

Microsoft

Exam Questions MS-102

Microsoft 365 Administrator Exam



NEW QUESTION 1

- (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 2

- (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 3

- (Topic 6)

You have a Microsoft 365 tenant.

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

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

Answer: D

NEW QUESTION 4

- (Topic 6)

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

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

You need to recommend a solution to manage resources in Intune that meets the following requirements:

? Local administrators must be able to manage only the resources in their respective office.

? Local administrators must be prevented from managing resources in other offices.

? Administrative effort must be minimized.

What should you include in the recommendation?

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

Answer: B

Explanation:

Reference:

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

NEW QUESTION 5

- (Topic 6)

You have a Microsoft 365 subscription.

You discover that some external users accessed center for a Microsoft SharePoint site. You modify the SharePoint sharing policy to prevent sharing, outside your organization. You need to be notified if the SharePoint sharing policy is modified in the future. Solution: From the Security & Compliance admin center you create a

threat management policy.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 6

- (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: At a command prompt, you run the winver.exe command. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://support.microsoft.com/en-us/windows/which-version-of-windows-operating-system-am-i-running-628bec99-476a-2c13-5296-9dd081cdd808>

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)

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 copy the Group Policy Administrative Templates from a Windows 10

computer to Server1. Does this meet the goal?

- A. yes
- B. No

Answer: A

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:

The Microsoft 365 admin center

The Microsoft 365 admin center

Group types:

The Microsoft 365 Defender portal

The Microsoft Entra admin center

The Microsoft Purview compliance portal

Group types:

Security only

Microsoft 365 only

Security only

Security and mail-enabled security only

Microsoft 365 and distribution only

Microsoft 365, mail-enabled security, and distribution only

Security, Microsoft 365, mail-enabled security, and distribution

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Portal:

The Microsoft 365 admin center

The Microsoft 365 admin center

Group types:

The Microsoft 365 Defender portal

The Microsoft Entra admin center

The Microsoft Purview compliance portal

Group types:

Security only

Microsoft 365 only

Security only

Security and mail-enabled security only

Microsoft 365 and distribution only

Microsoft 365, mail-enabled security, and distribution only

Security, Microsoft 365, mail-enabled security, and distribution

NEW QUESTION 10

HOTSPOT - (Topic 6)

HOTSPOT

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

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

You plan to provide User4 with early access to Microsoft 365 feature and service updates. You need to identify which Microsoft 365 setting must be configured, and which user can modify the setting. The solution must use the principle of least privilege. What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Microsoft 365 setting:

Office installation options

Privileged access

Release preferences

User:

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Microsoft 365 setting:

Office installation options

Privileged access

Release preferences

User:

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

NEW QUESTION 10

- (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 Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the Azure AD credentials.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

Reference:

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

NEW QUESTION 13

- (Topic 6)

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

SharePoint Content_Export

↓ Restart report

↓ Download report

🗑 Delete

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

Items included from the search:
All items, excluding ones that have unrecognized format, are encrypted, or weren't indexed for other reasons.

Exchange content format:
One PST file for each mailbox.

De-duplication for Exchange content:
Not enabled.

SharePoint document versions:
Included

Export files in a compressed (zipped) folder:
Yes

The export data was prepared within region:
Default region

Close

Feedback

What will be excluded from the export?

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

Answer: B

Explanation:

Unrecognized file formats are excluded from the search.

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide>

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

NEW QUESTION 17

- (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 20

HOTSPOT - (Topic 6)

You have a Microsoft 365 tenant that contains devices enrolled in Microsoft Intune. The devices are configured as shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Android
Device3	iOS

You plan to perform the following device management tasks in Microsoft Endpoint Manager:

- ? Deploy a VPN connection by using a VPN device configuration profile.
- ? Configure security settings by using an Endpoint Protection device configuration profile.

You support the management tasks.

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

NOTE: Each correct selection is worth one point.

VPN device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VPN device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

Endpoint Protection device configuration profile:

Device1 only
Device1 and Device2 only
Device1 and Device3 only
Device1, Device2 and Device3

NEW QUESTION 21

- (Topic 6)

You have a Microsoft 365 E5 subscription.

You define a retention label that has the following settings:

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

You need to prevent the removal of the label once the label K applied to a lie What should you select in the retention label settings?

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

Answer: B

NEW QUESTION 25

HOTSPOT - (Topic 6)

HOTSPOT

You have a Microsoft 365 subscription.

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

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

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

NOTE: Each correct selection is worth one point.

- C. Sitel only
- D. Group1 and Group2 only
- E. Group1, Group2, and Sitel

Answer: E

Explanation:

Assign sensitivity labels to Microsoft 365 groups in Azure Active Directory
Azure Active Directory (Azure AD), part of Microsoft Entra, supports applying sensitivity labels published by the Microsoft Purview compliance portal to Microsoft 365 groups.
In addition to using sensitivity labels to protect documents and emails, you can also use sensitivity labels to protect content in the following containers: Microsoft Teams sites, Microsoft 365 groups (formerly Office 365 groups), and SharePoint sites.
When you configure a label policy, you can:
Choose which users and groups see the labels. Labels can be published to any specific user or email-enabled security group, distribution group, or Microsoft 365 group (which can have dynamic membership) in Azure AD.
Reference:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-teams-groups-sites>
<https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide>

NEW QUESTION 34

HOTSPOT - (Topic 6)

Your company has a Azure AD tenant named comoso.onmicrosoft.com that contains the users shown in the following table.

Name	Role
User1	Password Administrator
User2	Security Administrator
User3	User Administrator
User4	None

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

- Reset the password of User4.
- Modify the value for the manager attribute of User4.

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

Reset the password of User4:

User1 and User3 only

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Reset the password of User4:

User1 and User3 only

User1 only

User2 only

User1 and User2 only

User1 and User3 only

User1, User2, and User3

Modify the value for the manager attribute of User4:

User3 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

NEW QUESTION 38

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.

Configure

Microsoft Intune

Save

Discard

Delete

MDM user scope ⓘ

None

Some

All

Groups

Select groups

Group1

>

MDM terms of use URL ⓘ

https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL ⓘ

https://enrollment.manage.microsoft.com/enrollmentserver/discov ...

MDM compliance URL ⓘ

https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM User scope ⓘ

None

Some

All

Groups

Select groups

Group2

>

MAM Terms of use URL ⓘ

MAM Discovery URL ⓘ

https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL ⓘ

Restore default MAM 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 39

- (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 admin center, you assign User1 the Compliance admin role.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Reference:

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

NEW QUESTION 40

HOTSPOT - (Topic 6)

HOTSPOT

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

? Contoso.com

? East.contoso.com

The forest contains the users shown in the following table.

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

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes No

User1 can authenticate to Azure AD by using a username of user1@contoso.com.

☒ ☐

User2 can authenticate to Azure AD by using a username of user2@contoso.com.

☐ ☐

User3 can authenticate to Azure AD by using a username of user3@contoso.com.

☐ ☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes
The UPN of user1 is user1@contoso.com so he can authenticate to Azure AD by using the username user1@contoso.com.
Box 2: No
The UPN of user2 is user2@east.contoso.com so he cannot authenticate to Azure AD by using the username user2@contoso.com.
Box 3: No
The UPN of user3 is user3@fabrikam.com so he cannot authenticate to Azure AD by using the username user3@contoso.com.

NEW QUESTION 44

- (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 subscription.
You need to prevent users from accessing your Microsoft SharePoint Online sites unless the users are connected to your on-premises network.
Solution: From the Endpoint Management admin center, you create a device configuration profile.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

NEW QUESTION 47

HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 E5 subscription.
From Azure AD Privileged Identity Management (PIM), you configure Role settings for the Global Administrator role as shown in the following exhibit.

Activation	
Setting	State
Activation maximum duration (hours)	8 hour(s)
On activation, require	Azure MFA
Require justification on activation	Yes
Require ticket information on activation	No
Require approval to activate	No
Approvers	None
Assignment	
Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	3 month(s)
Allow permanent active assignment	No
Expire active assignments after	15 day(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

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

Answer Area

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

will lose the role after eight hours

can reactivate the role every eight hours

can reactivate the role every 15 days

will lose the role after 15 days

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

for up to eight hours

for up to three months

for up to 15 days

until the requests are revoked manually

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: will lose the role after eight hours
From exhibit: Activation, Activation maximum duration (hours): 8 hour(s)
Box 2: for up to three months
We see from exhibit: Assignment, Expire eligible assignment after: 3 month(s)

NEW QUESTION 49

HOTSPOT - (Topic 6)
You configure a data loss prevention (DLP) policy named DLP1 as shown in the following exhibit.

Choose the types of content to protect

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

Content contains

Any of these

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

Retention labels

1 year

Add

+ Add group

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

DLP1 cannot be applied to

Exchange email

SharePoint sites

OneDrive accounts

DLP1 will be applied only to documents that have

both a credit card number and the 1 year label applied

either a credit card number or the 1 year label applied

between 85 and 100 credit card numbers

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 54

- (Topic 6)
You have a Microsoft 365 subscription.
You view the Service health Overview as shown in the following exhibit.

Passing Certification Exams Made Easy

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

Service health

October 18, 2022 4:20 PM

Overview Issue history Reported issues

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

 Report an issue  Customize

Active issues

Issue title Affected service Issue type

> Microsoft service health (6)

Issues in your environment that require action (0)

Microsoft service health

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

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

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

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

Answer: B

Explanation:

Service Support admin

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

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

Incorrect:

* Message center reader

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

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

* Reports reader

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

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

Reference:

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

NEW QUESTION 59

HOTSPOT - (Topic 6)

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

The subscription has the default inbound anti-spam policy and a custom Safe Attachments policy.

You need to identify the following information:

- The number of email messages quarantined by zero-hour auto purge (ZAP)
 - The number of times users clicked a malicious link in an email message
- Which Email & collaboration report should you use? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Answer Area

To identify the number of emails quarantined by ZAP:

Threat protection status

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

To identify the number of times users clicked a malicious link in an email:

Mailflow status report

Mailflow status report

Spoof detections

Threat protection status

URL threat protection

NEW QUESTION 62

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

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

Passing Certification Exams Made Easy

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

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 63

HOTSPOT - (Topic 6)
HOTSPOT

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

Name	Role
User1	Global admin
User2	None
User3	None

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

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

You need to identify which users can add apps to the private store, and which users can assign apps from Microsoft Store for Business.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Can add apps to the private store:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

Can assign apps from Microsoft Store for Business:

▼

User2 only

User1 and User2 only

User2 and User3 only

User1, User2, and User3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Can add apps to the private store:

▼

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

Can assign apps from Microsoft Store for Business:

▼

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

NEW QUESTION 64

- (Topic 6)
 You have a Microsoft 365 E5 subscription.
 From the Microsoft 365 Defender portal, you plan to export a detailed report of compromised users.
 What is the longest time range that can be included in the report?

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

Answer: C

Explanation:

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

NEW QUESTION 68

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

NEW QUESTION 70

- (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 Active Directory domain. You deploy a Microsoft Entra tenant.

Another administrator configures the domain to synchronize to the Microsoft Entra tenant.

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

You review Microsoft Entra Connect Health and discover that all the user account synchronizations completed successfully.

You need to ensure that the 10 user accounts are synchronized to the Microsoft Entra tenant.

Solution: From Microsoft Entra Connect, you modify the filtering settings. Does this meet the goal?

- A. Yes
B. No

Answer: B

NEW QUESTION 72

- (Topic 6)

You have a Microsoft 365 subscription.

You need to configure a compliance solution that meets the following requirements: Defines sensitive data based on existing data samples

Automatically prevents data that matches the samples from being shared externally in Microsoft SharePoint or email messages

Which two components should you configure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

A: Classifiers

This categorization method is well suited to content that isn't easily identified by either the manual or automated pattern-matching methods. This method of categorization is more about using a classifier to identify an item based on what the item is, not by elements that are in the item (pattern matching). A classifier learns how to identify a type of content by looking at hundreds of examples of the content you're interested in identifying.

Where you can use classifiers

Classifiers are available to use as a condition for: Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition Communication compliance

Sensitivity labels can use classifiers as conditions, see Apply a sensitivity label to content automatically.

Data loss prevention

E: Organizations have sensitive information under their control such as financial data, proprietary data, credit card numbers, health records, or social security numbers. To help protect this sensitive data and reduce risk, they need a way to prevent their users from inappropriately sharing it with people who shouldn't have it. This practice is called data loss prevention (DLP).

Reference:
<https://learn.microsoft.com/en-us/microsoft-365/compliance/classifier-learn-about> <https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp>

NEW QUESTION 77

HOTSPOT - (Topic 6)

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

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

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

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 78

- (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 forest functional level to Windows Server 2016.
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 80

- (Topic 6)

You have a Microsoft 365 subscription that uses Microsoft 365 Defender.
You need to compare your company's security configurations to Microsoft best practices and review improvement actions to increase the security posture.
What should you use?

- A. Microsoft Secure Score
- B. Cloud discovery
- C. Exposure distribution

- D. Threat tracker
- E. Exposure score

Answer: A

NEW QUESTION 81

HOTSPOT - (Topic 6)

HOTSPOT

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

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

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

If a high-severity incident is triggered for Device1, an incident email notification will be sent.

Yes

☐

No

☐

If a low-severity incident is triggered for Computer1, an incident notification email will be sent.

☐☐

If a low-severity incident is triggered for Device3, an incident notification email will be sent.

☐☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No

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

Box 2: No

Computer1 does not belong to either Group1 or Group2

Box 3: Yes

Device3 belongs to both Group1 and Group2.

Note: Understanding alert severity

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

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

NEW QUESTION 85

- (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 Active Directory forest. You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.

• User passwords must be 10 characters or more.
Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 90

- (Topic 6)
You have a Microsoft 365 subscription that uses Microsoft Defender for Endpoint.
All the devices in your organization are onboarded to Microsoft Defender for Endpoint.
You need to ensure that an alert is generated if malicious activity was detected on a device during the last 24 hours.
What should you do?

- A. From the Microsoft Purview compliance portal, create a data loss prevention (DLP) policy.
- B. From Alerts queue, create a suppression rule and assign an alert.
- C. From Advanced hunting, create a query and a detection rule.
- D. From the Microsoft Purview compliance portal, create an audit log search.

Answer: C

NEW QUESTION 91

HOTSPOT - (Topic 6)
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	MFA Status
User1	Group1	Enabled
User2	Group1, Group2	Enforced

You have the named locations shown in the following table.

Named location	IP range
Montreal	133.107.0.0/16
Toronto	193.77.10.0/24

You create a conditional access policy that has the following configurations:

- Users or workload identities: o Include: Group1
o Exclude: Group2
- Cloud apps or actions: Include all cloud apps
- Conditions:
o Include: Any location
o Exclude: Montreal
- Access control: Grant access, Require multi-factor authentication
User1 is on the multi-factor authentication (MFA) blocked users list.

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

Answer Area	Statements	Yes	No
	User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input type="radio"/>	<input type="radio"/>
	User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
	User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access Microsoft Office 365 from a device that has an IP address of 133.107.10.20.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.15.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Office 365 from a device that has an IP address of 193.77.10.20.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 96

- (Topic 6)
Your company has on-premises servers and an Azure AD tenant.
Several months ago, the Azure AD Connect Health agent was installed on all the servers. You review the health status of all the servers regularly.
Recently, you attempted to view the health status of a server named Server1 and discovered that the server is NOT listed on the Azure AD Connect Servers list.
You suspect that another administrator removed Server1 from the list. You need to ensure that you can view the health status of Server1.
What are two possible ways to achieve the goal? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

- A. From Azure Cloud shell, run the Connect-Azure AD cmdlet.
- B. From Server1, change the Azure AD Connect Health Services Startup type to Automatic (Delayed Start)
- C. From Server1, change the Azure AD Connect Health Services Startup type to Automatic
- D. From Windows PowerShell, run the Register-AzureADConnectHealthsyncAgent cmdlet.
- E. From Server1, reinstall the Azure AD Connect Health agent

Answer: DE

NEW QUESTION 100

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 104

- (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.)



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 106

HOTSPOT - (Topic 6)

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

Name	Member of	Role
User1	Group1	User Administrator
User2	Group1	None
User3	Group2	None
User4	None	Global Administrator

You enable self-service password reset (SSPR) for Group1. You configure security questions as the only authentication method for SSPR.
Which users can use SSPR, and which users must answer security questions to reset their password? To answer, select the appropriate options in the answer

area.
NOTE; Each correct selection is worth one point.
Answer Area

Users that can use SSPR:

User1, User2, and User4 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

Users that must answer security questions to reset their password:

User1 and User2 only

User1 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Users that can use SSPR:

User1, User2, and User4 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

Users that must answer security questions to reset their password:

User1 and User2 only

User1 only

User2 only

User1 and User2 only

User1, User2, and User3 only

User1, User2, and User4 only

User1, User2, User3, and User4

NEW QUESTION 108

- (Topic 6)
You have a Microsoft 365 E3 subscription that uses Microsoft Defender for Endpoint Plan 1.
Which two Defender for Endpoint features are available to the subscription? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.

- A. advanced hunting
- B. security reports
- C. digital certificate assessment
- D. device discovery
- E. attack surface reduction (ASR)

Answer: BE

Explanation:
B: Overview of Microsoft Defender for Endpoint Plan 1, Reporting
The Microsoft 365 Defender portal (<https://security.microsoft.com>) provides easy access to information about detected threats and actions to address those threats.
The Home page includes cards to show at a glance which users or devices are at risk, how many threats were detected, and what alerts/incidents were created. The Incidents & alerts section lists any incidents that were created as a result of triggered alerts. Alerts and incidents are generated as threats are detected across devices.
The Action center lists remediation actions that were taken. For example, if a file is sent to quarantine, or a URL is blocked, each action is listed in the Action center on the History tab.
The Reports section includes reports that show threats detected and their status. E: What can you expect from Microsoft Defender for Endpoint P1?
Microsoft Defender for Endpoint P1 is focused on prevention/EPP including:
Next-generation antimalware that is cloud-based with built-in AI that helps to stop ransomware, known and unknown malware, and other threats in their tracks.
(E) Attack surface reduction capabilities that harden the device, prevent zero days, and offer granular control over access and behaviors on the endpoint.
Device based conditional access that offers an additional layer of data protection and breach prevention and enables a Zero Trust approach.
The below table offers a comparison of capabilities are offered in Plan 1 versus Plan 2.

Capabilities	P1	P2
Unified security tools and centralized management	✓	✓
Next-generation antimalware	✓	✓
Attack surface reduction rules	✓	✓
Device control (e.g.: USB)	✓	✓
Endpoint firewall	✓	✓
Network protection	✓	✓
Web control / category-based URL backing	✓	✓
Device-based conditional access	✓	✓
Controlled folder access	✓	✓
APIs, SIEM connector, custom TI	✓	✓
Application control	✓	✓
Endpoint detection and response		✓
Automated investigation and remediation		✓
Threat and vulnerability management		✓
Threat intelligence (Threat Analytics)		✓
Sandbox (deep analysis)		✓
Microsoft Threat Experts**		✓

**Includes Targeted Attack Notifications (TAN) and Experts On Demand (EOD). Customers must apply for TAN. EOD is available for purchase as an add-on.

Incorrect:

Not A: P2 is by far the best fit for enterprises that need an EDR solution including automated investigation and remediation tools, advanced threat prevention and threat and vulnerability management (TVM), and hunting capabilities.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/defender-endpoint-plan-1>

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/microsoft-defender-for-endpoint-plan-1-now-included-in-m365-e3/ba-p/3060639>

NEW QUESTION 113

HOTSPOT - (Topic 6)

You have an Azure subscription and an on-premises Active Directory domain. The domain contains 50 computers that run Windows 10.

You need to centrally monitor System log events from the computers.

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

NOTE: Each correct selection is worth one point.

In Azure:	<div><div></div><div><div>Add and configure the Diagnostics settings for the Azure Activity Log.</div><div>Add and configure an Azure Log Analytics workspace.</div><div>Add an Azure Storage account and Azure Cognitive Search</div><div>Add an Azure Storage account and a file share.</div></div></div>
On the computers:	<div><div></div><div><div>Create an event subscription.</div><div>Modify the membership of the Event Log Readers group.</div><div>Enroll in Microsoft Endpoint Manager.</div><div>Install the Microsoft Monitoring Agent.</div></div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

In Azure:

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

On the computers:

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

NEW QUESTION 114

- (Topic 6)

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

You plan to implement a hybrid configuration that has the following requirements:

- Minimizes the number of times users are prompted for credentials when they access Microsoft 365 resources
- Supports the use of Azure AD Identity Protection

You need to configure Azure AD Connect to support the planned implementation. Which two options should you select? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Password Hash Synchronization
- B. Password writeback
- C. Directory extension attribute sync
- D. Enable single sign-on
- E. Pass-through authentication

Answer: AB

NEW QUESTION 119

- (Topic 6)

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

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: AE

Explanation:

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

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

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

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

NEW QUESTION 121

- (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 Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

You discover that 10 user accounts in an organizational unit (OU) are NOT synchronized to Azure AD. All the other user accounts synchronized successfully. You review Azure AD Connect Health and discover that all the user account synchronizations completed successfully. You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From Azure AD Connect, you modify the filtering settings. Does this meet the goal?

- A. Yes
- B. No

Answer: A

NEW QUESTION 125

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

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2:

Step 3:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

From the Microsoft Entra admin center, configure on-premises integration password writeback.

From the Microsoft Entra admin center, configure the authentication methods for SSPR.

From the Microsoft Entra admin center, configure the registration settings for SSPR.

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

Step 1: Validate permissions for the Microsoft Entra Connect account.

Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.

Step 3: Select Password writeback in Microsoft Entra Connect.

NEW QUESTION 130

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

-enabled

-Force

-RestrictiveRetention

-RetentionPolicyTagLinks

-SystemTag

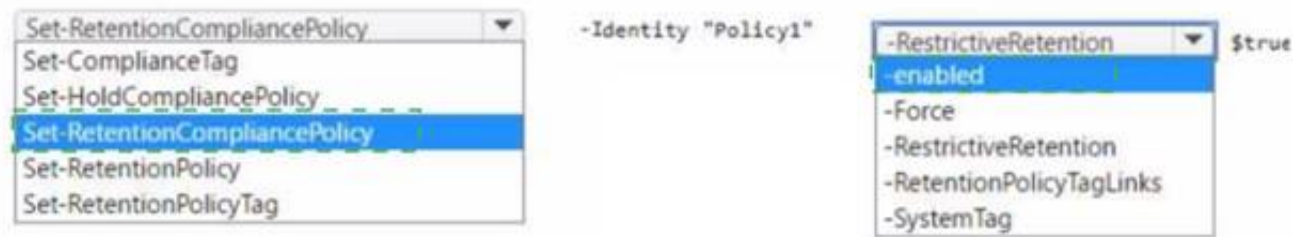
\$true

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 133

- (Topic 6)

You have a Microsoft 365 E5 subscription.

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

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

Solution: From the Azure Active Directory admin center, you assign SecAdmin1 the Teams Administrator role.

Does this meet the goal?

- A. Yes
- B. no

Answer: B

NEW QUESTION 136

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 140

- (Topic 6)

You have a Microsoft 365 subscription.

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

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

Answer: A

Explanation:

Privileged access management

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

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

Reference:

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

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

NEW QUESTION 144

- (Topic 6)

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Office 365. You have the policies shown in the following table.

Name	Type
Policy1	Anti-phishing
Policy2	Anti-spam
Policy3	Anti-malware
Policy4	Safe Attachments

All the policies are configured to send malicious email messages to quarantine. Which policies support a customized quarantine retention period?

- A. Policy1 and Policy2 only
- B. Policy2 and Policy4 only
- C. Policy3 and Policy4 only
- D. Policy1 and Policy3only

Answer: A

NEW QUESTION 148

- (Topic 6)

You have a Microsoft 365 subscription.

You need to add additional onmicrosoft.com domains to the subscription. The additional domains must be assignable as email addresses for users.

What is the maximum number of onmicrosoft.com domains the subscription can contain?

- A. 1
- B. 2
- C. 5
- D. 10

Answer: C

Explanation:

You are limited to five onmicrosoft.com domains in your Microsoft 365 environment, so make sure to check for spelling and to assess your need if you choose to create a new one.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/setup/domains-faq>

NEW QUESTION 151

- (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.

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 152

- (Topic 6)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. Your company purchases a Microsoft 365 subscription.

You need to ensure that User1 is assigned the required role to create file policies and manage alerts in the Cloud App Security admin center.

Solution: From the Azure Active Directory admin center, you assign the Compliance administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Answer: A

NEW QUESTION 157

- (Topic 6)

You have a Microsoft 365 tenant that contains a Windows 10 device. The device is onboarded to Microsoft Defender for Endpoint.

From Microsoft Defender Security Center, you perform a security investigation. You need to run a PowerShell script on the device to collect forensic information.

Which action should you select on the device page?

A. Initiate Live Response Session

B. Initiate Automated Investigation

C. Collect investigation package

D. Go hunt

Answer: A

Explanation:

Reference:

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

NEW QUESTION 162

HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription.

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

An Exchange Online administrator recently created a role named Role1 from a computer on the network.

You need to identify the name of the administrator by using an audit log search.

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

NOTE: Each correct selection is worth one point.

Activities to search for:

	▼
Exchange mailbox activities	
Site administration activities	
Show results for all activities	
Role administration activities	

Field to filter by:

	▼
Item	
User	
Detail	
IP address	

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Activities to search for:

▼

Exchange mailbox activities

Site administration activities

Show results for all activities

Role administration activities

Field to filter by:

▼

Item

User

Detail

IP address

NEW QUESTION 164

HOTSPOT - (Topic 6)

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

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

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

SharePoint

S

Site1

Share

Search Documents

+ New

↑ Upload

Quick edit

Sync

⋮

All Documents

Filter

Info

Edit

Documents

Name

Modified

Modified By

+ Add column

File1.docx

About a minute ago

Prvi

File2.docx

A few seconds ago

Prvi

File3.docx

A few seconds ago

Prvi

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

User1:

▼

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

▼

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Passing Certification Exams Made Easy

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

User1:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

User2:

File1.docx only

File1.docx and File2.docx only

File1.docx, File2.docx, and File3.docx

NEW QUESTION 169

- (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 173

HOTSPOT - (Topic 6)
You have a Microsoft 365 E5 subscription and an Azure AD tenant named contoso.com.
All users have computers that run Windows 11, are joined to contoso.com, and are protected by using BitLocker Drive Encryption (BitLocker).
You plan to create a user named Admin1 that will perform following tasks:
• View BitLocker recovery keys.
• Configure the usage location for the users in contoso.com.
You need to assign roles to Admin1 to meet the requirements. The solution must use the principle of least privilege. Which two roles should you assign? To answer, select the appropriate roles in the answer area.
NOTE: Each correct selection is worth one point

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Devices

- ☐ Cloud Device Administrator ⓘ
- ☐ Desktop Analytics Administrator ⓘ
- ☐ Intune Administrator ⓘ
- ☐ Printer Administrator ⓘ
- ☐ Printer Technician ⓘ
- ☐ Windows 365 Administrator ⓘ

Global

- ☐ Global Administrator ⓘ

Identity

- ☐ Application Administrator ⓘ
- ☐ Application Developer ⓘ
- ☐ Authentication Administrator ⓘ
- ☐ Cloud Application Administrator ⓘ
- ☐ Conditional Access Administrator ⓘ
- ☐ Domain Name Administrator ⓘ
- ☐ External Identity Provider Administrator ⓘ
- ☐ Guest Inviter ⓘ
- ☐ Helpdesk Administrator ⓘ
- ☐ Hybrid Identity Administrator ⓘ
- ☐ License Administrator ⓘ
- ☐ Password Administrator ⓘ

NEW QUESTION 176

- (Topic 6)

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

Policy1

Edit policy

Delete policy

Status

On

Description

Add a description

Severity

Medium

Edit

Category

Information governance

Conditions

Activity is FileModified

Aggregation

Aggregated

Threshold

5 activities

Edit

Window

60 minutes

Scope

All users

Email recipients

User1@M365x082103.onmicrosoft.com

Daily notification limit

25

Edit

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

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

Answer: D

NEW QUESTION 179

- (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:

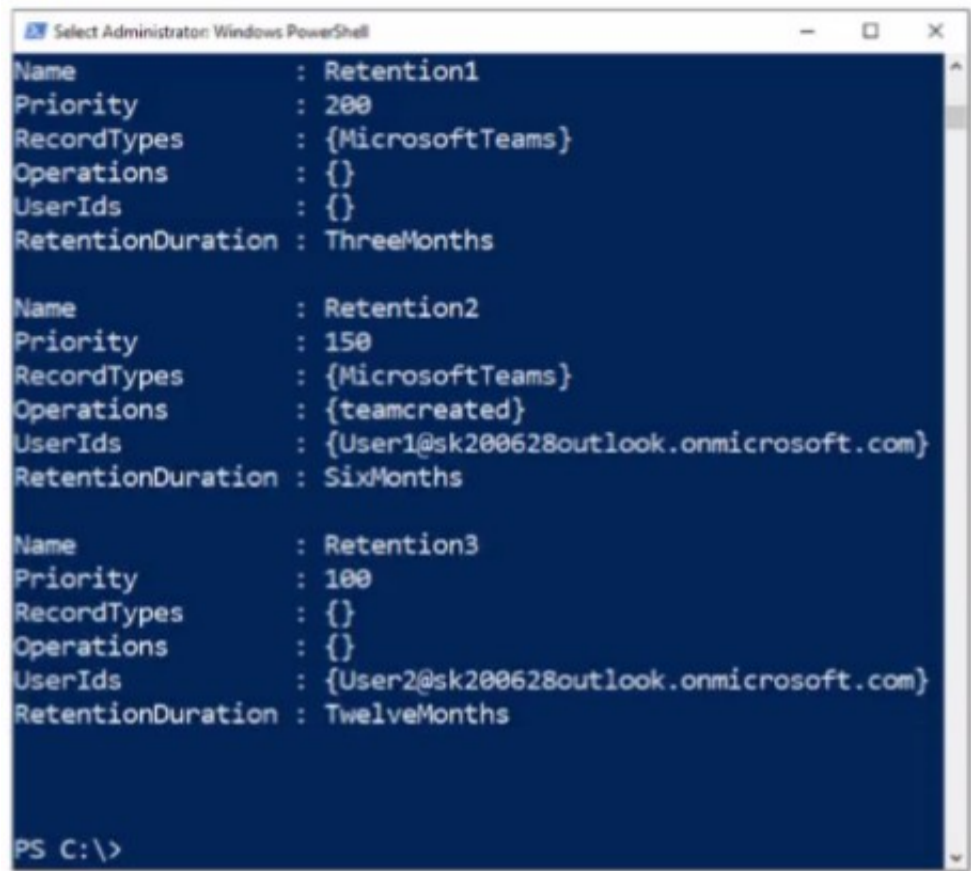
Reference:

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

NEW QUESTION 180

HOTSPOT - (Topic 6)

You have a Microsoft 365 ES subscription that has three auto retention policies as show 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

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

not retained

retained for 90 days

retained for six months

retained for one year

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

not retained

retained for 90 days

retained for six months

retained for one year

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

not retained

retained for 90 days

retained for six months

retained for one year

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

not retained

retained for 90 days

retained for six months

retained for one year

NEW QUESTION 185

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.	

NEW QUESTION 187

- (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 Active Directory forest. You deploy Microsoft 365.
 You plan to implement directory synchronization.
 You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- User passwords must be 10 characters or more.

Solution: Implement pass-through authentication and configure password protection in the Azure AD tenant. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 192

- (Topic 6)
 You have a Microsoft 365 E5 tenant.
 You need to be notified when emails with attachments that contain sensitive personal data are sent to external recipients.
 Which two policies can you use? Each correct answer presents a complete solution.
 NOTE: Each correct selection is worth one point.

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

Answer: AD

NEW QUESTION 197

- (Topic 6)

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

- Windows 10
- Android
- OS

On which devices can you configure the Endpoint DLP policies?

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

Answer: D

Explanation:

Endpoint data loss prevention (Endpoint DLP) extends the activity monitoring and protection capabilities of DLP to sensitive items that are physically stored on Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices. Once devices are onboarded into the Microsoft Purview solutions, the information about what users are doing with sensitive items is made visible in activity explorer and you can enforce protective actions on those items via DLP policies.
<https://docs.microsoft.com/en-us/microsoft-365/compliance/endpoint-dlp-learn-about?view=o365-worldwide>

NEW QUESTION 201

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 within the assignment period.

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

Box 2: No

Admin2 is member of Group2.
The Exchange Administrator role assignment has Group2 as a member. The assignment type: Eligible
June 20, 2023 is with the assignment period. The assignment must be approved.
Note: Eligible assignment requires member or owner to perform an activation to use the role. Activations may also require providing a multi-factor authentication (MFA), providing a business justification, or requesting approval from designated approvers.
Box 3: Yes
Admin3 is member of Gropu1 and Group2.
The User Administrator role assignment has Group1 as a member. The assignment type: Active
May 1, 2023 is with the assignment period.

NEW QUESTION 206

- (Topic 6)
You have a Microsoft 365 E5 tenant that contains 100 Windows 10 devices.
You plan to deploy a Windows 10 Security Baseline profile that will protect secrets stored in memory.
What should you configure in the profile?

- A. Microsoft Defender Credential Guard
- B. BitLocker Drive Encryption (BitLocker)
- C. Microsoft Defender
- D. Microsoft Defender Exploit Guard

Answer: A

NEW QUESTION 208

- (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 211

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 212

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].

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

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

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain only

contoso221018.onmicrosoft.com domain and all its subdomains only

contoso221018.onmicrosoft.com and east.contoso221018.onmicrosoft.com domains only

contoso221018.onmicrosoft.com, east.contoso221018.onmicrosoft.com, and contoso.com domains

NEW QUESTION 216

HOTSPOT - (Topic 6)

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

Passing Certification Exams Made Easy

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

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 218

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 219
HOTSPOT - (Topic 6)
Your company uses Microsoft Defender for Endpoint.
The devices onboarded to Microsoft Defender for Endpoint are shown in the following table.

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

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

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

You create a suppression rule that has the following settings:

- Triggering IOC: Any IOC
- Action: Hide alert
- Suppression scope: Alerts on ATP1 device group

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

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
After you create the suppression rule, Alert1 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, Alert3 is visible in the alerts queue.	<input checked="" type="radio"/>	<input type="radio"/>
After you create the suppression rule, a new alert triggered on Device2 is visible in the alerts queue.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 223

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Sitel. You need to perform the following tasks:

- Create a sensitive info type named SIT1 based on a regular expression.
- Add a watermark to all new documents that are matched by SIT1.

Which two settings should you use in the Microsoft Purview compliance portal? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 226

- (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.

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

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

Solution: From the Microsoft 365 admin center, you assign SecAdmin1 the Exchange Administrator role.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You need to assign the Security Administrator role. Reference:

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

NEW QUESTION 227

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 231

- (Topic 6)

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

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

Azure AD Connect has the following settings:

? Password Hash Sync: Enabled

? Pass-through authentication: Enabled

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

Which users should you identify?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 232

- (Topic 6)

: 241

You have a Microsoft 365 tenant that contains 1,000 iOS devices enrolled in Microsoft Intune. You plan to purchase volume-purchased apps and deploy the apps to the devices. You need to track used licenses and manage the apps by using Intune. What should you use to purchase the apps?

- A. Microsoft Store for Business
- B. Apple Business Manager
- C. Apple iTunes Store
- D. Apple Configurator

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/apps/vpp-apps-ios>

NEW QUESTION 234

- (Topic 6)

You have a Microsoft 365 E5 tenant. Users store data in the following locations:

? Microsoft Teams

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

- A. 1
- B. 2
- C. 3
- D. 4

Answer: C

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

NEW QUESTION 235
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.

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Device1:

No profiles

Profile1 only

Profile4 only

Profile1 and Profile4 only

Profile1, Profile1, and Profile4 only

Device2:

No profiles

Profile1 only

Profile2 only

Profile3 only

Profile1 and Profile2 only

Profile2 and Profile3 only

NEW QUESTION 238

- (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 assign User2 the Security Reader role. You instruct User2 to sign in as user2@contoso.com.
Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

This is not a permissions issue so you do not need to assign the Security Reader role. The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION 243

- (Topic 6)

You have a Microsoft 365 E5 tenant. You configure sensitivity labels.

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

You need to ensure that the users can apply the sensitivity labels when they use Word for the web.

What should you do?

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

Answer: B

NEW QUESTION 244

DRAG DROP - (Topic 6)

DRAG DROP

You have a Microsoft 365 subscription.

In the Exchange admin center, you have a data loss prevention (DLP) policy named Policy1 that has the following configurations:

? Block emails that contain financial data.

? Display the following policy tip text: Message blocked.

From the Security & Compliance admin center, you create a DLP policy named Policy2 that has the following configurations:

? Use the following location: Exchange email.

? Display the following policy tip text: Message contains sensitive data.

? When a user sends an email, notify the user if the email contains health records.

What is the result of the DLP policies when the user sends an email? To answer, drag the appropriate results to the correct scenarios. Each result may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Results	Answer Area
The email will be blocked, and the user will receive the policy tip: Message blocked.	When the user sends an email that contains financial data and health records: <div>Result</div>
The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.	When the user sends an email that contains only financial data: <div>Result</div>
The email will be allowed, and the user will receive the policy tip: Message blocked.	
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.	
The email will be allowed, and a message policy tip will NOT be displayed.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked. If you've created DLP policies in the Exchange admin center, those policies will continue to work side by side with any policies for email that you create in the Security & Compliance Center. But note that rules created in the Exchange admin center take precedence. All Exchange mail flow rules are processed first, and then the DLP rules from the Security & Compliance Center are processed.

Box 2: The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

NEW QUESTION 245

- (Topic 6)

Your on-premises network contains an Active Directory domain.

You have a Microsoft 365 subscription.

You need to sync the domain with the subscription. The solution must meet the following requirements:

On-premises Active Directory password complexity policies must be enforced. Users must be able to use self-service password reset (SSPR) in Azure AD. What should you use?

- A. password hash synchronization
- B. Azure AD Identity Protection

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

Answer: D

Explanation:

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

NEW QUESTION 248

- (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 253

DRAG DROP - (Topic 6)
DRAG DROP
You have a Microsoft 365 E5 tenant. You need to implement compliance solutions that meet the following requirements:

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

Which solution should you use for each requirement? To answer, drag the appropriate solutions to the correct requirements. Each solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content. NOTE: Each correct selection is worth one point.

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Capture employee communications for examination by designated reviewers:

Use a file plan to manage retention labels:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Solutions

Data loss prevention

Information governance

Insider risk management

Records management

Answer Area

Identify, monitor, and automatically protect sensitive information:

Data loss prevention

Capture employee communications for examination by designated reviewers:

Insider risk management

Use a file plan to manage retention labels:

Information governance

NEW QUESTION 254

HOTSPOT - (Topic 6)
You have several devices enrolled in Microsoft Endpoint Manager. You have a Microsoft Azure Active Directory (Azure AD) tenant that includes the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

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

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 259

- (Topic 6)

You have a Microsoft 365 subscription.

You have a data loss prevention (DLP) policy that blocks sensitive data from being shared in email messages.

You need to modify the policy so that when an email message containing sensitive data is sent to both external and internal recipients, the message is only prevented from being delivered to the external recipients.

What should you modify?

- A. the policy rule exceptions
- B. the DLP policy locations
- C. the policy rule conditions
- D. the policy rule actions

Answer: C

NEW QUESTION 261

HOTSPOT - (Topic 6)

You have a Microsoft 365 E5 tenant that contains 500 Windows 10 devices and a Windows 10 compliance policy.

You deploy a third-party antivirus solution to the devices.

You need to ensure that the devices are marked as compliant.

Which three settings should you modify in the compliance policy? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured
Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured
Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

NEW QUESTION 264

- (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 Active Directory domain. You deploy an Azure AD tenant.

Another administrator configures the domain to synchronize to Azure AD.

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

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

You need to ensure that the 10 user accounts are synchronized to Azure AD. Solution: From the Synchronization Rules Editor, you create a new outbound synchronization rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

Reference:

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

NEW QUESTION 266

HOTSPOT - (Topic 6)

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

Name	Role	Office 365 role group
User1	None	Compliance Data Administrator
User2	Global Administrator	None

You create a retention label named Label 1 that has the following configurations:

- Retains content for five years
- Automatically deletes all content that is older than five years

You turn on Auto labeling for Label1 by using a policy named Policy1. Policy1 has the following configurations:

- Applies to content that contains the word Merger
- Specifies the OneDrive accounts and SharePoint sites locations

You run the following command.

Set-RetentionCompliancePolicy Policy1 -RestrictiveRetention Strue -Force

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 add Exchange email as a location to Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input type="radio"/>
User2 can add the word Acquisition to Policy1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can add Exchange email as a location to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can remove SharePoint sites from Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can add the word Acquisition to Policy1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 270

HOTSPOT - (Topic 6)

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

The subscription has the following two anti-spam policies:

- Name: AntiSpam1
- Priority: 0
- Include these users, groups and domains
 - o Users: User3
 - o Groups: Group1
- Exclude these users, groups and domains
 - o Groups: Group2
- Message limits
 - o Set a daily message limit 100
- Name: AntiSpam2
- Priority: 1
- Include these users, groups and domains
 - o Users: User1
 - o Groups: Group2
- Exclude these users, groups and domains
 - o Users: User3
- Message limits
 - o Set a daily message limit 50

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 send a maximum of 150 email messages per day.	<input type="radio"/>	<input type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can send a maximum of 150 email messages per day.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can send a maximum of 50 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can send a maximum of 100 email messages per day.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 271

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
<div><div><div>Start-ADSyncSyncCycle</div><div>Start-ADSyncSyncCycle</div><div>Set-ADSyncScheduler</div><div>Invoke-ADSyncRunProfile</div></div><div>-PolicyType</div><div><div>Delta</div><div>Delta</div><div>Initial</div><div>Full</div></div></div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area
<div><div><div>Start-ADSyncSyncCycle</div><div>Start-ADSyncSyncCycle</div><div>Set-ADSyncScheduler</div><div>Invoke-ADSyncRunProfile</div></div><div>-PolicyType</div><div><div>Delta</div><div>Delta</div><div>Initial</div><div>Full</div></div></div>

NEW QUESTION 273

- (Topic 6)

You have a new Microsoft 365 E5 tenant. You need to enable an alert policy that will be triggered when an elevation of Microsoft Exchange Online administrative privileges is detected. What should you do first?

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

Answer: A

Explanation:

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

Example: Elevation of Exchange admin privilege

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

Reference:

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

NEW QUESTION 276

- (Topic 6)

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

In the Microsoft Endpoint Manager admin center, you discover many stale and inactive devices.

You enable device clean-up rules.

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

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

Answer: D

NEW QUESTION 280

- (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 285

- (Topic 6)

Your company has three main offices and one branch office. The branch office is used for research.

The company plans to implement a Microsoft 365 tenant and to deploy multi-factor authentication.

You need to recommend a Microsoft 365 solution to ensure that multi-factor authentication is enforced only for users in the branch office.

What should you include in the recommendation?

- A. Azure AD password protection
- B. a Microsoft Intune device configuration profile
- C. a Microsoft Intune device compliance policy
- D. Azure AD conditional access

Answer: D

NEW QUESTION 286

- (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 291

HOTSPOT - (Topic 6)

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure AD by using the Azure AD Connect Express Settings. Password write back is disabled.

You create a user named User1 and enter Pass in the Password field as shown in the following exhibit.

New Object - User



Create in: Adatum.com/

Password:

Confirm password:

☐ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

< Back

Next >

Cancel

The Azure AD password policy is configured as shown in the following exhibit. Password policy Set the password policy for all users in your organization. Days before passwords expire 90 Days before a user is notified about 14 expiration You confirm that User1 is synced to Azure AD. 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 sign in to Azure AD.	<input type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 can sign in to Azure AD.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can change the password immediately by using the My Apps portal.	<input type="radio"/>	<input checked="" type="radio"/>
From Azure AD, User1 must change the password every 90 days.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 295

HOTSPOT - (Topic 6)

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

Name	Role
User1	Global Administrator
User2	Billing Administrator
User3	None

You enable self-service password reset for all users. You set Number of methods required to reset to 1, and you set Methods available to users to Security questions only.

What information must be configured for each user before the user can perform a self- service password reset? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User1:
Email address only
Phone number only
Security questions only
Phone number and email address

User2:
Email address only
Phone number only
Security questions only
Phone number and email address

User3:
Email address only
Phone number only
Security questions only
Phone number and email address

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

User1:
Email address only
Phone number only
Security questions only
Phone number and email address

User2:
Email address only
Phone number only
Security questions only
Phone number and email address

User3:
Email address only
Phone number only
Security questions only
Phone number and email address

NEW QUESTION 297

- (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 301

- (Topic 6)

You purchase a new computer that has Windows 10, version 21H1 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 21H1 and the latest quality update only.
- B. Install the latest feature update and all the quality updates released since version 21H1.
- C. Install the latest feature update and the latest quality update only.
- D. Install all the feature updates released since version 21H1 and all the quality updates released since version 21H1 only.

Answer: C

NEW QUESTION 306

DRAG DROP - (Topic 6)

You have a Microsoft 365 subscription.

You need to review reports to identify the following:

- The storage usage of files stored in Microsoft Teams
- The number of active users per team

Which report should you review for each requirement? To answer, drag the appropriate reports to the correct requirements. Each report 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

Report	Requirements
The device usage report in Teams	The storage usage of files stored in Microsoft Teams:
The OneDrive usage report	Number of active users per Microsoft Team:
The SharePoint site usage report	
The Teams usage report in Teams	
The User activity report in Teams	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Report	Requirements
The device usage report in Teams	The storage usage of files stored in Microsoft Teams: The SharePoint site usage report
The OneDrive usage report	Number of active users per Microsoft Team: The Teams usage report in Teams
The SharePoint site usage report	
The Teams usage report in Teams	
The User activity report in Teams	

NEW QUESTION 311

- (Topic 6)

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

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

- A. Windows 11 and Windows 10 only
- B. Windows 11, Windows 10-Windows8.1.andmacOS
- C. Windows 11 and macOS only
- D. Windows 11 only
- E. Windows 11. Windows 10, and Windows8.1 only

Answer: C

NEW QUESTION 316

- (Topic 6)

You have a Microsoft 365 subscription. You add a domain named contoso.com.

When you attempt to verify the domain, you are prompted to send a verification email to admin@contoso.com.

You need to change the email address used to verify the domain. What should you do?

- A. From the Microsoft 365 admin center, change the global administrator of the Microsoft 365 subscription.
- B. Add a TXT record to the DNS zone of the domain.
- C. From the domain registrar, modify the contact information of the domain.
- D. Modify the NS records for the domain.


Answer: C

NEW QUESTION 319

HOTSPOT - (Topic 6)

You have a Microsoft 365 ES tenant.
You have the alerts shown in the following exhibit.

View alerts



Export

Filter

<input type="checkbox"/>	Severity	Alert name	Status	Tags	Category	Activity count	Last occurrence...
<input type="checkbox"/>	Medium	Alert1	Active	-	Threat management	2	3 minutes ago
<input type="checkbox"/>	High	Alert5	Resolved	-	Permissions	1	8 minutes ago

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

Answer Area

For Alert1, you can change Status to

Investigating only

Investigating or Resolved only

Investigating or Dismissed only

Investigating, Resolved, or Dismissed

For Alert5, you can

not change Status

change Status to Dismissed only

change Status to Dismissed or Active only

change Status to Dismissed or Investigating only

change Status to Dismissed, Investigating, or Active

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

For Alert1, you can change Status to

Investigating only

Investigating or Resolved only

Investigating or Dismissed only

Investigating, Resolved, or Dismissed

For Alert5, you can

not change Status

change Status to Dismissed only

change Status to Dismissed or Active only

change Status to Dismissed or Investigating only

change Status to Dismissed, Investigating, or Active

NEW QUESTION 321

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 322


HOTSPOT - (Topic 6)

You have a Microsoft 365 subscription that contains three groups named All users, Sales team, and Office users, and two users shown in the following table.

Name	Member of
User1	All users, Sales team
User2	All users, Office users

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

Home / Policy Management

 Notifications

Policy configurations


Create

Copy

Reorder priority

Remove

Total policy configurations: 3

Name	Priority 	Recommendation status
Office Users Policy	0	
Sales Team Policy	1	
All users	2	

The policies use the settings shown in the following table.

Policy	Default Shared Folder Location	Default Office Theme
All users	https://sharepoint.contoso.com/addins_all_users	Colorful
Office Users Policy	https://sharepoint.contoso.com/addins_office_users	White
Sales Team Policy	https://sharepoint.contoso.com/addins_sales_team_users_	Dark Gray

What is the default share folder location for User1 and the default Office theme for User2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

Colorful

Dark Gray

White

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

The default Office theme for User 2 is:

Colorful

Dark Gray

White

NEW QUESTION 324

- (Topic 6)
You have a Microsoft 365 E5 subscription.
You need to identify which users accessed Microsoft Office 365 from anonymous IP addresses during the last seven days.
What should you do?

- A. From the Cloud App Security admin center, select Users and accounts.
- B. From the Microsoft 365 security center, view the Threat tracker.
- C. From the Microsoft 365 admin center, view the Security & compliance report.
- D. From the Azure Active Directory admin center, view the Risky sign-ins report.

Answer: A

NEW QUESTION 328

HOTSPOT - (Topic 6)
HOTSPOT
You have a Microsoft 365 tenant.
You create a retention label as shown in the Retention Label exhibit. (Click the Retention Label tab.)

Create retention label

✓ Name

✓ Retention settings

● Finish

Review and finish

Name

Name

6Months

Edit

Retention settings

Retention period

6 months

Edit

Retention action

Retain and Delete

Edit

Based on

Based on when it was created

Edit

Back

Create label

Cancel

You create a label policy as shown in the Label Policy exhibit. (Click the Label Policy tab.)

Auto-labeling > Create auto-labeling policy

✓ Name

● Info to label

● Create content query

○ Scope

○ Label

○ Finish

Apply label to content matching this query

Conditions

ProjectX

+ Add condition

Back

Next

Cancel

The label policy is configured as shown in the following table.

Configuration	Value
Label to auto-apply	6Months
Locations	Exchange email

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
Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input type="radio"/>
Any sent email message that contains the word ProjectX will be retained for six months.	<input type="radio"/>	<input type="radio"/>
Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- Box 1: No
- Box 2: Yes
- Box 3: No

NEW QUESTION 331
- (Topic 6)

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

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

You plan to enable VPN access for the devices.
 What is the minimum number of configuration policies required?

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

Answer: D

NEW QUESTION 336

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

85

to

100

Instance count

2

to

Any

Add

Create group

+ Add condition

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.

Passing Certification Exams Made Easy

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

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 checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File2.txt.	<input checked="" type="radio"/>	<input type="radio"/>
Sensitivity1 is applied to File3.xlsx.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 339
HOTSPOT - (Topic 5)
You are evaluating the use of multi-factor authentication (MFA).
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
Users will have 14 days to register for MFA after they sign in for the first time.	<input type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input type="radio"/>	<input type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Users will have 14 days to register for MFA after they sign in for the first time.	<input checked="" type="radio"/>	<input type="radio"/>
Users must use the Microsoft Authenticator app to complete MFA.	<input checked="" type="radio"/>	<input type="radio"/>
After registering, users must use MFA for every sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 343

HOTSPOT - (Topic 5)

You need to ensure that the Microsoft 365 incidents and advisories are reviewed monthly.

Which users can review the incidents and advisories, and which blade should the users use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users:

Admin1 and Admin3 only	▼
Admin1 only	
Admin1 and Admin3 only	
Admin1, Admin2, and Admin3 only	
Admin1, Admin2, Admin3, and Admin4	

Blade:

Service Health	▼
Reports	
Service Health	
Message center	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Users:

Admin1 and Admin3 only	▼
Admin1 only	
Admin1 and Admin3 only	
Admin1, Admin2, and Admin3 only	
Admin1, Admin2, Admin3, and Admin4	

Blade:

Service Health	▼
Reports	
Service Health	
Message center	

NEW QUESTION 348

- (Topic 4)

You are evaluating the required processes for Project1.

You need to recommend which DNS record must be created while adding a domain name for the project.

Which DNS record should you recommend?

- A. host (A)
- B. host information
- C. text (TXT)
- D. alias (CNAME)

Answer: D

Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.

Note:

There are several versions of this question in the exam. The question has two possible correct answers:

Text (TXT)

Mail exchanger (MX)

incorrect answer options you may see on the exam include the following: alias (CNAME)

Host (A) host (AAA)

Pointer (PTR) Name Server (NS)

host information (HINFO) pointer (PTR)

Reference:

<https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider>

NEW QUESTION 350

- (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 351

- (Topic 3)

You create the planned DLP policies.

You need to configure notifications to meet the technical requirements. What should you do?

- A. From the Microsoft 365 security center, configure an alert policy.
- B. From the Microsoft Endpoint Manager admin center, configure a custom notification.
- C. From the Microsoft 365 admin center, configure a Briefing email.
- D. From the Microsoft 365 compliance center, configure the Endpoint DLP settings.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 354

HOTSPOT - (Topic 3)

You need to ensure that User2 can review the audit logs. The solutions must meet the technical requirements.

To which role group should you add User2, and what should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role group:

	▼
Reviewer	
Global reader	
Data Investigator	
Compliance Management	

Tool:

	▼
Exchange admin center	
SharePoint admin center	
Microsoft 365 admin center	
Microsoft 365 security center	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Role group:

▼
Reviewer
Global reader
Data Investigator
Compliance Management

Tool:

▼
Exchange admin center
SharePoint admin center
Microsoft 365 admin center
Microsoft 365 security center

NEW QUESTION 358

- (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 363

- (Topic 3)

You need to configure the compliance settings to meet the technical requirements. What should you do in the Microsoft Endpoint Manager admin center?

- A. From Compliance policies, modify the Notifications settings.
- B. From Locations, create a new location for noncompliant devices.
- C. From Retire Noncompliant Devices, select Clear All Devices Retire State.
- D. Modify the Compliance policy settings.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 364

- (Topic 2)

You need to meet the technical requirement for the EU PII data. What should you create?

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

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies>

EU PII wants both documents and email message to be preserved so S&C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

NEW QUESTION 368

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 369

- (Topic 2)
You need to recommend a solution for the security administrator. The solution must meet the technical requirements.
What should you include in the recommendation?

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

Answer: B

Explanation:

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

NEW QUESTION 372

DRAG DROP - (Topic 2)
You need to meet the requirement for the legal department.
Which three actions should you perform in sequence from the Security & Compliance admin center? 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
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References: <https://www.sherweb.com/blog/ediscovery-office-365/>

NEW QUESTION 373

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

- A. Server1
- B. Server2
- C. Server3
- D. Server4

E. Servers5

Answer: A

Explanation:

However, if the case study had required that the DCs can't have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

NEW QUESTION 377

- (Topic 2)

Which report should the New York office auditors view?

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

Answer: C

Explanation:

References:

<https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies>

This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

NEW QUESTION 382

- (Topic 2)

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

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

Answer: A

NEW QUESTION 383

HOTSPOT - (Topic 1)

As of March, how long will the computers in each office remain supported by Microsoft? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Seattle:

6 months
18 months
24 months
30 months
5 years

New York:

6 months
18 months
24 months
30 months
5 years

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> March Feature Updates: Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date

References:

<https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>

NEW QUESTION 386

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

MS-102 Practice Exam Features:

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

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