

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)

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

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

Answer: C

Explanation:

References:

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

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

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

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

Your network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).

You manage Windows 10 devices by using Microsoft System Center Configuration Manager (Current Branch).

You configure a pilot for co-management.

You add a new device named Device1 to the domain. You install the Configuration Manager client on Device1.

You need to ensure that you can manage Device1 by using Microsoft Intune and Configuration Manager. Solution: Define a Configuration Manager device collection as the pilot collection. Add Device1 to the collection.

Does this meet the goal?

- A. Yes
- B. NO

Answer: A

Explanation:

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

NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (Exam Topic 3)

You need to configure automatic enrollment in Intune. The solution must meet the technical requirements. What should you configure, and to which group should you assign the configurations? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure: ▼

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

Group: ▼

- UserGroup1
- UserGroup2
- DeviceGroup1
- DeviceGroup2

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Reference:

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

NEW QUESTION 10

- (Exam Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements. To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group: ▼

- Reviewer
- Global reader
- Data Investigator
- Compliance Management

Tool: ▼

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text Description automatically generated

Reference:

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

NEW QUESTION 10

- (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 13

- (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 14

- (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 15

- (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 assign User2 the Allow logon locally user right. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

This is not a permissions issue. 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 20

- (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.

From the 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 the Microsoft 365 Defender, you modify the roles of the US eDiscovery Managers role group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 25

- (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="radio"/> | <input type="radio"/> |
| App3 is displayed in the Company Portal. | <input checked="" type="radio"/> | <input type="radio"/> |
| Excel is installed on Device1. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 29

- (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 33

- (Exam Topic 5)

You have a Microsoft 365 tenant.

Company policy requires that all Windows 10 devices meet the following minimum requirements:

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

You need to prevent devices that do not meet the requirements from accessing resources in the tenant. Which two components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: BD

Explanation:

Reference:

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

NEW QUESTION 34

- (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 35

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You register two applications named App1 and App2 to Azure AD.

You need to ensure that users who connect to App1 require multi-factor authentication (MFA). MFA is required only for App1. What should you do?

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

Answer: A

Explanation:

Use Conditional Access policies

If your organization has more granular sign-in security needs, Conditional Access policies can offer you more control. Conditional Access lets you create and define policies that react to sign in events and request additional actions before a user is granted access to an application or service.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authenticati>

NEW QUESTION 37

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

A user named user1@contoso.com was recently provisioned.

You need to use PowerShell to assign a Microsoft Office 365 E3 license to User1. Microsoft Bookings must NOT be enabled.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

```

-Scopes User.ReadWrite.All, Organization.Read.All
Connect-AzureAD
Connect-MgGraph
Connect-MSOLService

$E3 = Get-AzureADUser | Where SkuPartNumber -eq 'EnterprisePack'
Get-MgSubscribedSku
Get-MSOLAccountSKU

$disabledPlans = $E3.ServicePlans | Where ServicePlanName -in ("MICROSOFTBOOKINGS") | select -ExcludeProperty ServicePlanID

$LicenseOptions= @(
    @(
        SkuId = $E3.SkuId
        DisabledPlans = $disabledPlans
    )
)

-UserId User1@contoso.com -AddLicenses $LicenseOptions -RemoveLicenses @()
Set-AzureADUser
Set-MgUserLicense
Set-MSOLUser
    
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Connect-MgGraph

Assign Microsoft 365 licenses to user accounts with PowerShell Use the Microsoft Graph PowerShell SDK

First, connect to your Microsoft 365 tenant.

Assigning and removing licenses for a user requires the User.ReadWrite.All permission scope or one of the other permissions listed in the 'Assign license' Microsoft Graph API reference page.

The Organization.Read.All permission scope is required to read the licenses available in the tenant. Connect-MgGraph -Scopes User.ReadWrite.All, Organization.Read.All

Box 2: Get-MgSubscribedSku

Run the Get-MgSubscribedSku command to view the available licensing plans and the number of available licenses in each plan in your organization. The number of available licenses in each plan is ActiveUnits - WarningUnits - ConsumedUnits.

Box 3: Set-MgUserLicense

Assigning licenses to user accounts

To assign a license to a user, use the following command in PowerShell.

Set-MgUserLicense -UserId \$userUPN -AddLicenses @{Skuld = "<Skuld>"} -RemoveLicenses @() This example assigns a license from the SPE_E5 (Microsoft 365 E5) licensing plan to the unlicensed user

belindan@litwareinc.com:

```
$e5Sku = Get-MgSubscribedSku -All | Where SkuPartNumber -eq 'SPE_E5'
```

```
Set-MgUserLicense -UserId "belindan@litwareinc.com" -AddLicenses @{Skuld = $e5Sku.Skuld}
```

```
-RemoveLicenses @()
```

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/assign-licenses-to-user-accounts-with-microsoft-365>

NEW QUESTION 39

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

You need to implement identity protection. The solution must meet the following requirements:

- > Identify when a user's credentials are compromised and shared on the dark web.
- > Provide users that have compromised credentials with the ability to self-remediate. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify when users have compromised credentials, configure:

- A registration policy
- A sign-in risk policy
- A user risk policy
- A multifactor authentication registration policy

To enable self-remediation, select:

- Generate a temporary password
- Require multi-factor authentication
- Require password change

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A user risk policy

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

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

Block access

Allow access but require a secure password change.

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

Box 2: Require password change

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

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

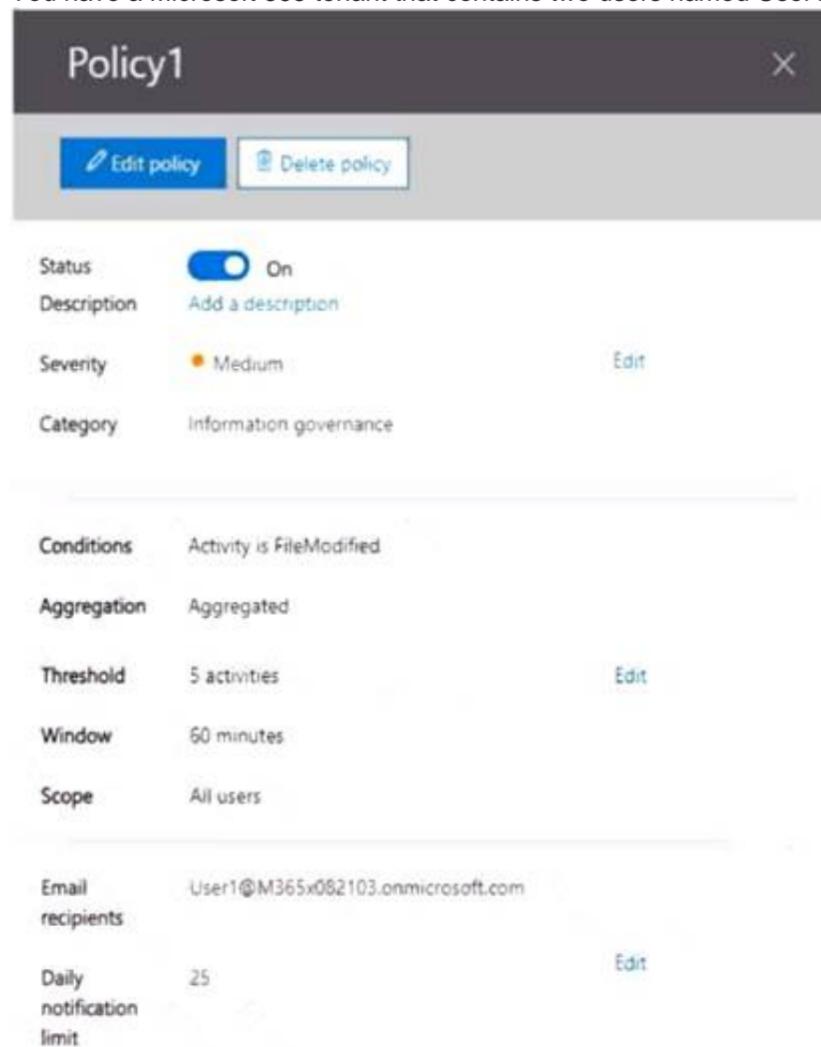
Reference:

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

NEW QUESTION 42

- (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.



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 46

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 47

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 E5 subscription.

From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

| Activation | |
|--|-----------|
| Setting | State |
| Activation maximum duration (hours) | 8 hour(s) |
| On activation, require | Azure MFA |
| Require justification on activation | Yes |
| Require ticket information on activation | No |
| Require approval to activate | No |
| Approvers | None |

| Assignment | |
|--|------------|
| Setting | State |
| Allow permanent eligible assignment | No |
| Expire eligible assignments after | 3 month(s) |
| Allow permanent active assignment | No |
| Expire active assignments after | 15 day(s) |
| Require Azure Multi-Factor Authentication on active assignment | Yes |
| Require justification on active assignment | Yes |

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

A user that is assigned the Global Administrator role as active [answer choice].

- will lose the role after eight hours
- can reactivate the role every eight hours
- can reactivate the role every 15 days
- will lose the role after 15 days

You can make the Global Administrator role available to activation requests [answer choice].

- for up to eight hours
- for up to three months
- for up to 15 days
- until the requests are revoked manually

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: will lose the role after eight hours

From exhibit: Activation, Activation maximum duration (hours): 8 hour(s) Box 2: for up to three months

We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 48

- (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:

File format:

- 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 53

- (Exam Topic 5)

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

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

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

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

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

| Name | Assigned to |
|---------|-------------|
| Policy1 | Group3 |
| Policy2 | Group2 |

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|-----------------------|----------------------------------|----------------------------------|
| Device1 is compliant. | <input type="radio"/> | <input checked="" type="radio"/> |
| Device2 is compliant. | <input type="radio"/> | <input checked="" type="radio"/> |
| Device3 is compliant. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 54

- (Exam Topic 5)

DRAG DROP

You have a Microsoft 365 E5 subscription. Several users have iOS devices.

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

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

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

Actions

Answer Area

- From the Microsoft Endpoint Manager admin center, add a device enrollment manager.
- From the Microsoft Endpoint Manager admin center, download a certificate signing request.
- Upload an Apple MDM push certificate to Microsoft Endpoint Manager.
- Create a certificate from the Apple Push Certificates Portal.
- From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 56

- (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 58

- (Exam Topic 5)

You have several devices enrolled in Microsoft Endpoint Manager.

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

| Name | Member of |
|-------|----------------|
| User1 | Group1 |
| User2 | Group1, Group2 |
| User3 | None |

The device type restrictions in Endpoint Manager are configured as shown in the following table.

| Priority | Name | Allowed platform | Assigned to |
|----------|-----------|-----------------------------|-------------|
| 1 | Policy1 | Android, iOS, Windows (MDM) | None |
| 2 | Policy2 | Windows (MDM) | Group2 |
| 3 | Policy3 | Android, iOS | Group1 |
| Default | All users | Android, Windows (MDM) | All users |

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

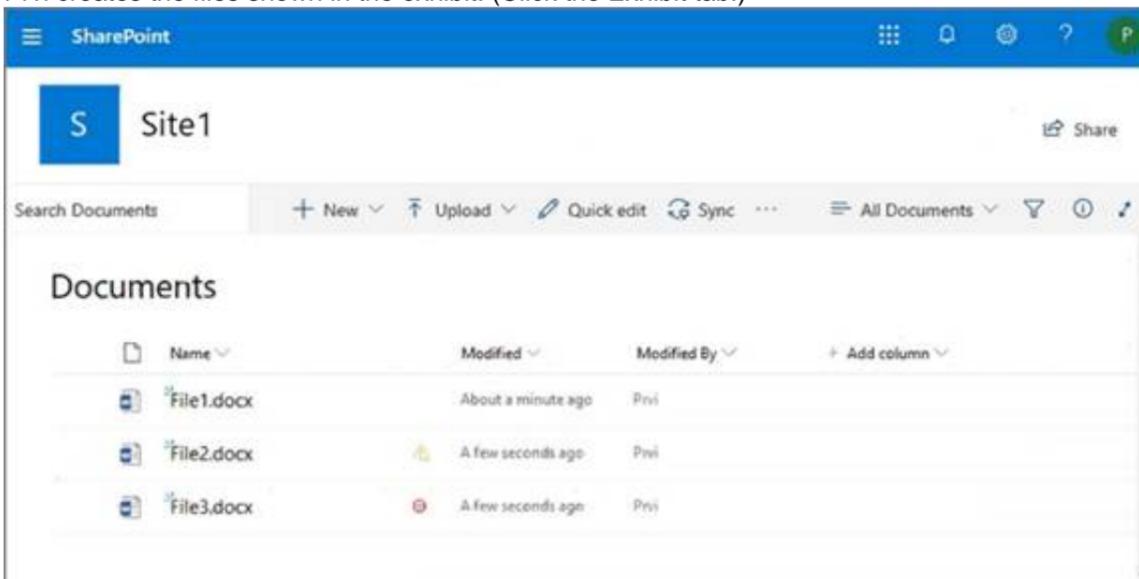
NEW QUESTION 61

- (Exam Topic 5)

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

| Role | Member |
|--------------|--------|
| Site owner | Prvi |
| Site member | User1 |
| Site visitor | User2 |

Prvi creates the files shown in the exhibit. (Click the Exhibit tab.)



Which files can User1 and User2 open? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

User1:

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

User2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

Reference:

<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/> <https://gcc.microsoftcrmpartals.com/blogs/office365-news/190220SPIcons/>

NEW QUESTION 66

- (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.

Use the drop-down menus to select the 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 70

- (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:

Group2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Billing admin manage service request
 Purchase new services Etc.

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

Box 2: User admin User admin

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

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

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

NEW QUESTION 74

- (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



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 78

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You plan to deploy a monitoring solution that meets the following requirements:

- > Captures Microsoft Teams channel messages that contain threatening or violent language.
- > Alerts a reviewer when a threatening or violent message is identified.

What should you include in the solution?

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

Answer: C

NEW QUESTION 81

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1. Site1 has the 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 loss prevention (DLP) policy names Policy1 as shown in the following exhibit.

How many files will be visible to user1 and User2 after Policy1 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:

User2:

NEW QUESTION 86

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 subscription.

You need to review metrics for the following: The daily active users in Microsoft Teams Recent Microsoft service issues

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

Answer Area

Teams daily active users:

Recent Microsoft service issues:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Usage reports

The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity

The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

You can view the health of your Microsoft services, including Office on the web, Yammer, Microsoft Dynamics CRM, and mobile device management cloud services, on the Service health page in the Microsoft 365 admin center. If you are experiencing problems with a cloud service, you can check the service health to determine whether this is a known issue with a resolution in progress before you call support or spend time troubleshooting.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/activity-reports/microsoft-teams-usage-activity> <https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

NEW QUESTION 88

- (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 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:

- 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 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:

- Admin5 only
- Admin3 and Admin4 only
- Admin4 and Admin5 only
- Admin3, Admin4, and Admin5 only**

NEW QUESTION 89

- (Exam Topic 5)

You implement Microsoft Azure Advanced Threat Protection (Azure ATP). You have an Azure ATP sensor configured as shown in the following exhibit.



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

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

Answer: B

NEW QUESTION 91

- (Exam Topic 5)

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

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

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

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

You add user as a device enrollment manager in Endpoint manager. For each of the following statements, select Yes if the statement is true. Otherwise, select No

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| User1 can enroll a maximum of 10 devices in Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User2 can enroll a maximum of 10 devices in Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User3 can enroll an unlimited number of devices in Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 can enroll a maximum of 10 devices in Endpoint Manager. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 can enroll a maximum of 10 devices in Endpoint Manager. | <input type="radio"/> | <input checked="" type="radio"/> |
| User3 can enroll an unlimited number of devices in Endpoint Manager. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 95

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant.

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

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

The company currently uses the following Office file types:

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

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

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

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

Answer Area

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

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

Office file types that support the sensitivity labels:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 100

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

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

How do you want the alert to be triggered?

- Every time an activity matches the rule
- When the volume of matched activities reaches a threshold
 - More than or equal to activities
 - During the last minutes
 - On
- When the volume of matched activities becomes unusual
 - On

You need to identify the following:

- > How many days it will take to establish a baseline for unusual activity.
- > Whether alerts will be triggered during the establishment of the baseline.

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

NOTE: Each correct selection is worth one point.

How many days it will take to establish the baseline:

Whether the alerts will be triggered during the establishment of the baseline:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

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

NEW QUESTION 103

- (Exam Topic 5)

Your company has a Microsoft 365 E5 tenant that contains a user named User1. You review the company's compliance score.

You need to assign the following improvement action to User1:Enable self-service password reset. What should you do first?

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

Answer: D

Explanation:

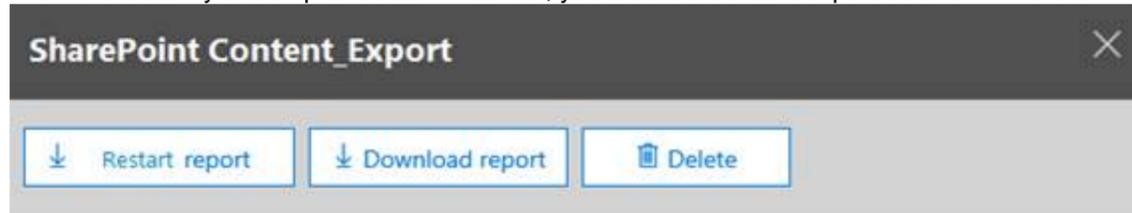
Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o>
<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-p>

NEW QUESTION 107

- (Exam Topic 5)

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



Status:

The export has completed. You can start downloading the results.

Items included from the search:

All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:

One PST file for each mailbox.

De-duplication for Exchange content:

Not enabled.

SharePoint document versions:

Included

Export files in a compressed (zipped) folder:

Yes

The export data was prepared within region:

Default region

Close

Feedback

What will be excluded from the export?

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

Answer: B

Explanation:

Unrecognized file formats are excluded from the search.

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o3> <https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report>

NEW QUESTION 109

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft 365 compliance policies to meet the following requirements:

- > Identify documents that are stored in Microsoft Teams and SharePoint Online that contain Personally Identifiable Information (PII).
- > Report on shared documents that contain PII. What should you create?

- A. an alert policy
- B. a data loss prevention (DLP) policy

- C. a retention policy
- D. a Microsoft Cloud App Security policy

Answer: B

Explanation:

Reference:

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

NEW QUESTION 112

- (Exam Topic 5)

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

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

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

What should you use?

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

Answer: D

Explanation:

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

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

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

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

Pass-through authentication

Active Directory Federation Services Reference:

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

NEW QUESTION 115

- (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 | Prvi | 04/24/2020 |
| - Label2 | 1 | Prvi | 04/24/2020 |
| Label3 | 0-highest | Prvi | 04/24/2020 |
| Label4 | 0-highest | Prvi | 04/24/2020 |
| - Label5 | 5 | Prvi | 04/24/2020 |
| Label6 | 0-highest | Prvi | 04/24/2020 |

Which labels can users apply to content?

- A. Label1, 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 116

- (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 117

- (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 User3 to modify the Defender for identity sensor configuration. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 120

- (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 124

- (Exam Topic 5)

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

User1 exceeds the default daily limit of allowed email messages and is on the Restricted entities list. You need to remove User1 from the Restricted entities list. What should you use?

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

Answer: D

Explanation:

Admins can remove user accounts from the Restricted entities page in the Microsoft 365 Defender portal or in Exchange Online PowerShell.

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal

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

> Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/removing-user-from-restricted-user>

NEW QUESTION 125

- (Exam Topic 5)

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

| Name | Member of |
|-------|----------------|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group1, Group2 |

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

The screenshot shows the 'Configure' page for Microsoft Intune. It includes sections for MDM (Mobile Device Management) and MAM (Mobile Application Management) settings. The MDM section has 'MDM user scope' set to 'Some' and 'Groups' set to 'Group1'. The MAM section has 'MAM User scope' set to 'Some' and 'Groups' set to 'Group2'. There are also fields for MDM terms of use URL, MDM discovery URL, MDM compliance URL, MAM Terms of use URL, MAM Discovery URL, and MAM Compliance URL.

You purchase a Windows 10 device named Device1.

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

NOTE: Each correct selection is worth one point.

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| If User1 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically. | <input type="radio"/> | <input type="radio"/> |
| If User2 joins Device1 to contoso.com, Device1 is enrolled in Intune automatically. | <input type="radio"/> | <input type="radio"/> |
| If User3 registers Device1 in contoso.com, Device1 is enrolled in Intune automatically. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 130

- (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 134

- (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 137

- (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-work> <https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-score-calculation?view=o365-worldwid>

NEW QUESTION 141

- (Exam Topic 5)

You have a Microsoft 365 tenant.

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

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

Answer: D

NEW QUESTION 145

- (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 148

- (Exam Topic 5)

HOTSPOT

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

| Name | Role |
|-------|---------------------------------|
| User1 | Global Administrator |
| User2 | Service Support Administrator |
| User3 | Cloud Application Administrator |
| User4 | None |

You plan to provide User4 with early access to Microsoft 365 feature and service updates.

You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:

▼

Office installation options

Privileged access

Release preferences

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:

▼

Office installation options

Privileged access

Release preferences

User:

▼

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

NEW QUESTION 150

- (Exam Topic 5)

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

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

You plan to enable VPN access for the devices.

What is the minimum number of configuration policies required?

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

Answer: D

NEW QUESTION 154

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Purview policies to meet the following requirements:

Identify documents that are stored in Microsoft Teams and SharePoint that contain Personally Identifiable Information (PII).

Report on shared documents that contain PII. What should you create?

- A. a data loss prevention (DLP) policy
- B. a retention policy
- C. an alert policy
- D. a Microsoft Defender for Cloud Apps policy

Answer: A

Explanation:

Demonstrate data protection

Protection of personal information in Microsoft 365 includes using data loss prevention (DLP) capabilities. With DLP policies, you can automatically protect sensitive information across Microsoft 365.

There are multiple ways you can apply the protection. Educating and raising awareness to where EU resident data is stored in your environment and how your employees are permitted to handle it represents one level of information protection using Office 365 DLP.

In this phase, you create a new DLP policy and demonstrate how it gets applied to the IBANs.docx file you stored in SharePoint Online in Phase 2 and when you attempt to send an email containing IBANs.

- > From the Security & Compliance tab of your browser, click Home.
- > Click Data loss prevention > Policy.
- > Click + Create a policy.
- > In Start with a template or create a custom policy, click Custom > Custom policy > Next.
- > In Name your policy, provide the following details and then click Next: a. Name: EU Citizen PII Policy
- b. Description: Protect the personally identifiable information of European citizens
- > Etc. Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-discovery-protection-reporting-in-office365-dev-t>

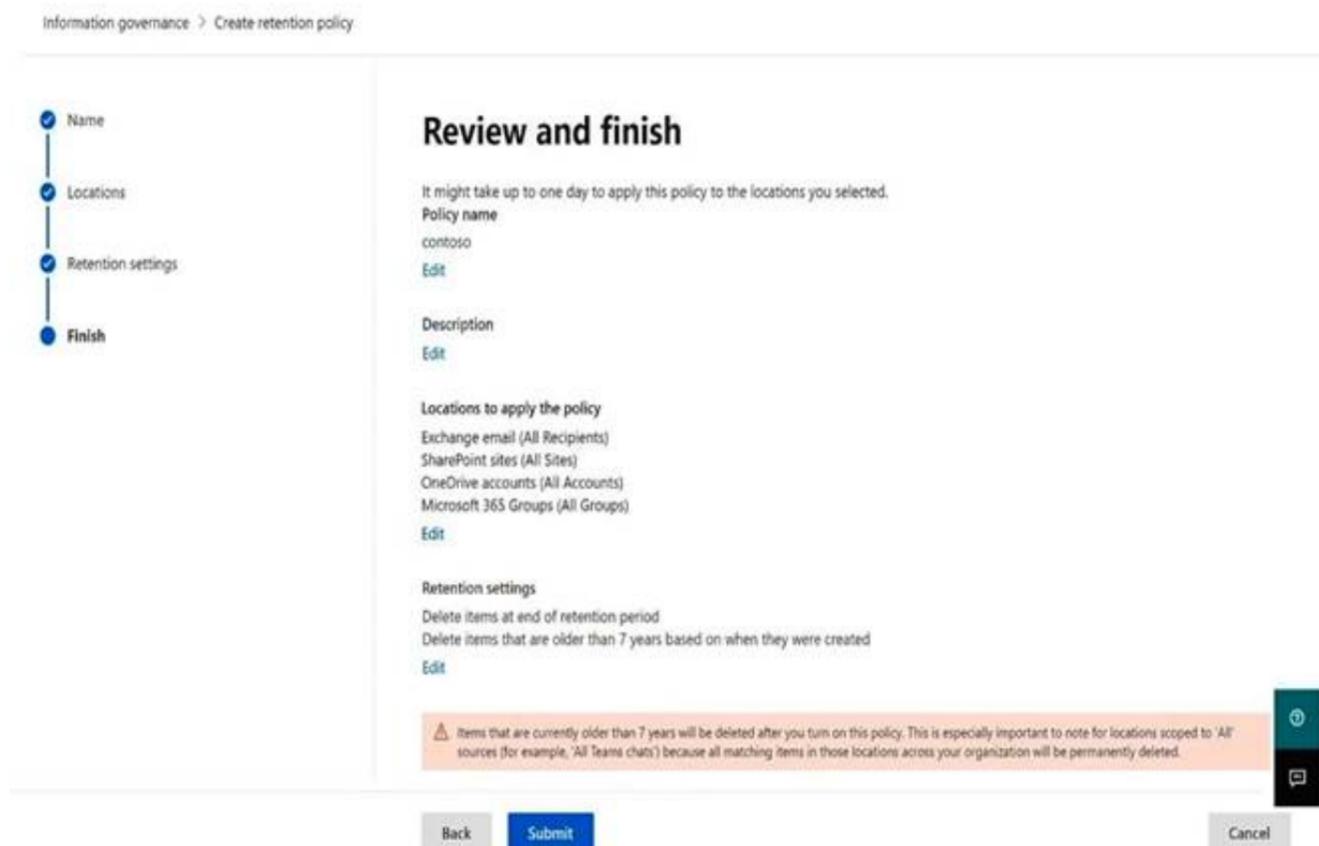
NEW QUESTION 157

- (Exam Topic 5)

HOTSPOT

You have a Microsoft 365 tenant.

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



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

NOTE: Each correct selection is worth one point.

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 159

- (Exam Topic 5)

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

| Name | Mailbox size |
|-------|--------------|
| User1 | 5 MB |
| User2 | 15 MB |
| User3 | 25 MB |
| User4 | 55 MB |

You have a Microsoft Office 365 retention label named Retention1 that is published to Exchange email.

You have a Microsoft Exchange Online retention policy that is applied to all mailboxes. The retention policy contains a retention tag named Retention2.

Which users can assign Retention1 and Retention2 to their emails? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can assign Retention1:

User4 only
 User3 and User4 only
 User2, User3, and User4 only
 User1, User2, User3, and User4

Users who can assign Retention2:

User4 only
 User3 and User4 only
 User2, User3, and User4 only
 User1, User2, User3, and User4

- 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/microsoft-365/compliance/retention-policies-exchange?view=o365-worldwide>

NEW QUESTION 164

- (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 169

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You plan to implement Microsoft Purview Privileged Access Management. Which Microsoft Office 365 workloads support privileged access?

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

Answer: A

Explanation:

Privileged access management

Having standing access by some users to sensitive information or critical network configuration settings in Microsoft Exchange Online is a potential pathway for compromised accounts or internal threat activities. Microsoft Purview Privileged Access Management helps protect your organization from breaches and helps to meet compliance best practices by limiting standing access to sensitive data or access to critical configuration settings. Instead of administrators having constant access, just-in-time access rules are implemented for tasks that need elevated permissions. Enabling privileged access management for Exchange Online in Microsoft 365 allows your organization to operate with zero standing privileges and provide a layer of defense against standing administrative access vulnerabilities.

Note: When will privileged access support Office 365 workloads beyond Exchange? Privileged access management will be available in other Office 365 workloads soon. Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-solution-overview> <https://learn.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management>

NEW QUESTION 174

- (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 179

- (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 182

- (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 185

- (Exam Topic 5)

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

```

Select Administrator Windows PowerShell
Name           : Retention1
Priority        : 200
RecordTypes    : {MicrosoftTeams}
Operations     : {}
UserIds        : {}
RetentionDuration : ThreeMonths

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

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

PS C:\>
    
```

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

Answer Area

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

- not retained
- retained for 90 days
- retained for six months
- retained for one year

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

- not retained
- retained for 90 days
- retained for six months
- retained for one year

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

- not retained
- retained for 90 days
- retained for six months
- retained for one year

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

- not retained
- retained for 90 days
- retained for six months
- retained for one year

NEW QUESTION 188

- (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 193

- (Exam Topic 5)
 You have a Microsoft 365 E5 tenant.
 You need to create a policy that will trigger an alert when unusual Microsoft Office 365 usage patterns are detected.
 What should you use to create the policy?

- A. the Microsoft 365 admin center
- B. the Microsoft Purview compliance portal
- C. the Microsoft Defender for Cloud Apps portal
- D. the Microsoft Apps admin center

Answer: C

NEW QUESTION 196

- (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 198

- (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 203

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

| Name | Platform |
|---------|------------|
| Device1 | Windows 11 |
| Device2 | Windows 10 |
| Device3 | Android |
| Device4 | iOS |

All the devices are onboarded To Microsoft Defender for Endpoint
 You plan to use Microsoft Defender Vulnerability Management to meet the following requirements:

- Detect operating system vulnerabilities.

Answer Area

Detect operating system vulnerabilities

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

Perform a configuration assessment of the operating system

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Detect operating system vulnerabilities

- Device1 only
- Device1 and Device2 only
- Device1, Device2, and Device3 only**
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

Perform a configuration assessment of the operating system

- Device1 only
- Device1 and Device2 only**
- Device1, Device2, and Device3 only
- Device1, Device2, and Device4 only
- Device1, Device2, Device3 and Device4

NEW QUESTION 204

- (Exam Topic 5)

You have a Microsoft 365 tenant.

You plan to implement Endpoint Protection device configuration profiles. Which platform can you manage by using the profile?

- A. Android
- B. CentOS Linux
- C. iOS
- D. Window 10

Answer: D

Explanation:

Reference:

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

NEW QUESTION 207

- (Exam Topic 5)

HOTSPOT

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

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

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

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

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

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

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

Answer Area

| Statements | Yes | No |
|---|-------------------------------------|--------------------------|
| If a high-severity incident is triggered for Device1, an incident email notification will be sent. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| If a low-severity incident is triggered for Computer1, an incident notification email will be sent. | <input type="checkbox"/> | <input type="checkbox"/> |
| If a low-severity incident is triggered for Device3, an incident notification email will be sent. | <input type="checkbox"/> | <input type="checkbox"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

Device1 is in Group2 as Name starts with Device and Tag contains Inventory. However, the Group2 has alert severity low.

Box 2: No

Computer1 does not belong to either Group1 or Group2 Box 3: Yes

Device3 belongs to both Group1 and Group2. Note: Understanding alert severity

Microsoft Defender Antivirus and Defender for Endpoint alert severities are different because they represent different scopes.

The Microsoft Defender Antivirus threat severity represents the absolute severity of the detected threat (malware), and is assigned based on the potential risk to the individual device, if infected.

Reference: <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/alerts-queue>

NEW QUESTION 209

- (Exam Topic 5)

Your company has offices in five cities. The company has a Microsoft 365 tenant.

Each office is managed by a local administrator. You plan to deploy Microsoft Intune.

You need to recommend a solution to manage resources in Intune that meets the following requirements: > Local administrators must be able to manage only the resources in their respective office.

- > Local administrators must be prevented from managing resources in other offices.
- > Administrative effort must be minimized.

What should you include in the recommendation?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 210

- (Exam Topic 5)

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

You need to be notified when a single user downloads more than 50 files during any 60-second period. What should you configure?

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

Answer: D

NEW QUESTION 211

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.

Which two policies can you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a data loss prevention (DLP) policy
- B. a sensitivity label policy
- C. a Microsoft Cloud App Security file policy
- D. a communication compliance policy
- E. a retention label policy

Answer: AD

NEW QUESTION 213

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site. You modify the sharePoint sharing policy to prevent sharing, outside your organization.

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

Solution: From the Security & Compliance admin center you create a threat management policy. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 215

- (Exam Topic 5)

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

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

Azure AD Connect has the following settings:

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

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 218

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription that includes the following active eDiscovery case:

- > Name: Case1
- > Included content: Group1, User1, Site1
- > Hold location: Exchange mailboxes, SharePoint sites, Exchange public folders The investigation for Case1 completes, and you close the case.

What occurs after you close Case1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Holds are turned off for:

Holds are placed on a delay hold for:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/close-or-delete-case?view=o365-worldwide>

NEW QUESTION 219

- (Exam Topic 5)

DRAG DROP

Your network contains an on-premises Active Directory domain that syncs to Azure Active Directory (Azure AD). The domain contains the servers shown in the following table.

| Name | Operating system | Configuration |
|---------|---------------------|-------------------------------------|
| Server1 | Windows Server 2016 | File Server Resource Manager (FSRM) |
| Server2 | Windows Server 2016 | None |

You use Azure Information Protection.

You need to ensure that you can apply Azure Information Protection labels to the file stores on Server1. Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

- Authorize Server1.
- Install the Microsoft Rights Management connector on Server2.
- Install a certificate on Server2.
- Install a certificate on Server1.
- Register a service principal name for Server1.
- Run GenConnectorConfig.ps1 on Server1.
- Run GenConnectorConfig.ps1 on Server2.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/install-configure-rms-connector> <https://docs.microsoft.com/en-us/azure/information-protection/configure-servers-rms-connector>

NEW QUESTION 223

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You view the Service Health Overview as shown in the following exhibit.

Service health October 18, 2022 4:20 PM

[Overview](#) | [Issue history](#) | [Reported issues](#)

View the issues and health status of all services that are available with your current subscriptions. [Learn more about Service Health](#)

Report an issue
Customize
☰

Active issues

| Issue title | Affected service | Issue type |
|--|------------------|------------|
| > Microsoft service health (6) | | |
| Issues in your environment that require action (0) | | |

Microsoft service health

Shows the current health status of your Microsoft services, and updates when we fix issues.

| Service | Status |
|-----------------------|--------------|
| Exchange Online | 3 advisories |
| Microsoft 365 suite | 2 advisories |
| Microsoft Teams | 1 advisory |
| OneDrive for Business | 1 advisory |
| SharePoint Online | 2 advisories |

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

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

Answer: C

Explanation:

Service Support admin

Assign the Service Support admin role as an additional role to admins or users who need to do the following in addition to their usual admin role:

- Open and manage service requests
- View and share message center posts
- Monitor service health Incorrect:

* Message center reader

Assign the Message center reader role to users who need to do the following:

- Monitor message center notifications
- Get weekly email digests of message center posts and updates
- Share message center posts
- Have read-only access to Azure AD services, such as users and groups

* Reports reader

Assign the Reports reader role to users who need to do the following:

- View usage data and the activity reports in the Microsoft 365 admin center
- Get access to the Power BI adoption content pack
- Get access to sign-in reports and activity in Azure AD
- View data returned by Microsoft Graph reporting API Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide>

NEW QUESTION 224

- (Exam Topic 5)

You have a Microsoft E5 subscription.

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 225

- (Exam Topic 5)

You have a Microsoft 365 subscription.

You configure a new Azure AD enterprise application named App1. App1 requires that a user be assigned the Reports Reader role.

Which type of group should you use to assign the Reports Reader role and to access App1?

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

Answer: C

Explanation:

To grant permissions to assignees to manage users and group access for a specific enterprise app, go to that app in Azure AD and open in the Roles and Administrators list for that app. Select the new custom role and complete the user or group assignment. The assignees can manage users and group access only for the specific app.

Note: You can add the following types of groups:

Assigned groups - Manually add users or devices into a static group.

Dynamic groups (Requires Azure AD Premium) - Automatically add users or devices to user groups or device groups based on an expression you create.

Note:

Security groups

Security groups are used for granting access to Microsoft 365 resources, such as SharePoint. They can make administration easier because you need only administer the group rather than adding users to each resource individually.

Security groups can contain users or devices. Creating a security group for devices can be used with mobile device management services, such as Intune.

Security groups can be configured for dynamic membership in Azure Active Directory, allowing group members or devices to be added or removed automatically based on user attributes such as department, location, or title; or device attributes such as operating system version.

Security groups can be added to a team.

Microsoft 365 Groups can't be members of security groups. Microsoft 365 Groups

Microsoft 365 Groups are used for collaboration between users, both inside and outside your company. With each Microsoft 365 Group, members get a group email and shared workspace for conversations, files, and calendar events, Stream, and a Planner.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/custom-enterprise-apps> <https://learn.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?> <https://learn.microsoft.com/en-us/mem/intune/apps/apps-deploy>

NEW QUESTION 229

- (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 Device Manager, you view the computer properties. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 234

- (Exam Topic 5)

HOTSPOT

Your network contains an on-premises Active Directory forest named contoso.com. The forest contains the following domains:

- > Contoso.com
- > East.contoso.com

The forest contains the users shown in the following table.

| Name | UPN suffix |
|-------|------------------|
| User1 | Contoso.com |
| User2 | East.contoso.com |
| User3 | Fabrikam.com |

The forest 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 | Disabled |

USER SIGN-IN



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

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 authenticate to Azure AD by using a username of user1@contoso.com. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| User2 can authenticate to Azure AD by using a username of user2@contoso.com. | <input type="checkbox"/> | <input type="checkbox"/> |
| User3 can authenticate to Azure AD by using a username of user3@contoso.com. | <input type="checkbox"/> | <input type="checkbox"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.

Box 2: No

The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.

Box 3: No

The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

NEW QUESTION 239

- (Exam Topic 5)

You have a Microsoft 365 E5 subscription.

You plan to implement records management and enable users to designate documents as regulatory records. You need to ensure that the option to mark content as a regulatory record is visible when you create retention labels.

What should you do first?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 241

- (Exam Topic 5)

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

You need to ensure that only devices marked as compliant can access Microsoft Office 365 apps. Which policy type should you configure?

- A. conditional access
- B. account protection
- C. attack surface reduction (ASR)
- D. Endpoint detection and response

Answer: A

Explanation:

Reference:

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

NEW QUESTION 242

- (Exam Topic 5)

You have an Azure AD tenant and a Microsoft 365 E5 subscription. The tenant contains the users shown in the following table.

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

You plan to implement Microsoft Defender for Endpoint.

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

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

Answer: A

NEW QUESTION 244

- (Exam Topic 5)

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

| Name | Severity | Status | Comment | Category |
|--------|----------|----------|----------|-------------------|
| Alert1 | Medium | Active | Comment1 | Threat management |
| Alert2 | Low | Resolved | Comment2 | Other |

Which properties of the alerts can you modify?

- A. Status only
- B. Status and Comment only
- C. Status and Severity only
- D. Status, Severity, and Comment only
- E. Status, Severity, Comment and Category

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/update-alert?view=o365-worldwide#>

NEW QUESTION 249

- (Exam Topic 5)

HOTSPOT

Your company uses a legacy on-premises LDAP directory that contains 100 users. The company purchases a Microsoft 365 subscription. You need to import the 100 users into Microsoft 365 by using the Microsoft 365 admin center.

Which type of file should you use and which properties are required? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File type to use:

- CSV
- JSON
- PST
- XML

Required properties for each user:

- Display Name and Department
- First Name and Last Name
- User Name and Department
- User Name and Display Name

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: CSV

Add multiple users in the Microsoft 365 admin center

- > Sign in to Microsoft 365 with your work or school account.
- > In the admin center, choose Users > Active users.
- > Select Add multiple users.
- > On the Import multiple users panel, you can optionally download a sample CSV file with or without sample data filled in.
- > Etc.

Note: More information about how to add users to Microsoft 365 Not sure what CSV format is?

A CSV file is a file with comma separated values. You can create or edit a file like this with any text editor or spreadsheet program, such as Excel.

Box 2: User Name and Display Name

What if I don't have all the information required for each user? The user name and display name are required, and you cannot add a new user without this information. If you don't have some of the other information, such as the fax, you can use a space plus a comma to indicate that the field should remain blank.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/add-several-users-at-the-same-time>

NEW QUESTION 252

- (Exam Topic 5)

You have a Microsoft 365 E5 tenant.

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

Which policy should you use?

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 257

- (Exam Topic 5)

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

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

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

Answer: C

NEW QUESTION 260

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

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