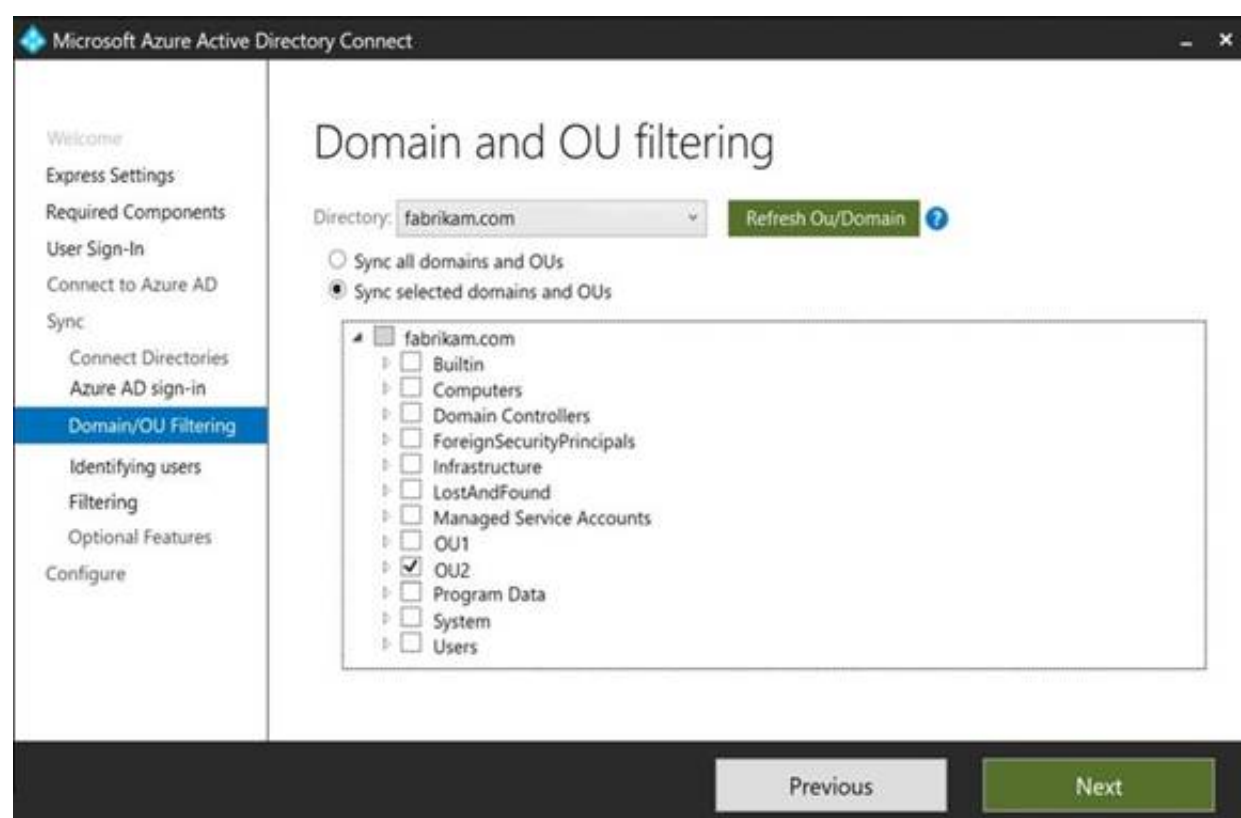
Your network contains an Active Directory domain named fabrikam.com. The domain contains the objects shown in the following table.

Name	Type	In organizational unit (OU)
User1	User	OU1
User2	User	OU1
Group1	Security Group – Global	OU1
User3	User	OU2
Group2	Security Group – Global	OU2

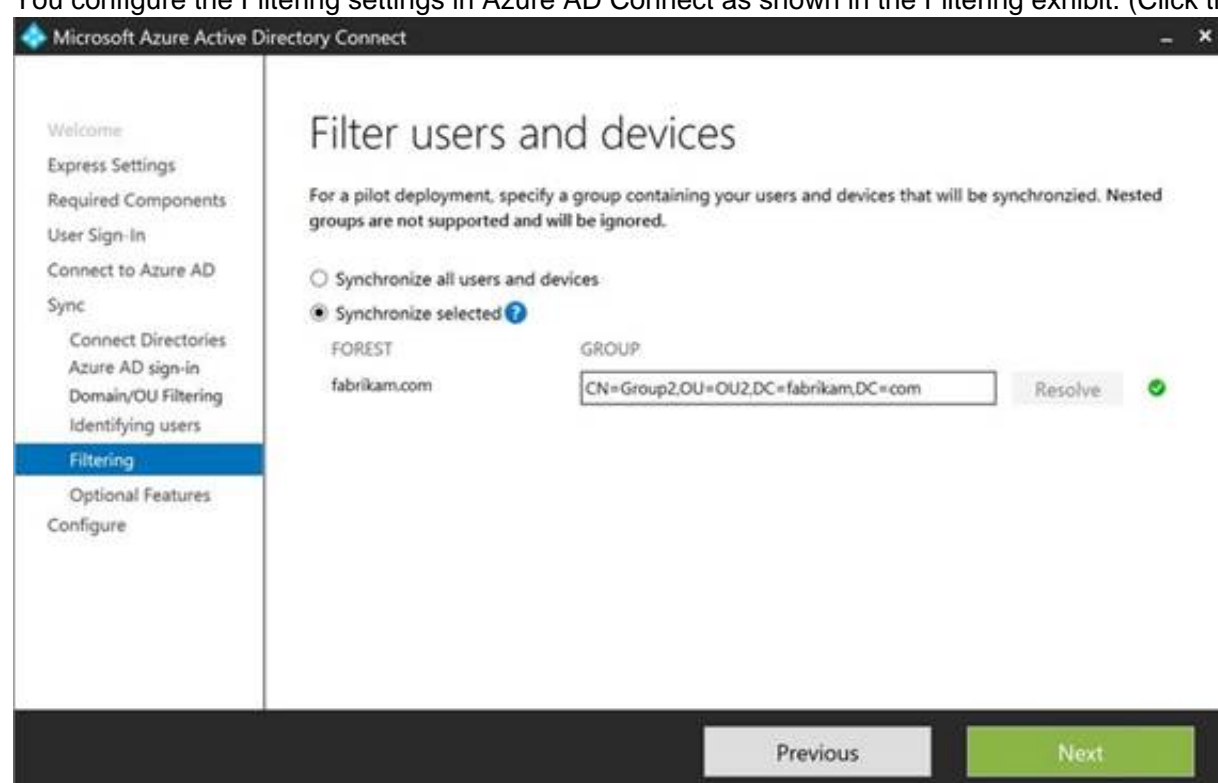
The groups have the members shown in the following table.

Group	Members
Group1	User1
Group2	User2, User3, Group1

You are configuring synchronization between fabrikam.com and an Azure AD tenant.
You configure the Domain/OU Filtering settings in Azure AD Connect as shown in the Domain/OU Filtering exhibit (Click the Domain/OU Filtering tab.)



You configure the Filtering settings in Azure AD Connect as shown in the Filtering exhibit. (Click the Filtering tab.)



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
User2 will synchronize to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
Group2 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>
User3 will synchronize to Azure AD.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: No

The filtering is configured to synchronize Group2 and OU2 only. The effect of this is that only members of Group2 who are in OU2 will be synchronized.

User2 is in Group2. However, the User2 account object is in OU1 so User2 will not synchronize to Azure AD. Box 2: Yes

Group2 is in OU2 so Group2 will synchronize to Azure AD. However, only members of the group who are in OU2 will synchronize. Members of Group2 who are in OU1 will not synchronize.

Box 3: Yes

User3 is in Group2 and in OU2. Therefore, User3 will synchronize to Azure AD. Reference:

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

NEW QUESTION 307

- (Exam Topic 5)

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

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices. You enable device clean-up rules.

What can you configure as the minimum number of days before a device is removed automatically?

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

Answer: D

NEW QUESTION 308

- (Exam Topic 5)

Your company has a Microsoft 365 E5 subscription. Users in the research department work with sensitive data.

You need to prevent the research department users from accessing potentially unsafe websites by using hyperlinks embedded in email messages and documents.

Users in other departments must not be restricted.

What should you do?

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

Answer: D

Explanation:

Use the Microsoft 365 Defender portal to create Safe Links policies.

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies

& Rules > Threat policies > Safe Links in the Policies section. Or, to go directly to the Safe Links page, use <https://security.microsoft.com/safelinksv2>.

* 1. On the Safe Links page, select Create to start the new Safe Links policy wizard.

* 2. On the Name your policy page, configure the following settings: Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.

* 3. When you're finished on the Name your policy page, select Next.

* 4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions):

Users: The specified mailboxes, mail users, or mail contacts.

*-> Groups:

Members of the specified distribution groups (including non-mail-enabled security groups within distribution groups) or mail-enabled security groups (dynamic distribution groups aren't supported).

The specified Microsoft 365 Groups.

Domains: All recipients in the specified accepted domains in your organization. Etc.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-links-policies-configure>

NEW QUESTION 313

- (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 315

- (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 320

- (Exam Topic 5)

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

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

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

Answer: B

NEW QUESTION 324

- (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.)

New audit retention policy

Name *

Policy1

Description

Record Types

AzureActiveDirectory ▾

Activities

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

Users:

Admin1 ▾

Duration *

☒ 90 Days

☐ 6 Months

☐ 1 Year

Priority *

100

Save

Cancel

After Policy1 is created, the following actions are performed:

- > Admin1 creates a user named User1.
- > Admin2 creates a user named User2.

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

NOTE: Each correct selection is worth one point.

User1:

▼

0 days

30 days

90 days

180 days

365 days

User2:

▼

0 days

30 days

90 days

180 days

365 days

- 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 329
- (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.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

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

NEW QUESTION 334
- (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 337

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

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