Microsoft.MS-500.v2023-06-13.q127

Exam Code:	MS-500
Exam Name:	Microsoft 365 Security Administration
Certification Provider:	Microsoft
Free Question Number:	127
Version:	v2023-06-13
# of views:	1636
# of Questions views:	1270
https://www.freepdfdumps.com/Microsoft.MS-500.v2023-06-13.q127.html	

NEW QUESTION: 1
You need to create Group2.
What are two possible ways to create the group?
A. a security group in the Azure AD admin center
B. an Office 365 group in the Microsoft 365 admin center
C. a distribution list in the Microsoft 365 admin center
D. a mail-enabled security group in the Microsoft 365 admin center
E. a security group in the Microsoft 365 admin center
Answer: A,E (LEAVE A REPLY)

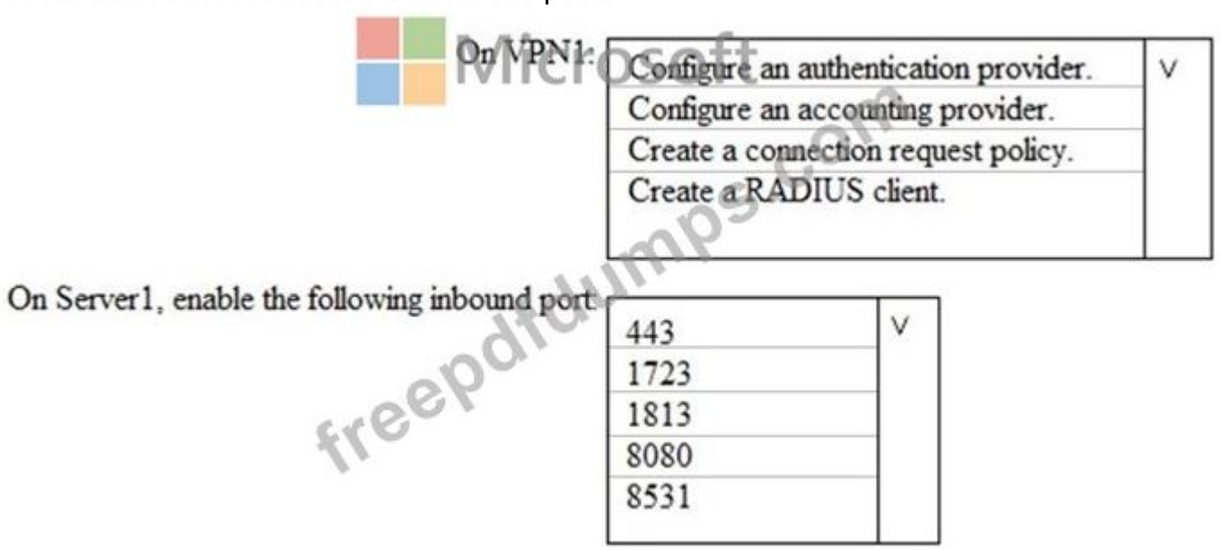
NEW QUESTION: 2
You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Endpoint Manager.
You need to enable Microsoft Defender Exploit Guard (Microsoft Defender EG) on the devices.
Which type of device configuration profile should you use?
A. Endpoint protection
B. Device restrictions
C. identity protection
D. Microsoft Defender for Endpoint
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3
You have a Microsoft 365 E5 subscription.
Some users are required to use an authenticator app to access Microsoft SharePoint Online.
You need to view which users have used an authenticator app to access SharePoint Online. The solution must minimize costs.
What should you do?
A. From the Azure Active Directory admin center, view the sign-ins.
B. From the Security & Compliance admin center, download a report.

C. From the Azure Active Directory admin center, view the authentication methods.
D. From the Azure Active Directory admin center, view the audit logs.
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

NEW QUESTION: 4
You have a Microsoft 365 subscription.
You need to be notified by email whenever an administrator starts an eDiscovery search.
What should you do from the Security & Compliance admin center?
A. From Search & investigation, create a guided search.
B. From Events, create an event.
C. From Alerts, create an alert policy.
D. From Search & Investigation, create an eDiscovery case.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION: 5
Your network contains an Active Directory domain named contoso.com. The domain contains a VPN server named VPN1 that runs Windows Server 2016 and has the Remote Access server role installed.
You have a Microsoft Azure subscription.
You are deploying Azure Advanced Threat Protection (ATP)
You install an Azure ATP standalone sensor on a server named Server1 that runs Windows Server 2016.
You need to integrate the VPN and Azure ATP.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

On VPN1:

Configure an authentication provider.	V
Configure an accounting provider.	
Create a connection request policy.	
Create a RADIUS client.	

On Server1, enable the following inbound port:

443	V
1723	
1813	
8080	
8531	

Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step6-vpn

NEW QUESTION: 6
You have a hybrid Microsoft 365 environment.
All computers run Windows 10 Enterprise and have Microsoft Office 365 ProPlus installed. All the computers are joined to Active Directory.
You have a server named Server1 that runs Windows Server 2016. Server1 hosts the telemetry database. You need to prevent private details in the telemetry data from being transmitted to Microsoft.
What should you do?
A. On Server1, run readinessreportcreator.exe
B. Configure a registry on Server1
C. Configure a registry on the computers
D. On the computers, run tdadm.exe
Answer: (SHOW ANSWER)
"To allow yourself and other administrators to identify the owners of Office files that have compatibility issues without revealing file names or specific locations, you can enable file obfuscation, which disguises Office file names, titles, and file paths. This setting is configured on the agent, which performs the obfuscation task before uploading data to the shared folder. The data that is stored on the local computer is not obfuscated." https://docs.microsoft.com/en-us/deployoffice/compat/manage-the-privacy-of-data-monitored-by-telemetry-in-office

NEW QUESTION: 7
You have a Microsoft 365 subscription that contains 100 users.
Microsoft Secure Score for the subscription is shown in the following exhibit.
Use the drop-down menus to select the answer choice that completes each statement based on the the information presented in the graphic.
NOTE: Each correct selection is worth one point.

Answer:

Answer in image below.

NEW QUESTION: 8

You are evaluating which devices are compliant in Intune.

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
Device2 is compliant.	○	○
Device5 is compliant.	○	○
Device6 is compliant.	○	○

Answer:

Statements	Yes	No
Device2 is compliant.	●	○
Device5 is compliant.	○	●
Device6 is compliant.	●	○

NEW QUESTION: 9

You have a Microsoft Defender for Endpoint deployment that has custom network indicators turned on. Microsoft Defender for Endpoint protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender foe Endpoint has the device groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp

Answer Area

Statements	Yes	No
From a web browser on Computer1, you can open http://www.contoso.com.	○	○
From a web browser on Computer1, you can open http://www.litwareinc.com/public.	○	○
From a web browser on Computer2, you can open http://www.litwareinc.com.	○	○

Answer:

NEW QUESTION: 10

A user stores the following files in Microsoft OneDrive:

File.docx

ImportantFile.docx

File_Important.docx

You create a Microsoft Cloud App Security file policy Policy1 that has the filter shown in the following exhibit.

To which files does Policy1 apply?

A. File_Important.docx only

B. File.docx, ImportantFile.docx, and File_Important.docx

C. File.docx only

D. ImportantFile.docx only

E. File.docx and File_Important.docx only
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/file-filters

NEW QUESTION: 11
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 questions 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 that contains 1,000 user mailboxes.
An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.
You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending email messages as User5.
Solution: You modify the permissions of the mailbox of User5, and then create an eDiscovery case.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

NEW QUESTION: 12
You have a Microsoft 365 subscription that uses an Azure Active Directory (Azure AD) tenant named contoso.com. OneDrive stores files that are shared with external users. The files are configured as shown in the following table.

Name	Applied label
File1	Label1
File2	Label1, Label2
File3	Label2

You create a data loss prevention (DLP) policy that applies to the content stored in OneDrive accounts. The policy contains the following three rules:
* Rulel:
* Conditions: Label 1, Detect content that's shared with people outside my organization
* Actions: Restrict access to the content for external users
* User notifications: Notify the user who last modified the content
* User overrides: On
* Priority: 0
* Rule2:
* Conditions: Label 1 or Label2
* Actions: Restrict access to the content
* Priority: 1
* Rule3:
* Conditions: Label2, Detect content that's shared with people outside my organization
* Actions: Restrict access to the content for external users

* User notifications: Notify the user who last modified the content
* User overrides: On
* Priority: 2

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

NOTE: Each correct selection is worth one point.

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
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

Answer:

Answer Area

Statements	Yes	No
External users can access File1.	○	○
The users in contoso.com can access File2.	○	○
External users can access File3.	○	○

NEW QUESTION: 13

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

Name	Group	Role
User1	Microsoft Defender for Identity Contoso Users	None
User2	Microsoft Defender for Identity Contoso Viewers	None
User3	Not applicable	Security administrator
User4	Not applicable	Security operator

You discover several security alerts are visible from the Microsoft Defender for Identity portal.
You need to identify which users m contoso.com can dose the security Alerts. Which users should you identify?
A. User1 and User2 only
B. User1 only
C. User4 only
D. User1 and User3 only
E. User3 and User4 only
Answer: (SHOW ANSWER)

NEW QUESTION: 14
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

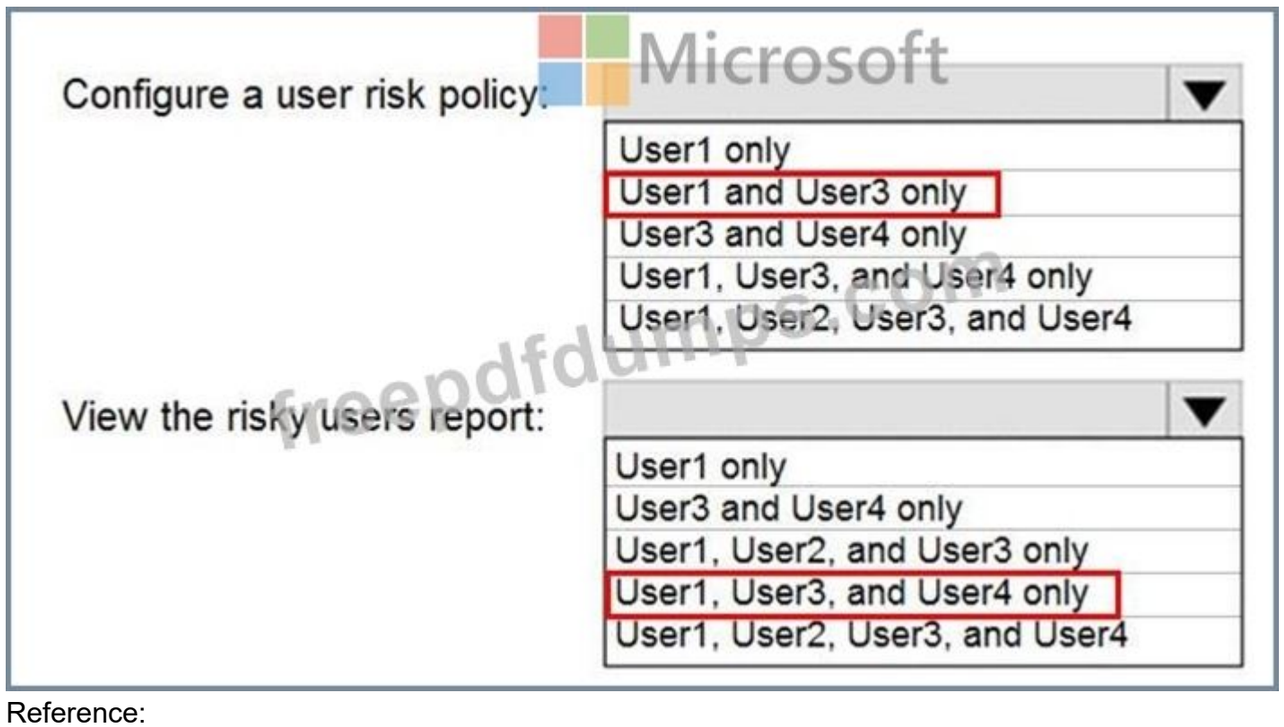
Name	Role
User1	Global administrator
User2	Compliance administrator
User3	Security administrator
User4	Security operator

You plan to implement Azure Active Directory (Azure AD) Identity Protection.
You need to identify which users can perform the following actions:
Configure a user risk policy.
View the risky users report.
Which users should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Configure a user risk policy:
- User1 only
- User1 and User3 only
- User3 and User4 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

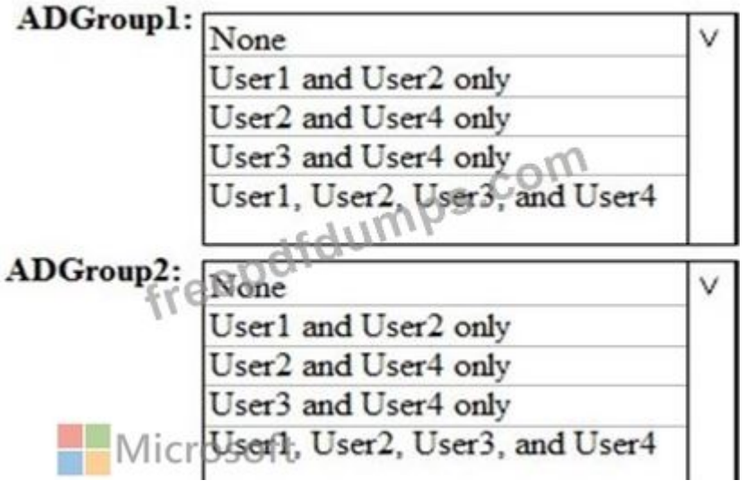
View the risky users report:
- User1 only
- User3 and User4 only
- User1, User2, and User3 only
- User1, User3, and User4 only
- User1, User2, User3, and User4

Answer:

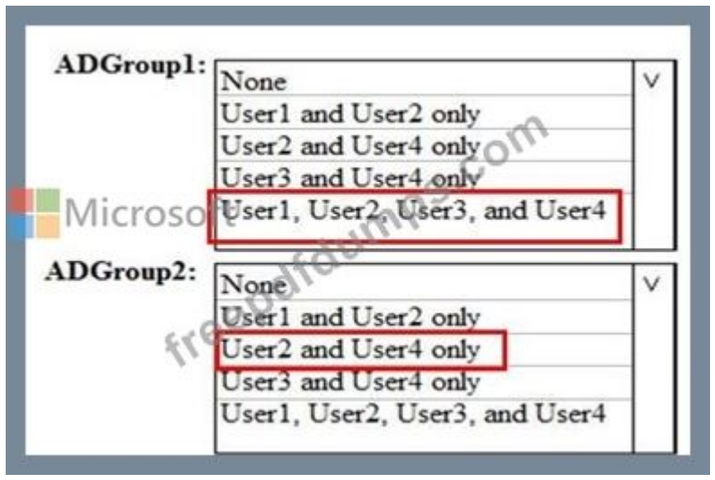


Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

NEW QUESTION: 15
Which users are members of ADGroup1 and ADGroup2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership#supported-values

NEW QUESTION: 16
Which role should you assign to User1?
A. Global administrator
B. User administrator
C. Privileged role administrator
D. Security administrator
Answer: D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim

NEW QUESTION: 17
You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager.
The Compliance policy settings are configured as shown in the following exhibit.

These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Mark devices with no compliance policy assigned as ⓘ — Compliant / **Not Compliant**

Enhanced jailbreak detection ⓘ — Enabled / **Disabled**

Compliance status validity period (days) ⓘ — 30

On February 25, 2020, you create the device compliance policies shown in the following table.

Name	Require BitLocker Drive Encryption (BitLocker)	Require Secure Boot	Mark device as not compliant	Assigned to
Policy1	Yes	No	5 days after noncompliance	Group1
Policy2	No	Yes	10 days after noncompliance	Group1, Group2

On March 1. 2020, users enroll Windows 10 devices in Microsoft Endpoint Manager as shown in the following table

Name	BitLocker enabled	Secure Boot enabled	Member of
Device1	Yes	No	Group1
Device2	No	No	Group2

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
On March 2, 2020, Device2 is marked as compliant.	○	○
On March 6, 2020, Device1 is marked as compliant.	○	○
On March 12, 2020, Device1 is marked as compliant.	○	○

Answer:

NEW QUESTION: 18

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

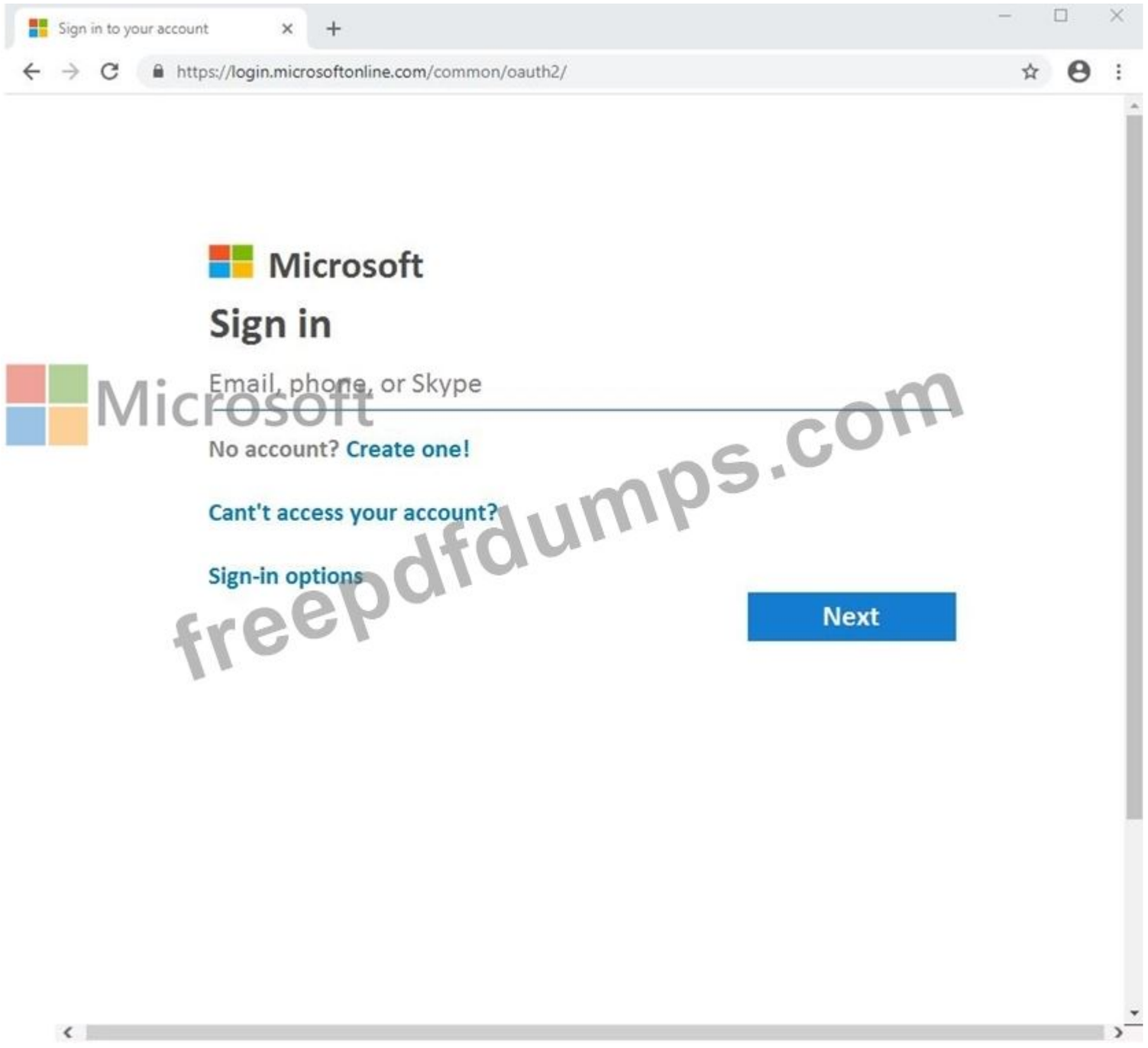
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe00019@onmicrosoft.com
Microsoft 365 Password: #HSP.ug?$p6un
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11122308

Microsoft

Get your work done
with Office 365

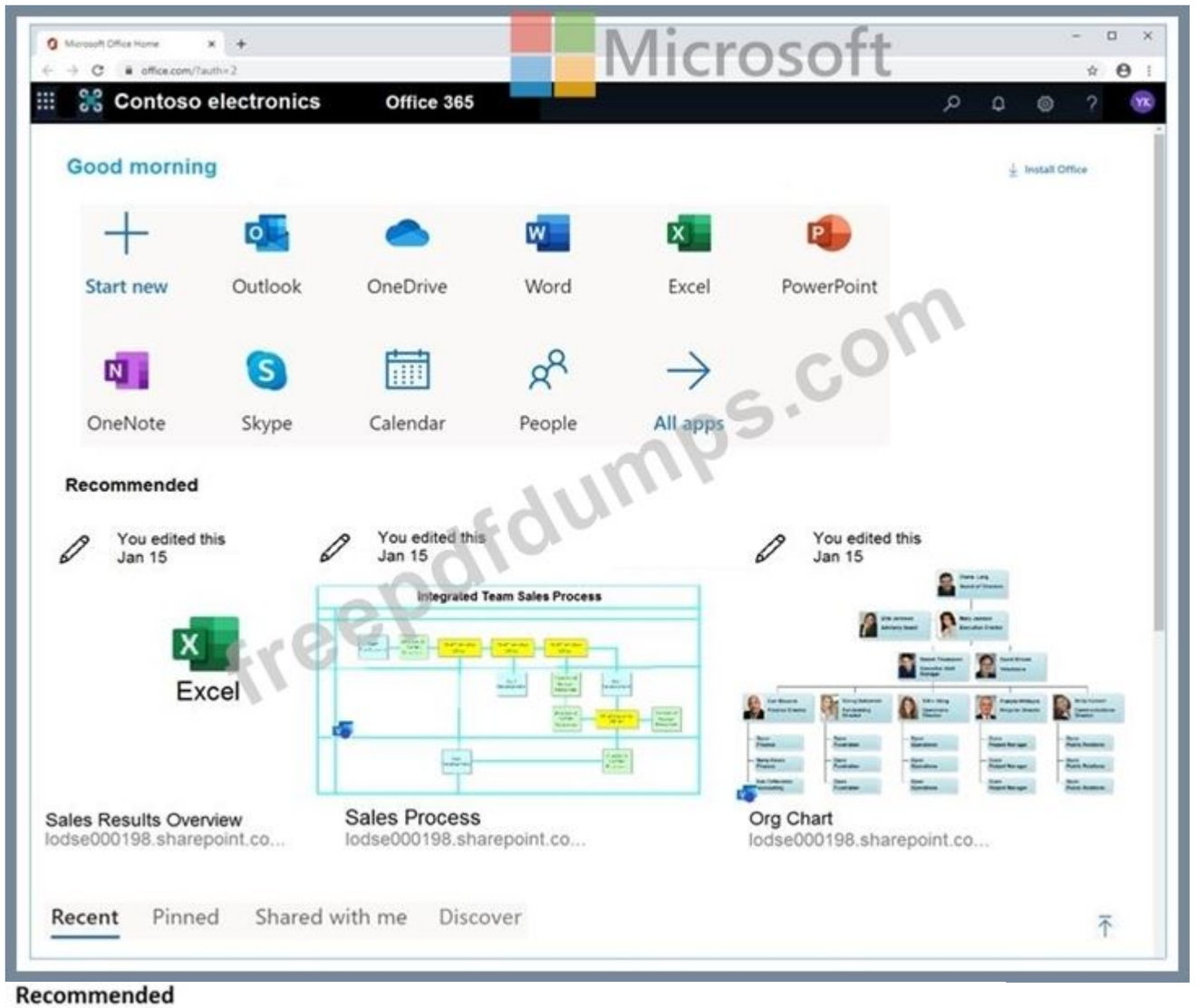
Microsoft

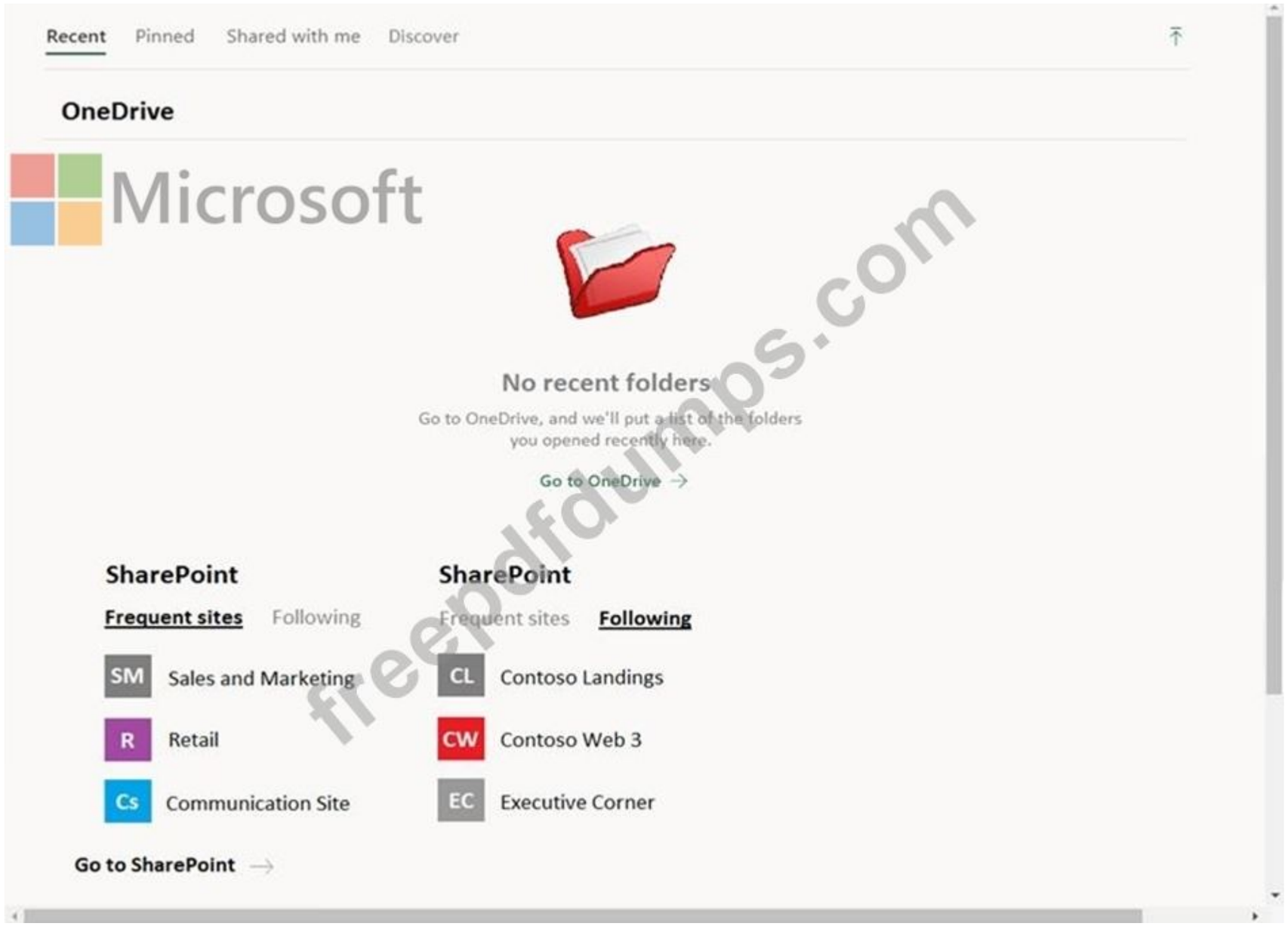
Microsoft

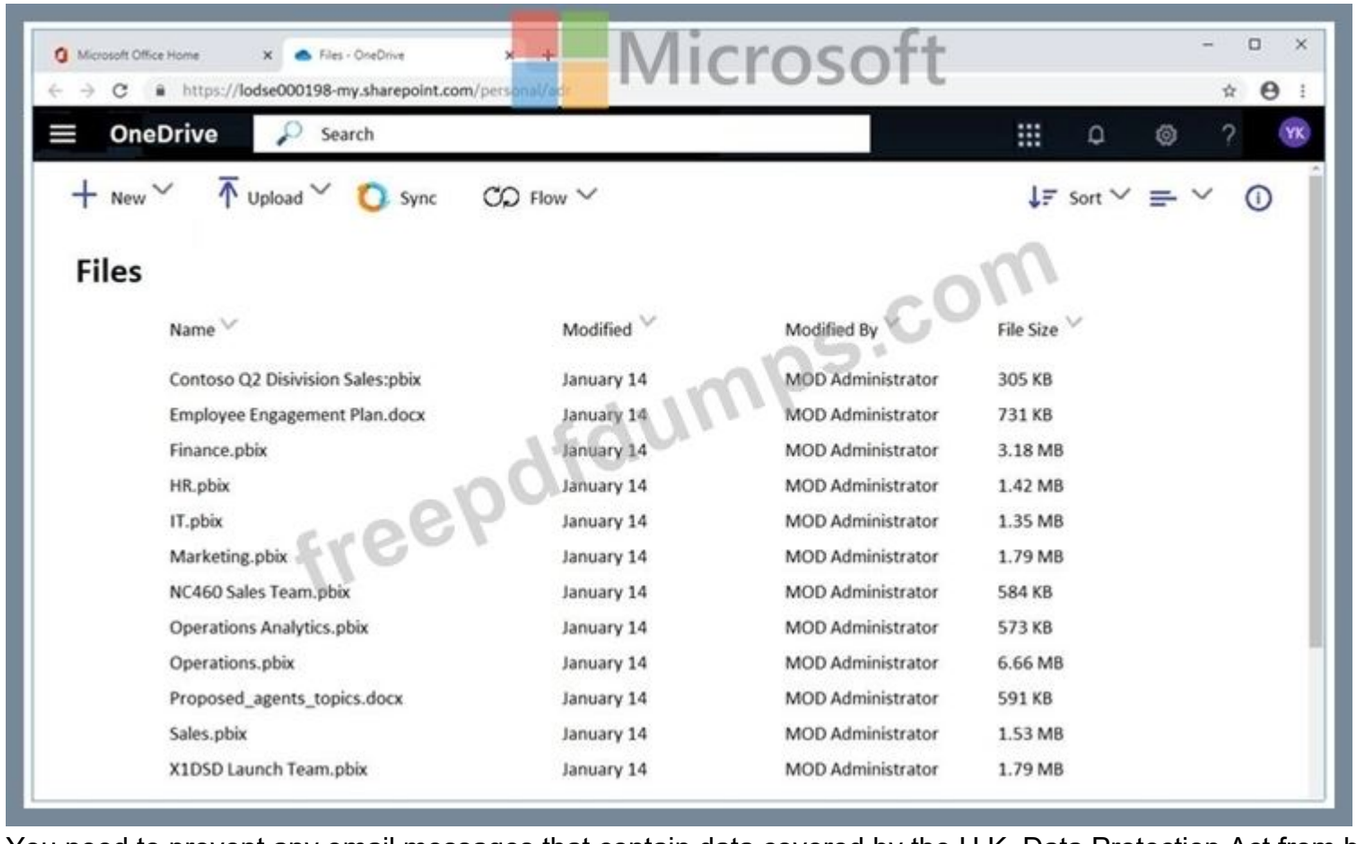
Microsoft

Access Office 365 apps and documents in one place with

Office.com







You need to prevent any email messages that contain data covered by the U.K. Data Protection Act from being sent to recipients outside of your organization, unless the messages are sent to an external domain named adatum.com.

To complete this task, sign in to the Microsoft 365 admin center.

(1) U. K. National Insurance Number (NINO

(2) U. S. / U.K. Passport Number

SWIFT Code

11. Click on Ok

12. Add an exception for recipients in the adatum.com domain

13. Add recipients for incident reports and click ok

14. Click save

15. Click save

Answer:

1. After signing into the Microsoft 365 admin center, navigate to Compliance Management in the Exchange Admin center.

2. Click on "Data Loss Prevention" option.

3. To add a new custom DLP policy, Click on (+) plus button to get the context menu

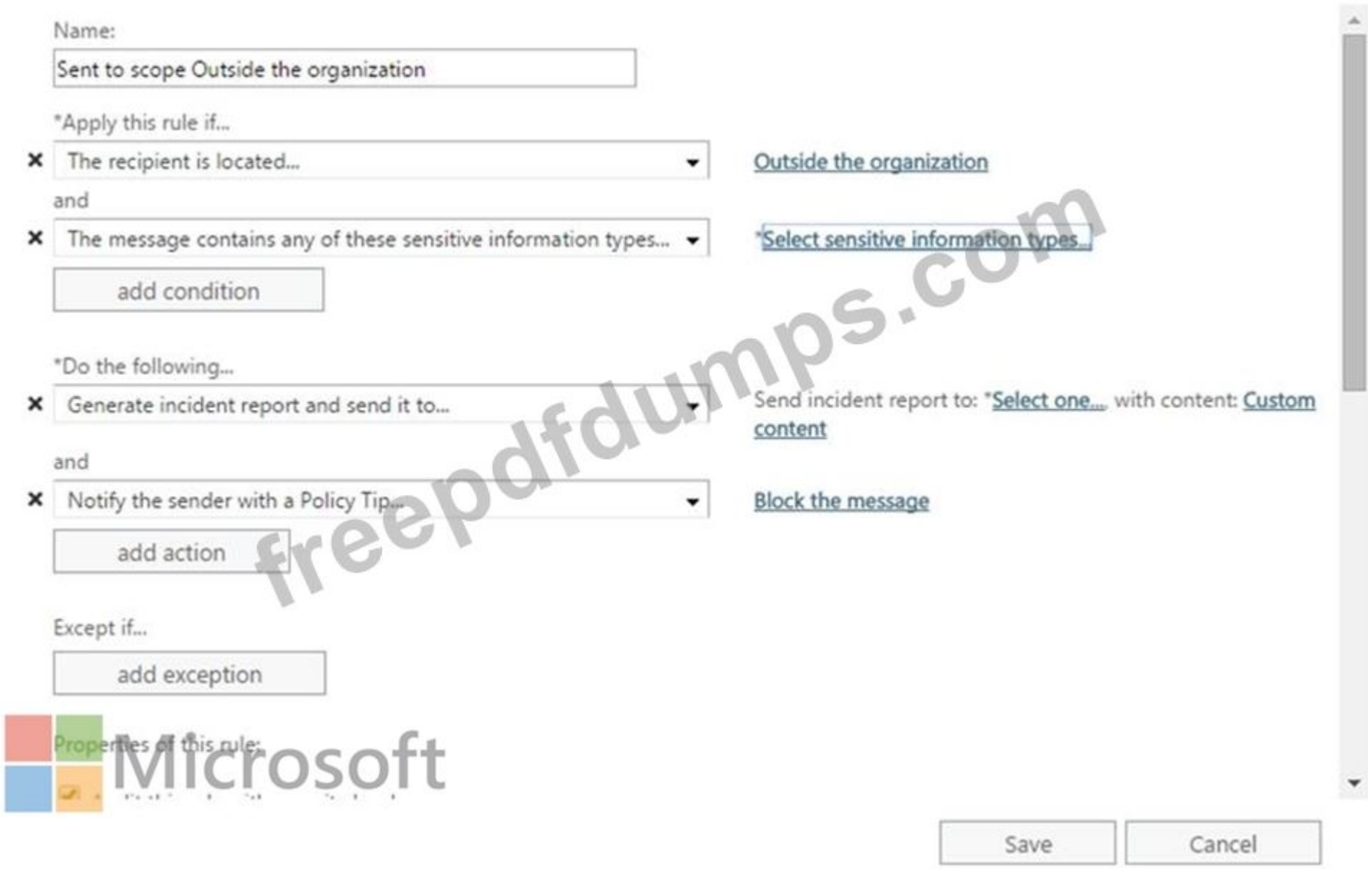
4. Click on "New Custom DLP policy" option, a new window appears where you have to enter policy name, description, state and mode of the requirement details. Click on save button to create policy and continue...

5. You will be back to the "Data Loss Prevention" screen with newly added policy information.

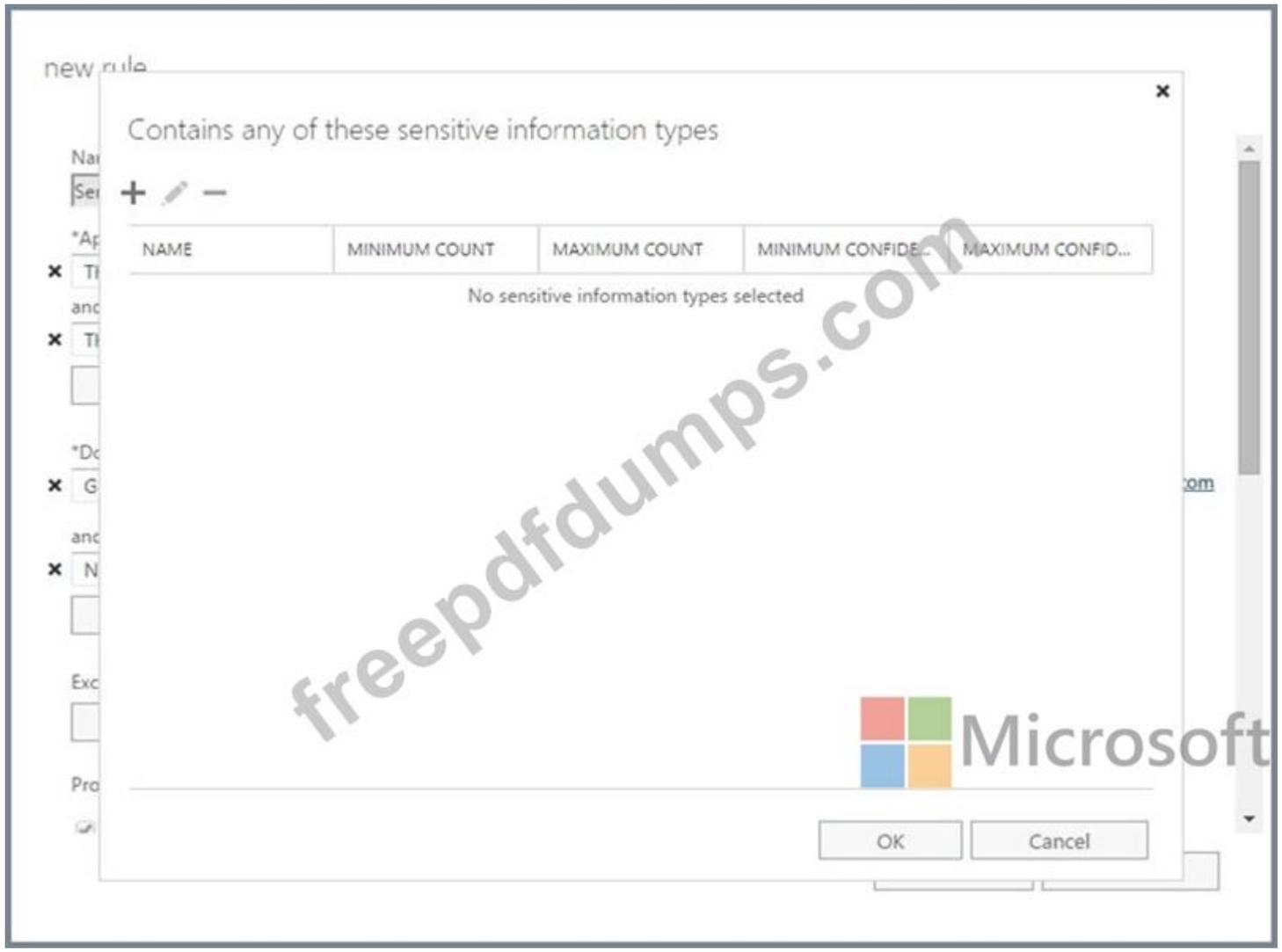
6. Double click on the added row to open the policy details, click on rules option in left part of the screen as depicted

7. Click on (+) plus button to add a new rule. Select the "Block messages with sensitive information" rule.

8. On the following screen, we can add condition, action, exceptions, rule activation and deactivation dates



9. Click on "Select Sensitive information Types" to specify the sensitive information details.



10. Click on (+) plus button and add the following Sensitive information Types:

B. Explanation

C. Explanation

D. Explanation

Reference:

https://events.collab365.community/configure-data-loss-prevention-policies-in-exchange-online-in-office-365/

NEW QUESTION: 19

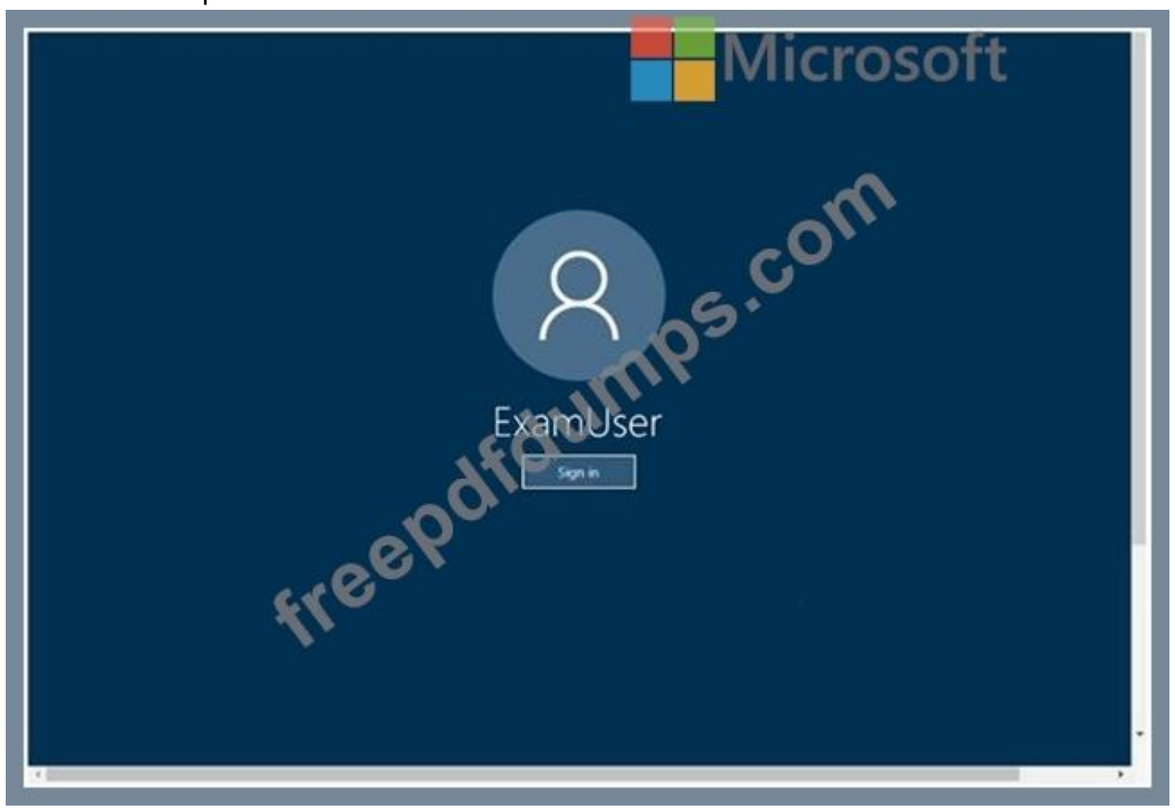
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to ensure that each user can join up to five devices to Azure Active Directory (Azure AD).
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

After signing into the Microsoft 365 admin center, click Admin centers > Azure Active Directory > Devices.
Navigate to Device Settings.
Set the Users may join devices to Azure AD setting to All.
Set the Additional local administrators on Azure AD joined devices setting to None.
Set the Users may register their devices with Azure AD setting to All.
Leave the Require Multi-Factor Auth to join devices setting on it default setting.
Set the Maximum number of devices setting to 5.
Set the Users may sync settings and app data across devices setting to All.

Click the Save button at the top left of the screen.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal
https://docs.microsoft.com/en-us/microsoft-365/compliance/use-your-free-azure-ad-subscription-in-office-365?view=o365-worldwide

NEW QUESTION: 20
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

Name	Microsoft 365 role	Role group
Admin1	Global Administrator	*None*
Admin2	Compliance admin	*None*
User3	User	Compliance Manager Contributors
User4	User	Compliance Manager Administrators
User5	User	*None*

You create an assessment named Assessment1 as shown in the following exhibit.

Which users can update the title of Assessment1, and which users can add User5 to the Compliance Manager Readers role group? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Can update the Assessment1 title:

- User4 only
- Admin2 and User4 only
- Admin1, Admin2, and User4 only
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Reader role group:

- Admin1 only
- Admin1 and Admin2 only
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

Answer:

Answer Area

Microsoft

Can update the Assessment1 title:

- User4 only
- Admin2 and User4 only
- **Admin1, Admin2, and User4 only**
- Admin1, Admin2, User3, and User4 only

Can add User5 to the Compliance Manager Reader role group:

- Admin1 only
- **Admin1 and Admin2 only**
- Admin1 and User4 only
- Admin1, Admin2, and User4 only

freepdfdumps.com

NEW QUESTION: 21

You have a Microsoft 365 subscription that uses a default domain name of contoso.com.

Microsoft Azure Active Directory (Azure AD) contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intune has two devices enrolled as shown in the following table:

Name	Platform
Device1	Android
Device2	Windows 10

Both devices have three apps named App1, App2, and App3 installed.

You create an app protection policy named ProtectionPolicy1 that has the following settings:

Protected apps: App1

Exempt apps: App2

Windows Information Protection mode: Block

You apply ProtectionPolicy1 to Group1 and Group3. You exclude Group2 from ProtectionPolicy1.

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:

NEW QUESTION: 22

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

Name	Multi-factor auth status
User1	Disabled
User2	Enabled
User3	Enforced

You configure the Security Operator role in Azure AD Privileged Identity Management (PIM) as shown in the following exhibit.

You add assignments to the Security Operator role as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Eligible
User3	Active

Which users can activate the Security Operator role?

A. User3 only

B. User2 and User3 only

C. Used and User2 only

D. User1,User2, and User3

E. User2 only

Answer: B (LEAVE A REPLY)

NEW QUESTION: 23

Your network contains an on-premises Active Directory domain named contoso.local that has a forest functional level of Windows Server 2008 R2.

You have a Microsoft 365 E5 subscription linked to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to install Azure AD Connect and enable single sign-on (SSO).

You need to prepare the domain to support SSO. The solution must minimize administrative effort.

What should you do?

A. Raise the forest functional level to Windows Server 2016.

B. Modify the UPN suffix of all domain users.

C. Populate the mail attribute of all domain users.

D. Rename the domain.

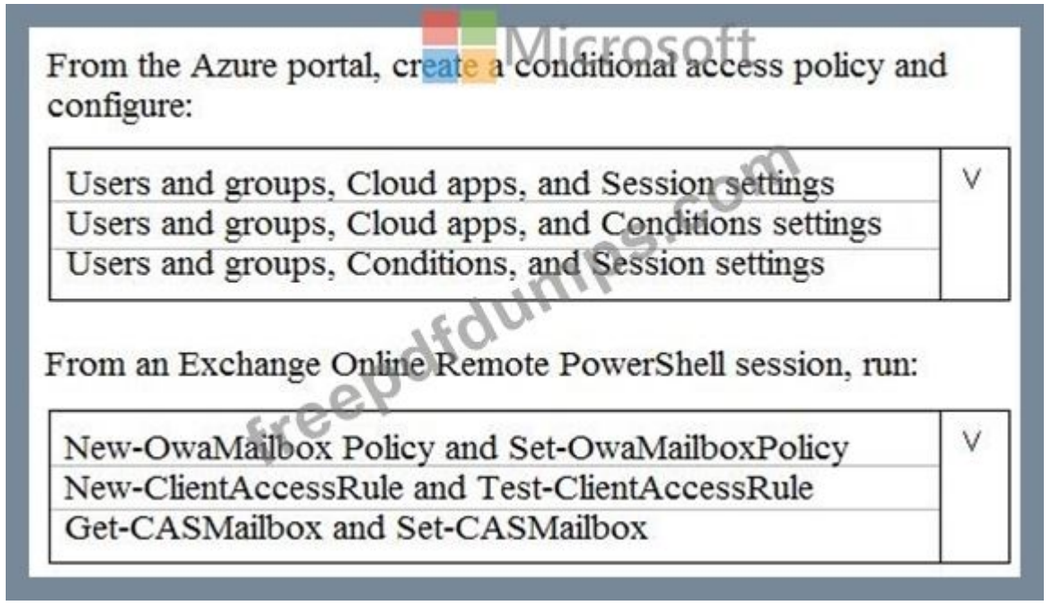
Answer: B (LEAVE A REPLY)

Reference:

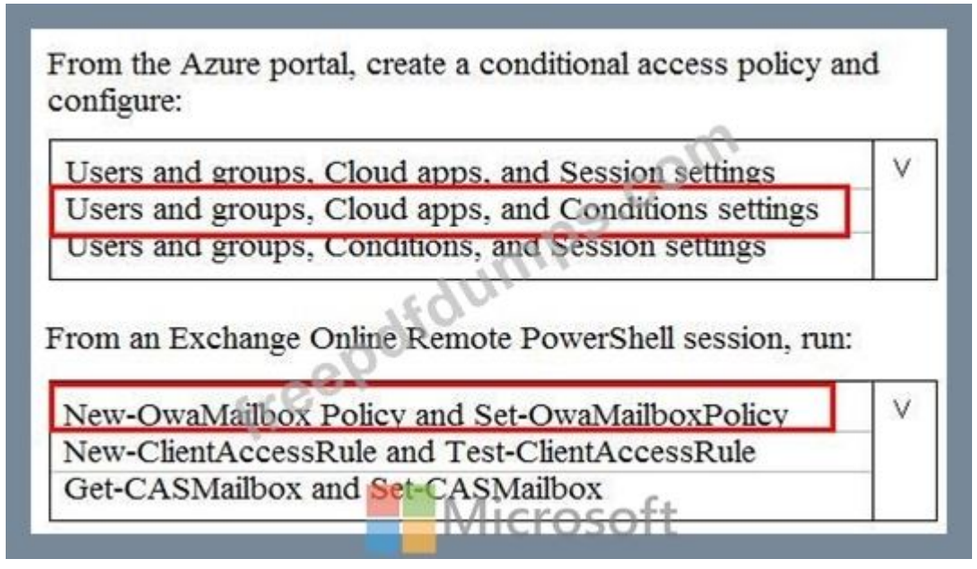
https://docs.microsoft.com/en-us/microsoft-365/enterprise/prepare-a-non-routable-domain-for-directory-synchronization?view=o365-worldwide

NEW QUESTION: 24
You have a Microsoft 365 subscription.
You have a Microsoft SharePoint Online site named Site1.
You have a Data Subject Request (DSR) case named Case1 that searches Site1.
You create a new sensitive information type.
You need to ensure that Case1 returns all the documents that contain the new sensitive information type.
What should you do?
A. From the Security & Compliance admin center, create a new Guided search.
B. From the Security & Compliance admin center, create a new Search by ID List.
C. From Site1, initiate a re-indexing of Site1.
D. From Site1, modify the search dictionary.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 25
You have a Microsoft 365 E5 subscription.
From Microsoft Azure Active Directory (Azure AD), you create a security group named Group1. You add 10 users to Group1.
You need to apply app enforced restrictions to the members of Group1 when they connect to Microsoft Exchange Online from non-compliant devices, regardless of their location.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 26
You have a Microsoft 365 subscription.
All computers run Windows 10 Enterprise and are managed by using Microsoft Intune.
You plan to view only security-related Windows telemetry data.
You need to ensure that only Windows security data is sent to Microsoft.
What should you create from the Intune admin center?
A. a device configuration profile that has device restrictions configured
B. a device configuration profile that has the Endpoint Protection settings configured
C. a device configuration policy that has the System Security settings configured
D. a device compliance policy that has the Device Health settings configured
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/intune/device-restrictions-windows-10#reporting-and-telemetry

NEW QUESTION: 27
You have a Microsoft 365 E5 subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains three groups named Group!, Group2. and Group3 and the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create a new access package as shown in the following exhibit.
You have a Microsoft 365 E5 subscription that uses Microsoft Endpoint Manager. The Compliance policy settings are configured as shown in the following exhibit.
These settings configure the way the compliance service treats devices. Each device evaluates these as a "Built-in Device Compliance Policy", which is reflected in device monitoring.

Answer:

NEW QUESTION: 28

You have a Microsoft 365 subscription that has Enable Security defaults set to No in Azure Active Directory (Azure AD).

You have a custom compliance manager template named Regulation1.

You have the assessments shown in the following table.

Name	Score	Status	Group	Product	Regulation
Assessment1	1200	Incomplete	Group1	Microsoft 365	Regulation1
Assessment2	900	Incomplete	Group2	Microsoft 365	Regulation2

Assessment1 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Enable multi-factor authentication for admins	Failed high risk	+27 points	0/27	Technical
Enable multi-factor authentication for non-admins	Failed high risk	+27 points	0/27	Technical

Assessment2 has the improvement actions shown in the following table.

Improvement action	Test status	Impact	Points achieved	Action type
Establish a threat intelligence program	None	+9 points	0/9	Operational
Configure a privileged access policy	Failed high risk	+15 points	0/15	Technical

You perform the following actions:

For Assessment2, change the Test status of Establish a threat intelligence program to Implemented.

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

Configure a privileged access policy.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	○
The Assessment1 score will increase by only 54 points.	○	○
The Assessment2 score will increase by only 78 points.	○	○

Answer:

Statements	Yes	No
Establish a threat intelligence program will appear as Implemented in Assessment1.	○	○
The Assessment1 score will increase by only 54 points.	○	○
The Assessment2 score will increase by only 78 points.	○	○

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide

https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-improvement-actions?view=o365-worldwide

NEW QUESTION: 29

You have a Microsoft 365 subscription linked to an Azure Active Directory (Azure AD) tenant that contains a user named User1. You need to grant User1 permission to search Microsoft 365 audit logs. The solution must use the principle of least privilege. Which rote should you assign to User1?

A. the View-Only Audit Logs role m the Security & Compliance admin

B. the Security reader role in the Azure Active Directory admin center

C. the View-Only Audit Logs role in the Exchange admin center

D. the Compliance Management role in the Exchange admin center

Answer: C (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 30

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

User1 needs to be able to create Data Subject Requests (DSRs) in the Microsoft 365 compliance center.

To which role or role group should you add User1?

A. the eDiscovery Manager role

B. the Compliance Data Administrator role

C. the Data Investigator role

D. the Records Management role group

Answer: A (LEAVE A REPLY)

NEW QUESTION: 31

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

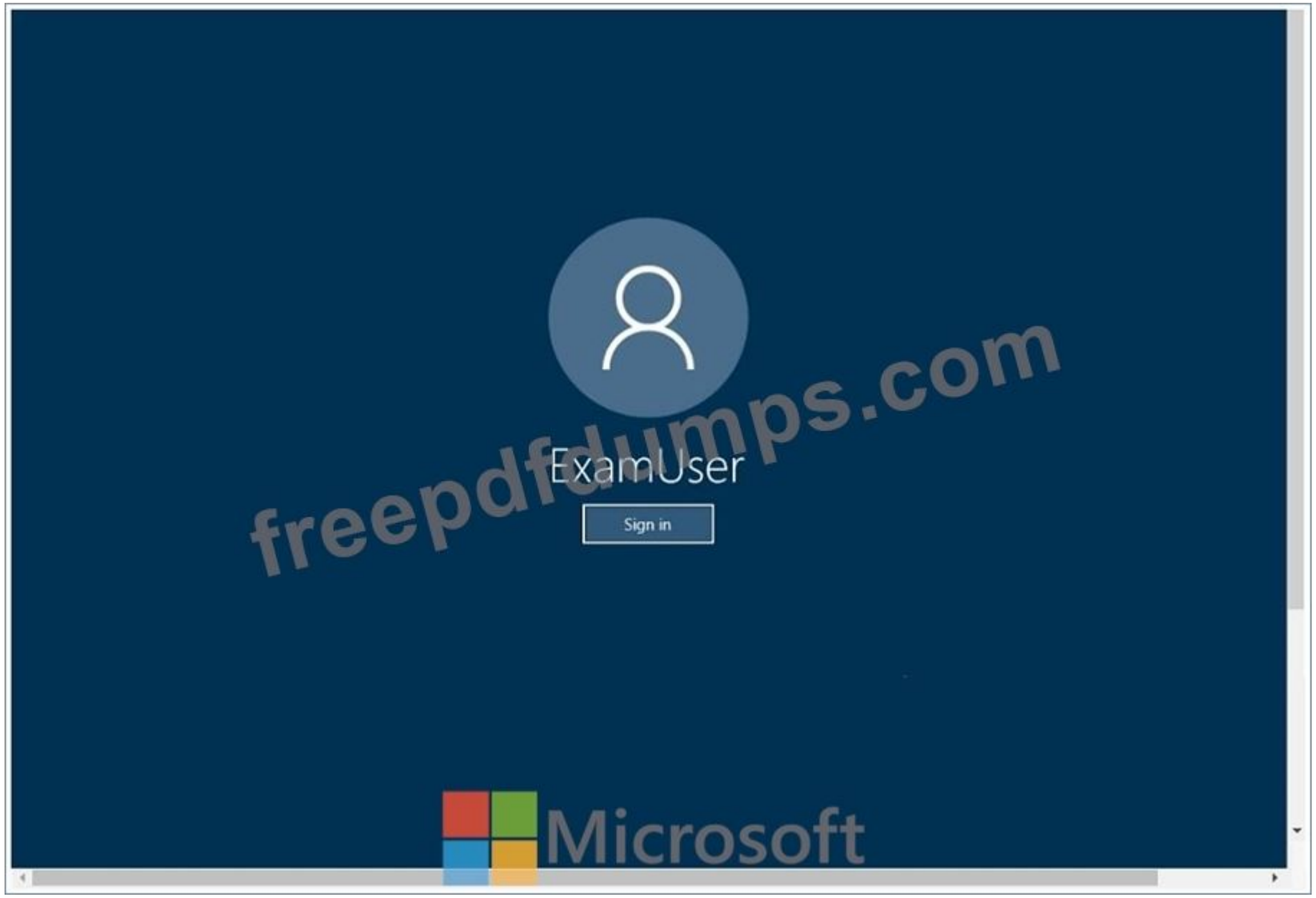
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to create a case that prevents the members of a group named Operations from deleting email messages that contain the word IPO.
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

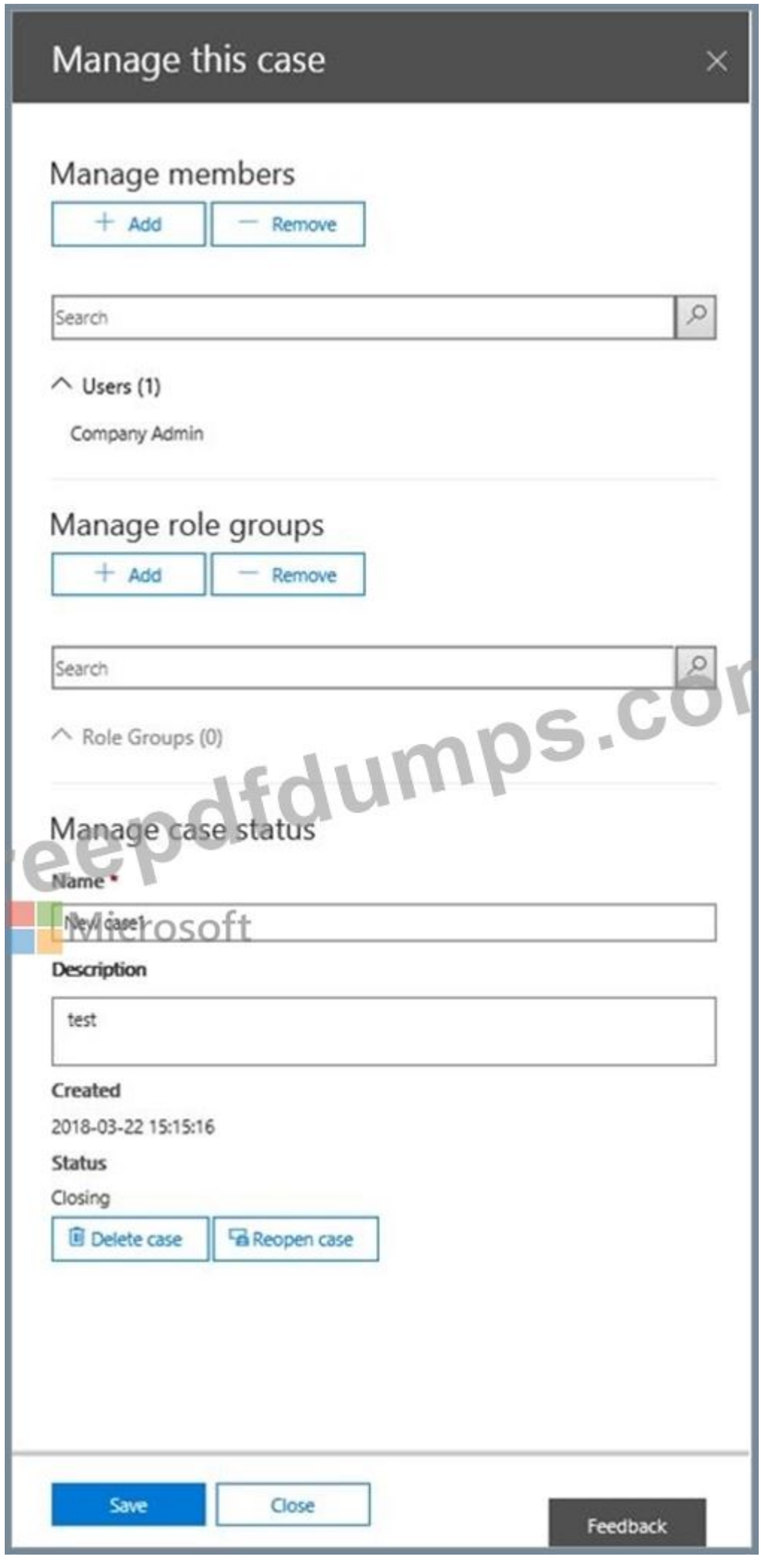
1. Navigate to the Security & Compliance Center.
2. In the Security & Compliance Center, click eDiscovery > eDiscovery, and then click Create a case.
3. On the New Case page, give the case a name, type an optional description, and then click Save. The case name must be unique in your organization.

The new case is displayed in the list of cases on the eDiscovery page.

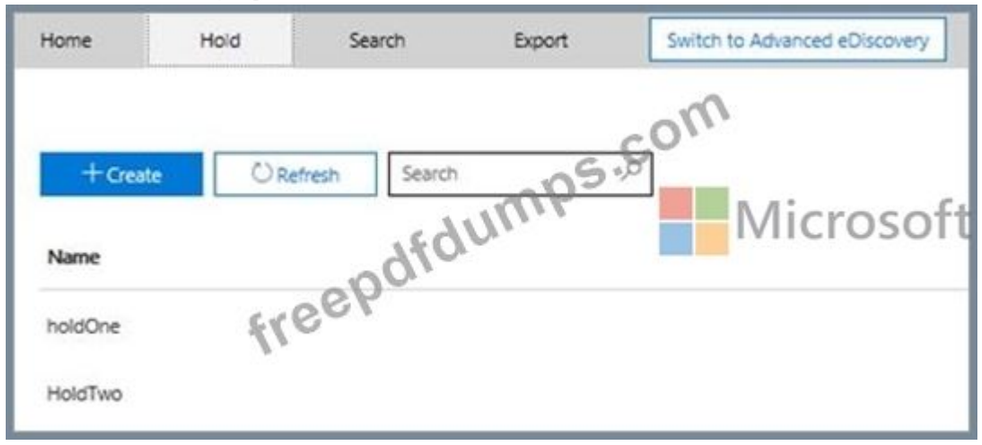
After you create a case, the next step is to add members to the case. The eDiscovery Manager who created the case is automatically added as a member. Members have to be assigned the appropriate eDiscovery permissions so they can access the case after you add them.

4. In the Security & Compliance Center, click eDiscovery > eDiscovery to display the list of cases in your organization.
5. Click the name of the case that you want to add members to.

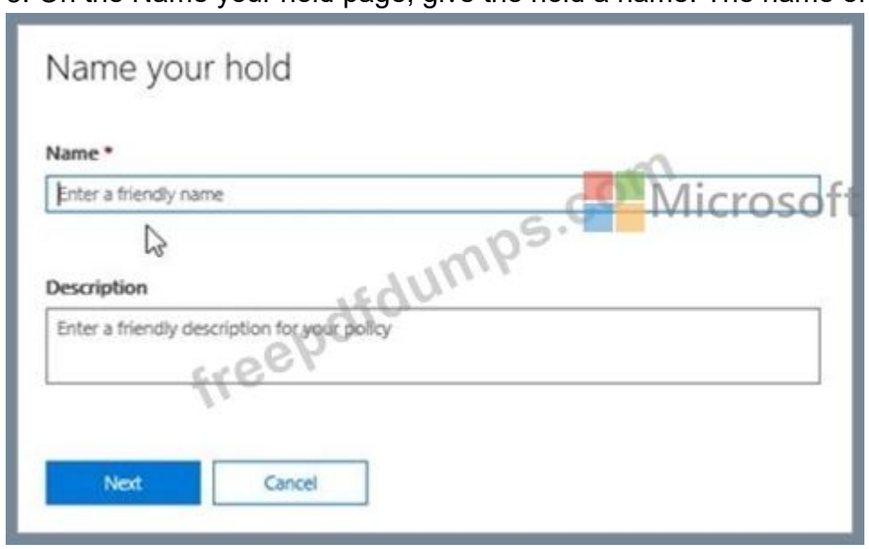
The Manage this case flyout page is displayed.



6. Under Manage members, click Add to add members to the case.
You can also choose to add a role group to the case. Under Manage role groups, click Add.
7. In the list of people or role groups that can be added as members of the case, click the check box next to the names of the people or role groups that you want to add.
8. After you select the people or role groups to add as members of the group, click Add.
In Manage this case, click Save to save the new list of case members.
9. Click Save to save the new list of case members.
You can use an eDiscovery case to create holds to preserve content that might be relevant to the case. You can place a hold on the mailboxes and OneDrive for Business sites of people who are custodians in the case. You can also place a hold on the group mailbox, SharePoint site, and OneDrive for Business site for an Office 365 Group. Similarly, you can place a hold on the mailboxes and sites that are associated with Microsoft Teams or Yammer Groups. When you place content locations on hold, content is held until you remove the hold from the content location or until you delete the hold.
To create a hold for an eDiscovery case:
1. In the Security & Compliance Center, click eDiscovery > eDiscovery to display the list of cases in your organization.
2. Click Open next to the case that you want to create the holds in.
3. On the Home page for the case, click the Hold tab.



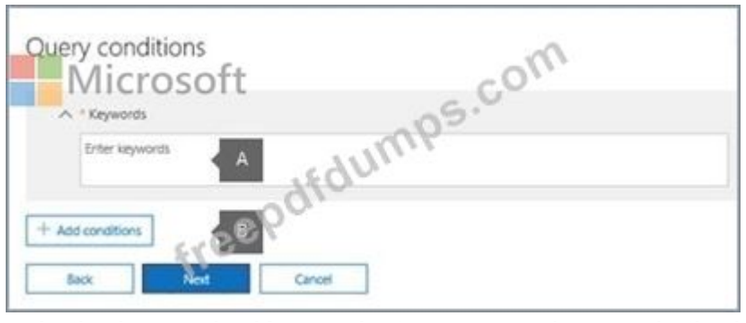
4. On the Hold page, click Create.
5. On the Name your hold page, give the hold a name. The name of the hold must be unique in your organization.



6. (Optional) In the Description box, add a description of the hold.
7. Click Next.

8. Choose the content locations that you want to place on hold. You can place mailboxes, sites, and public folders on hold.

a. Exchange email - Click Choose users, groups, or teams and then click Choose users, groups, or teams again. to specify mailboxes to place on hold. Use the search box to find user mailboxes and distribution groups (to place a hold on the mailboxes of group members) to place on hold. You can also place a hold on the associated mailbox for a Microsoft Team, a Yammer Group, or an Office 365 Group. Select the user, group, team check box, click Choose, and then click Done.



a. In the box under Keywords, type a search query in the box so that only the content that meets the search criteria is placed on hold. You can specify keywords, message properties, or document properties, such as file names. You can also use more complex queries that use a Boolean operator, such as AND, OR, or NOT. If you leave the keyword box empty, then all content located in the specified content locations will be placed on hold.

b. Click Add conditions to add one or more conditions to narrow the search query for the hold. Each condition adds a clause to the KQL search query that is created and run when you create the hold. For example, you can specify a date range so that email or site documents that were created within the date ranged are placed on hold. A condition is logically connected to the keyword query (specified in the keyword box) by the AND operator. That means that items have to satisfy both the keyword query and the condition to be placed on hold.

9. After configuring a query-based hold, click Next.

10. Review your settings, and then click Create this hold.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery-cases?view=o365-worldwide

NEW QUESTION: 32

You have a Microsoft 365 subscription that contains 1,000 user mailboxes.

An administrator named Admin1 must be able to search for the name of a competing company in the mailbox of a user named User5.

You need to ensure that Admin1 can search the mailbox of User5 successfully. The solution must prevent Admin1 from sending User5.

Solution: You start a message trace, and then create a Data Subject request (DSR) case.

Does this meet the goal?

A. Yes

B. No

Answer: B (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/ediscovery/ediscovery?view=exchserver-2019

NEW QUESTION: 33

You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.

On January 1. you create the sensitivity label shown in the following table.

Setting	Value
Name	Label1
Assign permissions now or let users decide?	Assign permissions now
User access to content expires	After 21 days
Assign permissions to specific users and groups	Co-Author: User1 and User2

On January 2, you publish label to User1.

On January 3. User 1 creates a Microsoft Word document named Doc1 and applies Label to the document.

On January 4. User2 edits Doc1.

On January 15, you increase the content expiry period for Label to 28 days.

When will access to Doc1 expire for User2?

A. January 31

B. January 23

C. January 24

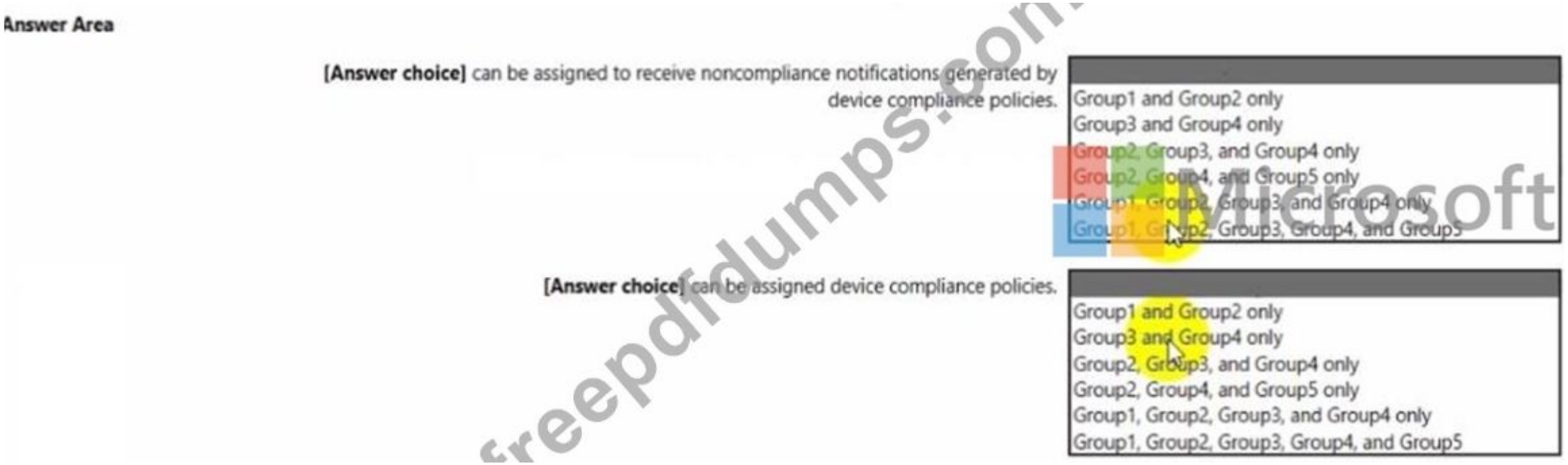
D. January 25

Answer: D (LEAVE A REPLY)

NEW QUESTION: 34

You have a Microsoft 365 subscription that contains the groups shown in the following exhibit.

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



Answer:

NEW QUESTION: 35

You have a Microsoft 365 E5 Subscription named cont0S0.C0rn.

You create a user named User'.

You Need to ensure that User1 can change Status of Microsoft Defender for Identity health alerts. The solution must use principle of the least principle.

What should you do?

A. From the Microsoft 365 admin center, add user' to the Azure ATP contoso.com Administrators group.

B. From the Microsoft 365 Defender portal, assign user' the Security Operator role.

C. From the Microsoft 365 admin center, add user' to the Azure ATP contoso.com users group.

D. From the Microsoft admin center, assign user1 the Hybrid Identity Administrator role.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 36
Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.
A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them.
Solution: You modify the content expiration settings of the label.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
You have a hybrid deployment of Azure Active Directory (Azure AD) that contains two users named User1 and User2.
You need to assign Role Based Access Control (RBAC) roles to User1 and User2 to meet the following requirements:
Use the principle of least privilege
Enable User1 to view sync errors by using Azure AD Connect Health
Enable User2 to configure Azure Active Directory Connect Health Settings Which two roles should you assign?
A. The Monitoring Contributor role in Azure Connect Health to User 2
B. The Contributor role in Azure AD Connect Health to User 2
C. The Security reader role in Azure AD to User 1
D. The Monitoring Readers role in Azure AD Connect Health to User1
E. The Security operator role in Azure AD to User2
F. The Reports reader role in Azure AD to User 1
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 38
You have a hybrid deployment of Microsoft 365 that contains the users shown in the following table.

Name	User mailbox	Multi-factor authentication (MFA)
User1	On-premises Microsoft Exchange Server	Required
User2	On-premises Microsoft Exchange Server	Disabled
User3	Microsoft Exchange Online	Required
User4	Microsoft Exchange Online	Disabled

You plan to use Microsoft 365 Attack Simulator.
You need to identify the users against which you can use Attack Simulator.
Which users should you identify?

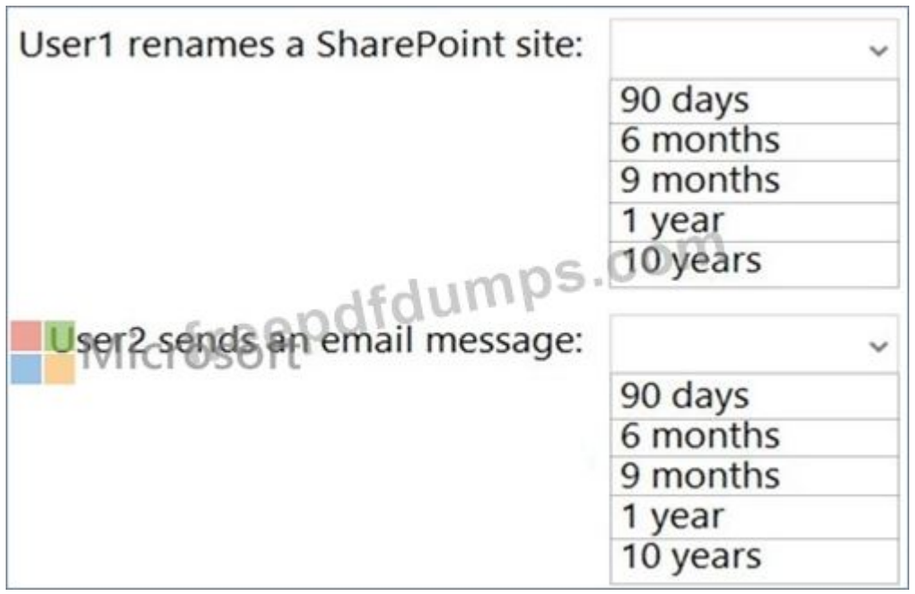
A. User1 and User3 only
B. User1, User2, User3, and User4
C. User3 only
D. User3 and User4 only
Answer: D (LEAVE A REPLY)
Each targeted recipient must have an Exchange Online mailbox.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/attack-simulator?view=o365-worldwide

NEW QUESTION: 39
You need to ensure that a user named Grady Archie can monitor the service health of your Microsoft 365 tenant. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to assign the Service Administrator role to Grady Archie.
In the Microsoft 365 Admin Center, type Grady Archie into the Search for users, groups, settings or tasks search box.
Select the Grady Archie user account from the search results.
In the Roles section of the user account properties, click the Edit link.
Select the Customized Administrator option. This will display a list of admin roles.
Select the Service admin role.
Click Save to save the changes.
Reference:
https://docs.microsoft.com/en-us/office365/enterprise/view-service-health

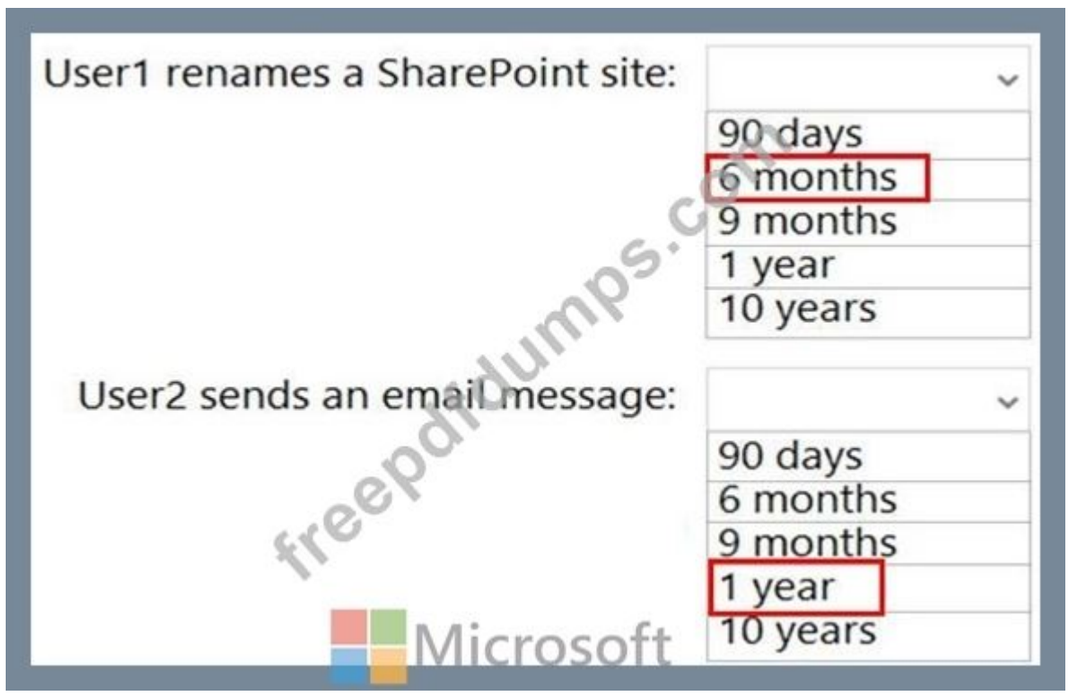
NEW QUESTION: 40
You have a Microsoft 365 E5 subscription that contains two users named User1 and User2.
You create the audit retention policies shown in the following table.

Priority	Policy name	Record type	Activities	Users	Duration
10	AuditRetention1	ExchangeItem	MailboxLogin	**None**	90 Days
20	AuditRetention2	ExchangeItem	Send, MailItemsAccessed	User1	9 Months
30	AuditRetention3	Sharepoint	**None**	User1	6 Months
40	AuditRetention4	Sharepoint	SiteRenamed	User1	9 Months
50	AuditRetention5	Sharepoint	SiteRenamed	**None**	10 Years

The users perform the following actions:
User1 renames a Microsoft SharePoint Online site.
User2 sends an email message.
How long will the audit log records be retained for each action? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

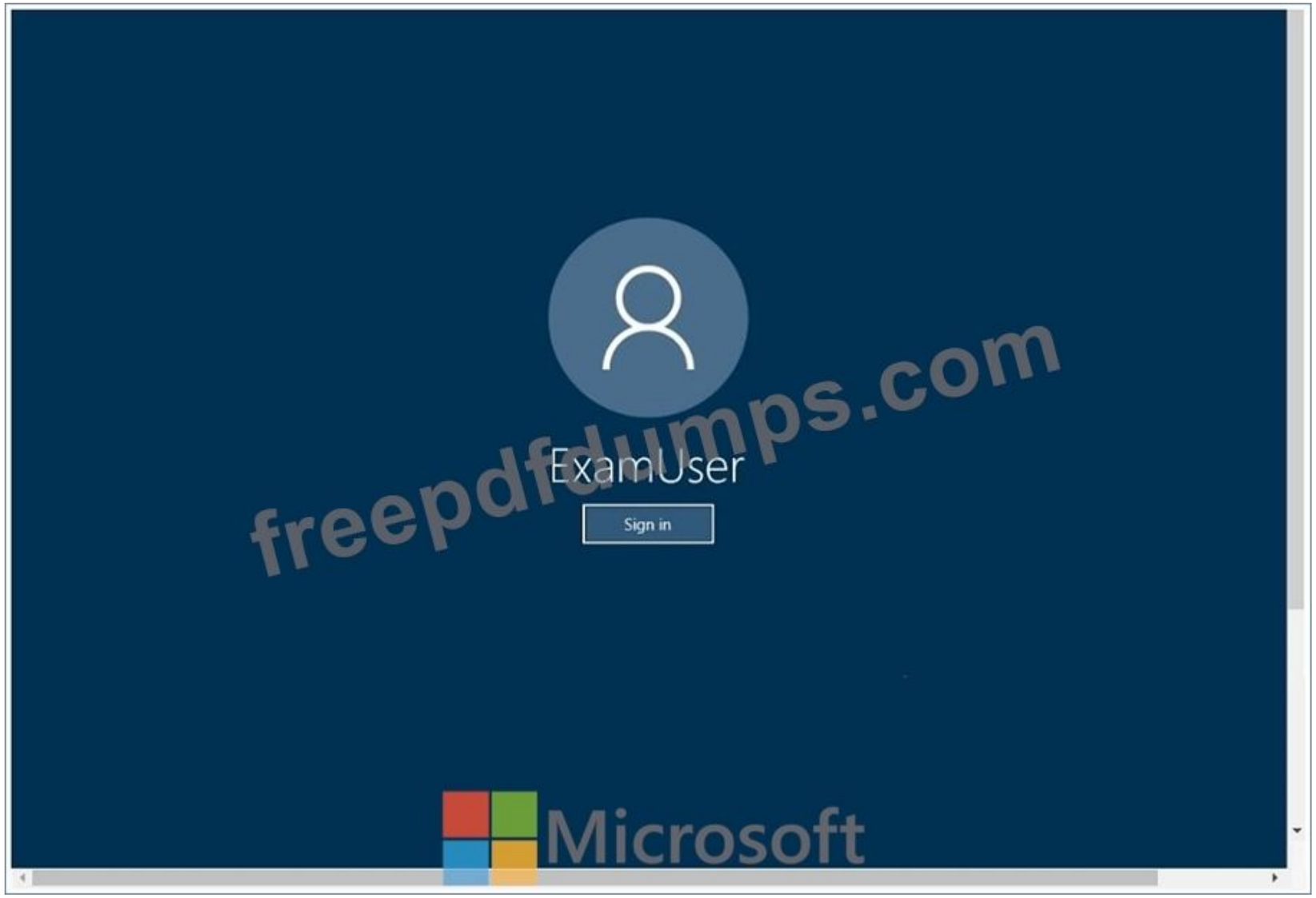


Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/audit-log-retention-policies?view=o365-worldwide

NEW QUESTION: 41
Your company has a Microsoft 365 E5 subscription that contains a user named User.
User1 leaves the company.
You need to identify all the personal data of User1 that is stored in the subscription.
What should you do in the Microsoft Purview compliance portal?
A. Create an eDscovery case.
B. Perform an audit.

C. Perform a content search.
D. Submit a Data Subject Request (DSR).
Answer: (SHOW ANSWER)
Find and export a user's personal data to help you respond to data subject requests for the General Data Protection Regulation (GDPR).
https://learn.microsoft.com/en-us/microsoft-365/compliance/microsoft-365-compliance-center?view=o365-worldwide

NEW QUESTION: 42
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to ensure that email messages in Exchange Online and documents in SharePoint Online are retained for eight years.
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

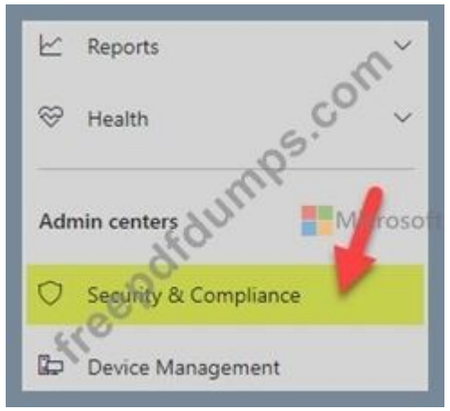
NB: For our purposes, the retention period will be 8 years.
For retaining email messages in Exchange Online:
Step 1: Create a retention tag

1. Navigate to the Exchange Admin Center
2. Navigate to Compliance management > Retention tags, and then click Add +
3. Select one of the following options:
Applied automatically to entire mailbox (default): Select this option to create a default policy tag (DPT). You can use DPTs to create a default deletion policy and a default archive policy, which applies to all items in the mailbox.
Applied automatically to a specific folder: Select this option to create a retention policy tag (RPT) for a default folder such as Inbox or Deleted Items.
Applied by users to items and folders (Personal): Select this option to create personal tags. These tags allow Outlook and Outlook on the web (formerly known as Outlook Web App) users to apply archive or deletion settings to a message or folders that are different from the settings applied to the parent folder or the entire mailbox.
4. The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:
Name: Enter a name for the retention tag. The tag name is for display purposes and doesn't have any impact on the folder or item a tag is applied to. Consider that the personal tags you provision for users are available in Outlook and Outlook on the web.
Apply this tag to the following default folder: This option is available only if you selected Applied automatically to a specific folder.
Retention action: Select one of the following actions to be taken after the item reaches its retention period:
Delete and Allow Recovery: Select this action to delete items but allow users to recover them using the Recover Deleted Items option in Outlook or Outlook on the web. Items are retained until the deleted item retention period configured for the mailbox database or the mailbox user is reached.
Permanently Delete: Select this option to permanently delete the item from the mailbox database.
Move to Archive: This action is available only if you're creating a DPT or a personal tag. Select this action to move items to the user's In-Place Archive.
Retention period: Select one of the following options:
Never: Select this option to specify that items should never be deleted or moved to the archive.
When the item reaches the following age (in days): Select this option and specify the number of days to retain items before they're moved or deleted. The retention age for all supported items except Calendar and Tasks is calculated from the date an item is received or created. Retention age for Calendar and Tasks items is calculated from the end date.
Comment: User this optional field to enter any administrative notes or comments. The field isn't displayed to users.
Step 2: Create a retention policy
1. Navigate to Compliance management > Retention policies, and then click Add +
2. In New Retention Policy, complete the following fields:
Name: Enter a name for the retention policy.
Retention tags: Click Add + to select the tags you want to add to this retention policy.
A retention policy can contain the following tags:
One DPT with the Move to Archive action.
One DPT with the Delete and Allow Recovery or Permanently Delete actions.
One DPT for voice mail messages with the Delete and Allow Recovery or Permanently Delete actions.
One RPT per default folder such as Inbox to delete items.
Any number of personal tags.
Step 3: Apply a retention policy to mailbox users
After you create a retention policy, you must apply it to mailbox users. You can apply different retention policies to different set of users.
Navigate to Recipients > Mailboxes.
In the list view, use the Shift or Ctrl keys to select multiple mailboxes.
In the details pane, click More options.
Under Retention Policy, click Update.
In Bulk Assign Retention Policy, select the retention policy you want to apply to the mailboxes, and then click Save.
For retaining documents in SharePoint Online

Access Security & Compliance Admin Center

1. Navigate to the Office 365 Admin Centers

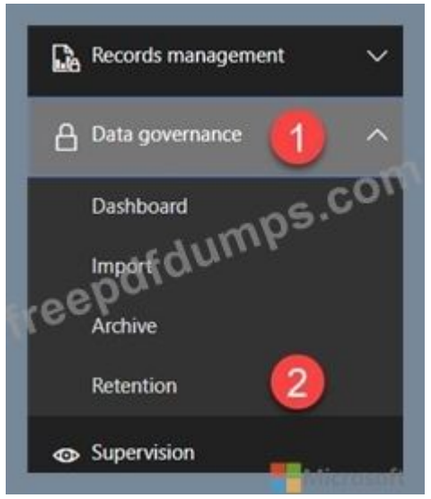
2. From the list of available Admin Centers, click on Security & Compliance



How to create and publish a Retention Policy on a SharePoint site

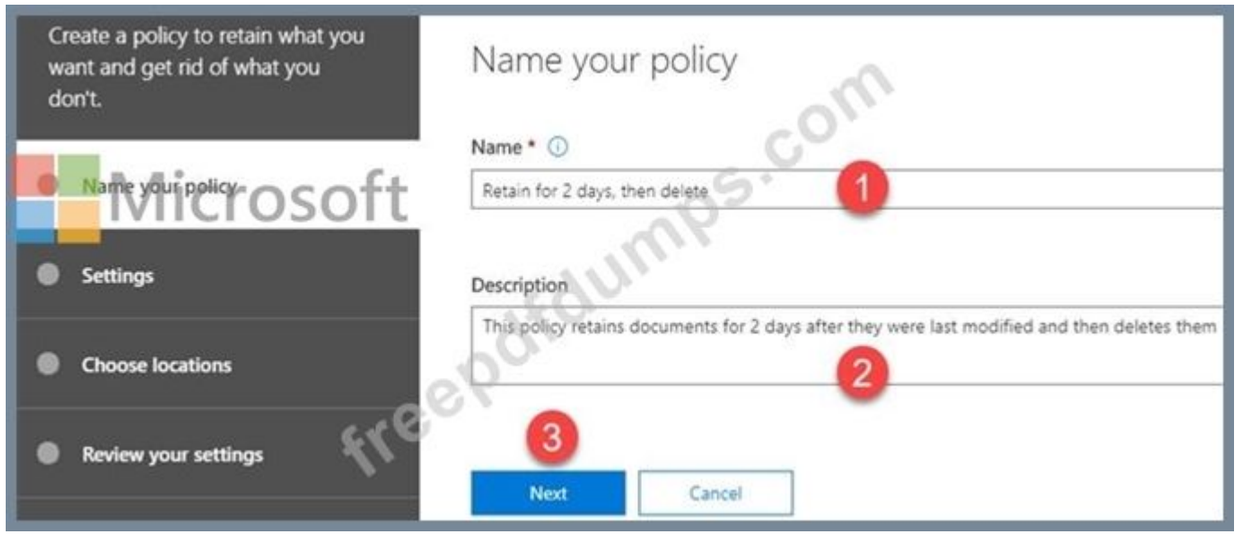
Now that we are in the Security & Compliance Admin Center, we are ready to create and publish a Retention Policy on a SharePoint site.

Under Data Governance, click Retention

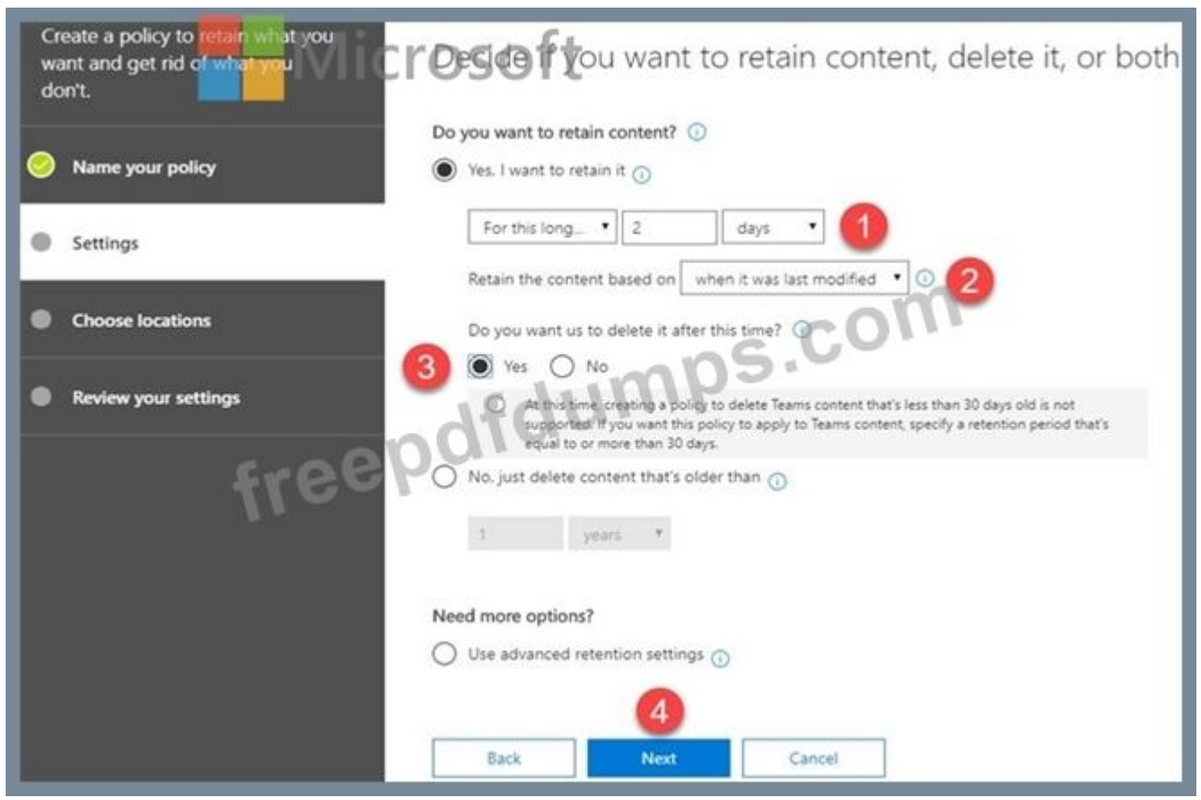


1. Hit Create button to create new Retention Policy

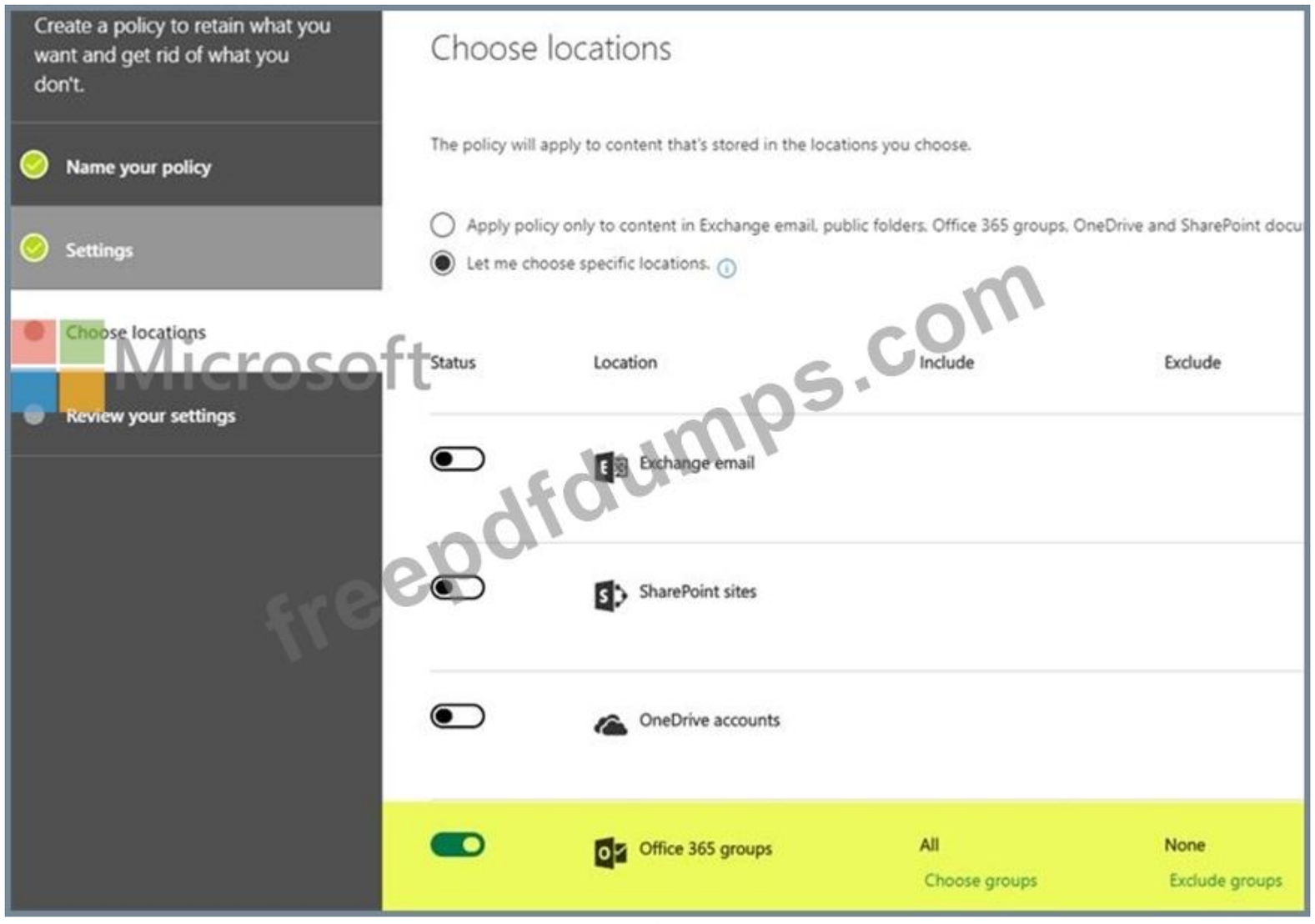
2. Give your policy a name and description. Hit Next



3. On the next screen is where you set up the logic. You can configure how many days, months, or years to retain the content for, specify whether you want the math (retention period) to be calculated from the Created Date or Last Modified Date. Lastly, you can also specify whether you want to keep or delete content after the Retention period expires. Hit Next

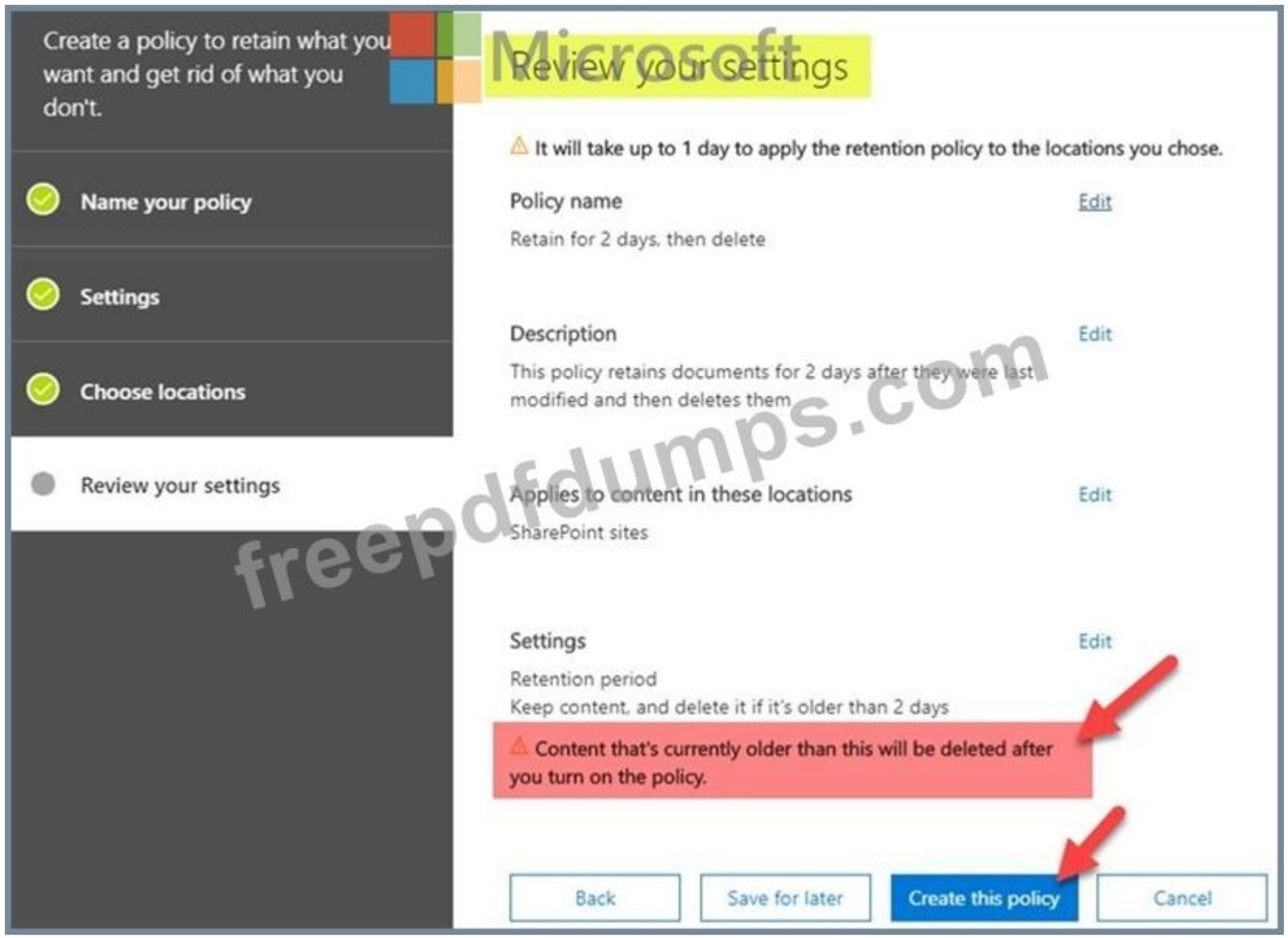


4. On the next screen, you get to choose where to apply the policy. You can apply it to email (Exchange), SharePoint sites, OneDrive accounts as well as Office 365 Groups.



5. In my case, I applied a policy to a single Office 365 Group Site

6. On a final screen, you need to review and confirm the settings and click Create this policy button. It is imperative to note the message you get to see at the bottom. It warns you that content might be deleted as soon as the policy takes effect according to the logic you set up in previous steps.



Reference:
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy#step-2-create-a-retention-policy
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-retention-policy#use-the-eac-to-apply-a-retention-policy-to-multiple-mailboxes
https://sharepointmaven.com/how-to-set-a-retention-policy-on-a-sharepoint-site/

NEW QUESTION: 43
You have a Microsoft 365 E5 subscription.
You plan to implement retention policies. Which item types can be retained?
A. code snippets
B. embedded images
C. voice memos from the Tea
Answer: (SHOW ANSWER)

NEW QUESTION: 44
You haw a Microsoft 365 subscription that contains the users shown in the following table.

Name	Azure Active Directory (Azure AD) role	Security group
User1	Directory writers	Group1, Group3
User2	Security administrator	Group1, Group2
User3	Azure Information Protection administrator	Group2, Group3
User4	Cloud application administrator	Group3, Group4

You need to ensure that User1, User2 , and User3 can use self-service password reset (SSPR). The solution must not affect User 4.
Solution: You enable SSPR for Group3.
.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
By default, self-service password reset is enabled for Directory writers and Security administrator but not for Azure Information Protection administrators and Cloud application administrators. Therefore, we must enable SSPR for User3 by applying it to Group2 and not Group3 as User4 is in Group3. User4 would thus be affected if we enable it on Group3.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-policy#administrator-reset-policy-differences

NEW QUESTION: 45
Von haw a Microsoft 365 subscription.
You need to ensure that users on manually designate which content will be subject to data toss prevention (DIP) polices?
What should you create first?
A. a retention label
B. a custom sensitive information type
C. a safe attachments policy
D. a Data Subject Request (OSR)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 46
Your company has a Microsoft 365 subscription that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

The company implements Windows Defender Advanced Threat Protection (Windows Defender ATP). Windows Defender ATP includes the roles shown in the following table:

Name	Permission	Assigned user group
Role1	View data, Active remediation actions, Alerts investigation	Group1
Role2	View data, Active remediation actions	Group2
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage portal system settings, Manage security settings	Group3

Windows Defender ATP contains the machine groups shown in the following table:

Rank	Machine group	Machine	User access
First	ATPGroup1	Device1	Group1
Last	Ungrouped machines (default)	Device2	Group2

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

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

Answer:

Statements	Yes	No
User1 can run an antivirus scan on Device1.	○	○
User2 can collect an investigation package from Device2.	○	○
User3 can isolate Device1.	○	○

NEW QUESTION: 47
You configure several Advanced Threat Protection (ATP) policies in a Microsoft 365 subscription.
You need to allow a user named User1 to view ATP reports in the Threat management dashboard.
Which role provides User1with the required role permissions?
A. Security reader
B. Message center reader
C. Compliance administrator
D. Information Protection administrator
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/view-reports-for-atp#what-permissions-areneeded-to-view-the-atp-reports

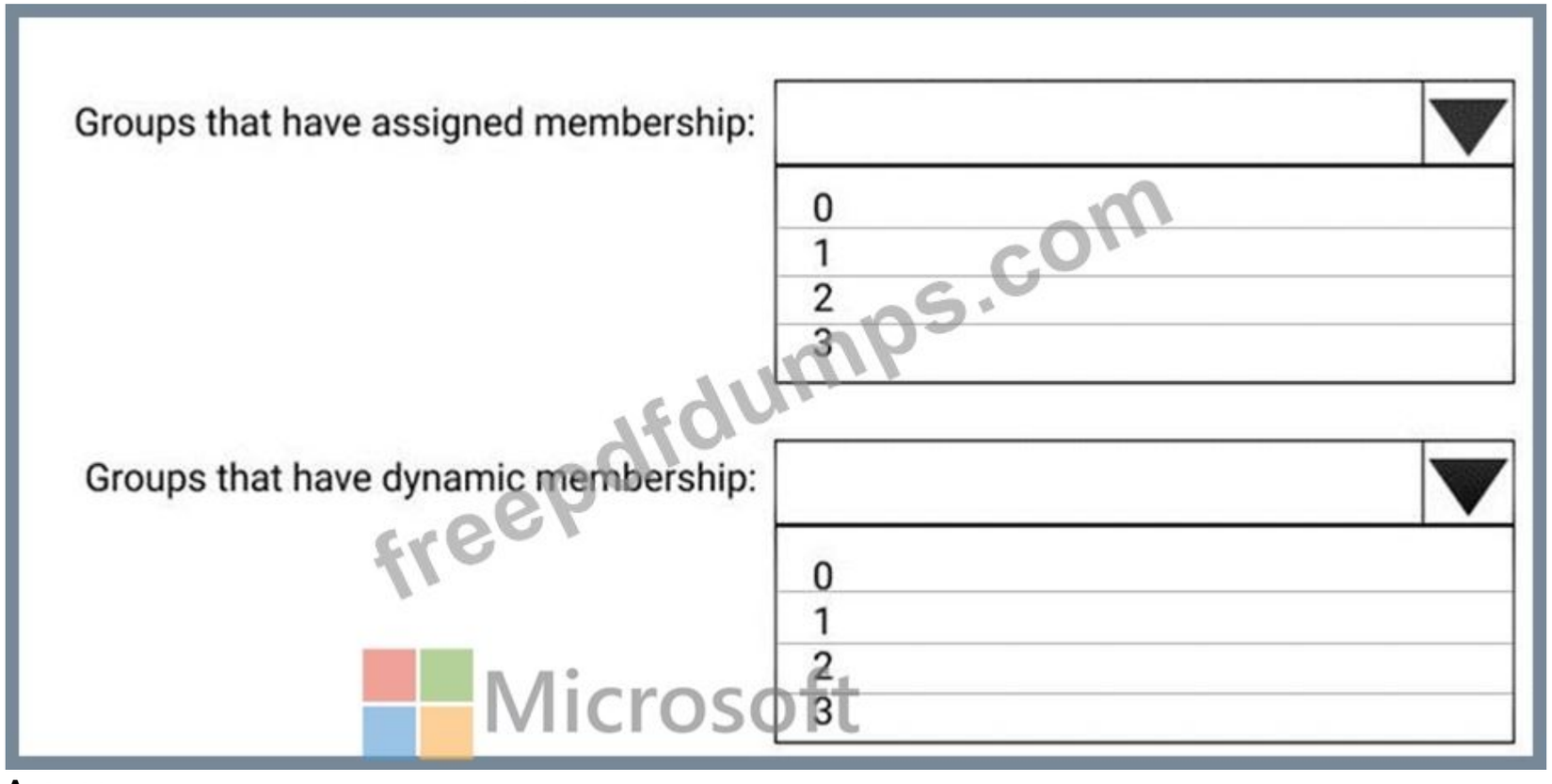
NEW QUESTION: 48
You need to create a policy that identifies content in Microsoft OneDrive that contains credit card numbers.
To complete this task, sign in to the Microsoft 365 portal.
Answer:
You need to configure auto-labeling in 'simulation' mode. In the policy, you can select the 'Credit Card' sensitive info type.
In the Microsoft 365 compliance center, navigate to sensitivity labels:
Solutions > Information protection
Select the Auto-labeling (preview) tab.
Select + Create policy.
For the page Choose info you want this label applied to: Select one of the templates, such as Financial or Privacy. You can refine your search by using the Show options for dropdown. Or, select Custom policy if the templates don't meet your requirements. Select Next.
For the page Name your auto-labeling policy: Provide a unique name, and optionally a description to help identify the automatically applied label, locations, and conditions that identify the content to label.
For the page Choose locations where you want to apply the label: Select OneDrive. Then select Next.
For the Define policy settings page: Keep the default of Find content that contains to define rules that identify content to label across all your selected locations. The rules use conditions that include sensitive information types and sharing options. For sensitive information types, you can select both built-in and custom sensitive information types.
Then select Next.
For the Set up rules to define what content is labeled page: Select + Create rule and then select Next.
On the Create rule page, name and define your rule, using sensitive information types and then select Save.
Click Next.
For the Choose a label to auto-apply page: Select + Choose a label, select a label from the Choose a sensitivity label pane, and then select Next.
For the Decide if you want to run policy simulation now or later page: Select Run policy in simulation mode if you're ready to run the auto-labeling policy now, in simulation mode. Otherwise, select Leave policy turned off. Select Next.
For the Summary page: Review the configuration of your auto-labeling policy and make any changes that needed, and complete the wizard.

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

NEW QUESTION: 49
You have a Microsoft 365 E5 subscription.
Users and device objects are added and removed daily. Users in the sales department frequently change their device.
You need to create three following groups:

Group	Requirement
1	All the devices of users where the Department attributes is set to Sales
2	All the devices where the Department attribute is set to Sales
3	All the devices where the deviceOwnership attribute is set to Company

The solution must minimize administrative effort.
What is the minimum number of groups you should create for each type of membership? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

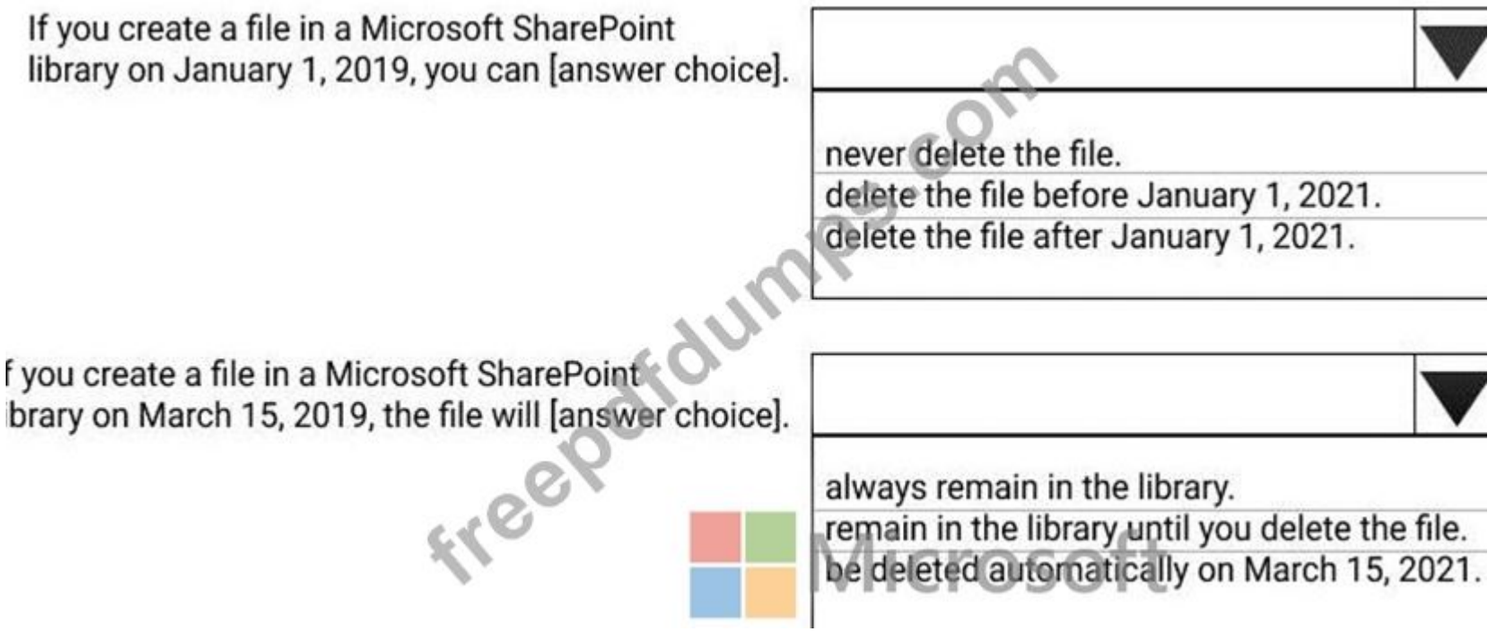


Answer:

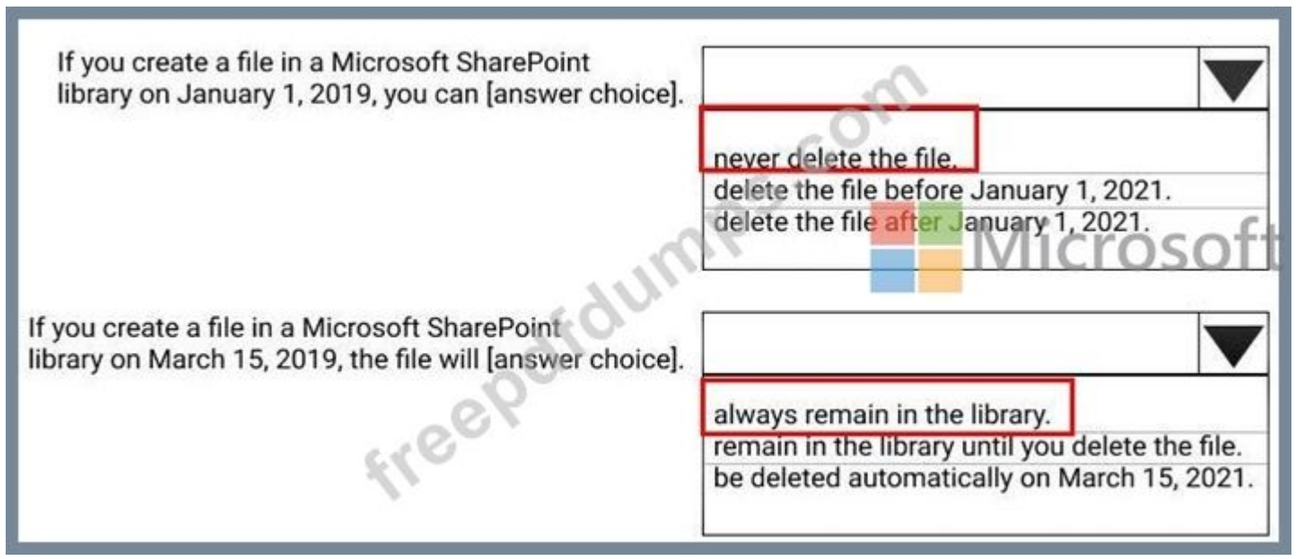
Reference:
https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/active-directory/users-groups-roles/groups-dynamic-membership.md

NEW QUESTION: 50
You have a Microsoft 365 subscription.
You create a retention label named Label1 as shown in the following exhibit.

You publish Label1 to SharePoint sites.
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:



Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

NEW QUESTION: 51
You have a hybrid Azure Active Directory (Azure AD) tenant that has pass- through authentication enabled.
You plan to implement Azure AD identity Protection and enable the user risk policy.
You need to configure the environment to support the user risk policy.
A. Enforce the multi-factor authentication (MFA) registration policy.
B. Configure a conditional access policy.
C. Enable the sign-in risk policy.
D. Enable password hash synchronization.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 52
Your company has a Microsoft 365 subscription.
The company does not permit users to enroll personal devices in mobile device management (MOM).
Users in the sales department have personal iOS devices.
You need to ensure that the sales department users can use the Microsoft Power BI app from iOS devices to access the Power BI data in your tenant. The users must be prevented from backing up the app's data to iCloud.
What should you create?
A. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a client apps condition
B. an app protection policy in Microsoft Endpoint Manager
C. a conditional access policy in Microsoft Azure Active Directory (Azure AD) that has a device state condition
D. a device compliance policy in Microsoft Endpoint Manager
Answer: (SHOW ANSWER)

NEW QUESTION: 53
You have a Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) deployment that has the custom network indicators turned on. Microsoft Defender ATP protects two computers that run Windows 10 as shown in the following table.

Name	Tag
Computer1	Kiosk1
Computer2	Tag1

Microsoft Defender ATP has the machine groups shown in the following table.

Rank	Name	Membership rule
1	Group1	Tag Contains 1
2	Group2	Name Ends with 2 And Tag Equals Tag1
3	Group3	Name Contains comp
Last	Ungrouped machines (default)	*None*

From Microsoft Defender Security Center, you create the URLs/Domains indicators shown in the following table.

URL/Domain	Action	Scope
http://www.contoso.com	Alert and block	Group1
http://www.litwareinc.com	Alert and block	Group2
http://www.litwareinc.com/public	Allow	All machines

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
From a web browser on Computer1, you can open http://www.contoso.com.	○	○
From a web browser on Computer1,you can open http://www.litwareinc.com/public.	○	○
From a web browser on Computer2, you can open http://www.litwareinc.com.	○	○

Answer:

NEW QUESTION: 54

You have an Azure Sentinel workspace.

You configure a rule to generate Azure Sentinel alerts when Azure Active Directory (Azure AD) Identity Protection detects risky sign-ins. You develop an Azure Logic Apps solution to contact users and verify whether reported risky sign-ins are legitimate.

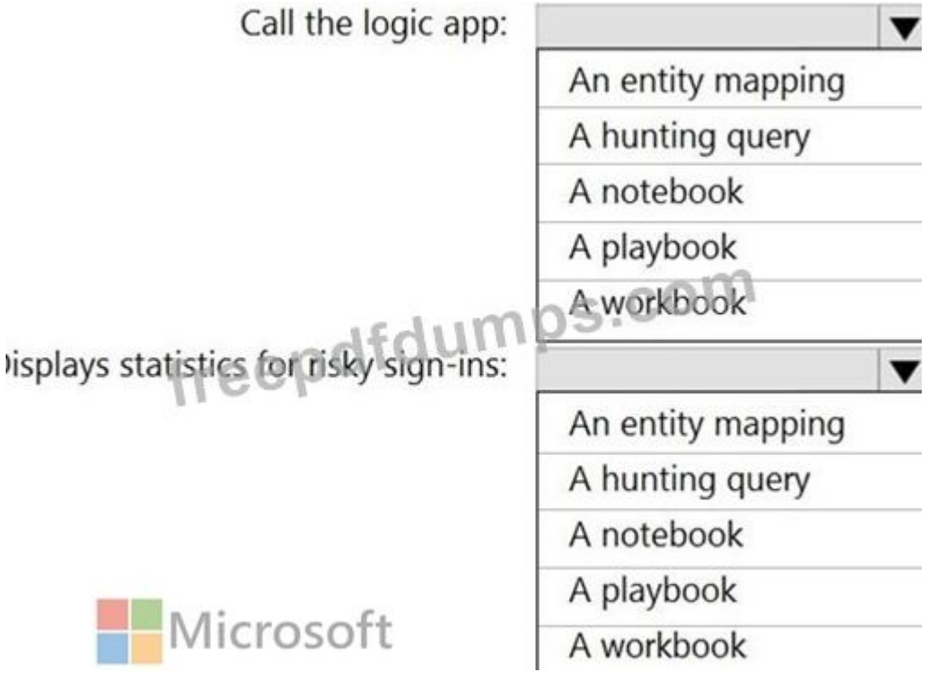
You need to configure the workspace to meet the following requirements:

Call the Azure logic app when an alert is triggered for a risky sign-in.

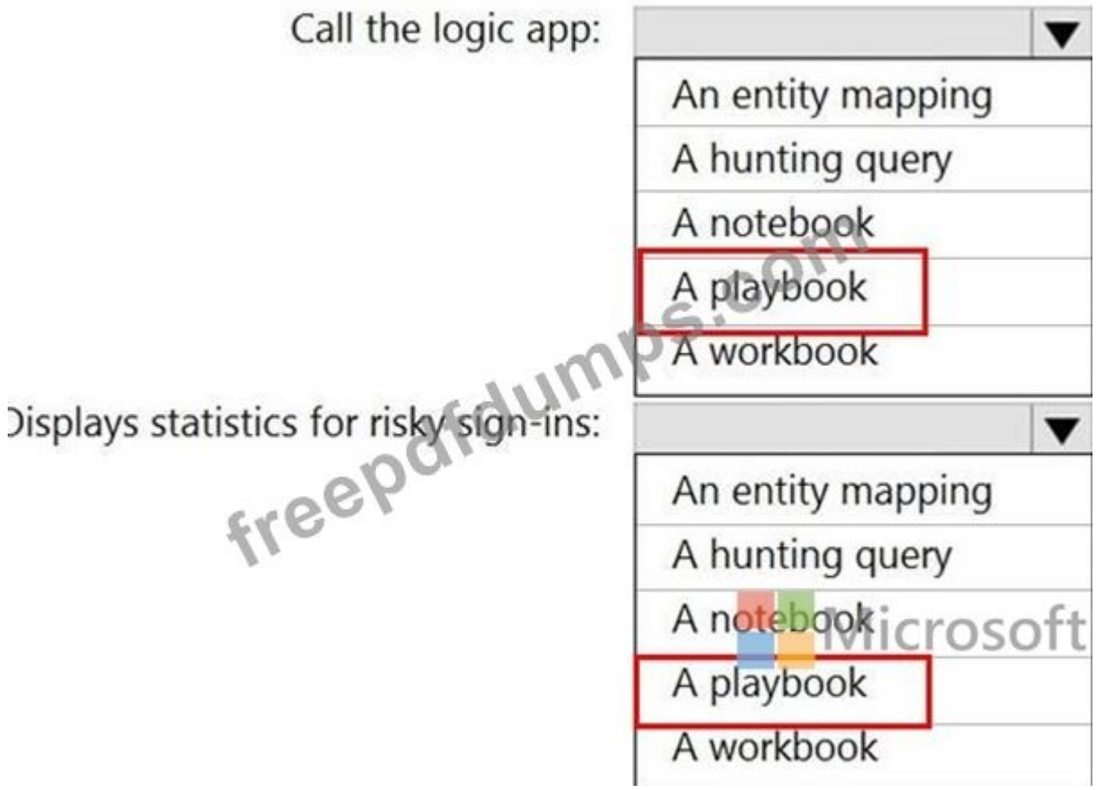
To the Azure Sentinel portal, add a custom dashboard that displays statistics for risky sign-ins that are detected and resolved.

What should you configure in Azure Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook

NEW QUESTION: 55
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 questions 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 an on-premises Active Directory domain named contoso.com.
You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Directory Service event log on Server1.
Does that meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION: 56
You have a Microsoft 365 subscription.
You have a Data Subject Request (DSR) case named Case1.
You need to ensure that Case1 includes all the email posted by the data subject to the Microsoft Exchange Online public folders.

Which additional property should you include in the Content Search query?

A. kind:externaldata

B. itemclass:ipm.externaldata

C. itemclass:ipm.post

D. kind:email

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/manage-gdpr-data-subject-requests-with-the-dsrcase-tool?view=o365-worldwide

NEW QUESTION: 57

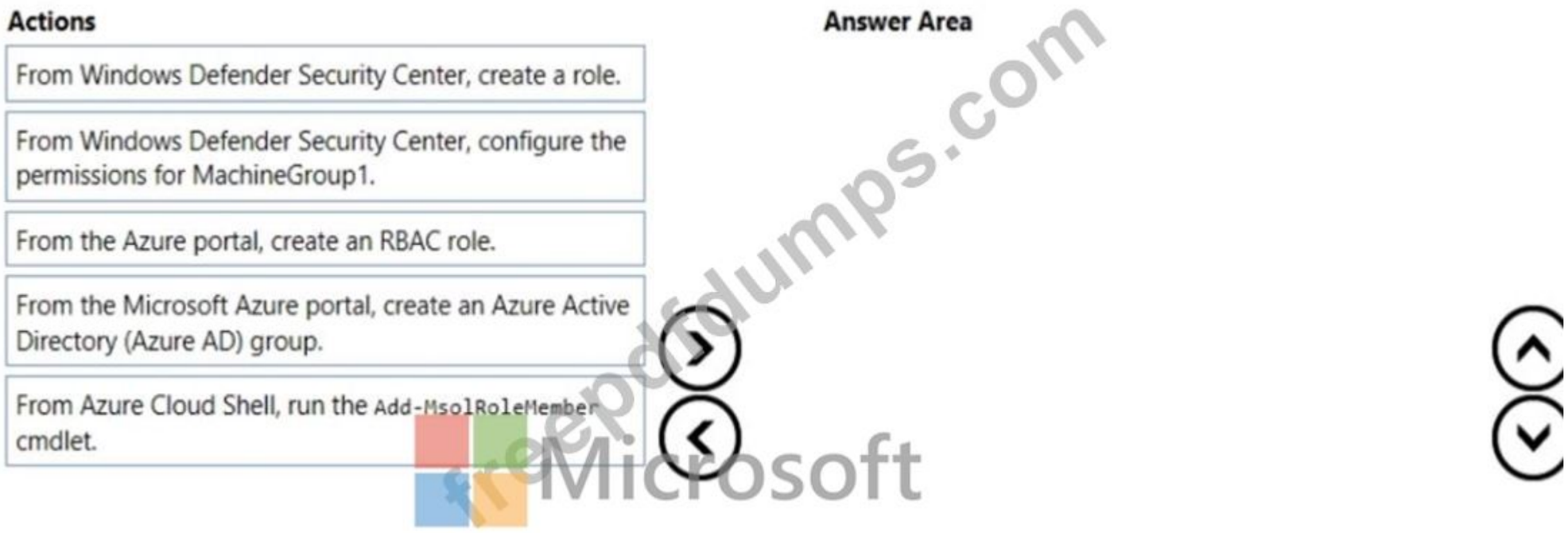
You have a Microsoft 365 E5 subscription.

All computers run Windows 10 and are onboarded to Windows Defender Advanced Threat Protection (Windows Defender ATP).

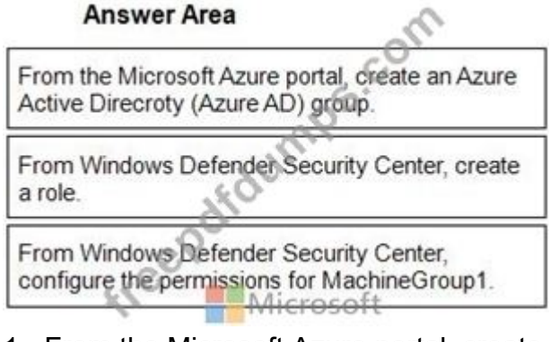
You create a Windows Defender machine group named MachineGroup1.

You need to enable delegation for the security settings of the computers in MachineGroup1.

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.



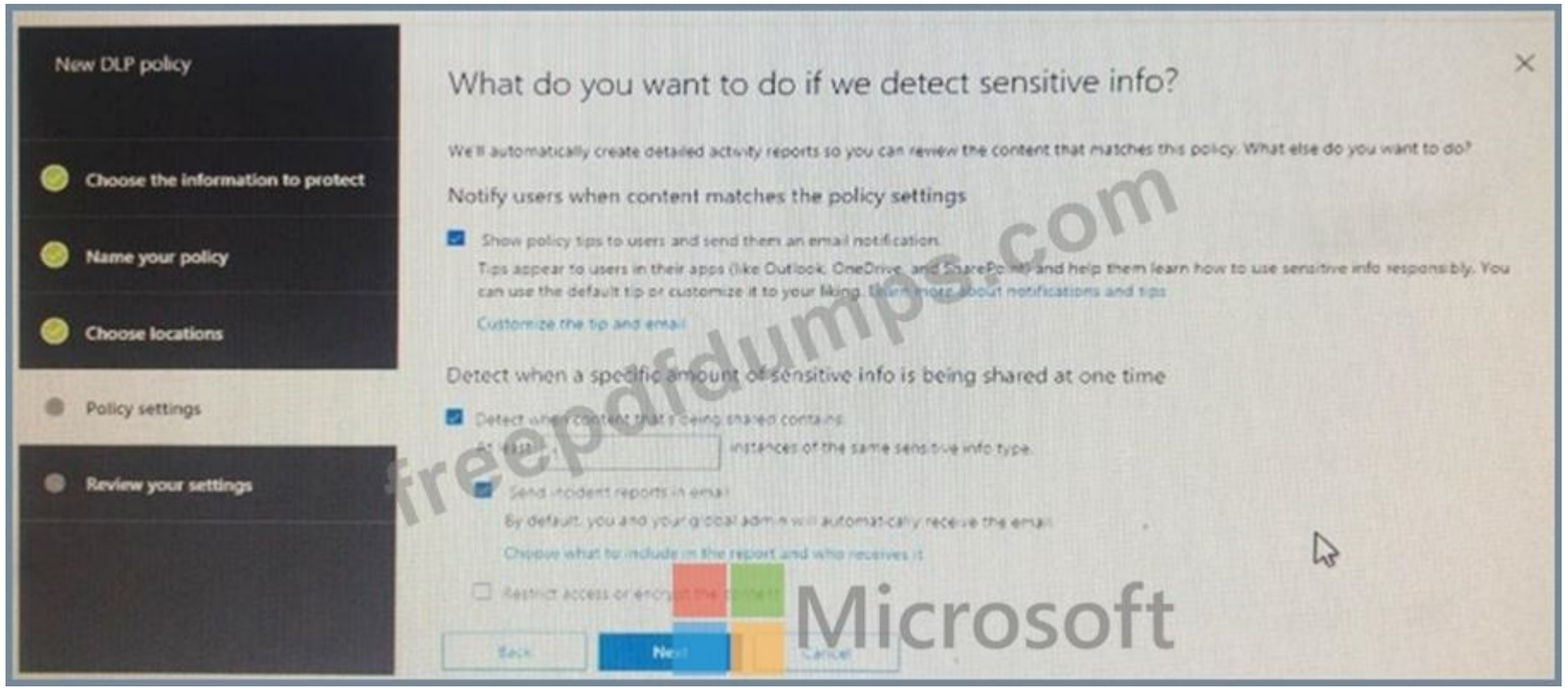
Answer:



1 - From the Microsoft Azure portal, create an Azure Active Direcroty (Azure AD) group.

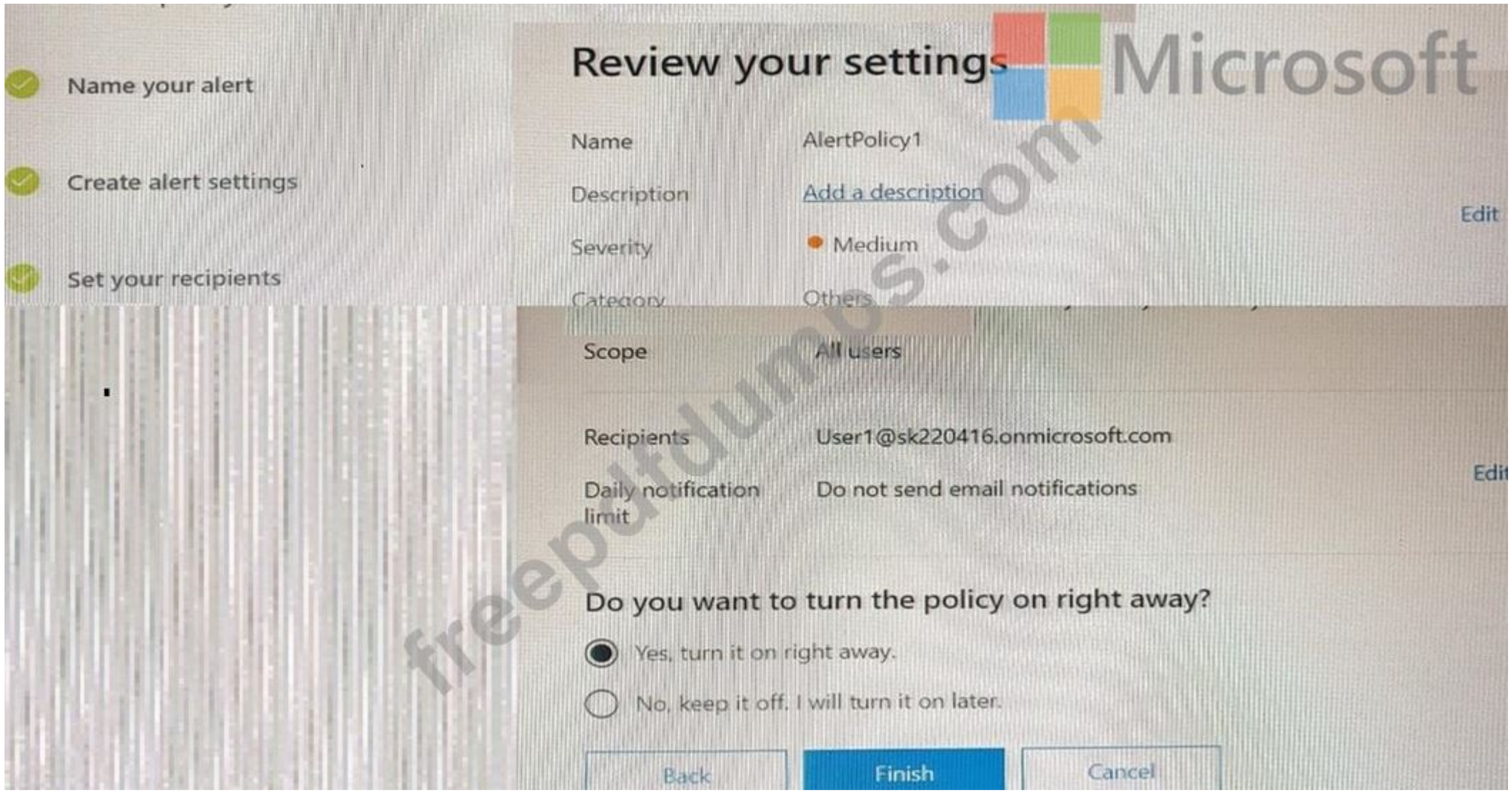
2 - From Windows Defender Security Center, create a role.
3 - From Windows Defender Security Center, configure the permissions for MachineGroup1.

NEW QUESTION: 58
You create a data loss prevention (DLP) policy as shown in the following shown:



What is the effect of the policy when a user attempts to send an email messages that contains sensitive information?
A. The user receives a notification and can send the email message
B. The user receives a notification and cannot send the email message
C. The email message is sent without a notification
D. The email message is blocked silently
Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies

NEW QUESTION: 59
You have a Microsoft 365 E5 subscription that contains a user named User1 and a Microsoft SharePoint Online site named Site1. You create the alert policy shown in the following exhibit.



To Site1, User1 uploads the files shown in the following table.

How many alerts will be generated in response to the file uploads?

A. 2

B. 3

C. 1

D. 4

Answer: D (LEAVE A REPLY)

NEW QUESTION: 60

Your on-premises network contains an Active Directory domain that syncs to Azure Active Directory (Azure AD) by using Azure AD Connect. The functional level of the domain. You need to deploy Windows Hello for Business. The solution must meet the following requirements:

* Ensure that users can access Microsoft 365 services and on-premises resources.

* Minimize administrative efforts

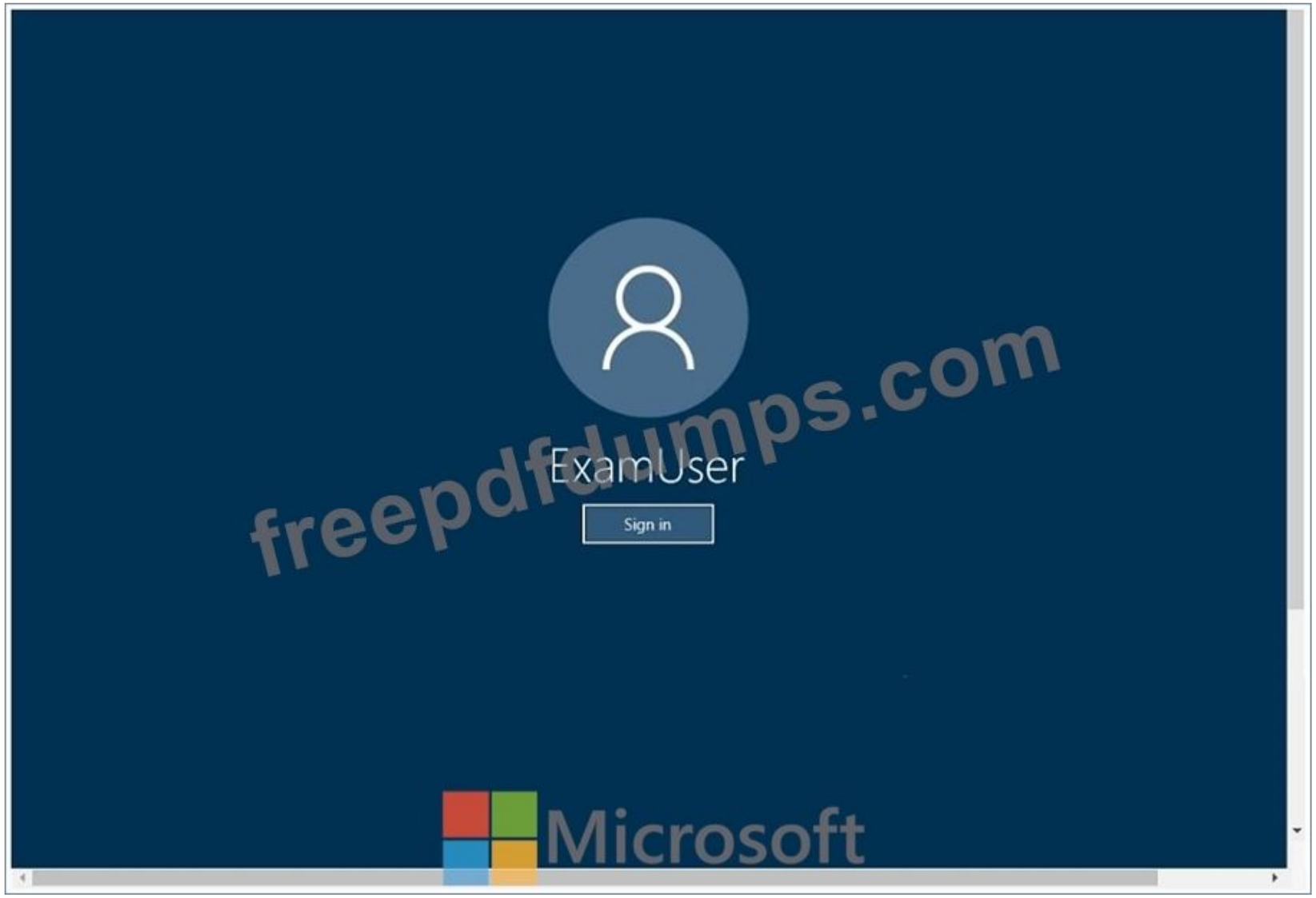
How should you deploy Windows Hello for Business, and which type of trust should you use? To answer, select the appropriate options in the answer area.

Answer:

Answer is as below.

NEW QUESTION: 61
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 questions 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 have a user named User1. Several users have full access to the mailbox of User1.
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
You run the Set-Maibox -Identity "User1" -AuditEnabled $true command.
Does that meet the goal?
A. Yes
B. No
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps

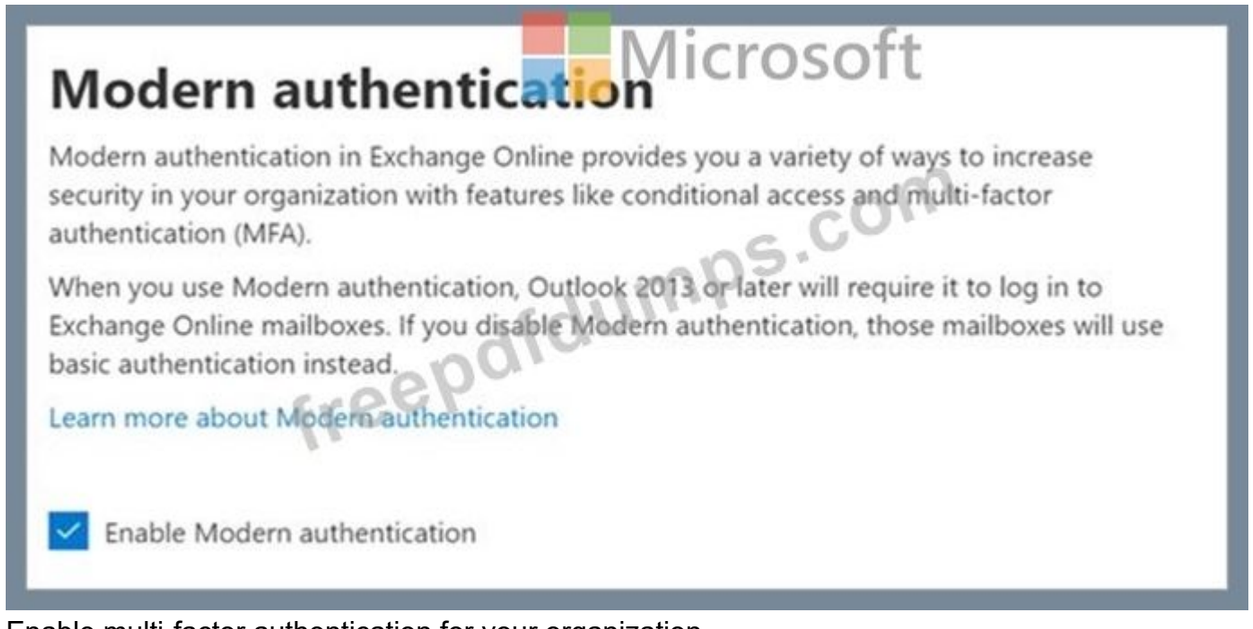
NEW QUESTION: 62
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to ensure that a user named Alex Wilber can register for multifactor authentication (MFA).
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

Enable Modern authentication for your organization
1. To enable modern authentication, from the admin center, select Settings > Settings and then in the Services tab, choose Modern authentication from the list.
2. Check the Enable modern authentication box in the Modern authentication panel.



Enable multi-factor authentication for your organization

1. In the admin center, select Users and Active Users.
2. In the Active Users section, Click on multi-factor authentication.
3. On the Multi-factor authentication page, select user if you are enabling this for one user or select Bulk Update to enable multiple users.
4. Click on Enable under Quick Steps.
5. In the Pop-up window, Click on Enable Multi-Factor Authentication.

After you set up multi-factor authentication for your organization, your users will be required to set up two-step verification on their devices.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide

NEW QUESTION: 63

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 that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.

The Compliance Manager Reader role is not assigned to any users.

You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.

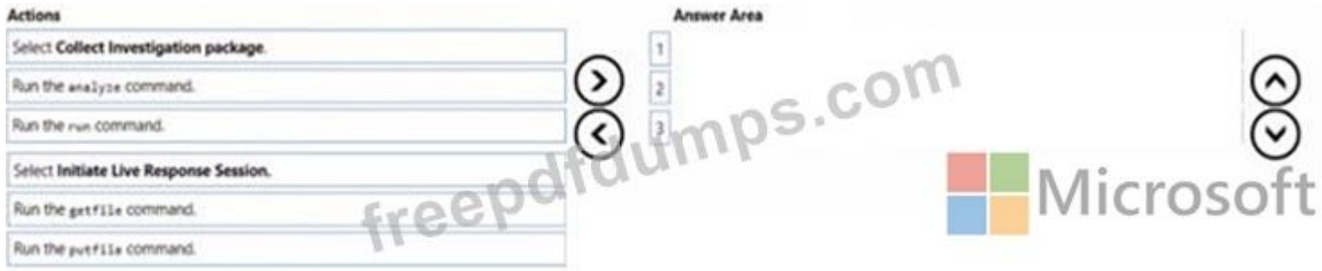
Solution: You recommend modifying the licenses assigned to User5.

Does this meet the goal?

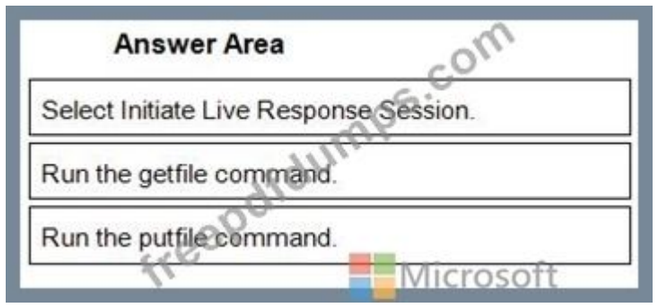
A. Yes

B. No
Answer: A (LEAVE A REPLY)

NEW QUESTION: 64
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Endpoint and contains a Windows 10 device named Device1.
You have a PowerShell script named script1 that collects forensic data and saves the results as a file on the device from which the script is run.
You receive a Microsoft Defender for Endpoint alert for suspicious activities on Device1.
You need to run script1 on Device1 and retrieve the output file of the script.
Which four actions should you perform in sequence in Microsoft 365 Defender portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



1 - Select Initiate Live Response Session.
2 - Run the getfile command.
3 - Run the putfile command.

NEW QUESTION: 65
You have a Microsoft 365 Enterprise E5 subscription.
You use Microsoft Defender for Endpoint.
You need to integrate Microsoft Defender for Office 365 and Microsoft Defender for Endpoint Where should you configure the integration?
A. From the Microsoft 365 Defender portal, select Explorer and then select MDE Settings
B. From the Microsoft 365 admin center, select Reports and then select Security & Compliance
C. From the Microsoft 365 admin center, select Settings, and then select Services fit add-ins
D. From the Microsoft 365 Defender portal, select Settings and then select Security center.
Answer: (SHOW ANSWER)

NEW QUESTION: 66

You have a Microsoft 365 E5 subscription that has Microsoft Defender for Cloud Apps enabled. You need to create an alert in Defender for Cloud Apps when source code is shared externally.
Which type of policy should you create?
A. Cloud Discovery anomaly detection
B. access
C. file
D. activity
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
You have a Microsoft 365 E5 subscription and a hybrid Microsoft Exchange Server organization.
Each member of a group named Executive has an on-premises mailbox. Only the Executive group members have multi-factor authentication (MFA) enabled. Each member of a group named Research has a mailbox in Exchange Online.
You need to use Microsoft Office 365 Attack simulator to model a spear-phishing attack that targets the Research group members.
The email address that you intend to spoof belongs to the Executive group members.
What should you do first?
A. From Azure ATP admin center, configure the primary workspace settings
B. From the Microsoft Azure portal, configure the user risk settings in Azure AD Identity Protection
C. Enable MFA for the Research group members
D. Migrate the Executive group members to Exchange Online
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/attack-simulator

NEW QUESTION: 68
You have a Microsoft 365 subscription that contains the users shown in the following table.

Name	Group	Role
User1	Group1	User administrator
User2	Group1	Security operator
User3	Group2	Security reader
User4	None	Global administrator

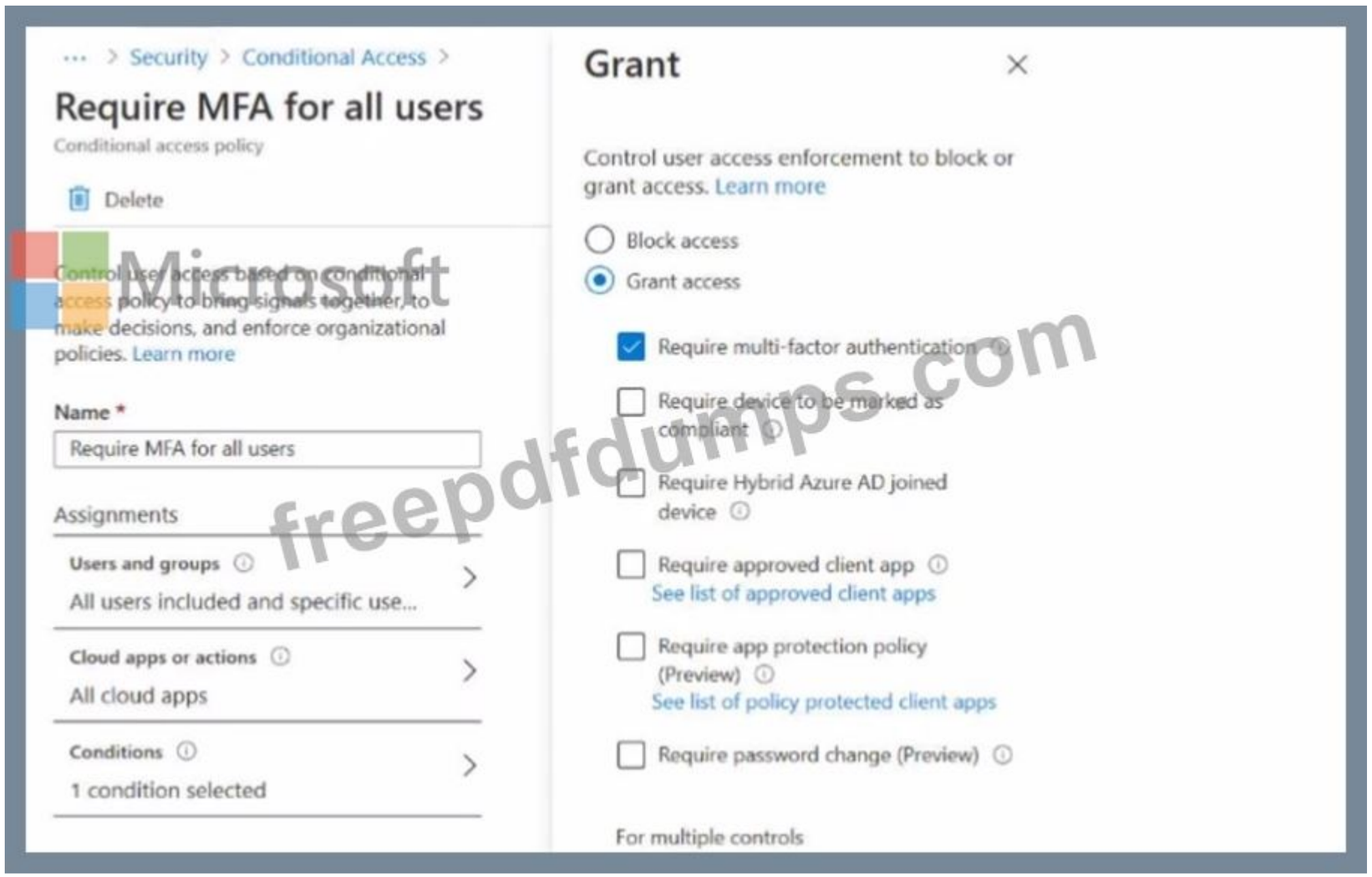
You enable self-service password reset for Group1 and configure security questions as the only authentication method for self-service password reset.
You need to identify which user must answer security questions to reset his password.
Which user should you identify?
A. User2

B. User4
C. User1
D. User3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
You have a Microsoft Sentinel workspace that has an Azure Active Directory (Azure AD) connector and an Office 365 connector.
From the workspace, you plan to create an analytics rule that will be based on a custom query and will run a security play.
You need to ensure that you can add the security playbook and the custom query to the rule.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

NEW QUESTION: 70
You have a Microsoft 365 Tenant.
A conditional access policy is configured for the tenant as shown in the Policy exhibit. (Click the Policy tab.)



The User Administrator role a configured as shown in the Hole setting exhibit (Click the Role setting tab.)

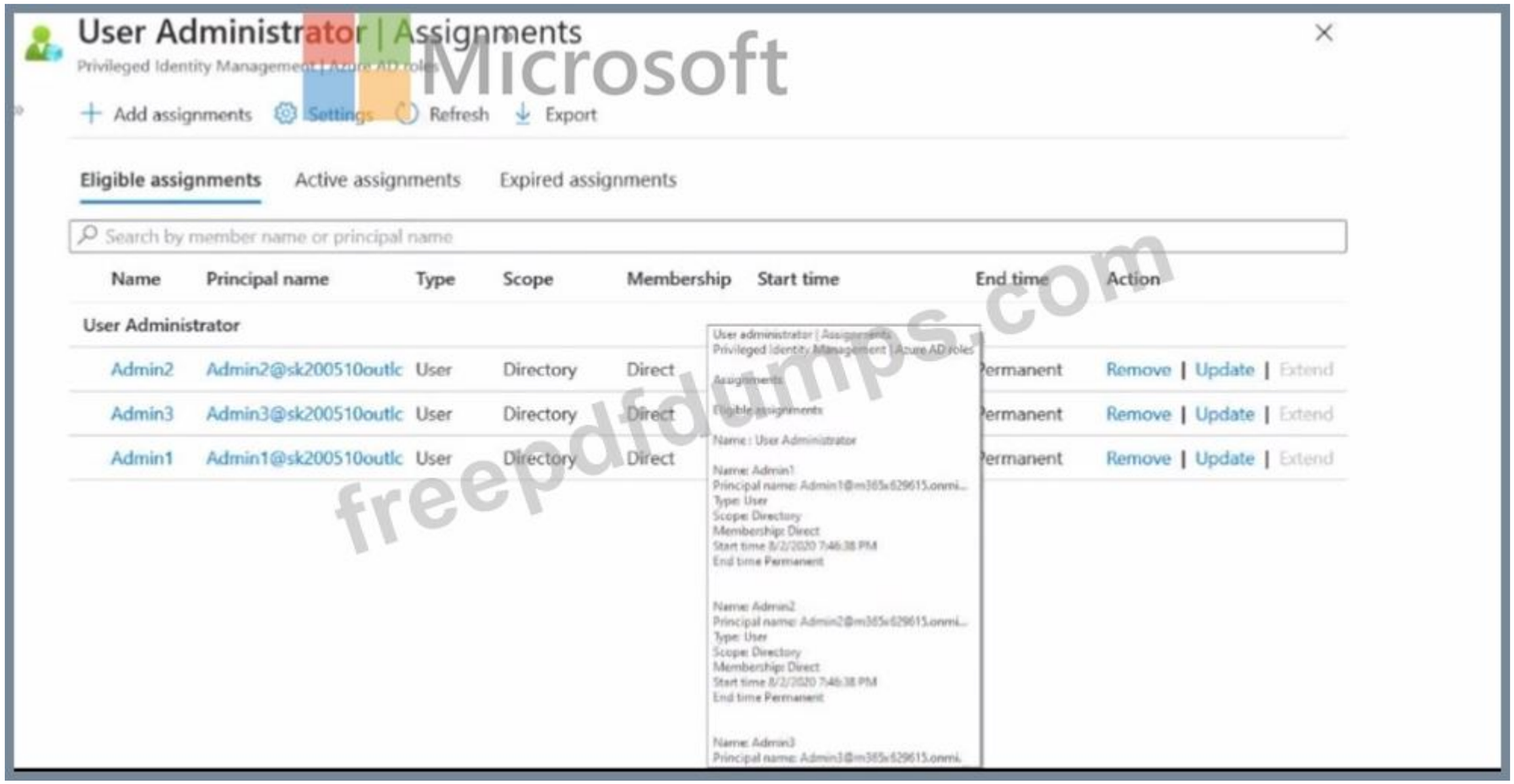
Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	1 Member(s), 0 Group(

Assignment

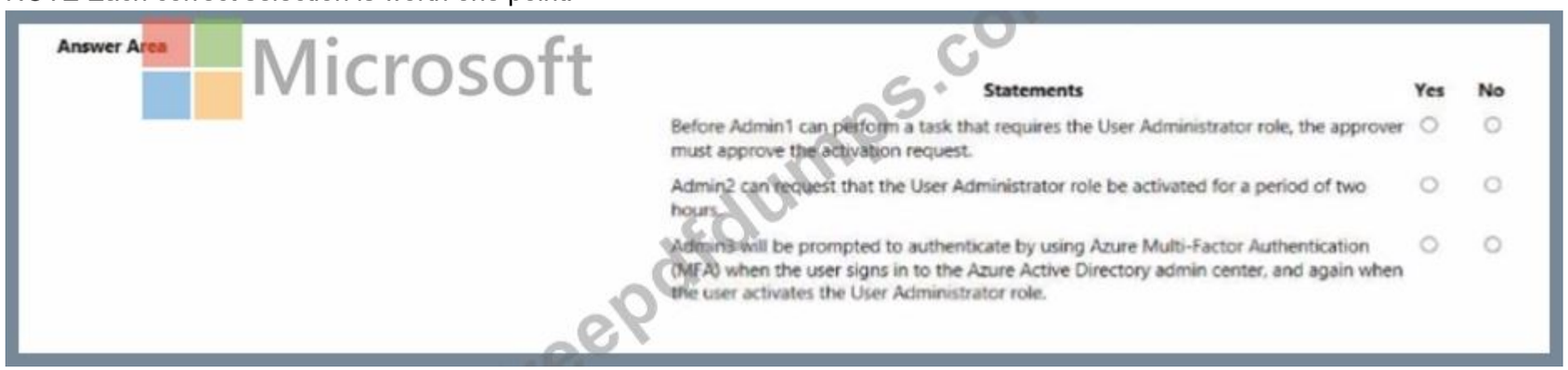
Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication o...	Yes

The User Administrator role has the assignments shown in the Assignments exhibit (Click the Assignments tab.)

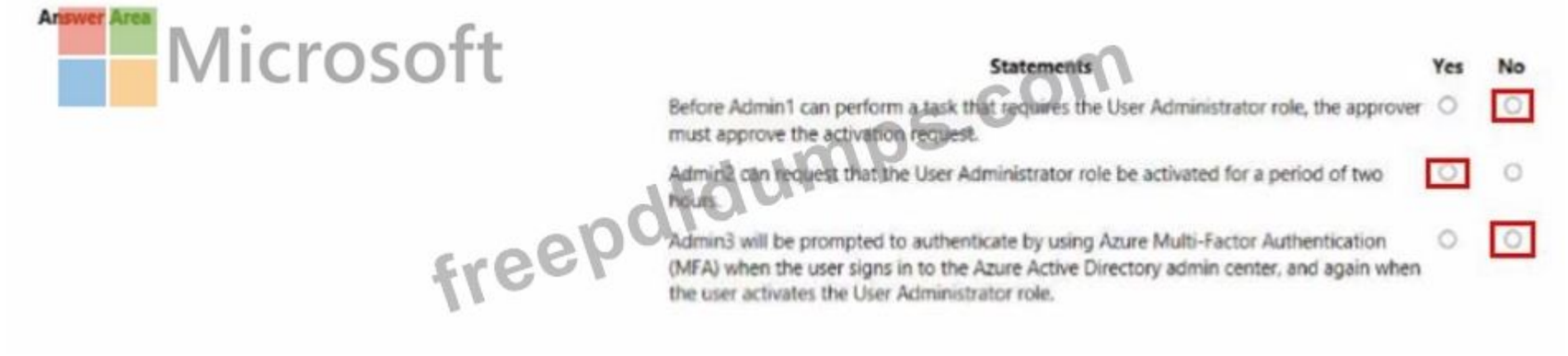


For each of the following statements, select yes If the statement is true. Otherwise select No.

NOTE Each correct selection is worth one point.



Answer:



NEW QUESTION: 71
You have a Microsoft 365 subscription.
You have a team named Team1 in Microsoft Teams.
You plan to place all the content in Team1 on hold.
You need to identify which mailbox and which Microsoft SharePoint site collection are associated to Team1.
Which cmdlet should you use?
A. Get-MailUser
B. Get-UnifiedGroup
C. Get-TeamChannel
D. Get-TeanMessagingSettings
Answer: (SHOW ANSWER)

NEW QUESTION: 72
You create an Azure Sentinel workspace.
You configure Azure Sentinel to ingest data from Azure Active Directory (Azure AD).
In the Azure Active Directory admin center, you discover Azure AD Identity Protection alerts. The Azure Sentinel workspace shows the status as shown in the following exhibit.

In Azure Log Analytics, you can see Azure AD data in the Azure Sentinel workspace.
What should you configure in Azure Sentinel to ensure that incidents are created for detected threats?
A. data connectors
B. rules
C. workbooks
D. hunting queries
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-custom

NEW QUESTION: 73

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

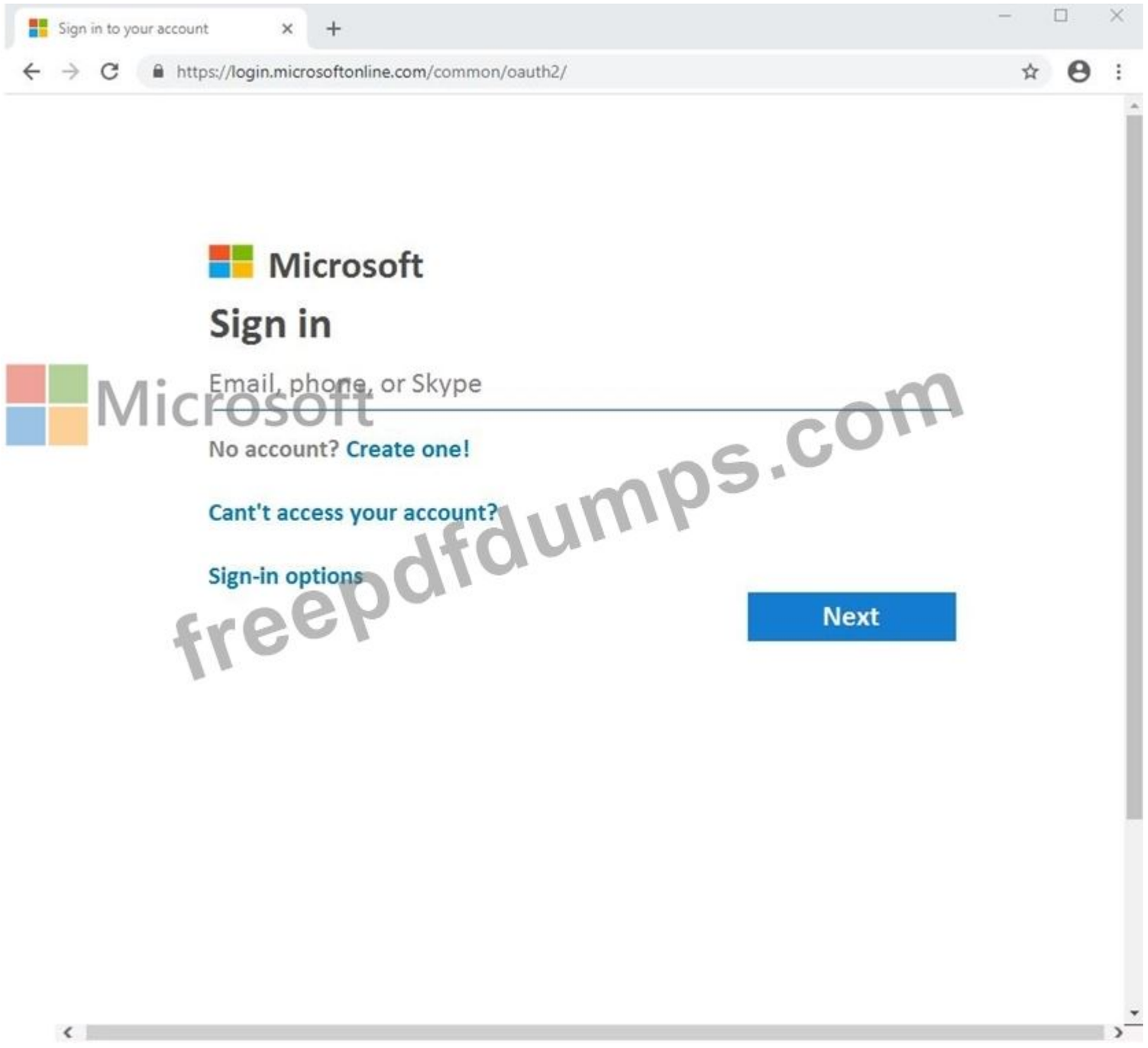
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe00019@onmicrosoft.com
Microsoft 365 Password: #HSP.ug?$p6un
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11122308

Microsoft

Get your work done
with Office 365

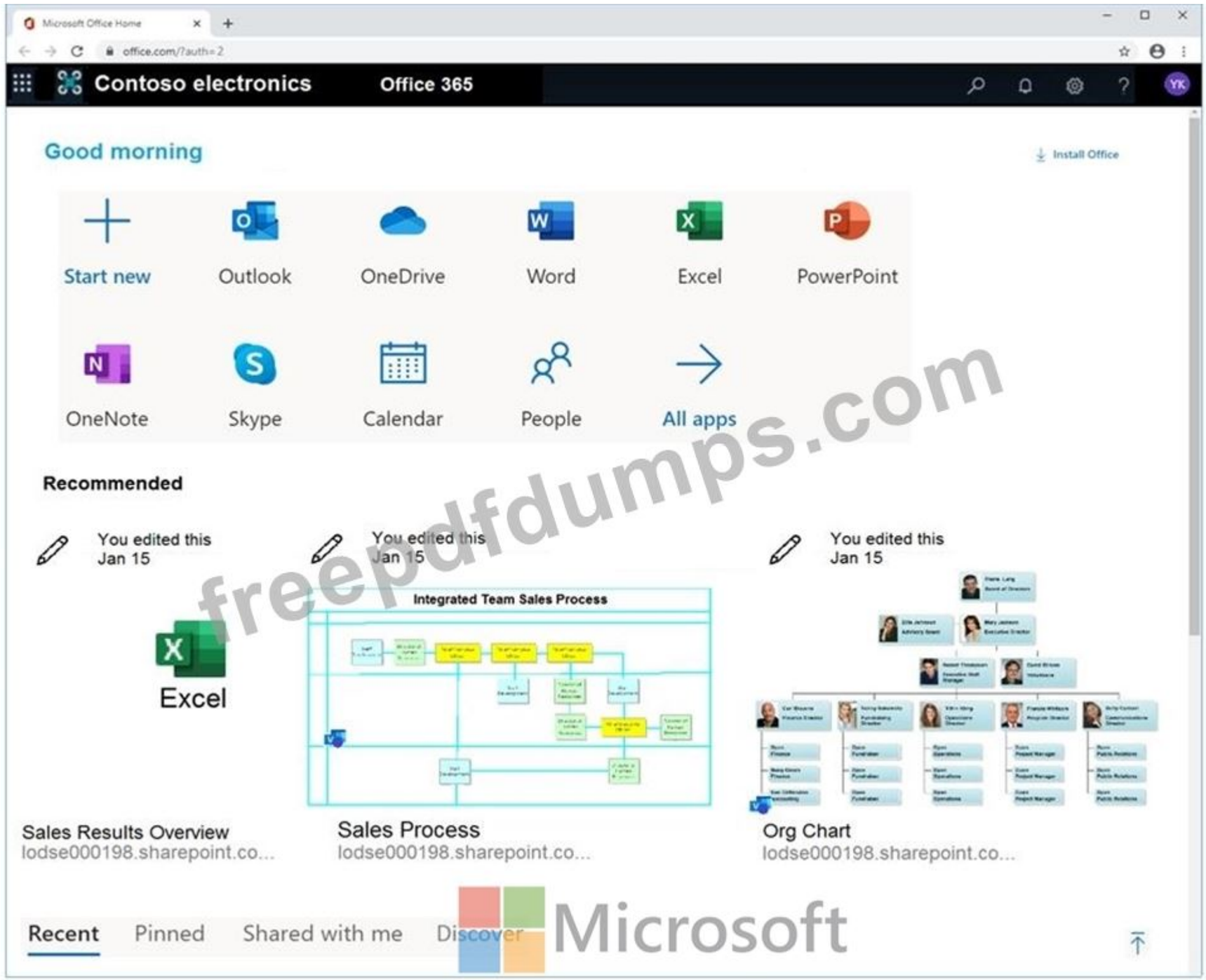
Microsoft

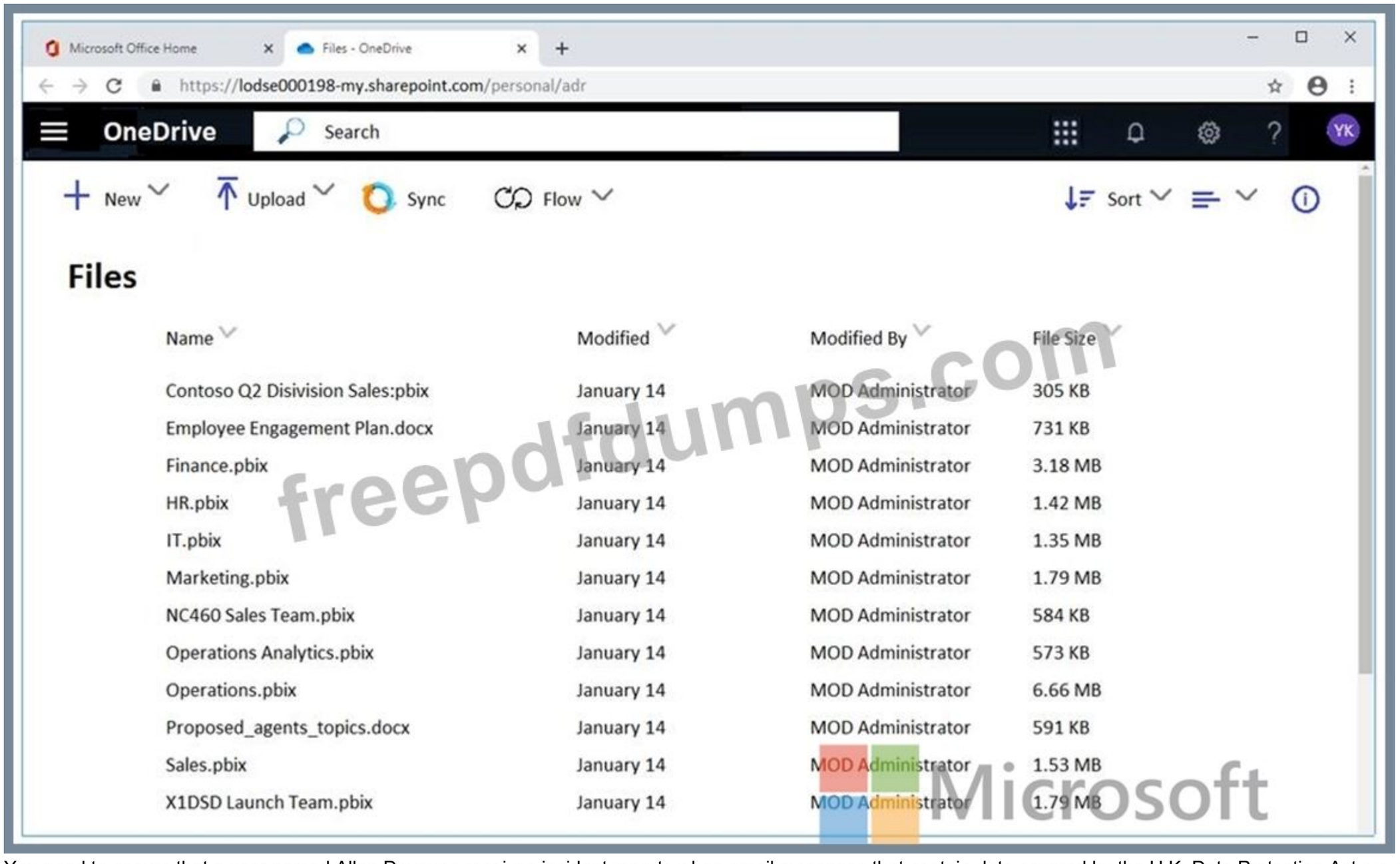
Microsoft

Microsoft

Access Office 365 apps and documents in one place with

Office.com





You need to ensure that a user named Allan Deyoung receives incident reports when email messages that contain data covered by the U.K. Data Protection Act are sent outside of your organization.

To complete this task, sign in to the Microsoft 365 admin center.

Answer:

1. In the Security & Compliance Center > left navigation > Data loss prevention > Policy > + Create a policy.
2. Choose the U.K. Data Protection Act template > Next.
3. Name the policy > Next.
4. Choose All locations in Office 365 > Next.
5. At the first Policy Settings step just accept the defaults,
6. After clicking Next, you'll be presented with an additional Policy Settings page Deselect the Show policy tips to users and send them an email notification option.

Select the Detect when content that's being shared contains option, and configure the number instances to be 10.

Select the Send incident reports in email option.
Select the Choose what to include in the report and who receives it link to add Allan Deyoung as a recipient.
7. > Next
8. Select the option to turn on the policy right away > Next.
9. Click Create to finish creating the policy.
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies?view=o365-worldwide
https://docs.microsoft.com/en-us/microsoft-365/compliance/what-the-dlp-policy-templates-include?view=o365-worldwide

NEW QUESTION: 74
You have multiple Microsoft 365 subscriptions.
You need to build an application that will retrieve the Microsoft Secure Score data of each subscription.
What should you use?
A. the Azure Monitor REST API
B. the Microsoft Defender for Endpoint API
C. the Microsoft Graph Security API
D. the Microsoft Office 365 Management API
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
You have a Microsoft 365 E5 subscription that contains three users named User1, User2 and User3.
You have Azure AD roles that have the role activation settings shown in the following table.

Name	Require justification on activation	Require approval to activate	Approver
Role1	No	Yes	User1
Role2	Yes	No	*Not applicable*

You have Azure AD roles that have the role assignment settings shown in the following table.

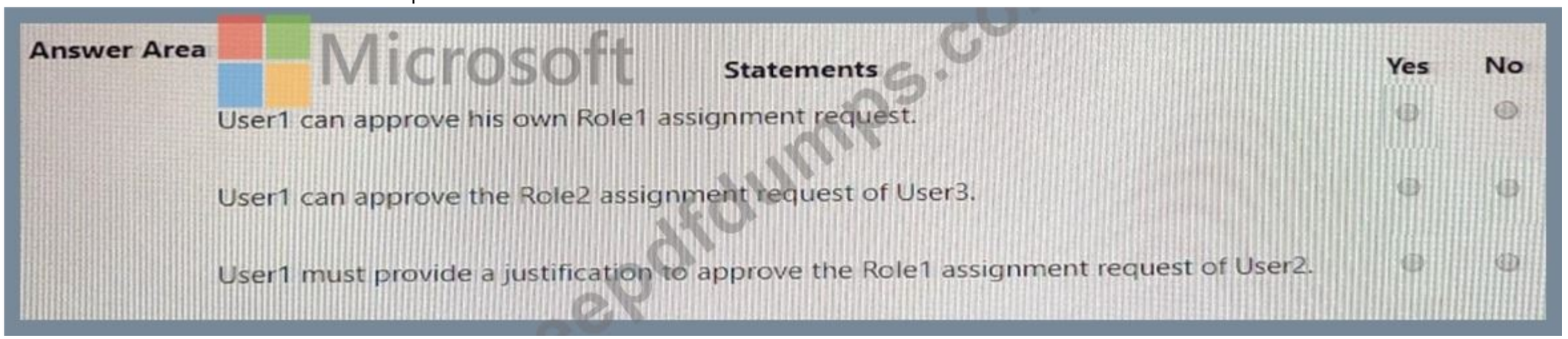
Name	Allow permanent eligible assignment	Allow permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have eligible users assigned as shown in the following table.

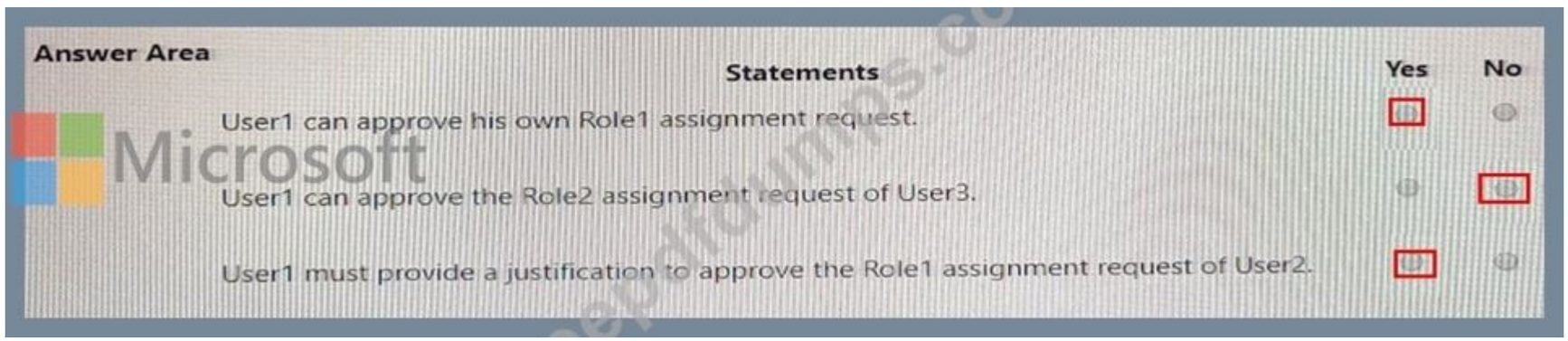
Name	Eligible assignment
Role1	User1, User2
Role2	User3

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:



NEW QUESTION: 76

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

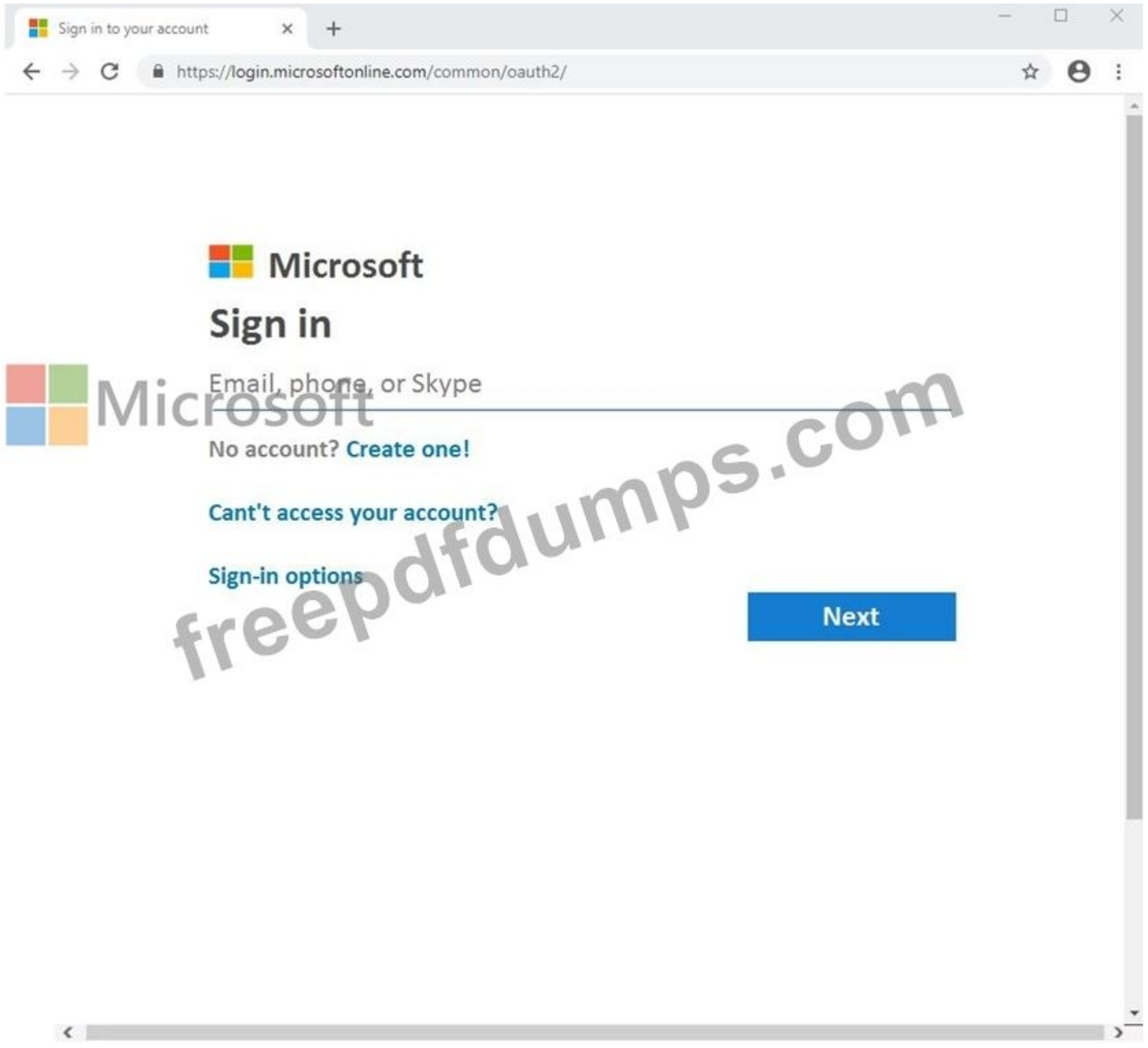
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe00019@onmicrosoft.com
Microsoft 365 Password: #HSP.ug?$p6un
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11122308

Microsoft

Get your work done
with Office 365

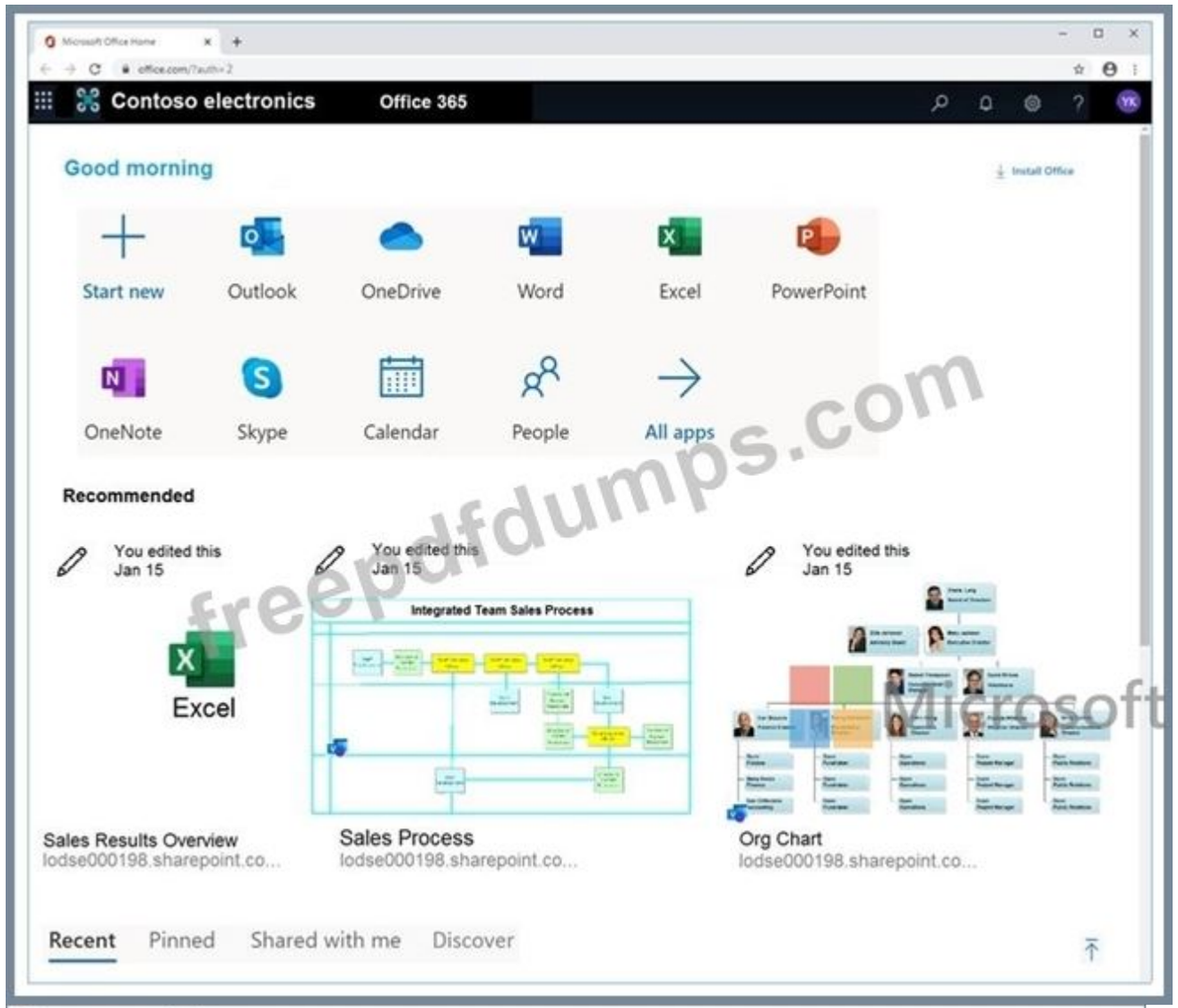
Microsoft

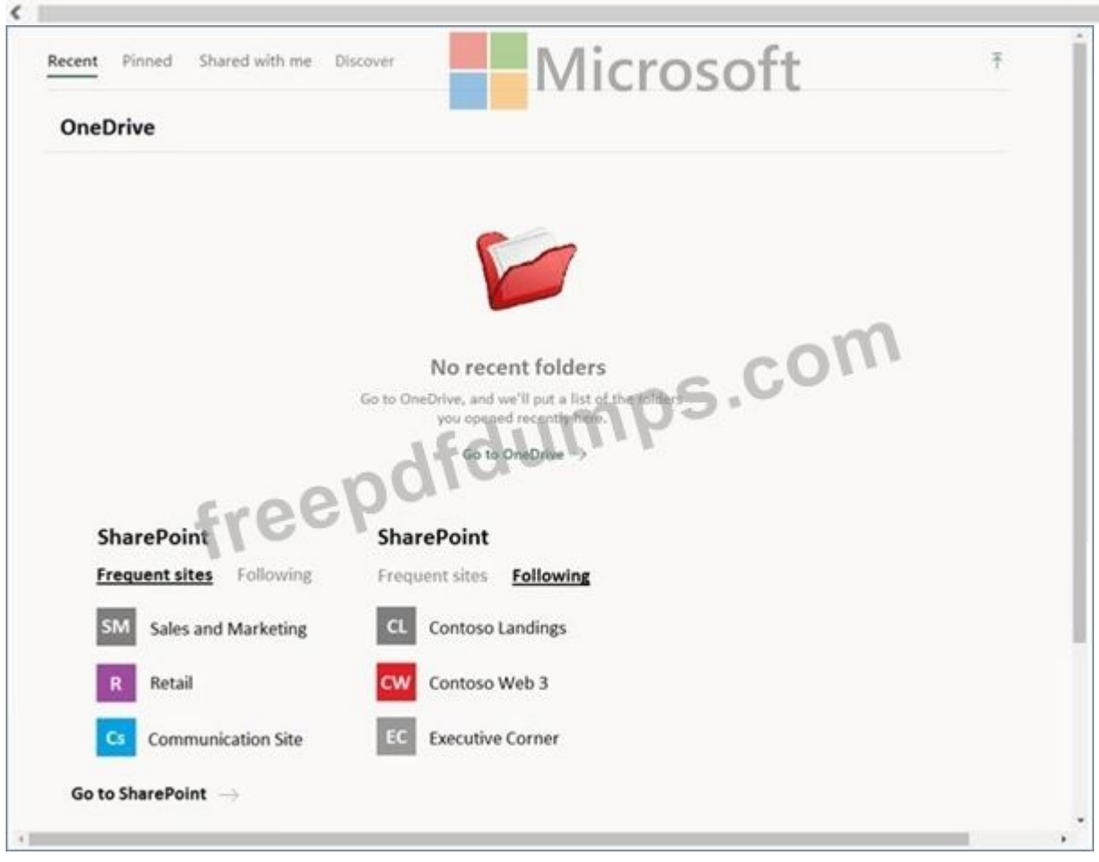
Microsoft

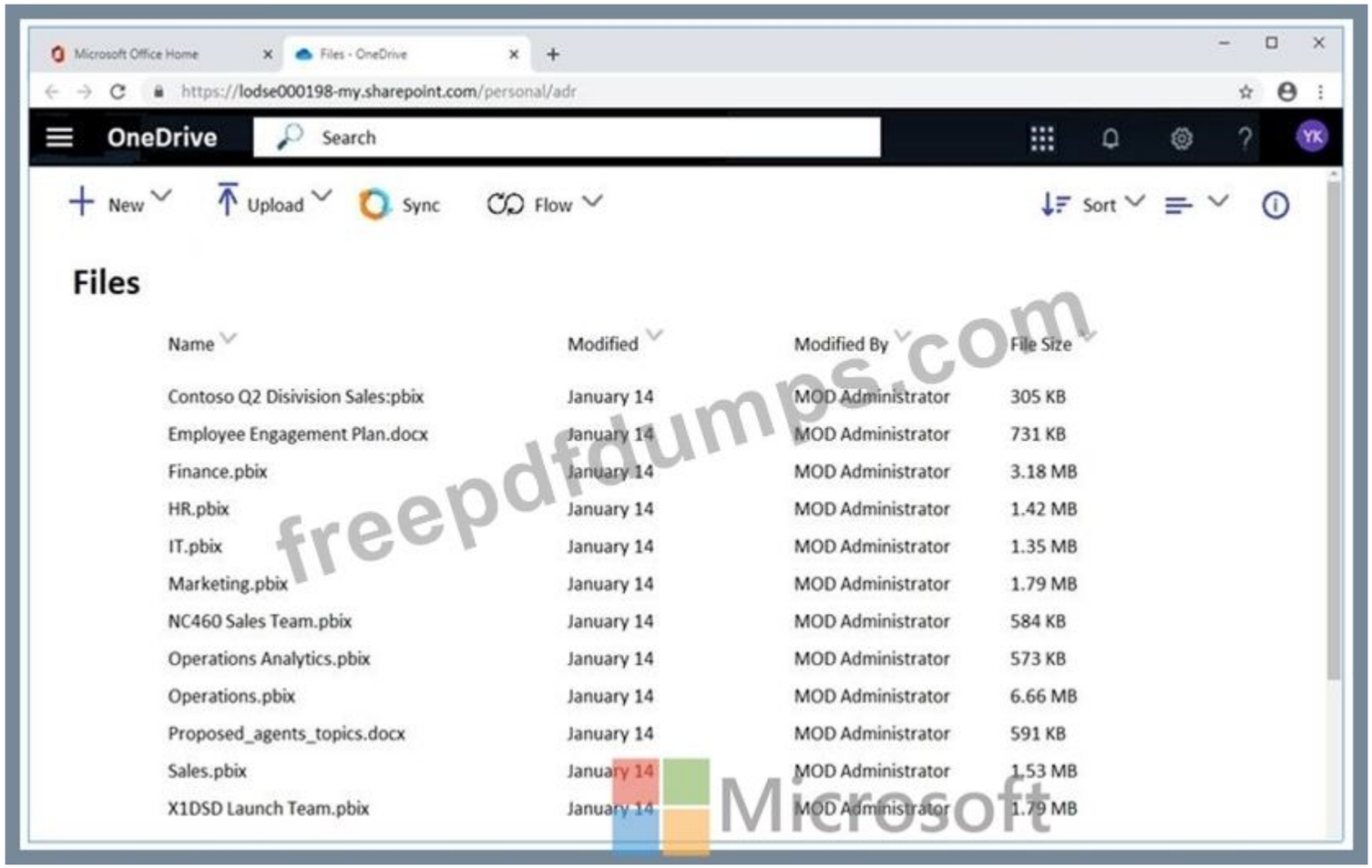
Microsoft

Access Office 365 apps and documents in one place with

Office.com







You plan to create a script to automate user mailbox searches. The script will search the mailbox of a user named Allan Deyoung for messages that contain the word injunction.
You need to create the search that will be included in the script.
To complete this task, sign in to the Microsoft 365 admin center.

Answer:

Step 1: Create a CSV file that contains information about the searches you want to run The comma separated value (CSV) file that you create in this step contains a row for each user that want to search. You can search the user's Exchange Online mailbox (which includes the archive mailbox, if it's enabled) and their OneDrive for Business site. Or you can search just the mailbox or the OneDrive for Business site. You can also search any site in your SharePoint Online organization. The script that you run in Step 3 will create a separate search for each row in the CSV file.

1. Copy and paste the following text into a .txt file using NotePad. Save this file to a folder on your local computer. You'll save the other scripts to this folder as well.

ExchangeLocation,SharePointLocation,ContentMatchQuery,StartDate,EndDate sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2000,12/31/2005 sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2006,12/31/2010 sarad@contoso.onmicrosoft.com,https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com,(lawsuit OR legal),1/1/2011,3/21/2016
,https://contoso.sharepoint.com/sites/contoso,,,3/21/2016
,https://contoso-my.sharepoint.com/personal/davidl_contoso_onmicrosoft_com,,1/1/2015,
,https://contoso-my.sharepoint.com/personal/janets_contoso_onmicrosoft_com,,1/1/2015, The first row, or header row, of the file lists the parameters that will be used by New-ComplianceSearch cmdlet to create a new Content Searches. Each parameter name is separated by a comm a. Make sure there aren't any spaces in the header row. Each row under the header row represents the parameter values for each search. Be sure to replace the placeholder data in the CSV file with your actual data.

2. Open the .txt file in Excel, and then use the information in the following table to edit the file with information for each search.

Parameter	Description
ExchangeLocation	The SMTP address of the user's mailbox.
SharePointLocation	The URL for the user's OneDrive for Business site or the URL for any site in your organization. For the URL for OneDrive for Business sites, use this format: https://<your organization>-my.sharepoint.com/personal/<user alias>_<your organization>_onmicrosoft_com. For example, https://contoso-my.sharepoint.com/personal/sarad_contoso_onmicrosoft_com.
ContentMatchQuery	The search query for the search. For more information about creating a search query, see Keyword queries and search conditions for Content Search.
StartDate	For email, the date on or after a message was received by a recipient or sent by the sender. For documents on SharePoint or OneDrive for Business sites, the date on or after a document was last modified.
EndDate	For email, the date on or before a message was sent by a sent by the user. For documents on SharePoint or OneDrive for Business sites, the date on or before a document was last modified.

3. Save the Excel file as a CSV file to a folder on your local computer. The script that you create in Step 3 will use the information in this CSV file to create the searches.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/create-report-on-and-delete-multiple-content-searches?view=o365-worldwide Keyword queries and search conditions for Content Search

https://docs.microsoft.com/en-us/microsoft-365/compliance/keyword-queries-and-search-conditions?view=o365-worldwide

NEW QUESTION: 77

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

Name	Role
Admin1	Groups administrator
Admin2	User administrator

You add internal as a blocked word in the group naming policy for contoso.com.

You add Contoso- as prefix in the group naming policy for 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.

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	○	○
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	○	○
Admin2 can create a security group named Contoso-internal.	○	○

Answer:

Statements	Yes	No
Admin1 can create an Office 365 group named Distribution.	○	○
Admin2 can create an Office 365 group named Contoso-FinanceInternal.	○	○
Admin2 can create a security group named Contoso-internal.	○	○

User Admin and Global Admin are exempt from group password policies.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/solutions/groups-naming-policy?view=o365-worldwide

NEW QUESTION: 78

You have a Microsoft 365 subscription that contains 20 data loss prevention (DLP) policies.

You need to identify the following:

* Rules that are applied without Triggering a policy alert
* The top 10 files that have matched DLP policies
* Alerts that are miscategorized

Which report should you use 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.

NOTE: Each correct selection is worth one point.

Reports

- DLP policy matches
- False positive and override
- Incident reports

Answer Area

Rules that are applied without triggering a policy alert: [ ]

The top 10 files that have matched DLP policies: [ ]

Alerts that are miscategorized: [ ]

Answer:

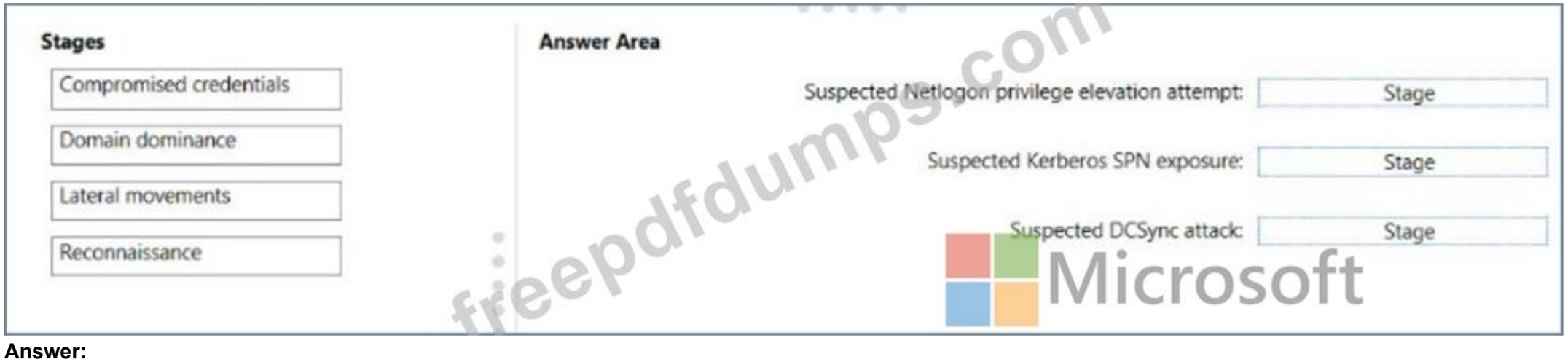
NEW QUESTION: 79

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

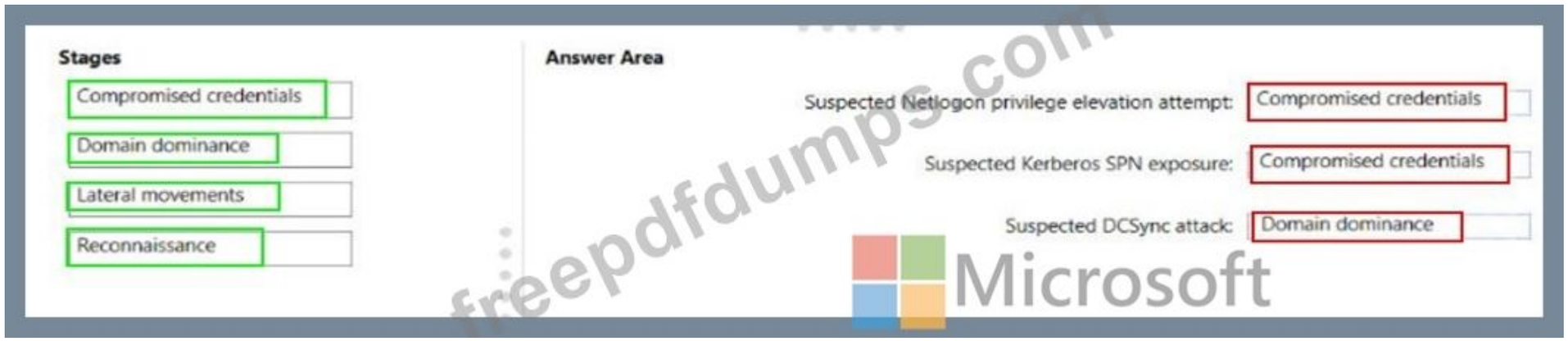
You receive the following alerts:

* Suspected Netlogon privilege elevation attempt
* Suspected Kerberos SPN exposure
* Suspected DCSync attack

To which stage of the cyber-attack kill chain does each alert map? To answer, drag the appropriate alerts to the correct stages. Each alert may be used once. more than once, or rot at all. You may need to drag the split bar between panes or scroll to view content



Answer:



NEW QUESTION: 80

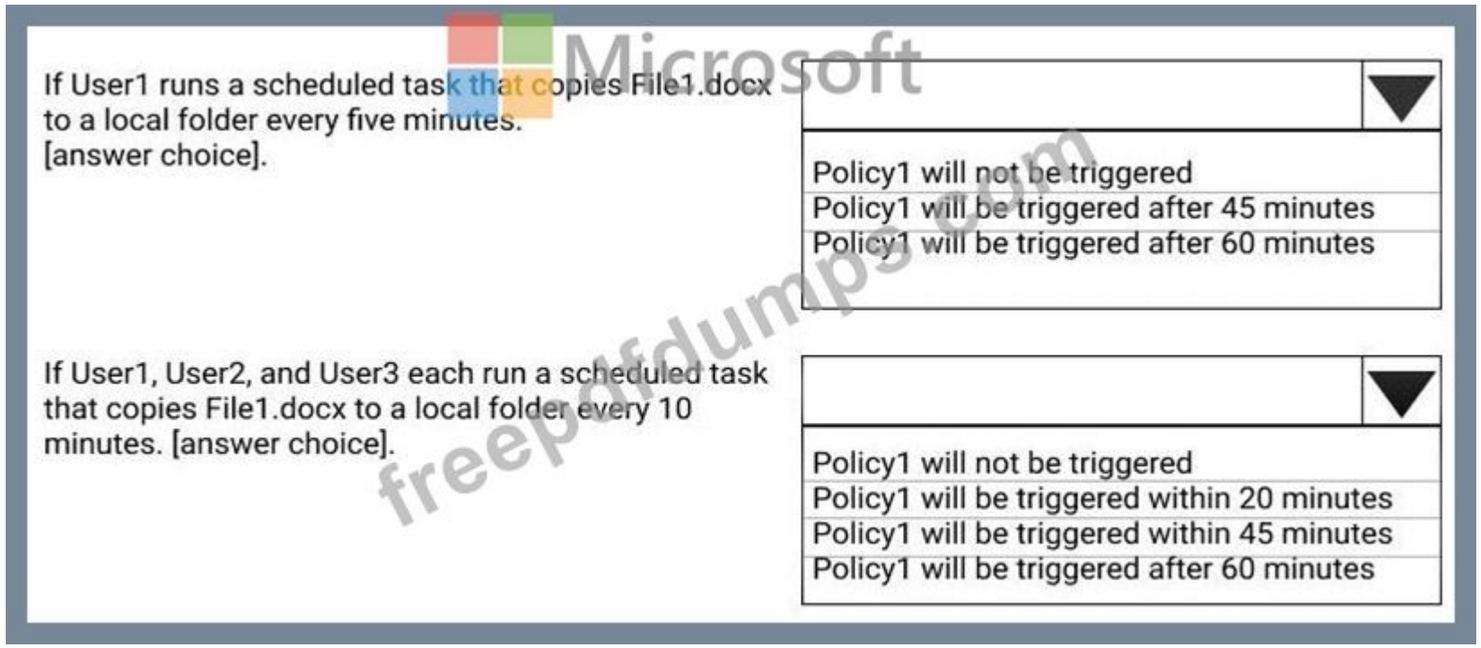
You have a Microsoft 365 subscription that include three users named User1, User2, and User3.

A file named File1.docx is stored in Microsoft OneDrive. An automated process updates File1.docx every minute.

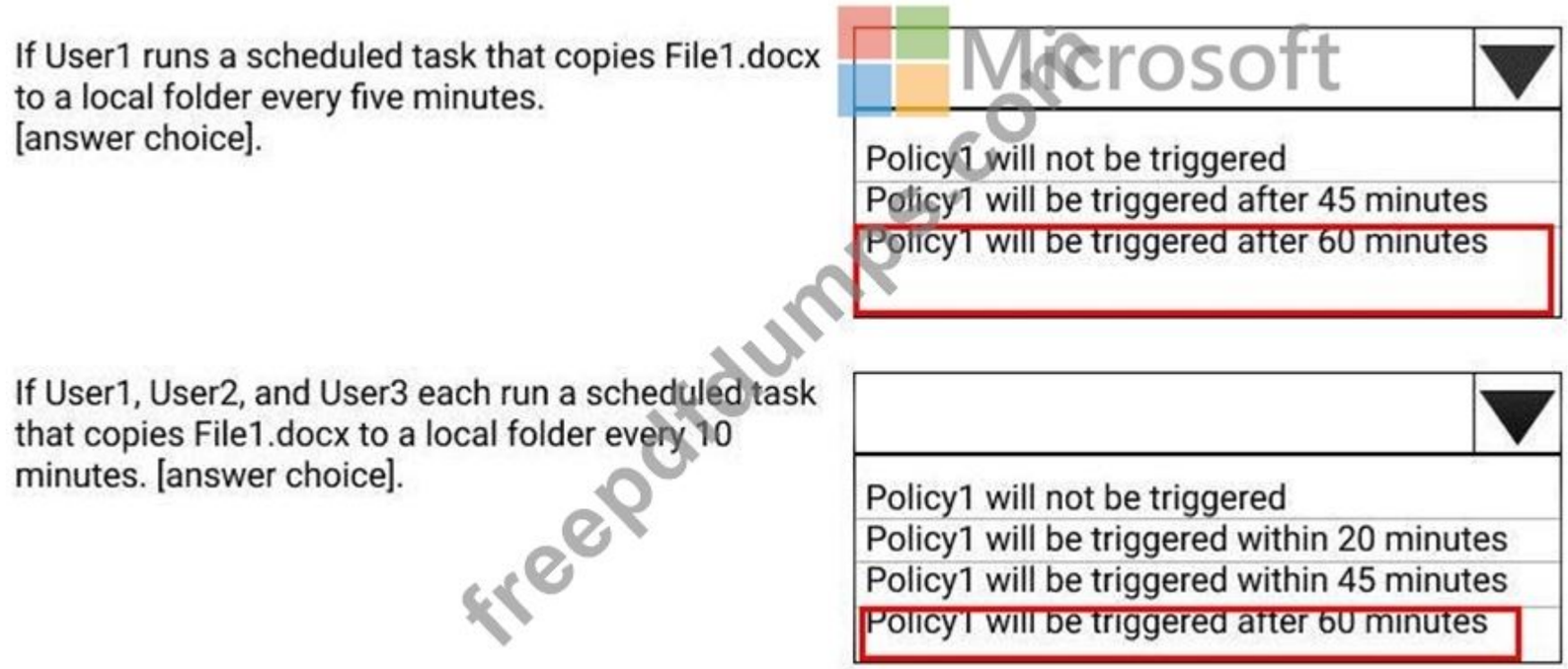
You create an alert policy named Policy1 as shown in the following exhibit.

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

NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

NEW QUESTION: 81

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 questions 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.

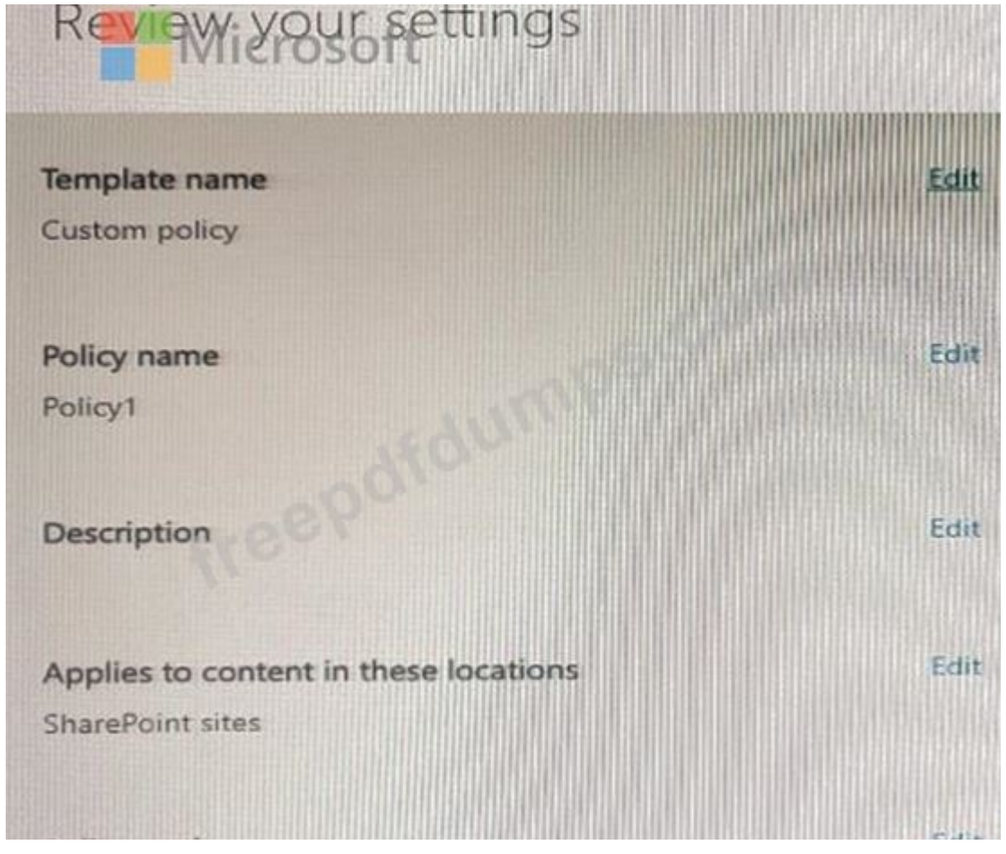
You have a user named User1. Several users have full access to the mailbox of User1.

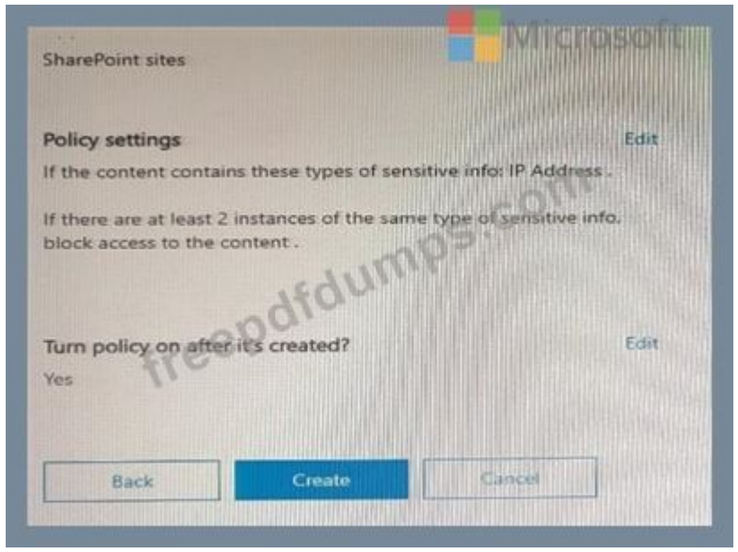
Some email messages sent to User1 appear to have been read and deleted before the user viewed them.
When you search the audit log in Security & Compliance to identify who signed in to the mailbox of User1, the results are blank.
You need to ensure that you can view future sign-ins to the mailbox of User1.
You run the Set-AuditConfig -Workload Exchange command.
Does that meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-audit/set-auditconfig?view=exchange-ps

NEW QUESTION: 82
You have a Microsoft E5 subscription that contains two users named User 1 and User2.
You have a Microsoft SharePoint site named Site1. Site1 stores files that contain IP addresses as shown in the following table.

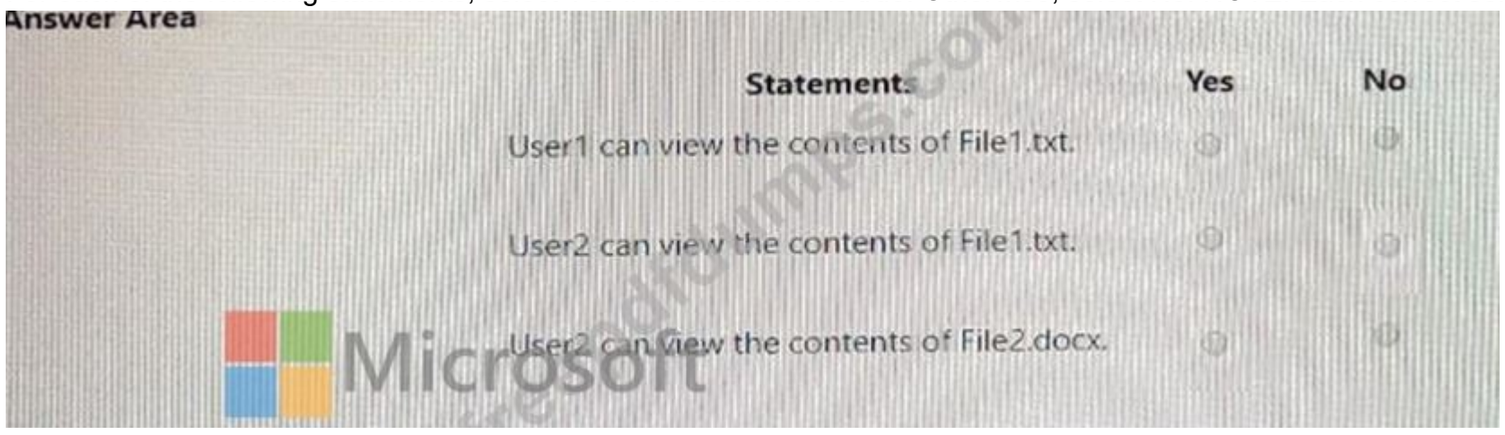
Name	Number of IP addresses
File1.txt	3
File2.docx	1

User1 is assigned the SharePoint admin role for Site1. User2 is a member of Sile1. You create the data loss prevention (DLP)1 policy shown in the following exhibit.

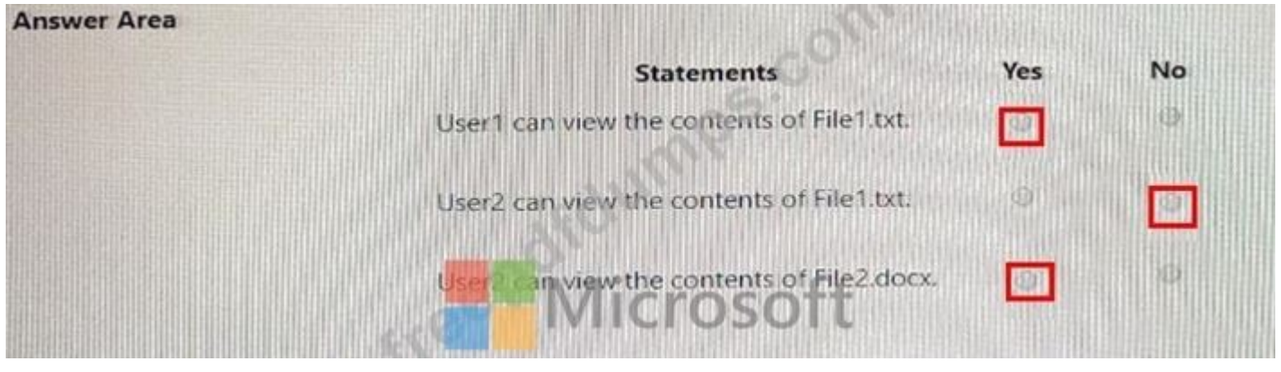




For each of the following statements, select Yes if the statement is true: Otherwise, select No. NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 83

You have a Microsoft 365 description that contains a user named User1.

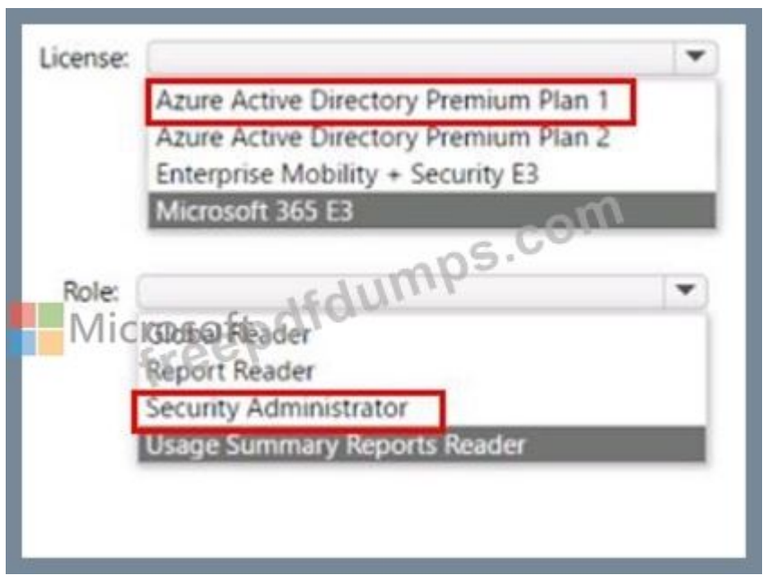
You need to that User1 can review registration and usage activity reports for Azure Multi-Factor Authentication (Azure MFA) for the subscription. The solution must meet the following requirements:

* Minimize Costs

* use the principle Of least privilege

What should you assign to user1?

Answer:



NEW QUESTION: 84
Your network contains an on-premises Active Directory domain and a Microsoft 365 subscription.
You plan to deploy a hybrid Azure Active Directory (Azure AD) tenant that has Azure AD Identity Protection risk policies enabled.
You need to configure Azure AD Connect to support the planned deployment.
Which Azure AD Connect authentication method should you select?
A. Federation with PingFederate
B. Pass-through authentication
C. Password Hash Synchronization
D. Federation with AD FS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 85
You haw a Microsoft 365 subscription.
You receive a General Data Protection Regulation (GOPR) request for the custom dictionary of a user From The Compliance admin center you need to create a content search, should you configure the content search?
A. .Condition; Type Operator Equals any of Value Office Roaming Service

B. Condition: We type Operator Equals any of Value dic
C. Condition: Type Operator Equals any of Value Documents
D. Condition: Title Operator Equals any of Value Normal. dot
Answer: (SHOW ANSWER)

NEW QUESTION: 86
You have a hybrid Microsoft 365 deployment that contains the Windows 10 devices shown in the following table.

Name	Trusted Platform Module (TPM) version	Joined to	Microsoft Intune enrolled
Device1	v2.0	Active Directory	Yes
Device2	v2.0	Azure Active Directory (Azure AD)	Yes
Device3	v1.3	Azure Active Directory (Azure AD)	Yes

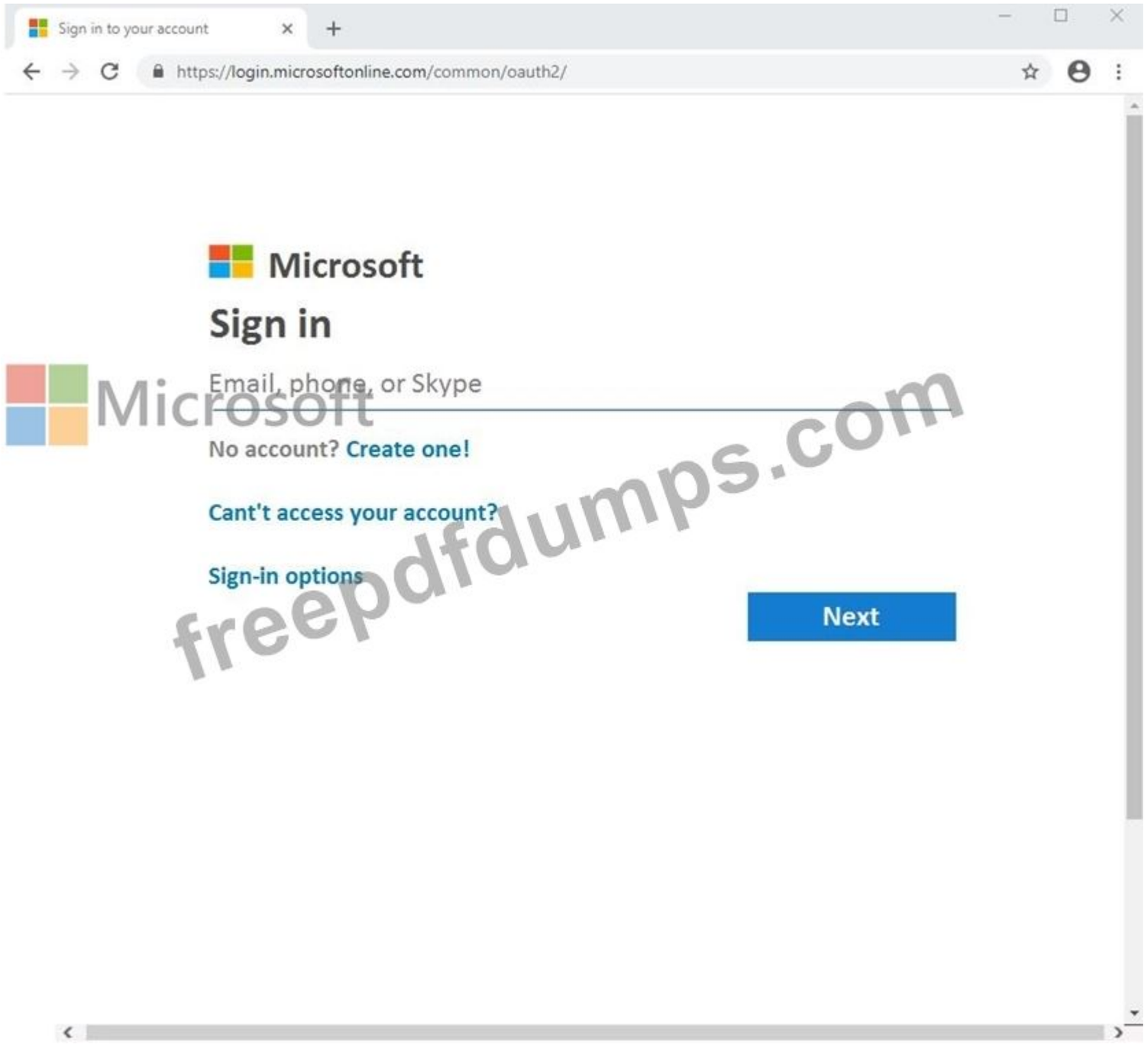
You assign a Microsoft Endpoint Manager disk encryption policy that automatically and silently enables BitLocker Drive Encryption (BitLocker) on all the devices.
Which devices will have BitLocker enabled?
A. Device 1, Device2, and Device3
B. Device2 only
C. Device1 and Device2 only
D. Device2 and Device3 only
Answer: B (LEAVE A REPLY)
To silently enable BitLocker, the device must be Azure AD Joined or Hybrid Azure AD Joined and the device must contain TPM (Trusted Platform Module) 2.0.
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/encrypt-devices

NEW QUESTION: 87
You need to recommend a solution for the user administrators that meets the security requirements for auditing.
Which blade should you recommend using from the Azure Active Directory admin center?
A. Sign-ins
B. Azure AD Identity Protection
C. Authentication methods
D. Access review
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-sign-ins

NEW QUESTION: 88
You have a Microsoft 365 subscription.
Some users access Microsoft SharePoint Online from unmanaged devices.
You need to prevent the users from downloading, printing, and synching files.

What should you do?
A. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) conditional access policy
B. From the SharePoint admin center, configure the Access control settings
C. From the Microsoft Azure portal, create an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy
D. Run the Set-SPODataConnectionSetting cmdlet and specify the AssignmentCollection parameter
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe00019@onmicrosoft.com
Microsoft 365 Password: #HSP.ug?$p6un
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11122308

Microsoft

Get your work done
with Office 365

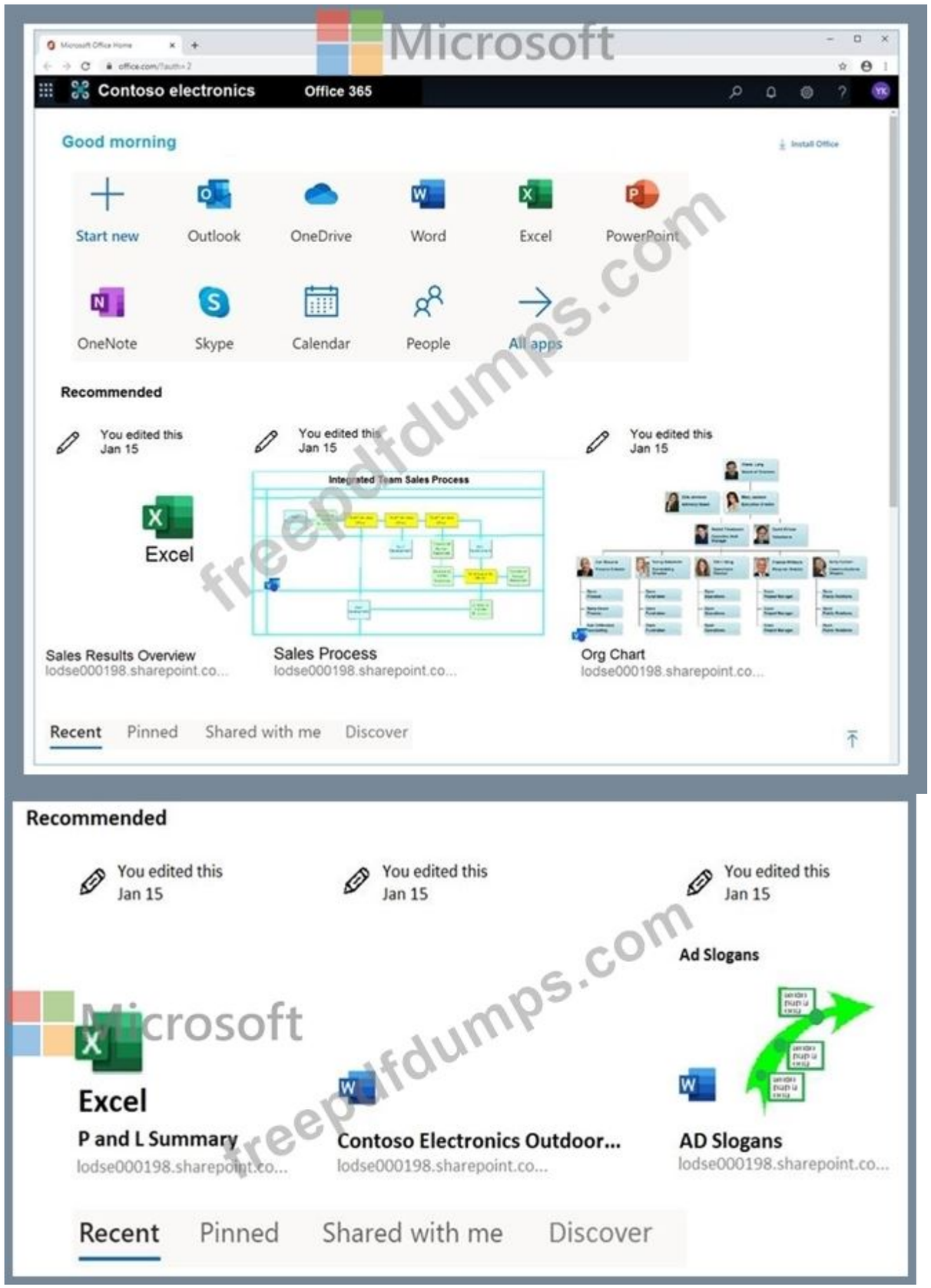
Microsoft

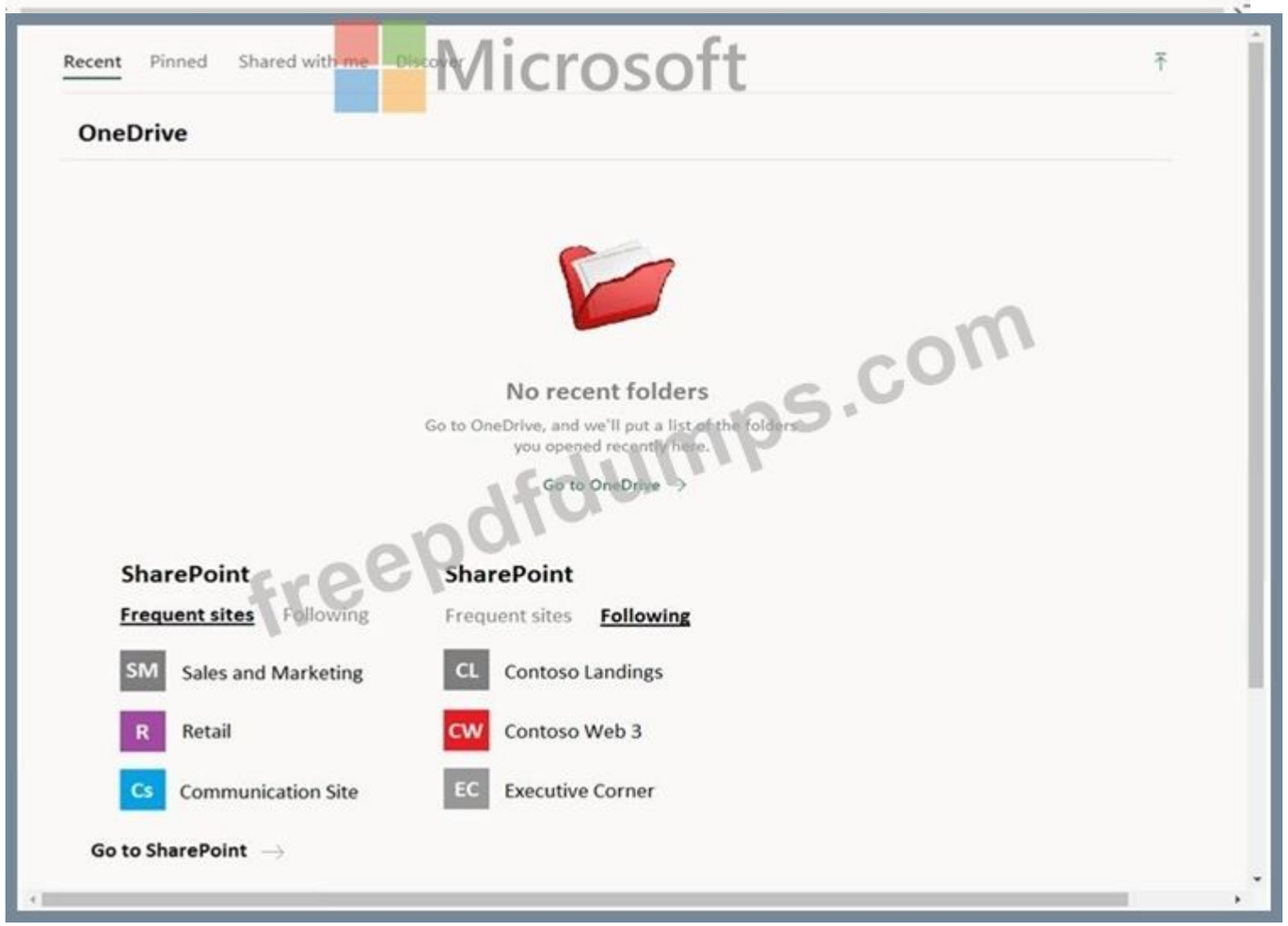
Microsoft

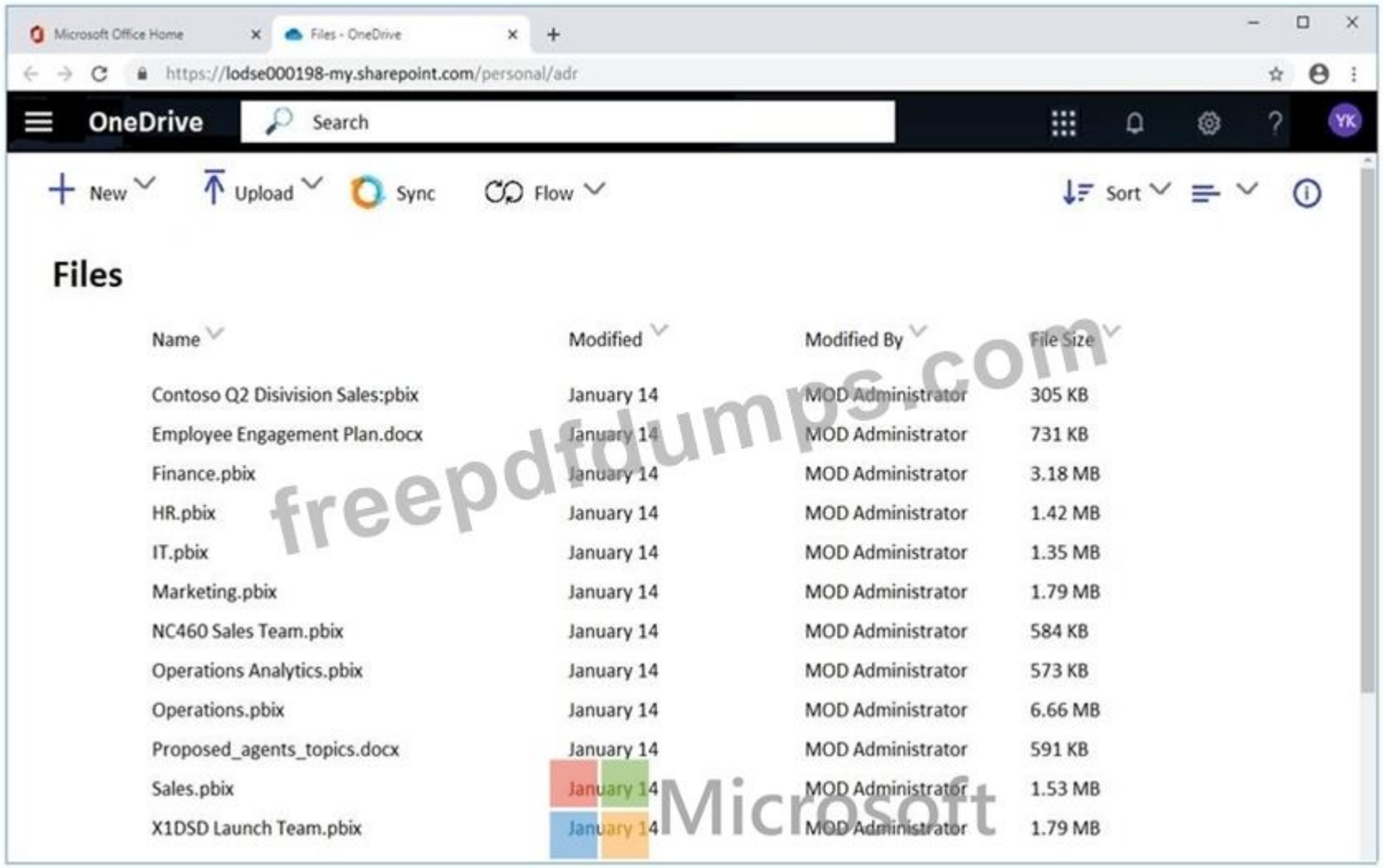
Microsoft

Access Office 365 apps and documents in one place with

Office.com







You need to ensure that all the email messages in the mailbox of a user named Allan Deyoung are retained for a period of 90 days, even if the messages are deleted.

To complete this task, sign in to the Microsoft 365 admin center.

Answer:

1. Navigate to the Exchange Admin Center
2. Navigate to Compliance management > Retention tags, and then click Add +
3. Select the Applied automatically to entire mailbox (default) option.
4. The New retention tag page title and options will vary depending on the type of tag you selected. Complete the following fields:

Name: Enter a name for the retention tag.

Retention action: Select Delete and Allow Recovery option.

Retention period: Select When the item reaches the following age (in days) option.

Comment: User this optional field to enter any administrative notes or comments. The field isn't displayed to users.

5. Navigate to Compliance management > Retention policies, and then click Add +
6. In New Retention Policy, complete the following fields:

Name: Enter a name for the retention policy.

Retention tags: Click Add + to select the tags you want to add to this retention policy.

After you create a retention policy, you must apply it.

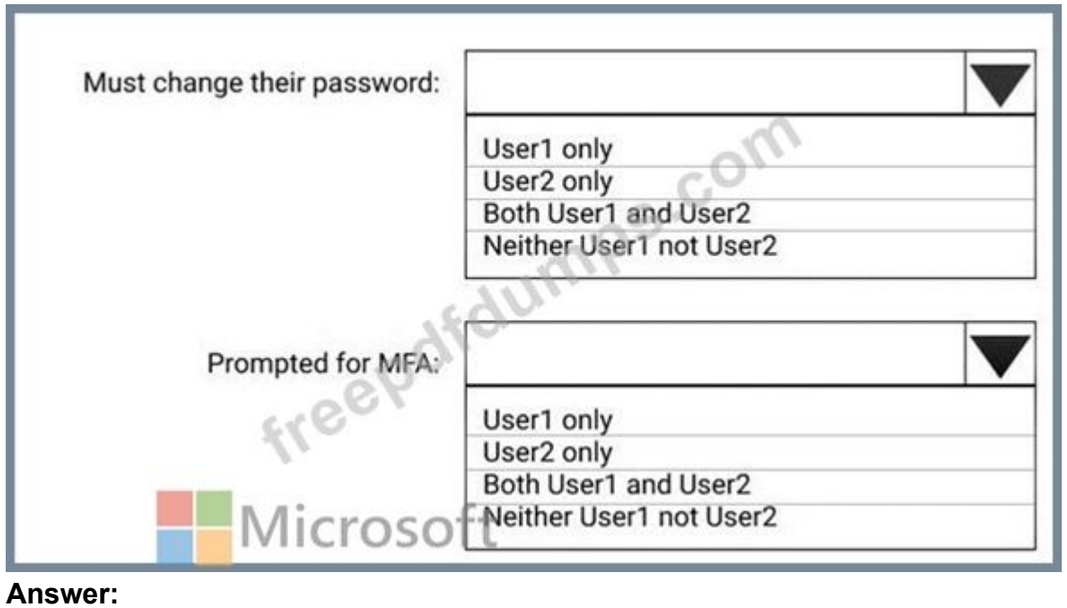
1. Navigate to Recipients > Mailboxes.
2. In the list view, select the mailbox to which you want to apply the retention policy, and then click Edit.
3. In User Mailbox, click Mailbox features.

4. In the Retention policy list, select the policy you want to apply to the mailbox, and then click Save.
Reference:
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy#step-3-apply-a-retention-policy-to-mailbox-users
https://docs.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/apply-retention-policy

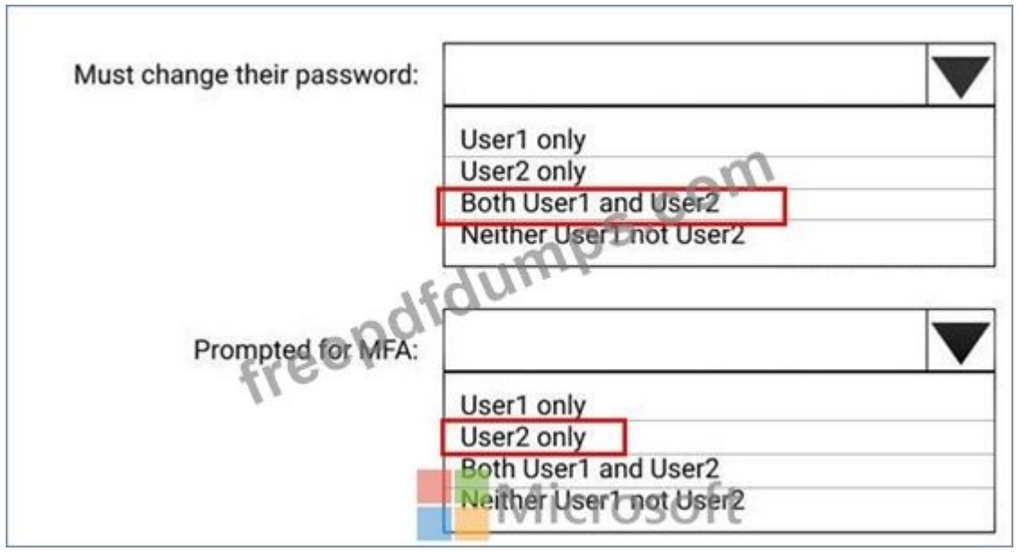
NEW QUESTION: 90
You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com that contains the users shown in the following table.

Name	Member	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:
Assignments: Include Group1, Exclude Group2
Conditions: Sign in risk of Low and above
Access: Allow access, Require password change
You need to identify how the policy affects User1 and User2.
What occurs when User1 and User2 sign in from an unfamiliar location? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 91
You need to recommend a solution to protect the sign-ins of Admin1 and Admin2.
What should you include in the recommendation?
A. a device compliance policy
B. an access review
C. a user risk policy
D. a sign-in risk policy
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy

NEW QUESTION: 92
You have a Microsoft 365 E5 subscription that contains the users shown1 in the following table.

Name	Email addr	Role
Admin1	admin1@contoso.com	Global Administrator
Admin2	admin2@contoso.com	Security Administrator
Admin3	admin3@contoso.com	Security Reader
Admin4	admin4@contoso.com	User Administrator
User1	user1@contoso.com	*None*

Azure AD Identity Protection detects that the account of User1 is at risk and generates an alert. How many users will receive the alert?
A. 1

B. 3
C. 4
D. 2
E. 5
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
You need to meet the technical requirements for User9. What should you do?
A. Assign the Privileged administrator role to User9 and configure a mobile phone number for User9
B. Assign the Compliance administrator role to User9 and configure a mobile phone number for User9
C. Assign the Security administrator role to User9
D. Assign the Global administrator role to User9
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access-to-pim

NEW QUESTION: 94
You have a Microsoft 365 subscription.
The Global administrator role is assigned to your user account. You have a user named Admin1.
You create an eDiscovery case named Case1.
You need to ensure that Admin1 can view the results of Case1.
What should you do first?
A. From the Azure Active Directory admin center, assign a role group to Admin1.
B. From the Microsoft 365 admin center, assign a role to Admin1.
C. From Security & Compliance admin center, assign a role group to Admin1.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions

NEW QUESTION: 95
You have a Microsoft 365 subscription.
A security manager receives an email message every time a data loss prevention (DLP) policy match occurs.
You need to limit alert notifications to actionable DLP events.
What should you do?
A. From the Security & Compliance admin center, modify the Policy Tips of a DLP policy.
B. From the Cloud App Security admin center, apply a filter to the alerts.
C. From the Security & Compliance admin center, modify the User overrides settings of a DLP policy.
D. From the Security & Compliance admin center, modify the matched activities threshold of an alert policy.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

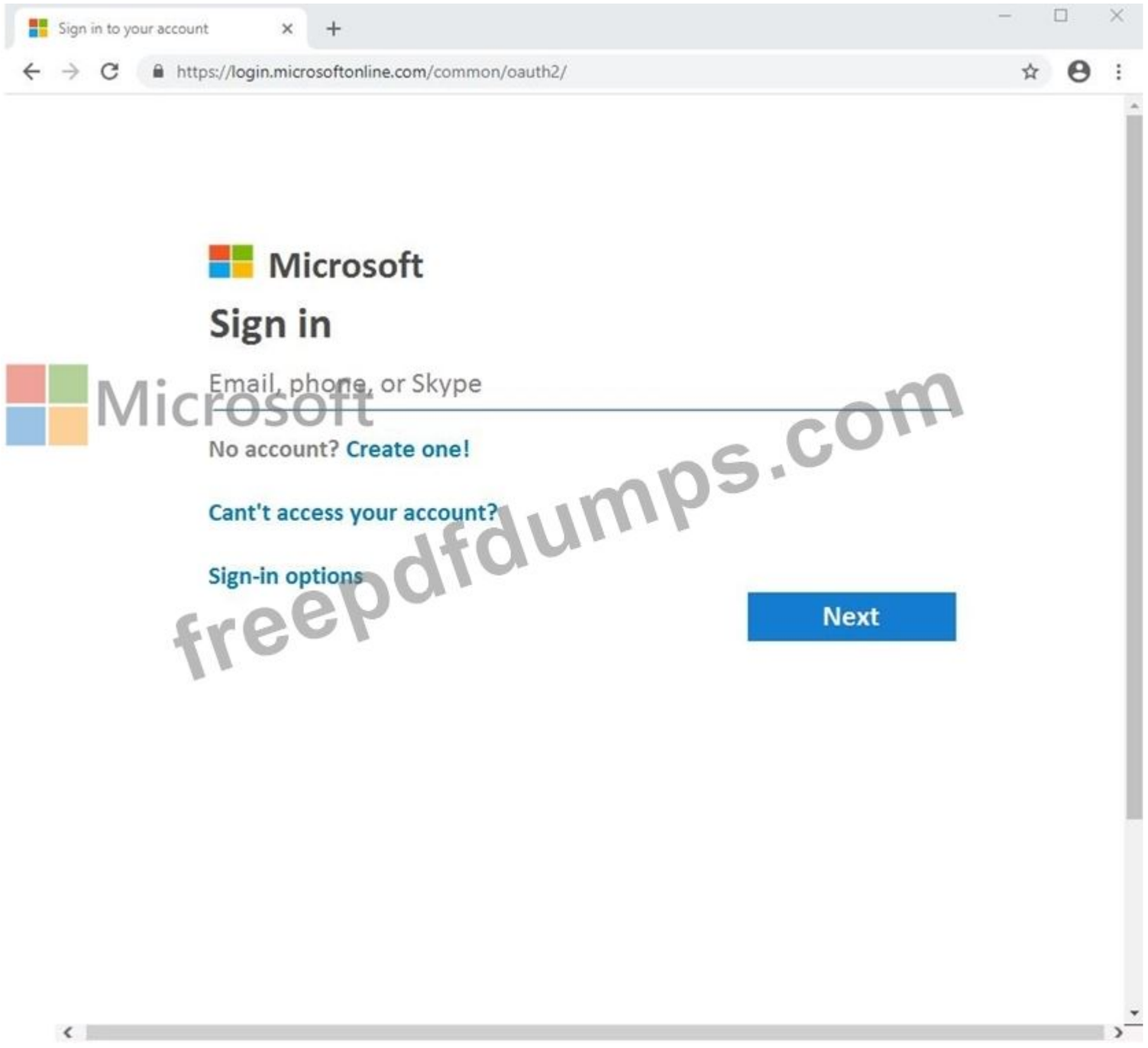
NEW QUESTION: 96
Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.
The security logs of the servers are collected by using a third-party SIEM solution.
You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?
A. Configure Event Forwarding on the domain controllers
B. Configure auditing in the Office 365 Security & Compliance center.
C. Turn on Delayed updates for the Azure ATP sensors.
D. Enable the Audit account management Group Policy setting for the servers.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

NEW QUESTION: 97
You have a Microsoft 365 tenant.
You need to implement a policy to enforce the following requirements:
* If a user uses a Windows 10 device that is NOT hybrid Azure Active Directory (Azure AD) joined, the user must be allowed to connect to Microsoft SharePoint Online only from a web browser. I he user must be prevented from downloading files or syncing files from SharePoint Online.
* If a user uses a Windows 10 device that is hybrid Azure AD joined, the user must be able connect to SharePoint Online from any client application, download files, and sync files.
What should you create?
A. a compliance policy in Microsoft Endpoint Manager that has the Device Health settings configured
B. a conditional access policy in Azure AD that has Session controls configured
C. a conditional access policy in Azure AD that has Client apps conditions configured
D. a compliance policy in Microsoft Endpoint Manager that has the Device Properties settings configured
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Your company has 500 computers.
You plan to protect the computers by using Windows Defender Advanced Threat Protection (Windows Defender ATP). Twenty of the computers belong to company executives.
You need to recommend a remediation solution that meets the following requirements:
Windows Defender ATP administrators must manually approve all remediation for the executives Remediation must occur automatically for all other users What should you recommend doing from Windows Defender Security Center?
A. Configure 20 system exclusions on automation allowed/block lists
B. Configure two alert notification rules
C. Download an offboarding package for the computers of the 20 executives
D. Create two machine groups
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/machine-groupswindows- defender-advanced-threat-protection

NEW QUESTION: 99
You have a Microsoft 365 subscription that contains several Windows 10 devices. The devices are managed by using Microsoft Intune.
You need to enable Windows Defender Exploit Guard (Windows Defender EG) on the devices.
Which type of device configuration profile should you use?
A. Endpoint protection
B. Device restrictions
C. Identity protection
D. Windows Defender ATP
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/intune/endpoint-protection-windows-10

NEW QUESTION: 100
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe00019@onmicrosoft.com
Microsoft 365 Password: #HSP.ug?$p6un
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11122308

Microsoft

Get your work done
with Office 365

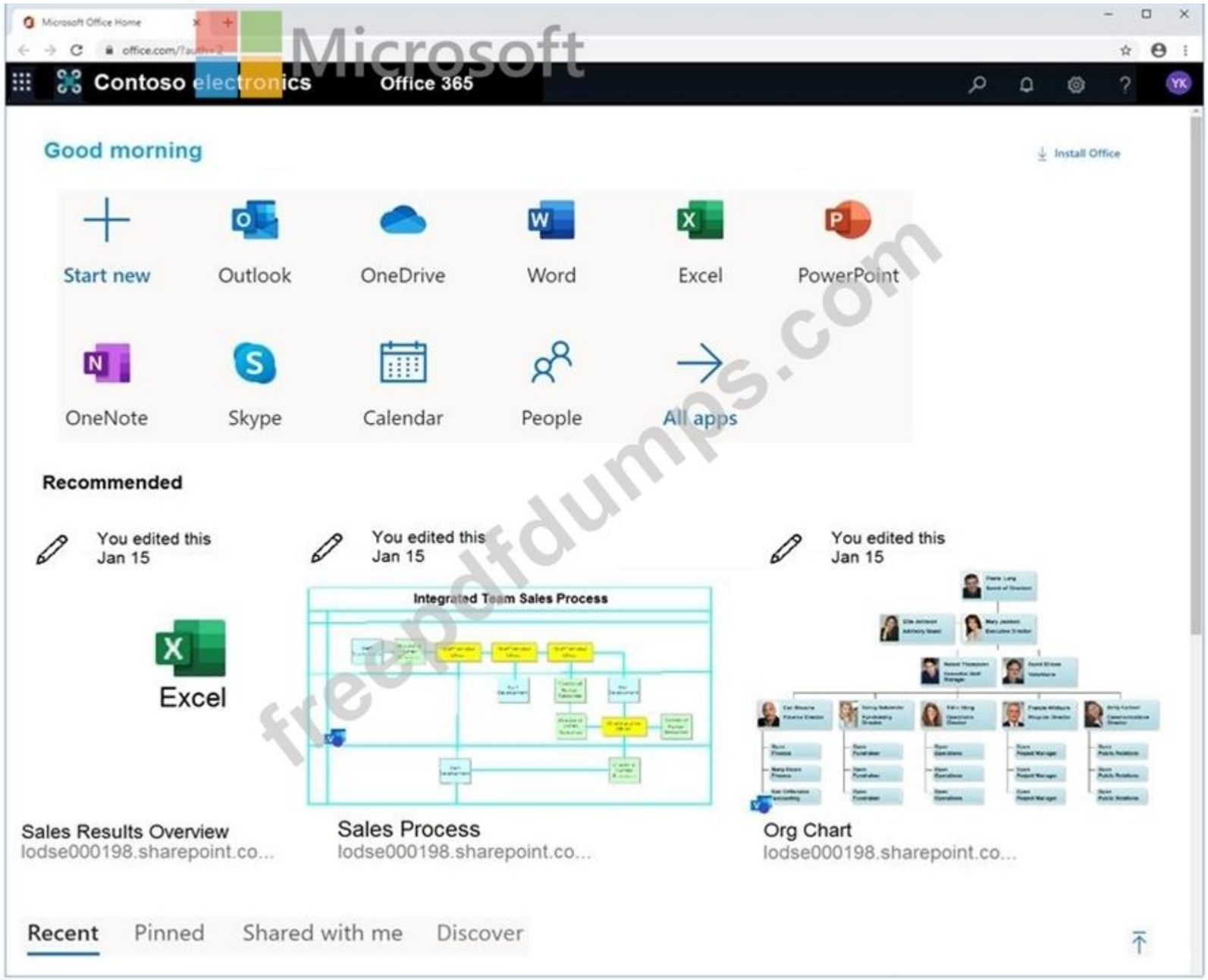
Microsoft

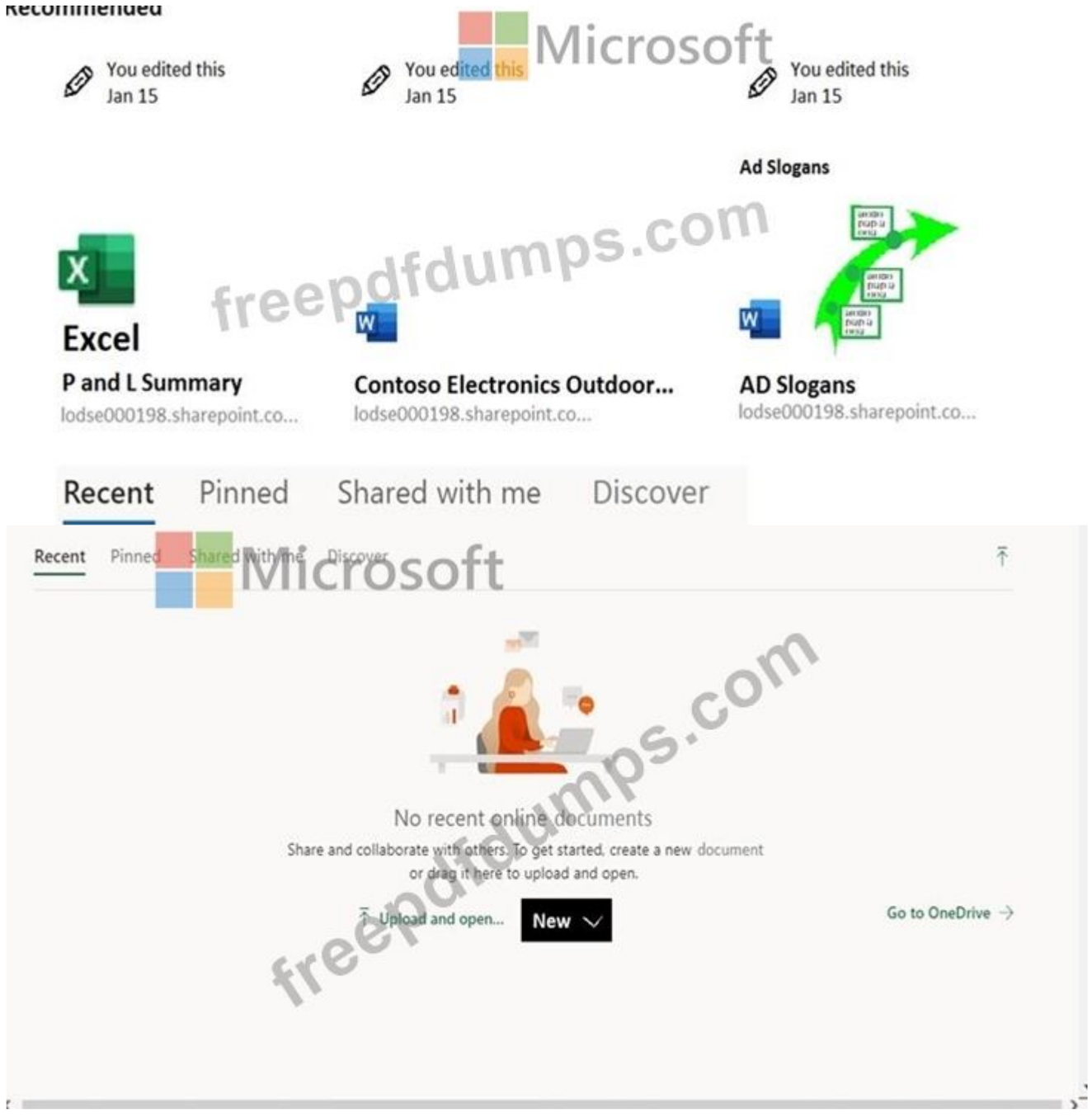
Microsoft

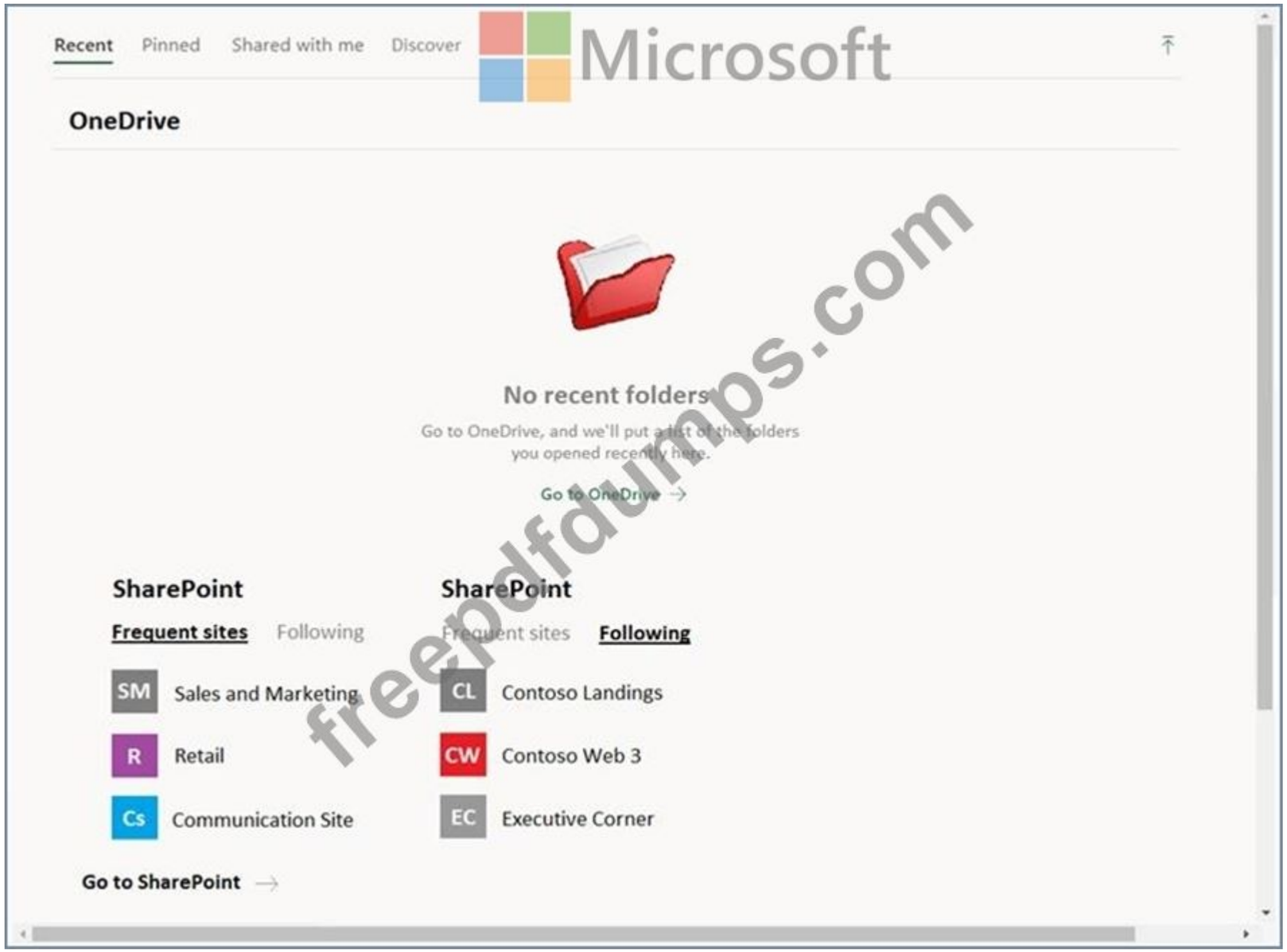
Microsoft

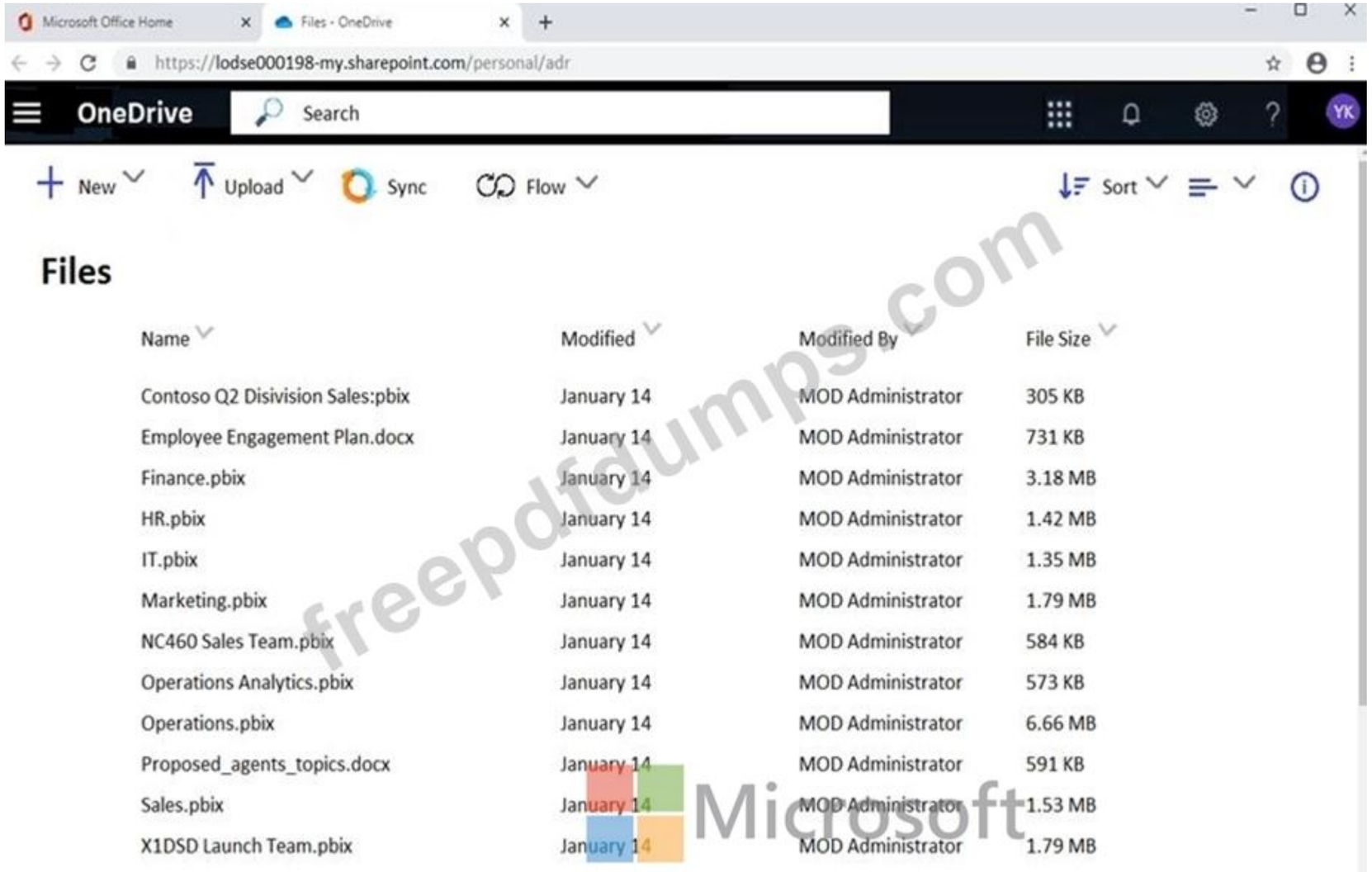
Access Office 365 apps and documents in one place with

Office.com









You need to ensure that a user named Allan Deyoung can perform searches and place holds on mailboxes, SharePoint Online sites, and OneDrive for Business locations. The solution must use the principle of least privilege.

To complete this task, sign in to the Microsoft 365 admin center.

Answer:

After signing in to the Microsoft 365 admin center, navigate to the Security & Compliance Center.

In the left pane of the security and compliance center, select Permissions, and then select the checkbox next to eDiscovery Manager.

On the eDiscovery Manager flyout page, do one of the following based on the eDiscovery permissions that you want to assign.

To make a user an eDiscovery Manager: Next to eDiscovery Manager, select Edit. In the Choose eDiscovery Manager section, select the Choose eDiscovery Manager hyperlink, and then select + Add. Select the user (or users) you want to add as an eDiscovery manager, and then select Add. When you're finished adding users, select Done. Then, on the Editing Choose eDiscovery Manager flyout page, select Save to save the changes to the eDiscovery Manager membership.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/assign-ediscovery-permissions?view=o365-worldwide

NEW QUESTION: 101

Your network contains an on-premises Active Directory domain. The domain contains servers that run Windows Server and have advanced auditing enabled.

The security logs of the servers are collected by using a third-party SIEM solution.

You purchase a Microsoft 365 subscription and plan to deploy Azure Advanced Threat Protection (ATP) by using standalone sensors.
You need to ensure that you can detect when sensitive groups are modified and when malicious services are created.
What should you do?
A. Configure auditing in the Office 365 Security & Compliance center.
B. Turn off Delayed updates for the Azure ATP sensors.
C. Modify the Domain synchronizer candidate's settings on the Azure ATP sensors.
D. Integrate SIEM and Azure ATP.
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

NEW QUESTION: 102
You have a Microsoft 365 E5 subscription that contains 100 users. Each user has a computer that runs Windows 10 and either an Android mobile device or an iOS mobile device. All the devices are registered with Azure AD.
You enable passwordless authentication for all the users.
You need to ensure that the users can sign in to the subscription by using passwordless authentication.
What should you instruct the users to do on their mobile device first?
A. Install the Microsoft Authenticator app.
B. Install a user certificate.
C. Register for self-service password reset (SSPR).
D. Install a device certificate.
Answer: A (LEAVE A REPLY)

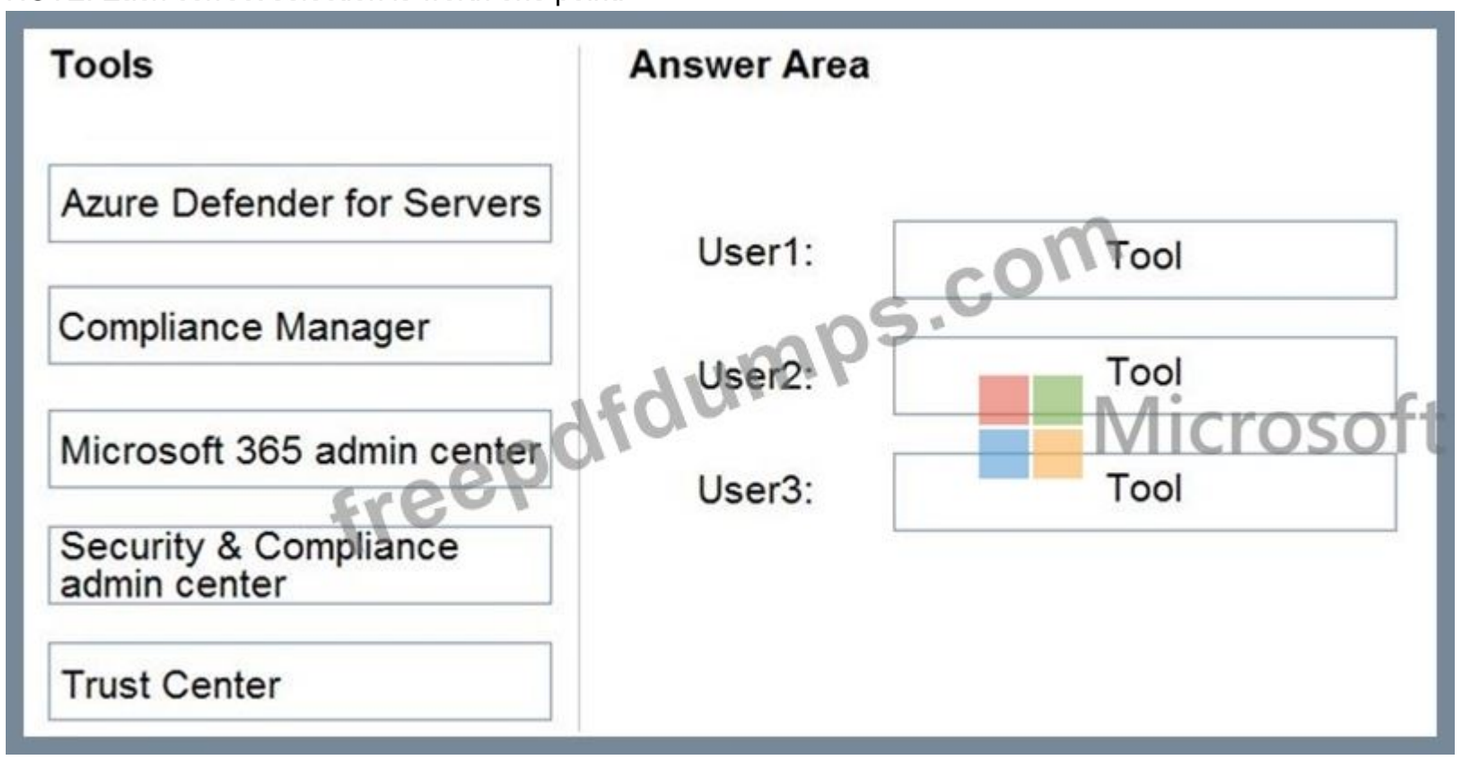
NEW QUESTION: 103
----------53
You have a Microsoft 365 E5 subscription that contains a user named User1.
The Azure Active Directory (Azure AD) Identity Protection risky users report identities User1.
For User1, you select Confirm user compromised.
User1 can still sign in.
You need to prevent User1 from signing in. The solution must minimize the impact on users at a lower risk level.
Solution: You configure the user risk policy to block access when the user risk level is high.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-investigate-risk

NEW QUESTION: 104
You have a Microsoft 365 E5 tenant that contains three users named User1, User2, and User3.
You need to assign roles or role groups to the users as shown in the following table.

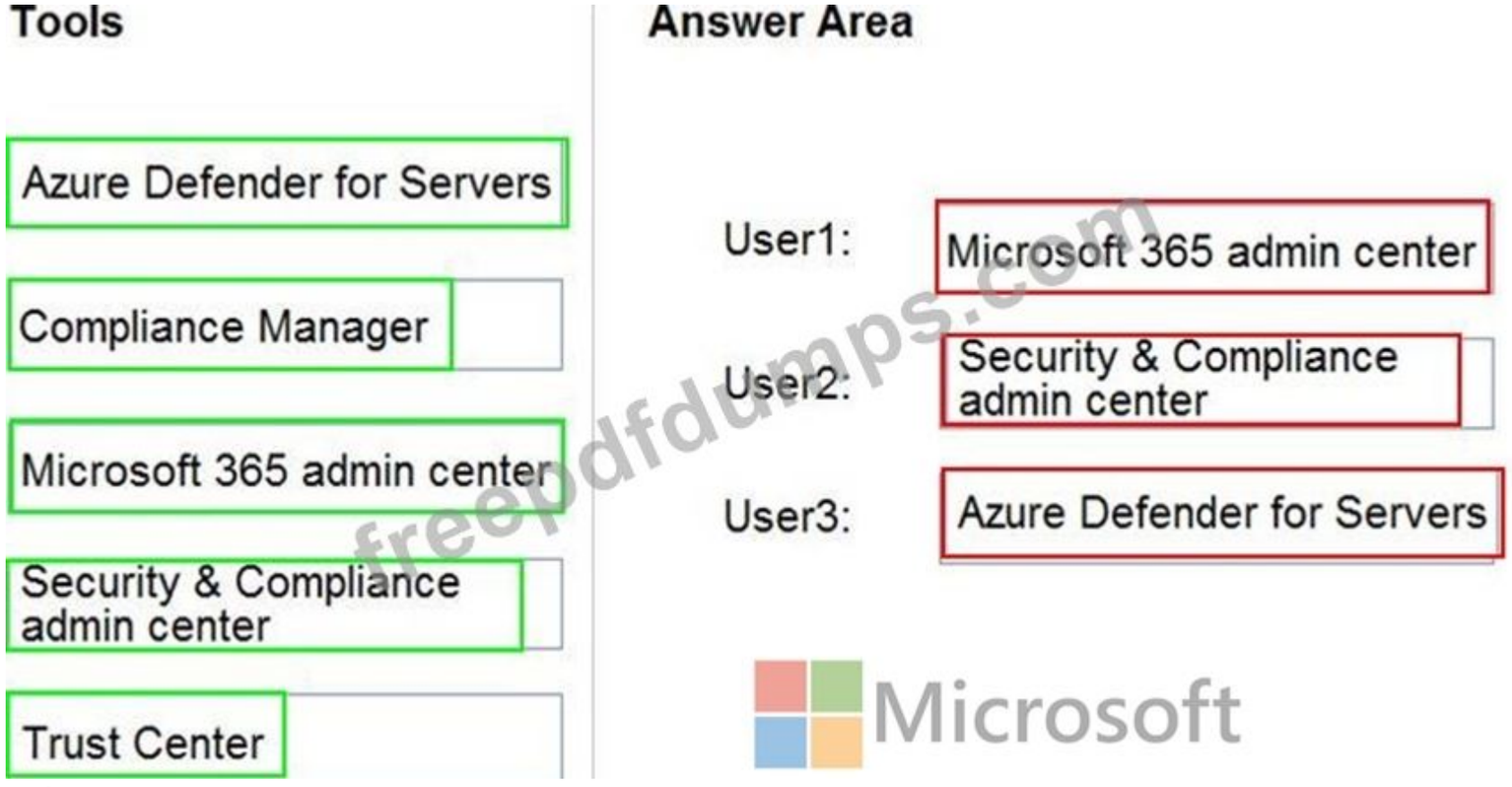
User	Role or role group
User1	SharePoint admin
User2	Data Investigator
User3	User admin

What should you use to assign a role or role group to each user? To answer, drag the appropriate tools to the correct roles or role groups. Each tool 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.



Answer:



Reference:

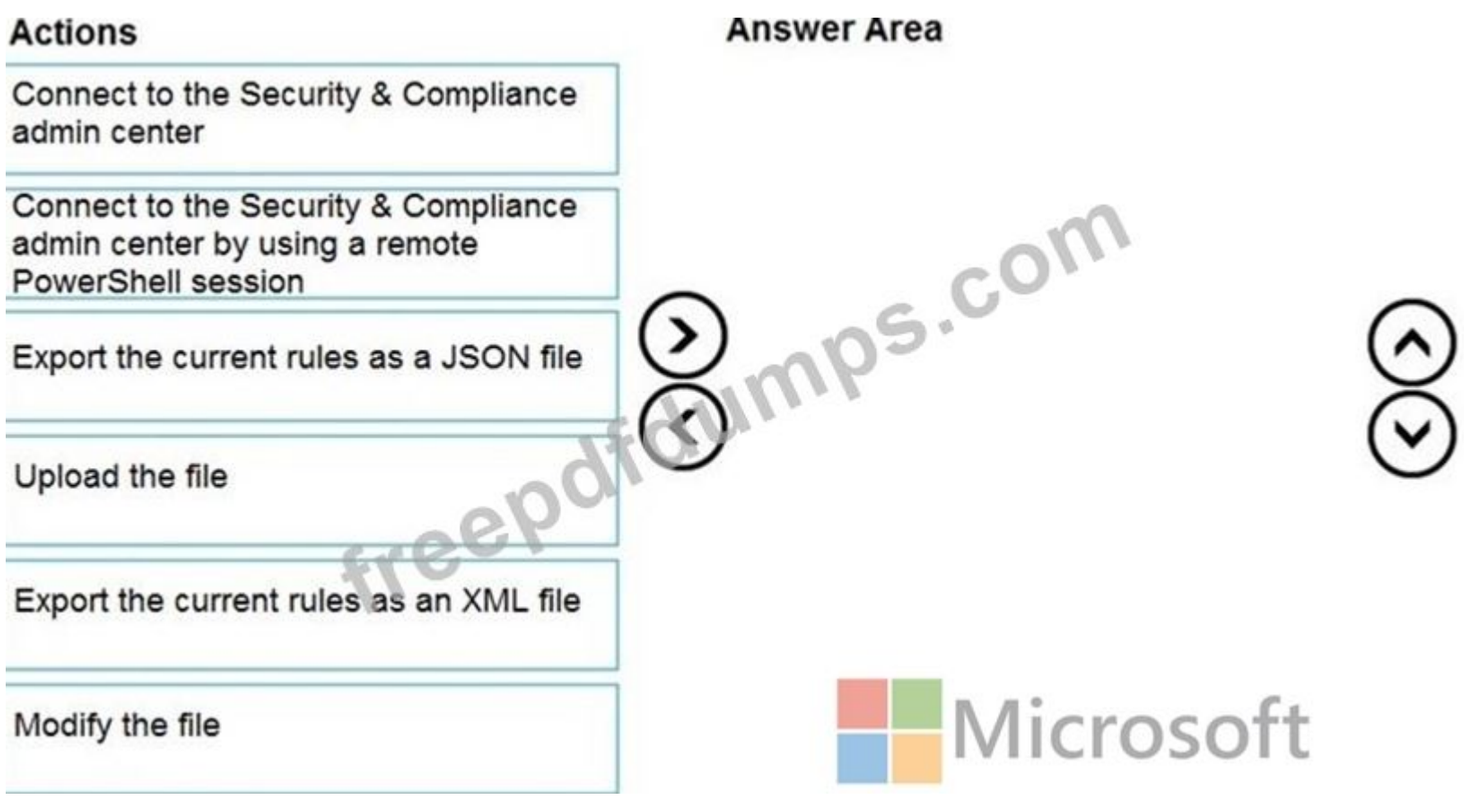
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/permissions-in-the-security-and-compliance-center?view=o365-worldwide

NEW QUESTION: 105

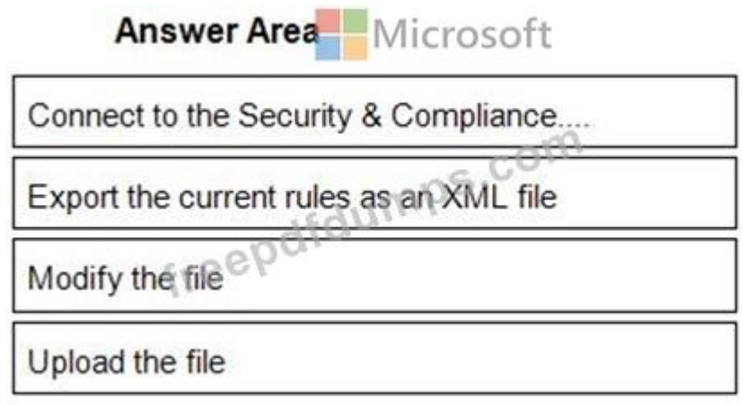
You have a Microsoft 365 subscription.

You need to include a custom sensitive information type in Data Subject Request (DSR) cases.

Which four 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.



Answer:



1 - Connect to the Security & Compliance....
2 - Export the current rules as an XML file
3 - Modify the file
4 - Upload the file
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/customize-a-built-in-sensitive-information-type?view=o365-worldwide

NEW QUESTION: 106
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 questions 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 an on-premises Active Directory domain named contoso.com.

You install and run Azure AD Connect on a server named Server1 that runs Windows Server.
You need to view Azure AD Connect events.
You use the Security event log on Server1.
Does that meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
Reference:
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

NEW QUESTION: 107
You have a Microsoft 365 E5 subscription that contains a security group named Group1 and the users shown in the following table.
You assign the Compliance Manager roles to the users as shown in the following table.
You add two assessments to Compliance Manager as shown in the following exhibit.

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 edit the title of Assessment1.	○	○
To Group1, User2 can add an assessment that uses the HIPA/HITECH (Intune) template.	○	○
To Group1, User3 can add an assessment that uses the HIPA/HITECH (Office 365) template.	○	○

Answer:

Statements	Yes	No
User1 can edit the title of Assessment1.	○	○
To Group1, User2 can add an assessment that uses the HIPA/HITECH (Intune) template.	○	○
To Group1, User3 can add an assessment that uses the HIPA/HITECH (Office 365) template.	○	○

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

NEW QUESTION: 108
You have a Microsoft 365 subscription named contofco.com
You need to configure Microsoft OneDrive for Business external sharing to meet the following requirements:
* Enable flic sharing for users that rave a Microsoft account
* Block file sharing for anonymous users.
What should you do?
A. From Advanced settings tor external sharing, select Allow or Nock sharing with people on specific domains and add contoso.com.
B. From the External sharing settings for OneDrive. select Existing external users.
C. From the External sharing settings for OneDrive, select New and existing external users.
D. From the External sharing settings for OneDrive. select Only people in your organization.
Answer: C (LEAVE A REPLY)
Reference:
https://www.sharepointdiary.com/2020/09/enable-external-sharing-in-onedrive-for-business.html

NEW QUESTION: 109
Which policies apply to which devices? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

Answer:

DevicePolicy1:

None
Device1 only
Device3 only
Device2 and Device3 only
Device1 and Device3 only
Device1, Device2, and Device3

DevicePolicy2:

None
Device4 only
Device2 and Device4 only
Device2, Device3, and Device 4 only

NEW QUESTION: 110

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You create and enforce an Azure Active Directory (Azure AD) Identity Protection sign-in risk policy that has the following settings:

Assignments: Include Group1, Exclude Group2

Conditions: User risk level of Medium and above

Access: Allow access, Require password change

The users attempt to sign in. The risk level for each user is shown in the following table.

User	User risk level
User1	High
User2	Medium
User3	High

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 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

Answer:

Statements	Yes	No
User1 must change his password.	○	○
User2 must change his password.	○	○
User3 must change his password.	○	○

NEW QUESTION: 111
You have a Microsoft 365 subscription.
You need to recommend a passwordless authentication solution that uses biometric authentication.
What should you include in the recommendation?
A. Windows Hello for Business
B. a smart card
C. the Microsoft Authenticator app
D. a PIN
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

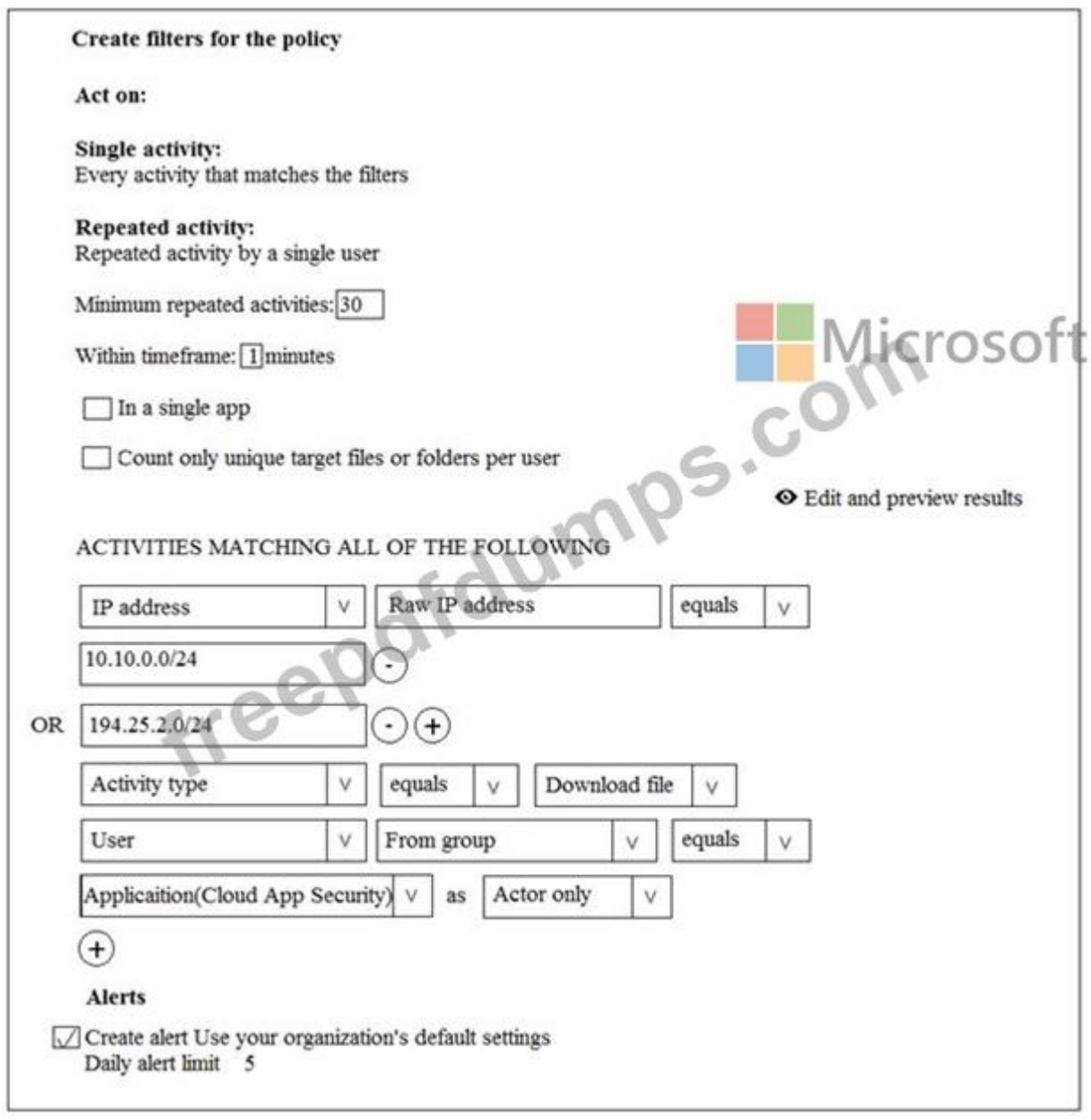
NEW QUESTION: 112
Your company has a Microsoft 365 subscription, a Microsoft Azure subscription, and an Azure Active Directory (Azure AD) tenant named contoso.com.
The in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

The tenant contains the users shown in the following table.

Name	Email address
User1	User1@contoso.com
User2	User2@contoso.com

You create the Microsoft Cloud App Security policy shown in the following exhibit.



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
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

Answer:

Statements	Yes	No
In the Monreal office, if User1 downloads 40 files in 30 seconds, an alert will be created.	○	○
In the Seattle, if User2 downloads one file per second for two minutes, an alert will be created.	○	○
In the New York office, if User1 downloads 40 files in 10 seconds, an alert will be created.	○	○

NEW QUESTION: 113

You have a Microsoft 365 E5 subscription.

You plan to implement Microsoft Sentinel to create incidents based on:

* Azure Active Directory (Azure AD) Identity Protection alerts
* Correlated events from the DeviceProcessEvents table

Which analytic rule types should you use for each incident type? To answer, drag the appropriate rule types to the correct incident types. Each rule type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Answer:

NEW QUESTION: 114

Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

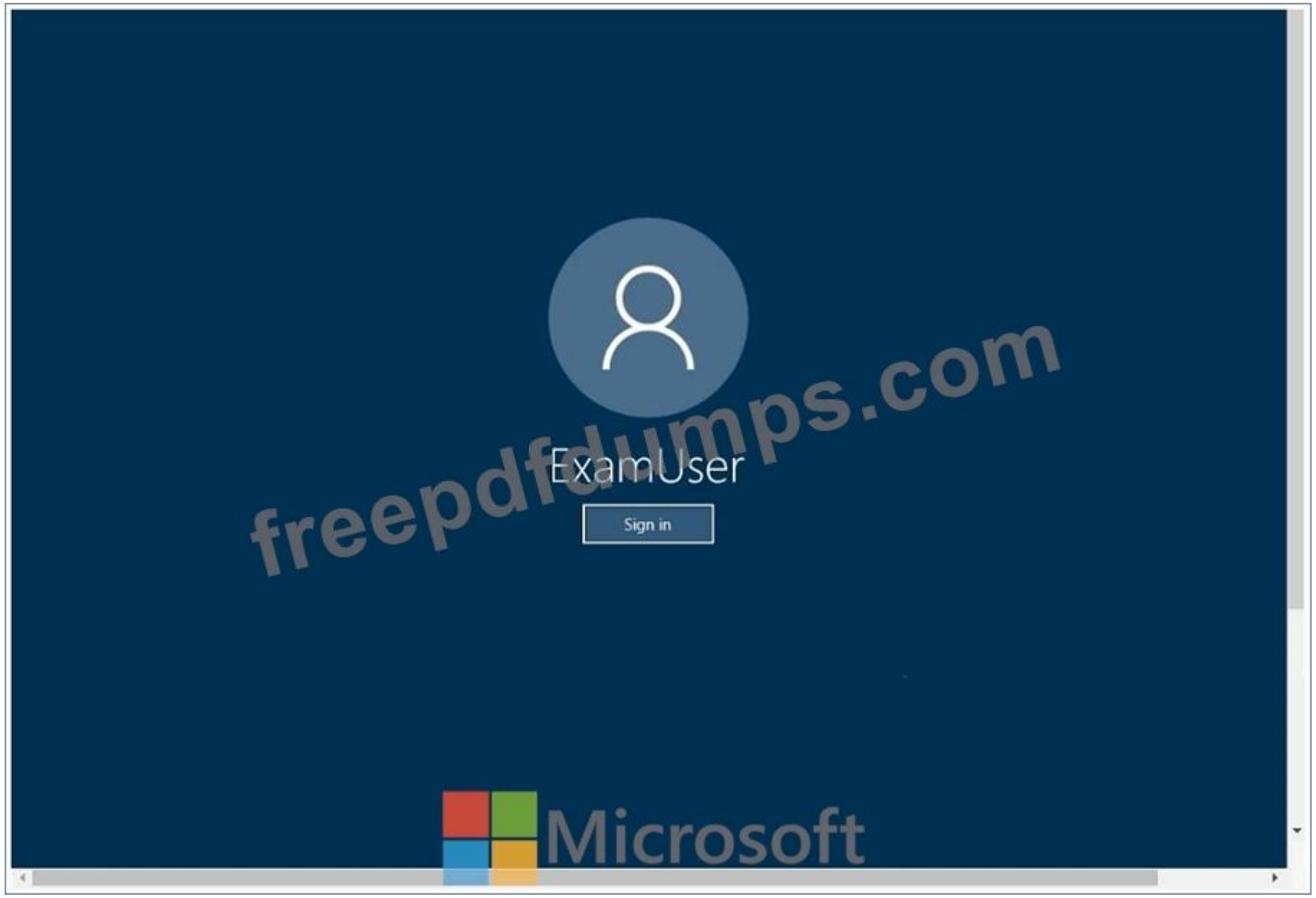
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.

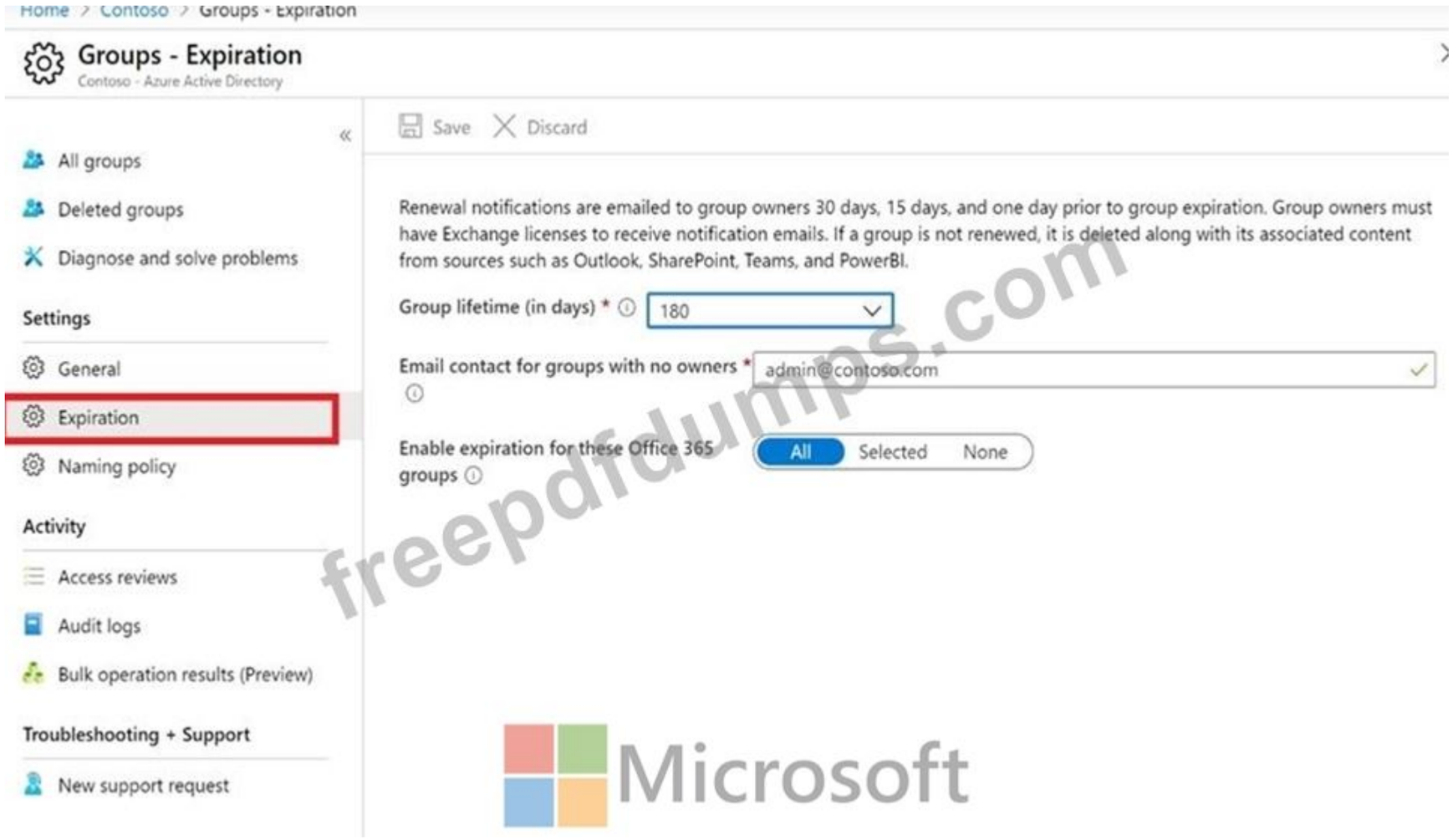
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com
Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to ensure that group owners renew their Office 365 groups every 180 days.
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

Set group expiration
1. Open the Azure AD admin center with an account that is a global administrator in your Azure AD organization.
2. Select Groups, then select Expiration to open the expiration settings.



3. On the Expiration page, you can:
Set the group lifetime in days. You could select one of the preset values, or a custom value (should be 31 days or more).
Specify an email address where the renewal and expiration notifications should be sent when a group has no owner.
Select which Office 365 groups expire. You can set expiration for:
All Office 365 groups
A list of Selected Office 365 groups
None to restrict expiration for all groups
Save your settings when you're done by selecting Save.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-lifecycle

NEW QUESTION: 115
Note: This question is part of 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 tenant. You create a label named CompanyConfidential in Microsoft Azure Information Protection.
You add CompanyConfidential to a global policy.

A user protects an email message by using CompanyConfidential and sends the label to several external recipients. The external recipients report that they cannot open the email message.
You need to ensure that the external recipients can open protected email messages sent to them.
Solution: You modify the encryption settings of the label.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
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 that contains the users shown in the following table.

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

You discover that all the users in the subscription can access Compliance Manager reports.
The Compliance Manager Reader role is not assigned to any users.
You need to recommend a solution to prevent a user named User5 from accessing the Compliance Manager reports.
Solution: You recommend assigning the Compliance Manager Reader role to User5.
Does this meet the goal?
A. No
B. Yes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 117
Which IP address space should you include in the MFA configuration?
A. 192.168.16.0/20
B. 172.16.0.0/24
C. 192.168.0.0/20
D. 131.107.83.0/28
Answer: (SHOW ANSWER)

NEW QUESTION: 118
Several users in your Microsoft 365 subscription report that they received an email message without the attachment. You need to review the attachments that were removed from the messages. Which two tools can you use? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.
A. the Exchange admin center
B. the Azure ATP admin center

C. Microsoft Azure Security Center
D. the Security & Compliance admin center
E. Outlook on the web
Answer: A,D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-quarantined-messages-and-files

NEW QUESTION: 119
You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.

Name	Role	Member of
Admin1	Global Administrator	*None*
User1	Global reader	Group1
User2	Global reader	Group2

You have the Privileged Access settings configured as shown in the following exhibit.

You have a privileged access policy that has the following settings:
* Policy name: New Transport Rule
* Policy type: Task
* Policy scope Exchange
* Approval Type: Manual
* Approver group: Group 1
User1 requests access to the New Transport Rule policy for a duration of two hours.
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:

:

NEW QUESTION: 120

You have an Azure Active Directory (Azure AD) tenant that has a Microsoft 365 subscription You recently configured the tenant to require multi factor authentication (MFA) for risky sign ins You need to review the users who required MFA.

What should you do?

A. From the Azure Active Directory admin center, review the Authentication methods activities.

B. From the Azure Active Directory admin center, download the sign-ms to a CSV file

C. From the Microsoft 365 admin center, review a Security & Compliance report.

D. From the Microsoft 365 Compliance admin center, run an audit log search and download the results to a CSV file

Answer: A (LEAVE A REPLY)

NEW QUESTION: 121

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

Name	Configuration
DC1	Domain controller
Server1	Member server

You plan to implement Azure Advanced Threat Protection (ATP) for the domain.

You install an Azure ATP standalone sensor on Server1.

You need to monitor the domain by using Azure ATP.

What should you do?

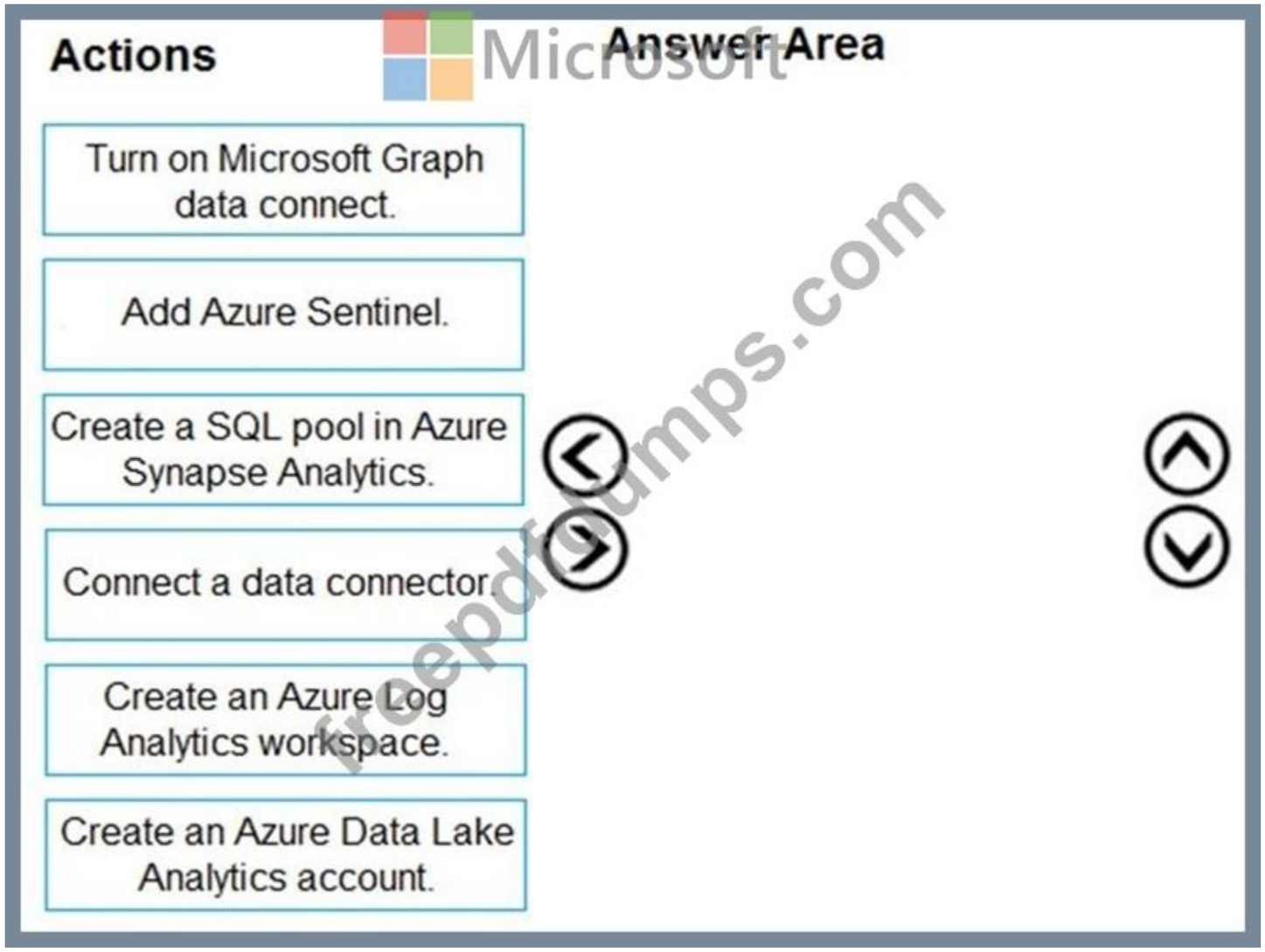
A. Configure port mirroring for DC1.

B. Configure port mirroring for Server 1.

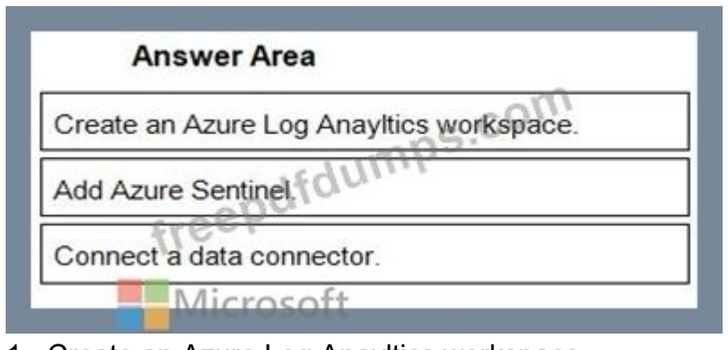
C. Install the Microsoft Monitoring Agent on Server!.

D. Install the Microsoft Monitoring Agent on DC1.
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-port-mirroring

NEW QUESTION: 122
You have an Azure subscription and a Microsoft 365 subscription.
You need to perform the following actions:
Deploy Azure Sentinel.
Collect the Microsoft 365 activity log by using Azure Sentinel.
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.



Answer:



1 - Create an Azure Log Anayltics workspace.

2 - Add Azure Sentinel.

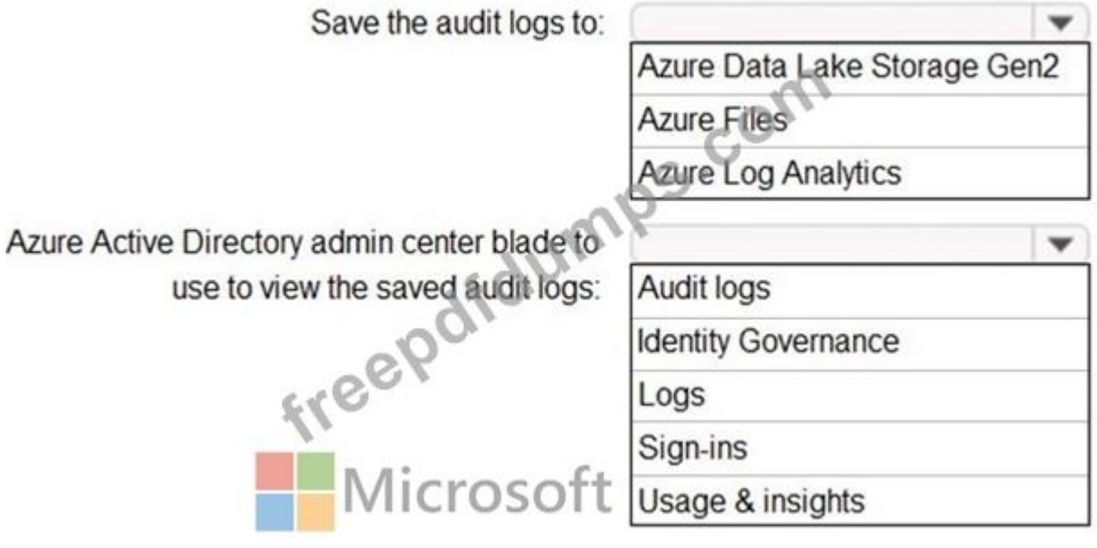
3 - Connect a data connector.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard

https://docs.microsoft.com/en-us/azure/sentinel/connect-office-365

NEW QUESTION: 123
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.



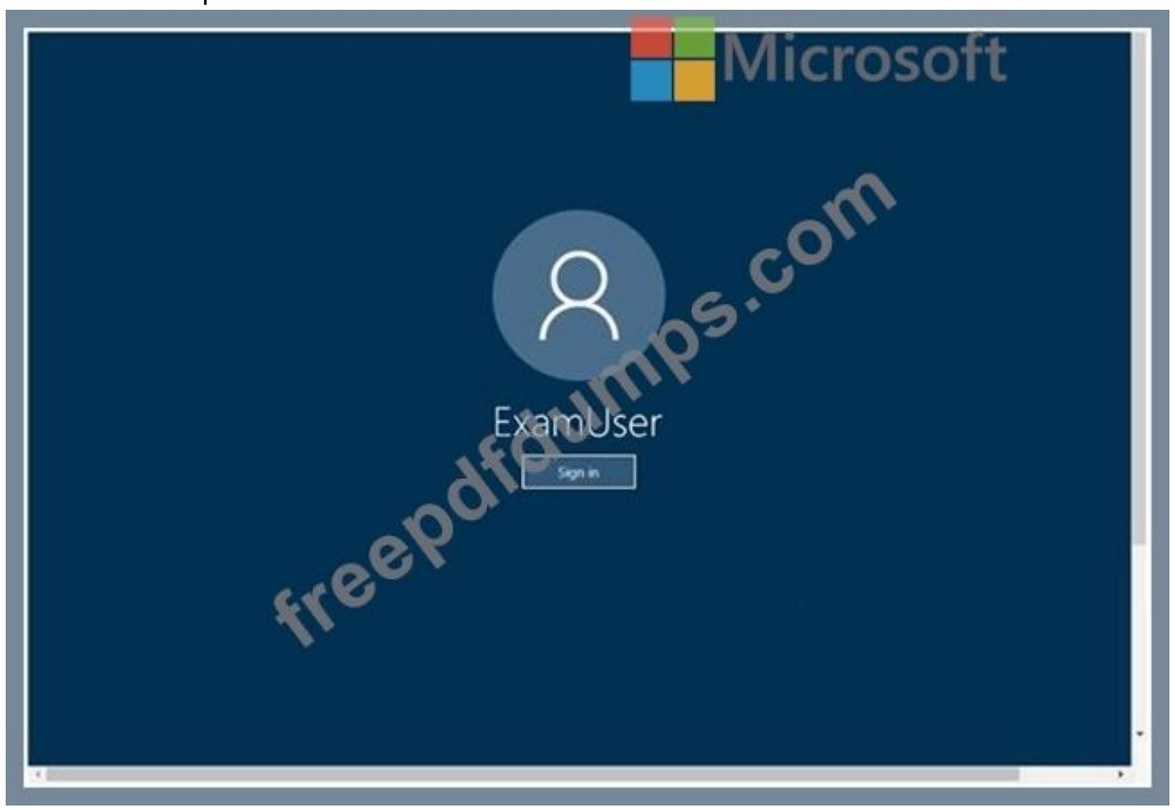
Answer:

Reference:
https://docs.microsoft.com/en-gb/azure/active-directory/reports-monitoring/howto-analyze-activity-logs-log-analytics

NEW QUESTION: 124
You recently created and published several labels policies in a Microsoft 365 subscription.
You need to view which labels were applied by users manually and which labels were applied automatically.
What should you do from the Security & Compliance admin center?
A. From Search & investigation, select Content search

B. From Data governance, select Events
C. From Search & investigation, select eDiscovery
D. From Reports, select Dashboard
Answer: D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/microsoft-365/compliance/view-label-activity-for-documents

NEW QUESTION: 125
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.
When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.
Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.
Labs are not timed separately, and this exam may more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.
Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.
Username and password



Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and click on the username below.
To enter your password, place your cursor in the Enter password box and click on the password below.
Microsoft 365 Username:
admin@LODSe244001@onmicrosoft.com

Microsoft 365 Password: &=Q8v@2qGzYz
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.
The following information is for technical support only:
Lab instance: 11032396
You need to ensure that a user named Lee Gu can manage all the settings for Exchange Online. The solution must use the principle of least privilege.
To complete this task, sign in to the Microsoft Office 365 admin center.

Answer:

In the Exchange Administration Center (EAC), navigate to Permissions > Admin Roles.
Select the group: Organization Management and then click on Edit.
In the Members section, click on Add.
Select the users, USGs, or other role groups you want to add to the role group, click on Add, and then click on OK.
Click on Save to save the changes to the role group.
Reference:
https://help.bittitan.com/hc/en-us/articles/115008104507-How-do-I-assign-the-elevated-admin-role-Organization-Management-to-the-account-that-is-performing-a-Public-Folder-migration-
https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo

NEW QUESTION: 126
You need to recommend an email malware solution that meets the security requirements.
What should you include in the recommendation? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

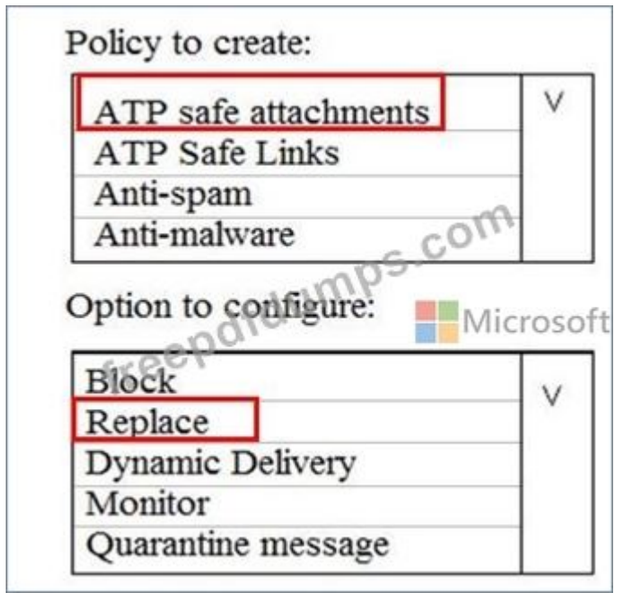
Policy to create:

ATP safe attachments
ATP Safe Links
Anti-spam
Anti-malware

Option to configure:

Block
Replace
Dynamic Delivery
Monitor
Quarantine message

Answer:



NEW QUESTION: 127
You have a Microsoft 365 subscription.
From the Microsoft 365 admin center, you create a new user.
You plan to assign the Reports reader role to the user.
You need to see the permissions of the Reports reader role.
Which admin center should you use?
A. Microsoft 365
B. Security & Compliance
C. Cloud App Security
D. Azure Active Directory
Answer: D (LEAVE A REPLY)