

Microsoft.MS-102-KR.v2026-06-01.q252

□□□□:	MS-102-KR
□□□□:	Microsoft 365 Administrator (MS-102 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	252
□□:	v2026-06-01
# □□ □:	177
# □□ □□□:	2520
https://www.krdump.com/Microsoft.MS-102-KR.v2026-06-01.q252.html	

NEW QUESTION: 1

□□□ □□□□ □□□ Microsoft SharePoint Online □□□□□ □□□□ □□□ □□□ □ □□□ □□□□□ □□□ □□□. □□□ □□ □□□?

- A. Microsoft Purview □□ □□ □□□□ DLP(□□□□ □□ □□) □□□ □□□□.
- B. SharePoint Online □□□□□ □□□ □□□□.
- C. Microsoft 365 Defender □□□□ □□ □□□ □□□□.
- D. SharePoint Online □□ □□□□ □□ □□□ □□□□□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 2

□□ □□ □□□ □□□□ □□□□ Azure AD □□□□ □□□□.

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Exchange Administrator

□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□. □□ □□□ □□□□ □□□?

- A. Microsoft 365 □□ □□
- B. Microsoft Purview □□ □□ □□
- C. Microsoft 365 Defender □□1
- D. Microsoft Entra □□ □□

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 3

Microsoft 365 E5 □□□ □□□□.

Endpoint□ Microsoft Defender □□□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

- A. Microsoft Intune □□ □□
- B. Microsoft Purview □□
- C. Microsoft 365 □□ □□
- D. Microsoft Defender □□

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 4

Microsoft Defender for Endpoint□ □□□□ Microsoft 365 E5 □□□ □□□□.

□□□□ □□□ □□ □□ □□ □□ □□□□□□.

Device1□□□□ □□□ □□□□ □□□□ □□□□ □□□□□□.

□ □□□□ □□□ □□ □□□□?

- A. Microsoft □□ □□□ - □□□ □□ □□□ □□□□□.
- B. Defender for Endpoint□ Microsoft Intune□ □□□□□.
- C. □□ □□□ □□□□□.
- D. □□□ □□□□ □□□□□□ □□□□□□.

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 5

contoso.com□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Microsoft Entra □□ □□□ □□□ □□□□□□□ User1□ User2□ □□□□ □ □□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.



Answer:

Answer Area  Microsoft

User1 can view the sign-ins for the following users:

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

User2 can view the sign-ins for the following users:

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

Explanation:

Answer Area

User1 can view the sign-ins for the following users: User1, User2, User3, and User4

User2 can view the sign-ins for the following users: User1 and User2 only

 Microsoft

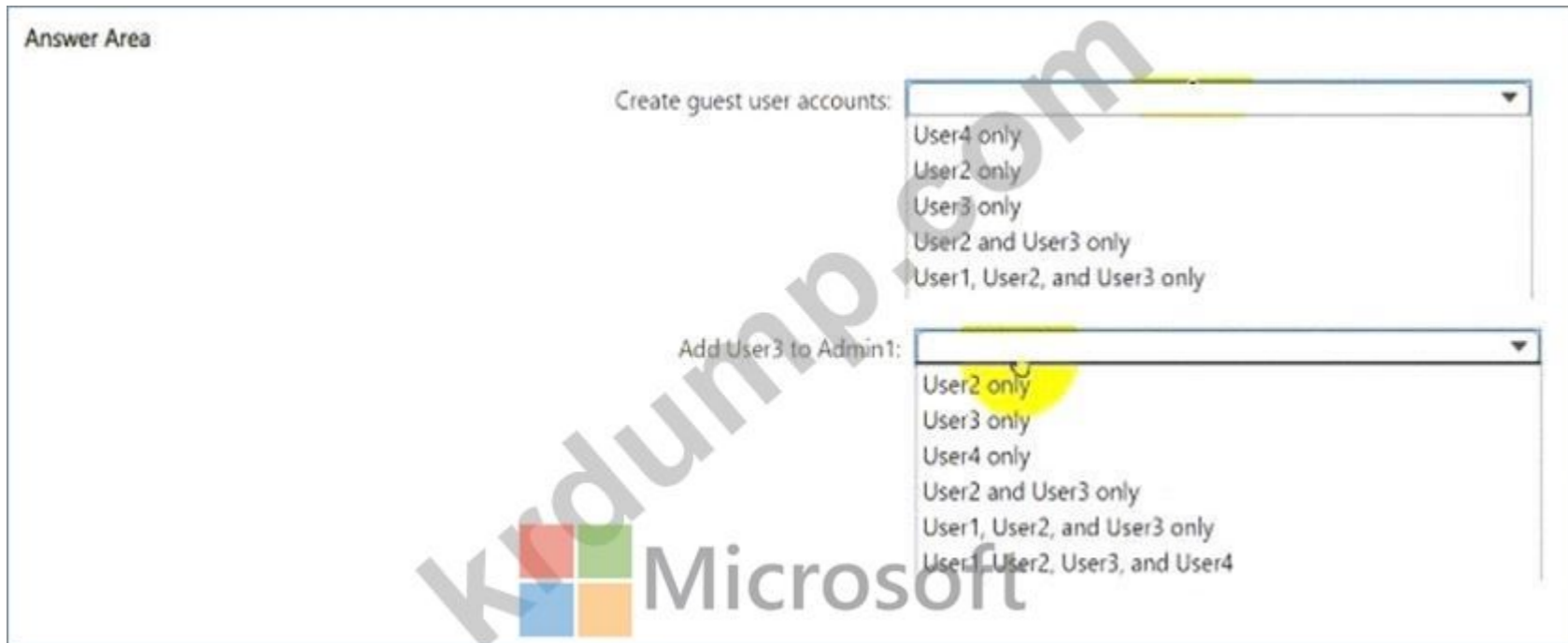
NEW QUESTION: 6

Microsoft Entra Privileged Role Administrator

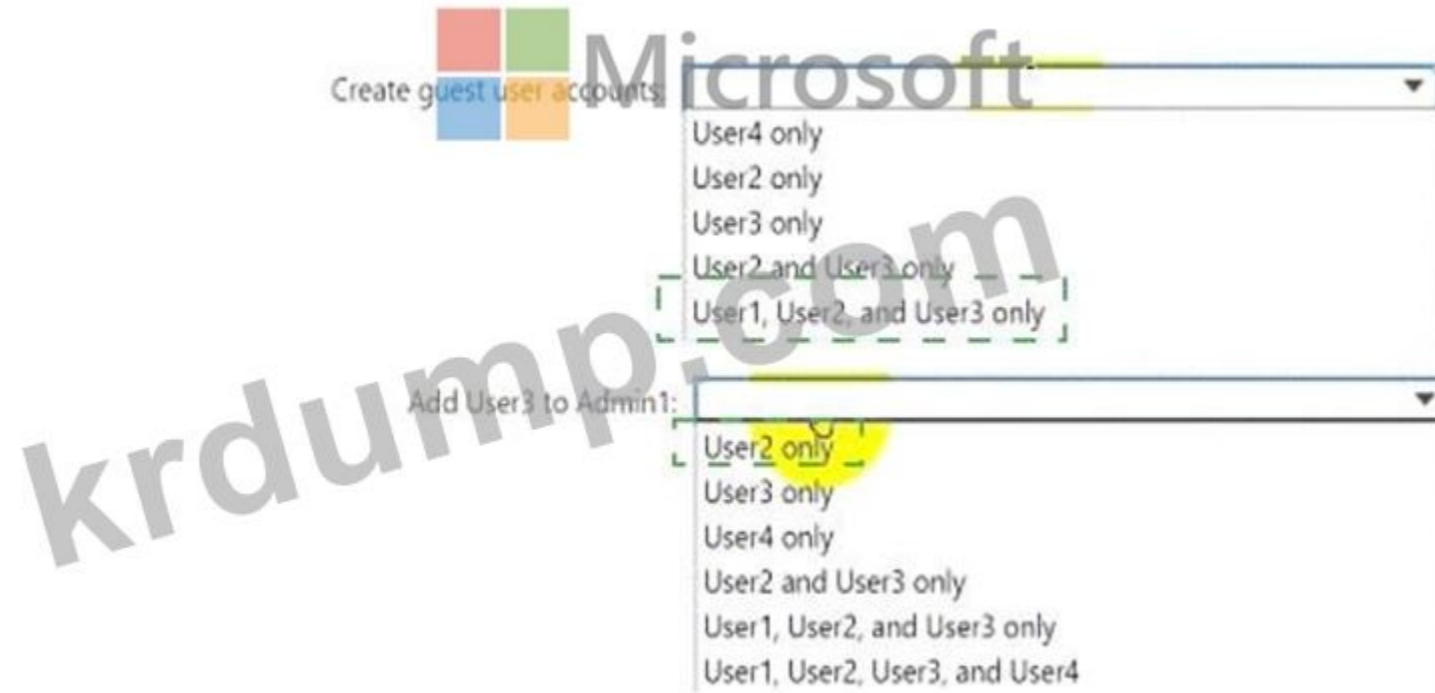
Name	Role
User1	Privileged Role Administrator
User2	User Administrator
User3	Security Administrator
User4	Billing Administrator

Admin1 is a Microsoft Entra Privileged Role Administrator. Admin1 is assigned the Privileged Role Administrator role.

Admin1 is assigned the Privileged Role Administrator role.



Answer:
Answer Area



Explanation:

Create guest user accounts: User1, User2, and User3 only

User1: Privileged Role Administrator role has the ability to manage role assignments in Azure AD, including creating guest accounts.

User2: User Administrator role can manage user accounts, including creating guest accounts.

User3: Security Administrator role does not typically include permissions for creating guest accounts, but in some configurations, they might have limited guest user management capabilities.

Add User3 to Admin1: User2 only

User2: User Administrator role has the permissions to add users to security groups like Admin1.

NEW QUESTION: 7

Answer Area Microsoft

Statements	Yes	No
User1 can reset the password of User3.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User2 can update the display name of User1.	<input type="checkbox"/>	<input type="checkbox"/>
User1 can reset the password of User2.	<input type="checkbox"/>	<input type="checkbox"/>

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User2 can update the display name of User1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User1 can reset the password of User2.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Box 1: No

User1 is assigned the Password Administrator for AU1 and AU2.

User3 is in AU2. User3 is User Administrator.

Password administrators cannot reset User Administrators passwords.

Note: Password Administrator

Users with this role have limited ability to manage passwords. This role does not grant the ability to manage service requests or monitor service health. Whether a Password Administrator can reset a user 's password depends on the role the user is assigned.

Role that password can be reset	Password Admin	Helpdesk Admin	Auth Admin	User Admin	Privileged Auth Admin	Global Admin
User Admin	<input type="checkbox"/>			✓	✓	✓
Usage Summary Reports Reader		✓	✓	✓	✓	✓

Box 2: Yes

Box 3: No

User1 is assigned the Password Administrator for AU1 and AU2.

User2 is in AU1. User2 is User Administrator.

Password administrators cannot reset User Administrators passwords.

Note: User Administrator

Can manage all aspects of users and groups, including resetting passwords for limited admins.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords>

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference>

NEW QUESTION: 9

Office 365 Microsoft Defender Microsoft 365 E5

To identify the number of emails quarantined by ZAP:

Mailflow status report

Spooof detections

Threat protection status

URL threat protection

Answer Area



Microsoft

To identify the number of emails quarantined by ZAP:

- Threat protection status
- Mailflow status report
- Spooof detections
- Threat protection status**
- URL threat protection

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

- Mailflow status report
- Mailflow status report**
- Spooof detections
- Threat protection status
- URL threat protection

Answer:

Answer Area



To identify the number of emails quarantined by ZAP:

Threat protection status ▼
 Mailflow status report
 Spoof detections
Threat protection status
 URL threat protection

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

Mailflow status report ▼
Mailflow status report
 Spoof detections
 Threat protection status
 URL threat protection

Explanation:

Answer Area



To identify the number of emails quarantined by ZAP:

Threat protection status ▼

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

Mailflow status report ▼

NEW QUESTION: 10

□□□

□□□ Microsoft Defender for Endpoint □ □□□□. Microsoft Defender for Endpoint □□ □□ □□ □□ □□ □□□□□.

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

□□ □□□ □□ Microsoft Defender for Endpoint □ computer1 □□□ □□□□ □□□□□□.



Device summary

Risk level ⓘ

None

Device details

Domain

adatum.com

OS

Windows 10 64-bit

Version 21H2

Build 19044.2130

□□□□ □□□ □□□ □ □□□ □□□□ □□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices


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



- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

Answer:

Answer Area



Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

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

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

Explanation:

Answer Area



Computer1 will be a member of [answer choice].

▼

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped devices

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

▼

- Group1 only
- Group1 and Group2 only
- Group1, Group2, Group3, and Group4
- Ungrouped devices

Box 1: Group3 and Group4 only

Computer1 has no Demo Tag.

Computer1 is in the adatum domain and OS is Windows 10.

Box 2: Group1, Group2, Group3 and Group4

NEW QUESTION: 11

Site1 is a Microsoft SharePoint site. Site1 contains a Microsoft 365 E5 license. Site1 has a DLP policy named DLP1. DLP1 has three rules. The rules are defined as follows:

Name	Number of IP addresses in the file
File1	2
File2	3

Site1 has a DLP policy named DLP1. DLP1 has three rules. The rules are defined as follows:

Name	Content contains	Policy tip	If there is a match, stop processing	Priority
Rule1	3 or more IP addresses	Tip1	No	0
Rule2	1 or more IP addresses	Tip2	Yes	1
Rule3	2 or more IP addresses	Tip3	No	2

Site1 has a DLP policy named DLP1.

Site1 has a DLP policy named DLP1. DLP1 has three rules. The rules are defined as follows:

Site1 has a DLP policy named DLP1.

Answer Area



File1: ▼
Tip2 only
Tip3 only
Tip2 and Tip3

File2: ▼
Tip1 only
Tip3 only
Tip1 and Tip2 only
Tip1, Tip2, and Tip3

Answer:
Answer Area



File1: ▼
Tip2 only
Tip3 only
Tip2 and Tip3

File2: ▼
Tip1 only
Tip3 only
Tip1 and Tip2 only
Tip1, Tip2, and Tip3

Explanation:

Answer Area

File1: ▼

File2: ▼

NEW QUESTION: 12

contoso.com Azure AD Microsoft 365

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

User5 is a member of the User Administrators group. User5 is also a member of the Exchange Administrators group. User5 is also a member of the Global Administrators group. User5 is also a member of the Microsoft Entra Privileged Identity Management (PIM) group. User5 is also a member of the Microsoft Entra Privileged Identity Management (PIM) group.

- A. User2 and User4 can create users.
- B. User4 can create users.
- C. Azure AD can create users.
- D. User1, User2, and User4 can create users.
- E. User2 and User4 can create users.
- F. Azure AD can create users.

Answer: A,E (LEAVE A REPLY)

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

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

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

Reference:

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

NEW QUESTION: 13

Microsoft 365 is used to manage users.

Microsoft Entra Privileged Identity Management (PIM) is used to manage users.

Global Administrator | Role settings

Privileged Identity Management | Microsoft Entra roles

Edit

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Allow permanent active assign	Azure MFA

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentici...	Yes
Require justification on active assignment	No



admin1@contoso.com
 Microsoft Entra administrator must configure [answer choice].

Answer Area

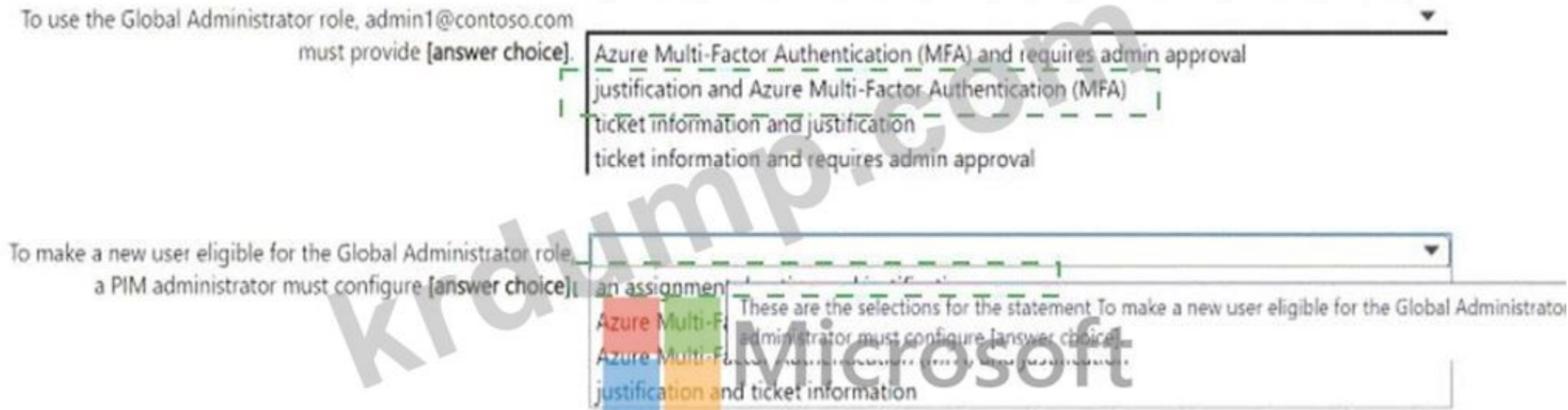
To use the Global Administrator role, admin1@contoso.com must provide [answer choice].

- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and Azure Multi-Factor Authentication (MFA) ticket information and justification
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and ticket information

To make a new user eligible for the Global Administrator role, a PIM administrator must configure [answer choice].

- an assignment justification and ticket information
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and ticket information
- Azure Multi-Factor Authentication (MFA) and requires admin approval justification and justification and ticket information

Answer:
ANSWER AREA



Explanation:

To use the Global Administrator role, admin1@contoso.com must provide: Azure Multi-Factor Authentication (MFA) The role settings indicate that " Require Azure Multi-Factor Authentication " is set to " Yes " for active assignments. Therefore, admin1@contoso.com must provide Azure MFA to use the Global Administrator role.

To make a new user eligible for the Global Administrator role, a PIM administrator must configure: an assignment that expires after 15 day(s) The settings show that eligible assignments expire after 15 days. Therefore, to make a new user eligible, a PIM administrator must configure an assignment with this expiration period.

NEW QUESTION: 14

Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP) is installed on a Windows 10 device. The device is connected to the Internet. Which of the following is a requirement for Microsoft Defender ATP to be able to detect threats?

A. The device must be connected to the Internet.

B. The device must be connected to a Microsoft Defender ATP server.

C. The device must be connected to a Microsoft Defender ATP cloud service.

D. The device must be connected to a Microsoft Defender ATP endpoint.

E. The device must be connected to a Microsoft Defender ATP gateway.

F. The device must be connected to a Microsoft Defender ATP proxy.

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/manage-indicators>

NEW QUESTION: 15

Microsoft 365 E5 includes Microsoft Defender for Office 365. Which of the following is a requirement for Microsoft Defender for Office 365 to be able to detect threats?

A. The device must be connected to the Internet.

B. The device must be connected to a Microsoft Defender for Office 365 server.

C. The device must be connected to a Microsoft Defender for Office 365 cloud service.

D. The device must be connected to a Microsoft Defender for Office 365 endpoint.

E. The device must be connected to a Microsoft Defender for Office 365 gateway.

F. The device must be connected to a Microsoft Defender for Office 365 proxy.

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

Microsoft

Domains to protect
 Domains to protect
 Mailbox intelligence
 Users to protect

Global settings for safe attachments
 Global settings for safe attachments
 The Safe Attachments policy settings
 The Safe Links policy settings

Answer:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection:

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365:

Microsoft

Domains to protect
 Domains to protect
 Mailbox intelligence
 Users to protect

Global settings for safe attachments
 Global settings for safe attachments
 The Safe Attachments policy settings
 The Safe Links policy settings

Explanation:

Answer Area

A user's email sending patterns must be used to minimize false positives for spoof protection: Domains to protect

Documents uploaded to Teams, SharePoint Online, and OneDrive must be protected by using Defender for Office 365: Global settings for safe attachments

NEW QUESTION: 16

Microsoft 365 E5

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

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

□□ □□ □□ □□ □□□□.

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

Microsoft Endpoint Manager □ □□□□ □□□□ □□ □□□ □□□□□.

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.



Yes No

App1 can be assigned as a required install for User3.

App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager.

App3 can be installed automatically for UserGroup1.

Answer:

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

Explanation:

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

Reference:

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

<https://docs.microsoft.com/en-us/mem/intune/apps/apps-windows-10-app-deploy>

MS-102-KR [redacted] DumpTop [redacted] MS-102-KR [redacted]! DumpTop [redacted] **MS-102-KR** [redacted], DumpTop MS-102-KR [redacted]
 [redacted]. [redacted] DumpTop MS-102-KR [redacted]. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 17

Microsoft 365 [redacted].

Microsoft 365 [redacted].

Microsoft 365 [redacted] Microsoft [redacted]?

A. Microsoft [redacted]

B. Azure [redacted]

C. Azure [redacted]

D. Azure [redacted]

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 18

[redacted] Microsoft 365 [redacted].

User1 [redacted] Azure AD [redacted].

Azure AD Connect [redacted].

Microsoft Azure Active Directory Connect

Welcome

Tasks

Review your solution

Synchronized Directories

DIRECTORY	ACCOUNT
Adatum.com	ADATUM.COM\MSOL_e785c048abcc

Synchronization Settings

SETTING	VALUE
SOURCE ANCHOR	mS-DS-ConsistencyGuid
SYNC CRITERIA	AlwaysProvision
AZURE AD APP AND ATTRIBUTE FILTERING	Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC	Disabled
GROUP WRITEBACK	Disabled
PASSWORD WRITEBACK	Disabled
AUTO UPGRADE	Enabled
SQL SERVER NAME	(localdb)
USER PRINCIPAL NAME	userPrincipalName
FILTER OBJECTS TO SYNCHRONIZE BY GROUP	Disabled
DEVICE WRITEBACK	Disabled
EXCHANGE HYBRID DEPLOYMENT	Disabled
PASSWORD HASH SYNCHRONIZATION	Enabled
USER WRITEBACK	Disabled
EXCHANGE MAIL PUBLIC FOLDERS	Disabled
SQL SERVER INSTANCE NAME	.\ADSync

Previous Exit

□□□□ □□ □□ □□□□ □ □□□ □□□□ □□ □□□□ □□□□ □□ □□□□.

□□□□: □□ □□ 1□□□□.

Answer Area

User1 [answer choice].

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

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

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

Answer:
Answer Area

User1 [answer choice].

- cannot change her password from any Microsoft portals
- cannot change her password from any Microsoft portals
- can change her password by using self-service password reset feature only
- can change her password from the Microsoft 365 admin center only

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

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

Explanation:

Answer Area

User1 [answer choice]. cannot change her password from any Microsoft portals

If the password for User1 is changed in Active Directory, [answer choice]. the password hash will be synchronized to Azure AD

NEW QUESTION: 19

Microsoft 365 E5 ☐☐☐☐ ☐☐, ☐☐☐☐ ☐☐ Microsoft Defender ☐☐☐☐ ☐☐☐☐. OAuth ☐☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐.

☐☐☐☐: Defender for Cloud Apps ☐ API ☐☐☐☐ ☐☐☐☐☐☐.

☐☐☐☐ ☐☐☐☐☐☐☐☐?

A. ☐

B. 000

Answer: B (LEAVE A REPLY)

NEW QUESTION: 20

Endpoint Microsoft Defender 365 E5

Microsoft Intune

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	iOS
Device4	Android

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint, Endpoint

Endpoint?

Endpoint: 1

Devices that can onboard to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Answer:

Devices that can onboarded to Microsoft Defender for Endpoint

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Explanation:

Devices that can onboarded to Microsoft Defender for Endpoint:

- Device 1 only
- Device 1 and Device 2 only
- Device 1 and Device 3 only
- Device 1 and Device 4 only
- Device 1, Device 2, and Device 4 only
- Device 1, Device 2, Device 3, and Device 4

Endpoint security policies that must be configured:

- A conditional access policy only
- A device compliance policy only
- A device configuration profile only
- A device configuration profile and a conditional access policy only
- Device configuration profile, device compliance policy, and conditional access policy

Reference:
<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-machines-onboarding?view=o365-worldwide>

NEW QUESTION: 21

Microsoft Defender for Endpoint is installed on Microsoft 365 E5 devices. Microsoft Defender for Cloud Apps is installed on 30 devices. How many devices are protected by both Microsoft Defender for Endpoint and Microsoft Defender for Cloud Apps?

- A. 30
- B. Cloud Discovery
- C. 30 devices
- D. Cloud Discovery

Answer: A (LEAVE A REPLY)

NEW QUESTION: 22

□□ □□□ □□□□ □□□ □□ □□□ □□□□ □□□.

Microsoft Cloud App Security □□ □□□□ □□ □□ □□□ □□ □ □□ □□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.


Minimum number of data sources:  ▼

1
3
6

Minimum number of log collectors: ▼

1
3
6

Answer:


Minimum number of data sources:  ▼

1
3
6

Minimum number of log collectors: ▼

1
3
6

Explanation:

Minimum number of data sources:  ▼

1
3
6

Minimum number of log collectors: ▼

1
3
6

References:

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

NEW QUESTION: 23

User1 is a Microsoft 365 E5 user. User1 is a member of the Restricted entities group in the Microsoft 365 Defender portal. User1 is also a member of the Restricted entities group in Exchange Online PowerShell. User1 is also a member of the Restricted entities group in the Microsoft 365 Defender portal. Which of the following actions can be performed by User1?

- A. Exchange Online PowerShell
- B. Microsoft Purview
- C. Microsoft 365 Defender
- D. Microsoft 365 Defender
- E. Microsoft Entra

Answer: (SHOW ANSWER)

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

Remove a user from the Restricted entities page in the Microsoft 365 Defender portal In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & collaboration > Review > Restricted entities. Or, to go directly to the Restricted entities page, use <https://security.microsoft.com/restrictedentities>.

Reference:

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

NEW QUESTION: 24

Microsoft 365 IS a Microsoft Defender for Cloud Apps user. Microsoft Entra 10 is an App1 user. App1 is a Microsoft 365 IS user. App1 is also a Microsoft 365 IS user. Which of the following actions can be performed by App1?

- A. Microsoft 365 Defender for Cloud Apps (SIEM) user
- B. Microsoft 365 Defender for Cloud Apps user
- C. App1 is a Microsoft AppControl user
- D. App1 is a Microsoft 365 IS user

Answer: D (LEAVE A REPLY)

NEW QUESTION: 25

Microsoft 365 E5 user is a Microsoft 365 E5 user. Microsoft 365 E5 user is also a Microsoft 365 E5 user. Microsoft 365 E5 user is also a Microsoft 365 E5 user. Microsoft 365 E5 user is also a Microsoft 365 E5 user. Which of the following actions can be performed by Microsoft 365 E5 user?

- A. Microsoft 365 E5 user
- B. Microsoft 365 E5 user (DLP) user
- C. Microsoft 365 E5 user
- D. Microsoft Cloud App Security user

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 26

Microsoft 365 Defender □□□□ □□□ □□□□ □□□□.
□□□ □□□ □□□ □□□□ □□□□□?

- A. 30□
- B. 60□
- C. 3□□
- D. 6□□
- E. 12□□

Answer: C (LEAVE A REPLY)

Data retention information for Microsoft Defender for Office 365

By default, data across different features is retained for a maximum of 30 days. However, for some of the features, you can specify the retention period based on policy. See the following table for the different retention periods for each feature.

Defender for Office 365 Plan 1

* Alert metadata details (Microsoft Defender for Office alerts)

90 days.

Note: By default, the alerts queue in the Microsoft 365 Defender portal displays the new and in progress alerts from the last 30 days. The most recent alert is at the top of the list so you can see it first.

Alerts

Export 30 Days Manage alerts Customize columns Filter

Filters: Status: New +1

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Impacted assets	First activity
Email reported by ...		Informational		In progress	Others	MDO	Jenny Sivalingam	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Custom detection -...		Medium		New	Execution	Custom detection	msdo@sdf3p1.on...	Apr 14, 2021
"> <img src=x oner...	+5	High	No threats found	New	Exploit	Custom detection	cont-denamarks	Apr 14, 2021
"> <img src=x oner...	+2	High	No threats found	New	Exploit	Custom detection	cont-mikebarden	Apr 7, 2021
Unfamiliar sign-in ...		Low		New	Initial access	AAD Identity Protection	bbsecadmin	Apr 14, 2021
Admin action sub...		Informational	Remediated	New	Suspicious activity	Automated investigation		Apr 14, 2021
Test email custom ...		Medium		New	Execution	Custom detection	Clare Love	Apr 14, 2021

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/mdo-data-retention>

NEW QUESTION: 27

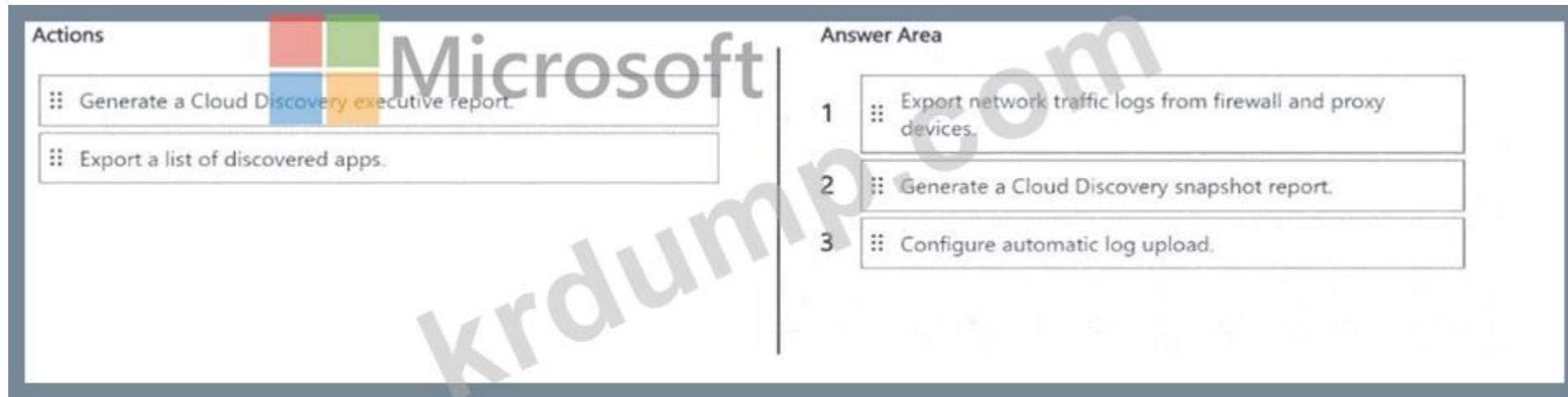
100 Windows 10 Microsoft 365 E5 .
 Windows 10 .
 ?

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

Answer: C (LEAVE A REPLY)

NEW QUESTION: 28

Microsoft 365 E5 Microsoft Defender .
 Cloud Discovery .



NEW QUESTION: 29

contoso.com. You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com. You need to ensure that the Microsoft Defender (Office 365) policy is applied to user1@fabunkam.com.

Policy1 is applied to user1@fabunkam.com. You need to ensure that the Microsoft Defender (Office 365) policy is applied to user1@contoso.com.

Policy1 is applied to user1@fabunkam.com. You need to ensure that the Microsoft Defender (Office 365) policy is applied to user1@contoso.com.

Policy1 is applied to user1@fabunkam.com. You need to ensure that the Microsoft Defender (Office 365) policy is applied to user1@contoso.com.

- A. Create a new policy and assign it to user1@contoso.com.
- B. Assign Policy1 to user1@contoso.com.
- C. Assign Policy1 to user1@fabunkam.com.
- D. Assign Policy1 to user1@contoso.com.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 30

Microsoft 365. You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com.

You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com.

You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com.

You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com. You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com.

You need to ensure that the Microsoft 365 ES policy is applied to user1@contoso.com.

- A. Classifiers
- B. Policies
- C. Rules
- D. Conditions
- E. Data Loss Prevention (DLP) policies

Answer: A,E (LEAVE A REPLY)

A: Classifiers

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

Where you can use classifiers

Classifiers are available to use as a condition for:

Office auto-labeling with sensitivity labels

Auto-apply retention label policy based on a condition

Communication compliance

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

Data loss prevention

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

Reference:

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

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

NEW QUESTION: 31

□□□ □□□ Microsoft 365 □ □□□□ □□□□.

□□□ □□□ □□□ □□ □□□ □□□□ □□□□□.

□□ □□ '□□'□□□ □□□ □□□ □□□ □□□□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Exchange □□ □□□ □□ □□ □□

B. Exchange □□ □□□ □□ □□

C. Microsoft 365 □□ □□ □□□ □□□ □□ □□(DLP) □□

D. Microsoft 365 □□ □□□ Dace □□□

Answer: A (LEAVE A REPLY)

MS-102-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-102-KR □□! DumpTop □ □□ **MS-102-KR** □□ □□□ □□□□□□, DumpTop MS-102-KR □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-102-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 32

□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.

Microsoft 365 □□□ □□□□.

□□□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□□□□ Active Directory □□ □□□ □□□ □□□□ □□□.

* □□□□ Microsoft Entra Self-Service Password Reset(SSPR)□ □□□ □ □□□ □□□.

□□□ □□□□ □□□?

A. □□□□ □□

B. Microsoft Entra Seamless Single Sign-On(Microsoft Entra Seamless SSO)

C. Microsoft Entra ID □□

D. □□□□ □□ □□□

Answer: (SHOW ANSWER)

NEW QUESTION: 33

Group1 Group2 Microsoft 365 E5. You need to configure authentication methods for Group1 and Group2.

* Group1 must use a method that does not require a user to enter a password.

* Group2 must use a method that requires a user to enter a password.

Which authentication methods should you configure for Group1 and Group2? (Select two.)

Options: A) Microsoft Authenticator B) Temporary Access Pass C) Email OTP D) Certificate-based authentication E) Passkey (FIDO2)


Methods

- Passkey (FIDO2)
- Certificate-based authentication
- Email OTP
- Microsoft Authenticator
- Temporary Access Pass
- Third-party software OATH tokens

Answer Area

Group1:

Group2:



Answer:

Methods

- Passkey (FIDO2)
- Certificate-based authentication
- Email OTP
- Microsoft Authenticator
- Temporary Access Pass
- Third-party software OATH tokens

Answer Area



Group1: Temporary Access Pass

Group2: Microsoft Authenticator

Explanation:

Which activity reports are available in the admin center?

- A. Microsoft 365 Reports
- B. Microsoft Purview Reports
- C. Microsoft Entra Reports
- D. Microsoft 365 Reports in the admin center

Answer: D (LEAVE A REPLY)

Microsoft 365 Reports in the admin center

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

Which activity reports are available in the admin center

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

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

Reference:

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

NEW QUESTION: 37

Microsoft 365 E5 includes Microsoft Defender for Cloud. Which Windows 11 activity reports are available in the admin center? Cloud Discovery is one of the reports. Which other reports are available?

- A. Microsoft 365 Reports
- B. Azure Monitor Agent
- C. Microsoft 365 Reports in the admin center
- D. Microsoft 365 Reports

Answer: C (LEAVE A REPLY)

NEW QUESTION: 38

Microsoft Defender XDR is included in Microsoft 365 E5.

Microsoft Defender for Cloud includes Microsoft Secure Score. Which other reports are available?

NEW QUESTION: 42

Microsoft Defender for Endpoint is installed on a Microsoft 365 E5 tenant. A file named File1.exe is detected as malicious. What is the next step to investigate the file?

- A. Download the file
- B. Upload the file to VirusShare
- C. Upload the file to Microsoft Defender for Cloud Apps

Answer: (SHOW ANSWER)

NEW QUESTION: 43

Azure AD is connected to Microsoft 365 E5. Microsoft Defender XDR is installed on the Azure AD tenant. An IP address is detected as malicious. What is the next step to investigate the IP address? (Select two.)

Answer Area



Answer:
Answer Area



Explanation:



NEW QUESTION: 44

Microsoft 365 E5 □□□ □□□□. □□ □□ □□ □□□□ □□□□ □□□. □□ □□□ □□□□ □□□?

- A. Microsoft Purview □□ □□ □□
- B. Microsoft Entra □□ □□
- C. Intune □□ □□
- D. Exchange □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 45

□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

□□: User1

UPN: user1@contoso.com

□□□ □□: user1@marketing.contoso.com

MFA □□ □□: □□□□□

User1□ user1@marketing.contoso.com □□□ □□□ □□□□ □□□ Outlook□ □□□□□□ □□ □□□□ □□□□ □ □□□□.

User1□ user1@marketing.contoso.com□ □□□□ □□□ Outlook□ □□□□ □ □□□ □□□□ □□□.

□□□ □□ □□□?

- A. User1□ MFA □□ □□□ □□□□□.
- B. User1□ □□□□□ □□□□□□.
- C. User1□ □□ □□ □□□ □□□ □□□□□.
- D. User1□ UPN□ □□□□□.

Answer: D (LEAVE A REPLY)

Microsoft's recommended best practices are to match UPN to primary SMTP address. This article addresses the small percentage of customers that cannot remediate UPN's to match.

Note: A UPN is an Internet-style login name for a user based on the Internet standard RFC 822. The UPN is shorter than a distinguished name and easier to remember. By convention, this should map to the user's email name. The point of the UPN is to consolidate the email and logon namespaces so that the user only needs to remember a single name.

Configure the Azure AD multifactor authentication registration policy

Azure Active Directory (Azure AD) Identity Protection helps you manage the roll-out of Azure AD multifactor authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you're signing in to.

Reference:

<https://docs.microsoft.com/en-us/windows/win32/ad/naming-properties#userprincipalname>

NEW QUESTION: 46

□□□ □□ 3□□ □□ 1□□ □□□ □□□□. □□□ □□□ □□□□□.

□ □□□ Microsoft 365 □□□□ □□□□ □□ □□ □□□ □□□ □□□□□.
□□ □□□□ □□□□□□ □□ □□ □□□ □□□□□ □□ Microsoft 365 □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□□?

- A. Microsoft Intune □□ □□ □□
- B. Azure AD □□□ □□□
- C. Microsoft Intune □□ □□ □□□
- D. Azure AD □□ □□

Answer: B ([LEAVE A REPLY](#))

MS-102-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-102-KR □□! DumpTop □ □□ **MS-102-KR** □□ □□□ □□□□□□, DumpTop MS-102-KR □□ □□□ □□□□□□□□
□□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-102-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 47

□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□□ □□□□.

Name	Type
Mailbox1	Microsoft Exchange Online mailbox
Account1	Microsoft OneDrive account
Site1	Microsoft SharePoint Online site
Channel	Microsoft Teams channel

□□ □□□ □□ □□□ □□□□ □□ □□□□ □□□ □□□□ □□□ □ □□□□?

- A. Mailbox1 □ Site1 □
- B. Mailbox1, Account1, Site1 □
- C. Account1 □ Site1 □
- D. Mailbox1, Account1, Site1, Channel1
- E. Account1, Site1, Channel1 □

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 48

□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Type	Number of devices	Operating system	Enrollment status
Corporate	150	Windows 11	Azure AD-joined, Microsoft Intune-managed
Bring your own device (BYOD)	25	Windows 11	Unmanaged

Microsoft Defender for Endpoint is a cloud-based endpoint protection solution that provides comprehensive security for Windows, macOS, and Linux devices. It offers real-time threat detection, investigation, and response capabilities. The solution is designed to protect against a wide range of threats, including malware, ransomware, and advanced persistent threats (APTs). It also provides visibility into device health and security posture, enabling IT administrators to identify and remediate vulnerabilities. Microsoft Defender for Endpoint is available as a standalone product or as part of the Microsoft 365 E5 license. The solution is managed through the Microsoft Defender Security Center console in the Microsoft 365 admin center. The console provides a centralized view of security alerts, incidents, and threat intelligence across all managed devices. It also offers detailed reports and analytics to help organizations understand their security posture and improve their overall security strategy. The solution is designed to be easy to deploy and manage, with minimal configuration required. It integrates with other Microsoft security products, such as Microsoft Defender for Office 365 and Microsoft Defender for Cloud, to provide a comprehensive security ecosystem. The solution is also available as a managed service, where Microsoft handles the day-to-day management and updates of the software. This allows organizations to focus on their core business operations while ensuring their endpoints are protected against the latest threats. The solution is designed to be scalable and flexible, allowing organizations to protect a large number of devices across different environments and geographies. It also provides detailed logging and reporting capabilities, enabling organizations to audit their security posture and identify areas for improvement. The solution is designed to be easy to integrate with existing IT infrastructure, with minimal disruption to operations. It also provides a rich set of APIs and integrations with third-party security tools, allowing organizations to extend their security capabilities and meet their specific requirements. The solution is designed to be easy to use and manage, with a user-friendly interface and comprehensive documentation. It also provides a range of support options, including technical assistance, training, and consulting services. The solution is designed to be easy to upgrade and maintain, with regular updates and patches to address new threats and vulnerabilities. It also provides a range of customization options, allowing organizations to tailor the solution to their specific needs and requirements. The solution is designed to be easy to integrate with existing IT infrastructure, with minimal disruption to operations. It also provides a rich set of APIs and integrations with third-party security tools, allowing organizations to extend their security capabilities and meet their specific requirements. The solution is designed to be easy to use and manage, with a user-friendly interface and comprehensive documentation. It also provides a range of support options, including technical assistance, training, and consulting services. The solution is designed to be easy to upgrade and maintain, with regular updates and patches to address new threats and vulnerabilities.

Onboarding method

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

Device type

Corporate:

BYOD:

Answer:

Onboarding method

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

Device Type

Corporate:

BYOD:

Explanation:

Onboarding method

- A local script
- Group Policy
- Integration with Microsoft Defender for Cloud
- Microsoft Intune
- Virtual Desktop Infrastructure (VDI) scripts

Device Type

Corporate: Microsoft Intune

BYOD: Integration with Microsoft Defender for Cloud

NEW QUESTION: 49

Office 365 is a cloud-based productivity suite that includes various applications and services. Microsoft 365 is a subscription-based version of Office 365 that includes additional services like Microsoft Defender for Office 365. Office 365 is a suite of productivity applications, while Microsoft 365 is a subscription-based version of Office 365 that includes additional services like Microsoft Defender for Office 365.

Answer Area



To configure the notifications:

- Briefing email
- Briefing email
- Help desk information
- Organization information

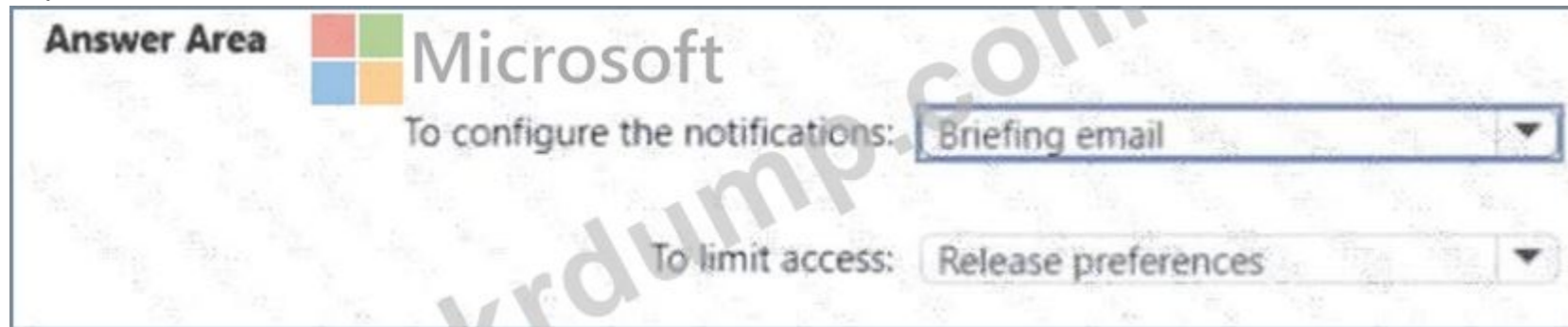
To limit access:

- Release preferences
- Privileged Access
- Release preferences
- Office installation options

Answer:



Explanation:



NEW QUESTION: 50

Microsoft Defender for Endpoint is installed on all Microsoft 365 devices. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint.

- A. Microsoft Purview DLP (Data Loss Prevention) policies.
- B. Microsoft Defender for Endpoint policies.
- C. Microsoft Defender for Endpoint policies.
- D. Microsoft Purview DLP (Data Loss Prevention) policies.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 51

The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint. The organization has a policy that requires all devices to be protected by Microsoft Defender for Endpoint.

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

Answer: E (LEAVE A REPLY)

NEW QUESTION: 52

Microsoft 365 Defender

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Cloud

Answer Area

Apps matching all of the following

Select a filter

+ Add a filter

Apply to:

All continuous reports

Trigger a policy match if all the following occur on the same day:

Alerts

Create an alert for each matching event with the policy's severity

Governance actions

- Tag app as sanctioned
- Tag app as unsanctioned
- Tag app as monitored
- Tag app with custom tag

Select app tag



Answer:



Apps matching all of the following

Select a filter ▼

+ Add a filter ✓

Apply to:

All continuous reports ▼

Trigger a policy match if all the following occur on the same day:

Alerts

Create an alert for each matching event with the policy's severity

Governance actions

Tag app as sanctioned

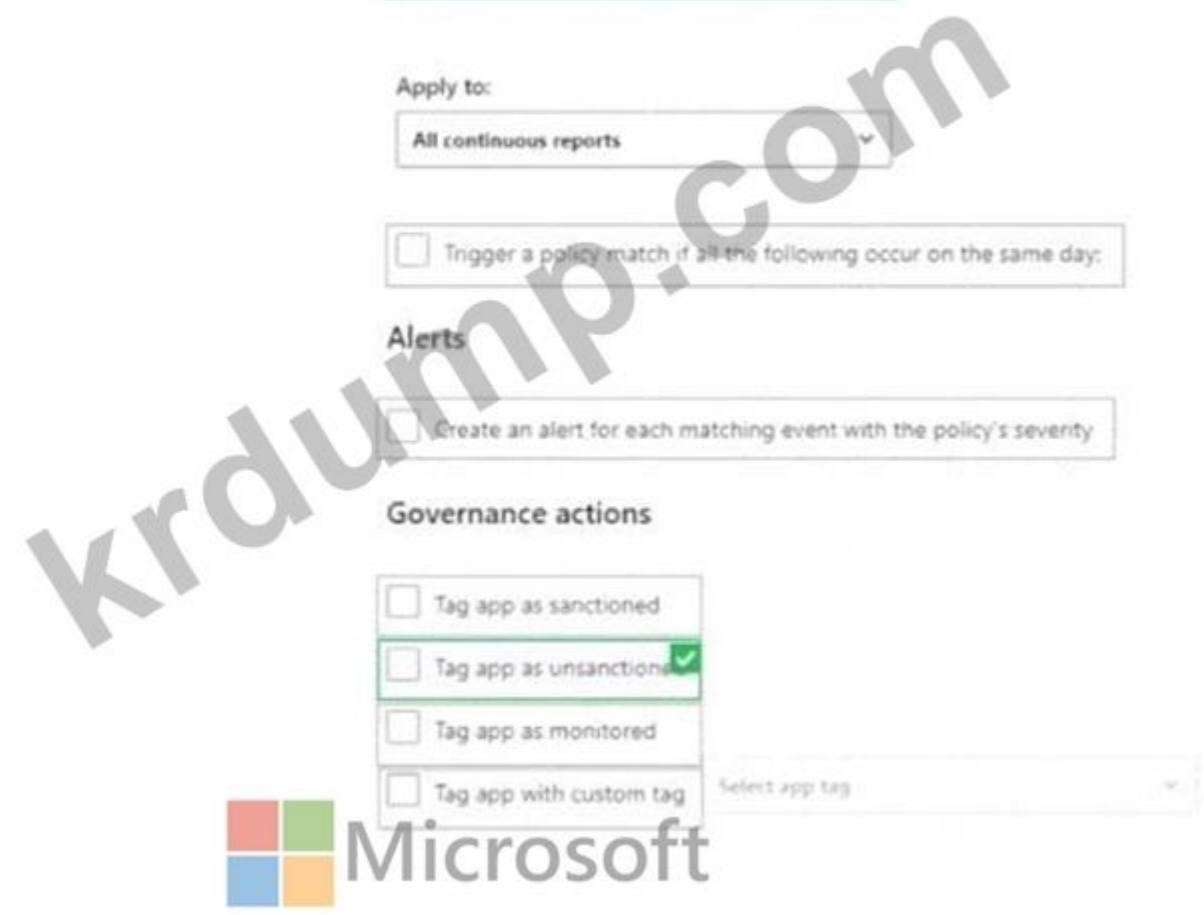
Tag app as unsanctioned ✓

Tag app as monitored

Tag app with custom tag

Select app tag ▼

Explanation:



NEW QUESTION: 53

□□□□□ Active Directory □□□□□ □□□□ □□□□.

Microsoft 365 □ □□□□□.

□□□□ □□□□ □□□ □□□□□□.

□□□□ ID□ □□ □□ □□□□ □□□□ □□□□. □□□□ □□ □□ □□□ □□□□ □□□□.

* Active Directory □ □□□ □ □□ □□ □□□□ Microsoft 365 □□□□ □□□□□□ □□□□ □ □□□ □□□□.

* □□□ □□□□□□ 10□ □□□□□□ □□□□.

□□□: □□□□ □□□ □□□□□ Microsoft Entra Password □□□ □□□□□□. □□□ □□□ □□□□□□?

- A. □
- B. □□□

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 54

Microsoft 365 E5 □□□ □□□□□.

□□□□ □□□ □□□ □□□□ □□□□ □ App1□□□□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□□.

□□□□ □□ □□□□□□ □□□□ □ □□□□ □□□ □□ □□ □□ □□□ □□□ □□□.

- A. □□ □□ □□(MFA)
- B. □□□ □□□ □□
- C. □□ □□
- D. □□□ □□ □□

Answer: **B** ([LEAVE A REPLY](#))

NEW QUESTION: 55

Microsoft 365 ES □□□ □□□□.

Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.

Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.

□□□: □□□□□ □□ □ □□(EDR) □□□ □□□□.

□□□ □□□ □□□□□?

- A. □
- B. □□□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

Azure AD □□□□ Microsoft 365 E5 □□□ □□□□. □□□□□ □□ □□ □□□ □□□□□ □□□□□.



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

Endpoint□ Microsoft Defender□ □□□ □□□□□.

Microsoft Defender for Endpoint□□ □□ □□ □□□ □□(RBAC)□ □□ □□□ □□□□□.

Microsoft 365 Defender □□□□ □□ □□□□□ □ □□ □□□□ □□□□ □□□.

□□ □□□□ □□□□ □□□?

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

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 57

Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender□ □□□□ □□□□.

App1□□□ □□□□ □□ □□□□.

□□ □□ □□□ □□□□ App1□ □□ □□ □□□□ □□□□ □□□.

* □□□ □□□ □□□ □□□□□ □□□□□.


* □□□ □□ □□ □□□ □□□□□.
□ □□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□□.

Enables the real-time monitoring of user activities:

- Conditional Access App Control
- Microsoft Purview Information Protection
- Score metrics

Blocks specific activities as needed:

- A session policy
- A file policy
- A session policy
- An access policy




Answer:
Answer Area

Enables the real-time monitoring of user activities:

- Conditional Access App Control
- Microsoft Purview Information Protection
- Score metrics

Blocks specific activities as needed:

- A session policy
- A file policy
- A session policy
- An access policy



Explanation:
Answer Area

Enables the real-time monitoring of user activities:

Blocks specific activities as needed:



NEW QUESTION: 58

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
User1□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□ □□□□ □□□□. □□□ □□□ □□□□ User1□ □□□□ □□□. □□ □□□ □□□□ □□□?
A. Microsoft 365 □□ □□

New × **Conditions** × **Device state (preview)** □ ×

Info

* Name
Policy1 ✓

Assignments

Users and groups ⓘ
0 users and groups selected >

Cloud apps ⓘ
1 app included >

Conditions ⓘ
0 conditions selected >

Access controls

Grant ⓘ
Block access >

Session ⓘ
0 controls selected >

Enable policy
On Off

Info

Sign-in risk ⓘ
Not configured >

Device platforms ⓘ
Not configured >

Locations ⓘ
Not configured >

Client apps (preview) ⓘ
Not configured >

Device state (preview) ⓘ
Not configured >

Info

Configure ⓘ
Yes No

Include Exclude

Select the device state condition used to exclude devices from policy.

Device Hybrid Azure AD joined ⓘ

Device marked as compliant ⓘ

Answer:

New Microsoft

Info

* Name
Policy1 ✓

Assignments

- Users and groups ⓘ
0 users and groups selected >
- Cloud apps ⓘ
1 app included >
- Conditions ⓘ
0 conditions selected >

Access controls

- Grant ⓘ
Block access >
- Session ⓘ
0 controls selected >

Enable policy

On Off

Conditions

Info

- Sign-in risk ⓘ
Not configured >
- Device platforms ⓘ
Not configured >
- Locations ⓘ
Not configured >
- Client apps (preview) ⓘ
Not configured >
- Device state (preview) ⓘ
Not configured >

Device state (preview)

Info

Configure ⓘ

Yes No

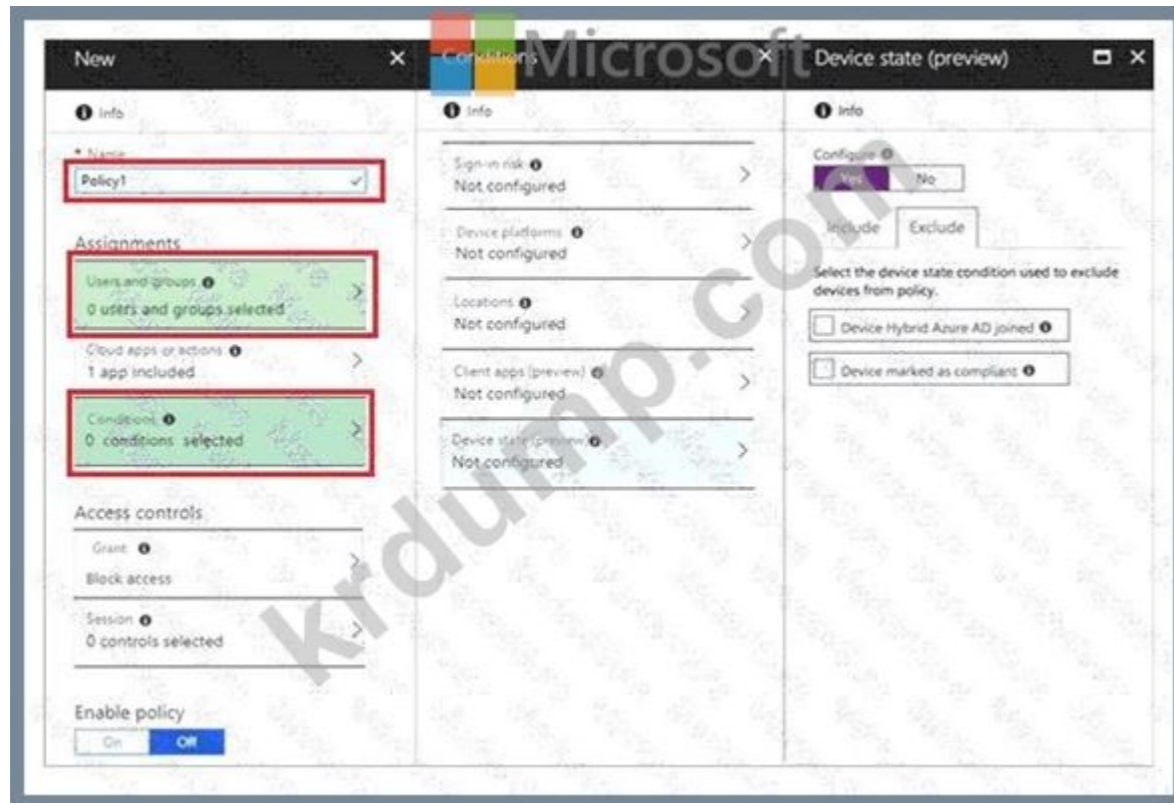
Include Exclude

Select the device state condition used to exclude devices from policy.

- Device Hybrid Azure AD joined ⓘ
- Device marked as compliant ⓘ

Explanation:

Suggested answer:



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

MS-102-KR □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-102-KR □□! DumpTop □ □□ **MS-102-KR** □□ □□□ □□□□□□, DumpTop MS-102-KR □□ □□□ □□□□□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-102-KR □□□ □□□□□. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 62

Microsoft 365 E5 □□□ □□□□. □□□ □□□□ □□ □□□□ □□ □□□□ □□ □□□□ □□□□ □□□□ □□□□. □□ □□□□ □□□□ □□□ □□ □□ □□(MFA)□ □□□□ □□□□. □□□ □□□ □□□□□ □□ □ □□ □□□ □□□ □□□□□. □□ □□ □□□ □□ □□□□ □□□□□ □□ □□□ □□, □□□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□ □□□. □□□ □□□□ □□□?

- A. □□ □□
- B. MFA □□ □□
- C. □□□ □□□ □□
- D. □□ □□□ □□□□ □□□(SSPR)

Answer: (SHOW ANSWER)

Self-remediation with self-service password reset

If a user has registered for self-service password reset (SSPR), then they can also remediate their own user risk by performing a self-service password reset.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock>

NEW QUESTION: 63

Office 365 Microsoft Defender Microsoft 365 .
 .
 .
 .

- A. .
- B. .
- C. .
- D. .
- E. .

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 64

Microsoft 365 E5 Microsoft Defender for Endpoint

Name	Platform
Device1	Windows 11
Device2	Android
Device3	Linux

.

Name	Template
Policy1	Microsoft Defender Antivirus
Policy2	Device Control

. a. .:



Answer:



Explanation:



NEW QUESTION: 65

Microsoft 365 E5

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group2

Microsoft 365 E5

* AntiSpam1

* : 0

* ,

o : User3

o : Group1

* ,

o : 2

*

o 100

* : AntiSpam2

* : 1

* ,

o : User! : Group2

* ,

o : User3

*

o 50

Microsoft 365 E5

Microsoft 365 E5

Answer Area



Statements

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

Answer:

Answer Area



Statements

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

Explanation:

Answer Area



Statements

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

NEW QUESTION: 66

Microsoft 365 E5 □□□ □□ □□□□ □□ Microsoft Defender □ □□□□ □□□□.

Defender for Cloud Apps □□ □□□ □□ □□□ □□□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□ □□□□ □ □□□?

□□□ □□□ □□□ □□□□ □□□□□.

A. □□□ □□ □□ □□

- B. 00 0000
- C. 000 00
- D. 0000 00 00
- E. Microsoft Power Automate 0000

Answer: C,E ([LEAVE A REPLY](#))

NEW QUESTION: 67

Endpoint Security 0 0000 Microsoft 365 E5 000 0000.
000 000 00 000 Endpoint Security Manager 000 0000 000.
00 000 000 000 0 000?

- A. 00 00 00 0 00 00
- B. Microsoft 365 0 00
- C. 00 00
- D. 00, 00 00 00, Microsoft 365 0 00
- E. 00 00 00, Microsoft 365 0 00 00

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 68

Office 365 0 Microsoft Defender 0 000000?
00 00000 0000 0000 00000.
000000 000 0000 000000 000 00 00 000 000 000.
00000 0 0000 000 00 0 00 00 000 00000?

- A. 7
- B. 45
- C. 30
- D. 15

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 69

Microsoft 365 ES 000 0000.
Microsoft 365 Defender 0000 000 Microsoft Secure Score 0 00000.
00 00 0000 000 0000 00000.
00 00 000 0000 000 0000 0 000 000.
00 000 0000 000?

- A. 00 00 00
- B. 000 00 00 00
- C. 00 00
- D. 00

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 70

Microsoft 365 E5 □□□□ □□□□.

□□□ □□ □□□□ □□□ □□ □□□ □□ □□□□□ □□□ □□ □□□ □□□ □□□.

□□ □ □□ □□□ □□□ □ □□□□? □ □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

A. □□ □□ □□

B. □□□ □□□ □□

C. Microsoft Cloud App Security □□ □□

D. □□□ □□ □□(DLP) □□

E. □□□□□□ □□ □□

Answer: (SHOW ANSWER)

NEW QUESTION: 71

□□ □□□□ Defender for ID □□□ □□□□ □□□?

A. □□1

B. □□2

C. □□3

D. □□4

E. □□5

Answer: A (LEAVE A REPLY)

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

NEW QUESTION: 72

□□□ Microsoft 365 □□□ □□□□ □□□□.

Microsoft Entra □□ □□ □□□□ □□ □□□ □□ □□ □□ □□□□□ □□ Microsoft Authenticator □□□ □□□□□.

Microsoft Authenticator on companion applications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. [Learn more](#)



□□□□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□□ □□□ □□ □□□□□□ □□□□ □□□?

A. □□□□□□□□ 365 □□□□□

B. □□□□□□□□ □□

C. □□□□□□□□ □□□

Protection settings

Set your outbound anti-spam settings for this policy.

Message limits

Set an external message limit

Set an internal message limit

Set a daily message limit

Restriction placed on users who reach the message limit

Forwarding rules

Automatic forwarding rules

Notifications

Send a copy of suspicious outbound messages or message that exceed these limits to these users and groups

Notify these users and groups if a sender is blocked due to sending outbound spam

Policy1 User1

User1 24

A. 720

B. 30

C. 1000

D. 1030

Answer: A (LEAVE A REPLY)

NEW QUESTION: 75

Microsoft 365 E5

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

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

NEW QUESTION: 78

Microsoft Endpoint Manager Device1 Windows 10 Microsoft 365

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

- A.
- B. Policy3
- C. Policy2
- D.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 79

Endpoint Microsoft Defender Microsoft Defender for Endpoint

Name	Device group
Device1	ATP1
Device2	ATP1
Device3	ATP2

Microsoft Defender for Endpoint

Name	Device
Alert1	Device1
Alert2	Device2
Alert3	Device3

- * IOC
 - *
 - * ATP1
- Alert1: Device1
Alert2: Device2
Alert3: Device3


Answer Area



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

Answer:

Answer Area



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

Explanation:

Answer Area



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

NEW QUESTION: 80

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

Exchange 2016 Retention1 Microsoft Office 365 Retention1.

Microsoft Exchange Online Retention2.

Retention1 Retention2? Microsoft Exchange Online.

Retention1: 1.

Answer:

Explanation:

- A. □□□ □□ □□ □□
- B. □□ □□ □□
- C. □□ □□□□ □□□□□
- D. □□□ □□

Answer: A ([LEAVE A REPLY](#))

Reference:

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

NEW QUESTION: 83

Microsoft 365 □□ □□ □□□□ Site1□□□□ Microsoft SharePoint Online □□□□ □□ □□□ □□ □□(DLP) □□□ □□□□□. Site1□□ □□ □□ □□□ □□□ □□□□ □□□□.

Role	Member
Site owner	Prvi
Site member	User1
Site visitor	User2

Prvi□ □□□ □□□ □□□ □□□□. (□□ □□ □□□□□.)

S Site1

Share

Search Documents

+ New Upload Quick edit Sync All Documents

Documents

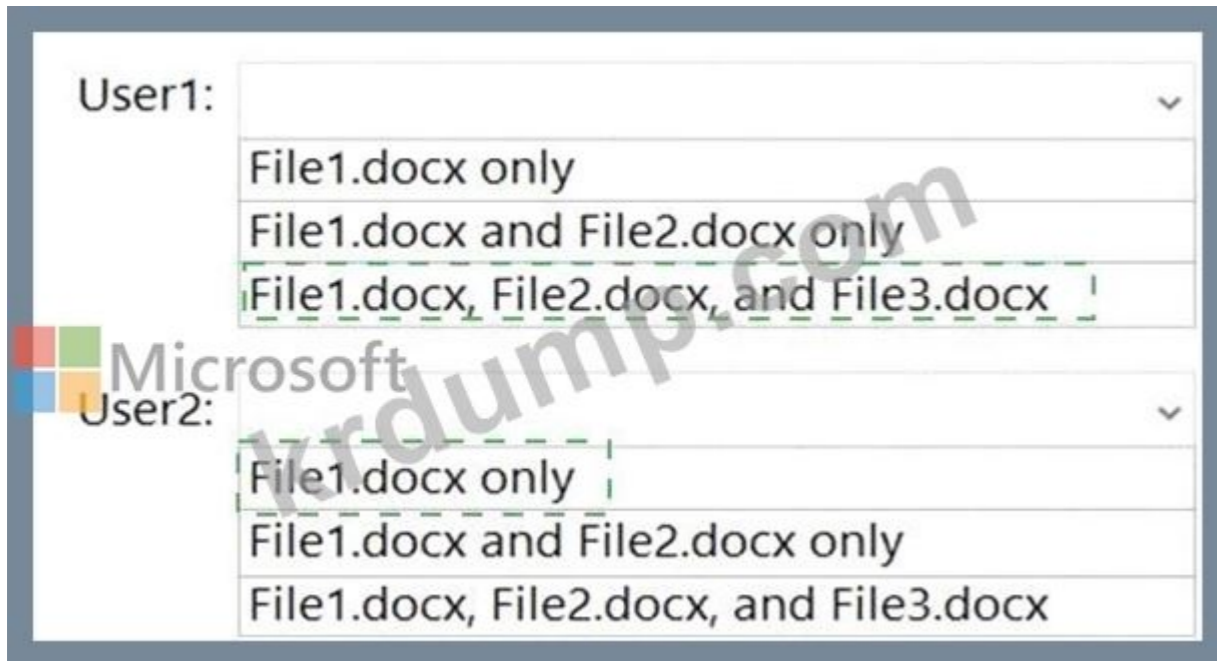
Name	Modified	Modified By	+ Add column
File1.docx	About a minute ago	Prvi	
File2.docx	A few seconds ago	Prvi	
File3.docx	A few seconds ago	Prvi	

User1 User2
 User1: File1.docx only
 User2: File1.docx only

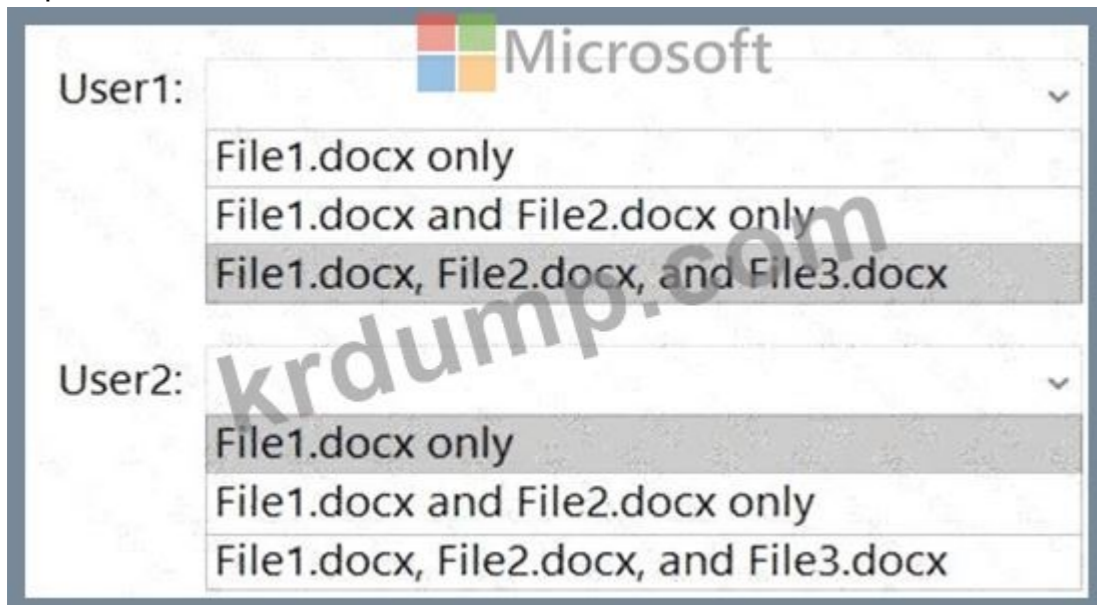
User1: File1.docx only, File1.docx and File2.docx only, File1.docx, File2.docx, and File3.docx

User2: File1.docx only, File1.docx and File2.docx only, File1.docx, File2.docx, and File3.docx

Answer:



Explanation:



Reference:

<https://sharepointmaven.com/4-security-roles-of-a-sharepoint-site/>

<https://gcc.microsoftcrmpartals.com/blogs/office365-news/190220SPIcons/>

NEW QUESTION: 84

Microsoft 365 □□□ □□□□.

□□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□ □□□ □□□ □□□ □□□ □□□ □□□ □□□.

□□□ □□□□ □□□?

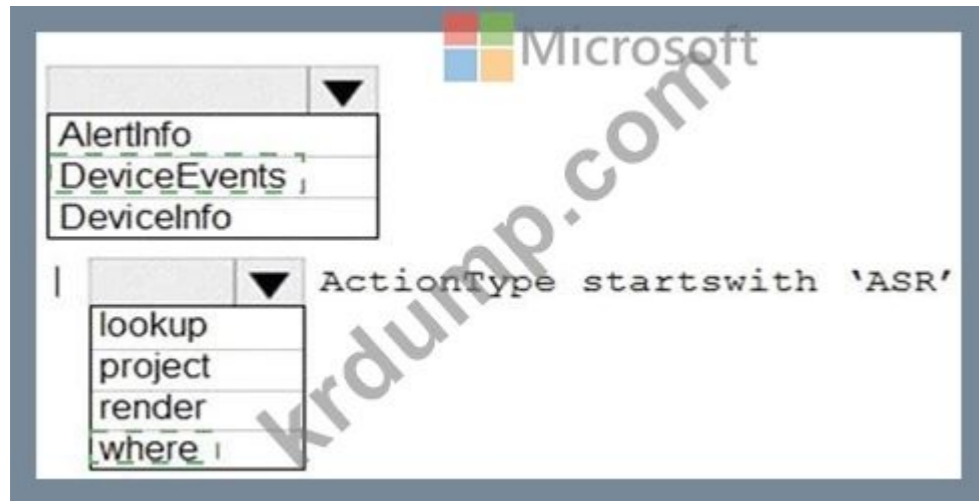
A. □□□ □□ □□ □□

B. □□ □□

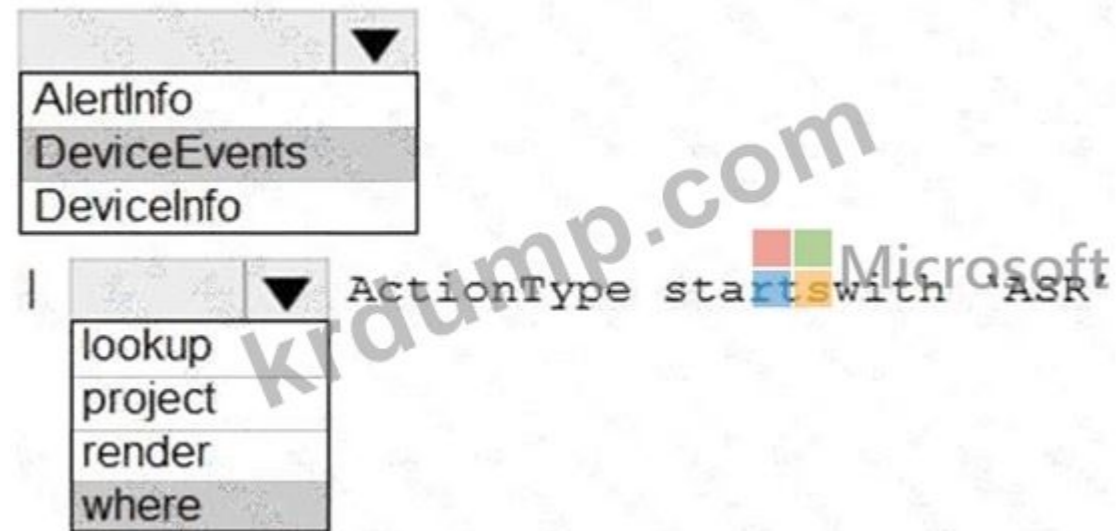
C. □□ □□

D. □□□ □□ □□(DLP) □□

Answer: C (LEAVE A REPLY)



Explanation:



Reference:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction-rules-part-3/ba-p/1360968>

NEW QUESTION: 87

Microsoft 365 E5 □□□ □□□□.
 □□ □□ □□(MFA)□ □□□□□ □□□.
 □□□□ □□ □□ □□□ □□□□ □□□□. □□□□ □□□□□ MFA□ □□□□ □□□□ □□□ □□□ MFA□ □□□ □□□□□□ □□□ □□□□□ □□ □□□□.
 □□□ □□□□ □□?

- A. □□
- B. Microsoft □□□
- C. FID02 □□ □
- D. □□□□
- E. □□□ OTP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 88

Microsoft 365 E5 □□□□ □□□□.

Which of the following is a Microsoft 365 security solution?

Microsoft Word is a Microsoft 365 Word document solution.

Microsoft Word is a Microsoft 365 Word document solution.

Which of the following is a Microsoft 365 security solution?

A. Microsoft 365 Security Solutions

B. Microsoft 365 Security Solutions

C. Microsoft SharePoint Online OneDrive Microsoft 365 Security Solutions

D. Azure Information Protection Microsoft 365 Compliance Center

Answer: A (LEAVE A REPLY)

NEW QUESTION: 89

Which of the following is a Microsoft 365 security solution?

SharePoint Online is a Microsoft 365 security solution.

Microsoft 365 Security Solutions is a Microsoft 365 security solution.

Microsoft 365 Security Solutions is a Microsoft 365 security solution.

Which of the following is a Microsoft 365 security solution?

A. Microsoft 365 Security Solutions

B. Microsoft 365 Security Solutions (DLP)

C. Microsoft 365 Security Solutions

D. Microsoft 365 Security Solutions

Answer: A (LEAVE A REPLY)

NEW QUESTION: 90

(contoso.com and fabrikam.com are Active Directory forests (AD DS) in the same organization.)

contoso.com and fabrikam.com are Active Directory forests (AD DS) in the same organization.

Microsoft 365 E5 is a Microsoft 365 security solution.

Microsoft 365 E5 is a Microsoft 365 security solution.

Which of the following is a Microsoft 365 security solution?

A. Microsoft Entra Connect Sync

B. Microsoft Entra Connect Sync

C. Microsoft Entra Connect Sync

D. Microsoft Entra Connect Sync (AD FS)

Answer: C (LEAVE A REPLY)

The correct answer is Microsoft Entra Connect Sync because it is the only Microsoft-supported solution that meets all of the stated requirements.

1. Support for multiple on-premises AD DS forests

Microsoft Entra Connect Sync is designed to synchronize identities from multiple on-premises Active Directory forests into a single Microsoft Entra tenant. Microsoft documentation explicitly states that when multiple forests are present, they can all be synchronized as long as they are reachable by the same Entra Connect server. A forest trust between contoso.com and fabrikam.com is a supported and common configuration.

2. Ability to sync only a subset of users

Microsoft Entra Connect Sync supports filtering and scoping at multiple levels (domain-based, OU-based, or attribute-based). Microsoft documentation lists pilot deployments and limited user synchronization as a primary use case, allowing administrators to synchronize only selected users from each forest.

3. Support for device objects and hybrid device scenarios

Microsoft Entra Connect Sync supports hybrid device identity , including Microsoft Entra hybrid joined devices. These devices are registered both in on-premises Active Directory and in Microsoft Entra ID, which is required for many Microsoft 365 and Conditional Access scenarios.

4. Device writeback support

Device writeback is a feature that allows device objects from Microsoft Entra ID to be written back into on- premises Active Directory. Microsoft documentation clearly identifies device writeback as a feature of Microsoft Entra Connect Sync .

Important documented behavior:

* Device writeback is supported when device objects and users are correctly located and configured in the same forest.

* Device writeback is not a feature of Cloud Sync or federation services.

Why the other options are incorrect

A). Microsoft Entra Cloud Sync

Cloud Sync is a lightweight provisioning agent and does not provide the full hybrid identity feature set required for this scenario. Microsoft documentation associates advanced device features and device writeback with Microsoft Entra Connect Sync, not Cloud Sync.

B). Microsoft Entra Domain Services

Microsoft Entra Domain Services is a managed domain service used to run legacy, domain-joined workloads in Azure. It does not synchronize on-premises forests into Microsoft Entra ID and is not a replacement for Entra Connect in hybrid identity scenarios.

D). Active Directory Federation Services (AD FS)

AD FS is an authentication and federation service. It does not synchronize users or devices to Microsoft Entra ID and does not support device writeback. Microsoft documentation positions AD FS as an authentication method, not a directory synchronization solution.

NEW QUESTION: 91

Microsoft 365 E5 □□□□ □□□□.

□□ □□ □□□ □□□ Retention1□□□ □□□ □□ □□□ □□□□.

Review your settings

Name [Edit](#)

Retention1

Description for admins [Edit](#)

Description for users [Edit](#)

File plan descriptors [Edit](#)

Reference Id:1

Business function/department Legal

Category: Compliance

Authority type: Legal

Retention [Edit](#)

7 years

Retain only

Based on when it was created



[Back](#) [Create this label](#) [Cancel](#)

Retention1은 어떤 용도로 사용되는지 설명하십시오.

Retention1은 어떤 용도로 사용되는지 설명하십시오.

Retention1은 어떤 용도로 사용되는지 설명하십시오?

A. Retention1은 데이터 백업을 위한 용도로 사용됩니다.

B. Retention1은 데이터 복구 용도로 사용됩니다.

C. Retention1은 데이터 백업/복구 용도로 사용됩니다.

D. Retention1은 CSV 형식으로 Retention1 데이터를 내보내줍니다.

Answer: (SHOW ANSWER)

Reference:

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

MS-102-KR은 어떤 용도로 사용되는지 설명하십시오. DumpTop은 MS-102-KR을 설명합니다! DumpTop은 MS-102-KR을 설명합니다, DumpTop MS-102-KR을 설명합니다. DumpTop MS-102-KR을 설명합니다. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 92

Group1은 Group2의 구성원인 Microsoft 365 E5 사용자입니다.

Group1은 Group2의 구성원인 Microsoft Entra ID 사용자입니다. Group1은 Group2의 구성원인 Microsoft Entra ID 사용자입니다.

* Group1은 Android용 Microsoft Entra ID용 MFA를 구성합니다.

* Group2는 Microsoft Exchange Online용 MFA를 구성합니다.

* Group1은 Group2의 구성원입니다.

Group1은 Group2의 구성원인 Microsoft 365 E5 사용자입니다?

정답: Group1은 Group2의 구성원입니다.

Answer Area



Group1: Conditional Access
Microsoft Entra ID Protection
Microsoft Entra Privileged Identity Management
Conditional Access
Per-user MFA
Microsoft Entra Security defaults

Group2: Conditional Access
Microsoft Entra ID Protection
Microsoft Entra Privileged Identity Management
Conditional Access
Per-user MFA
Microsoft Entra Security defaults

Answer:
Answer Area



Group1: Conditional Access
Microsoft Entra ID Protection
Microsoft Entra Privileged Identity Management
Conditional Access
Per-user MFA
Microsoft Entra Security defaults

Group2: Conditional Access
Microsoft Entra ID Protection
Microsoft Entra Privileged Identity Management
Conditional Access
Per-user MFA
Microsoft Entra Security defaults

Explanation:

Answer Area

Group1: Conditional Access

Group2: Conditional Access

NEW QUESTION: 93

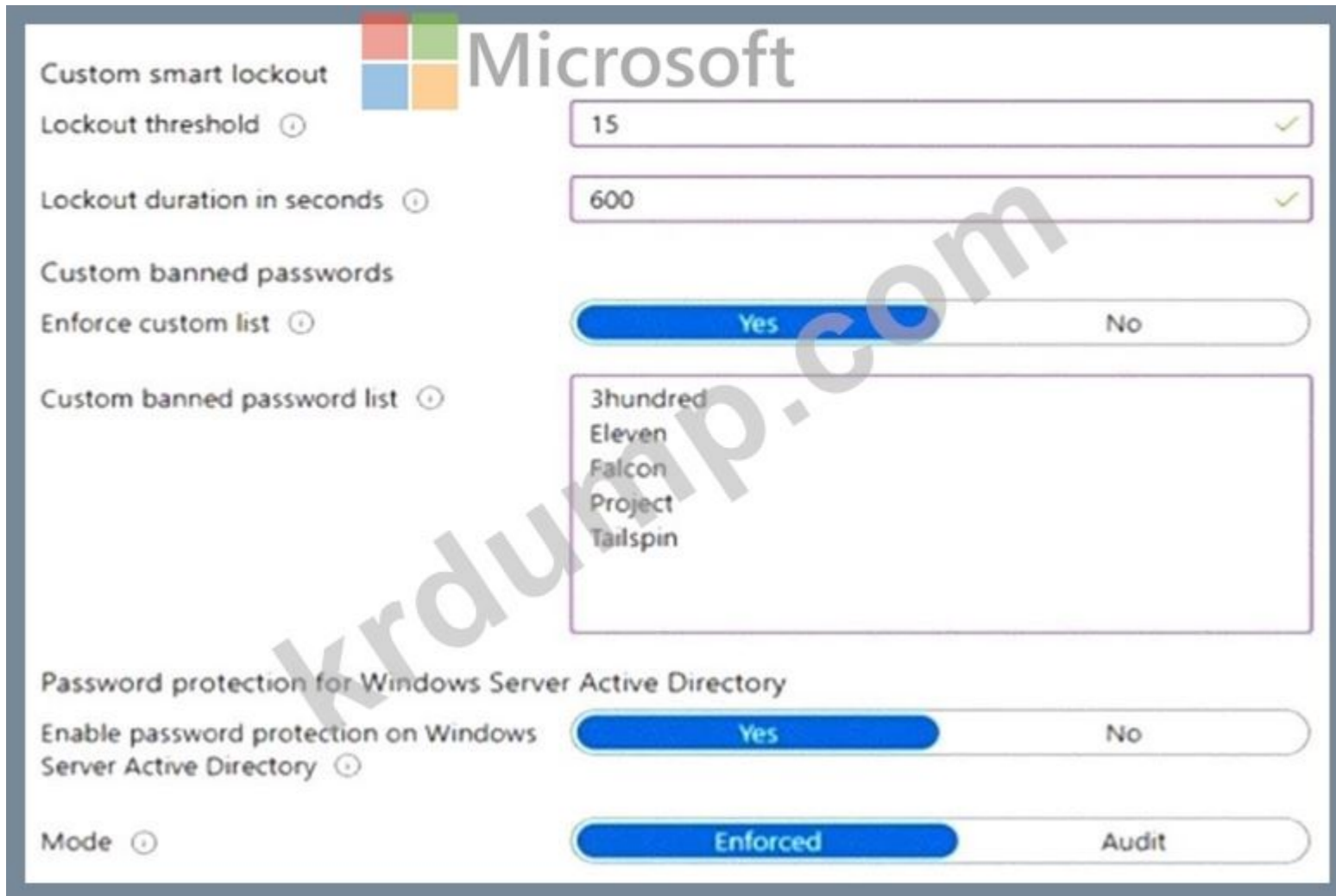
Microsoft 365 E5 users are assigned to the Microsoft Purview Compliance Protection group. Which Microsoft 365 E5 feature can be used to protect the data of these users?

- A. Microsoft Purview
- B. Microsoft Defender for Office 365
- C. Azure AD ID Protection
- D. Azure AD Conditional Access

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 94

User1 is a Microsoft 365 E5 user. Which Azure AD feature can be used to protect the data of this user?



User1 [redacted]

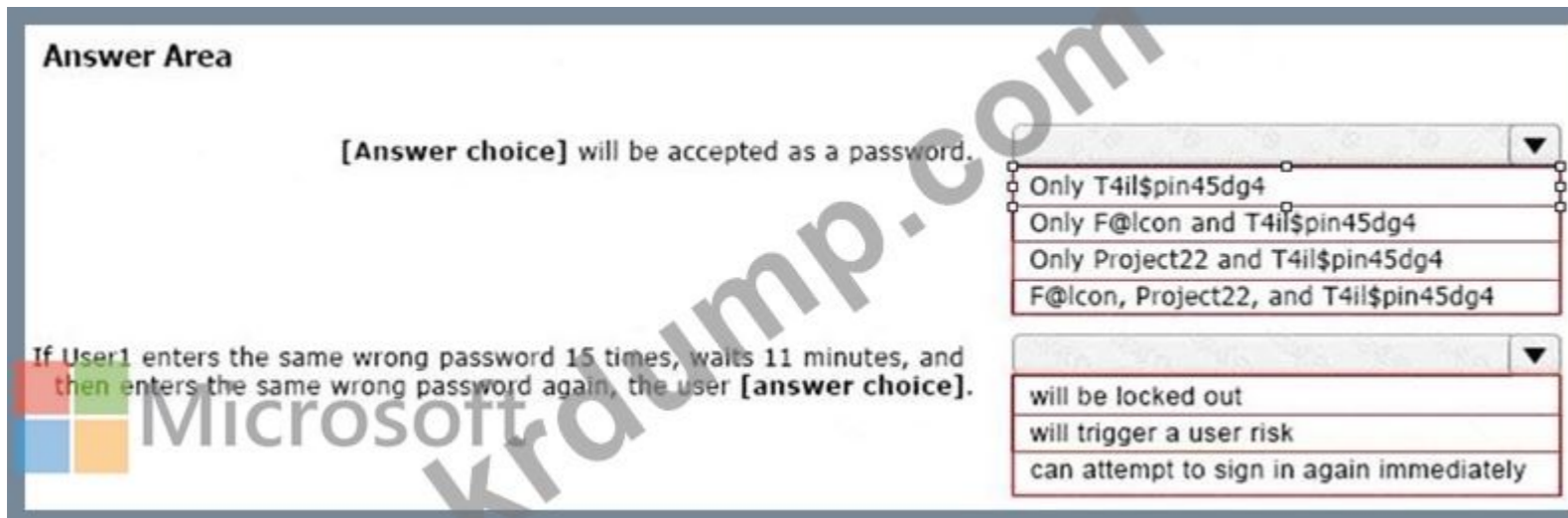
* [redacted]

* [redacted]22

* T4il\$pin45dg4

[redacted]

[redacted]: [redacted] 1[redacted].



Answer:

Answer Area

[Answer choice] will be accepted as a password.

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

Microsoft

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

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

Explanation:

Answer Area

[Answer choice] will be accepted as a password.

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

Microsoft

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

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

Box 1: Only T4il\$pin45dg4

Box 2: can attempt to sign in immediately

Note: Manage Azure AD smart lockout values

Based on your organizational requirements, you can customize the Azure AD smart lockout values.

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

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

Sign in to the Entra portal.

Search for and select Azure Active Directory, then select Security > Authentication methods > Password protection.

Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

The default is 10 for Azure Public tenants and 3 for Azure US Government tenants.

Set the Lockout duration in seconds, to the length in seconds of each lockout.

The default is 60 seconds (one minute).

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

Reference:

NEW QUESTION: 95

Scenario: You have an Azure AD tenant named Contoso. You have two users, User1 and User2, who are members of the Contoso.com domain. You need to ensure that User1 can sign in to Azure AD using their Contoso.com UPN suffix.


What should you do to ensure that User1 can sign in to Azure AD using their Contoso.com UPN suffix?

Options: A) Add the Contoso.com domain to the Azure AD tenant. B) Add the Contoso.com domain to the Active Directory forest. C) Add the Contoso.com domain to the Azure AD tenant and add User1 to the Contoso.com domain. D) Add the Contoso.com domain to the Active Directory forest and add User1 to the Contoso.com domain.

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

What should you do to ensure that User1 can sign in to Azure AD using their Contoso.com UPN suffix? (Select all that apply.)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning




This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN

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

User2 is user2@fabrikam.com. You need to ensure that User2 can sign in to Azure AD using their Contoso.com UPN suffix.

What should you do to ensure that User2 can sign in to Azure AD using their Contoso.com UPN suffix?

Options: A) Add the Contoso.com domain to the Azure AD tenant. B) Add the Contoso.com domain to the Active Directory forest. C) Add the Contoso.com domain to the Azure AD tenant and add User2 to the Contoso.com domain. D) Add the Contoso.com domain to the Active Directory forest and add User2 to the Contoso.com domain.

Which of the following is true?

A. The on-premises Active Directory domain is named contoso.com.

B. The on-premises Active Directory domain is named contoso.local.

Answer: (SHOW ANSWER)

The on-premises Active Directory domain is named contoso.com. You can enable users to sign on using a different UPN (different domain), by adding the domain to Microsoft 365 as a custom domain. Alternatively, you can configure the user account to use the existing domain (contoso.com).

NEW QUESTION: 96

Contoso has an on-premises Active Directory forest named contoso.com. The forest functional level is Windows Server 2008 R2.

Microsoft 365 is configured with the following settings:

• The domain is contoso.com.

• The domain is contoso.com.

• The domain is contoso.com.

• The domain is contoso.com.

A. Microsoft 365 is configured with the domain contoso.local.

B. contoso.com is configured as a DNS MX record for the domain.

C. Active Directory is configured with the domain contoso.com.

D. Active Directory is configured with the domain contoso.com and the UPN suffix is contoso.com.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 97

Microsoft 365 E5 is configured with the following settings:

* *.docx

* *.docx

* *.important.docx

Microsoft Defender Cloud Policy1 is configured with the following settings:

Files matching all of the following

Edit and preview results

File name

contains words

"Important" "File"

+ Add a filter

Policy1 is configured with the following settings:

A. ImportantFile.docx

B. File.docx, ImportantFile.docx, Fileimportant.docx

C. Fileimportant.docx

D. *.docx

E. ImportantFile.docx and Fileimportant.docx

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 98

contoso.com Azure AD

Name	Usage location	Membership
User1	United States	Group1, Group2
User2	Not set	Group2
User3	Not set	Group1
User4	Canada	Group1

Group1

Office 365 Enterprise E3

Office 365 E3

A. 3

B. 4

C. 2

D. 1

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 99

Windows 10 2004

Windows 10 2004

Windows 10 2004

A. Windows 10 2004

B. Windows 10 2004

C. Windows 10 2004

D. Windows 10 2004

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 100

contoso.com Azure AD Microsoft 365

contoso.com Azure AD Microsoft 365

contoso.com Azure AD Microsoft 365

A. Microsoft 365

B. Microsoft Entra

C. Azure AD Identity Protection

D. Microsoft Entra

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 101

Microsoft 365

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

AU1

Name	Role
Admin1	AU1\User Administrator
Admin2	Global Administrator

Answer Area



Statements

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

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Admin1 can reset the password of User1: Yes

Admin1 has the User Administrator role within AU1. User1 is a member of Group1, which is included in AU1 's dynamic membership rule.

Admin1 can reset the password of User2: No

User2 is a member of both Group1 and Group2. However, User2's job title contains " Executive, " which excludes them from AU1 's dynamic membership rule. Therefore, Admin1 cannot reset User2 's password.

Admin2 can reset the password of User3: Yes

Admin2 has the Global Administrator role, which grants the ability to reset passwords for any user within the organization, including User3.

NEW QUESTION: 102

Microsoft 365 E5 provides auditing solutions.

Microsoft Exchange Online provides auditing solutions for all Microsoft 365 services.

Which of the following is a Microsoft Purview auditing solution?

- A. Microsoft Purview Audit Solutions
- B. Microsoft 365 Audit Solutions
- C. Microsoft Exchange Online Audit Solutions
- D. Microsoft Exchange Online Audit Solutions

Answer: A (LEAVE A REPLY)

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

This capability provides visibility into the activities performed across your Microsoft 365 organization.

Note: Permissions alert policies

Example: Elevation of Exchange admin privilege

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

Reference:

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

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

NEW QUESTION: 103

Microsoft 365 E5 provides auditing solutions for all Microsoft 365 services. Which of the following is a Microsoft Purview auditing solution?

Microsoft 365 E5 provides auditing solutions for all Microsoft 365 services.

Which of the following is a Microsoft Purview auditing solution?

Microsoft Exchange Online provides auditing solutions for all Microsoft 365 services.

Which of the following is a Microsoft Purview auditing solution?

- A. Azure AD Connect
- B. Azure AD Connect
- C. Microsoft Exchange Online Audit Solutions
- D. Microsoft Exchange Online Audit Solutions

Answer: (SHOW ANSWER)

NEW QUESTION: 104

Endpoint Protection Microsoft Defender for Endpoint provides auditing solutions for all Microsoft 365 E5 services.

Microsoft Defender for Endpoint provides auditing solutions for all Microsoft 365 E5 services.

Which of the following is a Microsoft Purview auditing solution?

- A. Microsoft Exchange Online Audit Solutions
- B. Microsoft Exchange Online Audit Solutions
- C. Microsoft Exchange Online Audit Solutions

Answer: C (LEAVE A REPLY)

NEW QUESTION: 105

Scenario: A company has a Microsoft 365 E5 license. The company has a Microsoft Teams chat room named ChatRoom1. The chat room contains a document named Document1.docx. The document contains sensitive information. The document is shared with a user named User1. User1 is not a member of the chat room. User1 is able to view the document. The user is not a member of the chat room. The user is able to view the document.

What is the reason for this behavior?

Microsoft 365 E5 license allows it.

SecAdmin1 is a member of the chat room.

SecAdmin1 is a member of the Microsoft Teams, SharePoint, OneDrive, and Office 365 Advanced Threat Protection(ATP) group.

SecAdmin1 is a member of the Azure Active Directory group named SecAdmin1.

What is the reason for this behavior?

A. SecAdmin1 is a member of the chat room.

B. SecAdmin1 is a member of the Microsoft Teams, SharePoint, OneDrive, and Office 365 Advanced Threat Protection(ATP) group.

Answer: (SHOW ANSWER)

NEW QUESTION: 106

Scenario: A company has a Microsoft Defender for Office 365 license. The company has a Microsoft Teams chat room named ChatRoom1. The chat room contains a document named Document1.docx. The document contains sensitive information. The document is shared with a user named User1. User1 is not a member of the chat room. User1 is able to view the document. The user is not a member of the chat room. The user is able to view the document.

What is the reason for this behavior?

Microsoft 365 E5 license allows it.

A. SecAdmin1 is a member of the chat room.

B. SecAdmin1 is a member of the Microsoft Teams, SharePoint, OneDrive, and Office 365 Advanced Threat Protection(ATP) group.

C. SecAdmin1 is a member of the Azure Active Directory group named SecAdmin1.

D. SecAdmin1 is a member of the Microsoft Teams, SharePoint, OneDrive, and Office 365 Advanced Threat Protection(ATP) group.

Answer: D (LEAVE A REPLY)

Safe Attachments for SharePoint, OneDrive, and Microsoft Teams

In organizations with Microsoft Defender for Office 365, Safe Attachments for SharePoint, OneDrive, and Microsoft Teams provides an additional layer of protection against malware. After files are asynchronously scanned by the common virus detection engine in Microsoft 365, Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation). Safe Attachments for SharePoint, OneDrive, and Microsoft Teams also helps detect and block existing files that are identified as malicious in team sites and document libraries.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments-for-spo-odfb-teams-about>

MS-102-KR is a Microsoft 365 certification exam. DumpTop offers MS-102-KR dumps. MS-102-KR! DumpTop offers MS-102-KR dumps. DumpTop MS-102-KR dumps. DumpTop MS-102-KR dumps. DumpTop MS-102-KR dumps. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 107

Scenario: A company has an Azure ATP license. The company has a Microsoft Teams chat room named ChatRoom1. The chat room contains a document named Document1.docx. The document contains sensitive information. The document is shared with a user named User1. User1 is not a member of the chat room. User1 is able to view the document. The user is not a member of the chat room. The user is able to view the document.

A. 1

B. 2

C. 3

D. ☐☐ 4

E. ☐☐ 5

Answer: A (LEAVE A REPLY)

References:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning> However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

Topic 2, A. DatumCase Study:

Overview

Existing Environment

This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.

Current Infrastructure

A). Datum recently purchased a Microsoft 365 subscription.

All user files are migrated to Microsoft 365.

All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.

Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.

A). Datum uses and processes Personally Identifiable Information (PII).

Problem Statements

Requirements

A). Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.

Business Goals

A). Datum wants to be fully compliant with all the relevant data privacy laws in the regions where it operates.

A). Datum wants to minimize the cost of hardware and software whenever possible.

Technical Requirements

A). Datum identifies the following technical requirements:

Centrally perform log analysis for all offices.

Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.

Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.

Provide the users in the finance department with access to Service assurance information in Microsoft Office 365.

Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.

If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user ' s user account.

A security administrator requires a report that shows which Microsoft 365 users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.

Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

NEW QUESTION: 108

Microsoft 365

Name	Members
AU1	Group1, User2
AU2	Group2, User3, User4

Name	Members
Group1	User1
Group2	User2, User4

Name	Role	Scope
User1	None	Not applicable
User2	Password Administrator	AU1
User3	License Administrator	Organization
User4	None	Not applicable

Answer Area

Statements	Yes	No
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input type="radio"/>
User3 can assign licenses to User1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Statements

	Yes	No
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can assign licenses to User1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area



Statements

	Yes	No
User2 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can reset the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can assign licenses to User1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 109

contoso.com Microsoft Entra Microsoft 365 Windows 10 Microsoft 365. How can you ensure that all users can access Microsoft 365 services from their Windows 10 devices? (Select two.)

- A. Microsoft Entra Connect
- B. Microsoft Authenticate
- C. Microsoft Entra Connect
- D. Microsoft Entra Connect

Answer: B (LEAVE A REPLY)

NEW QUESTION: 110

Microsoft 365 Defender eDiscovery Manager US eDiscovery Manager. How can you ensure that all users can access Microsoft 365 services from their Windows 10 devices? (Select two.)

- A. Microsoft 365 Defender eDiscovery Manager
- B. Microsoft 365 Defender eDiscovery Manager
- C. Microsoft 365 Defender eDiscovery Manager
- D. Microsoft 365 Defender eDiscovery Manager

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 111

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □□ □□□ □□□ □

□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

Windows 10 □ □□□□ □□□□ □□□□.

□□□ Windows 10 □□□ □□□□ □□□.

□□ □□: □□ □□□□□ □□□ □□□ □□□□□.

A. □

B. □□□

Answer: B ([LEAVE A REPLY](#))

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

NEW QUESTION: 112

(□□□ 1,000□□ Windows □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.)

□□□ □□ □□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. Microsoft Intune □□ □□

B. Microsoft Purview □□

C. □□□□□□□ □□□ □□

D. Microsoft 365 □□ □□

Answer: C ([LEAVE A REPLY](#))

The correct answer is the Microsoft Defender portal .

Explanation:

* Exposure Score is a security metric provided by Microsoft Defender for Endpoint . It measures an organization's overall security posture by evaluating device configuration, vulnerabilities, and security controls across endpoints.

* Microsoft documentation defines Exposure Score as part of the Microsoft Defender Vulnerability Management experience, which is accessed through the Microsoft Defender portal .

* The Exposure Score helps administrators:

* Understand how vulnerable devices are across the organization

* Track improvements to security posture over time

* Prioritize remediation actions based on risk

* Microsoft explicitly states that Exposure Score is viewed and managed within the Microsoft Defender portal , which serves as the central dashboard for Defender for Endpoint, Defender for Office 365, and related security services.

Why the other options are incorrect

A). the Microsoft Intune admin center

Intune focuses on device management, compliance, and configuration profiles. While it provides device health and compliance reporting, it does not display the Defender Exposure Score.

B). the Microsoft Purview portal

Microsoft Purview is used for data governance, compliance, insider risk, and information protection. It has no functionality related to endpoint exposure scoring.

D). the Microsoft 365 admin center

The Microsoft 365 admin center is designed for tenant-wide administration such as users, licenses, and services. It does not provide detailed endpoint security metrics like Exposure Score.

NEW QUESTION: 113

Microsoft 365 E5 □□□ □□□□.

□□ □□□ □□ □□□ □□ □□□ □□□□□.

How do you want the alert to be triggered?

- Every time an activity matches the rule
- When the volume of matched activities reaches a threshold

More than or equal to activities

During the last minutes

 Microsoft
On ▾

- When the volume of matched activities becomes unusual

On ▾

□□ □□□ □□□□ □□□.

* □□□□□ □□□ □□ □□□□ □□□□ □ □□□ □□□□□?

* □□□□ □□□□ □□ □□□ □□□□□ □□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10

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

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Answer:

How many days it will take to establish the baseline:

- 1
- 5
- 7
- 10


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

- Alerts will be triggered.
- Alerts will not be triggered.
- Alerts will be triggered only after the process to establish the baseline has been running for one day.

Explanation:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.



To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

▼

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence


Answer:
Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.



▼

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence


Explanation:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable domains to protect
- Enable users to protect
- Phishing email threshold



To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

▼

- Add trusted senders and domains
- Enable intelligence for impersonation protection
- Enable spoof intelligence

Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

User impersonation protection prevents specific internal or external email addresses from being impersonated as message senders. For example, you receive an email message from the Vice President of your company asking you to send her some internal company information. Would you do it? Many people would send the reply without thinking.

You can use protected users to add internal and external sender email addresses to protect from impersonation. This list of senders that are protected from user impersonation is different from the list of recipients that the policy applies to (all recipients for the default policy; specific recipients as configured in the Users, groups, and domains setting in the Common policy settings section). When you add internal or external email addresses to the Users to protect list, messages from those senders are subject to impersonation protection checks. The message is checked for impersonation if the message is sent to a recipient that the policy applies to (all recipients for the default policy; Users, groups, and domains recipients in custom policies). If impersonation is detected in the sender ' s email address, the action for impersonated users is applied to the message.

Box 2: Add trusted senders and domains

Trusted senders and domains

Trusted senders and domain are exceptions to the impersonation protection settings. Messages from the specified senders and sender domains are never classified as impersonation-based attacks by the policy. In other words, the action for protected senders, protected domains, or mailbox intelligence protection aren ' t applied to these trusted senders or sender domains. The maximum limit for these lists is 1024 entries.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

NEW QUESTION: 116

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □□□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□□ □□□ □□□ □□ □□□ □□□□ □□□□.

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □□□ □□ □□□ □□□ □□□□.

SecAdmin1□ Microsoft Teams, SharePoint, OneDrive□ □□ Microsoft Defender for Office 365 □□ □ □□□ □□□ □ □□□ □□□□ □□□.

□□ □□: Microsoft 365 □□ □□□□ SecAdmin1□□ SharePoint □□□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 117

□□□

Microsoft 365 □□□ □□□□.

□□ □□□ □□ □□□ □□□□ □□□.

Microsoft Teams□ □□ □□ □□□

□□ Microsoft □□□ □□

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Teams daily active users:

- Microsoft Secure Score
- Adoption Score
- Service health
- Usage reports

Recent Microsoft service issues:

- Microsoft Secure Score
- Adoption Score
- Service health
- Usage reports

Answer:
Answer Area

Teams daily active users:

- Microsoft Secure Score
- Adoption Score
- Service health
- Usage reports

Recent Microsoft service issues:

- Microsoft Secure Score
- Adoption Score
- Service health
- Usage reports

Explanation:

Answer Area



Box 1: Usage reports

The daily active users in Microsoft Teams

Microsoft 365 Reports in the admin center - Microsoft Teams usage activity The brand-new Teams usage report gives you an overview of the usage activity in Teams, including the number of active users, channels and messages so you can quickly see how many users across your organization are using Teams to communicate and collaborate. It also includes other Teams specific activities, such as the number of active guests, meetings, and messages.

Box 2: Service Health

Recent Microsoft service issues

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

Reference:

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

<https://learn.microsoft.com/en-us/microsoft-365/enterprise/view-service-health>

NEW QUESTION: 118

□□ □□ □□□ □□□□ □□□ Microsoft 365 □□□ □□□□.

Name	Department	Job title
User1	IT engineering	Technician
User2	Engineering	Senior executive
User3	Finance	Manager

AU1□□□ □□□ □□ □□□ □□□ □□□ □□ AU1 □□ □□□ □□□ □□□□□.

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin1 can reset the password of User2.	<input type="radio"/>	<input checked="" type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 119

□□□

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.

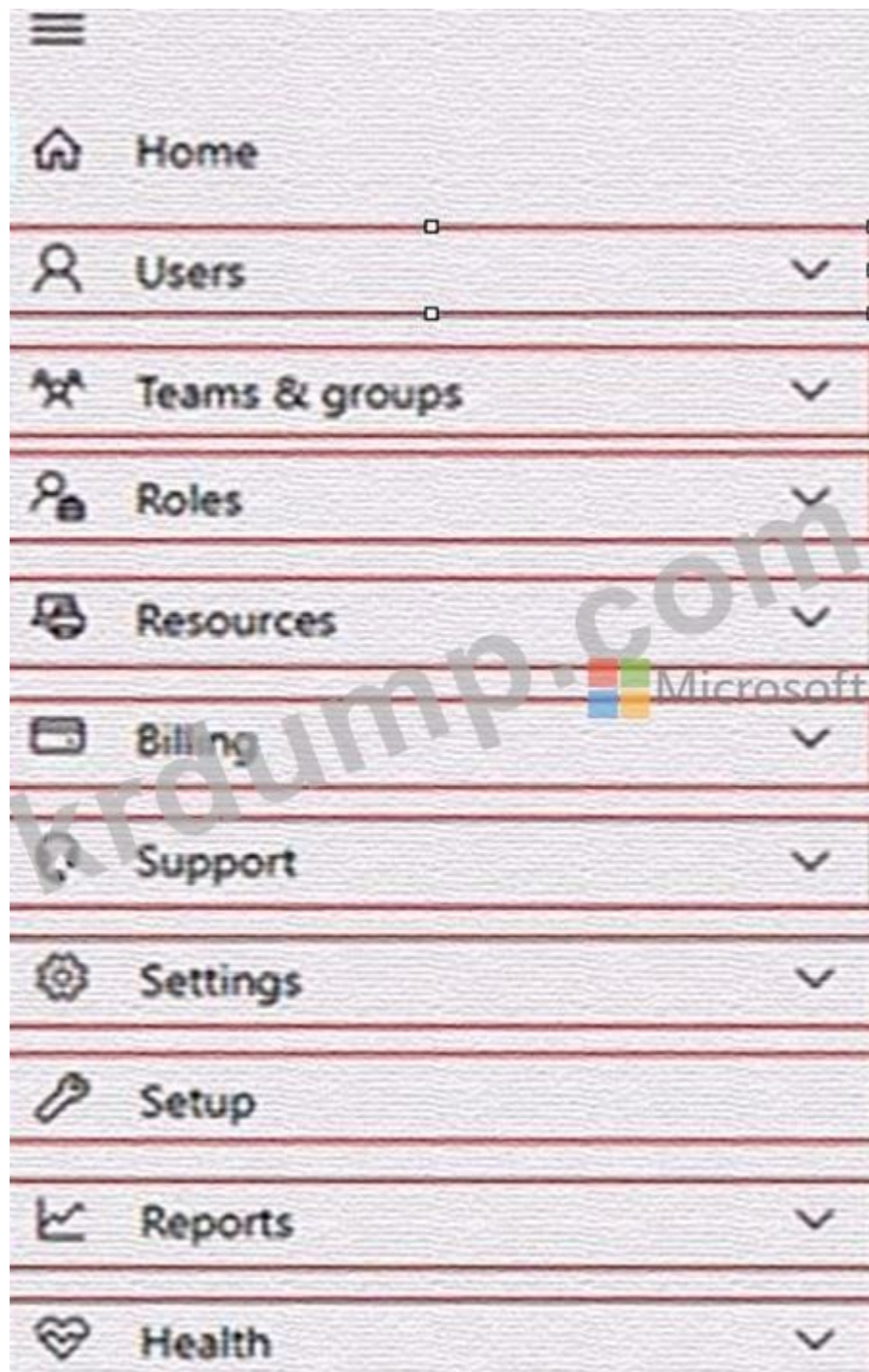
□□ □□□ □□□□ □□□.

□□□ □□ □□□ □□□□□.

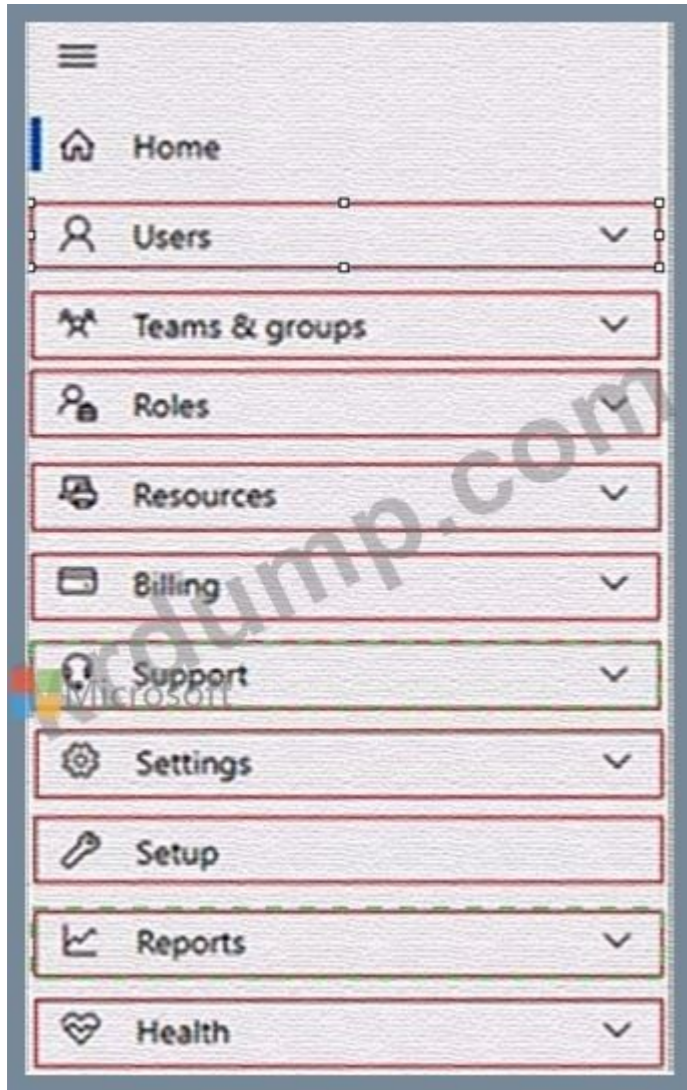
Microsoft□ □□□ □□□ □□□ □□□□.

Microsoft 365 □□ □□□□ □□ □ □□ □□□□ □□□□ □□□□ □□ □□□ □□□□□.

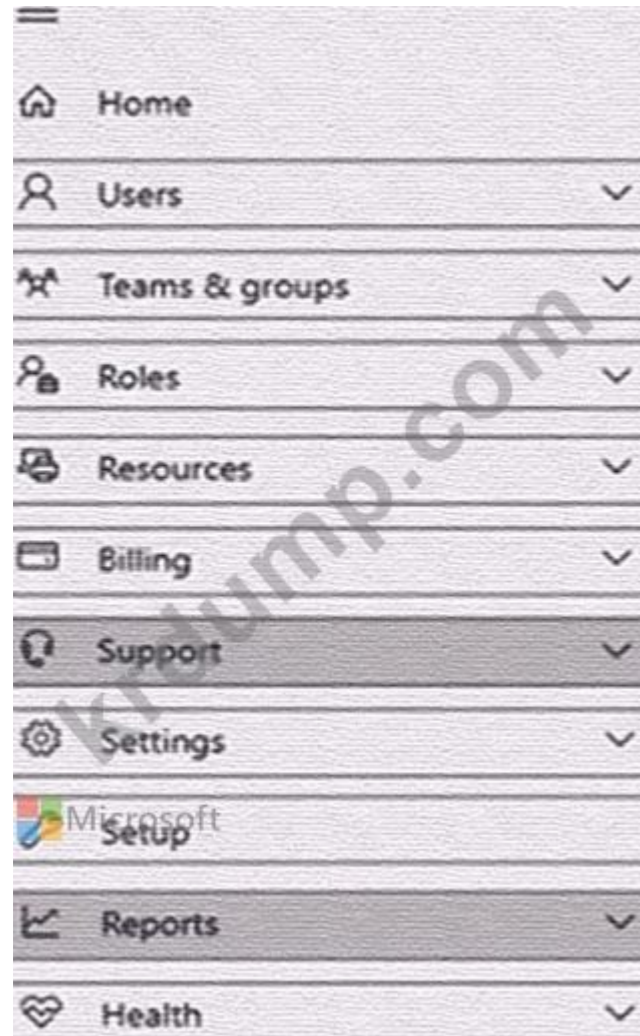
□□□□: □□ □□□ 1□□□□□.



Answer:



Explanation:



Box 1: Reports

View the Adoption Score of the company.

How to enable Adoption Score

To enable Adoption Score:

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

Box 2: Support

Create a new service request to Microsoft.

Sign in to Microsoft 365 with your Microsoft 365 admin account, and select Support > New service request.

If you 're in the admin center, select Support > New service request.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/admin/adoption/adoption-score>

<https://support.microsoft.com/en-us/topic/contact-microsoft-office-support-fd6bb40e-75b7-6f43-d6f9-c13d10850e77>

NEW QUESTION: 120

User1 is a Microsoft 365 E5 user. You need to ensure that User1 can view the company's Microsoft 365 E5 license usage report.

* Which PowerShell cmdlet should you run? (Select the correct answer.)

* Which cmdlet should you run? (Select the correct answer.)

User1 is a Microsoft 365 E5 user. You need to ensure that User1 can view the company's Microsoft 365 E5 license usage report.

Name	Phishing confidence level (PCL)
Mail1	Low
Mail2	Medium
Mail3	High
Mail4	Very high

Which mailboxes should be included in the investigation?

- A. Mail2, Mail3, Mail4
- B. Mail3, Mail4
- C. Mail1, Mail2, Mail3, Mail4
- D. Mail4

Answer: B (LEAVE A REPLY)

NEW QUESTION: 121

Azure AD Connect is installed on a server.

Windows 10 Pro is installed on a server with 1,000 users.

Microsoft 365 E3 is installed on a server.

Which Windows 10 Enterprise feature should be used to manage the server?

Which feature should be used?

- A. Microsoft Intune. Edition. Microsoft Endpoint Manager.
- B. Windows 10 Enterprise Upgrade. Microsoft SharePoint Online.
- C. Microsoft Endpoint Manager. Windows Autopilot.
- D. Azure Active Directory.

Answer: (SHOW ANSWER)

MS-102-KR questions and answers. DumpTop MS-102-KR! DumpTop MS-102-KR questions and answers, DumpTop MS-102-KR questions and answers. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 122

Microsoft Entra ID is installed on a server. Which Active Directory feature should be used to manage the server?



Allan Yoo is a user in your Active Directory. You are configuring Microsoft Entra Connect Sync. Microsoft 365 is installed on the computer. You are using the Microsoft Entra admin center. You are configuring the user account for Allan Yoo. The user account is Allan@adatum.com. The user account is located in the adatum.com domain. The user account is located in the adatum.com domain. The user account is located in the adatum.com domain.

Answer Area

Statements	Yes	No
From the Microsoft Entra admin center, you can reset the password of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Microsoft Entra admin center, you can configure the job title of Allan Yoo.	<input type="radio"/>	<input type="radio"/>
From the Microsoft Entra admin center, you can configure the usage location of Allan Yoo.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

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

Explanation:
Answer Area

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

NEW QUESTION: 123

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users. After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically. Fabrikam does NOT plan to implement identity federation. After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN. You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN. You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

- A. Password hash synchronization and SSO
- B. Password hash synchronization and SSO
- C. Password hash synchronization and SSO
- D. Password hash synchronization and SSO

Answer: (SHOW ANSWER)

Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users. After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically. Fabrikam does NOT plan to implement identity federation. After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN. You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN. You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.

Reference:

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

Topic 5, Litware, IrkLitware, Irk. is a consulting company that has a main office in Montreal and a branch office in Seattle?

Ltware collaborates with a third-party company named A. Datum Corporation.

The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.

Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Azure AD Premium P2 licenses.

The subscription contains a verified DNS domain named litware.com.

Azure AD Connect is installed and has the following configurations:

- * Password hash synchronization is enabled.
- * Synchronization is enabled for the LitwareAdmins OU only.

Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.

The Azure AD tenant has Security defaults enabled.

Litware identifies the following issues:

- * Admin1 cannot create conditional access policies.
- * Admin4 receives an error when attempting to use SSPR.
- * Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.

Litware plans to implement the following changes:

- * Implement Microsoft Intune.
- * Implement Microsoft Teams.
- * Implement Microsoft Defender for Office 365.
- * Ensure that users can install Office 365 apps on their device.
- * Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
- * Configure Azure AD Connect to sync the Montreal Users OU and the Seattle Users OU.

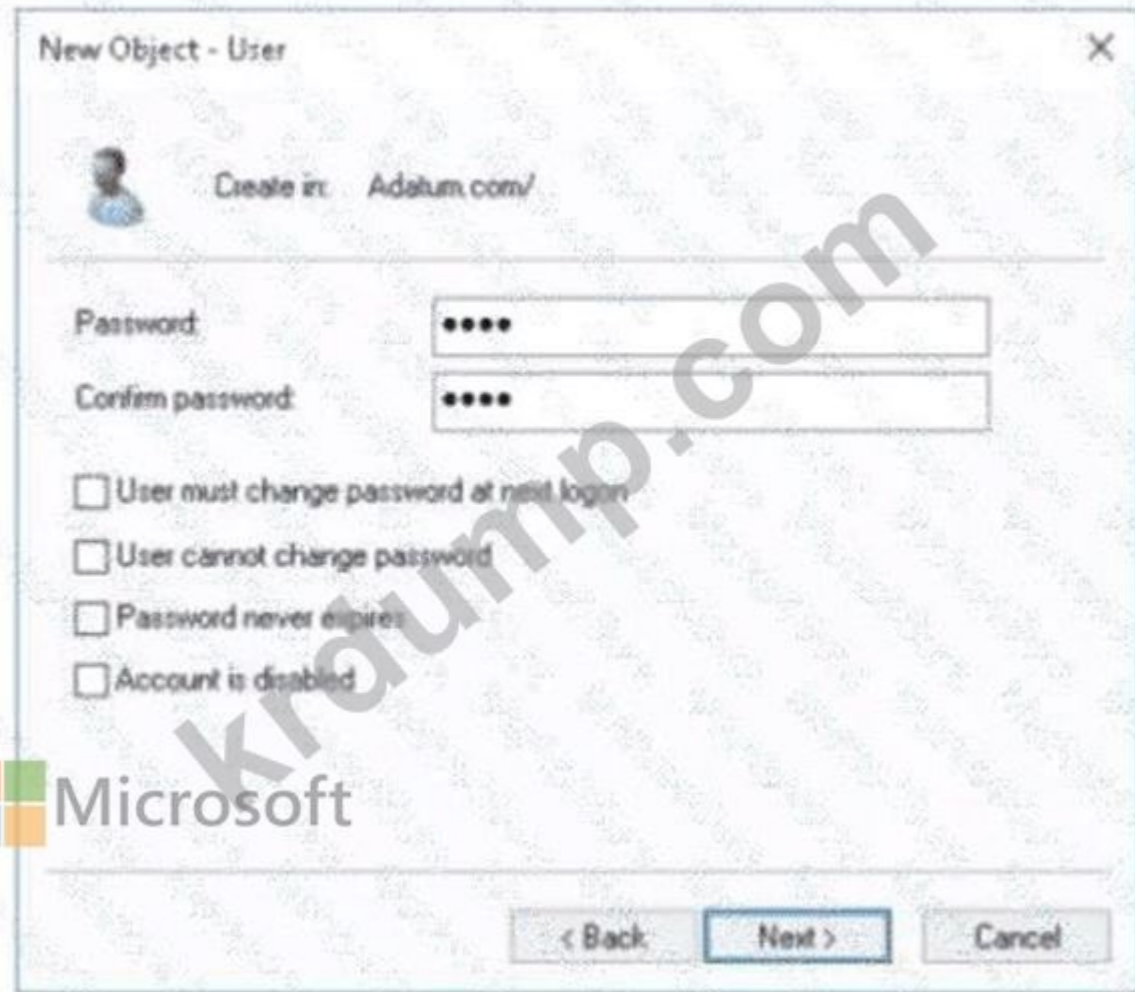
Litware identifies the following technical requirements:

- * Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
- * Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
- * Litware users must be able to invite A. Datum users to participate in the following activities:
 - o Join Microsoft Teams channels,
 - o Join Microsoft Teams chats,
 - o Access shared files.
- * Just in time access to critical administrative roles must be required.

- * Microsoft 365 incidents and advisories must be reviewed monthly.
- * Office 365 service status notifications must be sent to Admin2.
- * The principle of least privilege must be used.

NEW QUESTION: 124

An administrator is configuring a new user in Azure AD Connect Express. The user is named User1 and is located in the adatum.com Active Directory. The user's password is Pass123456.



The administrator is configuring a new user in Azure AD Connect Express. The user is named User1 and is located in the adatum.com Active Directory. The user's password is Pass123456.



Microsoft

Statements

Yes

No

User1 can sign in to Azure AD.

User1 can change the password immediately by using the My Apps portal.

From Azure AD, User1 must change the password every 90 days.

Answer:

Answer Area

Statements

Yes

No

User1 can sign in to Azure AD.

User1 can change the password immediately by using the My Apps portal.

From Azure AD, User1 must change the password every 90 days.

Explanation:

Answer Area

Statements

Yes

No

User1 can sign in to Azure AD.

User1 can change the password immediately by using the My Apps portal.

From Azure AD, User1 must change the password every 90 days.

NEW QUESTION: 125

□□□□□ □□□□□□ Active Directory □□□□□ Microsoft Endpoint Configuration Manager □□□□□ □□□□□ □□□□□.

- Group1
 - Group2: Group1
 - * Group3:
 - * Group4: Group1, Group2
 - * Group5: Group1
- Group1 can set Enable policy for Policy1 to On.
 Group2 can set Enable policy for Policy1 to Off.
 Group3: Group1

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

Answer:

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

Explanation:

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

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

Conditional Access policies can be enabled in report-only mode.

During sign-in, policies in report-only mode are evaluated but not enforced.

Results are logged in the Conditional Access and Report-only tabs of the Sign-in log details.

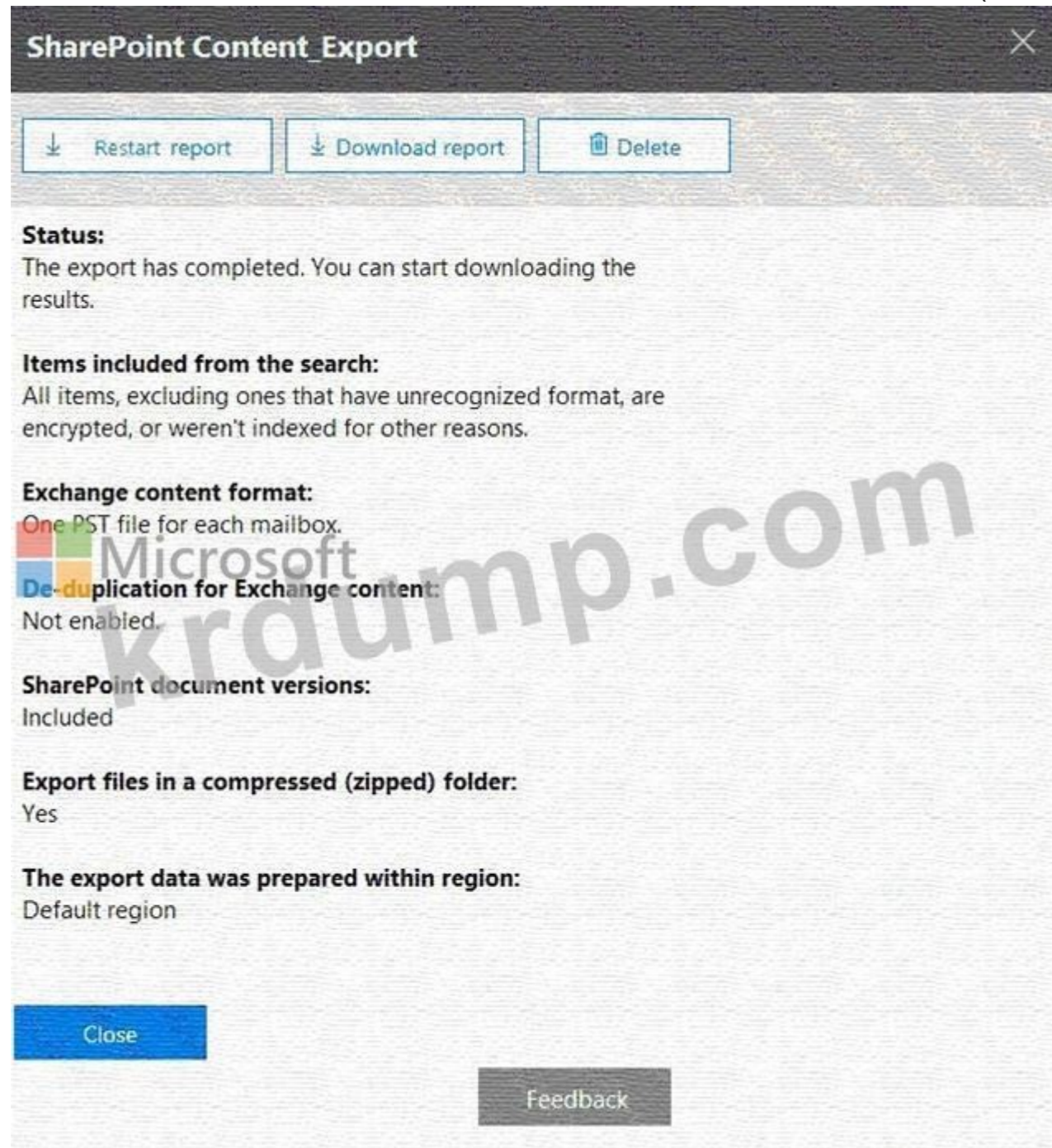
Customers with an Azure Monitor subscription can monitor the impact of their Conditional Access policies using the Conditional Access insights workbook.

Reference:

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

NEW QUESTION: 127

□□ □□ □□ □□ □□□□ □□□ □□□ □□ □□□ □□□□□ □□□□□. (□□ □□ □□□□□.)



□□□□ □□□□ □□□ □□□□□?

- A. 10MB XLSX □□
- B. 5MB MP3 □□
- C. 5KB RTF □□
- D. 80MB PPTX □□

Answer: B (LEAVE A REPLY)

Unrecognized file formats are excluded from the search.

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

These types of files are considered to be unsupported file types.

Reference:

https://docs.microsoft.com/en-us/microsoft-365/compliance/partially-indexed-items-in-content-search?view=o365-worldwide
https://docs.microsoft.com/en-us/office365/securitycompliance/export-a-content-search-report

NEW QUESTION: 128

Microsoft 365 □□□ □□□□.

Microsoft 365 □□ □□□□ □□ □□□ □□ Microsoft 365 □ □□ □□□□ □□□.

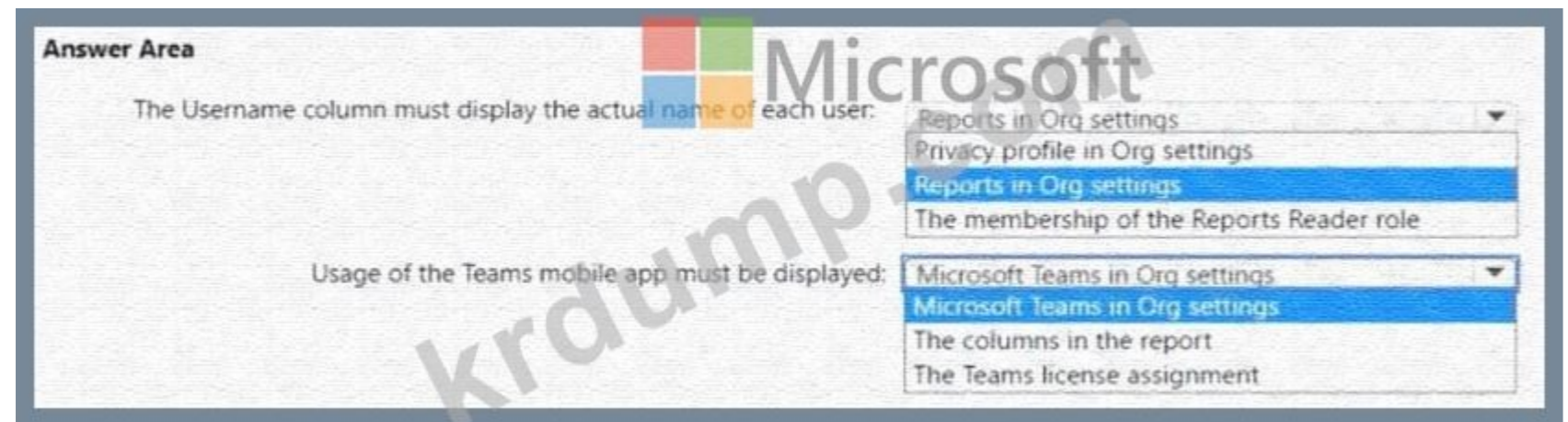


□□□□ □□ □□ □□□ □□□□□ □□□□ □□□.

* □□□ □□ □□□ □ □□□□ □□ □□□ □□□□□ □□□.

* Microsoft Teams □□□ □□ □□□□ □□□□□ □□□.

□ □□ □□□ □□ □□□ □□□□ □□□□ □□□ □□□ □□□ □□□□□□□□. □□: □ □□□ 1□□□□.



Answer:

Answer Area

The Username column must display the actual name of each user:

- Reports in Org settings
- Privacy profile in Org settings
- Reports in Org settings
- The membership of the Reports Reader role

Usage of the Teams mobile app must be displayed:



- Microsoft Teams in Org settings
- Microsoft Teams in Org settings
- The columns in the report
- The Teams license assignment

Explanation:

Answer Area

The Username column must display the actual name of each user:



Reports in Org settings

Usage of the Teams mobile app must be displayed:

Microsoft Teams in Org settings

NEW QUESTION: 129

□□□ □□□□ Microsoft E5 □□□□ □□□□.
□□□ ISO/IEC 27001:2013 □□□ □□ □□□ □□□□ □□□.
□□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?

- A. □□ □□ □□
- B. □□ □□□□
- C. □□□□□□ □□□
- D. □□□ □□ □□(DSR)

Answer: ([SHOW ANSWER](#))

Reference:

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

NEW QUESTION: 130

□□ □□ □□□ □□□□ □□□ Microsoft Entra□ □□□□□ □□□ □□□□.

Name	Description
User1	On-premises directory synchronization service account
User2	Contributor for Microsoft Entra Connect Health
User3	Application Administrator in Microsoft Entra ID

□□ □□□ □□ □ □□ □□□□ □□□□ □□□.

* Microsoft Entra Connect Health □□ □□□ □□□ □□□□□.

* Microsoft Entra Connect Health □□□ □□□□□.

□ □□□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

View sync errors in Microsoft Entra Connect Health:

User2 ▼
User1
User2
User3

Configure Microsoft Entra Connect Health settings:

User1 ▼
User1
User2
User3




Answer:
Answer Area

View sync errors in Microsoft Entra Connect Health:

User2 ▼
User1
User2
User3

Configure Microsoft Entra Connect Health settings:

User1 ▼
User1
User2
User3



Explanation:

Answer Area



View sync errors in Microsoft Entra Connect Health:

Configure Microsoft Entra Connect Health settings:

NEW QUESTION: 131

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

□□□□ □□ □ □□ □□□ Android □□□ □□ □□□□ □□□□ □□□□□□□□. □□ □□□ □□ □□□ □□ □□□□ □□ □□□□ Microsoft Exchange Online □□□□ □□□□ □ □□□□.


□□□ □□ □□□ □□□□ □□□ □□□□ □□ □ □□ □□□□ □□□□ □□□.

□ □□ □□□ □□ □□□□ □□□ □□□□ □□□? □□□□ □□□ □□ □□□ □□□ □□□□□□□□. □ □□ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□ □ □□□□□□ □□□ □□□□□□ □ □□ □□□□.

□□□□: □□ □□□ 1□□□□□.

- Solutions**
- An app configuration policy
 - An app protection policy
 - A compliance policy
 - A configuration profile

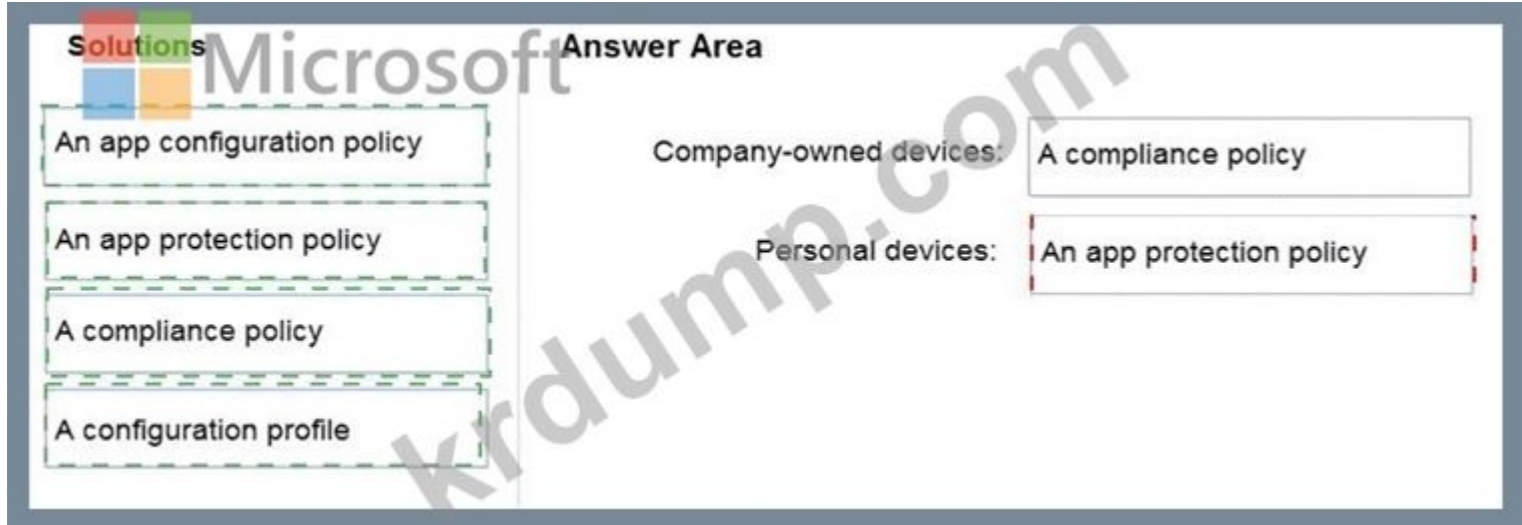
Answer Area



Company-owned devices:

Personal devices:

Answer:



Solutions

- An app configuration policy
- An app protection policy
- A compliance policy
- A configuration profile

Answer Area

Company-owned devices:

Personal devices:

Explanation:

Company-owned devices: A compliance policy

Personal devices: An app protection policy

NEW QUESTION: 132

Microsoft 365 E5 □□□ □□ Endpoint Defender for Endpoint□ □□□□ □□□□. Endpoint Defender for Endpoint□ □□ □□ □□□ □□□□□ □□□□ □□□□. Defender for Endpoint□ □□□□ Device1□□□□ □□□ □□□□. Device1□ □□ □□□□ □□ □ □□□ □□□ □□□□ □□□□ □□□.

- A. □□□□ □□□ □□□□□□.
- B. □□ □□□ □□□□□.
- C. □□□ □□ □□□ □□□□□.
- D. □□1□ □□□□□.

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 133

Microsoft Intune□ □□□ Android □□ 200□□ □□□ Microsoft 365 E5 □□□ □□□□. □□ Microsoft □□ □□□□ □□ □□ □□□□□ □□□□ Policy!□□ □□□ Android □ □□ □□□ □□□□. Policy!□□ □□ □□ □□□ □□ □□ □□□ □□ □□□ □□□□.

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

- Microsoft SharePoint Online
- OneDrive
- local storage
- Microsoft SharePoint Online
- Microsoft SharePoint Online and OneDrive

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

- any app
- any app
- only managed apps
- only unmanaged apps

Explanation:

Answer Area

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

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

NEW QUESTION: 134

Microsoft Defender for Microsoft 365 E5 scans all files in the organization's OneDrive for Business (ODfB) files. The scan is performed on a daily basis. How long does it take to scan all files in the organization's ODfB files?

- A. 24 hours
- B. 48 hours
- C. 72 hours
- D. 96 hours

Answer: B (LEAVE A REPLY)

NEW QUESTION: 135

Microsoft Defender for Endpoint is installed on three devices. Which device will be scanned by Defender Update?

Name	Platform
Device1	Windows 11
Device2	Linux
Device3	MacOS

Defender Update scans all files in the organization's OneDrive for Business (ODfB) files. The scan is performed on a daily basis. How long does it take to scan all files in the organization's ODfB files?

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

Answer: C (LEAVE A REPLY)

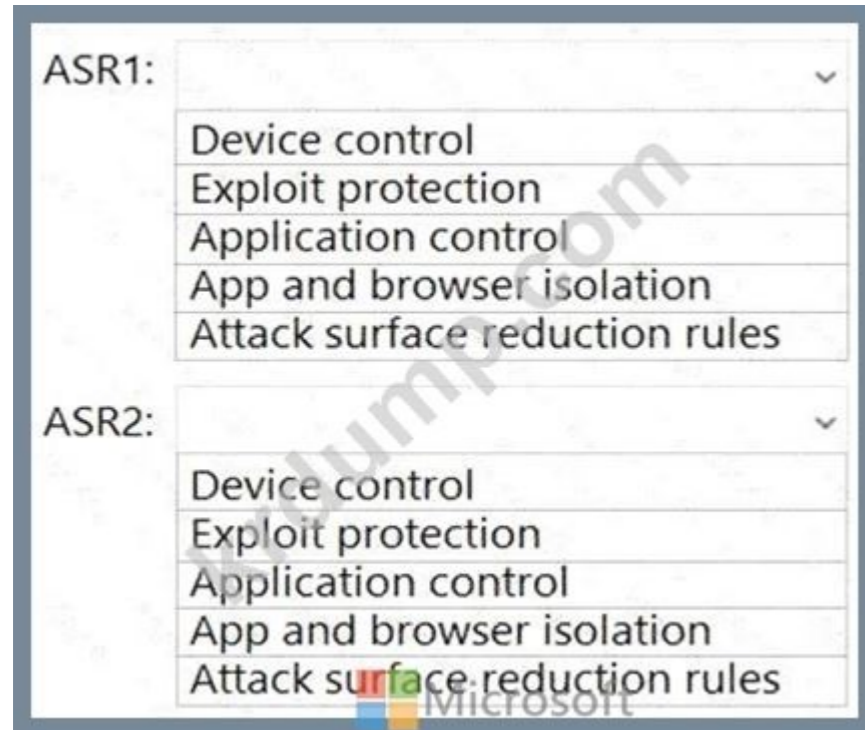
NEW QUESTION: 136

100% Windows 10 % % % % Microsoft 365 % % % % . % % % % Microsoft Endpoint Manager % % % % % % % % .

ASR1 % ASR2 % % % % % % % % (ASR) % % % % % % % % . ASR1 % Microsoft Defender Application Guard % % % % % % % % . ASR2 % Microsoft Defender SmartScreen % % % % % % % % % % .

% % % % % % ASR % % % % % % % % ? % .


% % % % : % % % % 1 % % % % .



Answer:



Can add apps to the private store:



Microsoft

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

Can assign apps from Microsoft Store for Business:

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

Answer:

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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



Explanation:

Can add apps to the private store:

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

Can assign apps from Microsoft Store for Business:

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



Reference:

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

<https://docs.microsoft.com/en-us/education/windows/education-scenarios-store-for-business#basic-purchaser-role>

NEW QUESTION: 138

Microsoft 365 E5.

Name	Member of	Multi-Factor Auth Status
User1	Group1	Disabled
User2	Group1, Group2	Enabled
User3	Group2	Disabled

Microsoft Entra ID.

* :

* : Group1

* : Group2

* : Microsoft Entra ID

* :

Microsoft 365 E5.

* : Policy1

* :

* : Group1

* ; 1

* : 1 1 1 1

* . 1

Microsoft 365 E5. Microsoft Entra ID.

Microsoft 365 E5.

Answer Area

Statements	Yes	No
User1 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User3 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 will be required to register for MFA on the next sign-in.	<input checked="" type="radio"/>	<input type="radio"/>
User2 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be required to register for MFA on the next sign-in.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

User1 will be required to register for MFA on the next sign-in: Yes

User1 is a member of Group1, which is included in the MFA registration policy. Since User1 is not excluded, they will be required to register for MFA on the next sign-in.

User2 will be required to register for MFA on the next sign-in: No

User2 is a member of both Group1 and Group2. Since Group2 is excluded from the MFA registration policy, User2 will not be required to register for MFA.

User3 will be required to register for MFA on the next sign-in: No

User3 is a member of Group2, which is excluded from the MFA registration policy. Therefore, User3 will not be required to register for MFA.

NEW QUESTION: 139

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

□ □□□□ Microsoft Authenticator □□ □□□ Android □□□ □□□ □□□, □□□ □□□□ □□□□□□.

□□ □□□□ □□□ □□ □□□ □□□ □□□ □□□□□.

* □□ : Policy1

* □□

o □□□ □ □□: Group1, Group2

o □□□□ □ □□ □□: □□ □□□□ □

* □□ □□

o □□ □□ □□ □□ □□ □□

* □□ □□□: □□

□□□ □□ Microsoft Authenticator □□□□ Enable □ Target □□□ □□□ □□□ □□ □□□□□. (□□ □□ □□□□□.)

Microsoft Authenticator settings



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

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

Enable and Target Configure

Enable

Microsoft
Include Exclude
Target All users Select groups

Add groups

Name	Type	Registration	Authentication mode	
Group1	Group	Optional	Passwordless	X
Group2	Group	Optional	Passwordless	X

00 0 000 00 000 000000 00 000000. 000 000 0000 000000.
0000: 00 000 100000.

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
User1 can sign in by using number matching in the Microsoft Authenticator app.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in by using a username and password.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can sign in by using number matching in the Microsoft Authenticator app.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 140

□□□ □□□□ □□ □□ □□ □□□□ □□□ comoso.onmicrosoft.com□□□ Azure AD □□□□ □□□□.

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

□□ □□ □□ □□ □ □□ □□□ □□□ □□□.

* User4 □ □□□□ □□□□□.

* User4 □ □□ □ □ □ □□□□.

□ □□ □ □ □ □□□ □□□ □□□? □□□□ □ □ □□□ □□ □□ □□□□.

□□□□: □ □ □□ 1□□□□.

Answer Area



Reset the password of User4:

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

Modify the value for the manager attribute of User4:

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

Answer:

Answer Area



Reset the password of User4:

- User1 and User3 only
- User1 only
- User2 only
- User1 and User2 only
- User1 and User3 only**
- User1, User2, and User3

Modify the value for the manager attribute of User4:

- User3 only
- User2 only
- User3 only**
- User1 and User3 only
- User2 and User3 only
- User1, User2, and User3

Explanation:

Answer Area

Reset the password of User4: User1 and User3 only

Modify the value for the manager attribute of User4: User3 only



NEW QUESTION: 141

Microsoft 365

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

Azure AD Connect

AD DS

AD DS

Active Directory AD DS Azure AD

AD DS

A. AD DS

- B. □□1 □□□
- C. User1□ User2□
- D. User1, User2, User3

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 142

□□□ 5□ □□□ □□□□ □□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□.
□ □□□□ □□ □□□□ □□□□□.
Microsoft Intune□ □□□ □□□□□.
□□ □□ □□□ □□□□ Intune□ □□□□ □□□□ □□□□ □□□□ □□□□.
□□ □□□□ □□□ □□□□ □□ □□□□ □□□ □ □□□ □□□.
□□ □□□□ □□ □□□□ □□□ □□□□ □□ □□□□ □□□.
□□□ □□□ □□□□□ □□□.
□□□□□ □□□ □□□□ □□□?

- A. □□ □□□□
- B. □□ □□
- C. □□ □□□
- D. □□□ □□□ □□

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 143

contoso.com□□□□ Azure AD □□□□ □□□□ Microsoft 365 □□□□ □□□□. □□□□□□ User1□□□□ □□□□ □□□□ □□□□.
Azure AD Identity Protection□ □□□□□□□.
User1□ Azure AD Identity Protection□□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□ □□□.
□□ □□□ User1□ □□□□ □□□?

- A. □□ □□
- B. □□□ □□□
- C. □□□
- D. □□□ □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 144

□□□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□□ □□□ Microsoft Defender for Endpoint□ □□□□□□□.
Microsoft Defender □□□□ □□ □□□□□ □□□ □□□ '□□□□ □□'□ □□□ □□ □□□□□ □□ □ □□□□□.
□□□□ □□□ □□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□, □□□□ □□ □□□□□ □□□ □□□ □ □□□ □□□.

Microsoft Defender □□□□ □□□ □□□□ □□□□?

- A. □□□□ □□ □□
- B. □□ □□ □□
- C. □□ □□
- D. □□ □□

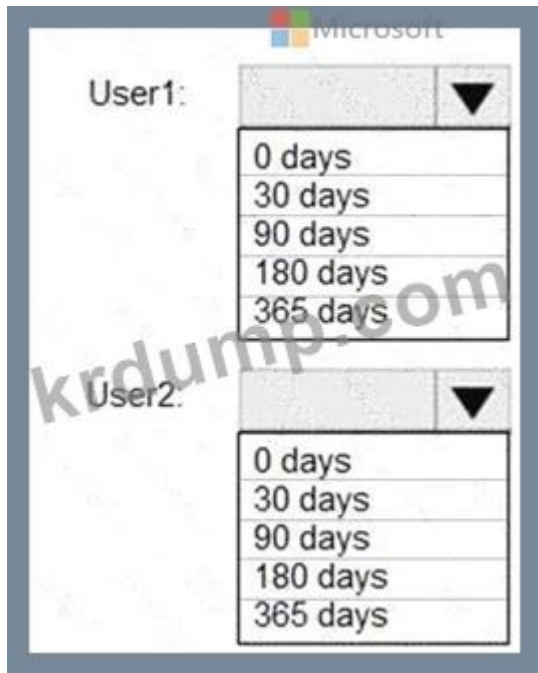
Answer: ([SHOW ANSWER](#))

NEW QUESTION: 145

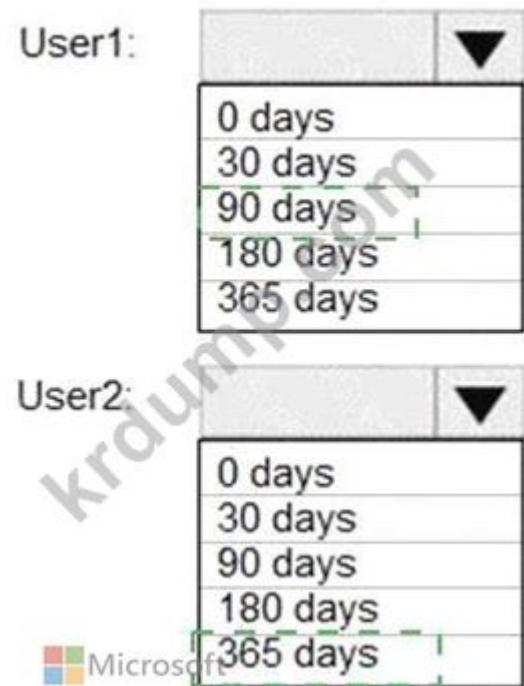
Admin1 □ Admin2 □□ □ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

□□ □□□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□ □□ □□□ □□ □□□□.

□□□ □□□ □□ □□ □□□ □□□□. (□□ □□ □□□□□.)



Answer:



Explanation:

Create retention label



Microsoft

Review and finish

Name

Name
6Months
[Edit](#)

Retention settings

Retention period
6 months
[Edit](#)

Retention action

Retain and Delete
[Edit](#)

Based on

Based on when it was created
[Edit](#)



[Back](#)

[Create label](#)

[Cancel](#)

Label Policy □□□ □□□ □□ □□□ □□□ □□□□. (Label Policy □□ □□□□□.)

- Name
- Info to label
- Create content query
- Scope
- Label
- Finish

Apply label to content matching this query

Conditions

ProjectX

+ Add condition



Cancel

□□ □□□ □□ □□ □□□□□□.

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

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

Answer Area



Microsoft
Statements

Any sent email message that contains the word ProjectX will be deleted immediately.

Yes

No

Any sent email message that contains the word ProjectX will be retained for six months.

Users are required to manually apply a label to email messages that contain the word ProjectX.

Answer:

Answer Area



Microsoft
Statements

Any sent email message that contains the word ProjectX will be deleted immediately.

Yes

No

Any sent email message that contains the word ProjectX will be retained for six months.

Users are required to manually apply a label to email messages that contain the word ProjectX.

Explanation:

Answer Area	Statements	Yes	No
	Any sent email message that contains the word ProjectX will be deleted immediately.	<input type="radio"/>	<input checked="" type="radio"/>
	Any sent email message that contains the word ProjectX will be retained for six months.	<input checked="" type="radio"/>	<input type="radio"/>
	Users are required to manually apply a label to email messages that contain the word ProjectX.	<input type="radio"/>	<input checked="" type="radio"/>

Box 1: No

Box 2: Yes

Box 3: No

Reference:

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

NEW QUESTION: 148

Microsoft 365 E5 □□□□ □□□□.

□□□□□ Microsoft Office 365 □□ □□□ □□□□ □□□ □□□□□ □□□ □□□□ □□□.

□□□ □□□□□ □□□ □□□□ □□□?

- A. Microsoft 365 □□ □□
- B. Microsoft Purview □□ □□ □□
- C. Microsoft Apps □□ □□
- D. □□□□ □ □□□ Microsoft Defender

Answer: D (LEAVE A REPLY)

NEW QUESTION: 149

Microsoft Store for Business□ □□□□ □□ User1□□□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□. User1□ Microsoft Store for Business□□ □□ □□□ □□□ □ □□□ □□□□ □□□.

* □□□□□ □□□□□ □□□□□.

* Microsoft Store□□ □□ □□□□□.

* □□ □□□ □□ □□ □□□ □□□ □□□□□.

□□□□ □□ □□□ □□□ □□□□ □□□.

User1□□ □□ Microsoft Store for Business □□□ □□□□ □□□?

- A. □□□□□
- B. Device Guard □□□
- C. □□□
- D. □□□

Answer: (SHOW ANSWER)

Reference:

<https://docs.microsoft.com/en-us/microsoft-store/microsoft-store-for-business-overview>

NEW QUESTION: 150

□□ □□ □□□ □□□ □□□ Microsoft 365 □□□□ □□□□.

Name	Type
Group1	Microsoft 365
Group2	Distribution
Group3	Mail-enabled security
Group4	Security

Compliance1 □□□ □□□ □□ □□□ □□ □□□□□.

□□ □□ □□□ □□□□ □□□ □□□□ □□□.

* □□□ □□ □□□□ Compliance1 □ □□□ □ □□□□.

* Compliance1 □ □□ □□

□□□□□ □□ □□□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Answer:

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Explanation:

Can be added to Compliance1 as recipients of noncompliance notifications:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Can be assigned to Compliance1:

- Group1 and Group4 only
- Group3 and Group4 only
- Group1, Group2 and Group3 only
- Group1, Group3, and Group4 only
- Group1, Group2, Group3, and Group4

Reference:

<https://www.itpromentor.com/devices-or-users-when-to-target-which-policy-type-in-microsoft-endpoint-manager-intune/>

NEW QUESTION: 151

Office 365 Microsoft Defender Microsoft 365

Microsoft Defender for Office 365


Microsoft Defender for Office 365

Microsoft Defender for Office 365

Microsoft Defender for Office 365 is a cloud-based security solution that provides protection for Microsoft 365 users and their data. It includes features such as anti-phishing, anti-spam, and anti-malware protection. Microsoft Defender for Office 365 is available as a standalone product or as part of the Microsoft 365 E5 license.

Microsoft Defender for Office 365 is available as a standalone product or as part of the Microsoft 365 E5 license.

Microsoft Defender for Office 365 is available as a standalone product or as part of the Microsoft 365 E5 license.

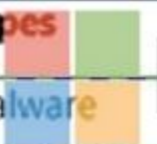
Policy Types 

Answer Area

Customize the common attachments filter:

Enable impersonation protection for sender domains:

Answer:


Policy Types 

Answer Area

Customize the common attachments filter:

Enable impersonation protection for sender domains:

Explanation:

Policy Types 

Answer Area

Customize the common attachments filter:

Enable impersonation protection for sender domains:

Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

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

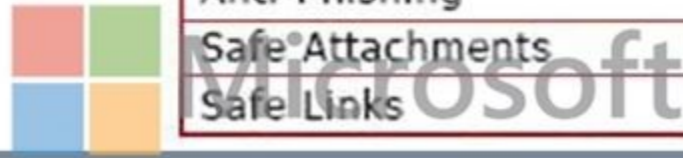
Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links



Answer:

Answer Area

Opening files in SharePoint that contain malicious content:

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

▼
Anti-spam
Anti-Phishing
Safe Attachments
Safe Links

Impersonation and spoofing attacks in email messages:

Explanation:

□□: □□□ 1□□□□.

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	<input type="radio"/>	<input type="radio"/>
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	<input type="radio"/>	<input type="radio"/>
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Statements	Yes	No
Defender for Endpoint blocks access to IP address 20.30.40.50 from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
Defender for Endpoint blocks access to IP address 2.23.10.15 from Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
Defender for Endpoint blocks access to IP address 131.107.10.50 from Device3.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 157

□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

□□ □□□□ □□ □□□ Microsoft Office□ □□□□□□.

* □□□ Microsoft 365 □

* □□ Office

* □□□ 2016

* □□□ 2019

□□ □□□□□ □□□ □□ Office □□ □□□ □□□□□□.

* .docx

* .xlsx

* .□□

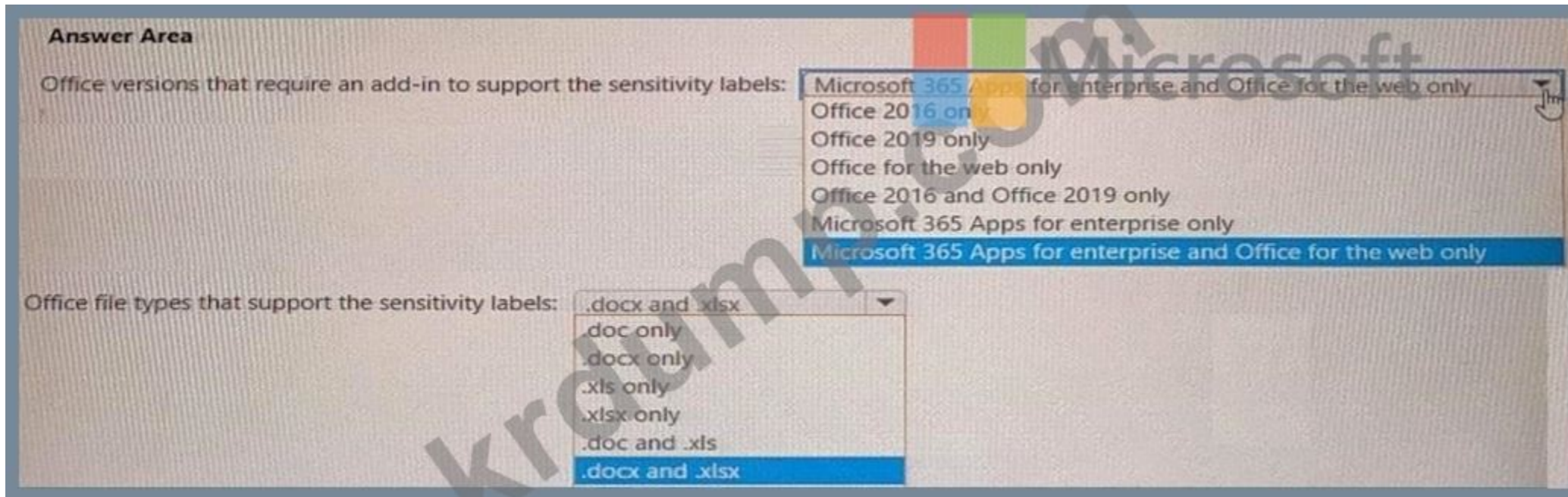
* □□

□□□ □□□□ □□□ □□□□□□. □□□ □□□□ □□□.

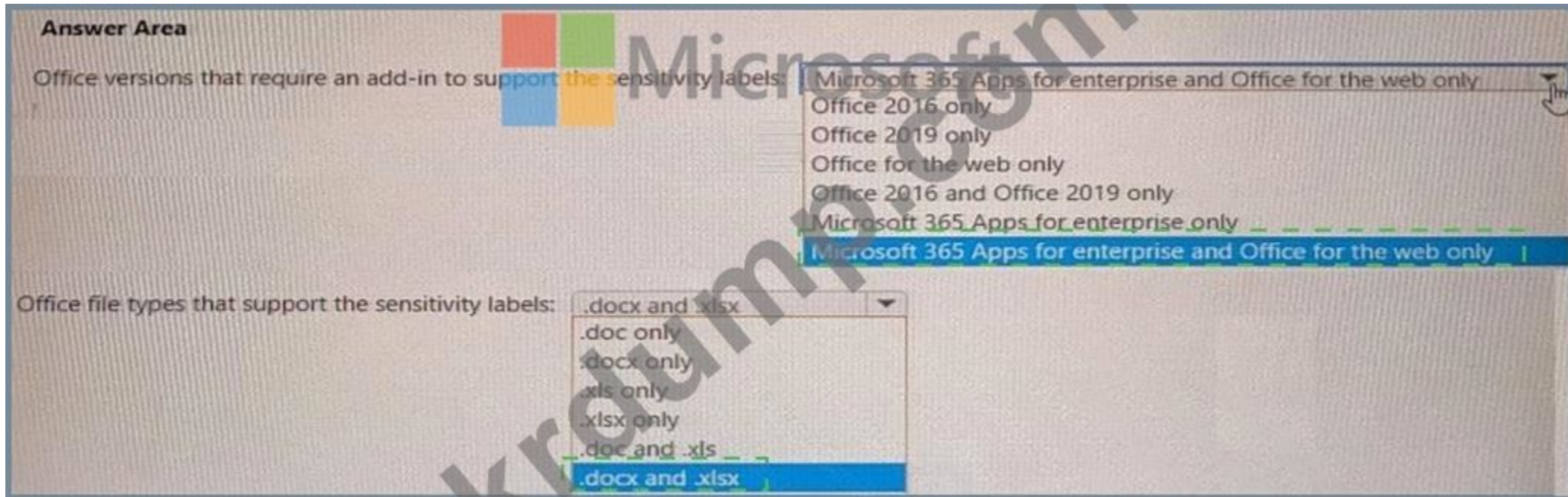
* □□□ □□□□ □□□□ □□ □□ □□□ □□□□ Office □□□ □□□□□□?

* □□□ □□□ □□□□ □□ □□□ □□□□□□?

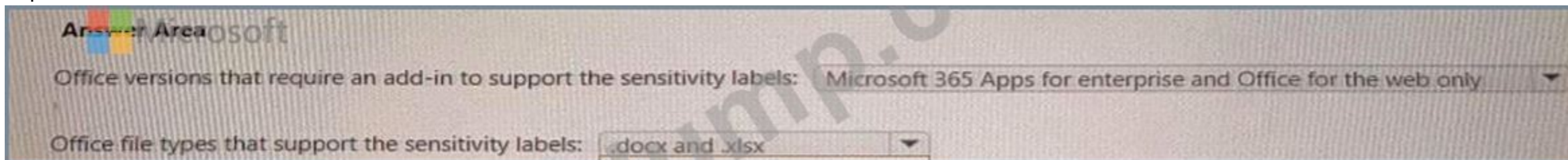
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ 1□□□□□.



Answer:



Explanation:



NEW QUESTION: 158

□□□□ User1□□□□ □□□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

□□□ □□ □□ □□□ □□□□□.

User1□□ □□ □□ □□□ □□□□ □□□□: □□ □□□ □□□□ □□□ □□.

□□ □□ □□□ □□ □□□□?

- A. Azure Active Directory (AAD) is the primary identity provider for Microsoft 365.
- B. Azure Active Directory (AAD) is the primary identity provider for Microsoft 365. AAD is used to manage user identities and access to Microsoft 365 services.
- C. Microsoft 365 uses Azure Active Directory (AAD) for user authentication and authorization.
- D. Azure Active Directory (AAD) is the primary identity provider for Microsoft 365. AAD is used to manage user identities and access to Microsoft 365 services.

Answer: D (LEAVE A REPLY)

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-assign-role-azure-portal>

NEW QUESTION: 159

User1 is a Microsoft 365 E5 user. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license.

User1 is assigned the Microsoft 365 E5 license. User1 is assigned the Microsoft 365 E5 license?

- A. User1 is assigned the Microsoft 365 E5 license.
- B. User1 is assigned the Microsoft 365 E5 license.
- C. User1 is assigned the Microsoft 365 E5 license.
- D. User1 is assigned the Microsoft 365 E5 license.

Answer: C (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/insider-risk-management-configure?view=o365-worldwide>

NEW QUESTION: 160

Microsoft 365 E5 users are assigned the DLP1 policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

DLP1 is a Data Loss Prevention (DLP) policy. DLP1 is a Data Loss Prevention (DLP) policy.

NEW QUESTION: 161

Microsoft 365 E5 users are assigned the Policy1 policy. Policy1 is a Data Loss Prevention (DLP) policy.

Exchange Online Protection (EOP) is a Data Loss Prevention (DLP) policy. Exchange Online Protection (EOP) is a Data Loss Prevention (DLP) policy.

* Exchange Online Protection (EOP) is a Data Loss Prevention (DLP) policy. Exchange Online Protection (EOP) is a Data Loss Prevention (DLP) policy.

* The email will be blocked, and the user will receive the policy tip: Message blocked.

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

* The email will be blocked, and the user will receive the policy tip: Message blocked.

* The email will be blocked, and the user will receive the policy tip: Message blocked.

* The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message blocked.

The email will be blocked, and the user will receive the policy tip: Message blocked.

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.
The email will be blocked, and the user will receive the policy tip: Message contains sensitive data.
The email will be allowed, and the user will receive the policy tip: Message blocked.
The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.
The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:	Result
When the user sends an email that contains only financial data:	Result

Answer:

Results

The email will be blocked, and the user will receive the policy tip: Message blocked.

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

The email will be allowed, and the user will receive the policy tip: Message blocked.

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

The email will be allowed, and a message policy tip will NOT be displayed.

Answer Area

When the user sends an email that contains financial data and health records:

The email will be blocked, and the user will receive the policy tip: Message blocked.

When the user sends an email that contains only financial data:

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

Explanation:

When the user sends an email that contains financial data and health records:	The email will be blocked, and the user will receive the policy tip: Message blocked.
When the user sends an email that contains only financial data:	The email will be allowed, and the user will receive the policy tip: Message contains sensitive data.

Box 1: The email will be blocked, and the user will receive the policy tip: Message blocked.

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

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

Reference:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/how-dlp-works-between-admin-centers>

NEW QUESTION: 162

User1 [redacted] Microsoft 365 [redacted].

User1 [redacted].

Microsoft Exchange Online [redacted].

Microsoft 365 □□□ □□□□.

User1□ 8□□ □□□ □□□ □□□ □□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. zure AD ID □□

B. Microsoft Entra □□□ ID

C. □□□ □□□

D. Azure AD □□ □□ ID □□(PJM)

Answer: D (LEAVE A REPLY)

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Require approval to activate privileged roles

Enforce multi-factor authentication to activate any role

Use justification to understand why users activate

Get notifications when privileged roles are activated

Conduct access reviews to ensure users still need roles

Download audit history for internal or external audit

Prevents removal of the last active Global Administrator and Privileged Role Administrator role assignments.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

NEW QUESTION: 163

Microsoft 365 E5 □□□ □□□□.

Group1□□□ □□□ □□□ □□□□ □□ Microsoft Defender to Cloud Apps□ □□□□□.

□□ 1□ □□□□ □□□□ □□ □□□ □□□□□□□ □□□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

Microsoft Defender

Settings > Cloud apps

System

- About
- Organization details
- Mail settings
- Scoped deployment and privacy
- Preview Features
- IP address ranges
- User groups
- API tokens
- SIEM agents
- Playbooks



Answer:

Answer Area

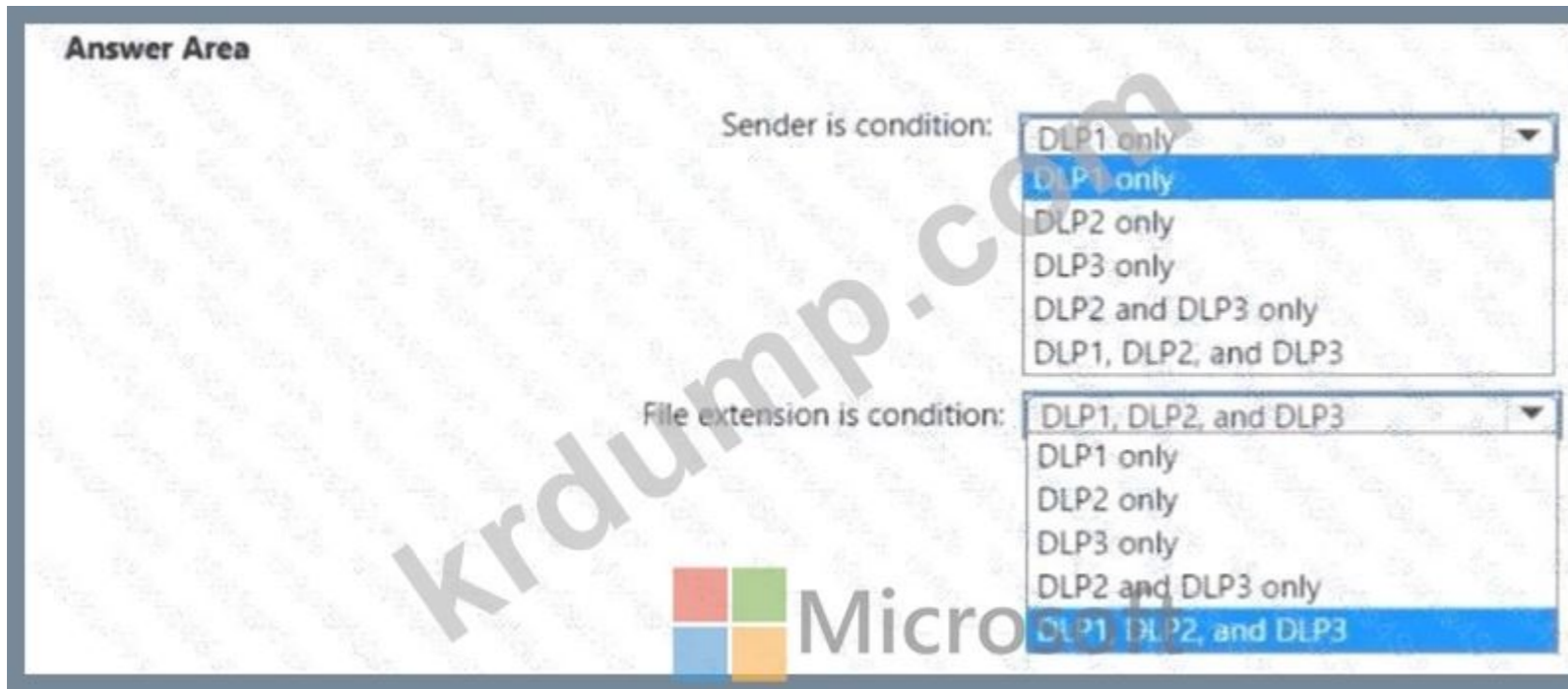
Microsoft Defender

Settings > Cloud apps

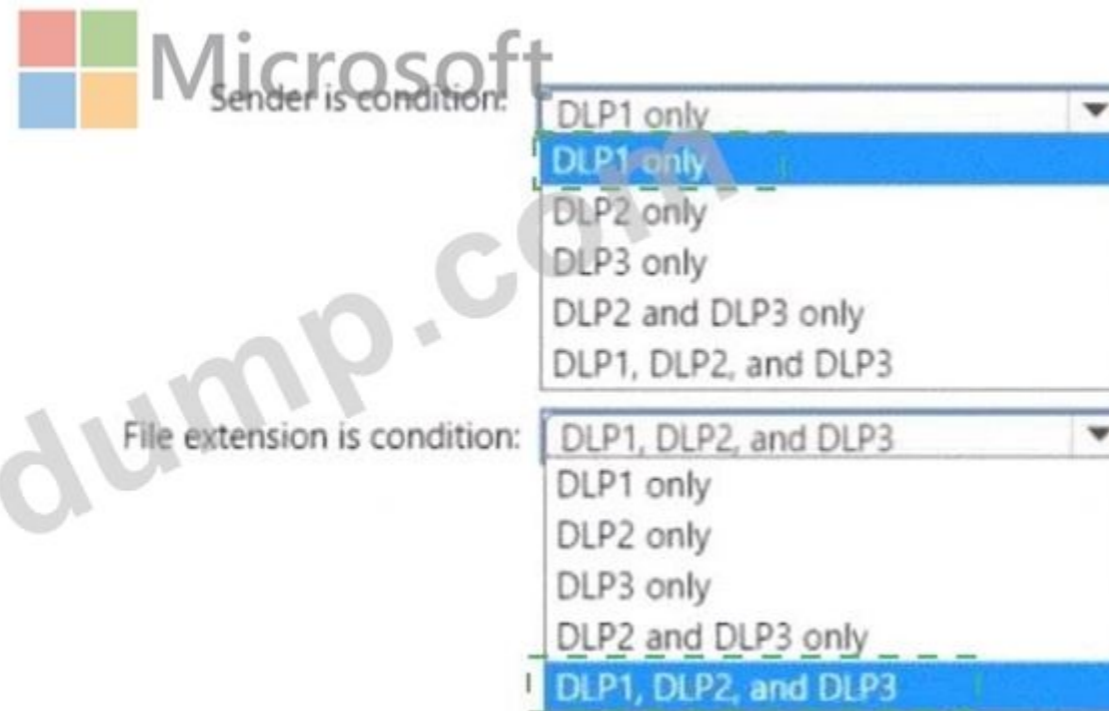
System

- About
- Organization details
- Mail settings
- Scoped deployment and privacy
- Preview Features
- IP address ranges
- User groups
- API tokens
- SIEM agents
- Playbooks

Explanation:



Answer:
Answer Area



Explanation:



NEW QUESTION: 165

You are a Microsoft 365 administrator. You have a Microsoft 365 tenant named Contoso.com. You have a Microsoft 365 group named Group1. You have a Microsoft 365 group named Group2. You have a Microsoft 365 group named Group3. You have a Microsoft 365 group named Group4. You have a Microsoft 365 group named Group5. You have a Microsoft 365 group named Group6. You have a Microsoft 365 group named Group7. You have a Microsoft 365 group named Group8. You have a Microsoft 365 group named Group9. You have a Microsoft 365 group named Group10. You have a Microsoft 365 group named Group11. You have a Microsoft 365 group named Group12. You have a Microsoft 365 group named Group13. You have a Microsoft 365 group named Group14. You have a Microsoft 365 group named Group15. You have a Microsoft 365 group named Group16. You have a Microsoft 365 group named Group17. You have a Microsoft 365 group named Group18. You have a Microsoft 365 group named Group19. You have a Microsoft 365 group named Group20. You have a Microsoft 365 group named Group21. You have a Microsoft 365 group named Group22. You have a Microsoft 365 group named Group23. You have a Microsoft 365 group named Group24. You have a Microsoft 365 group named Group25. You have a Microsoft 365 group named Group26. You have a Microsoft 365 group named Group27. You have a Microsoft 365 group named Group28. You have a Microsoft 365 group named Group29. You have a Microsoft 365 group named Group30. You have a Microsoft 365 group named Group31. You have a Microsoft 365 group named Group32. You have a Microsoft 365 group named Group33. You have a Microsoft 365 group named Group34. You have a Microsoft 365 group named Group35. You have a Microsoft 365 group named Group36. You have a Microsoft 365 group named Group37. You have a Microsoft 365 group named Group38. You have a Microsoft 365 group named Group39. You have a Microsoft 365 group named Group40. You have a Microsoft 365 group named Group41. You have a Microsoft 365 group named Group42. You have a Microsoft 365 group named Group43. You have a Microsoft 365 group named Group44. You have a Microsoft 365 group named Group45. You have a Microsoft 365 group named Group46. You have a Microsoft 365 group named Group47. You have a Microsoft 365 group named Group48. You have a Microsoft 365 group named Group49. You have a Microsoft 365 group named Group50. You have a Microsoft 365 group named Group51. You have a Microsoft 365 group named Group52. You have a Microsoft 365 group named Group53. You have a Microsoft 365 group named Group54. You have a Microsoft 365 group named Group55. You have a Microsoft 365 group named Group56. You have a Microsoft 365 group named Group57. You have a Microsoft 365 group named Group58. You have a Microsoft 365 group named Group59. You have a Microsoft 365 group named Group60. You have a Microsoft 365 group named Group61. You have a Microsoft 365 group named Group62. You have a Microsoft 365 group named Group63. You have a Microsoft 365 group named Group64. You have a Microsoft 365 group named Group65. You have a Microsoft 365 group named Group66. You have a Microsoft 365 group named Group67. You have a Microsoft 365 group named Group68. You have a Microsoft 365 group named Group69. You have a Microsoft 365 group named Group70. You have a Microsoft 365 group named Group71. You have a Microsoft 365 group named Group72. You have a Microsoft 365 group named Group73. You have a Microsoft 365 group named Group74. You have a Microsoft 365 group named Group75. You have a Microsoft 365 group named Group76. You have a Microsoft 365 group named Group77. You have a Microsoft 365 group named Group78. You have a Microsoft 365 group named Group79. You have a Microsoft 365 group named Group80. You have a Microsoft 365 group named Group81. You have a Microsoft 365 group named Group82. You have a Microsoft 365 group named Group83. You have a Microsoft 365 group named Group84. You have a Microsoft 365 group named Group85. You have a Microsoft 365 group named Group86. You have a Microsoft 365 group named Group87. You have a Microsoft 365 group named Group88. You have a Microsoft 365 group named Group89. You have a Microsoft 365 group named Group90. You have a Microsoft 365 group named Group91. You have a Microsoft 365 group named Group92. You have a Microsoft 365 group named Group93. You have a Microsoft 365 group named Group94. You have a Microsoft 365 group named Group95. You have a Microsoft 365 group named Group96. You have a Microsoft 365 group named Group97. You have a Microsoft 365 group named Group98. You have a Microsoft 365 group named Group99. You have a Microsoft 365 group named Group100.

- A.
 - B.
- Answer: (SHOW ANSWER)

NEW QUESTION: 166

You are a Microsoft 365 administrator. You have a Microsoft 365 tenant named Contoso.com.

Home > sensitivity


Labels Label policies Auto-labeling(preview)

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

+ Create a label Publish labels Refresh

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

- Which labels are applied to the content?
- A. Label3, Label4, Label6
 - B. Label1, Label2, Label3, Label4, Label5, Label6
 - C. Label1, Label2, Label5

Answer Area  Microsoft

Block a vulnerable app until the app is updated:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

Block an application executable based on a file hash:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

Answer:

Answer Area

Block a vulnerable app until the app is updated:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

Block an application executable based on a file hash:

- An allow or block file
- A file indicator
- A remediation request
- An update ring

Explanation:

Answer Area



Block a vulnerable app until the app is updated:

▼
An allow or block file
A file indicator
A remediation request
An update ring

Block an application executable based on a file hash:

▼
An allow or block file
A file indicator
A remediation request
An update ring

Box 1: A remediation request

Block a vulnerable app until the app is updated.

Block vulnerable applications

How to block vulnerable applications

Go to Vulnerability management > Recommendations in the Microsoft 365 Defender portal.

Select a security recommendation to see a flyout with more information.

Select Request remediation.

Select whether you want to apply the remediation and mitigation to all device groups or only a few.

Select the remediation options on the Remediation request page. The remediation options are software update, software uninstall, and attention required.

Pick a Remediation due date and select Next.

Under Mitigation action, select Block or Warn. Once you submit a mitigation action, it is immediately applied.

Review the selections you made and Submit request. On the final page you can choose to go directly to the remediation page to view the progress of remediation activities and see the list of blocked applications.

Box 2: A file indicator

Block an application executable based on a file hash.

While taking the remediation steps suggested by a security recommendation, security admins with the proper permissions can perform a mitigation action and block vulnerable versions of an application. File indicators of compromise (IOC)s are created for each of the executable files that belong to vulnerable versions of that application. Microsoft Defender Antivirus then enforces blocks on the devices that are in the specified scope.

The option to View details of blocked versions in the Indicator page brings you to the Settings > Endpoints > Indicators page where you can view the file hashes and response actions.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/tvm-block-vuln-apps>

NEW QUESTION: 169

□□□□□ Microsoft Entra □□□□ □□□ Azure □□□ □□□□.


□□ □□□□ Microsoft Entra Connect□ Express Settings□ □□□□ Active Directory Domain Services(AD DS)□□ □□□□ □□□□□□.

□□ □□□ □□□□ □□□(SSPR)□ □□□ □□□□□.

□□□□ □□□□□□ □□□□□□ □□□□ □□□□□□ AD DS□ □□□□□□ □□□□ □□□.

□□ □□□ □□□□ □□□□ □□□? □□□□ □□□ □□□ □□□ □□□ □□□□□□. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□ □□□ □□□□□□ □□□□ □ □□□□ □ □ □□□□.

□□□□: □□ □□□ 1□□□□.

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

Answer:

Actions

- From the Microsoft Entra admin center, configure on-premises integration password writeback.
- From the Microsoft Entra admin center, configure the authentication methods for SSPR.
- From the Microsoft Entra admin center, configure the registration settings for SSPR.
- Select Group writeback in Microsoft Entra Connect.
- Select Password writeback in Microsoft Entra Connect.

Answer Area

- Step 1: Validate permissions for the Microsoft Entra Connect account.
- Step 2: From the Microsoft Entra admin center, configure on-premises integration password writeback.
- Step 3: Select Password writeback in Microsoft Entra Connect.

Explanation:

Actions

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

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

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

Select Group writeback in Microsoft Entra Connect.

Select Password writeback in Microsoft Entra Connect.

Answer Area

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

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

Step 3: Select Password writeback in Microsoft Entra Connect.



NEW QUESTION: 170

Microsoft 365 E5 □□□□ □□□□.

□□□□□ 1,000□□ □□□ iOS □□□ □□□ □□□□□. □□□ □□□□□□ □□□□□ □□ □□□□□.

□□ □□ □□□ □□□□ Microsoft Intune □□ □□□ □□□□ □□□.

* □□□ □□□□□ □□□□□□□

* □□□ □□□ □□□□□□□

* □□□ □□ □□□□ □□□□□□.

□□□ □□□□ □□□?

A. □□ □□ □□(ADE)

B. BYOD(Bring Your Own Device) □□□ □ □□ □□

C. Apple Configurator □□

Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 171

2,000□ □□□ □□□ □□□□ □□ Microsoft 365 □□□ □□□□.

□□□□□ Microsoft 365 □□□ □□□ □□□□ □□□□ □□ □□□□□ 30□□□□ □□ □□□□ □□□□ □□□□ □□□.

□□□ □□□□ □□□?

- A.
- B.
- C.
- D.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 172

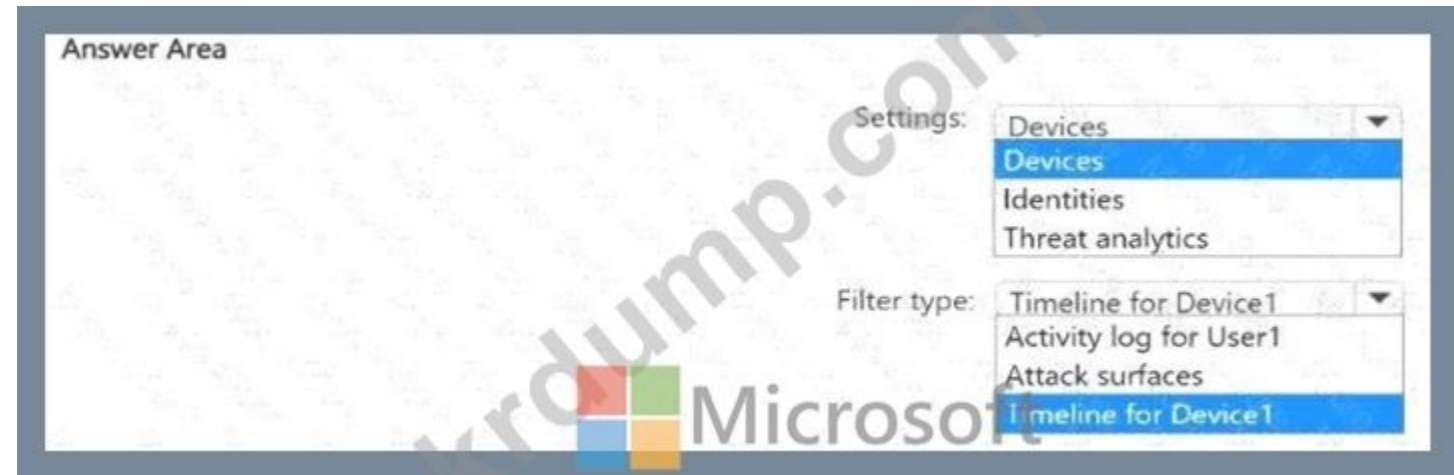
User1 is a user in an Azure Active Directory (Azure AD) tenant. User1 is a member of the Microsoft 365 Admin role. Cloud App Security is installed in the tenant. User1 is trying to view the activity log for a device in the tenant. User1 is unable to view the activity log for the device. What should User1 do to view the activity log for the device?

- A.
- B.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 173

User1 is a user in a Microsoft 365 E5 tenant. User1 is a member of the Microsoft Defender for Endpoint Admin role. Device1 is a Windows 11 device in the tenant. User1 is trying to view the activity log for Device1 in the Microsoft Defender for Endpoint console. User1 is unable to view the activity log for Device1. What should User1 do to view the activity log for Device1?



Answer:

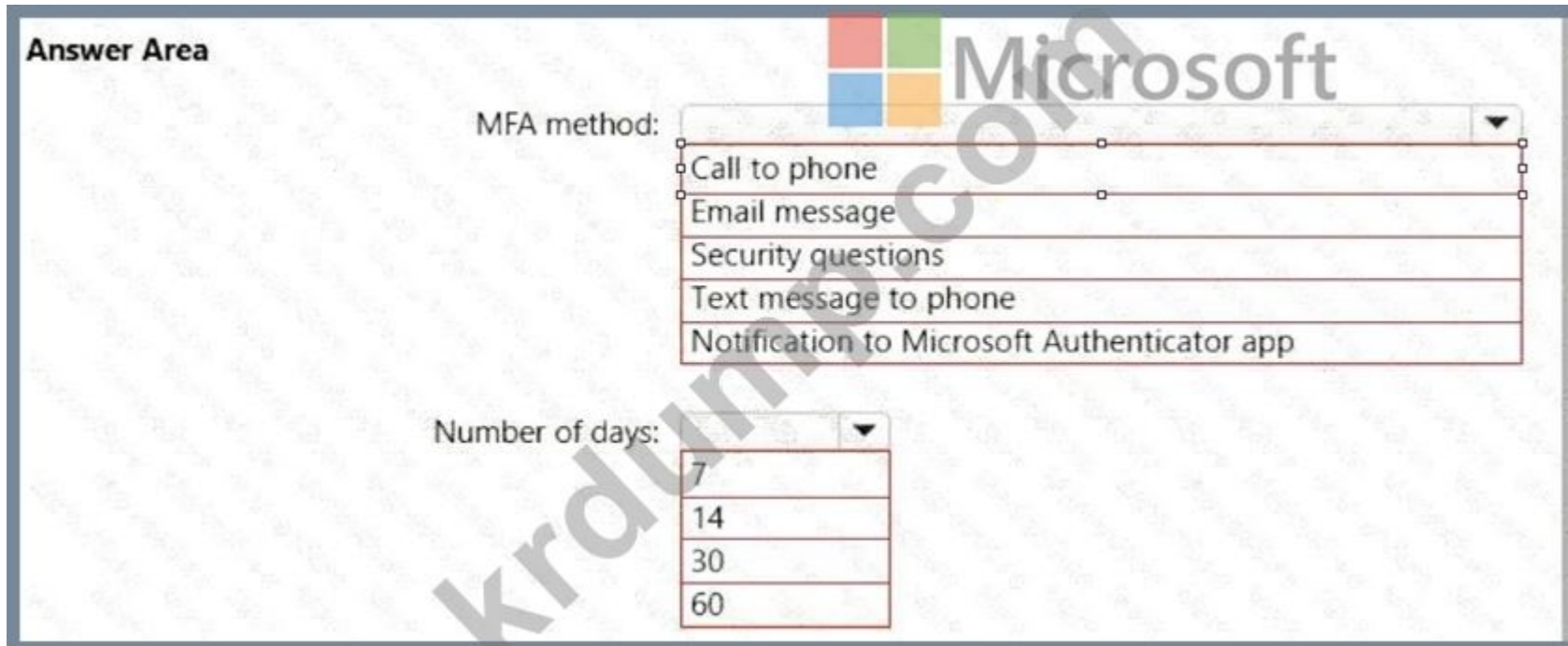
Answer Area

Portal: Microsoft 365 admin center

Feature: Configuration analyzer

NEW QUESTION: 175

□□□
□□□ Microsoft 365 E5 □□□□ □□□□.
□□ □□□ □□□ □□ □□□□□□□□.
□□□□ □□□□ □□□□ □□□□□□□□.
□□□□ □□ □□ □□ □□(MFA) □□□□ □□□□ □ □□□, □□□□ MFA□ □□□□ □□ □□□ □□□□? □□□□□□ □□ □□□□ □□□ □□□ □□□□□□□□.
□□□□: □□ □□□□ 1□□□□□.



Answer:

Answer Area

MFA method:

- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app

Number of days:

- 7
- 14
- 30
- 60

Explanation:


Answer Area

MFA method:

- Call to phone
- Email message
- Security questions
- Text message to phone
- Notification to Microsoft Authenticator app

Number of days:

- 7
- 14
- 30
- 60



Box 1: Notification to Microsoft Authenticator app

Do users have 14 days to register for Azure AD Multi-Factor Authentication?

Users have 14 days to register for MFA with the Microsoft Authenticator app from their smart phones, which begins from the first time they sign in after security defaults has been enabled. After 14 days have passed, the user won't be able to sign in until MFA registration is completed.

Box 2: 14

Azure AD Identity Protection will prompt your users to register the next time they sign in interactively and they'll have 14 days to complete registration. During this 14-day period, they can bypass registration if MFA isn't required as a condition, but at the end of the period they'll be required to register before they can complete the sign-in process.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/solutions/empower-people-to-work-remotely-secure-sign-in>

<https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy>

NEW QUESTION: 176

Microsoft 365 E5 □□□□ □□□□.

□□ □□□ □□ □□□□ ISO 27001 □□□ □□□□ □□□.

□□□□ □□□ □□ □□□□ □□□.

A. Microsoft J6i □□ □□ □□□□ □□ □□ □□□ □□□□.

B. Microsoft 365 □□ □□□□ □□□ □□□ □□□□□□.

C. □□ □□ □□□□□ □□□ □□□□□.

D. Azure Portal □ □□□□ □□ □□□ □□□ □□ □□□ □□□□□.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 177

Microsoft 365 E5 □□□ □□□□ □□□ Microsoft Defender for Cloud Apps □ □□□□ □□□□. OAuth □ □□□ □□□ □ □□□ □□□□ □□□.

□□ □□: Microsoft 365 □ □□□□ □□ Defender □ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 178

Microsoft 365 Enterprise E5 □□□ □□□□.

App1 □□□□ □□□□ □□ □□ Azure AD □□□□□□ □□□□□□ □□□ □□□□□.

□□□ App1 □ □□□ □ □□ □□□ □□□ □□ 2□□ □□□ □□□□□ □□ □□□.

□□□□ □□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *

App1 policy ✓

What does this policy apply to?

Users and groups ✓

Assignments

Users or workload identities ⓘ
All users

Include Exclude

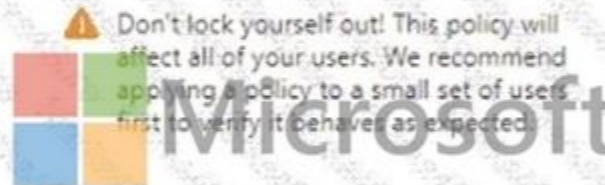
- None
 All users
 Select users and groups

Cloud apps or actions ⓘ

No cloud apps, actions, or authentication contexts selected ✓

Conditions ⓘ

0 conditions selected



Access controls

Grant ⓘ ✓
0 controls selected

Session ⓘ

0 controls selected

Enable policy

Report only On Off ✓

Answer:

Answer Area

New ...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

App1 policy ✓

Assignments

Users or workload identities ⓘ

All users

Cloud apps or actions ⓘ ✓

No cloud apps, actions, or authentication contexts selected

Conditions ⓘ

0 conditions selected

Access controls

Grant ⓘ ✓

0 controls selected

Session ⓘ

0 controls selected

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

What does this policy apply to?

Users and groups ✓

Include Exclude

- None
- All users
- Select users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.



Microsoft



Explanation:

New ...
Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *
App1 policy ✓

What does this policy apply to?
Users and groups ✓

Assignments

Users or workload identities ⓘ
All users

Cloud apps or actions ⓘ
No cloud apps, actions, or authentication contexts selected ✓

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected ✓

Session ⓘ
0 controls selected

Enable policy
Report-only On Off ✓

Include Exclude

None
 All users
 Select users and groups

⚠ Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Microsoft

NEW QUESTION: 179

D. 0020 0030

E. 002, 003, 0040

Answer: B (LEAVE A REPLY)

NEW QUESTION: 184

Microsoft Endpoint Manager 00 00 0000 00000 00000.

00 00 00 00 00000 0000 Microsoft Azure Active Directory(Azure AD) 00000 00000.

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

Endpoint Manager 00 00 00 0000 00 00 00 000000.

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

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 185

Microsoft 365 E5

Name	Membership type	Membership rule
Group1	Assigned	Not applicable
Group2	Dynamic	(user.department -eq "Finance")
Group3	Dynamic	(user.department -eq "R&D")

Name	Department	Assigned group membership
User1	Finance	Group1
User2	Technical	None
User3	R&D	Group1

- *
- o
- * : Group1
- * : Group2, Group3
- o
- *
- *
- *
- *
- *

Statements	Yes	No
User1 can sign in to App1.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to App1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to App1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Statements

User1 can sign in to App1.

Yes

No

User2 can sign in to App1.

User3 can sign in to App1.

Explanation:

Answer Area

Statements

User1 can sign in to App1.

Yes

No

User2 can sign in to App1.

User3 can sign in to App1.

NEW QUESTION: 186

Microsoft 365 E5 □□□ □□□□.

Microsoft Defender for Endpoint□ Microsoft Intune□ □□□□□.

Intune□ □□□ □ □□□ Defender for Endpoint□ □□□□ □□□□□□ □□ □□□.

□□□: □□ □□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □□□

B. □

Answer: (SHOW ANSWER)

NEW QUESTION: 187

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □

□ □ □□, □□ □□□□ □□□ □□ □ □□□□.

□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□□ □□□ □□ □□□ □□□□ □□□□.

User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Compliance Manager □□□ □□□□□ User1□ □□□□□ □□□.

□□ □□: Microsoft 365 □□ □□□□ User1□□ □□ □□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 188

□□□

□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

Microsoft 365 E5 □□□ □□□□□.

Azure AD Connect □□□□ □□□□ □□□□ □□□.

□□ □□□ □□□□ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area

Install: ▼

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server: ▼

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Answer:

Answer Area

Install:

- The Azure AD Application Proxy connector
- Azure AD Connect
- The Azure AD Connect provisioning agent
- Active Directory Federation Services (AD FS)

Server:

- Server1 only
- Server2 only
- Server3 only
- Server1 or Server2 only
- Server1 or Server3 only
- Server1, Server2, or Server3

Explanation:

Answer Area

Install:

	▼
The Azure AD Application Proxy connector	
Azure AD Connect	
The Azure AD Connect provisioning agent	
Active Directory Federation Services (AD FS)	

Server:

	▼
Server1 only	
Server2 only	
Server3 only	
Server1 or Server2 only	
Server1 or Server3 only	
Server1, Server2, or Server3	

Box 1: The Azure AD Connect provisioning agent

Install the Azure AD Connect provisioning agent

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

With Azure AD Connect cloud sync, provisioning from AD to Azure AD is orchestrated in Microsoft Online Services. An organization only needs to deploy, in their on-premises or IaaS-hosted environment, a light-weight agent that acts as a bridge between Azure AD and AD. The provisioning configuration is stored in Azure AD and managed as part of the service.

Box 2: Server1 or Server2 only.

Cloud provisioning agent requirements include:

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

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

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

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-install>

<https://docs.microsoft.com/en-us/azure/active-directory/cloud-sync/how-to-prerequisites>

NEW QUESTION: 189

□□ □□ □□ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Platform	Azure Active Directory (Azure AD)
Device1	Windows 10	Joined
Device2	Windows 10	Registered
Device3	Windows 10	Not joined or registered
Device4	Android	Registered

Endpoint Protection is installed on all devices.

Endpoint Protection is configured to protect all devices.

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

Answer: A (LEAVE A REPLY)

Reference:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION: 193

Microsoft 365 is deployed to all devices.

Endpoint Protection is installed on all devices.

Endpoint Protection is configured to protect all devices.

- A. Windows 10
- B. CentOS Linux
- C. iOS
- D. Windows 10

Answer: D (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 194

Endpoint Protection is installed on all devices.

Endpoint Protection is configured to protect all devices.

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:

Actions	Answer Area
Create a data loss prevention (DLP) policy.	Assign eDiscovery permissions.
Create an eDiscovery case.	Create an eDiscovery case.
Create a label.	Create a hold.
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Explanation:

Assign eDiscovery permissions.
Create an eDiscovery case.
Create a hold.

References:

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

NEW QUESTION: 195

Microsoft 365 E5 _____.

Microsoft Defender _____.

_____.

_____.

_____.



Answer:



Explanation:

1. Analysis 2. Take Action

NEW QUESTION: 196

Microsoft 365 E5 □□□ □□□□.

□□□□ Microsoft Defender for Endpoint □□□ □□□□ □□□□ □□□□ □□□□. Defender for Endpoint □ Microsoft Defender for Cloud Apps □ □□□ □□□□□ □□□□ □□□□.

Cloud Discovery □ App1 □□□ □□□ □ □□ □□□□□□.

Microsoft Edge □□ App1 □ □□□□ □□ □□□□ □□□. □□□□ □□□ □□□ □ □□□ □□□.

□□ □□□ □ □□□ □□□□ □□, Defender for Endpoint □ Defender for Cloud □ □□□□ □□ □□□ □□□□ □□□□ □□□?



user1 is a Microsoft 365 E5 user. You need to ensure that user1 has the correct licenses assigned to their account. Which cmdlet should you use to assign licenses to user1?

Options:

- A. Get-MgUserLicenseDetail
- B. Set-MgUserLicense
- C. Update-MgSubscription
- D. Update-MgSubscriberSku



Answer:



Explanation:



NEW QUESTION: 199

Microsoft 365 E5 user. You need to ensure that user1 has the correct licenses assigned to their account. Which cmdlet should you use to assign licenses to user1?

Options:

- A. Get-MgUserLicenseDetail
- B. Set-MgUserLicense
- C. Update-MgSubscription
- D. Update-MgSubscriberSku

- A. Get-MgUserLicenseDetail
- B. Set-MgUserLicense
- C. Update-MgSubscription
- D. Update-MgSubscriberSku

Answer: (SHOW ANSWER)

NEW QUESTION: 200

□□□

Microsoft 365 E5 □□□ □□□□.

Azure AD Privileged Identity Management(PIM)□□ □□ □□□ □□ □□□ □□□ □□□ □□ □□ □□□ □□□□□.

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


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

□□□□ □□□ □□□ □□□□ □ □□□□ □□□□ □□ □□□□ □□□□ □□□□ □□□ □□□□□.

Answer Area

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

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



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

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

Answer:

Answer Area

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

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



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

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

Explanation:

Answer Area

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

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



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

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

Box 1: will lose the role after eight hours

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

NEW QUESTION: 201

Microsoft 365 □□□ □□□□.

□□ □□ □□□ □□ □□□□.

Policy setting	Policy name	Managers	
	Description	If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com	Edit
	Applied to	Except if the email is sent to member of: test1ww@M365x289755.onmicrosoft.com	
	Safety tips > User impersonation	Off	Edit
	Safety tips > Domain impersonation	Off	
	Safety tips > Unusual characters	Off	
	Mailbox intelligence	Off	
Spool	Enable antispoofting protection	On	
	Action	Quarantine the message	Edit
Advanced settings	Advanced phishing thresholds	3 - More Aggressive	Edit

□□□□ □□□ □□□ □□□ □ □□□□ □□□□ □□□□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

Answer Area

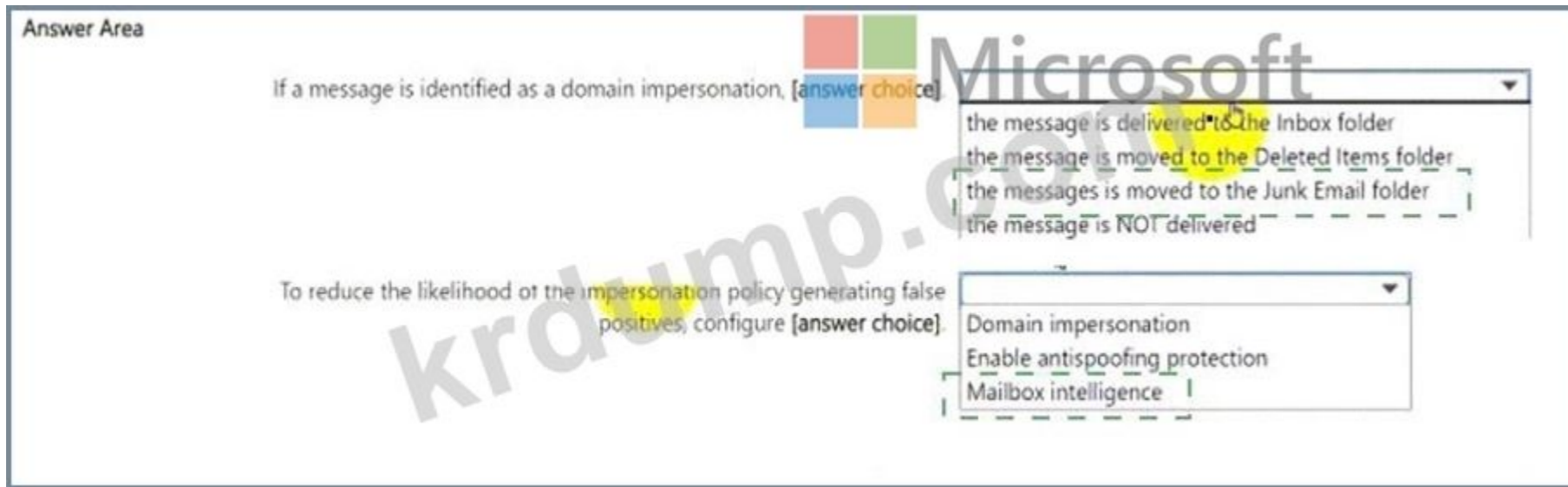
If a message is identified as a domain impersonation, [answer choice]

- the message is delivered to the Inbox folder
- the message is moved to the Deleted Items folder
- the messages is moved to the Junk Email folder
- the message is NOT delivered

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice]

- Domain impersonation
- Enable antispoofting protection
- Mailbox intelligence

Answer:



Explanation:

If a message is identified as a domain impersonation: the message is moved to the Junk Email folder According to the anti-phishing policy settings shown in the exhibit, messages identified as domain impersonation should be moved to the Junk Email folder to reduce the risk of phishing attacks.

To reduce the likelihood of the impersonation policy generating false positives, configure: Mailbox intelligence Mailbox intelligence helps in reducing false positives by using machine learning and historical email patterns to make better decisions about which emails are legitimate and which are not.

NEW QUESTION: 206

Microsoft 365 E5

Name	Group
Device1	DeviceGroup1
Device2	DeviceGroup2

08:00

* : !

*

o 70:

o (3)

o :

* : User1@contoso.com, User2@contoso.com

08:02

* :

*

o : .

o : DevtceGroup1, DeviceGroup2

* : User1@contoso.com

Microsoft 365 Defender

Time	Alert name	Severity	Impacted assets
08:05	Activity1	Low	Device1
08:07	Activity1	Low	Device1
08:08	Activity1	Medium	Device1
08:15	Activity2	Medium	Device2
08:16	Activity2	Medium	Device2
08:20	Activity1	High	Device1
08:30	Activity3	Medium	Device2
08:35	Activity2	High	Device2

08:05: 08:05 08:07 08:08 08:15 08:16 08:20 08:30 08:35. 08:05 08:07 08:08 08:15 08:16 08:20 08:30 08:35. 08:05: 08:05 100000.

Answer Area

Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.



Microsoft

Yes

No

Answer:

Answer Area

Statements

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.

	Yes	No
User1@contoso.com will receive two incident notification emails for the alert at 08:05.	<input type="radio"/>	<input checked="" type="radio"/>
User2@contoso.com will receive an incident notification email for the alert at 08:07.	<input checked="" type="radio"/>	<input type="radio"/>
User1@contoso.com will receive an incident notification email for the alert at 08:20.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

User1@contoso.com will receive two incident notification emails for the alert at 08:05.

Yes

No

User2@contoso.com will receive an incident notification email for the alert at 08:07.

User1@contoso.com will receive an incident notification email for the alert at 08:20.

NEW QUESTION: 207

□□□

□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□.

Microsoft 365 E5 □□□ □□□□.

□□□□ □□□□ □□□ □□□□□.

□□□□ □□ □□□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□ □□□□ □□□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□□.

Answer Area

Microsoft

Tool:

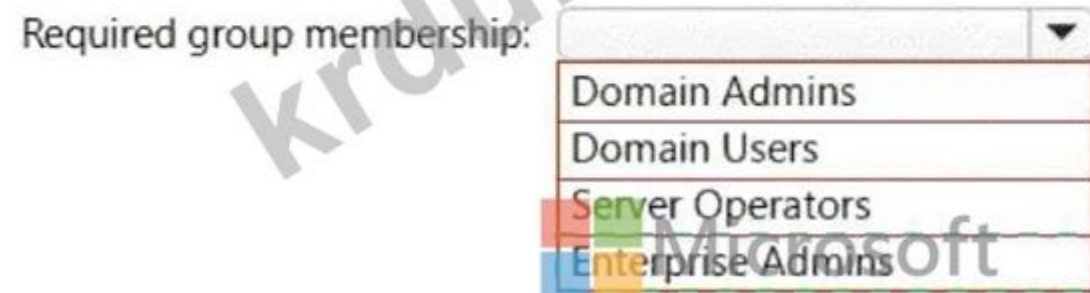
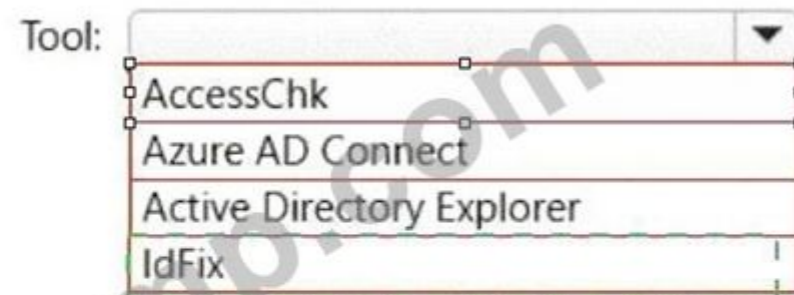
- AccessChk
- Azure AD Connect
- Active Directory Explorer
- IdFix

Required group membership:

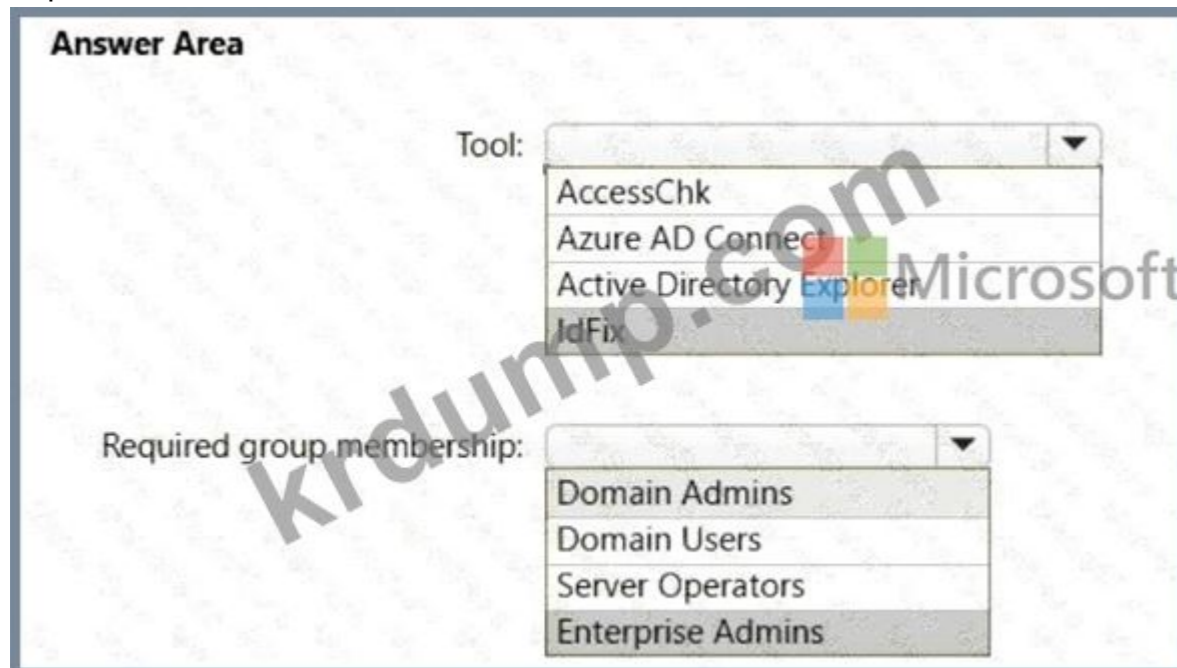
- Domain Admins
- Domain Users
- Server Operators
- Enterprise Admins

Answer:

Answer Area



Explanation:



Box 1: IdFix

Query and fix invalid object attributes with the IdFix tool

Microsoft is working to reduce the time required to remediate identity issues when onboarding to Microsoft

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

The IdFix tool provides you the ability to query, identify, and remediate the majority of object synchronization errors in your Windows Server AD forests in preparation for deployment to Microsoft 365.

The utility does not fix all errors, but it does find and fix the majority. This remediation will then allow you to successfully synchronize users, contacts, and groups from on-premises Active Directory into Microsoft 365.

Note: IdFix might identify errors beyond those that emerge during synchronization. The most common example is compliance with rfc 2822 for smtp addresses. Although invalid attribute values can be

synchronized to the cloud, the product group recommends that these errors be corrected.

Incorrect:

* AccessChk

Box 2: Enterprise Admins

IdFix permissions requirements

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

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

* Enterprise Admins

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

Incorrect:

* Domain Admins

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

* Server Operator

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

* Domain Users - too few permissions

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

Reference:

<https://microsoft.github.io/idfix/>

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

NEW QUESTION: 208

□□□

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

User4□□ Microsoft 365 □□ □ □□□ □□□□□ □□ □□ □□□ □□□ □□□□□.

□□ Microsoft 365 □□□ □□□□ □□□, □□□ □□ □□□□ □□□ □□□ □ □□□ □□□□ □□□.

□□□□ □□ □□□ □□□ □□□□ □□□.

□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area



Microsoft 365 setting:

Office installation options

Privileged access

Release preferences

User:

User1 only

User2 only

User3 only

User1 and User2 only

User1 and User3 only

Answer:

Answer Area

Microsoft 365 setting:

▼

- Office installation options
- Privileged access
- Release preferences

User:

▼

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

Explanation:

Answer Area

Microsoft 365 setting:

▼

- Office installation options
- Privileged access
- Release preferences



User:

▼

- User1 only
- User2 only
- User3 only
- User1 and User2 only
- User1 and User3 only

NEW QUESTION: 209

Microsoft 365 □□□ □□□□.

□□ □□□ □□□□□ □□□□ □□□□ □□□.

* Microsoft Teams □ □□□ □□□ □□□ □□□

* □□ □□ □□□ □

□ □□ □□□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□ □□□□□. □ □□□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□□. □ □□□ □□

□□□ □□□ □□□ □□□□□ □□□□ □ □ □□□□.

Report

The device usage report in Teams

The OneDrive usage report

The SharePoint site usage report

The Teams usage report in Teams

The User activity report in Teams

Requirements

The storage usage of files stored in Microsoft Teams:

Number of active users per Microsoft Team:



B. 0002

C. 0003

D. 0004

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 211

000

00000 0-0000 Active Directory 0000 Microsoft 365 000 0000 0000.

00 00000 00 00 00 00 0000 0000 0000.

Name	Member of	In organizational unit (OU)
User1	Group1	OU1
User2	Group2	OU1

00 00000 00 00 000 000 0000 0000.

Name	Member of	In OU
Group1	None	Sales
Group2	Group1	OU1

Azure AD Connect 0 0000 0000.

00 000 00 000 0 OU 0000 00000.

□□ □□: □□□ □□ □□□□□ □□□ □□□□□ □□□ □□□ □□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

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

Reference:

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

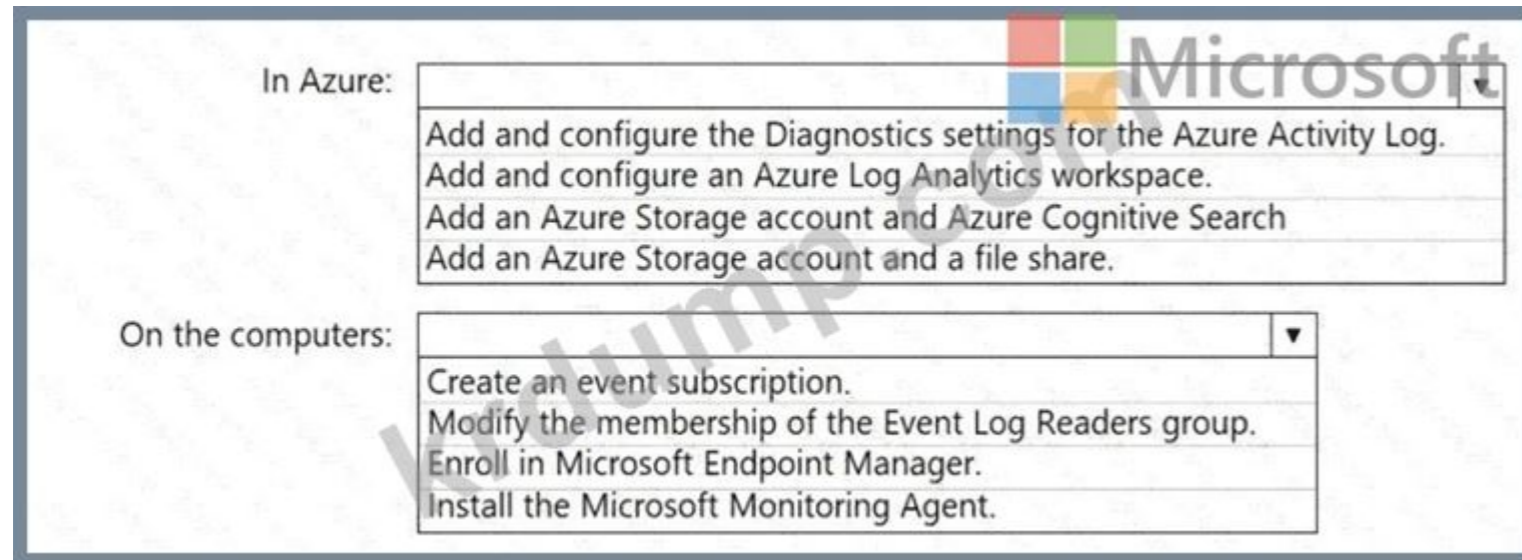
NEW QUESTION: 213

Azure □□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows 10 □□□□ 50□□ □□□□ □□□□.

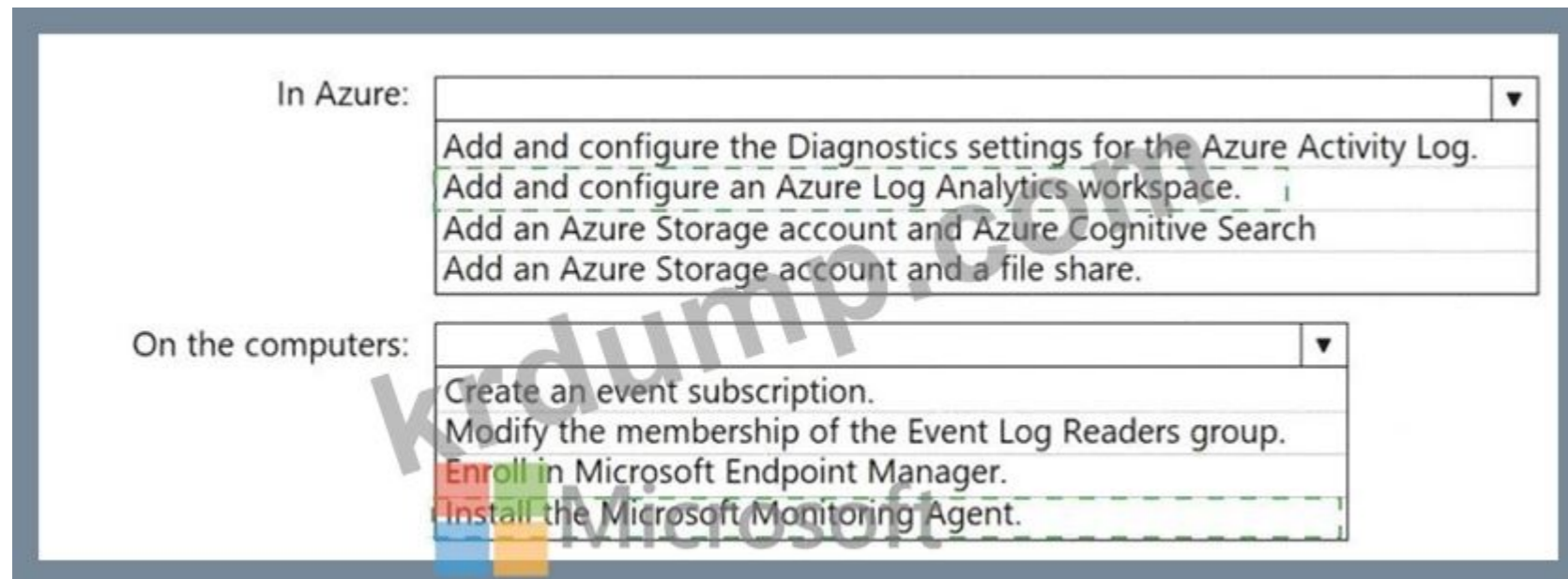
□□□□ □□□ □□ □□□□ □□□□ □□□□□□ □□□.

□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

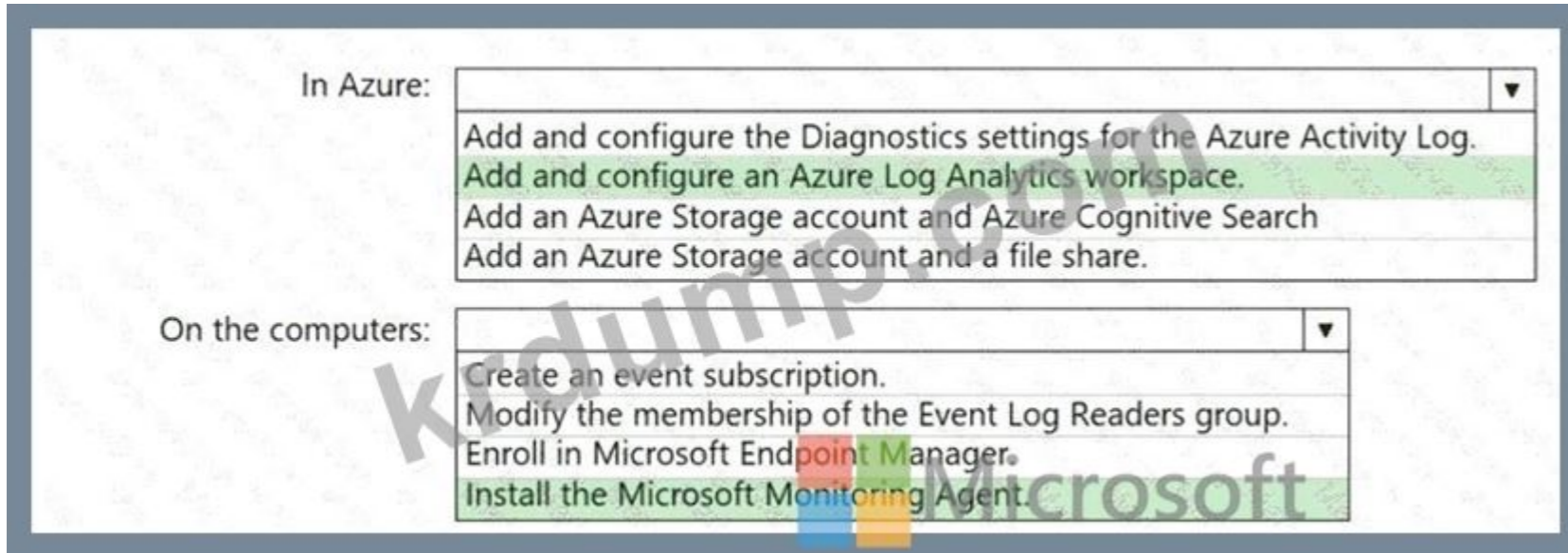
□□□□: □□ □□□ 1□□□□□.



Answer:



Explanation:



Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer>

NEW QUESTION: 214

2,500 Windows 10 users (User1, User2, ..., User2500) are using Microsoft 365 E5 licenses. You need to ensure that all users can enroll their devices in Microsoft Intune. What should you do?



Azure Active Directory (Azure AD) settings: Require Multi-Factor Auth to join devices is set to Yes. Maximum number of devices per user is set to 5.



Microsoft Endpoint Manager settings: User2 is enrolled in Microsoft Endpoint Manager (DEM). User2's device is not enrolled in Intune. What should you do to ensure that all users can enroll their devices in Intune?

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 215

Windows 11 is installed on a Microsoft 365 E5 device. Microsoft Defender for Endpoint is installed on the device. What is the minimum Windows 11 version required for Microsoft Defender for Endpoint to be installed on the device?

- A. 19H2
- B. 20H2
- C. 21H2
- D. 22H2

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 216

Microsoft 365 E5 is installed on a device. Policy1 is a Conditional Access policy that requires MFA for all users. Policy1 is assigned to the device. What is the minimum Windows 11 version required for Policy1 to be enforced on the device?

Options: 19H2, 20H2, 21H2, 22H2



Answer:
Answer Area



Explanation:



NEW QUESTION: 217

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□1□ □□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□□. SSPR□ □□ □□□ □□ □□□□ □□ □□□ □□□□□. □□ □□□□ SSPR□ □□□ □ □□, □□ □□□□ □□□□□ □□□□□ □□ □□ □□□ □□□ □□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□. □□□□: □□ □□□ 1□□□□.

Users that can use SSPR:


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

Users that must answer security questions to reset their password:

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

Answer:

Answer Area



Users that can use SSPR:

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

Users that must answer security questions to reset their password:

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

Explanation:

Answer Area



Users that can use SSPR: User1, User2, and User4 only

Users that must answer security questions to reset their password: User1 and User2 only

NEW QUESTION: 218

contoso.com Active Directory .

.

Choose locations to apply the policy

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

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

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

NEW QUESTION: 220

Microsoft 365 E5

Name	Member of
User1	Group1
User2	Group2
User3	None

AU1

AU1

Members Role assignments

Add users and groups, or select and remove them. The administrators assigned to this unit will manage these users and groups. Adding groups doesn't add users to the unit, it lets the assigned admins manage group settings.

Add users Add groups Upload users

Filter Search this list



MEMBERS

	Email address	Last sign-in	Member type	
<input type="checkbox"/>	User1	User1@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:25 PM	User
<input type="checkbox"/>	User3	User3@sk220912outlook.onmicrosoft.com	November 4, 2022 at 10:27 PM	User

General **Assigned** Permissions

You can assign this role to users and groups, and select users and groups to remove or manage them.

[Learn more about assigning admin roles](#)

<input type="checkbox"/>	Admin name	Last sign-in	Scope
<input type="checkbox"/>	Group1	Unavailable for groups	Organization
<input type="checkbox"/>	Group2	Unavailable for groups	AU1

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Answer Area



Microsoft

Statements

User1 can reset the password of User3.

Yes

No

User2 can reset the password of User3.

User2 can reset the password of User1.

Answer:

Answer Area			
Statements	Yes	No	
User1 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>	
User2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>	
User2 can reset the password of User1.	<input type="radio"/>	<input type="radio"/>	

Explanation:

Answer Area

Statements	Yes	No
User1 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User3.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can reset the password of User1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 221

contoso.com is a Microsoft 365 tenant. User1 is a member of the Admins group. User2 is a member of the Users group. User3 is a member of the Users group. User1 can reset the password of User3. User2 can reset the password of User3. User2 can reset the password of User1. Which Microsoft 365 tool can be used to configure the password reset policy for User1? (Select two.)

- A. Microsoft Entra ID
- B. Microsoft Entra ID
- C. Microsoft Intune
- D. Microsoft Intune

Answer: (SHOW ANSWER)

NEW QUESTION: 222

contoso.com is a Microsoft 365 ES tenant. user1@contoso.com is a member of the Admins group. User2 is a member of the Users group. User3 is a member of the Users group. User1 can reset the password of User3. User2 can reset the password of User3. User2 can reset the password of User1. Which Microsoft Defender (Office 365) tool can be used to configure the password reset policy for User1? (Select two.)

□□□□ □□□□□ □□□□□ □□ □□□.

Policy1 □ □□ □□□ □□ □□□?

- A. □□ □□□ □□□ □□□ □□□□□.
- B. □□□ □□□□ □□□□□.
- C. □□□ □□□ □□□□ □□□□□.
- D. □□□ □□□□□ □□□ □□□□□.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 223

Microsoft 365 E5 □□□ □□□□.

□□□□□□ □□□□ □□□□□□ □□□□ □□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

* □□□ □□□ □□ KQL □□□□□□.

* □□ 1□□ □□□ □□□□ □□□□□□.

□□□□□ □□□ □□□□ □□□?

- A. Microsoft 365 □□ □□
- B. □□□□□ □□
- C. Azure Monitor □□ □□
- D. Microsoft 365 Defender □ □□ □□□

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 224

□□ □□ □□ □□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

Microsoft Endpoint Manager □□ □□ □□ □□□ Office □ □□ □□□ □□□□.

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

□□□ □□ □□ □□□ □□□ □□□□□.

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

□□ □ □□□ □□ □□□ □□□□□ □□ □□□□□. □□□ □□□ □□□□ □□□□□.

□□□□: □□ □□□ 1□□□□.

Statements

Yes

No

User1 has their cache cleared on close.

User2 has Cursor movement set to Visual.

User3 has Cursor movement set to Visual.

Answer:

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

Explanation:

Statements

Yes

No

User1 has their cache cleared on close.

User2 has Cursor movement set to Visual.

User3 has Cursor movement set to Visual.

Reference:

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

NEW QUESTION: 225

Q: An organization has a hybrid environment with on-premises Active Directory and Azure AD. The organization wants to ensure that all users have the latest version of Office 365 applications. Which of the following actions should the administrator take to ensure that all users have the latest version of Office 365 applications?

A. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

B. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

C. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

D. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

E. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

F. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

G. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

H. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

I. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

J. Configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications and configure the Office 365 Group Policy Objects (GPOs) to update Office 365 applications.

10 users completed Azure AD Connect synchronization successfully. However, 10 user accounts are excluded from the synchronization cycle by a filtering rule. What is the most likely cause of this?

- A. The user accounts are not in the Azure AD Connect sync scope.
- B. The user accounts are excluded by a filtering rule.

Answer: B (LEAVE A REPLY)

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

Reference:

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

NEW QUESTION: 226

Microsoft Endpoint Manager is configured to sync user accounts from Microsoft Azure Active Directory (Azure AD). The following table shows the roles assigned to three users in Azure AD.

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

Endpoint Manager is configured with the following policies:

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

Which of the following statements are true? (Select all that apply.)

Microsoft Statements

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

Answer:
Answer Area

Microsoft Statements

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

Explanation:

□□□□: □□ □□□ 1□□□□.



Answer:



Explanation:



NEW QUESTION: 230

□□, □□, □□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Entra ID Protection □ □□□ □□□□.
□□ □□□□ □□□(VDI) □ □□□□. □□ VDI □□□ □□□ □□□□.
□□□□ □□□□ VDI □□□ Microsoft 365 □ □□□□□.
□□ VDI □□□□ □□ □□□ □□□□ □□ Microsoft 365 □ □□□□ □ □□□ □□□□□□.
VDI □□□□□ Microsoft □ □□□□□ □□ □□ □□□ □□□□ □□□ □□□.
365. □□□□ ID □□□ □□□□ VDI □□□ □□□□ □□□□ □□□.

- A. □□□ □ □□ □□
- B. □□□ □□□ □□
- C. □□ □□ □□
- D. Microsoft 365 □ ExpressRoute

Answer: A (LEAVE A REPLY)

NEW QUESTION: 231

Contoso.com is a Microsoft Azure Active Directory (Azure AD) tenant. Contoso.com is an ID provider for Microsoft Defender. Contoso.com is a member of the Defender for Identity Contoso Administrators group.

Name	Member of group	Azure AD role
User1	Defender for Identity Contoso Administrators	None
User2	Defender for Identity Contoso Users	None
User3	None	Security administrator
User4	Defender for Identity Contoso Administrators	Global administrator

User1 is a member of the Defender for Identity Contoso Administrators group. User2 is a member of the Defender for Identity Contoso Users group. User3 is a Security administrator. User4 is a Global administrator.

- A.
- B.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 232

500 Windows 10 devices are enrolled in the Windows 10 compliance policy. The policy is configured to require encryption of data storage on device. The policy is also configured to require firewall, Trusted Platform Module (TPM), antivirus, and antispypware. The policy is also configured to require Microsoft Defender Antimalware, Microsoft Defender Antimalware minimum version, Microsoft Defender Antimalware security intelligence up-to-date, and Real-time protection.

Answer Area

Windows 10 compliance policy
Windows 10 and later

Encryption

Encryption of data storage on device Require Not configured

Device Security

Firewall Require Not configured

Trusted Platform Module (TPM) Require Not configured

Antivirus Require Not configured

Antispypware Require Not configured

Defender

Microsoft Defender Antimalware Require Not configured

Microsoft Defender Antimalware minimum version Not configured

Microsoft Defender Antimalware security intelligence up-to-date Require Not configured

Real-time protection Require Not configured

Answer:

Answer Area

Windows 10 compliance policy

Windows 10 and later

Encryption		
Encryption of data storage on device	Require	Not configured

Device Security		
Firewall	Require	Not configured
Trusted Platform Module (TPM)	Require	Not configured
Antivirus	Require	Not configured
Antispyware	Require	Not configured

Defender		
Microsoft Defender Antimalware	Require	Not configured
Microsoft Defender Antimalware minimum version	Not configured	
Microsoft Defender Antimalware security intelligence up-to-date	Require	Not configured
Real-time protection	Require	Not configured

Explanation:

Windows 10 compliance policy
Windows 10 and later



Microsoft

Encryption

Encryption of data storage on device Require Not configured

Device Security

Firewall Require Not configured

Trusted Platform Module (TPM) Require Not configured

Antivirus Require Not configured

Antispyware Require Not configured

Defender

Microsoft Defender Antimalware Require Not configured

Microsoft Defender Antimalware minimum version Not configured

Microsoft Defender Antimalware security intelligence up-to-date Require Not configured

Real-time protection Require Not configured

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

NEW QUESTION: 233

□□□ □□□□□□ Azure Active Directory(Azure AD)□ □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

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

Azure Information Protection□ □□□□□.

Server1□ □□ □□□□ Azure Information Protection □□□□ □□□ □ □□□ □□□□ □□□.

□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□ □□□ □□□ □□□□□.

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

Answer:

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

Explanation:

Answer Area

Install the Microsoft Rights Management connector on Server2.

Authorize Server1.

Run GenConnectorConfig.ps1 on Server1.

Reference:

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

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

NEW QUESTION: 234

Microsoft 365 E5 □□□ □□□□.

□□ □□□□ iOS □□□ □□□□ □□□□.

Microsoft Endpoint Manager□ iOS □□□ □□□□□ □□□.

Microsoft Endpoint Manager□□ iOS/iPadOS □□ □□□□ □□ □ □□□ □□□□ □□□.

□□ □ □□ □□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□ □□□ □□ □□□□ □□□□□□.

ACTIONS

Answer Area

From the Microsoft Endpoint Manager admin center, add a device enrollment manager.

From the Microsoft Endpoint Manager admin center, download a certificate signing request.

Upload an Apple MDM push certificate to Microsoft Endpoint Manager

Create a certificate from the Apple Push Certificates Portal.

From the Microsoft Endpoint Manager admin center, configure device enrollment restrictions.

Answer:



Actions

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

Answer Area

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

Explanation:

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

Reference:

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

NEW QUESTION: 235

□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Type
Label1	Sensitivity
Label2	Retention

□□ □□ □□ □□ □□□ □□□□.

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

□□□ □□□□□ □□ □□□ □ □ □□□?

A. File1, File2, Mail1, Mail2

- B. File1 Mail
- C. File2 Mail2
- D. File1 File2
- E. File1

Answer: B (LEAVE A REPLY)

NEW QUESTION: 236

Microsoft 365 MFA Policy1 is configured to require MFA for all users. You need to ensure that users can access the application without MFA. What should you do?

- A. IP address of the application is added to the MFA Policy1.
- B. VPN is configured for the application.
- C. MFA is disabled for the application.
- D. MFA is disabled for all users.

Answer: (SHOW ANSWER)

NEW QUESTION: 237

You have an Azure AD tenant named contoso.com. The tenant contains two users, User1 and User2. User1 is a member of the Administrators group. User2 is a member of the Users group. You need to ensure that User1 can access the application without MFA. What should you do?

Name	UPN suffix
User1	Contoso.com
User2	Fabrikam.com

contoso.com Azure AD (contoso.com)

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

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

Azure AD Connect sync

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

USER SIGN-IN



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

User2 user2@fabrikam.com Azure AD

User2 Azure AD

Microsoft Entra User2 user2@contoso.com

?

A.

B.

Answer: B (LEAVE A REPLY)

This is not a permissions issue so you do not need to assign the Security Reader role.

The on-premises Active Directory domain is named contoso.com. User2 could sign on as user2@contoso.com but you would first need to change the UPN of User2 to user2@contoso.com.

NEW QUESTION: 238

Microsoft 365 Office 365 Microsoft Defender

Microsoft Defender for Office 365 is configured to protect the content of email messages in the Microsoft 365 E5 tenant. The DLP policy is configured to detect sensitive information and protect it. The DLP policy is configured to protect sensitive information in email messages. The DLP policy is configured to protect sensitive information in email messages. The DLP policy is configured to protect sensitive information in email messages.

Microsoft Defender for Office 365 is configured to protect the content of email messages in the Microsoft 365 E5 tenant. The DLP policy is configured to detect sensitive information and protect it. The DLP policy is configured to protect sensitive information in email messages. The DLP policy is configured to protect sensitive information in email messages. The DLP policy is configured to protect sensitive information in email messages.

- A. Rule1
- B. Rule2
- C. Rule3
- D. Rule4

Answer: B (LEAVE A REPLY)

NEW QUESTION: 239

Scenario

Site1 is a Microsoft SharePoint site. DLP1 is a DLP policy (DLP) in Microsoft 365 E5. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages.

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

Site1 is a Microsoft SharePoint site. DLP1 is a DLP policy (DLP) in Microsoft 365 E5. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages.

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

Site1 is a Microsoft SharePoint site. DLP1 is a DLP policy (DLP) in Microsoft 365 E5. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages.

Site1 is a Microsoft SharePoint site. DLP1 is a DLP policy (DLP) in Microsoft 365 E5. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages. DLP1 is configured to protect sensitive information in email messages.

Answer Area

File1.docx:

	▼
Rule1 tip only	
Rule2 tip only	
Rule3 tip only	
Rule1 tip and Rule2 tip only	
Rule1 tip, Rule2 tip, and Rule3 tip	

File2.docx:

	▼
Rule1 tip only	
Rule3 tip only	
Rule4 tip only	
Rule1 tip and Rule4 tip only	
Rule1 tip, Rule3 tip, and Rule4 tip	

Answer:

Answer Area

ile1.docx:

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

ile2.docx:

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

Explanation:

Answer Area

File1.docx:

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

File2.docx:

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

Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3.

Rule1 has the highest priority.

NEW QUESTION: 242

Microsoft 365 E5 □□□ □□□□.

Mailbox1□□□ □□□□ □□□□ □□ □□□ □□□□ □□□ □□□□□.

□□ □□ □□□ □□□□□ Office 365□ Microsoft Defender□ □□□□ □□□.

* Mailbox1□□ □□ □□□□ □□□□□ □□□□ □□□□□.

* □□□ □□ □□ □□ □□□□ □□ □□ □ □□□ □□□ □□□□□.

□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

Answer Area

Policies

- Anti-phishing
- Anti-spam
- Anti-malware
- Safe Attachments
- Safe Links

Rules

- Tenant Allow/Block Lists
- Email authentication settings
- DKIM
- Advanced delivery
- Enhanced filtering
- Quarantine policies



Answer:



Explanation:

Safe Attachments policy: This policy allows you to specify how to handle email attachments that might contain malware. You can create a custom policy for Mailbox1 and set the action to Do not scan attachments.

This will ensure that incoming email is not filtered for Mailbox1. You can also enable the Redirect attachment option to send a copy of the original attachment to another mailbox for analysis1.

Anti-phishing policy: This policy helps you protect your organization from impersonation and spoofing attacks. You can create a default policy for all other mailboxes in the subscription and enable the following features: Impersonation protection, Spoof intelligence, and Domain authentication. These features will help you detect and block emails that try to impersonate your users, domains, or trusted senders2.

NEW QUESTION: 243

Q: A user reports that they cannot access their email in Outlook. The user is using Windows 10 and Outlook 2019. The user's email account is configured correctly, and the user can access their email in a web browser. What should you do to resolve the issue?

A. Verify that the user's Outlook profile is configured correctly.

B. Verify that the user's Outlook profile is configured correctly.

C. Verify that the user's Outlook profile is configured correctly.

D. Verify that the user's Outlook profile is configured correctly.

E. Verify that the user's Outlook profile is configured correctly.

A.

B.

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 244

Microsoft 365 Defender alerts are categorized by severity and status.

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

Which alert is categorized as a threat management alert?

- A. Alert1
- B. Alert2
- C. Alert1 and Alert2
- D. Alert1, Alert2, and Other
- E. Alert1, Alert2, and Threat management

Answer: (SHOW ANSWER)

Reference:

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

NEW QUESTION: 245

Microsoft 365 Defender alerts are categorized by severity and status.

Microsoft Office 365 Admin messages are categorized by severity and status.

Which message is categorized as a threat management alert?

Which message is categorized as a threat management alert?

Which message is categorized as a threat management alert?

- A. Microsoft 365 Defender alerts are categorized by severity and status.
- B. Microsoft 365 Defender alerts are categorized by severity and status.
- C. Microsoft 365 Defender alerts are categorized by severity and status.
- D. Microsoft 365 Defender alerts are categorized by severity and status.

Answer: (SHOW ANSWER)

The Message center in the Microsoft 365 admin center is where you would go to view a list of the features that were recently updated in the tenant. This is where Microsoft posts official messages with information including new and changed features, planned maintenance, or other important announcements.

The messages displayed in the Message center can also be viewed by using the Office 365 Admin mobile app.

Reference:

<https://docs.microsoft.com/en-us/office365/admin/manage/message-center>

<https://docs.microsoft.com/en-us/office365/admin/admin-overview/admin-mobile-app>

NEW QUESTION: 246

Site1 is a Microsoft SharePoint site. Site2 is a Microsoft 365 E5 tenant. Site1 is connected to Site2.

* Site1 is connected to Site2. Site1 is connected to Site2.

* SIT10 0000 00 0 000 00000 00000.

Microsoft Purview 00 00 0000 00 0 00 000 0000 000? 00000 00 0000 000 000 000000.

0000: 00 000 10000.

Answer Area



- Insider risk management
- Records management
- Privacy risk management
- Subject rights requests

Answer:

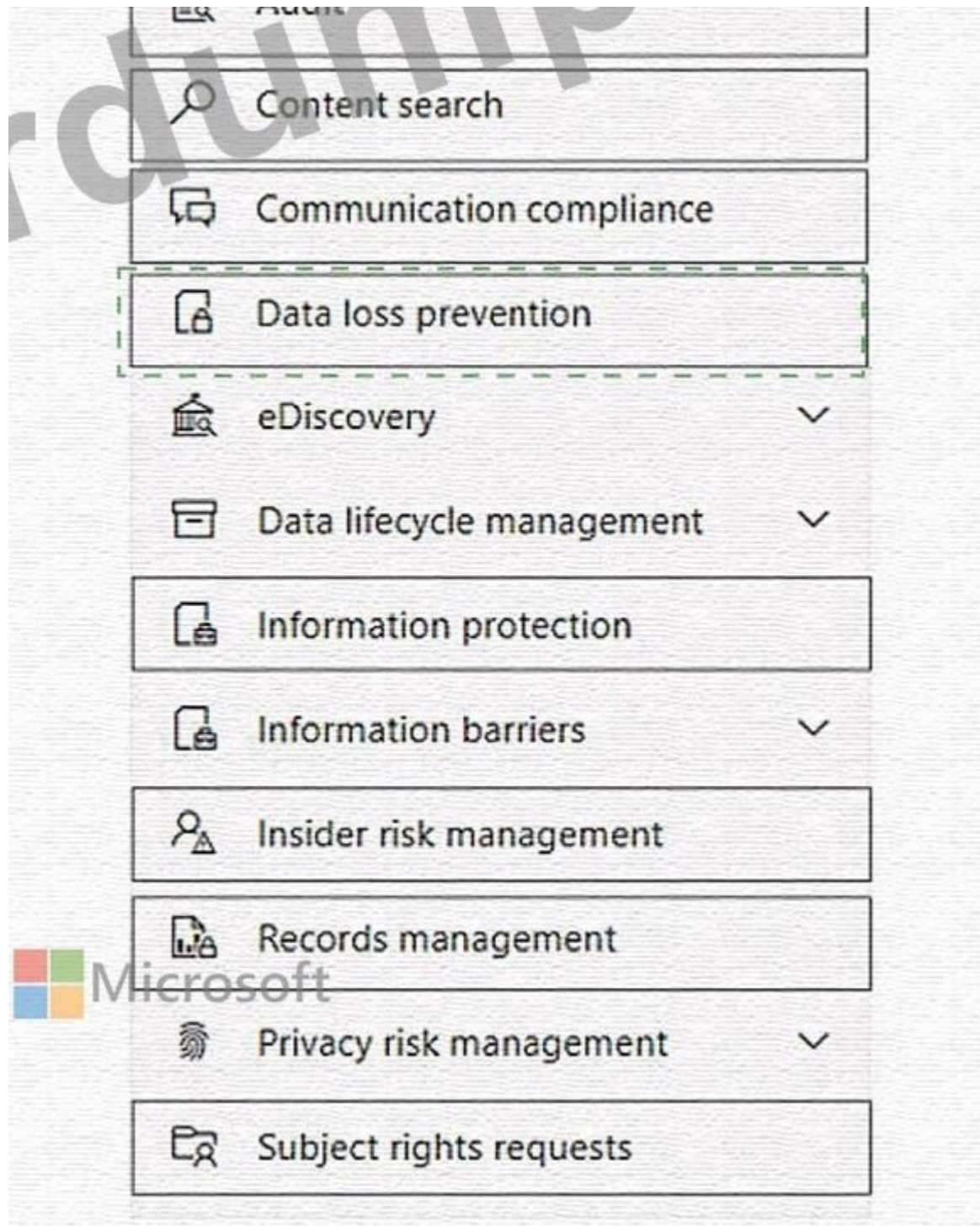
Answer Area

Microsoft Purview

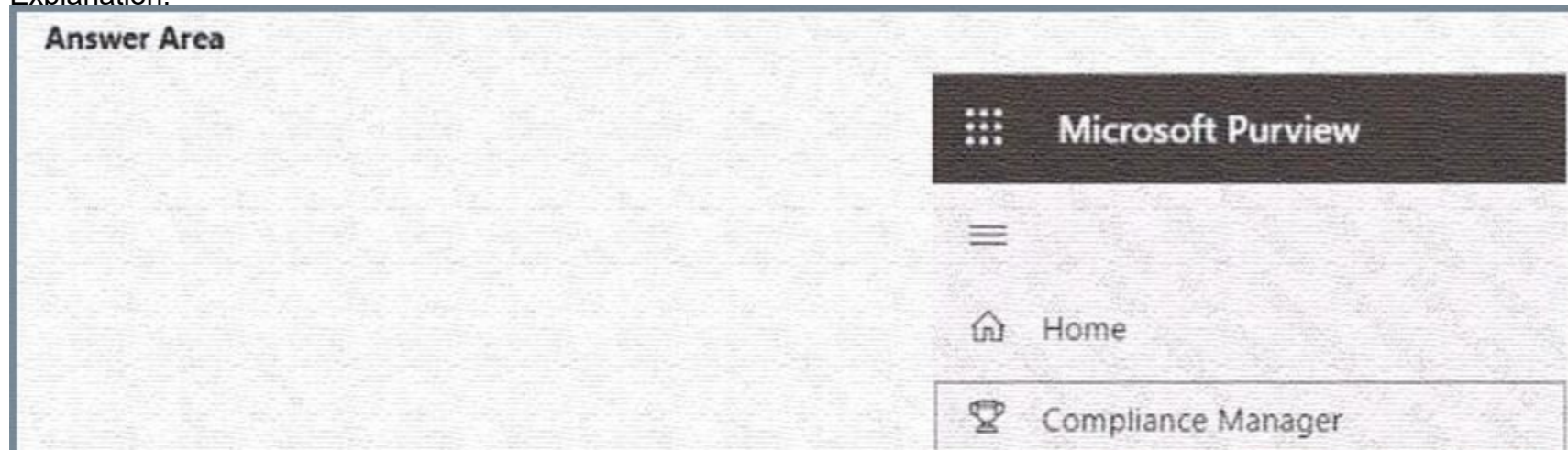
- Home
- Compliance Manager
- Data classification
- Data connectors**
- Reports

















Solutions

- Catalog
- App governance
- Audit



Explanation:



-  Data classification
-  Data connectors
-  Reports
- Solutions**
-  Catalog
-  App governance
-  Audit
-  Content search
-  Communication compliance
-  Data loss prevention
-  eDiscovery
-  Data lifecycle management
-  Information protection
-  Information barriers
-  Insider risk management
-  Records management
-  Privacy risk management
-  Subject rights requests

□□□ □□□□ □□ □□ □□□□ □□□□.

Microsoft Intune □ □□ □□□ □□□□ Microsoft 365 E5 □□□□ □□□□. □ □□□□□ □□ □□□□ □□□□.
□□ □□□□ □□ □□□□ □□ □□□ □□□ □ □□□ □□ □□□□.
□□□ □□□□ □□□□?

- A. □□ □□
- B. □□ □□□
- C. □□ □□□□
- D. □□□ □□□ □□

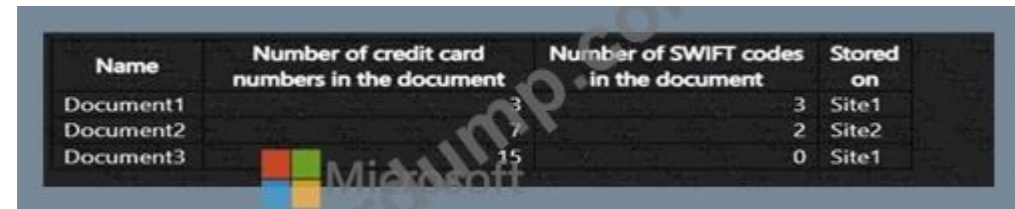
Answer: A (LEAVE A REPLY)

Reference:

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

NEW QUESTION: 248

□□□ Site1 □ Site2 □□ □□□ Microsoft SharePoint Online □□□ □ □□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□ □□ □□ □□ □□ □□□□ □□□ □□□□.



Name	Number of credit card numbers in the document	Number of SWIFT codes in the document	Stored on
Document1	3	3	Site1
Document2	2	2	Site2
Document3	15	0	Site1

) □□□ □□□□□.

Sensitive info types

Credit Card Number	Low confidence	Instance count	1	to	5
SWIFT Code	Low confidence	Instance count	1	to	2

Add

OR

Group name * Group operator

Sensitive info types

Credit Card Number	Low confidence	Instance count	10	to	Any
--------------------	----------------	----------------	----	----	-----


Add

Evaluate predicate for (available for Exchange workload only)

Message or attachment Message only Attachments only

Create group

Save Cancel



Create rule

Content contains

Group name * Group operator

If you specify "All of these" for the "Content contains" condition, you can't add more than one retention label and one sensitivity label to a group. This is because emails and documents can have only one retention label and one sensitivity label assigned to them at a time.

Sensitive info types

Credit Card Number Instance count to

SWIFT Code Instance count to

Add

Group name * Group operator

Sensitive info types

Credit Card Number Instance count to


□□ □ □□□ □□, □□□ □□□□ '□' □□□□, □□□ □□□ '□□□□' □ □□□□□□□.
□□: □□ □□□ 1□□□□.

Statements	Yes	No
DLP1 applies to Document1.	<input type="radio"/>	<input type="radio"/>
DLP1 applies to Document2.	<input type="radio"/>	<input type="radio"/>
DLP1 applies to Document3.	<input type="radio"/>	<input type="radio"/>

Answer:

□□□□: □□ □□□ 1□□□□.

Answer Area



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

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

Answer:
Answer Area



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

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

Explanation:


```

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

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

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

PS C:\>

```

0000 0000 0000 0000 0000 0 00000 00000 00 00000 00000 0000 00000 000000. 0000 00 100000.

Answer Area

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

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

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

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

Answer:

Answer Area

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

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

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

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

Explanation:

Answer Area

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

If User2 adds a channel in Microsoft Teams, the event is [answer choice] retained for 90 days

MS-102-KR ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ MS-102-KR ☐☐! DumpTop ☐ ☐☐ **MS-102-KR** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop MS-102-KR ☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop MS-102-KR ☐☐☐ ☐☐☐☐☐. <https://www.dumptop.com/Microsoft/MS-102-KR-dump.html> (572 Q&As Dumps, **30%OFF Special Discount: KrDump**)