

Exam Questions MS-102

Microsoft 365 Administrator Exam

<https://www.2passeasy.com/dumps/MS-102/>



NEW QUESTION 1

- (Topic 6)

You have a Microsoft 365 tenant that uses Microsoft Endpoint Manager for device management. You need to add the phone number of the help desk to the Company Portal app. What should you do?

- A. From Customization in the Microsoft Endpoint Manager admin center, modify the support information for the tenant.
- B. From the Microsoft Endpoint Manager admin center, create an app configuration policy.
- C. From the Microsoft 365 admin center, modify Organization information.
- D. From the Microsoft 365 admin center, modify Help desk information.

Answer: A

Explanation:

Reference:

<https://systemcenterdudes.com/intune-company-portal-customization/>

NEW QUESTION 2

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant

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

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

NOTE: Each correct selection is worth one point.

Choose locations to apply the policy

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

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

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	Exchange email	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	SharePoint sites	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Off	OneDrive accounts	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Teams chat and channel messages	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Devices	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Microsoft Cloud App Security	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	On-premises repositories	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Choose locations to apply the policy

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

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

Status	Location	Included	Excluded
<input checked="" type="checkbox"/> Off	Exchange email	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Off	SharePoint sites	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Off	OneDrive accounts	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Off	Teams chat and channel messages	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Devices	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	Microsoft Cloud App Security	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> Off	On-premises repositories	<input type="checkbox"/>	<input type="checkbox"/>

NEW QUESTION 3

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory domain. The domain contains the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2022	Domain controller
Server2	Windows Server 2016	Member server
Server3	Server Core installation of Windows Server 2022	Member server

You purchase a Microsoft 365 E5 subscription.

You need to implement Azure AD Connect cloud sync.

What should you install first and on which server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Install:

Server:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: The Azure AD Connect provisioning agent Install the Azure AD Connect provisioning agent

How is Azure AD Connect cloud sync different from Azure AD Connect sync?

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their

on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

* An on-premises server for the provisioning agent with Windows 2016 or later.

This server should be a tier 0 server based on the Active Directory administrative tier model. Installing the agent on a domain controller is supported.

Note: Windows Server Core is a minimal installation option for the Windows Server operating system (OS) that has no GUI and only includes the components required to perform server roles and run applications.

NEW QUESTION 4

- (Topic 6)

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-users-portal-after-spam>

NEW QUESTION 5

- (Topic 6)

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

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

You have a Microsoft 365 E5 subscription that contains a user named User1. You need to enable User1 to create Compliance Manager assessments.

Solution: From the Microsoft 365 compliance center, you add User1 to the Compliance Manager Assessors role group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center.md>

NEW QUESTION 6

- (Topic 6)

Your company has 10,000 users who access all applications from an on-premises data center.

You plan to create a Microsoft 365 subscription and to migrate data to the cloud. You plan to implement directory synchronization.

User accounts and group accounts must sync to Azure AD successfully. You discover that several user accounts fail to sync to Azure AD.

You need to resolve the issue as quickly as possible. What should you do?

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

Answer: B

Explanation:

IdFix is used to perform discovery and remediation of identity objects and their attributes in an on-premises Active Directory environment in preparation for migration to Azure Active Directory. IdFix is intended for the Active Directory administrators responsible for directory synchronization with Azure Active Directory.

Reference:

<https://docs.microsoft.com/en-us/office365/enterprise/prepare-directory-attributes-for-synch-with-idfix>

NEW QUESTION 7

- (Topic 6)

You have a Microsoft 365 tenant.

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

What should you use?

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

Answer: D

Explanation:

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

NEW QUESTION 8

- (Topic 6)

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-authentication>

NEW QUESTION 9

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to configure a group naming policy.

Which portal should you use, and to which types of groups will the policy apply? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Portal:

Group types:

Group types:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal:

Group types:

Group types:

NEW QUESTION 10

- (Topic 6)

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

Name	Configuration
Group1	Global security group
User1	Enabled user account
User2	Disabled user account

You configure Azure AD Connect to sync contoso.com to Azure AD.
 Which objects will sync to Azure AD?

- A. Group1 only
- B. User1 and User2 only
- C. Group1 and User1 only
- D. Group1, User1, and User2

Answer: D

Explanation:

Disabled accounts

Disabled accounts are synchronized as well to Azure AD. Disabled accounts are common to represent resources in Exchange, for example conference rooms. The exception is users with a linked mailbox; as previously mentioned, these will never provision an account to Azure AD.

The assumption is that if a disabled user account is found, then we won't find another active account later and the object is provisioned to Azure AD with the userPrincipalName and sourceAnchor found. In case another active account will join to the same metaverse object, then its userPrincipalName and sourceAnchor will be used.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/connect/concept-azure-ad-connect-sync-user-and-contacts>

NEW QUESTION 10

- (Topic 6)

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 14

- (Topic 6)

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

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

What should you do on the computer?

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

Answer: B

NEW QUESTION 16

- (Topic 6)

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 21

HOTSPOT - (Topic 6)

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 and MAM terms of use, discovery, and compliance URLs.

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:

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

NEW QUESTION 26

HOTSPOT - (Topic 6)

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

Name	Role
User1	Global Administrator
User2	Security Administrator, Guest Inviter
User3	None
User4	Password Administrator

External collaboration settings have default configuration.

You need to identify which users can perform the following administrative tasks:

- Modify the password protection policy.
- Create guest user accounts.

Which users should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Modify the password protection policy:

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

Create new guest users in Azure AD:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Modify the password protection policy:

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

Create new guest users in Azure AD:

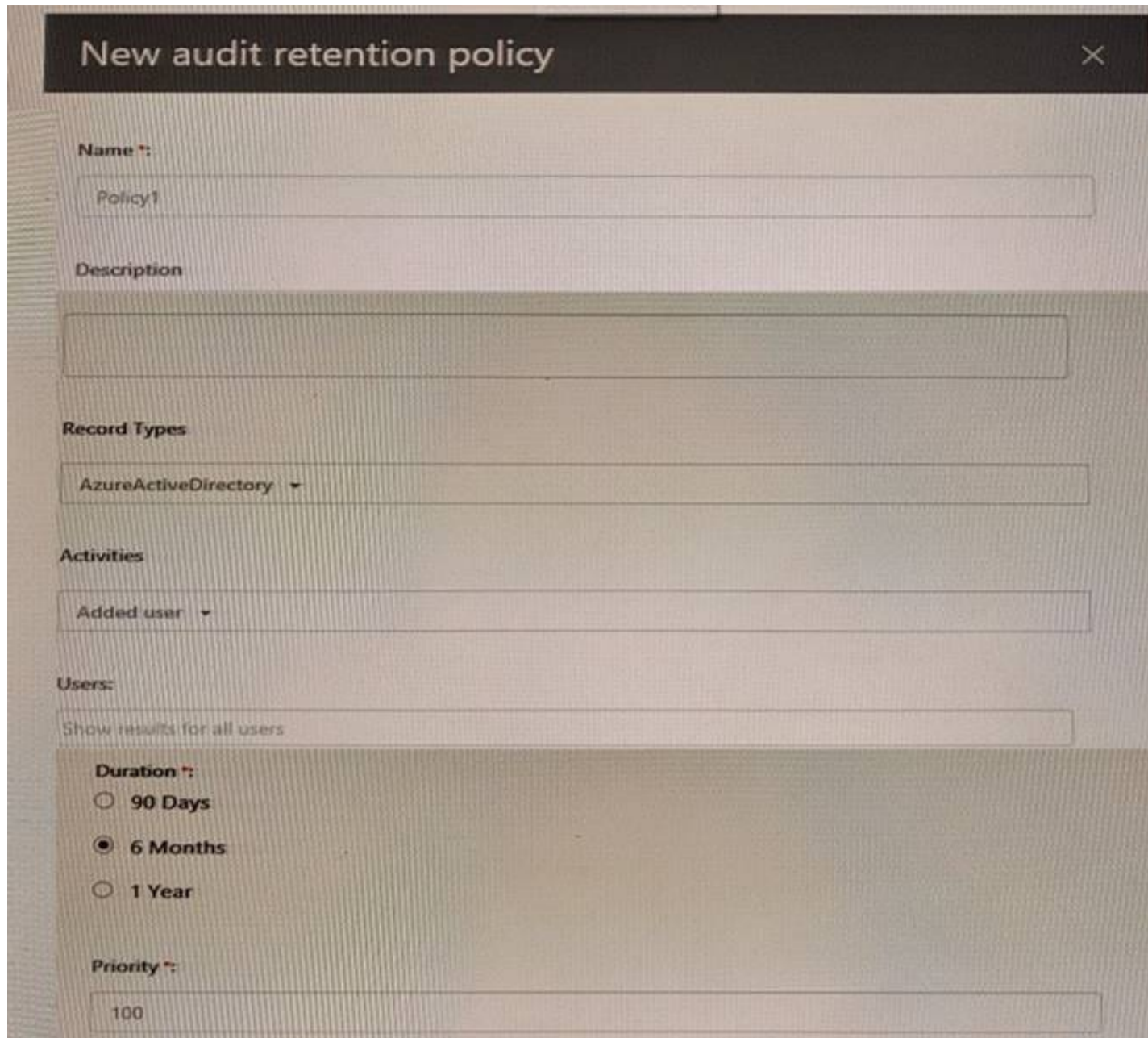
- User1 only
- User1 and User2 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

NEW QUESTION 31

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that has auditing turned on. The subscription contains the users shown in the following table.

Name	License
Admin1	Microsoft Office 365 E5
Admin2	None



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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:



NEW QUESTION 36

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint. You plan to perform device discovery and authenticated scans of network devices. You install and register the network scanner on a device named Device1.
 What should you do next?

- A. Connect Defender for Endpoint to Microsoft Intune.
- B. Apply for Microsoft Threat Experts - Targeted Attack Notifications.
- C. Create an assessment job.
- D. Download and run an onboarding package.

Answer: C

NEW QUESTION 41

HOTSPOT - (Topic 6)

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

Name	Member of	Passwordless capable	Multi-factor authentication (MFA) method registered
User1	Group1	Capable	Microsoft Authenticator app (push notification)
User2	Group2	Capable	Microsoft Authenticator app (push notification)
User3	Group1, Group2	Capable	Mobile phone, Windows Hello for Business

Each user has a device with the Microsoft Authenticator app installed.

From Microsoft Authenticator settings for the subscription, the Enable and Target settings are configured as shown in the exhibit. (Click the Exhibit tab.)

Microsoft Authenticator settings

Number Matching will begin to be enabled for all users of the Microsoft Authenticator app starting 27th of February 2023. [Learn more](#)

The Microsoft Authenticator app is a flagship authentication method, usable in passwordless or simple push notification approval modes. The app is free to download and use on Android/iOS mobile devices. [Learn more](#).

Enable and Target Configure

Enable

Include Exclude

Target All users Select groups

[Add groups](#)

Name	Type	Registration	Authentication mode
Group1	Group	Optional	Passwordless

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 use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

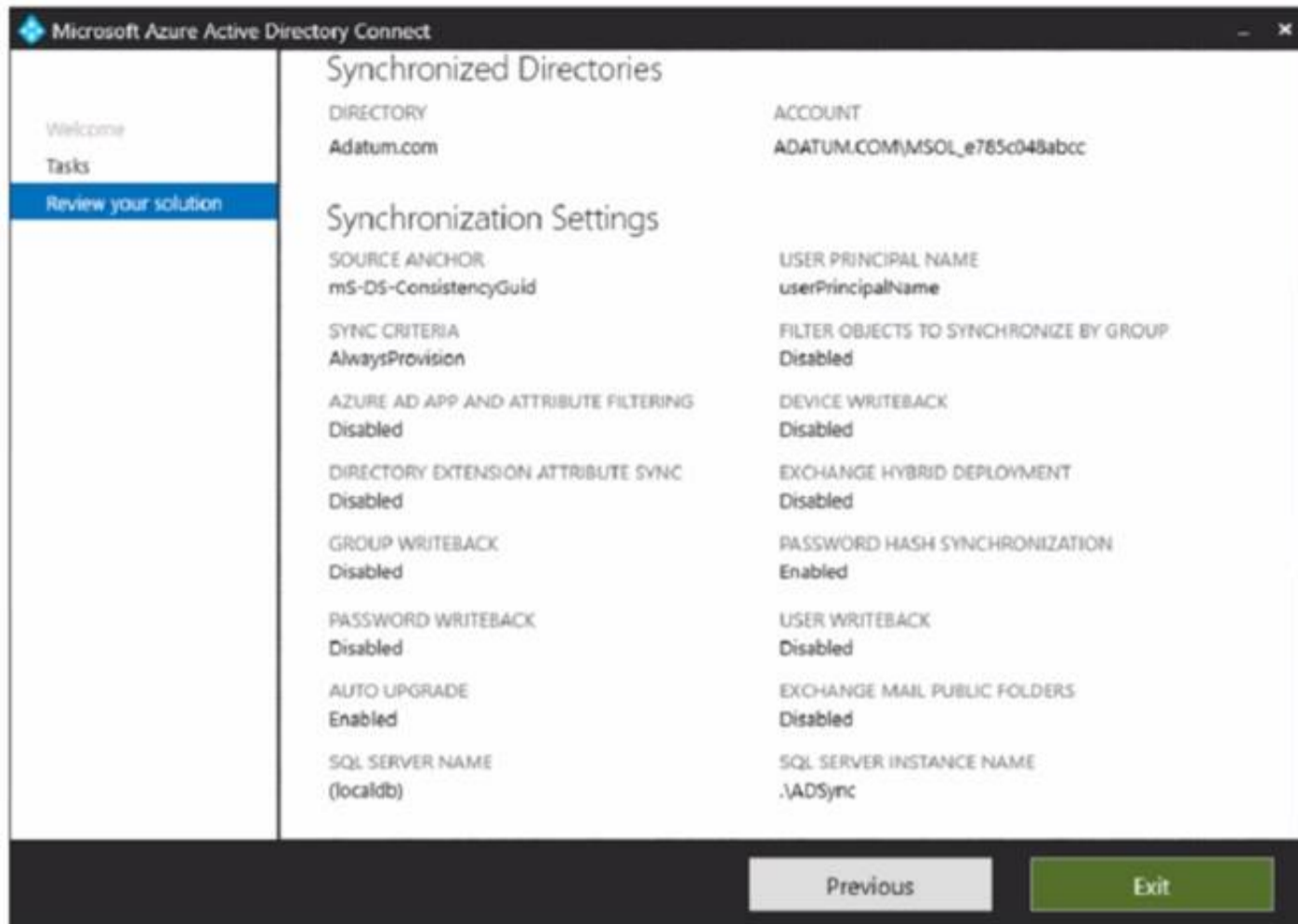
Answer Area

Statements	Yes	No
User1 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can use number matching during sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 44

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain that is synced to Azure AD as shown in the following exhibit.



An on-premises Active Directory user account named Allan Yoo is synchronized to Azure AD. You view Allan's account from Microsoft 365 and notice that his username is set to Allan @>ddatum.onmicrosoft.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
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Azure portal, you can reset the password of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 49

- (Topic 6)

Your network contains three Active Directory forests. There are forests trust relationships between the forests.

You create an Azure AD tenant.

You plan to sync the on-premises Active Directory to Azure AD.

You need to recommend a synchronization solution. The solution must ensure that the synchronization can complete successfully and as quickly as possible if a single server fails.

What should you include in the recommendation?

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

Answer: A

Explanation:

Azure AD Connect can be active on only one server. You can install Azure AD Connect on another server for redundancy but the additional installation would need to be in Staging mode. An Azure AD connect installation in Staging mode is configured and ready to go but it needs to be manually switched to Active to perform directory synchronization.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom>

NEW QUESTION 51

HOTSPOT - (Topic 6)

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 type="radio"/>	<input type="radio"/>
Excel is installed on Device1.	<input type="radio"/>	<input type="radio"/>

NEW QUESTION 53

- (Topic 6)

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

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

The devices are managed by using Microsoft Intune.

You plan to use a configuration profile to assign the Delivery Optimization settings. Which devices will support the settings?

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

Answer: A

NEW QUESTION 56

HOTSPOT - (Topic 6)

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

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

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

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

The policies use the settings shown in the following table.

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 60

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains two users named User1 and User2 and the groups shown in the following table.

Name	Members
Group1	User1
Group2	User2, Group1

You have a Microsoft Intune enrollment policy that has the following settings:

? MDM user scope: Some

? uk.co.certification.simulator.questionpool.PList@184e72e0

? MAM user scope: Some

? uk.co.certification.simulator.questionpool.PList@184e7360 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can enroll Device1 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User1 can enroll Device2 in Intune by using automatic enrollment	<input checked="" type="radio"/>	<input type="radio"/>
User2 can enroll Device2 in Intune by using automatic enrollment	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 64

- (Topic 6)

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

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

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

User2 fails to authenticate to Azure AD when signing in as user2@fabrikam.com. You need to ensure that User2 can access the resources in Azure AD. Solution: From the Microsoft Entra admin center, you add fabrikam.com as a custom domain. You instruct User2 to sign in as user2@fabrikam.com. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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

NEW QUESTION 67

FILL IN THE BLANK - (Topic 6)

You have a Microsoft 365 subscription.

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

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

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

Does this meet the goal?

A Yes

A. No

Answer: A

NEW QUESTION 68

HOTSPOT - (Topic 6)

HOTSPOT

Assessment	Score	Progress	actions	Group	Standard
SP800	15444	Incomplete 72%	3 of 450 completed	Group1	Microsoft 365 NIST 800-53
Data Protection Baseline	14370	Incomplete 70%	3 of 489 completed	Group2	Microsoft 365 Data Protection Baseline

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

Answer Area

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:
 Answer Area

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

NEW QUESTION 72

- (Topic 6)

You enable the Azure AD Identity Protection weekly digest email. You create the users shown in the following table.

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

Which users will receive the weekly digest email automatically?

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

Answer: E

Explanation:

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

NEW QUESTION 74

HOTSPOT - (Topic 6)

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

Name	Azure Active Directory (Azure AD) role	Microsoft Store for Business role	Member of
User1	Application administrator	Basic Purchaser	Group1
User2	None	Purchaser	Group2
User3	None	Basic Purchaser	Group3

You perform the following actions:

- ? Provision the private store in Microsoft Store for Business.
 - ? Add an app named App1 to the private store.
 - ? Set Private store availability for App1 to Specific groups, and then select Group3.
- For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User2 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>
User3 can install App1 from the private store.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements

Yes No

User1 can install App1 from the private store.

User2 can install App1 from the private store.

User3 can install App1 from the private store.

NEW QUESTION 78

DRAG DROP - (Topic 6)

You have an Azure subscription that is linked to a hybrid Microsoft Entra tenant.

All users sync from Active Directory Domain Services (AD DS) to the tenant by using Express Settings in Microsoft Entra Connect.

You plan to implement self-service password reset (SSPR).

You need to ensure that when a user resets or changes a password, the password syncs with AD DS.

Which actions should you perform in sequence? To answer, drag the appropriate actions to the correct order. Each action 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.

Actions	Answer Area
From the Microsoft Entra admin center, configure on-premises integration password writeback.	Step 1: Validate permissions for the Microsoft Entra Connect account.
From the Microsoft Entra admin center, configure the authentication methods for SSPR.	Step 2: <input type="text"/>
From the Microsoft Entra admin center, configure the registration settings for SSPR.	Step 3: <input type="text"/>
Select Group writeback in Microsoft Entra Connect.	
Select Password writeback in Microsoft Entra Connect.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions	Answer Area
From the Microsoft Entra admin center, configure on-premises integration password writeback.	Step 1: Validate permissions for the Microsoft Entra Connect account.
From the Microsoft Entra admin center, configure the authentication methods for SSPR.	Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.
From the Microsoft Entra admin center, configure the registration settings for SSPR.	Step 3: Select Password writeback in Microsoft Entra Connect.
Select Group writeback in Microsoft Entra Connect.	
Select Password writeback in Microsoft Entra Connect.	

NEW QUESTION 81

HOTSPOT - (Topic 6)

From the Microsoft Purview compliance portal, you create a retention policy named Policy 1.

You need to prevent all users from disabling the policy or reducing the retention period. How should you configure the Azure PowerShell command? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 86

HOTSPOT - (Topic 6)
 HOTSPOT

You have a Microsoft 365 subscription.

You are planning a threat management solution for your organization.

You need to minimize the likelihood that users will be affected by the following threats:

? Opening files in Microsoft SharePoint that contain malicious content

? Impersonation and spoofing attacks in email messages

Which policies should you create in Microsoft 365 Defender? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

NEW QUESTION 88

HOTSPOT - (Topic 6)

HOTSPOT

Your network contains an on-premises Active Directory domain. You have a Microsoft 365 E5 subscription.

You plan to implement directory synchronization.

You need to identify potential synchronization issues for the domain. The solution must use the principle of least privilege.

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

Answer Area

Tool:

<input type="checkbox"/>	AccessChk
<input type="checkbox"/>	Azure AD Connect
<input type="checkbox"/>	Active Directory Explorer
<input type="checkbox"/>	IdFix

Required group membership:

<input type="checkbox"/>	Domain Admins
<input type="checkbox"/>	Domain Users
<input type="checkbox"/>	Server Operators
<input type="checkbox"/>	Enterprise Admins

- A. Mastered
- B. Not Mastered

Answer: A**Explanation:**

Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft 365. A portion of this effort is intended to address the time involved in remediating the Windows Server Active Directory (Windows Server AD) errors reported by the directory synchronization tools such as Azure AD Connect and Azure AD Connect cloud sync. The focus of IdFix is to enable you to accomplish this task in a simple, expedient fashion.

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Windows Server AD forests in preparation for deployment to Microsoft 365. The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365. Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

The user account that you use to run IdFix must have read and write access to the AD DS domain.

If you aren't sure if your user account meets these requirements, and you're not sure how to check, you can still download and run IdFix. If your user account doesn't have the right permissions, IdFix will simply display an error when you try to run it.

* Enterprise Admins

The Enterprise Admins group exists only in the root domain of an Active Directory forest of domains. The group is a Universal group if the domain is in native mode. The group is a Global group if the domain is in mixed mode. Members of this group are authorized to make forest-wide changes in Active Directory, like adding child domains.

Incorrect:

* Domain Admins

Members of the Domain Admins security group are authorized to administer the domain. By default, the Domain Admins group is a member of the Administrators group on all computers that have joined a domain, including the domain controllers. The Domain Admins group is the default owner of any object that's created in Active Directory for the domain by any member of the group. If members of the group create other objects, such as files, the default owner is the Administrators group.

* Server Operator

Server Operators can log on to a server interactively; create and delete network shares; start and stop services; back up and restore files; format the hard disk of the computer; and shut down the computer. Any service that accesses the system has the Service identity.

* Domain Users - too few permissions

The Domain Users group includes all user accounts in a domain. When you create a user account in a domain, it's automatically added to this group.

NEW QUESTION 89

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a user named User1. Azure AD Password Protection is configured as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ

Lockout duration in seconds ⓘ

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

3hundred
 Eleven
 Falcon
 Project
 Tailspin

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Enforced Audit

User1 attempts to update their password to the following passwords:

- ? F@lcon
- ? Project22
- ? T4il\$pin45dg4

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

[Answer choice] will be accepted as a password.

▼

- Only T4il\$pin45dg4
- Only F@lcon and T4il\$pin45dg4
- Only Project22 and T4il\$pin45dg4
- F@lcon, Project22, and T4il\$pin45dg4

If User1 enters the same wrong password 15 times, waits 11 minutes, and then enters the same wrong password again, the user [answer choice].

▼

- will be locked out
- will trigger a user risk
- can attempt to sign in again immediately

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Only T4il\$pin45dg4

Box 2: can attempt to sign in immediately Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values. Customization of the smart lockout settings, with values specific to your organization, requires Azure AD Premium P1 or higher licenses for your users. Customization of the smart lockout settings is not available for Azure China 21Vianet tenants.

To check or modify the smart lockout values for your organization, complete the following steps:

- ? Sign in to the Entra portal.
- ? Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.
- ? Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.
- ? The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.
- ? Set the Lockout duration in seconds, to the length in seconds of each lockout.
- ? The default is 60 seconds (one minute).

If the first sign-in after a lockout period has expired also fails, the account locks out again. If an account locks repeatedly, the lockout duration increases.

NEW QUESTION 94

- (Topic 6)

You have a Microsoft 365 subscription.

You have an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Security Administrator
User2	Global Administrator
User3	Service Support Administrator

You configure Tenant properties as shown in the following exhibit.

Technical contact

 ✓

Global privacy contact

 ✓

Privacy statement URL

 ✓

Which users will be contacted by Microsoft if the tenant experiences a data breach?

- A. Used only
- B. User2 only
- C. User3 only
- D. Used and User2 only
- E. User2 and User3 only

Answer: B

Explanation:

Microsoft 365 is committed to notifying customers within 72 hours of breach declaration. The customer's tenant administrator will be notified.

Reference:

<https://learn.microsoft.com/en-us/compliance/regulatory/gdpr-breach-office365>

NEW QUESTION 97

- (Topic 6)

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

Name	Passwordless authentication	Multi-factor authentication (MFA) method registered
User1	Not configured	Microsoft Authenticator app (push notification)
User2	Configured	Microsoft Authenticator app (push notification)
User3	Not configured	Mobile phone
User4	Not configured	Email

You plan to create a Conditional Access policy that will use GPS-based named locations. Which users can the policy protect?

- A. User2 and User4 only
- B. User1 and User3 only
- C. User1 only
- D. User1, User2, User3, and User4

Answer: C

NEW QUESTION 100

- (Topic 6)

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-worldwide>

NEW QUESTION 101

DRAG DROP - (Topic 6)

Your company purchases a cloud app named App1.

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

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

Actions

Answer Area

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Answer Area

- Deploy Azure Active Directory (Azure AD) Application Proxy.
- From the Cloud App Security admin center, add an app connector.
- Sign in to App1.
- Create a conditional access policy.
- From the Azure Active Directory admin center, configure the Diagnostic settings.
- From the Azure Active Directory admin center, add an app registration for App1.



- From the Cloud App Security admin center, add an app connector.
- Create a conditional access policy.
- Sign in to App1.

NEW QUESTION 102

HOTSPOT - (Topic 6)

HOTSPOT

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

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

You add the following assignment for the User Administrator role:

- ? Scope type: Directory
- ? Selected members: Group1
- ? Assignment type: Active
- ? Assignment starts: Mar 15, 2023
- ? Assignment ends: Aug 15, 2023

You add the following assignment for the Exchange Administrator role:

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
On July 15, 2023, Admin1 can reset the password of a user.	<input type="checkbox"/>	<input type="checkbox"/>
On June 20, 2023, Admin2 can manage Microsoft Exchange Online.	<input type="checkbox"/>	<input type="checkbox"/>
On May 1, 2023, Admin3 can reset the password of a user.	<input type="checkbox"/>	<input type="checkbox"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

Admin1 is member of Group1.

The User Administrator role assignment has Group1 as a member. The assignment type: Active

July 15, 2023 is with the assignment period.

A User Administrator can manage all aspects of users and groups, including resetting passwords for limited admins.

Box 2: No

Admin2 is member of Group2.

The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible

June 20, 2023 is with the assignment period. The assignment must be approved.

Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.

Box 3: Yes

Admin3 is member of Group1 and Group2.

The User Administrator role assignment has Group1 as a member. The assignment type: Active

May 1, 2023 is with the assignment period.

NEW QUESTION 105

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

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

Site1 contains the files shown in the following table.

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

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

- Rule1 tip only
- Rule2 tip only
- Rule3 tip only
- Rule1 tip and Rule2 tip only
- Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

- Rule1 tip only
- Rule3 tip only
- Rule4 tip only
- Rule1 tip and Rule4 tip only
- Rule1 tip, Rule3 tip, and Rule4 tip

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3. Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

NEW QUESTION 109

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Endpoint security.

You need to create a group and assign the Endpoint Security Manager role to the group. Which type of group can you use?

- A. Microsoft 365 only
- B. security only
- C. mail-enabled security and security only
- D. mail-enabled security, Microsoft 365, and security only
- E. distribution, mail-enabled security, Microsoft 365, and security

Answer: D

NEW QUESTION 113

HOTSPOT - (Topic 6)

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

Name	Platform	Intune
Device1	iOS	Enrolled
Device2	macOS	Not enrolled

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Device1: Microsoft Endpoint Manager
 A local script
 Group Policy
Microsoft Endpoint Manager
 An app from the Google Play store
 Integration with Microsoft Defender for Cloud

Device2: A local script
A local script
 Group Policy
 Microsoft Endpoint Manager
 An app from the Google Play store
 Integration with Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Device1: Microsoft Endpoint Manager
 A local script
 Group Policy
Microsoft Endpoint Manager
 An app from the Google Play store
 Integration with Microsoft Defender for Cloud

Device2: A local script
A local script
 Group Policy
 Microsoft Endpoint Manager
 An app from the Google Play store
 Integration with Microsoft Defender for Cloud

NEW QUESTION 116

HOTSPOT - (Topic 6)

Your company has a Microsoft 365 subscription That contains the domains shown in the following exhibit.

Domains

+ Add domain Buy domain Refresh

Domain name ↑	Status	Choose columns
<input type="checkbox"/> contoso221018.onmicrosoft.com (Default)	Healthy	
<input type="checkbox"/> contoso.com	Incomplete setup	
<input type="checkbox"/> east.contoso221018.onmicrosoft.com	No services selected	

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

An administrator can create usernames that contain the [answer choice].

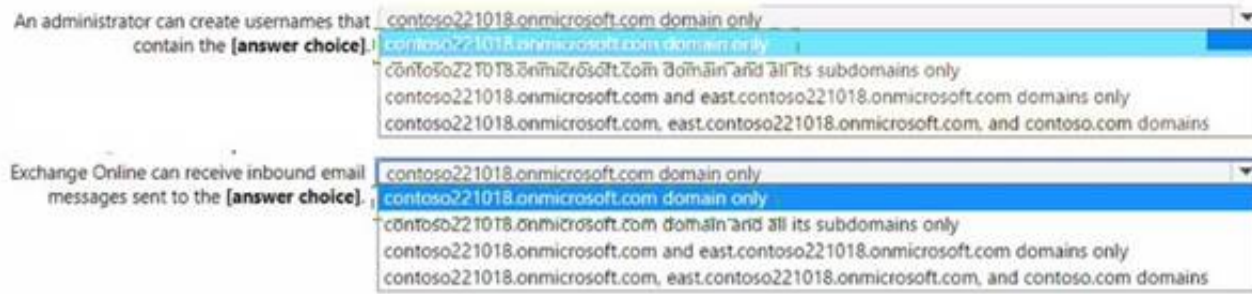
Exchange Online can receive inbound email messages sent to the [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 118

HOTSPOT - (Topic 6)

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

Name	Member of Microsoft 365 role group
Admin1	Content Explorer List viewer Content Explorer Content viewer
Admin2	Security Administrator Content Explorer List Viewer

You have labels in Microsoft 365 as shown in the following table.

Name	Type
Label1	Sensitivity
Label2	Retention

The content in Microsoft 365 is assigned labels as shown in the following table.

Name	Type	Label
File1	File in SharePoint Online	Label1
Mail1	Email message in Exchange Online	Label2

You have labels in Microsoft 365 as shown in the following table.

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

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Admin1 can view the contents of File1 by using Content explorer.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can view the contents of File1 by using Content explorer.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can use Content explorer to verify that Label2 is assigned to Mail1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 119

HOTSPOT - (Topic 6)

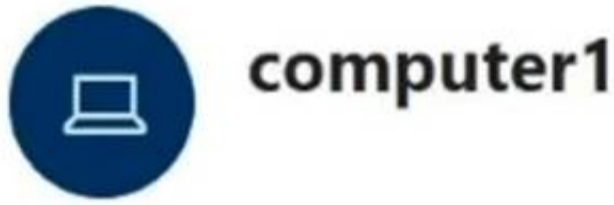
HOTSPOT

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 122

- (Topic 6)

You have the sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels

Label policies

Auto-labeling(preview)

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

+ Create a label Publish labels Refresh

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

Which labels can users apply to content?

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

Answer: D

Explanation:

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

NEW QUESTION 124

- (Topic 6)

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-risk-policies>

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

NEW QUESTION 127

FILL IN THE BLANK - (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer Area

Save the audit logs to:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Save the audit logs to:

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

NEW QUESTION 131
 HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Intune. You have devices enrolled in Intune as shown in the following table. You create the device configuration profiles shown in the following table.

Name	Platform	Assignments: Included groups	Assignments: Excluded groups	Scope tags
Profile1	Windows 10 and later	Group1	Group3	Tag1, Tag2
Profile2	Android Enterprise	All devices	Group2	Tag1, Tag2
Profile3	Android Enterprise	Group2, Group3	Group3	Tag1
Profile4	Windows 10 and later	Group3	None	Default

Which profiles will be applied to each device? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.

Device 1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device 2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Device 1:

- No profiles
- Profile1 only
- Profile4 only
- Profile1 and Profile4 only
- Profile1, Profile1, and Profile4 only

Device 2:

- No profiles
- Profile1 only
- Profile2 only
- Profile3 only
- Profile1 and Profile2 only
- Profile2 and Profile3 only

NEW QUESTION 132

HOTSPOT - (Topic 6)

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

Name	Member of
User1	Group1
User2	Group2

You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

In Microsoft Endpoint Manager, you create an enrollment status page profile that has the following settings:

- ? Show app and profile configuration progress: Yes
- ? Allow users to collect logs about installation errors: Yes
- ? Only show page to devices provisioned by out-of-box experience (OOBE): No
- ? Assignments: Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 enrolls Device1 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 enrolls Device2 in Microsoft Endpoint Manager, the enrollment status page will appear.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 137

- (Topic 6)

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

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

You have a computer that runs Windows 10.

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

Solution: From the Settings app, you select Update & Security to view the update history. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 141

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create a data loss prevention (DLP) policy that will be applied to all available locations.

Which conditions can you use in the DLP rules of the policy?

- A. sensitive info types
- B. content search queries
- C. keywords
- D. sensitivity labels

Answer: C

Explanation:

Apply retention labels to content automatically if it matches specific conditions, that includes cloud attachments that are shared in email or Teams, or when the content contains:

Specific types of sensitive information.

Specific keywords that match a query you create.

Pattern matches for a trainable classifier.

Note: Retention policies can be applied to the following locations: Exchange mailboxes

SharePoint classic and communication sites OneDrive accounts

Microsoft 365 Group mailboxes & sites Skype for Business

Exchange public folders

Teams channel messages (standard channels and shared channels) Teams chats

Teams private channel messages Yammer community messages Yammer user messages

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/retention> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-exchange-conditions-and-actions>

NEW QUESTION 146

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to create the data loss prevention (DLP) policies shown in the following table.

Name	Apply to location
DLP1	Exchange email
DLP2	SharePoint sites
DLP3	OneDrive accounts

You need to create DLP rules for each policy.

Which policies support the sender is condition and the file extension is condition? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sender is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

File extension is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Sender is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

File extension is condition:

- DLP1 only
- DLP2 only
- DLP3 only
- DLP2 and DLP3 only
- DLP1, DLP2, and DLP3

NEW QUESTION 150

- (Topic 6)

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 154

HOTSPOT - (Topic 6)

Your network contains an Active Directory domain and an Azure AD tenant.

You implement directory synchronization for all 10,000 users in the organization. You automate the creation of 100 new user accounts.

You need to ensure that the new user accounts synchronize to Azure AD as quickly as possible.

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

Answer Area

-PolicyType

- Start-ADSyncSyncCycle
- Set-ADSyncScheduler
- Invoke-ADSyncRunProfile

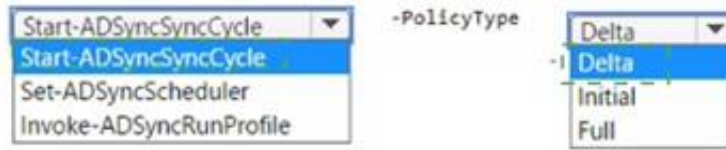
- Delta
- Initial
- Full

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 159

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution for monitoring and reporting application access. The solution must meet the following requirements:

- Support KQL for querying data.
- Retain report data for at least one year.

What should you include in the recommendation?

- A. a security report in Microsoft 365 Defender
- B. End point analytics
- C. Microsoft 365 usage analytics
- D. Azure Monitor workbooks

Answer: D

NEW QUESTION 163

- (Topic 6)

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

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

Answer: B

NEW QUESTION 164

HOTSPOT - (Topic 6)

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

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

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

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

You perform the following actions:

? For the Data Protection Baseline assessment, change the Test status of Establish a threat intelligence program to Implemented.

? Enable multi-factor authentication (MFA) for all users.

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

NOTE: Each correct selection is worth one point.

Statements

Yes No

Establish a threat intelligence program will appear as Implemented in the SP800 assessment.

The SP800 assessment score will increase by 54 points.

The Data Protection Baseline score will increase by 9 points.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 168

- (Topic 6)

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 170

HOTSPOT - (Topic 6)

You have 2,500 Windows 10 devices and a Microsoft 365 E5 tenant that contains two users named User1 and User2. The devices are not enrollment in Microsoft Intune.

In Microsoft Endpoint Manager, the Device limit restrictions are configured as shown in the following exhibit.

Device limit restrictions

Define how many devices each user can enroll.

Priority	Name	Device limit	Assigned
Default	All Users	2	Yes

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

Users may register their devices with Azure AD ⓘ

All None

[Learn more on how this setting works](#)

Require Multi-Factor Auth to join devices ⓘ

Yes No

Maximum number of devices per user ⓘ

5

From Microsoft Endpoint Manager, you add User2 as a device enrollment manager (DEM).

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input type="radio"/>
User2 can enroll all the devices in Intune.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can enroll only five devices in Intune.	<input type="radio"/>	<input checked="" type="radio"/>
User1 can join only five devices to Azure AD.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can enroll all the devices in Intune.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 171

HOTSPOT - (Topic 6)

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:

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

NEW QUESTION 172

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365. You need to configure policies to meet the following requirements:

? Customize the common attachments filter.

? Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. 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	Answer Area
<input type="checkbox"/> Anti-malware <input type="checkbox"/> Anti-phishing <input type="checkbox"/> Anti-spam <input type="checkbox"/> Safe Attachments	Customize the common attachments filter: <input type="text"/> Enable impersonation protection for sender domains: <input type="text"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Anti-malware

Customize the common attachments filter. See step 5 below.

* 1. Use the Microsoft 365 Defender portal to create anti-malware policies

In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use <https://security.microsoft.com/antimalwarev2>

* 2. On the Anti-malware page, select Create to open the new anti-malware policy wizard. On the Name your policy page, configure these settings:

Name: Enter a unique, descriptive name for the policy. Description: Enter an optional description for the policy.

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

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

* 5. On the Protection settings page, configure the following settings: Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

* 6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains. Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

NEW QUESTION 177

HOTSPOT - (Topic 6)

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:

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

NEW QUESTION 180

- (Topic 6)

You have an Azure AD tenant.

You have 1,000 computers that run Windows 10 Pro and are joined to Azure AD. You purchase a Microsoft 365 E3 subscription.

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

What should you do?

- A. From the Microsoft Endpoint Manager admin center, create a Windows Autopilot deployment profile
- B. Assign the profile to all the computer
- C. Instruct users to restart their computer and perform a network restart.
- D. Enroll the computers in Microsoft Intun
- E. Create a configuration profile by using the Edition upgrade and mode switch templat

- F. From the Microsoft Endpoint Manager admincenter, assign the profile to all the computers and instruct users to restart their computer.
- G. From Windows Configuration Designer, create a provisioning package that has an EditionUpgrade configuration and upload the package to a Microsoft SharePoint Online sit
- H. Instruct users to run the provisioning package from SharePoint Online.
- I. From the Azure Active Directory admin center, create a security group that has dynamic device membershi
- J. Assign licenses to the group and instruct users to sign in to their computer.

Answer: B

NEW QUESTION 185

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

You have a sensitivity label configured as shown in the Sensitivity label exhibit. (Click the Sensitivity label tab.)

Review your settings and finish

Name

Sensitivity1

Display name

Sensitivity1

Description for users

Sensitivity1

Scope

File.Email

Encryption

Content marking

Watermark: Watermark

Header: Header

Auto-labeling

Group settings

Site settings

Auto-labeling for database columns

None

You have an auto-labeling policy as shown in the Auto-labeling policy exhibit. (Click the Auto-labeling policy tab.)

Auto-labeling policy

[Edit Policy](#) [Delete Policy](#)

Policy name
Auto-labeling policy

Description

Label in simulation
Sensitivity1

Info to label
IP Address

Apply to content in these locations
Exchange email All

Rules for auto-applying this label
Exchange email 1 rule

Mode
On

Comment

A user sends an email that contains the components shown in the following table.

Type	File	Includes IP address
Mail body	Not applicable	No
Attachment	File1.docx	Yes
Attachment	File2.xml	Yes

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

Statements	Yes	No
Sensitivity1 is applied to the email.	<input type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to the email.	<input checked="" type="radio"/>	<input type="radio"/>
A watermark is added to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
A header is added to File2.xml.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 190

HOTSPOT - (Topic 6)

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

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

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

? Name: AutoLabel1

? Label to auto-apply: Sensitivity1

? Rules for SharePoint Online sites: Rule1-SPO

? Choose locations where you want to apply the label: Site1

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

Edit rule

Name *
Rule1-SPO

Description
Rule1 description

^ Conditions

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

^ Content contains sensitive info types 🗑

Default All of these 🗑

Sensitive info types

IP Address Accuracy to Instance count to 🗑

Add v

Create group

+ Add condition v

Save Cancel

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

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Sensitivity1 is applied to File1.docx.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input type="radio"/>	<input type="radio"/>

NEW QUESTION 191

- (Topic 5)

You need to configure Azure AD Connect to support the planned changes for the Montreal Users and Seattle Users OUs. What should you do?

- A. From the Microsoft Azure AD Connect wizard, select Customize synchronization options.
- B. From PowerShell, run the Add-ADSyncConnectorAttributeInclusion cmdlet.
- C. From PowerShell, run the start-ADSyncSyncCycle cmdlet.
- D. From the Microsoft Azure AD Connect wizard, select Manage federation.

Answer: A

NEW QUESTION 192

- (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 196

- (Topic 3)

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

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 200

- (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/safe-attachments.md>

NEW QUESTION 201

- (Topic 3)

You need to create the DLP policy to meet the technical requirements. What should you configure first?

- A. sensitive info types
- B. the Insider risk management settings
- C. the event types
- D. the sensitivity labels

Answer: A

Explanation:

Reference:

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

NEW QUESTION 206

- (Topic 2)

You need to meet the technical requirement for large-volume document retrieval. What should you create?

- A. a data loss prevention (DLP) policy from the Security & Compliance admin center
- B. an alert policy from the Security & Compliance admin center
- C. a file policy from Microsoft Cloud App Security
- D. an activity policy from Microsoft Cloud App Security

Answer: D

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts>

NEW QUESTION 210

HOTSPOT - (Topic 2)

You need to meet the technical requirement for the SharePoint administrator. What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

From the Security & Compliance admin center, perform a search by using:

▼
Audit log
Data governance events
DLP policy matches
eDiscovery

Filter by:

▼
Activity
Detail
Item
User agent

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance#step-3-filter-the-search-results>

NEW QUESTION 215

- (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 217

- (Topic 1)

You need to ensure that the support technicians can meet the technical requirement for the Montreal office mobile devices. What is the minimum of dedicated support technicians required?

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

Answer: B

Explanation:

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

NEW QUESTION 221

- (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/comange/how-to-enable>

NEW QUESTION 226

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You plan to implement identity protection by configuring a sign-in risk policy and a user risk policy. Which type of risk is detected by each policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sign-in risk policy:

User risk policy:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Sign-in risk policy:

User risk policy:

NEW QUESTION 229

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

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

Compliance settings [Edit](#)

Microsoft Defender ATP

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

Device Health

Rooted devices **Block**
 Require the device to be at or under the Device Threat Level

System Security

Require a password to unlock mobile devices **Require**
 Required password type **Device default**
 Encryption of data storage on device. **Require**
 Block apps from unknown sources **Block**

Actions for noncompliance [Edit](#)

Action	Schedule
Mark device noncompliant	Immediately
Retire the noncompliant device	Immediately

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

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

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

Rooted devices will be

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

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

Rooted devices will be

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

NEW QUESTION 232

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You create a Conditional Access policy that blocks access to an app named App1 when users trigger a high-risk sign-in event.

You need to reduce false positives for impossible travel when the users sign in from the corporate network.

What should you configure?

- A. exclusion groups
- B. multi-factor authentication (MFA)
- C. named locations
- D. user risk policies

Answer: C

NEW QUESTION 233

HOTSPOT - (Topic 6)

You have Microsoft 365 subscription.

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

Policy1

Status On

Name your alert

Description

[Add a description](#)

Severity

Low

Category

Threat management

Policy contains tags

-

Create alert settings

Conditions

Activity is FileMalwareDetected

Aggregation

Aggregated

Scope

All users

Threshold

20

Window

2 hours

Severity

Low

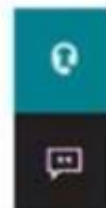
Set your recipients

Recipients

User1@sk220912outlook.onmicrosoft.com

Daily notification limit

100



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

Policy1 will trigger an alert if malware is detected in [answer choice].

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

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
 5
 12
 20
 100

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Policy1 will trigger an alert if malware is detected in [answer choice].

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

The maximum number of email messages that Policy1 will generate per day is [answer choice].

5
 5
 12
 20
 100

NEW QUESTION 237

HOTSPOT - (Topic 6)

You have a hybrid deployment of Azure AD that contains the users shown in the following table.

Name	Description
User1	Azure AD Connect sync account
User2	Contributor for Azure AD Connect Health
User3	Application administrator in Azure AD

You need to identify which users can perform the following tasks:

- View sync errors in Azure AD Connect Health.
- Configure Azure AD Connect Health settings.

Which user should you identify for each task? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

View sync errors in Azure AD Connect Health:

User2
 User1
 User2
 User3

Configure Azure AD Connect Health settings:

User1
 User1
 User2
 User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

View sync errors in Azure AD Connect Health:

Configure Azure AD Connect Health settings:

NEW QUESTION 238

HOTSPOT - (Topic 6)

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

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

Site1 contains the files shown in the following table.

Name	Label
File1	None
File2	Retention1
File3	Retention2
File4	Retention3

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

Answer Area

Rename:

Delete:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area

Rename:

Delete:

NEW QUESTION 240

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant.

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

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

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 242

- (Topic 6)

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 244

HOTSPOT - (Topic 6)

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

Name	Member of	Azure Active Directory (Azure AD) role
User1	Group1	Global administrator
User2	Group2	Cloud device administrator

You configure an Enrollment Status Page profile as shown in the following exhibit.

Settings

The enrollment status page appears during initial device setup. If enabled, users can see the installation progress of assigned apps and profiles.

Show app and profile installation progress. Yes No

Show time limit error when installation takes longer than specified number of minutes.

Show custom message when time limit error occurs. Yes No

Allow users to collect logs about installation errors. Yes No

Only show page to devices provisioned by out-of-box experience (OOBE) Yes No

Block device use until all apps and profiles are installed Yes No

You assign the policy to Group1.
 You purchase the devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android

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

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.	<input checked="" type="radio"/>	<input type="radio"/>
If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>
If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 249
 - (Topic 6)

You have a Microsoft 365 subscription that contains a user named User1.
 You need to ensure that User1 can search the Microsoft 365 audit logs from the Security & Compliance admin center.
 Which role should you assign to User1?

- A. View-Only Audit Logs in the Security & Compliance admin center
- B. View-Only Audit Logs in the Exchange admin center
- C. Security reader in the Azure Active Directory admin center
- D. Security Reader in the Security & Compliance admin center

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?view=o365-worldwide>

NEW QUESTION 251

- (Topic 6)

You have a Microsoft 365 subscription that contains an Azure AD tenant named contoso.com.
 Corporate policy states that user passwords must not include the word Contoso. What should you do to implement the corporate policy?

- A. From Azure AD Identity Protection, configure a sign-in risk policy.
- B. From the Microsoft Entra admin center, create a conditional access policy.
- C. From the Microsoft 365 admin center, configure the Password policy settings.
- D. From the Microsoft Entra admin center, configure the Password protection settings.

Answer: D

NEW QUESTION 252

- (Topic 6)

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

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

Answer: D

Explanation:

Microsoft 365 Reports in the admin center

You can easily see how people in your business are using Microsoft 365 services. For example, you can identify who is using a service a lot and reaching quotas, or who may not need a Microsoft 365 license at all.

Which activity reports are available in the admin center

Depending on your subscription, here are the available reports in all environments.

Report	Public	GCC	GCC-High	DoD	Office 365 operated by 21Vianet
Microsoft browser usage	Yes	No ¹	No ¹	No ¹	No ¹
Email activity	Yes	Yes	Yes	Yes	Yes
Email apps usage	Yes	Yes	Yes	Yes	Yes
Mailbox usage	Yes	Yes	Yes	Yes	Yes
Office activations	Yes	Yes	Yes	Yes	Yes

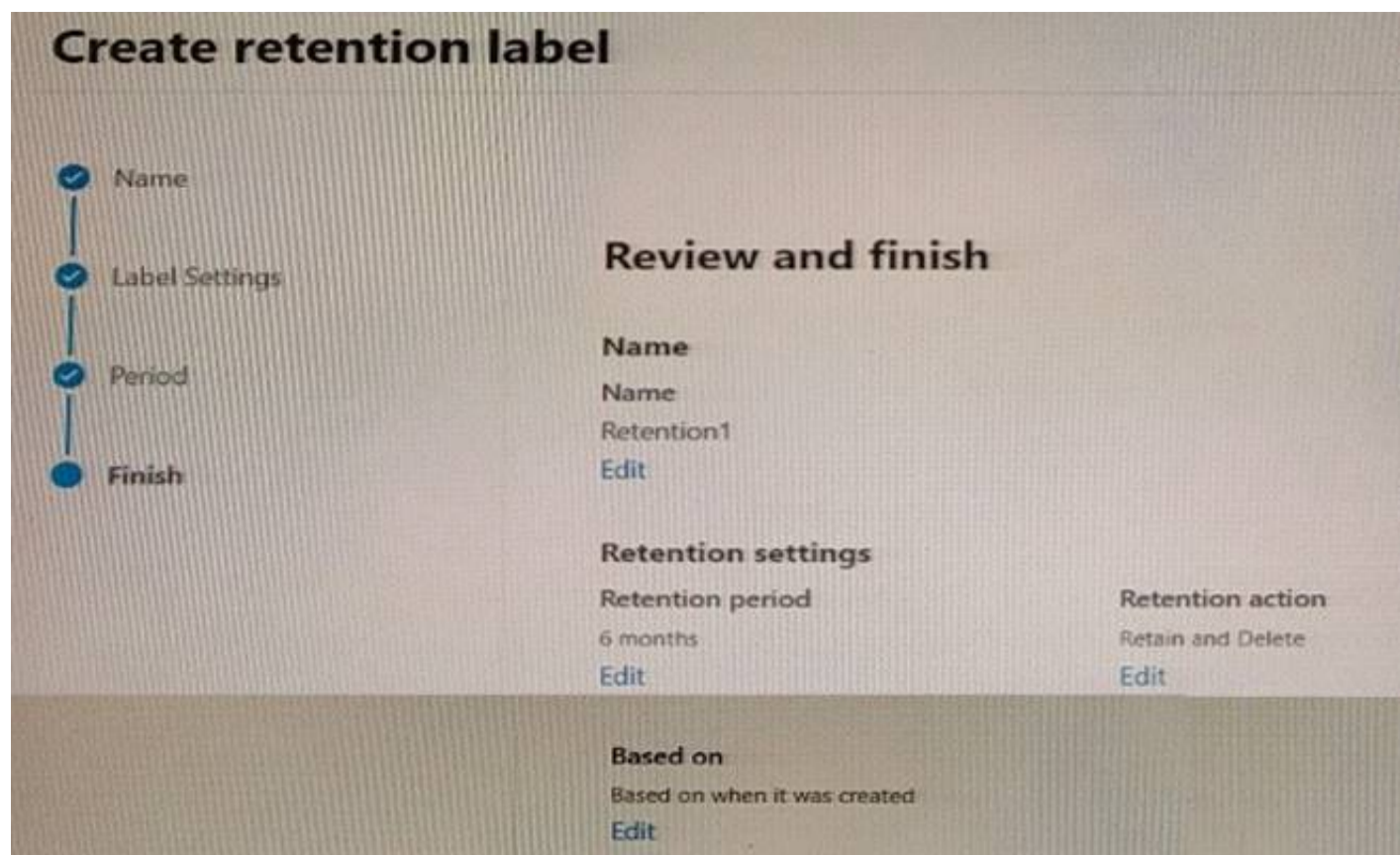
Reference:

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

NEW QUESTION 257

- (Topic 6)

You have a Microsoft 365 subscription.
 You create a retention label named Retention1 as shown in the following exhibit.



You apply Retention1 to all the Microsoft OneDrive content. On January 1, 2020, a user stores a file named File1 in OneDrive. On January 10, 2020, the user modifies File1. On February 1, 2020, the user deletes File1. When will File1 be removed permanently and unrecoverable from OneDrive?

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

Answer: B

NEW QUESTION 258

- (Topic 6)

You have a Microsoft 365 subscription. You need to identify which administrative users performed eDiscovery searches during the past week. What should you do from the Security & Compliance admin center?

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

Answer: D

NEW QUESTION 263

- (Topic 6)

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

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

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

Answer: C

NEW QUESTION 268

- (Topic 6)

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

Name	Type
Label1	Sensitivity
Label2	Retention

You have the items shown in the following table.

Name	Stored in	Description
File1	Microsoft SharePoint	File document that has Label1 applied
File2	Microsoft Teams channel	File document that has Label2 applied
Mail1	Microsoft Exchange Online	Email message that has Label1 applied
Mail2	Microsoft Exchange Online	Email message that has Label2 applied

Which items can you view in Content explorer?

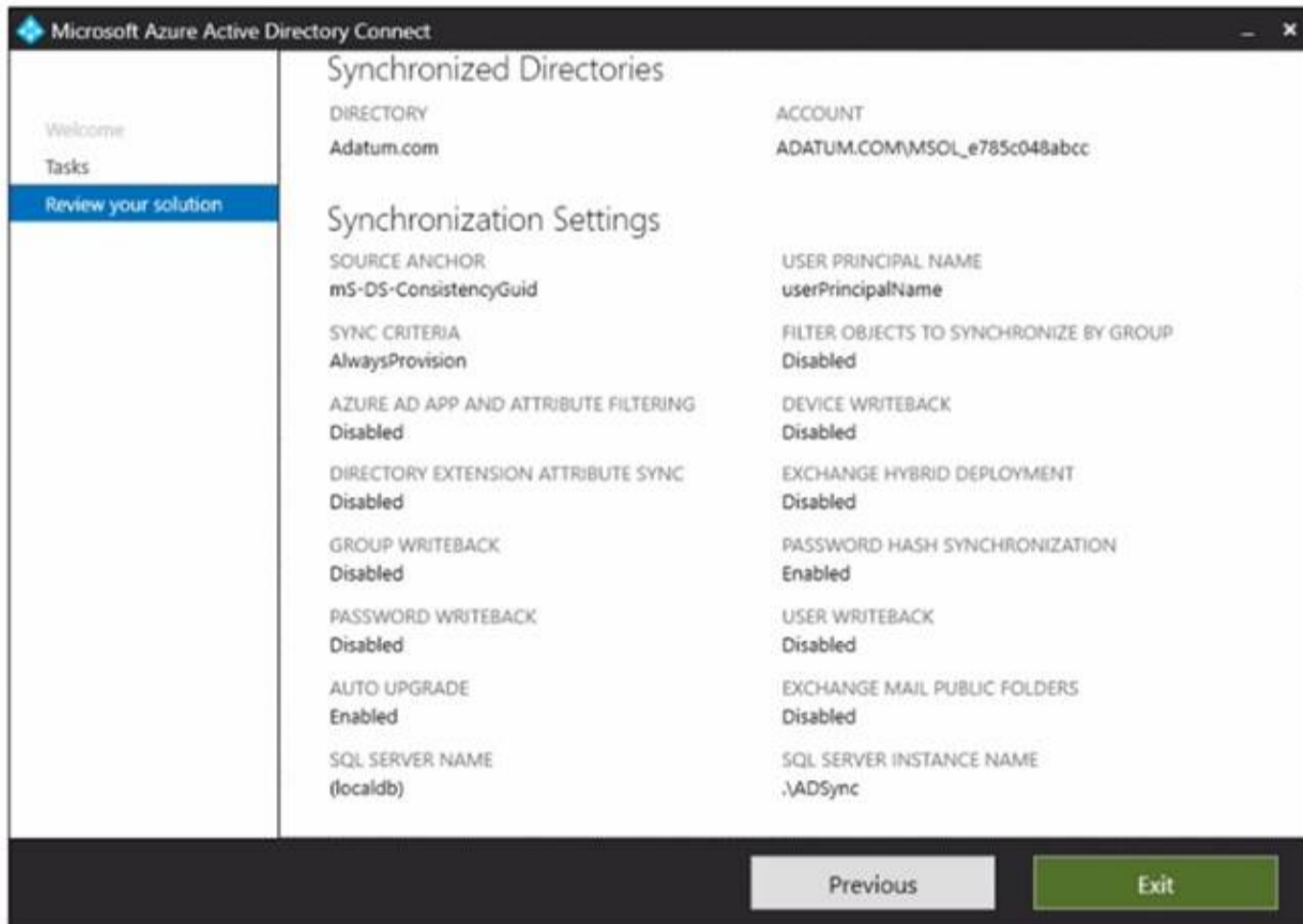
- A. File1 only
- B. File1 and File2 only
- C. File1 and Mail1 only
- D. File2 and Mail2 only
- E. File1, File2, Mail1, and Mail2

Answer: C

NEW QUESTION 273

HOTSPOT - (Topic 6)

Your company has a hybrid deployment of Microsoft 365. An on-premises user named User1 is synced to Azure AD. Azure AD Connect is configured 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

User1 [answer choice].

If the password for User1 is changed in Active Directory, [answer choice].

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

User1 [answer choice].

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using Self-Service Password Reset feature only
- can change her password from the Microsoft 365 admin center only

If the password for User1 is changed in Active Directory, [answer choice].

- the password hash will be synchronized to Azure AD
- the password hash will be synchronized to Azure AD
- a new randomly generated password will be assigned to User1
- the password hash in Azure AD will be unchanged

NEW QUESTION 275

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription.

You have an Azure AD tenant named contoso.com that contains the following users:

- Admin1
- Admin2
- User1

Contoso.com contains an administrative unit named AIM that has no role assignments. User1 is a member of AU1. You create an administrative unit named AU2 that does NOT have any members or role assignments. 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
You can add Admin1 as a member of AU1.	<input type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
You can add Admin1 as a member of AU1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add User1 as a member of AU2.	<input checked="" type="radio"/>	<input type="radio"/>
You can assign Admin2 the User administrator role for AU1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 276

- (Topic 6)

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

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

Your network contains an on-premises Active Directory domain. The domain contains domain controllers that run Windows Server 2019. The functional level of the forest and the domain is Windows Server 2012 R2.

The domain contains 100 computers that run Windows 10 and a member server named Server1 that runs Windows Server 2012 R2.

You plan to use Server1 to manage the domain and to configure Windows 10 Group Policy settings.

You install the Group Policy Management Console (GPMC) on Server1.

You need to configure the Windows Update for Business Group Policy settings on Server1. Solution: You raise the domain functional level to Windows Server 2019. You copy the

Group Policy Administrative Templates from a Windows 10 computer to the Netlogon share on all the domain controllers.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 279

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual MS-102 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the MS-102 Product From:

<https://www.2passeasy.com/dumps/MS-102/>

Money Back Guarantee

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