

Microsoft.MS-101.v2022-10-08.q216

□□□□:	MS-101
□□□□:	Microsoft 365 Mobility and Security
□□□:	Microsoft
□□ □□ □□□:	216
□□:	v2022-10-08
# □□ □:	2511
# □□ □□□:	2160
https://www.krdump.com/Microsoft.MS-101.v2022-10-08.q216.html	

NEW QUESTION: 1

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

□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□□□ □□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□ Active Directory □□□□ □□□□.

Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□ □□ □□□.

□□□ □□ □□□ □□□□□.

Device1□□□ □ □□□ □□□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.

Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □ □□.

□□□: □□ □□ □□ □□□□ □□ □□ □□□□ □□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: ([SHOW ANSWER](#))

□□: [□□]

NEW QUESTION: 2


Microsoft 365 □□□ □□□□□.

□□□□□ 51.40.15.0/24□ IP □□ □□□ □□□□□.

Exchange Online □□□□ □□□ □□□□□ □□□□□□ Role1□□□ □□□ □□□□□□□.

□□ □□ □□□ □□ □□□□ □□□ □□□□ □□□.

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

Activities to search for:  Microsoft ▼

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

Field to filter by: ▼

Item
User
Detail
IP address


Answer:

Activities to search for: ▼

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

Field to filter by: ▼

Item
User
Detail
IP address



NEW QUESTION: 3

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

Microsoft 365 □□□ □□□□□.

You can open File1 from:

- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

□□

You can open File1 from:

- App1 only
- App1 and App2 only
- App1 and App3 only
- App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

- App1 only
- App3 only
- App1 and App2 only
- App2 and App3 only
- App1, App2, and App3

NEW QUESTION: 5

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

Name	Role
User1	Global admin
User2	None
User3	None

□□□□□ Microsoft Store□□ □□ □□□□ □□□□□□□□.

Microsoft Store permissions.

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

Microsoft Store permissions. Can add apps to the private store? Can assign apps from Microsoft Store for Business? Options: User2 only, User1 and User2 only, User2 and User3 only, User1, User2, and User3.

Can add apps to the private store: [Microsoft logo] ▼
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

□□:

<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: 6

Microsoft 365

Name	Role
User1	Exchange administrator
User2	Security administrator
User3	None

cmdlet

```
Set-MailboxAuditBypassAssociation -Identity User2
-AuditByPassEnabled $true
```

* User1

* User2

* User3

Microsoft Statements	Yes	No
The action performed by User1 is audited.	<input type="radio"/>	<input type="radio"/>
The action performed by User2 is audited.	<input type="radio"/>	<input type="radio"/>
The action performed by User3 is audited.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
The action performed by User1 is audited.	<input checked="" type="radio"/>	<input type="radio"/>
The action performed by User2 is audited.	<input type="radio"/>	<input checked="" type="radio"/>
The action performed by User3 is audited.	<input checked="" type="radio"/>	<input type="radio"/>

Statements

Yes No

The action performed by User1 is audited.

The action performed by User2 is audited.

The action performed by User3 is audited.

□□:

<https://docs.microsoft.com/en-us/powershell/module/exchange/set-mailboxauditbypassassociation?view=exchan>

NEW QUESTION: 7

Microsoft 365 E5 □□□ □□□□.

□□□□ □□ □□ □□□ □□□ □□□ □□□□.

Name	Platform	Owner	Enrolled in Microsoft Endpoint Manager
Device1	Android	User1	Yes
Device2	Android	User1	No
Device3	iOS	User1	No
Device4	Windows 10	User2	Yes
Device5	Windows 10	User2	No
Device6	iOS	User2	Yes

Microsoft Endpoint Manager □ □ □□ □□□□ □□ □□□□ □□ □□□ □ □□□□?

- A. □□1, □□4 □ □□6
- B. □□2, □□3 □ □□5
- C. □□1, □□2, □□3 □ □□6
- D. □□1, □□2, □□4 □ □□5

Answer: C (LEAVE A REPLY)

□□

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

□ iOS/iPadOS □□ Android □ □□□ □□ □□ □□□ □□□ □ □□□□.

□□:

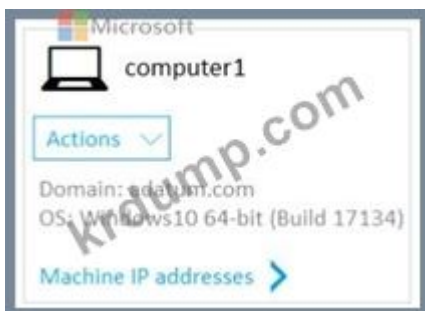
<https://docs.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview>

NEW QUESTION: 8

□□□□ Microsoft Defender ATP(Advanced Threat Protection)□ □□□□□. Microsoft Defender ATP□□ □□ □□ □□□ □□□ □□□□□□.

Rank	Machine 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 machines (default)	Not applicable

□□ □□□ □□ □□□ 1□□□ □□□□ Microsoft Defender ATP□ □□□□□□.



□□□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only
- Ungrouped machines

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 machines

Answer:

Computer1 will be a member of [answer choice].

- Group3 only
- Group4 only
- Group3 and Group4 only**
- Ungrouped machines

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 machines

NEW QUESTION: 9

You are a system administrator for a company that has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. The company has a Microsoft Store application named App1. App1 is used by the finance department and the sales department. App1 is used by 20 users. App2 is used by the marketing department. App2 is used by 100 users.

The company is planning to upgrade its Windows 8.1 computers to Windows 10. The company has 2,000 computers.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

You need to identify the applications that are used by the finance department and the sales department.

App1 App2 UpgradeDecision

App1 ReadyForWindows

Which application is used by the finance department and the sales department?

A. App1

B. App2

Answer: B (LEAVE A REPLY)

App1 "ReadyForWindows" (2% of users) is used by the finance department and the sales department. App2 is used by the marketing department.

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

NEW QUESTION: 10

You are a system administrator for a company that has a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com. The company has a Microsoft Store application named App1. App1 is used by the finance department and the sales department. App1 is used by 20 users. App2 is used by the marketing department. App2 is used by 100 users.

The company is planning to upgrade its Windows 8.1 computers to Windows 10. The company has 2,000 computers.

You need to identify the applications that are used by the finance department and the sales department.

Name	Microsoft Store for Business role	Azure AD role
User1	Purchaser	None
User2	Basic Purchaser	None
User3	None	Application administrator
User4	None	Cloud application administrator

You need to identify the applications that are used by the finance department and the sales department.

* App1 App2 UpgradeDecision

* App1 ReadyForWindows

App1 App2 UpgradeDecision

App1 ReadyForWindows

A. App1 App2

B. User1 App2

C. User3 App2

D. User3 App2

Answer: (SHOW ANSWER)

NEW QUESTION: 11

contoso.com Azure AD(Azure Active Directory) Microsoft 365 E5

Microsoft Endpoint Manager Microsoft Endpoint Manager

DNS ?

:

- A. AutoDiscover.contoso.com CNAME
- B. EnterpriseEnrollment.contoso.com CNAME
- C. EnterpriseRegistration.contoso.com TXT
- D. _SIP._TLS.contoso.com SRV
- E. _SIPfederationTLS.contoso.com SRV
- F. EnterpriseRegistration.contoso.com CNAME
- G. EnterpriseEnrollment.contoso.com TXT

Answer: (SHOW ANSWER)

:[]

/:

<https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#simplify-windows-enrollment-without-azure-ad-premium>

NEW QUESTION: 12

Microsoft 365

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1 Policy1

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 7 years

No, just delete content that's older than ⓘ

2 years

Delete the content based on when it was created ⓘ

Need more options?

Use advanced retention settings ⓘ

Microsoft

Policy2 Policy2 . (

□□ □□□ □□□ □□ □□□□□.

* □□□ □ □□: Group1

* □□□□ □: Microsoft Office 365 Exchange Online

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

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

Yes

No

User1 can access Microsoft Exchange Online from Device1.

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 14

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

Exchange Online□ □□□□ □□□ □□□□□.

Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

The screenshot shows the 'New' policy configuration page in Microsoft Intune. The 'Conditions' section is highlighted with a red box. The 'Device state (preview)' section shows 'Device marked as compliant' selected.

Conditions

- 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)

Configure: Yes (selected) No

Include Exclude

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

- Device Hybrid Azure AD joined
- Device marked as compliant

Answer:

The screenshot shows the 'New' policy configuration page in Microsoft Intune. The 'Conditions' section is highlighted with a red box.

Conditions

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

□ □



NEW QUESTION: 15

Microsoft 365 E5. The following table shows the user assignments for the policy.

Name	Member of
User1	UserGroup1
User2	UserGroup2
User3	UserGroup3

The following table shows the device state for the policy.

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

The following table shows the app assignments for the policy.

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

Microsoft Endpoint Manager. The following table shows the policy configuration.

The policy is assigned to all users. The policy is assigned to all devices. The policy is assigned to all devices. The policy is assigned to all devices.

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

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"/>

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

NEW QUESTION: 16

□□□□ Windows Defender ATP(Advanced Threat Protection) □ □□□□□. Windows Defender ATP □□ □□ □□ □□□ □□□ □□□ □□□□ □□□□.

Rank	Machine 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 machines (default)	Not applicable

□□ □□□ □□ □□□ 1□□□ □□□□ Windows Defender ATP □ □□□□□□.

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

Name	Number of IP addresses in the file
File1.docx	1
File2.txt	3
File3.docx	2
File4.bmp	3
File5.docx	3

Site1 □□□□□□ □□ □□ □□□ □□□□□□.

Name	Role
User1	Contrib
User2	Visitor

□□ □□□ □□ DLP(Dataless Prevention) □□ □□ Policy1□ □□□□.



□□'□ □□□ □□□ □ user1□ User2□ □ □ □□ □□□ □□ □□□□ □□ □□□□ □□□ □□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:

If you copy the file to your local computer, you [answer choice].

If you email the document to a user outside your organization, the user [answer choice].

cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

cannot open the document
can open the document indefinitely
can open the document for up to 7 days
can open the document for up to 30 days

□□

krdump.com

Use 1: 3

Use 2: 2



NEW QUESTION: 18

contoso.com is a Microsoft 365 tenant. The following table shows the user and group membership information.

Name	Member of
User1	Group1
User2	Group1, Group2

The following table shows the compliance status of the devices.

Name	Compliance status
Device1	Compliant
Device2	Noncompliant

App1 is an application that is protected by the following Conditional Access policies.

Name	Includes	Excludes	Device state includes	Device state excludes	Grant
Policy1	Group1	None	All device states	Device marked as compliant	Block access
Policy2	Group1	Group2	None	None	Block Access
Policy3	Group1	None	All device states	None	Grant access

Which of the following statements are true? Select all that apply.

Statements	Yes	No
User1 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can access App1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from Device1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

□□:

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

NEW QUESTION: 19

Azure □□□ □□□□□ Active Directory □□□□ □□□□. □□□□□ Windows 10□ □□□ □ 50□□ □□□□ □□□□. □□□□ □□ □□ □□□□ □□□□ □□□□□ □□□. □□□ □□□□□□□□? □□□□□ □□ □□□□ □□□ □□□□□□□□. □□: □ □□□ □□□ 1□□ □□□ □□□□□.

In Azure:

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

On the computers:

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

Answer:

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

□□:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer>

NEW QUESTION: 20

Microsoft 365 □□□ □□□□.

User1 □□□ □□□□ Microsoft Exchange Online □ □□□□ □□□□.

User1 □ □□□ □□ □□□ □□ □□ □□□□ □□□.

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

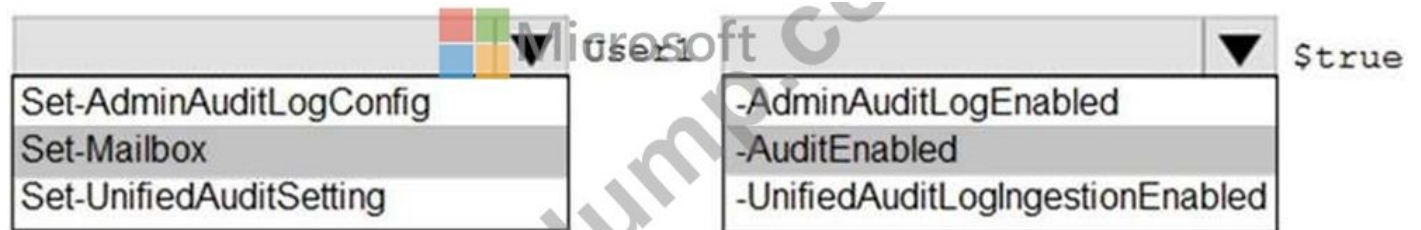
□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□



□□ □□□(□ □□□□ Holly Sharp □ □□) □ □□ □□□ □□□□□□ □□ PowerShell □□

□ □□□□□. Set-Mailbox username -AuditEnabled \$true

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins>

[https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?](https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps)

view=exchange-ps

NEW QUESTION: 21

□□ □□ □□□ □□□□ □□□ Microsoft Azure □□ □□□□(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3 □ Group1 □ □□□□□□.

□□□□ Windows Defender ATP(Advanced Threat Protection) □ □□□□□. Windows

Defender ATP □□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	None

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>

Answer:

statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 22

□□:

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

NEW QUESTION: 25

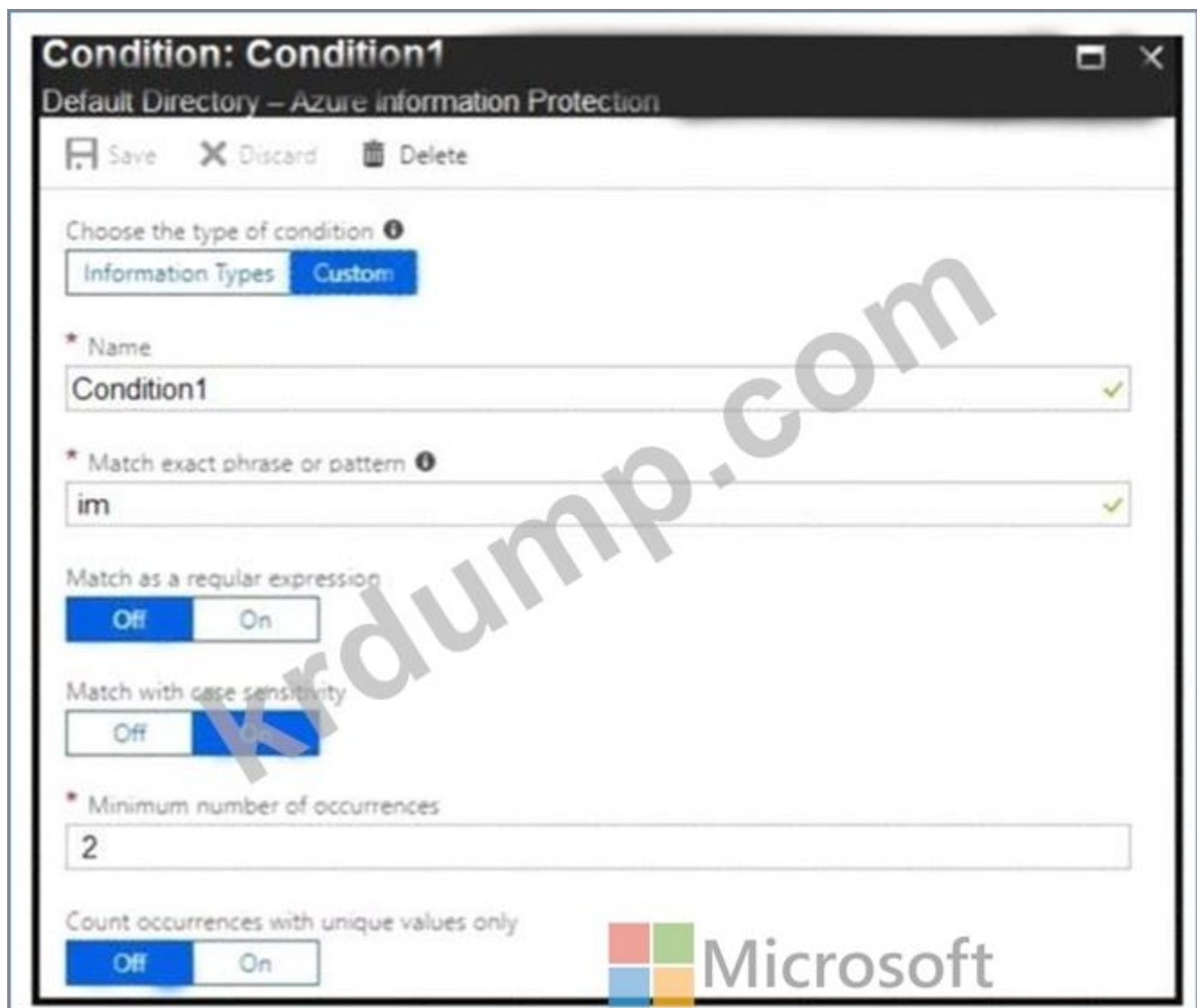
contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

User1□□□ □□□□ □□ □□ □□ Windows 10 □□□ □□□ □□□□.

Name	Text in file
File1.docx	Importing and exporting is easy. For import, you need a source, and for export, you need a destination.
File2.docx	You must declare what you want to import. Dangerous items cannot be imported. If you want to import valuables, you must pay customs.
File3.docx	IM are initials for instant messaging. You can use Microsoft Skype for IM, but there are also other IM programs.

Azure Information Protection□□ □□□□ □□□□□□ □□□ Label1□□□□ □□□□ □□□□.

Label1□ □□□ □□ □□□□□□.



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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Label1 applies to File1.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Label1 applies to File2.docx.	<input type="radio"/>	<input checked="" type="radio"/>
Label1 applies to File3.docx.	<input checked="" type="radio"/>	<input type="radio"/>

□□

Statements	Yes	No
Label1 applies to File1.docx.	<input type="radio"/>	<input checked="" type="radio"/>
Label1 applies to File2.docx.	<input checked="" type="radio"/>	<input type="radio"/>
Label1 applies to File3.docx.	<input type="radio"/>	<input checked="" type="radio"/>

□□□□ □□□ "im"□□ □□□□□ □□□□□. □□ □□ □□□ □ □ □□□□ □□□.

□□ 1: □□□

File1.docx□□ "□□□□"□□ □□□ □ □□ □□□□□.

□□ 2: □

File2.docx□□ "import"□□ □□□ "imported"□□ □□□ □ □ □□ □□□□. □□ 3: □□□

File3.docx□□ "IM"□ □□□□ □□□ □□□□□ □□□□ □□□□.

□□:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

NEW QUESTION: 26

Microsoft 365 □□□ □□□□.

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

User1□□□ □□□□ □□□□□ Project X□□ □□□ □□□ □□ □□ □□ □□□□ □□□□ □□□□ □□□.

□□ □□□ □□ □□□?

- A. □□ □ □□ □□ □□ □□□□ □□□ □□ □□(DLP) □□□ □□□□.
- B. □□ □ □□ □□ □□ □□□□ □□□ □ □□□ □□□ □□□□.
- C. □□ □ □□ □□ □□ □□□□ □□□ □ □□□ □□□ □□, □□□□□.
- D. □□ □ □□ □□ □□ □□□□ □□□ □□□ □□□□□.
- E. Exchange □□ □□□□ □□ □□ □□□ □□ □□

Answer: (SHOW ANSWER)

DLP □□□□ □ □□ □□ □□□ □□□□□.

□□□□ □□□ □□: Exchange Online, SharePoint Online □ □□□□□ OneDrive □□□□ □

□ □□□ Microsoft Teams □□ □ □□ □□□.

□□□□ □□□ □□□ □□□□ □□□□ □□□□ □□□ □□:

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

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

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

□□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□ □□□ □□□□ □□□ □□□

□ □□□□.

□□:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/data-loss-prevention-policies>

NEW QUESTION: 27

500□□ Windows 10 □□□ Windows 10 □□ □□ □□□ □□□□ Microsoft 365 E5 □□□□ □□□□.

□□□□ □□ □□□□ □□ □□□□ □□□□□.

□□□□ □□□□ □□□ □□□□ □□□ □□□□ □□□.

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

□□: □ □□□ □□□□ 1□□ □□□ □□□□□.

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-do-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-do-date	Require	Not configured
Real-time protection	Require	Not configured

□□:

<https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows>

NEW QUESTION: 28

□□ □□ □□□ □□□ Microsoft Azure ATP(Advanced Threat Protection) □□ □□□ □□□ □. (□□ □□ □□ □□□□□.)



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



Azure ATP □ □□□□ □□□□ □□□□□ □□□□ □□□.
 □□ □ □□ □□□ □□□□ □□□□ □□□? □□□□□ □□ □□□□ □□ □□□ □□ □□
 □□ □□□□ □□□ □□□ □□□□□□□.

Actions	Answer Area
Modify the integration setting for the workspace.	
Delete the workspace.	
Regenerate the access keys.	
Create a new workspace.	
Modify the Azure ATP user roles.	

Answer:

Actions	Answer Area
Modify the integration setting for the workspace.	Delete the workspace.
Delete the workspace.	Create a new workspace.
Regenerate the access keys.	Regenerate the access keys.
Create a new workspace.	
Modify the Azure ATP user roles.	

□□:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step1>

NEW QUESTION: 29

□□□□ Microsoft Defender ATP(Advanced Threat Protection) □ □□□□□. Microsoft Defender ATP □□ □□ □□ □□□ □□□ □□□ □□□□□.

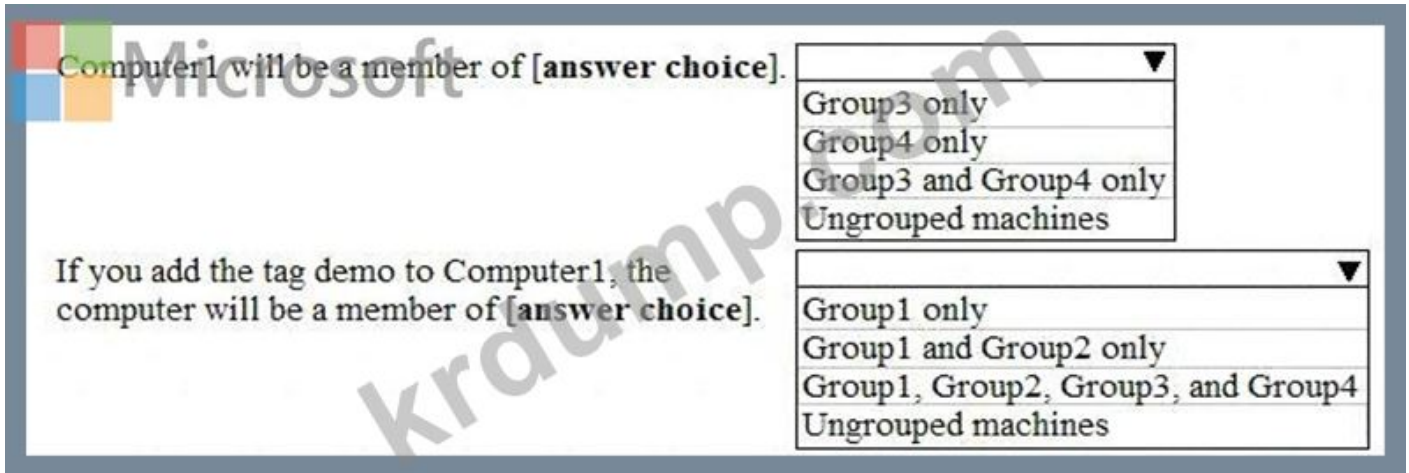
Rank	Machine group	Members
1	Group1	Tag Equals demo And OS In Windows 10
2	Group2	Tag Equals demo
3	Group3	Domain Equals adatum.com
4	Group4	Domain Equals adatum.com And OS In Windows 10
Last	Ungrouped machines (default)	Not applicable

□□ □□□ □□ □□□ 1□□□ □□□□ Microsoft Defender ATP □ □□□□□□.

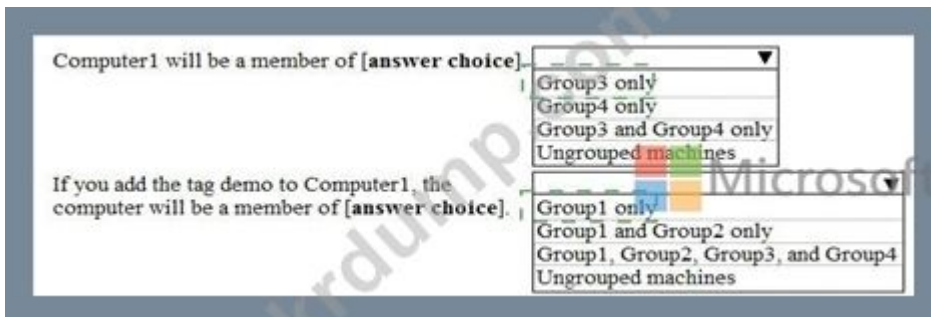


□□□□ □□□ □□□□ □ □□□ □□□□ □□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□

□ □□□ □□□

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

- □□□ □□ □□□□ □□□□ □□ □□ □□ □□ □□□□ □□□□□□. □□ 1□ □□

□ - □□□ 1□ □□ 3□ □□□□□□ □□□.

□□ □□ □□□ □□□ adatum.com □□ 2□ □□□□ □□□ - □□□ 1□ □□ □□□ □□□

□ □□□ □□ 1□□ □□□ □□□.

□□□□ "□□"□□ □□□ □□□□ □□ OS□ Windows 10□□ □□□□□.

NEW QUESTION: 30

□□□□ Microsoft System Center Configuration Manager(□□ □□) □ Microsoft Intune□ □□ □□ □□□ □□ □□□□□.

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

- A. Windows 10 □□□ □□□□□□□ □□□□□.
- B. iOS □□□ VPN □□□□ □□□□□.
- C. Windows 10 □□□ VPN □□□□ □□□□□.
- D. Android □□□ □□□□□□□ □□□□□.

Answer: B,D (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/sccm/comanage/overview>

<https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles>

NEW QUESTION: 31

□□□ contoso.com□□□ Azure AD(Azure Active Directory) □□□□ □□□□ Microsoft 36S □□□ □□□□. □ □□□ SharePoint Online □□ □□□□□□ 2TB□ □□□□ □□□□□. □□□□□ □□ □□ □□□ □□□□ □□□□.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

Azure Portal□□ □□ □□□ □□□ □□□□□□□□.

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

Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area



Label1 can now be used as a sensitivity label or an Azure Information Protection label.

Yes

No

Label2 can now be used as a retention label or an Azure Information Protection label.

Label3 can now be used as a sensitivity label or an Azure Information Protection label.

□□



Label1 can now be used as a sensitivity label or an Azure Information Protection label.

Label2 can now be used as a retention label or an Azure Information Protection label.

Label3 can now be used as a sensitivity label or an Azure Information Protection label.

MS-101 ... DumpTop ... MS-101 ...! DumpTop ... MS-101 ... MS-101 ... DumpTop MS-101 ... MS-101 ... DumpTop MS-101 ... <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps, 30%OFF Special Discount: KrDump)

NEW QUESTION: 32

Azure AD(Azure Active Directory) ... Microsoft 365 E5 ... Group1

Name	Role
Admin1	Conditional Access administrator
Admin2	Security administrator
Admin3	User administrator

...

□□: □□1

□□:

- □□□ □ □□: Group1

- □□□□ □ □□ □□: □□ □□□□ □

□□□ □□:

□□, □□□ □□ □□

□□ □□: □□ □□

□□□□ □□ Enabled Security □□□□ Yes□ □□□□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

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"/>

□□:

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

NEW QUESTION: 33

□□□ Microsoft 365 □□□ □□□□.

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

* □□□ □□□□□□ □□□ □□□□□ 20□ □□ □□□□□ □□□.

* □□□ □□□ □□□□ □□□ □□□ □□□□ □□□.

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

□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area



Answer:

Answer Area



NEW QUESTION: 34

Microsoft 365 .

iPad .

ipad Microsoft Word

?

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

Answer: ([SHOW ANSWER](#))

:

<https://docs.microsoft.com/en-us/intune/app-protection-policy>

NEW QUESTION: 35

Microsoft Azure Active Directory(Azure AD) .

Name	Member of
User1	Group1
User2	Group2

Microsoft Intune .

Intune .

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3.
Policy2	Require	Group4

□□ □□□ □□ □□□ □□□ □□□□□.

□□ □□□ □□□ □□ □□□□□.

□□□ □ □□: Group1

□□□□ □: Microsoft Office 365 Exchange Online

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

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

Yes

No

User1 can access Microsoft Exchange Online from Device1.

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

Answer:

Statements

Yes

No

User1 can access Microsoft Exchange Online from Device1.

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

NEW QUESTION: 36

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

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

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

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

□□□ □□□□ □□□□.

Microsoft 365 E5 □□□ □□□□.

SecAdmin1□□□ □ □□ □□□□ □□□ □□□□.

SecAdmin1 Microsoft Teams, SharePoint OneDrive Office 365 Microsoft Defender

Microsoft 365 SecAdmin1 Exchange

A.

B.

Answer: B (LEAVE A REPLY)

https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/office-365-atp?view=o365-worldwide

NEW QUESTION: 37

(DLP) (ICD-9-CM)

DLP (ICD-9-CM)

Content contains

Any of these ▾

PII Identifiers

Sensitive info type

U.S. Social Security Number (SSN)

Instance count

min 1 max any

Match accuracy

min 50 max 100

Add ▾

and ▾

Any of these ▾

Medical Terms

Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count

min 1 max any

Match accuracy

min 50 max 100

Add ▾

Answer:

Content contains

Any of these ▾

PII Identifiers
Sensitive info type

U.S. Social Security Number (SSN)

Instance count: min 1, max any

Match accuracy: min 50, max 100

Add ▾

and ▾

Any of these ▾


Medical Terms
Sensitive info type

International Classification of Diseases (ICD-9-CM)

Instance count: min 1, max any

Match accuracy: min 50, max 100

Add ▾



□□: [□□]

□□/□□:

□□:

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

<https://docs.microsoft.com/en-us/office365/securitycompliance/what-the-sensitive-information-types-look-for#international-classification-of-diseases-icd-9-cm>

NEW QUESTION: 38

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

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

Microsoft Azure ATP(Advanced Threat Protection)□ □□□□ □□□ □□□□□ □□□□□□□ □□□.

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

- A. Azure ATP □□□ □□□ □□ □□ □□□□ □□□□□□.
- B. Azure ATP □□□ □□□ □□ □□□ □□□□□□.
- C. Azure ATP □□ □□□ □□□ □□□ □□ □□□ □□□□□□.
- D. Azure ATP □□ □□□ □□□ □□□ □□ □□ □□□□ □□□□□□.

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

□□/□□:

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5>

NEW QUESTION: 39

□□□□□ contoso.com□□□ □-□□□□ Active Directory □□□□ □□□□ □□□□. □□□ □□ 1,000□□ Windows 10 □□□ □□□□ □□□□.

10□□ □□□ □□□ □□ Windows Defender ATP(Advanced Threat Protection)□ □□ □□ (PoC) □□□ □□□□□. □□□ □□□□ □□ Windows Defender ATP □□ □□□□ □□□ □□□□□ □□□□□.

□□ □□□ Windows Defender ATP□ □□□□ □□□□□.

□□□□ Windows Defender ATP □□□□ □□□□ □□□.

□□□ □□ □□ □□□?

A. □ □□□ □□□□□□.

B. □□ □□□ □□□□.

C. □□□ □□□ □□□□□□□.

D. □□ □□□ □□□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 40

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□ Active Directory □□□□□ □□□□ □□□□.

□□ □□□ □□ Microsoft System Center Configuration Manager(□□ □□)□ □□□□□.

□□ □□ □□□ Windows 10 □□□ □□□□.

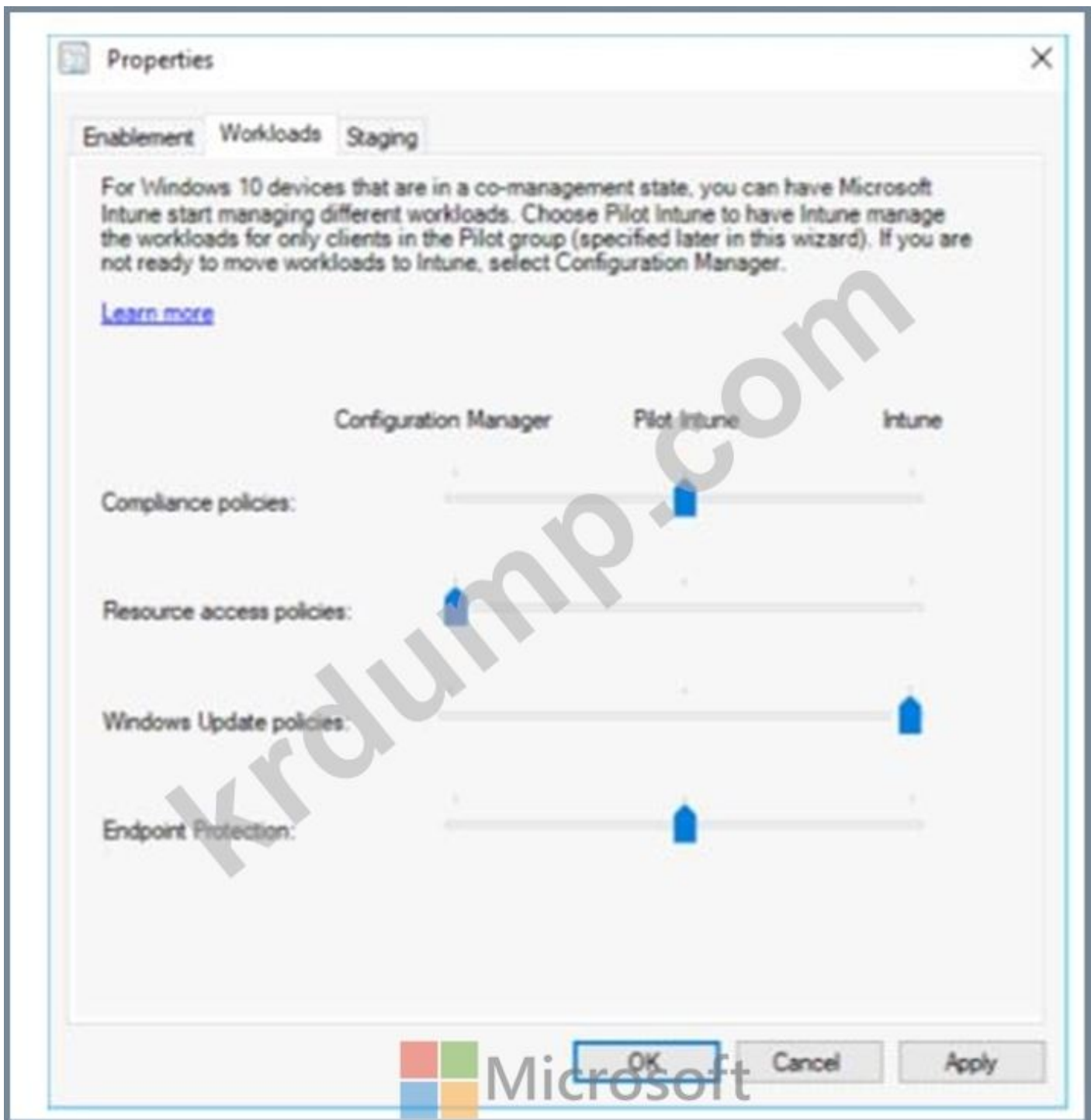
Name	Collection
Device1	Collection1
Device2	Collection2

□□□ □□ Configuration Manager □□ □□□ □□□□□.

Intune□ □□ □□: □□□

□□□ □□□: Collection2

□□ □□□ □□ □□ □□ □□□□□ □□□□□.



00 0 00 00 00 00 000 00 00000. 000 000 0000 00000.
 00: 0 000 000 100 000 0000.

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 41

contoso.com Azure AD(Azure Active Directory) Microsoft 365 .

User1 Group1 .

User1 Group1 .

User1 Group1 .

User1 Group1 .

.

?

A. Azure AD -

B. -

C. Azure AD -

Answer: C (LEAVE A REPLY)

NEW QUESTION: 42

Microsoft 365 .

.

Microsoft SharePoint files that are affected by the policy will be [answer choice].

Once the policy is created, [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

NEW QUESTION: 43

Microsoft Intune 3

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

Intune

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

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

Name	Assigned to
Policy2	Group2
Policy3	Group3

Statements

- Device1 is compliant. Yes No
- Device2 is compliant. Yes No
- Device3 is compliant. Yes No

Answer:

- Policy1 applies to Device3. Yes No
- Policy2 applies to Device2. Yes No

-
-
-
-

NEW QUESTION: 44

Microsoft 365 □□□ □□□□.

□□□□ App1□□□□ □ □□ □□ □□□□□ □□□□□.

Microsoft Cloud App Security□ Cloud Discovery□□ □□□ □ □□□□ □□ □□ □□□□□□

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

□□□ □□□ □□□ □□□ □□□ □□□ □□ □□□.

Cloud Discover □□□□ □□□ □□□□ □□□□?

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

Answer: (SHOW ANSWER)

□□/□□:

□□:

<https://docs.microsoft.com/en-us/cloud-app-security/discovered-app-queries>

NEW QUESTION: 45

contoso.com□□□ Azure AD(Azure Active Directory) □□□□ □□□ Microsoft 365 □□□ □□

□□. □□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

Policy1□□□ DLP(□□□□ □□ □□) □□□□ □□□□□. Policy1□ PII(□□ □□ □□)□

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

User1□ PII□ □□□ □□□ □□ □□□□□ □□ □ □□□□□?

- A. User2 □□
- B. □□□ 2 □ □□□ 3□
- C. □□□2, □□□3, □□□4□
- D. □□□2, □□□3, □□□4, □□□5

Answer: B (LEAVE A REPLY)

□□

□□□ □□□ "□□ □□"□ □□□□□. □□□ □□□ Active Directory □□ Azure Active Directory □□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□□.

□□:

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

NEW QUESTION: 46

Microsoft System Center Configuration Manager() contoso.com
Active Directory .

Windows 10 Windows 8.1 .

Windows 8.1 Windows 10 .

?

: 1 .

First action to perform:	<ul style="list-style-type: none">Enroll the devices in Microsoft Intune.Configure device compliance in Microsoft Intune.Create a Microsoft Azure Log Analytics workspace.Add an alias (CNAME) record to the DNS zone of contoso.com.
Second action to perform:	<ul style="list-style-type: none">Configure all the devices to have a commercial ID.Configure software inventory in Configuration Manager.Configure all the devices to join the Windows Insider Program.Configure and restart the Windows Update service on all the devices.

Answer:

First action to perform:	<ul style="list-style-type: none">Enroll the devices in Microsoft Intune.Configure device compliance in Microsoft Intune.Create a Microsoft Azure Log Analytics workspace.Add an alias (CNAME) record to the DNS zone of contoso.com.
--------------------------	--

Second action to perform:	<ul style="list-style-type: none">Configure all the devices to have a commercial ID.Configure software inventory in Configuration Manager.Configure all the devices to join the Windows Insider Program.Configure and restart the Windows Update service on all the devices.
---------------------------	---

□□

First action to perform:	<ul style="list-style-type: none">Enroll the devices in Microsoft Intune.Configure device compliance in Microsoft Intune.Create a Microsoft Azure Log Analytics workspace.Add an alias (CNAME) record to the DNS zone of contoso.com.
Second action to perform:	<ul style="list-style-type: none">Configure all the devices to have a commercial ID.Configure software inventory in Configuration Manager.Configure all the devices to join the Windows Insider Program.Configure and restart the Windows Update service on all the devices.

□□:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started>

<https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started>

MS-101 ☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop ☐☐ ☐☐☐☐ ☐☐☐ MS-101 ☐☐!
DumpTop ☐ ☐☐ **MS-101** ☐☐ ☐☐☐ ☐☐☐☐☐☐, DumpTop MS-101 ☐☐ ☐☐☐ ☐☐☐
☐☐☐☐☐ ☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐☐☐☐ ☐☐☐☐☐ ☐☐ DumpTop MS-101 ☐☐☐
☐☐☐☐☐. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 47

contoso.com☐☐☐ Microsoft Azure Active Directory(Azure AD) ☐☐☐☐ ☐☐☐☐.
☐☐ ☐☐☐ ☐☐☐ App1, App2 ☐ App3☐☐☐ ☐ ☐☐ ☐☐ ☐☐☐☐☐☐ ☐☐☐☐.
☐☐☐ WIP(Windows Information Protection)☐ ☐☐☐☐☐. WIP☐☐ ☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐
☐.

- * Windows ☐☐ ☐☐ ☐☐☐: ☐☐
- * ☐☐☐ ☐: App1
- * ☐☐ ☐: App2

App1☐☐ File1☐☐☐☐☐☐ ☐☐☐ ☐☐☐☐☐.

☐☐☐☐☐☐☐☐☐☐? ☐☐☐☐☐☐ ☐☐ ☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐☐.
☐☐☐: ☐ ☐☐☐☐☐☐☐☐ 1☐☐☐☐☐☐☐☐☐☐☐☐☐.

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

Answer:

Statements



If User1 performs the initial device enrollment for Device1, the Enrollment Status Page will show.

If User1 performs the initial device enrollment for Device2, the Enrollment Status Page will show.

If User2 performs the initial device enrollment for Device2, the Enrollment Status Page will show.

□□

You can open File1 from:

▼
App1 only
App1 and App2 only
App1 and App3 only
App1, App2 and App3

If you open File1 in App1, App2, and App3, an action will be logged for:

▼
App1 only
App3 only
App1 and App2 only
App2 and App3 only
App1, App2, and App3

NEW QUESTION: 48

contoso.com Active Directory . □□ □□□□ □□□

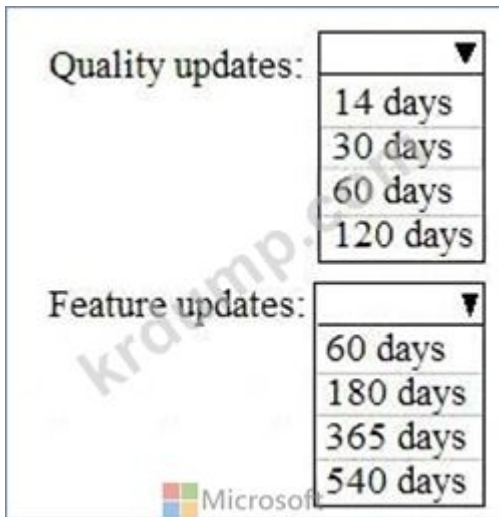
Windows 10 □□□□ □□□□ □□□□□.

Windows □□□□□ □□□□ Windows 10 □□□ □□□□□□□.

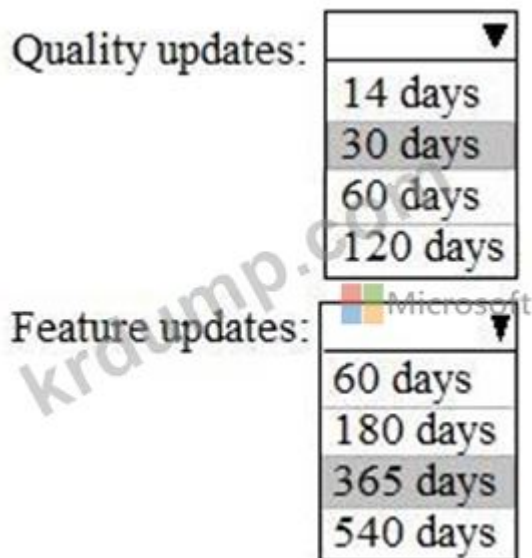
Windows 10 □□□□□ □□□ □ □□ □□ □□□□□□? □□□□□ □□ □□□□ □□

□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb>

NEW QUESTION: 49

Minimum number of data sources:

Minimum number of log collectors:

□□

Minimum number of data sources:

Minimum number of log collectors:



□□:

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

NEW QUESTION: 52

□□ □□ □□□ □□□□ □□□□ 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□□ □□□ □□□□□.

Statements

Yes **No**

App1 can be assigned as a required install for User3. Yes No

App2 can be uninstalled from Device2 by using Microsoft Endpoint Manager. Yes No

App3 can be installed automatically for UserGroup1. Yes No

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"/>

□□:

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

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

NEW QUESTION: 53

□□□□ Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP) □ □□□□

□.

Microsoft Defender ATP □ □□□□ □□□ □□ □□ □□ □□□□.

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 checked="" type="radio"/>

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

NEW QUESTION: 54

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

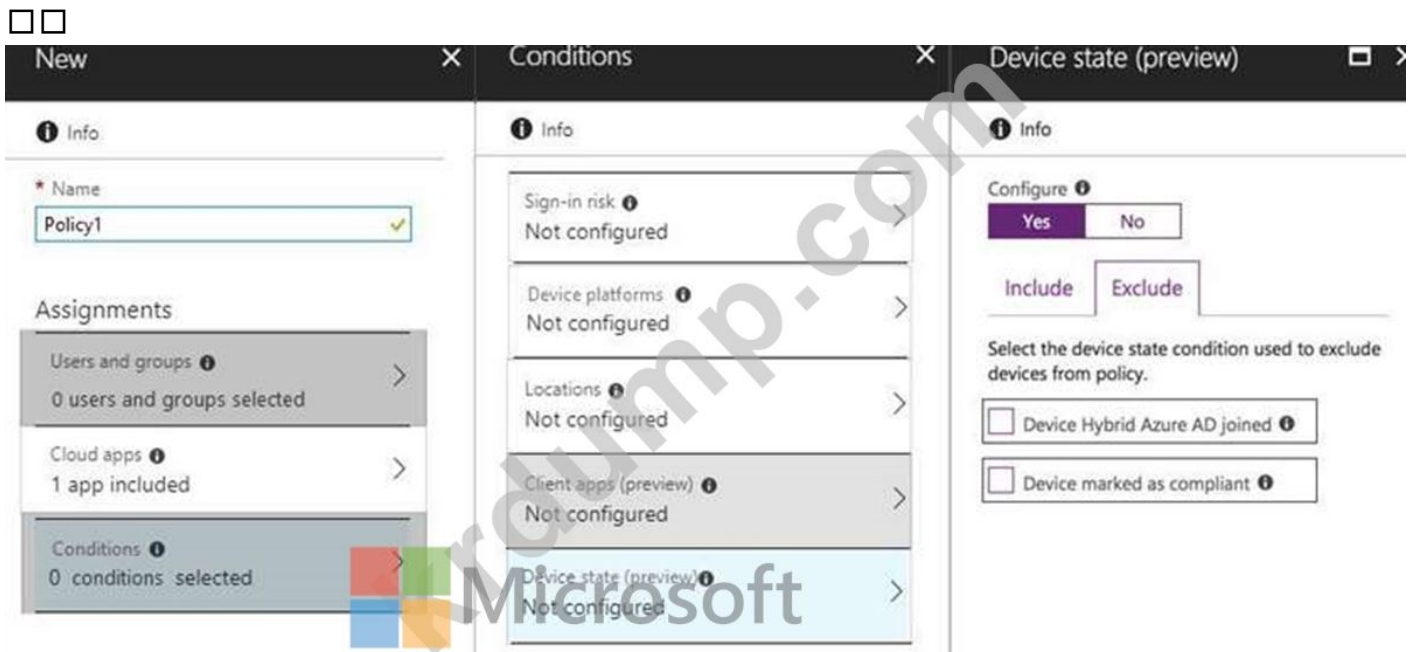
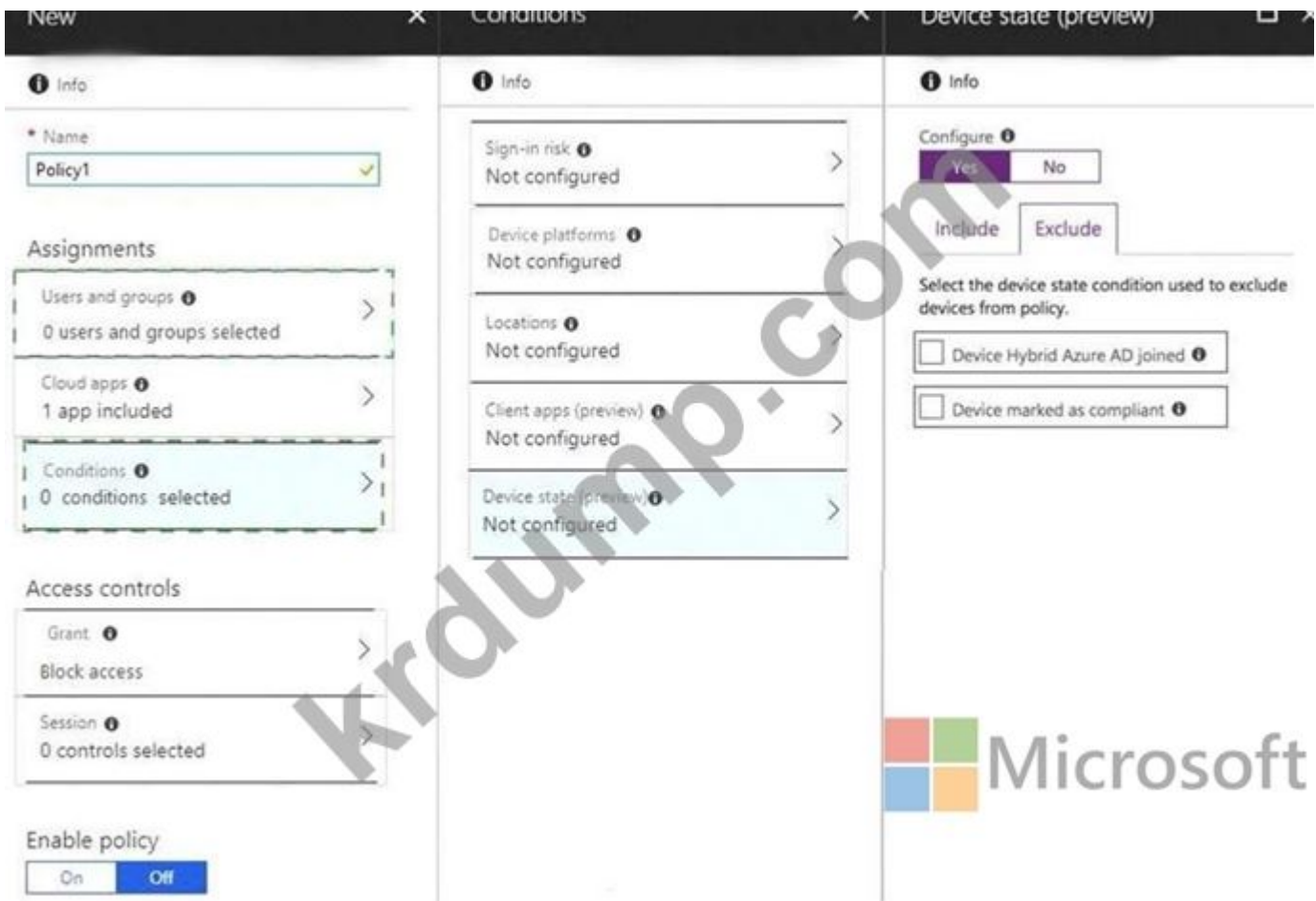
Exchange Online□ □□□□ □□□ □□□□□.

Policy1□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

The screenshot shows the Microsoft Intune console with three panes: 'New', 'Conditions', and 'Device state (preview)'.
 - **New pane:** Shows the policy name 'Policy1'. Under 'Assignments', 'Users and groups' has 0 selected, and 'Cloud apps' has 1 app included. 'Conditions' shows 0 selected. At the bottom, the 'Enable policy' toggle is set to 'Off'.
 - **Conditions pane:** Lists several conditions that are 'Not configured': Sign-in risk, Device platforms, Locations, Client apps (preview), and Device state (preview).
 - **Device state (preview) pane:** Shows a 'Configure' section with 'Yes' selected. Below it are 'Include' and 'Exclude' tabs. Under 'Select the device state condition used to exclude devices from policy', two checkboxes are visible: 'Device Hybrid Azure AD joined' and 'Device marked as compliant', both of which are currently unchecked.

Answer:



NEW QUESTION: 55

Microsoft 365 □□□ □□□□.

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

User1□□□ □□□□ □□□□□ ProjectX□□ □□□ □□□ □□ □□ □□□□ □□□□ □□□□.

□□□ □□□□□□□□□?

- A. □□ □ □□ □□ □□□□ □□□ □ □□□ □□□ □□□□□.
- B. Microsoft Cloud App Security□□ □□ □□□ □□□□.
- C. □□ □ □□ □□ □□ □□□□ □□□ □□□ □□□□□.
- D. □□ □ □□ □□ □□ □□□□ □□□ □□ □□(DLP) □□□ □□□□.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 56

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

contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

Workspace1□□□ Azure ATP(Advanced Threat Protection) □□ □□□ □□□□.

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

Azure ATP □□□ □□□ □□□□ □□□.

□□□: □□□ 3□□ Azure ATP □□ □□□ □□□□□ □□□□□□. □□□ □□□ □□□□ □?

- A. □□□
- B. □

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

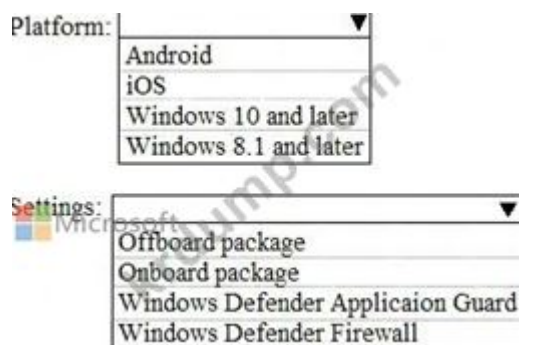
NEW QUESTION: 57

Microsoft 365 □□□ □□□□.

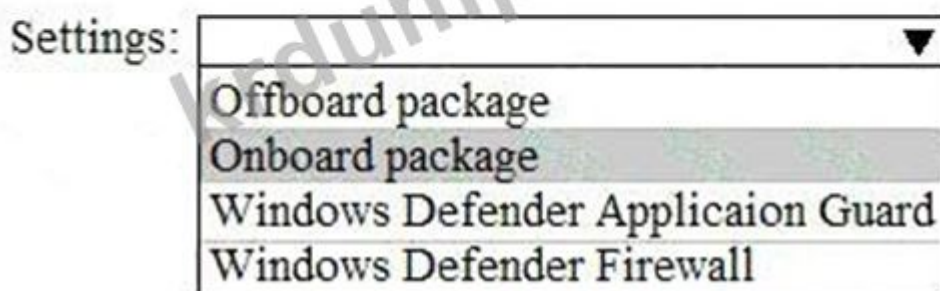
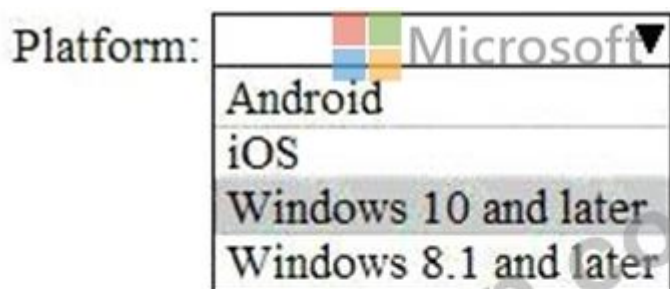
MDM(□□□ □□ □□)□ □□□ □□□□ □□ □□□ □□ Windows Defender ATP(Advanced Threat Protection)□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



<https://docs.microsoft.com/en-us/intune/advanced-threat-protection>

NEW QUESTION: 58

500 Windows 10 Microsoft Endpoint Manager

Microsoft 365 .

Microsoft Office 365

.

?

A.

B.

C. (ASR)

D.

Answer: ([SHOW ANSWER](#))

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

NEW QUESTION: 59

Microsoft 365 .

□□ □ □□ eDiscovery □□□ □□□ □□ □□□□ □□□□ □□□.
□□ □ □□ □□ □□ □□□□ □□□ □□ □□□?

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

Answer: D (LEAVE A REPLY)

□□: [□□]

NEW QUESTION: 60

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

Microsoft 365 □□□ □□□□.

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

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

- A. □
- B. □□□

Answer: (SHOW ANSWER)

SharePoint Online□ □□□ □□□□ IP □□ □□ □□□ □□□□ □□□□□ □□□□
□ □□□□.

□□:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlineand-OneDrive-for/ba-p/46678>

NEW QUESTION: 61

Microsoft 365 □□□□ □□□□.

□□ □□□□□ Enterprise Mobility + Security □□□□□ □□□□□.
□□□□ □□□ Microsoft Azure Active Directory(Azure AD)□ □□□ □ □□□ Microsoft Intune
□ □□□□ □□□□□ □□ □□□.
□□□ □□□□ □□□?

- A. Intune □□ □□□ □□ □□ □□
- B. Intune □□ □□□ □□ □□ □□□
- C. Azure Active Directory □□ □□□ MAM □□□ □□
- D. Azure Active Directory □□ □□□ MDM □□□ □□

Answer: D (LEAVE A REPLY)

□□/□□:

□□:

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

MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
 DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□
 □□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 62

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

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□□
 Active Directory □□□□ □□□□.

Microsoft System Center Configuration Manager(□□ □□)□ □□□□□ Windows 10 □□□ □□
 □□□.

□□ □□□ □□ □□□□ □□□□□.

Device1□□□□ □ □□□ □□□□ □□□□□. Device1□ Configuration Manager □□□□□□
 □□□□□.

Microsoft Intune □ Configuration Manager□ □□□□□ Device1□ □□□ □ □□□ □□□□ □
 □□.

□□□: Configuration Manager □□ □□□□ □□□ □□□□□ □□□□□. □□□□□ Device1
 □ □□□□□.

□□□ □□□ □□□□□□?

A. □

B. □□□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 63

□□□ contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ Microsoft 365 □
 □□ □□□□. □□□ □□ □□ □□ □□□ □□□ □□ 4□□ □□□ □□□□ □□□□□□.

Name	Operating system
User1	Windows 8
User2	Windows 10
User3	Android 8.0
User4	iOS 11

Microsoft Intune Microsoft 365

- A. 1, 2
- B. 1, 2, 3, 4
- C. 1 2
- D. User2

Answer: D (LEAVE A REPLY)

NEW QUESTION: 64

Active Directory Windows 8.1 2,000

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

App1 App2 UpgradeDecision ReadyForWindows

- A.
- B.

Answer: A (LEAVE A REPLY)

App1 "(2%) App2

:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

NEW QUESTION: 65

Office Microsoft 365

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

Microsoft Endpoint Manager

Home / Policy Management Notifications

Policy configurations

+ Create Copy Reorder priority Remove Total policy configurations: 3

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

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

User1 User2 Office ?

100

The default shared folder location for User1 is:

https://sharepoint.contoso.com/addins_all_users

https://sharepoint.contoso.com/addins_office_users

https://sharepoint.contoso.com/addins_sales_team_users_

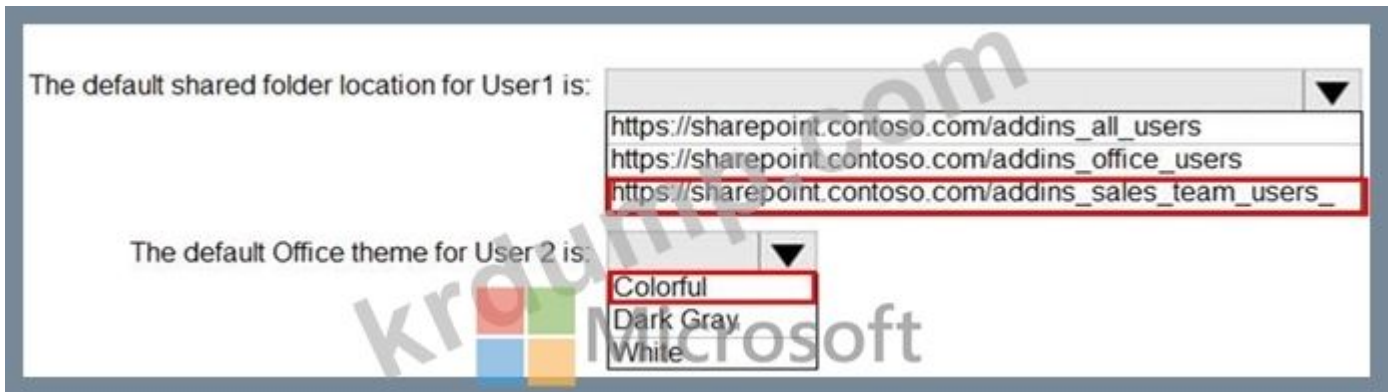
The default Office theme for User 2 is:

Colorful

Dark Gray

White

Answer:



□□:

<https://docs.microsoft.com/en-us/deployoffice/overview-office-cloud-policy-service>

NEW QUESTION: 66

□ Microsoft 365 □□□ □□□□.

User1□□□ □□□□ Microsoft Exchange Online□ □□□□ □□□□.

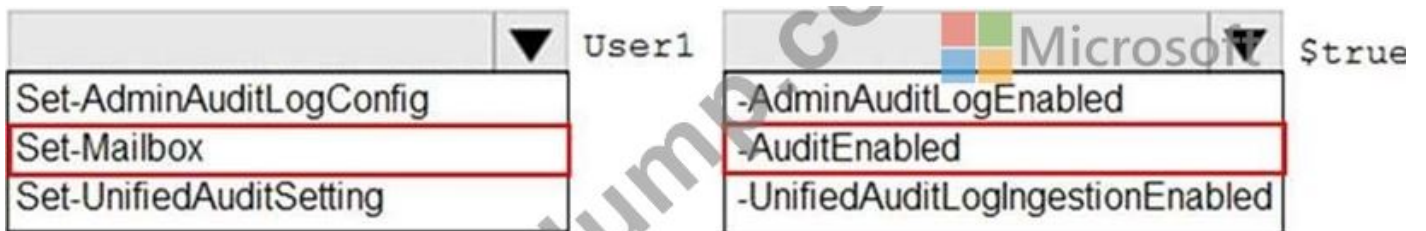
User1□ □□□ □□ □□□ □□ □□ □□□□ □□□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:



□□:

□□ □□□(□ □□□□ Holly Sharp□ □□)□ □□ □□□ □□□□□□□ □□ PowerShell □□ □□□□□. Set-Mailbox username -AuditEnabled \$true

□□:

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins>

[https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?](https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps)

view=exchange-ps

NEW QUESTION: 67

Microsoft 365 □□□ □□□□.

□□ □□□□ □□ □□ □□□ □□□□□.

Policy1



Microsoft



Edit policy

Delete policy

Status

On

Description

Description

Severity

Low

[Edit](#)

Category

Threat management

Conditions

Activity is Detected malware in file

Aggregation

Aggregated

Threshold

20 activities

[Edit](#)

Window

120 minutes

Scope

All users

Email recipients

User1@sk190107outlook.onmicrosoft.com

Daily notification limit

100

[Edit](#)

[Close](#)

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

C. □□ □ □□□□□ □□ □□□ □□ □□

D. Exchange □□ □□□ □□ □□

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

□□/□□:

□□:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-exo-rules>

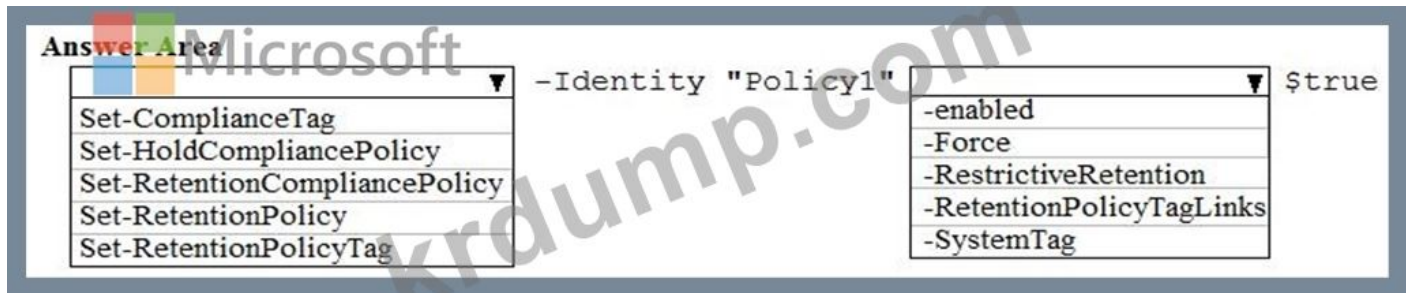
NEW QUESTION: 69

□□ □ □□ □□ □□ □□□□ Policy1□□□ □□ □□□ □□□□.

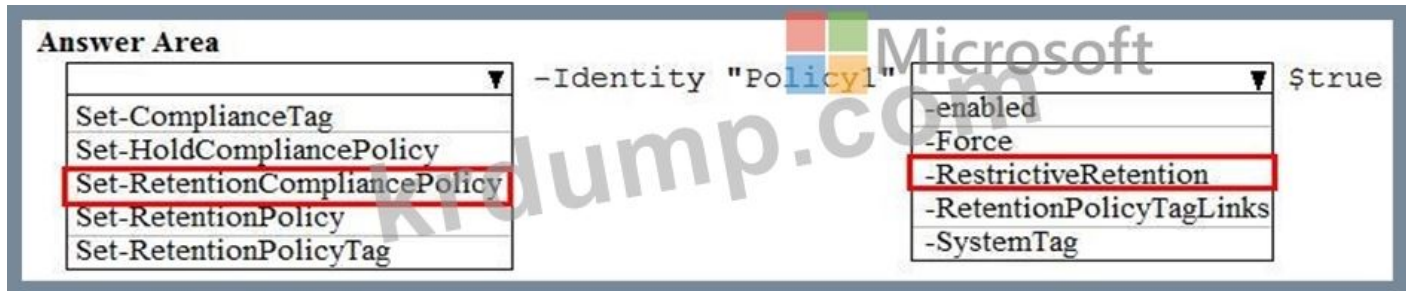
□□ □□□□ □□□ □□□□□□□ □□ □□□ □□□ □□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncompliancepolicy?view=exchange-ps>

NEW QUESTION: 70

□□□□□ contoso.com□□□ Active Directory □□□□ □□□□. □□□□□ 100□□

Windows 8.1 □□□ □□□□.

□□□ □□ Windows 10 Enterprise □□□□ Windows 8.1 □□□ □□□ □□□□□.

Windows 10 □□ □□□ □□□□ □□□.

□□□ □□□□ □□□?

A. □□□□□ □□□

B. □□ □□ □□□□□

C. □□□ □ □□ □□ □□

D. Windows □□ □□ □□

Answer: ([SHOW ANSWER](#))

□□/□□:

□□:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

NEW QUESTION: 71

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

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□ Active Directory □□□□ □□□□.

Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□ □□ □□□.

□□□ □□ □□□ □□□□□.

Device1□□□ □ □□□ □□□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.

Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □ □□.

□□□: Active Directory □□□□□ Device1□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

□□: [□□]

NEW QUESTION: 72

□□□□□ Microsoft Store□ □□□□ □□□.

□□ □□□□ □□□ □□ □ □□□□□?

A. □□□2

B. □□□3

C. □□□4

D. □□□5

Answer: C (LEAVE A REPLY)

□□: [□□]

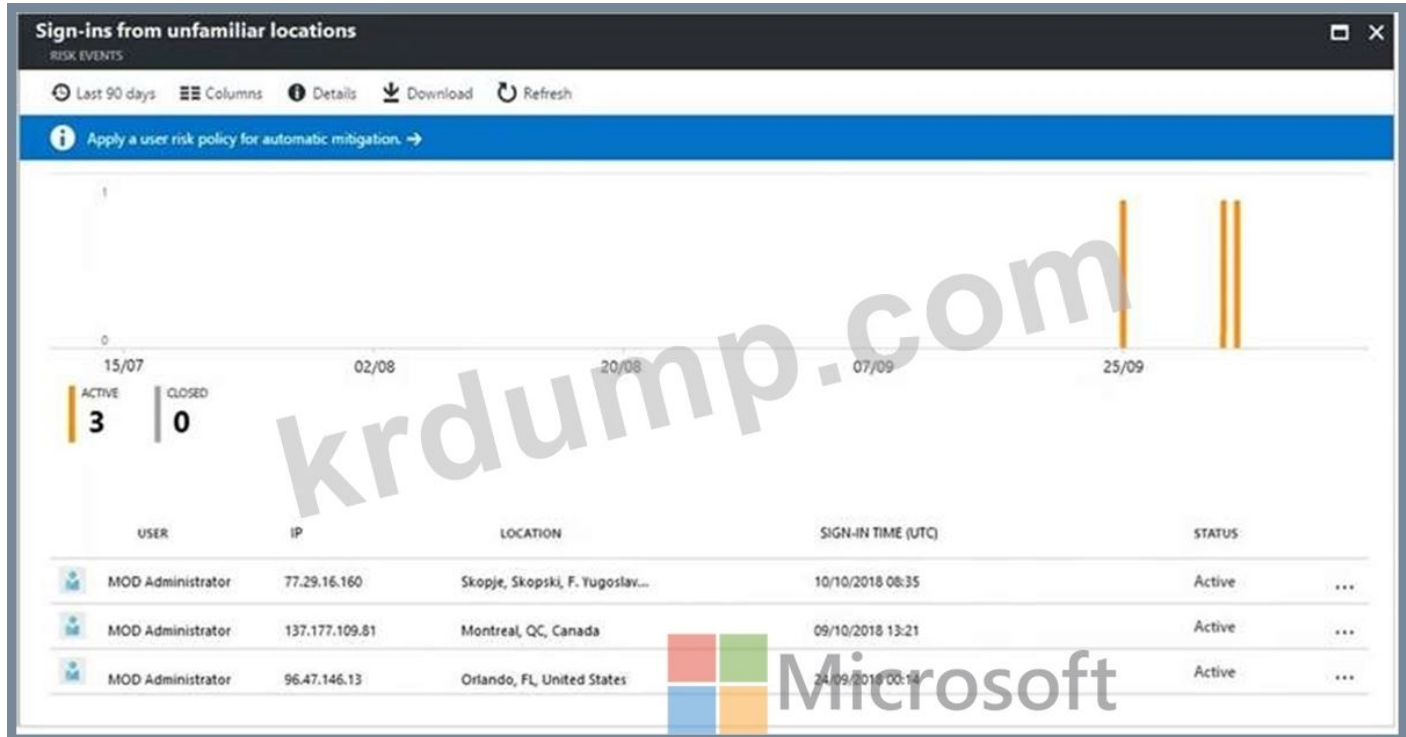
□□/□□:

□□:

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

NEW QUESTION: 73

Microsoft Azure Active Directory(Azure AD) ID



: 1

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

Answer:

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

NEW QUESTION: 74

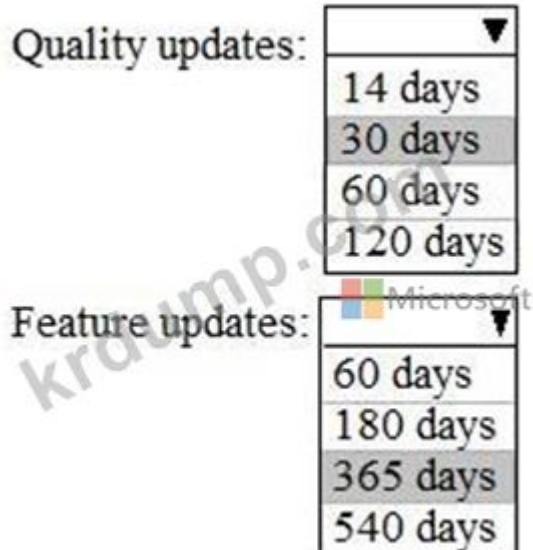
contoso.com Active Directory . . .
Windows 10 .
Windows . Windows 10 .
Windows 10 ? .
 .
: 1 .



Answer:



□□



□□:

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wufb>

NEW QUESTION: 75

Windows 10 Enterprise□ □□□□ □□□□ □□□ □□□□ □□□□.
IT □□□□ □□ □□□□□ □□□□ □ □□□ □ Windows □□ □□□ □□□ □□□□□.
□□□.
□□□ 30□ □□ Windows□ □□□□□□□ □□□ □□ □□□.
□□ □ □□ □□ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.
A. □□□□ □□ □□
B. □□ □□□□ □□ □□
C. □□ □□ □□ □□□□ □□ □□□ □□
D. □□ □□□□□□ □□□ □ □□
E. □□□□ □□ □ □□ □□□□□ □□□ □ □□

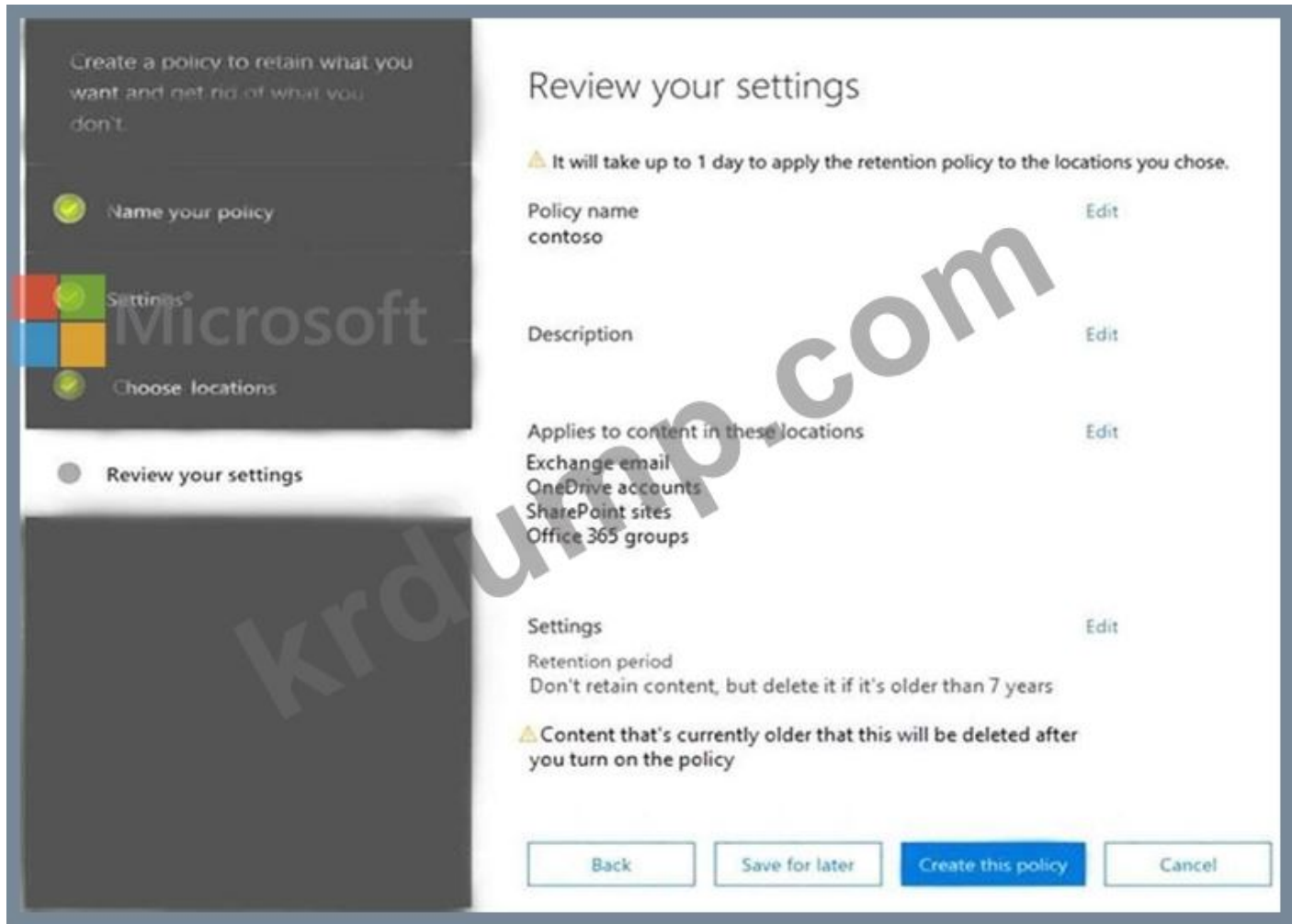
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 76

: 161

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □
□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□□ □□□□ □ □□□□. □□□□□ □□□ □□□ □□
□□□ □□□□ □□□□.
Microsoft 365 □□□ □□□□□.
□□ □ □□ □□ □□ □□□□ eDiscovery Manager □□ □□□ □□□□ US eDiscovery
Managers□□ □□ □□□ □□□□.

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



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

Microsoft SharePoint files that are affected by the policy will be [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [answer choice].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

Answer:

Microsoft SharePoint files that are affected by the policy will be [answer choice].

- recoverable for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, [answer choice].

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

□□

Microsoft SharePoint files that are affected by the policy will be **[answer choice]**.

- recovered for up to seven years
- deleted seven years after they were created
- retained for only seven years from when they were created

Once the policy is created, **[answer choice]**.

- some data may be deleted immediately
- data will be retained for a minimum of seven years
- users will be prevented from permanently deleting email messages for seven years

NEW QUESTION: 79

Microsoft 365 E5 □□□□ □□□□.

□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□.

- * □□ □□□ □□□□ □□ □□□□ □□□□□.
- * □□□ □□□ □□, □□□□ □ □□□□ □□□□□.
- * □□□ □□□□ □□□□ □□ □□ □□□□□□□ □□□□□.

Answer:

NEW QUESTION: 80

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

contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.
 Workspace1□□□ Azure ATP(Advanced Threat Protection) □□ □□□ □□□□.
 □□□□□□ □□ □□ □□□ □□□□ □□□□□.

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
File1 will be deleted automatically on February1, 2020.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 does not complete the disposition review within 90 days of receiving the notification, File2 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input checked="" type="radio"/>
File3 will be deleted automatically after February 1, 2021.	<input type="radio"/>	<input checked="" type="radio"/>

:

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

<https://docs.microsoft.com/en-us/office365/securitycompliance/disposition-reviews>

NEW QUESTION: 83

Microsoft 365 .

Name	Type
Group1	Distribution
Group2	Mail-enabled security
Group3	Security

Windows 10 .

?

A. Group3

B. Group1 Group3

C. Group2 Group3

D. 1. 2. 3

Answer: ([SHOW ANSWER](#))

:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines-configure#create-the-profile>

<https://docs.microsoft.com/en-us/microsoft-365/admin/create-groups/compare-groups?view=o365-worldwide>

NEW QUESTION: 84

Microsoft 365 E3 100 users. User1 is a member of Team1. An audit log search from the Security & Compliance admin center will provide the answer to question 1. An audit log search from the Security & Compliance admin center will provide the answer to question 2. An audit log search from the Security & Compliance admin center will provide the answer to question 3.

Statements	Yes	No
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input checked="" type="radio"/>	<input type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input checked="" type="radio"/>
An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input checked="" type="radio"/>	<input type="radio"/>

□□:

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%2farticle%2f0d4d0f35-390b-4518-800e-0c7ec95e946c>

<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

NEW QUESTION: 85

Microsoft 365 E3 100 users. User1 is a member of Team1. An audit log search from the Security & Compliance admin center will provide the answer to question 1. An audit log search from the Security & Compliance admin center will provide the answer to question 2. An audit log search from the Security & Compliance admin center will provide the answer to question 3.

- A. Exchange e Discovery Manager
- B. Exchange Audit Log Search
- C. Microsoft 365 Security & Compliance Admin Center
- D. Azure Active Directory Audit Log Search

Answer: A (LEAVE A REPLY)

□□:

<https://docs.microsoft.com/en-us/Exchange/permissions/feature-permissions/policy-and-compliance-permissions?view=exchserver-2019>

NEW QUESTION: 86

Microsoft 365

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Endpoint Manager

Priority	Name	Allowed platform	Assigned to
1	TypeRest1	Android, Windows (MDM)	Group1
2	TypeRest2	iOS	Group2

Microsoft Endpoint Manager

Priority	Name	Device limit	Assigned to
1	LimitRest1	7	Group2
2	LimitRest2	10	Group1
3	LimitRest3	5	Group3

Statements

- | | Yes | No |
|---|-----------------------|-----------------------|
| User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |
| User3 can enroll up to five Android devices in Microsoft Endpoint Manager. | <input type="radio"/> | <input type="radio"/> |

Answer:

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

Statements	Yes	No
User1 can enroll up to 10 Windows 10 devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User2 can enroll up to 10 iOS devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>
User3 can enroll up to five Android devices in Microsoft Endpoint Manager.	<input type="radio"/>	<input type="radio"/>

NEW QUESTION: 87

contoso.com Active Directory . 100 Windows 8.1 . Windows 10 Enterprise Windows 8.1 . Windows 10 . ?

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

Answer: B (LEAVE A REPLY)

:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

NEW QUESTION: 88

DLP1 (DLP) .

Choose the types of content to protect

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

Content contains *

Any of these ▾

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

Retention labels

1year ✕

Add ▾

+ Add group

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□

□□: □ □□□ □□□ 1□□ □□□ □□□□.

DLP1 will be applied only to documents that have [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1year label applied
- either a credit card number or the 1year label applied
- between 85 and 100 credit card numbers

Answer:

Statements

Device1 is compliant.

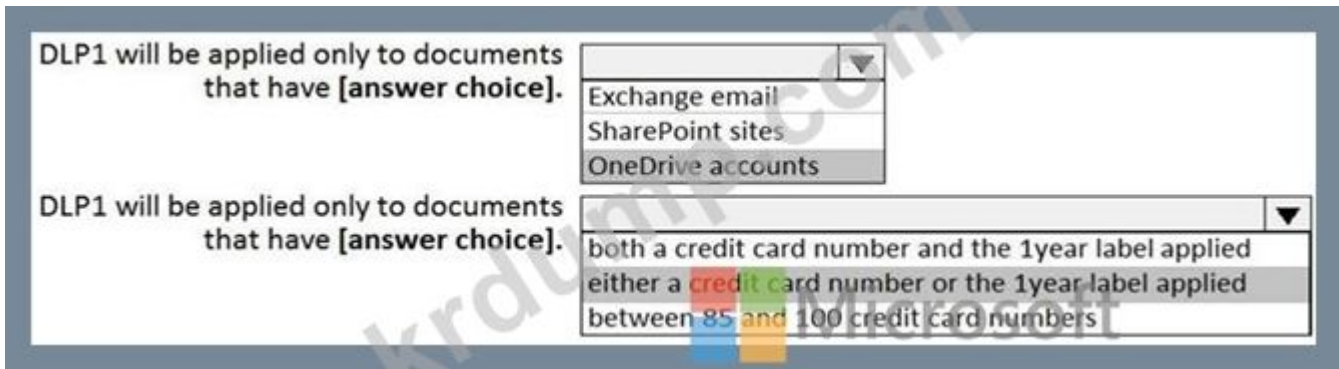
Yes

No

Device2 is compliant.

Device3 is compliant.

□□



□□:

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

NEW QUESTION: 89

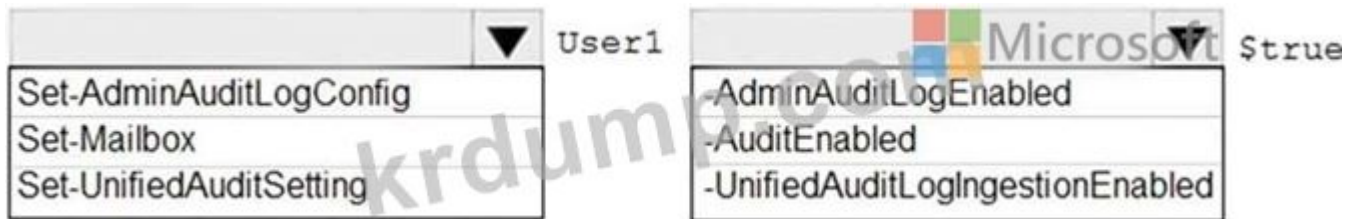
□ Microsoft 365 □□□ □□□□.

User1□□□ □□□□ Microsoft Exchange Online□ □□□□ □□□□.

User1□ □□□ □□ □□□ □□ □□ □□□□ □□□.

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

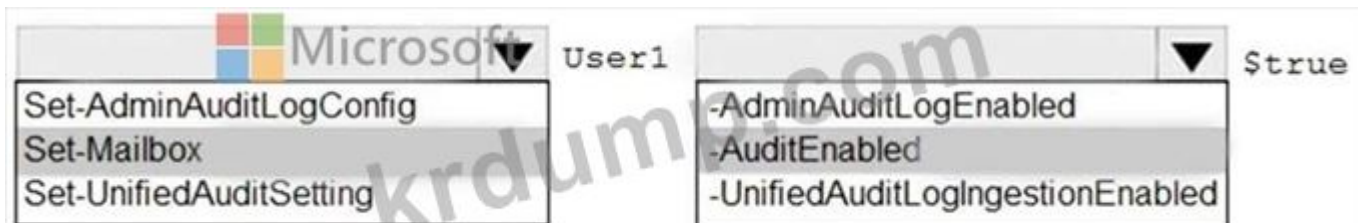
□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□



□□ □□□(□ □□□□ Holly Sharp□ □□)□ □□ □□□ □□□□□□ □□ PowerShell □□

□ □□□□□. Set-Mailbox username -AuditEnabled \$true

<https://support.microsoft.com/en-us/help/4026501/office-auditing-in-office-365-for-admins>

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-mailbox?view=exchange-ps>

view=exchange-ps

NEW QUESTION: 90

contoso.com Active Directory

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

File1.abc Server1 . File2.abc Server2 . App1, App2 App3 .abc .

WIP(Windows Information Protection) .

* : App2

* : App1

* Windows :

* : IPv4 : 192.168.1.1-192.168-1.255

File1.abc

.

:

Statements	Yes	No
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can open File1.abc in App1.	<input checked="" type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input checked="" type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input checked="" type="radio"/>

.

Statements	Yes	No
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

.

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/crea>

NEW QUESTION: 91

□□□ □□□ □□(□□)□ □□□□.
□□□□ □□ □□ □□(PII)□ □□□ □□□□ □□ □□□□□□.
□□ □□ □ □□ □□□□□ □□□□ DLP(□□□□ □□ □□) □□□□ □□□□□. □□□□ □□ □
□□ □□ □□□□□□.

New DLP policy

- ✔ Choose the information to protect
- ✔ Name your policy
- ✔ Choose locations
- ✔ Policy settings

● Review your settings



Review your settings

Template name Edit
U.K. Personally Identifiable Information (PII) Data

Policy name Edit
U.K. Personally Identifiable Information (PII) Data

Description Edit

Applies to content in these locations Edit
Exchange email
SharePoint sites
OneDrive accounts

Policy settings Edit
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.
If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? Edit
Yes

 Microsoft

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

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

Answer:

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
 DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□
 □□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 92

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □
 □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □
 □□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
 □ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□ □□□ □□□ □□
 □□□□ □□□□ □□□□□.
 contoso.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□□.
 Workspace1□□□ Azure ATP(Advanced Threat Protection) □□ □□□ □□□□□.
 □□□□□ □□ □□ □□□ □□□□□ □□□□□□.

Name	Member of group	Azure AD role
User1	Azure ATP Workspace1 Administrators	None
User2	Azure ATP Workspace1 Users	None
User3	None	Security administrator
User4	Azure ATP Workspace1 Users	Global administrator

Azure ATP .

: Azure ATP User4.

?

A.

B.

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

Azure ATP .

Azure Active Directory Azure ATP .

.

<https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-role-groups>

NEW QUESTION: 93

Microsoft Cloud App Security.

Cloud App Security SIEM() .

Windows Server 2016 SIEM .

.

: 1 .

First action to perform:	<input type="text" value="Install Java 8."/>
Second action to perform:	<input type="text" value="Run the Set-MMagent cmdlet."/>

Answer:

Microsoft Intune Configuration Manager Device1 .

Configuration Manager Device1 .
?

A.

B.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 97

Active Directory Windows 10 Pro . Microsoft 365
Windows 10 Enterprise . SSO Windows Hello
Microsoft 365
? . : 1

A. Microsoft Azure Active Directory(Azure AD)

B.

C. Microsoft Intune

D. TPM

E.

Answer: (SHOW ANSWER)

:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-hybrid-aadj-ssso-base

NEW QUESTION: 98

contoso.com Azure AD(Azure Active Directory) Microsoft 365

Name	Username	Type
User1	User1@contoso.com	Member
User2	User2@sub.contoso.com	Member
User3	User3@adatum.com	Member
User4	User4@outlook.com	Guest
User5	User5@gmail.com	Guest

Policy1 DLP() . Policy1 PII()

User1 PII?

A. User2

B. 2 3

C. 2, 3, 4

D. 2, 3, 4, 5

Answer: (SHOW ANSWER)

□□□ □□□ "□□ □□"□ □□□□□. □□□ □□□ Active Directory □□ Azure Active Directory □□□□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□□. □□:

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

NEW QUESTION: 99

□□ □□ □□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2

□□□□ Microsoft Intune□ □□□□□.

□□ □□ □□ □□ □□□ Intune□ □□□□ □□□□.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3.
Policy2	Require	Group4

□□ □□□ □□ □□□ □□□ □□□□□.

□□ □□□ □□□ □□ □□□□□.

□□□ □ □□: Group1

□□□□ □: Microsoft Office 365 Exchange Online

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

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

User1 can access Microsoft Exchange Online from Device1.

Yes

No

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 100

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

Policy1
✕

Edit policy

Delete policy

Status On

Description Description

Severity Low Edit

Category Threat management

Conditions Activity is Detected malware in file

Aggregation Aggregated

Threshold 20 activities Edit

Window 120 minutes

Scope All users

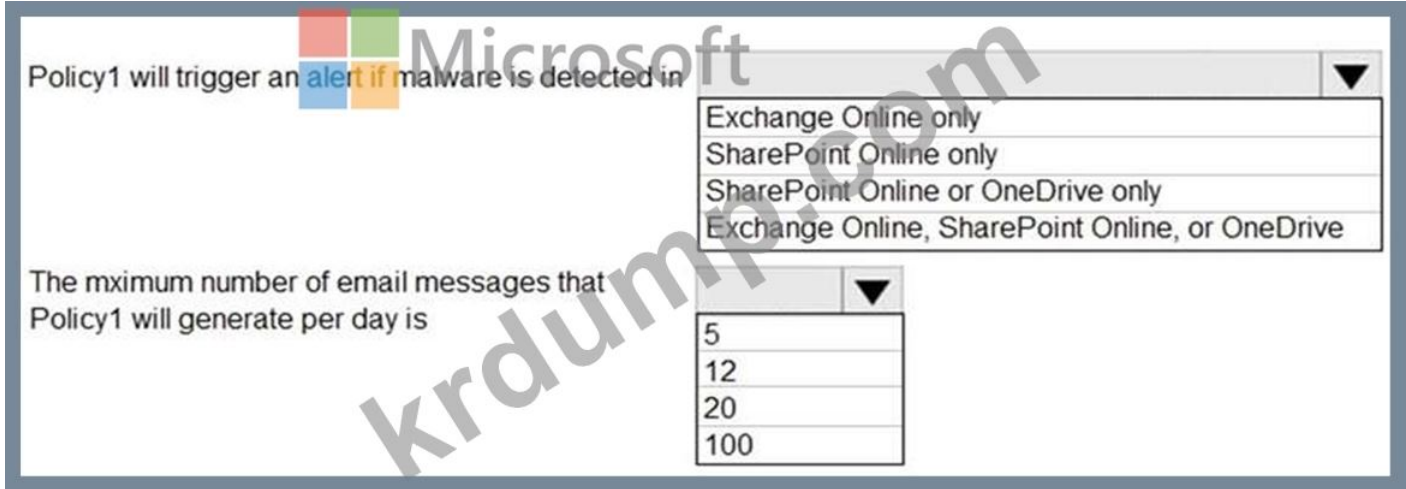
Email recipients User1@sk190107outlook.onmicrosoft.com

Daily notification limit 100 Edit

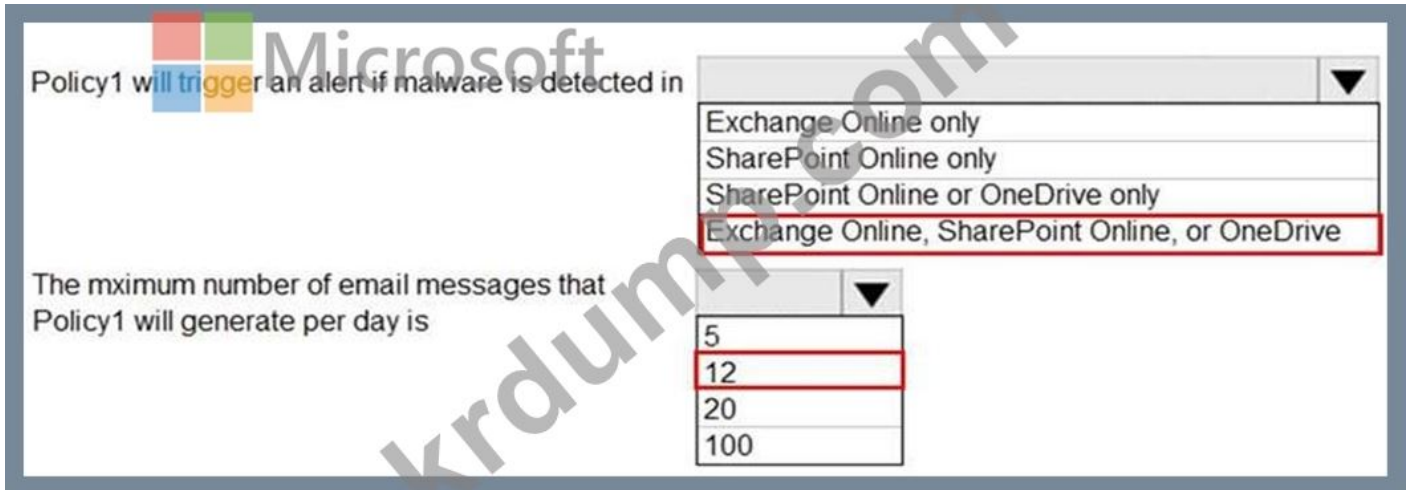
Close

Policy1 will trigger an alert if malware is detected in
 Exchange Online only
 SharePoint Online only
 SharePoint Online or OneDrive only
 Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is
 5
 12
 20
 100



Answer:



Policy1 will trigger an alert if malware is detected in
 Exchange Online only
 SharePoint Online only
 SharePoint Online or OneDrive only
 Exchange Online, SharePoint Online, or OneDrive

The maximum number of email messages that Policy1 will generate per day is
 5
 12
 20
 100

NEW QUESTION: 101

Scenario: A company has a Microsoft 365 environment. The company wants to ensure that all data is backed up and recoverable. The company has a policy that requires that all data be backed up and recoverable. The company has a policy that requires that all data be backed up and recoverable. The company has a policy that requires that all data be backed up and recoverable.

Microsoft 365 eDiscovery Manager

US eDiscovery Managers

Windows PowerShell New-ComplianceSecurityFiltercmdlet

Windows PowerShell New-ComplianceSecurityFiltercmdlet

□□□ □□□ □□□□□?

A. □

B. □□□

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

□□: [□□]

□□/□□:

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search>

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-ComplianceSecurityFilter?view=exchange-ps>

NEW QUESTION: 102

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

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

□□□□□□ Microsoft Azure Active Directory(Azure AD)□ □□□□□ contoso.com□□□ Active Directory □□□□ □□□□.

Microsoft System Center Configuration Manager(□□ □□)□ □□□□ Windows 10 □□□ □□ □□□.

□□□ □□ □□□ □□□□□.

Device1□□□ □ □□□ □□□□ □□□□□. Device1□ Configuration Manager □□□□□□ □□□□□.

Microsoft Intune □ Configuration Manager□ □□□□ Device1□ □□□ □ □□□ □□□□ □ □□.

□□□: Active Directory □□□ Device1□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

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

□□:

<https://www.scconfigmgr.com/2017/11/30/how-to-setup-co-management-part-6/>

NEW QUESTION: 103

□□□ □□ □□□ □□ □□□ □□□□□□□

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

Actions

- 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 Area

Answer:

Actions

- 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 Area

Assign eDiscovery permissions.
Create an eDiscovery case.
Create a hold.

□□:

□□:

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

NEW QUESTION: 104

Microsoft 365 □□□ □□□□.

□□ □□□□□ Microsoft Azure Active Directory Premium □□□□□ □□□□□.

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

Marketing□□□ □□□ □□□□ □□□□□ Azure AD(Azure Active Directory)□ □□□ □ □□

□□□ □□□□ Intune□ □□□□□ □□ □□□. □□□ □□ □□□□ Intune□ □□□ 5□□

□□□□□ □□□□□ □□□.

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

□□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Device enrollment

Microsoft Intune

Search (Ctrl+F)

Overview

Quick start

Manage

Apple enrollment

Android enrollment

Windows enrollment

Terms and conditions

Enrollment restrictions

Device categories

Corporate device identifiers

Device enrollment managers

Monitor

Enrollment failures

Audit logs

Incomplete user enrollments

Answer:



□□:

DEM(□□ □□ □□□)□ Azure AD □□□ □□□ □□□ □ □□ Intune □□□□ □□□□ □ □
□ 1,000□□ □□□ □□□ □ □□□□. □□□ □□□□ Intune□ □□□□ □□□ □□□ □ □
□ □□□ □□□□ □□ □□□ □□□ □□□ □ □□□□.

□□ □.

□□ □□ □ □□.

□□□ □□ □□□□ Intune □□□ □□□ 5□□ □□□□□ □□□□□ □□□.

<https://docs.microsoft.com/en-us/intune/enrollment/device-enrollment-manager-enroll>

<https://docs.microsoft.com/en-us/intune/enrollment/enrollment-restrictions-set>

NEW QUESTION: 105

□□□ Microsoft 365 □□□ □□□□.

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

* □□□ □□□□□□ □□□ □□□□□ 20□ □□ □□□□□ □□□.

* □□□ □□□ □□□□ □□□ □□□ □□□□ □□□.

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

□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Computer1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Server1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Answer:

Computer1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

Server1-London:

	▼
Group1	
Group2	
Group3	
Ungrouped machines	

MS-101 <https://www.dumpst.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 107

Microsoft Office 365 eDiscovery cases created by User1. Export data from Advanced eDiscovery.

User	Task
User1	<ul style="list-style-type: none">Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content.View the eDiscovery cases created by User1.Configure case settings.Place content on hold.
User2	<ul style="list-style-type: none">View the eDiscovery cases created by User1.Export data from Advanced eDiscovery.

User1: eDiscovery Administrator, eDiscovery Manager, Records Management, Reviewer, Security Administrator
User2: eDiscovery Administrator, eDiscovery Manager, Records Management, Reviewer, Security Administrator

Answer:

User1:	<ul style="list-style-type: none">eDiscovery AdministratoreDiscovery ManagerRecords ManagementReviewerSecurity Administrator
User2:	<ul style="list-style-type: none">eDiscovery AdministratoreDiscovery ManagerRecords ManagementReviewerSecurity Administrator

□□

User1:  Microsoft ▼

- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

User2: ▼

- eDiscovery Administrator
- eDiscovery Manager
- Records Management
- Reviewer
- Security Administrator

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION: 108

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

Cloud App Security□ SIEM(□□ □□ □ □□□ □□)□ □□□ □□□□□.

Windows Server 2016□ □□□□ □□□□ SIEM □□□□□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

First action to perform:



- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Answer:

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.



□□

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas>

NEW QUESTION: 109

Microsoft 365 □□□ □□□□.

□□ □□□□□ Microsoft 365 E3 □□□□□ □□□□□.

□□□ □□ □□□ □□□□□□.

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

- A. 2□
- B. 1□
- C. 30□
- D. 90□

Answer: (SHOW ANSWER)

□□:

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

NEW QUESTION: 110

□□□□□ Microsoft System Center Configuration Manager(□□ □□)□ □□□□ contoso.com

□□□ Active Directory □□□□ □□□□.

Windows 10 □ Windows 8.1 □□□ □□□□.

□□ Windows 8.1 □□□ □□□□□ □□ □□□ □□□□ □□ Windows 10 □□□ □□□□ □

□ □□□ □□□ □ □□□ □□□□ □□□.

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

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

Answer:

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

□□

First action to perform:

- Enroll the devices in Microsoft Intune.
- Configure device compliance in Microsoft Intune.
- Create a Microsoft Azure Log Analytics workspace.
- Add an alias (CNAME) record to the DNS zone of contoso.com.

Second action to perform:

- Configure all the devices to have a commercial ID.
- Configure software inventory in Configuration Manager.
- Configure all the devices to join the Windows Insider Program.
- Configure and restart the Windows Update service on all the devices.

□□:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-get-started>

<https://docs.microsoft.com/en-us/windows/deployment/update/update-compliance-get-started>

NEW QUESTION: 111

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

- A. Device1 □□
- B. Device1 □ Device2□ □□
- C. Device1, Device2 □ Device3□ □□
- D. Device1, Device2 □ Device4□ □□
- E. □□1, □□2, □□3 □ □□4

Answer: A (LEAVE A REPLY)

□□: [□□]

□□/□□:

<https://docs.microsoft.com/en-us/mem/analytics/overview>

NEW QUESTION: 112

Windows 10 □□□□□ □□ Intune □□ □□□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Settings to configure in Azure AD:

▼
Device settings
Mobility (MDM and MAM)
Organizational relationships
User settings

Settings to configure in Intune:

▼
Device compliance
Device configuration
Device enrollment
Mobile Device Management Authority


Answer:

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority



□□:

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

NEW QUESTION: 113

□ Microsoft 365 □□□ □□□□□.

Microsoft 365 E3 □□□□□ □□□ 100□□ □□□□ □□□□.

□□ □ □□ □□ □□ □□□□ □□□ □□□□□□.

6□□ □ □□□□ □□ □□□ □□ □□□ □□□□ □□□□.

□□1: 14□ □□ Team1□□□ □□ □□ □□□ □□□□□?

□□2: 30□ □□ User1□ □□□□ □□ □□□ □□□□□?

□□ 3: 60□ □□ □□□□ □□□ □□ □□□□ □□□ □□□ □□□□□?

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area	Statements	Yes	No
	An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input type="radio"/>	<input type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area	Statements	Yes	No
	An audit log search from the Security & Compliance admin center will provide the answer to question 1.	<input checked="" type="radio"/>	<input type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 2.	<input type="radio"/>	<input checked="" type="radio"/>
	An audit log search from the Security & Compliance admin center will provide the answer to question 3.	<input checked="" type="radio"/>	<input type="radio"/>

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and-compliance?redirectSourcePath=%252farticle%252f0d4d0f35-390b-4518-800e-0c7ec95e946c>

<https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing>

NEW QUESTION: 114

Microsoft 365

Microsoft 365

* Microsoft 20

* Microsoft

Microsoft? Microsoft

Microsoft 100

Answer Area



Answer:

Answer Area



Microsoft

Answer Area



NEW QUESTION: 115

Microsoft 365
Microsoft 365
Microsoft 20
Microsoft
Microsoft?
Microsoft
Microsoft 100

□□□□□ □□□□□ Active Directory □□□□□ □□□□□ □□□□□. □□□□□ Windows Server 2019□ □□□□□ □□□ □□□□□ □□□□□ □□□□□. □□□□□ □□□□□ □□ □□□□ Windows Server 2012 R2□□□□.

□□□□□ Windows 10□ □□□□□ □□□□□ 100□□□□ Windows Server 2012 R2□ □□□□□ Server1□□□□□ □□□□ □□□□ □□□□□.

Server1□ □□□□□ □□□□□ □□□□□ Windows 10 □□ □□ □□□□ □□□□ □□□□□.

Server1□ GPMC(□□ □□ □□ □□)□ □□□□□□.

Server1□□ □□□□□□ Windows □□□□□ □□ □□ □□□□ □□□□□ □□□□.

□□□□: □□□□ □□ □□□□ Windows Server 2019□ □□□□□. Windows 10 □□□□□□ □□ □□

□□ □□□□□□ Netlogon □□□□ □□ □□ □□ □□□□□ □□□□□□.

□□□□ □□□□ □□□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

□□: [□□]

NEW QUESTION: 116

□□□□ Microsoft 365 □□□□ □□□□□.

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

* □□□□ □□□□□□□□ □□□□ □□□□□□ 20□ □□ □□□□□□ □□□□.

* □□□□ □□□□ □□□□□ □□□□ □□□□ □□□□ □□□□.







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







□ □□□□ □□□□ □□□□□□□□.

□□: □ □□□ □□□□ 1□□ □□□□ □□□□□.

<p>ATP anti-phishing</p>  <p>Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.</p>	<p>ATP safe attachments</p>  <p>Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.</p>	<p>ATP Safe Links</p>  <p>Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.</p>
<p>Anti-spam</p>  <p>Protect your organization's email from spam, including what actions to take if spam is detected.</p>	<p>DKIM</p>  <p>Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.</p>	<p>Anti-malware</p>  <p>Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.</p>

Answer:

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.

ATP anti-phishing  Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.	ATP safe attachments  Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.	ATP Safe Links  Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.
Anti-spam  Protect your organization's email from spam, including what actions to take if spam is detected.	DKIM  Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.	Anti-malware  Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.


NEW QUESTION: 117

Policy setting	Policy name Description Applied to	Managers
		If the email is sent to: IrvinS@M365x289755.OnMicrosoft.com MiriamG@M365x289755.OnMicrosoft.com Except if the email is sent to member of: test1ww@M365x289755.OnMicrosoft.com
Impersonation	Users to protect Protect all domains I own Protect specific domains Action > User impersonation Action > Domain impersonation Safety tips > User impersonation Safety tips > Domain impersonation Safety tips > Unusual characters Mailbox intelligence	On - 3 User(s) specified On On - 2 Domain(s) specified Move message to the recipients' Junk Email folders Delete the message before it's delivered Off Off Off Off
Spoof	Enable antispoofing protection Action	On Quarantine the message
Advanced settings	Advanced phishing thresholds	3 - More Aggressive

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

If a message is identified as a domain impersonation, [answer choice].

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].




	the message is delivered to the Inbox folder
	the message is moved to the Deleted Items folder
	the messages are moved to the Junk Email folder

	Advanced phishing thresholds
	Domain impersonation
	Enable antispoofting protection
	Mailbox intelligence

Answer:

If a message is identified as a domain impersonation, [answer choice].

To reduce the likelihood of the impersonation policy generating false positives, configure [answer choice].



	the message is delivered to the Inbox folder
	the message is moved to the Deleted Items folder
	the messages are moved to the Junk Email folder

	Advanced phishing thresholds
	Domain impersonation
	Enable antispoofting protection
	Mailbox intelligence

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-anti-phishing-policies#learn-about-atp-anti-phishing-policy-options>

NEW QUESTION: 118

Microsoft 365 □□□ □□□□.

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

Microsoft 365□□ □□ □□□ □□□□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Answer Area

Set-AdminAuditLogConfig Set-AuditConfig Set-AuditConfigurationRule Set-SupervisoryReviewPolicyV2	-AdminAuditLogEnabled -AdminAuditLogParameters -LogLevel -UnifiedAuditLogIngestionEnabled	\$false
---	--	---------

Answer:

Answer Area

Set-AdminAuditLogConfig Set-AuditConfig Set-AuditConfigurationRule Set-SupervisoryReviewPolicyV2	-AdminAuditLogEnabled -AdminAuditLogParameters -LogLevel -UnifiedAuditLogIngestionEnabled	\$false
---	--	---------

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/turn-audit-log-search-on-or-off>

NEW QUESTION: 119

□□□□ Microsoft Cloud App Security □ □□□□□.
Cloud App Security □ SIEM(□□ □□ □ □□□ □□) □ □□□ □□□□□□.
Windows Server 2016 □ □□□□ □□□□ SIEM □□□□□□ □□□□ □□□□.
□□□ □□□□□□□□□? □□□□□□ □□ □□□□ □□□ □□□ □□□□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□□.

First action to perform:	<ul style="list-style-type: none">Install Java 8.Install Microsoft .NET Framework 3.5.Add the Windows Internal Database feature.Add the Setup and Boot Event Collection feature.
Second action to perform:	<ul style="list-style-type: none">Run the Set-MMagent cmdlet.Add the Setup and Boot Event Collection feature.Run the java command and specify the -jar parameter.Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Answer:

First action to perform:	<ul style="list-style-type: none">Install Java 8.Install Microsoft .NET Framework 3.5.Add the Windows Internal Database feature.Add the Setup and Boot Event Collection feature.
Second action to perform:	<ul style="list-style-type: none">Run the Set-MMagent cmdlet.Add the Setup and Boot Event Collection feature.Run the java command and specify the -jar parameter.Run the Install-WindowsFeature cmdlet and specify the -source parameter.

□□:
□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas>

NEW QUESTION: 120

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□□. □□□□ □ □□□□ □
□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □
□□ □□□□ □□ □ □□□ □□ □□ □□□□ □□□ □□□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□□ □□□ □ □□□□. □□□□□□ □□□ □□□ □□
□□□ □□□□ □□□□.
□□□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□□ Windows 8.1□
□□□□□ □□ □□ □□ □□ □□□□□ □□□□ 2,000□□ □□□□ □□□□□.

Name	Application count	Used by
App1	20	Finance department, sales department
App2	100	Marketing department

□□□□□ □□□ □□ □□□□ □□□□□.

App1 □ App2□ UpgradeDecision □□□ □□□□□ □□ □□□□ □□□□ □□□.

□□□: App2□ ReadyForWindows □□□ □□ □□□□□ □□□□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

App1□ "□□ □□ □□"(2% □□)□□□ □□□□□□ □□□ □□□□□□. App2□ □□□ □□ □□□ □□ □□□.

□□:

<https://docs.microsoft.com/en-us/windows/deployment/upgrade/upgrade-readiness-identify-apps>

NEW QUESTION: 121

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

□□ □□ □□□ □□ □□ □□ □□□□□.

Priority	Name	Allowed platform	Assigned to
1	iOS	iOS	Marketing
2	Android	Android	Engineering
Default	All users	All platforms	All users

□□ □□ □□□ □□ □□ □□ □□□□□.

Priority	Name	Device limit	Assigned to
1	Engineering	15	Engineering
2	Wet Region	5	Engineering
Default	All users	10	All users

Engineering □□□ □□□□ □□ □□□□ □□□ □□□□□? □□□□□ □□ □□□□ □□ □□□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

□□: [□□]

NEW QUESTION: 123

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

□□□□ □□ □□□ □□□□ □□□ □ □□□ □□□□ □□□.

User1□□ □□ □□□ □□□□ □□□?

- A. Microsoft 365 □□ □□□ □□□ □□ □□□ □□□□□.
- B. Microsoft 365 □□ □□ □□□ eDiscovery Manager □□□□□□.
- C. Exchange □□ □□□ □□ □□ □□ □□□□□.
- D. Azure Active Directory □□ □□□ Information Protection □□□ ID□□□□.

Answer: B (LEAVE A REPLY)

NEW QUESTION: 124

□□□ □□□□ 5,000□□ Windows 10 □□□ □□□□. □□ □□□ Windows Defender□ □□ □□ □□□□□.

ATP(Advanced Threat Protection).

□□ 7□ □□ □□□□ □□ □□□ Windows Defender ATP □□ □□□□ □□□□ □□□.

Windows Defender ATP□□ □□□ □□□□ □□□?

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

Answer: B (LEAVE A REPLY)

□□:

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

□□□ □□ □□ □□

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

windows-defender-advanced-threat-protection

NEW QUESTION: 125

□□□ Microsoft 365 □□□ □□□□.

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







* □□□ □□□□□□ □□□ □□□□□ 20□ □□ □□□□□ □□□.

* □□□ □□□ □□□□ □□□ □□□ □□□□ □□□.







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

□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

<p>ATP anti-phishing</p>  <p>Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.</p>	<p>ATP safe attachments</p>  <p>Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.</p>	<p>ATP Safe Links</p>  <p>Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.</p>
<p>Anti-spam</p>  <p>Protect your organization's email from spam, including what actions to take if spam is detected.</p>	<p>DKIM</p>  <p>Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.</p>	<p>Anti-malware</p>  <p>Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.</p>

Answer:

<p>ATP anti-phishing</p>  <p>Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.</p>	<p>ATP safe attachments</p>  <p>Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.</p>	<p>ATP Safe Links</p>  <p>Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.</p>
<p>Anti-spam</p>  <p>Protect your organization's email from spam, including what actions to take if spam is detected.</p>	<p>DKIM</p>  <p>Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.</p>	<p>Anti-malware</p>  <p>Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.</p>

NEW QUESTION: 126


Windows 10 _____ Intune _____
 _____? _____
 _____: _____ 100 _____

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment
- Mobile Device Management Authority



Answer:

Settings to configure in Azure AD:

- Device settings
- Mobility (MDM and MAM)**
- Organizational relationships
- User settings

Settings to configure in Intune:

- Device compliance
- Device configuration
- Device enrollment**
- Mobile Device Management Authority

□□:

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

NEW QUESTION: 127

Microsoft 365 □□□ □□□□.

Exchange □□ □□□□ □□□ □□ □□□□ □□ Policy1□□□ DLP(□□□□ □□ □□) □□ □□□□.

* □□ □□□□ □□□ □□□□□ □□□□□□.

* □□ □□ □□ □□□□ □□□□□□. □□□□ □□□□□□□□.

□□ □□ □□ □□ □□ □□□□ □□ □□□ □□□□□ Policy2□□□ DLP □□□□ □□□□.

* □□ □□□ □□□□□□□□. □□□□ □□□□□□□□.

* □□ □□ □□ □□□ □□: □□□□ □□□ □□□□ □□□□ □□□□.


* □□□□ □□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□ □□□□□ □□□□.

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

□□: □□□□ □□□ □□□ □□□□ □□□□.

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

Protection settings

 HYOK (AD RMS)


Select the protection action type

Set permissions

Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
sk180818.onmicrosoft.com	Reviewer
User1@sk180818.onmicrosoft.com	Co-Owner
User2@sk180818.onmicrosoft.com	Co-Author

[+Add permissions](#)



Label1 □ File1□□□ □□□ □□□□□.

File1 □ User1, User2, User3 □ User4□□ □□□ □□ □□□ □□□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Yes

No

User2 can modify File1.

User3 can print File1.

User4 can read File1.

Answer:

Yes

No

User2 can modify File1.

User3 can print File1.

User4 can read File1.

□□

Statements

	Yes	No
User2 can modify File1.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
User3 can print File1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
User4 can read File1.	<input type="checkbox"/>	<input checked="" type="checkbox"/>

☐☐:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permiss>

NEW QUESTION: 129

SharePoint ☐☐☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐. ☐☐☐ ☐☐☐☐☐☐☐☐☐? ☐☐☐☐ ☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐☐☐☐. ☐☐: ☐☐☐☐☐☐☐☐ 100 ☐☐☐☐☐☐☐☐.

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

- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- Item
- User agent

Answer:

Answer Area

- Set-ComplianceTag
- Set-HoldCompliancePolicy
- Set-RetentionCompliancePolicy
- Set-RetentionPolicy
- Set-RetentionPolicyTag

Identity "Policy1"

- enabled
- Force
- RestrictiveRetention
- RetentionPolicyTagLinks
- SystemTag

\$true

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

- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- Item
- User agent



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

NEW QUESTION: 130

Microsoft 365 users can perform tasks. For example, a user can download all Security & Compliance reports. Another user can create and manage Security & Compliance alerts.

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

Users can perform tasks. For example, a user can download all Security & Compliance reports. Another user can create and manage Security & Compliance alerts.

User1:
 Records Management
 Security Administrator
 Security Reader
 Supervisory Review

User2:
 Compliance Administrator
 Organization Management
 Security Administrator
 Security Reader
 Supervisory Review

Answer:



□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-center#mapping-of-role-groups-to-assigned-roles>

NEW QUESTION: 131

Microsoft 365 □□□ □□□□.

□□ □ □□ □□□ □□ □□□ □□□□ □□□□.

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

Name	Task
User1	Download all Security & Compliance reports
User2	Create and manage Security & Compliance alerts.

□□□□ □□ □□ □□□ □□□□ □□□.

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

□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

User1:

▼
Records Management
Security Administrator
Security Reader
Supervisory Review

User2:

▼
Compliance Administrator
Organization Management
Security Administrator
Security Reader
Supervisory Review

Answer:

User1:

▼
Records Management
Security Administrator
Security Reader
Supervisory Review

User2:

▼
Compliance Administrator
Organization Management
Security Administrator
Security Reader
Supervisory Review

□ □

User1:

▼
Records Management
Security Administrator
Security Reader
Supervisory Review

User2:

▼
Compliance Administrator
Organization Management
Security Administrator
Security Reader
Supervisory Review

□ □:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-cent>

NEW QUESTION: 132

Microsoft Cloud App Security requires a minimum number of data sources and log collectors to be installed on a Windows 10 device. What is the minimum number of data sources and log collectors required?

Minimum number of data sources:

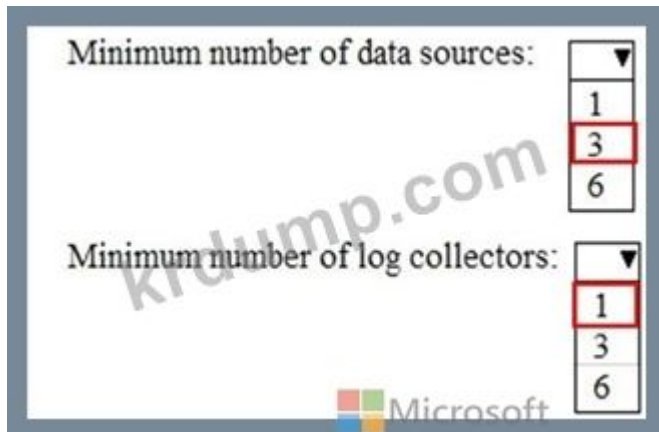
▼
1
3
6

Minimum number of log collectors:

▼
1
3
6



Answer:



Reference:

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

NEW QUESTION: 133

Azure Active Directory Connect syncs data from on-premises Active Directory to Azure Active Directory. How often does the sync process run by default? What is the minimum number of data sources and log collectors required for Microsoft Cloud App Security to be installed on a Windows 10 device?



In Azure:

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

On the computers:

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

Answer:

In Azure:

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

On the computers:

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

□□

In Azure:

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

On the computers:

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

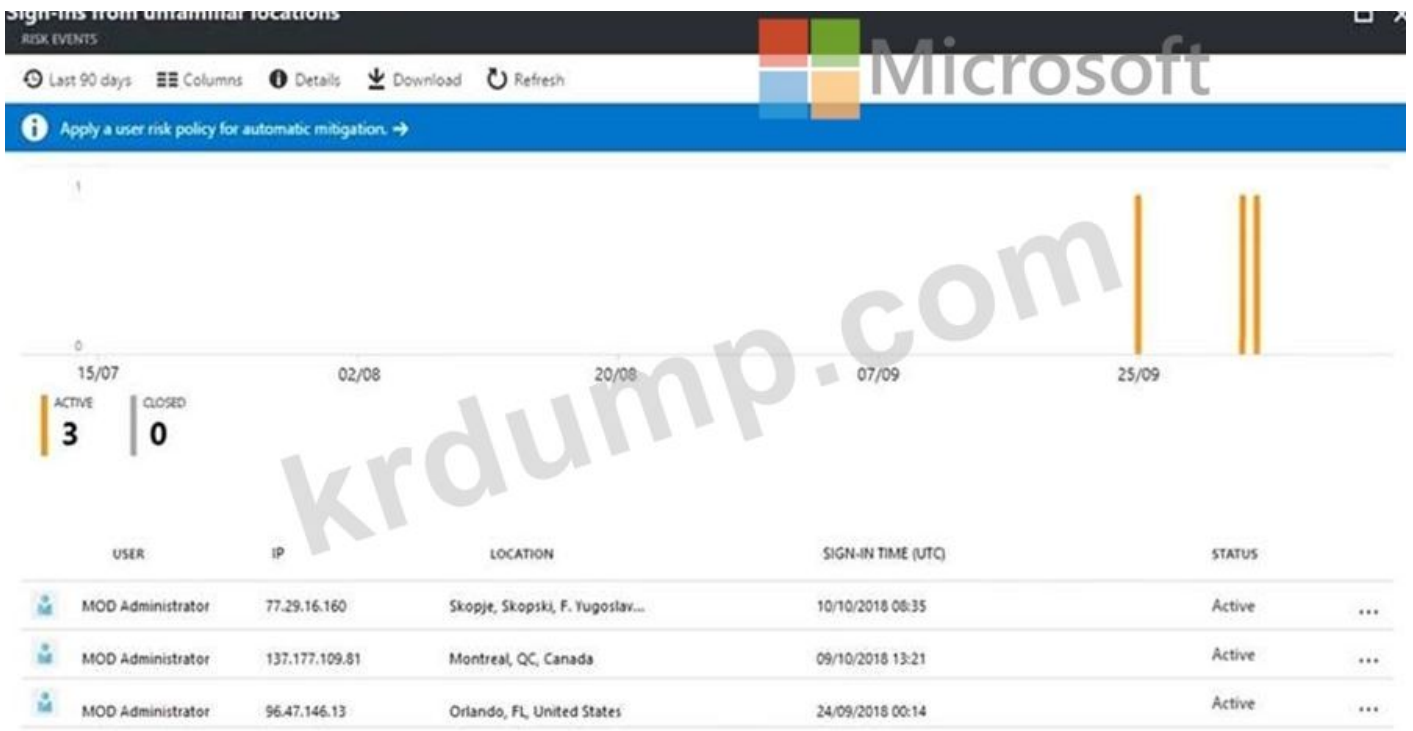
□□:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-collect-windows-computer>

NEW QUESTION: 134

□□ □□ □□□ □□□□ □□□ Microsoft Azure □□ □□□□(Azure AD) □□□□ □□□□.

Microsoft Azure Active Directory(Azure AD) ID [redacted]



[redacted]
[redacted]
[redacted]: [redacted]

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

Microsoft

Answer:

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

[redacted]:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>
<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations

NEW QUESTION: 136

Device1 Windows 10 Microsoft Endpoint Manager 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. Policy3
- B. Policy2
- C.
- D. Policy

Answer: A (LEAVE A REPLY)

MS-101 DumpTop MS-101! DumpTop MS-101, DumpTop MS-101. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps, 30%OFF Special Discount: **KrDump**)

NEW QUESTION: 137

Microsoft Azure Active Directory(Azure AD) ID



□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□

□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

Microsoft

- named location in Azure AD
- sign-in risk policy
- user risk policy

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

Answer:

To require multi-factor authentication when signing in to unfamiliar locations, you must create a [answer choice].

- named location in Azure AD
- sign-in risk policy
- user risk policy

To avoid generating alerts when signing in to the Montreal location, create [answer choice].

- a named location in Azure AD
- a sign-in risk policy
- a user risk policy

□□:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted>

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy>

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/quickstart-configure-named-locations>

NEW QUESTION: 138

□□□□ https://myapps.microsoft.com □ □□□□ □□□ □ □□ □□□□ □□□□□.
 "□□□□ □□□□□□□□. □ □□□□□ □□□ □□ □□□□□□□□. □□ □□, □ □□ □□□
 □□□ □□□□□ □□ □ □□□□□. □□□□□ □□□ □□□□ □□□□. □□ □□□□□ □□
 □□□." □□□□ □□□□□ □□□□ □□ □□□ □□□□□□?

- A. Microsoft Azure Active Directory(Azure AD) ID □□ □□
- B. Microsoft Azure Active Directory(Azure AD) □□□ □□□ □□
- C. □□ □ □□ □□ □□ □□
- D. □□ □ □□ □□ □□□ □□ □□(DIP) □□

Answer: (SHOW ANSWER)

□□:

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

NEW QUESTION: 139

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

Operating system	Quantity
Windows 8.1	5
Windows 10	5
Windows Server 2016	5

□□□ Windows Defender ATP(Advanced Threat Protection) □ □□□□□ □□□□. □□□□ □
 □□ □□□ □□□ □□□□□□ □□□□ □□□ □□□□.
 □ □□ □□□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□□ □□□ □□□ □□ □□
 □ □□□□□□□□□. □ □□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□□. □□□□
 □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □ □□□□□.
 □□: □ □□□ □□□ □□□ □□□ □□□□□.

Methods	Answer Area
A Microsoft Azure ATP sensor	Windows 8.1: <input type="text"/>
A local script	Windows 10: <input type="text"/>
Microsoft Monitoring Agent	Windows Server 2016: <input type="text"/>

Answer:

Methods	Answer Area
A Microsoft Azure ATP sensor	Windows 8.1: Microsoft Monitoring Agent
A local script	Windows 10: A local script
Microsoft Monitoring Agent	Windows Server 2016: Microsoft Monitoring Agent

□□:

□□:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/onboard-downlevel-windows-defender-advanced-threat-protection>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-endpoints-windows-defender-advanced-threat-protection>

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/configure-server-endpoints-windows-defender-advanced-threat-protection>

NEW QUESTION: 140

□□ □□ □□□ Microsoft Azure Active Director(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2

Your company uses Microsoft Intune.

Several devices are enrolled in Intune as shown in the following table.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

□□ □□□ □□ □□□ □□□ □□□□□.

* □□ □□□ □□□ □□ □□□□□.

* □□□ □ □□: Group1

* □□□□ □: Microsoft Office 365 Exchange Online

NEW QUESTION: 143

sk180818.onmicrosoft.com is a Microsoft Azure Active Directory (Azure AD) tenant. It contains four users as shown in the following table.

Name	Username	Type
User1	User1@sk180818.onmicrosoft.com	Member
User2	User2@sk180818.onmicrosoft.com	Member
User3	User3@sk180818.onmicrosoft.com	Member
User4	User4@gmail.com	Guest

Azure Information Protection (AIP) is configured on the tenant with a protection policy named Label1. The policy settings are shown in the following screenshot.

Protection settings

HYOK (AD RMS)

Select the protection action type

Set permissions

Set user-defined permissions (Preview)

USERS	PERMISSIONS
AuthenticatedUsers	Viewer
sk180818.onmicrosoft.com	Reviewer
User1@sk180818.onmicrosoft.com	Co-Owner
User2@sk180818.onmicrosoft.com	Co-Author

[+Add permissions](#)

Label1 is applied to a file named File1. The file is shared with the following users and permissions:

File1 is shared with User1, User2, User3, and User4. The permissions are as follows:

User1: Co-Owner
User2: Co-Author
User3: Reviewer
User4: Viewer

Statements

	Yes	No
User2 can modify File1.	<input type="radio"/>	<input type="radio"/>
User3 can print File1.	<input type="radio"/>	<input type="radio"/>
User4 can read File1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User2 can modify File1.	<input checked="" type="radio"/>	<input type="radio"/>
User3 can print File1.	<input type="radio"/>	<input checked="" type="radio"/>
User4 can read File1.	<input type="radio"/>	<input checked="" type="radio"/>

□□:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-usage-rights#rights-included-in-permissions-levels>

NEW QUESTION: 144

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

Microsoft 365 □□□ □□□□.

□□ □ □□ □□ □□ □□□□ eDiscovery Manager □□ □□□ □□□□ US eDiscovery Managers□□ □□ □□□ □□□□.

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

□□ □□: Windows PowerShell□□ □□□ □□ □□□ □□□□ New-ComplianceSecurityFilter cmdlet□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

□□/□□:

□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-filtering-for-content-search>

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-content-search/new-compliancesecurityfilter?view=exchange-ps>

NEW QUESTION: 145

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

□□ □□ □□□ □□□□ □□□□.

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

□□ □□□□ □□ □□□□□ □□□□ □□□□ □□ □□□□?

A. Admin2, Admin3 □ Admin4□ □□

B. Admin1, Admin2, Admin3 □ Admin4

C. Admin2 □ Admin3 □□

D. Admin3 □□

E. Admin1 □ Admin3 □□

Answer: E (LEAVE A REPLY)

□□□□□ □□ □□□ □□□□ □□□□ □□□□. □□ □□□ □□□ □□□, □□ □□ □□ □□ □□□□ □□□ □□□ □□□□ □□□□□.

NEW QUESTION: 146

□□□□ <https://myapps.microsoft.com>□ □□□□ □□□ □ □□ □□□□ □□□□□.



□□



□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/permissions-in-the-security-and-compliance-cent>

NEW QUESTION: 149

□□□□□ contoso.com□□□ Active Directory □□□□ □□□□. □□□□□ 100□□ Windows 8.1 □□□ □□□□. □□□□ □□ Windows 10 Enterprise □□□□ Windows 8.1 □□□□ □□□□□□. Windows 10 □□ □□□ □□□□□ □□□□. □□□□ □□□□□ □□□□?

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

Answer: C (LEAVE A REPLY)

<https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-10-with-the-microsoft-deployment-toolkit> □□ □□ □□□□□□ □□□□ □□ □□□□ □□□□. □□□□ □□ □□□□ □□□□ □□ □□ □□□□□□ □□□□ □□□□□□. □ □□□□□ □□□□ □□□□□□ □□□□□ □□ □□ Windows 10 □□□□□ □□□□□ □□ □□□□ □□□□. <https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/refresh-a-windows-7-computer-with-windows-10> □□□□ □□ □□□□ □□□□□□ □□□□ □□□□□□. □□□□

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

NEW QUESTION: 150

3□□ □□□□ □ □□□□ □□□□ □□□□ Microsoft□ □□□ □□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ □□□ 1□□ □□□ □□□□□.



Answer:

- 24□□
- 18□□

<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> 3□ □□ □□□□: 9□ □□□□□□ 18□□ □□ □□□ □□ □□ □□□□: □□□□□□ 30□□ □□ □□□□ □□:

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

NEW QUESTION: 151


Microsoft 365 □□□ □□□□. □□□ □□ □□ □□ □□□□ □□□□ □□□□. □□□□ □□ □□□ □□□ □□ □□□□ □□□□□ □□□. □□ □□□□ □□□ Microsoft SharePoint□□ □□ □□ □□□ □□□□ □□ □ □□□ □□ □□ □□ □□ □□ □□ □□ □□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ □□□ 1□□ □□□ □□□□□.

Opening files in SharePoint that contain malicious content:

- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links



Answer:

Opening files in SharePoint that contain malicious content:

- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links

Impersonation and spoofing attacks in email messages:

- Anti-spam
- ATP anti-phishing
- ATP safe attachments
- ATP Safe Links

□□:

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

MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
 DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□
 □□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 152

□□□□ Microsoft Azure ATP(Advanced Threat Protection) □ Microsoft Defender ATP□ □□□
 □□.
 Microsoft Defender ATP□ Azure ATP□ □□□□ □□□.
 □□□ □□□□□□□□□?

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

□□

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

□□:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-retention/set-retentioncom>

NEW QUESTION: 154

□□ □□□ □□ Microsoft Azure Information Protection □ □□□□ □□□□ □□□ Microsoft OneDrive □ □□□□.

Protection settings ⓘ

Azure (cloud key) HYOK (AD RMS)

Select the protection action type ⓘ

- Set permissions
 Set user-defined permissions (Preview)

USERS

PERMISSIONS

M365x901434.onmicrosoft.com

Co-Owner

...

+ Add permissions

Content expiration

Always Never **By days**

Number of days the content is valid

30 ✓

Allow offline access

Balance security requirements (includes access after revocation) with the flexibility to open protected content without an Internet connection. [More information and recommended settings](#)

Always Never **By days**

Number of days the content is available without an Internet connection

7 ✓

Protection template ID - template id is automatically generated after template is saved

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

If you copy the file to your local computer, you [answer choice]

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

Answer:

If you copy the file to your local computer, you [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

If you email the document to a user outside your organization, the user [answer choice].

- cannot open the document
- can open the document indefinitely
- can open the document for up to 7 days
- can open the document for up to 30 days

:

:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-protection>

NEW QUESTION: 155

contoso.com Azure AD(Azure Active Directory) Microsoft 36S . SharePoint Online 2TB . .

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

Azure Portal .

true .

: 1 .

Answer Area

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>

Answer:

- * Group1
- * Microsoft Office 365 Exchange Online
- * contoso.com, Azure AD(Azure Active Directory)

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 157

contoso.com Azure AD(Azure Active Directory)

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

Microsoft Intune contoso.com

Configure

Microsoft Intune

Save Discard Delete

MDM user scope None Some All

Groups Select groups >
Group1

MDM terms of use URL

MDM discovery URL

MDM compliance URL

[Restore default MDM URLs](#)

MAM User scope None Some All

Groups Select groups >
Group2

MAM Terms of use URL

MAM Discovery URL

MAM Compliance URL

[Restore default MAM URLs](#)

Device1 is a Windows 10 device.
User1 is a user in the contoso.com domain.
User2 is a user in the contoso.com domain.
User3 is a user in the contoso.com domain.

Statements

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

Answer:

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

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

:

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

NEW QUESTION: 158

□□□ □□□ □□(□□)□ □□□□.

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

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

□□ □□ □□□□□.

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].



- allowed
- blocked without warning
- blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

- allowed
- blocked without warning
- blocked, but the user can override the policy

NEW QUESTION: 159

Microsoft 365 □□□ □□□□.

□□□□□ 51.40.15.0/24□ IP □□ □□□ □□□□□.

Exchange Online □□□□ □□□ □□□□□ □□□□□ Role1□□□ □□□ □□□□□□.

□□ □□ □□□ □□ □□□□ □□□ □□□□ □□□.

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

□□ □□□□ □□□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Activities to search for: Microsoft ▾

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

Field to filter by: Microsoft ▾

- Item
- User
- Detail
- IP address

Answer:

Activities to search for:

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

Field to filter by:

- Item
- User
- Detail
- IP address

NEW QUESTION: 160

Microsoft Office 365 .

eDiscovery .

User	Task
User1	<ul style="list-style-type: none"> • Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. • View the eDiscovery cases created by User1. • Configure case settings. • Place content on hold.
User2	<ul style="list-style-type: none"> • View the eDiscovery cases created by User1. • Export data from Advanced eDiscovery.

.

? .

: 1 .

- User1:
- eDiscovery Administrator
 - eDiscovery Manager
 - Records Management
 - Reviewer
 - Security Administrator

- User2:
- eDiscovery Administrator
 - eDiscovery Manager
 - Records Management
 - Reviewer
 - Security Administrator

Answer:



□□



□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION: 161

□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □□□□ □ □□□□ □ □□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □□□ □ □□□□ □□ □ □□□□ □□ □ □□□ □□ □ □□□ □□ □ □□□ □□ □ □□□□ □□ □ □□□□. □□□□ □□□ □□ □ □□□ □□□□ □□ □ □□□□. □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ Windows Server 2019□ □□□□ □□□ □□□□□ □□□□ □□□□. □□□□□ □□□□ □□ □□□□ Windows Server 2012 R2□□□□. □□□□□ Windows 10□ □□□□ □□□ 100□□□ Windows Server 2012 R2□ □□□□□ Server1□□□□ □□□ □□□ □□□□□. Server1□ □□□□ □□□□□ □□□□□ Windows 10 □□ □□ □□□ □□□ □□□□□. Server1□ GPMC(□□ □□ □□ □□)□ □□□□□□. Server1□□ □□□□□□ Windows □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

□□ □□: Windows 10 □□□□□ Server1□ □□ □□ □□ □□□□ □□□□□.
 □□□ □□□ □□□□□?

A. □

B. □□□

Answer: ([SHOW ANSWER](#))

□□: [□□]

NEW QUESTION: 162

□□ □□ □□□ □□□□ □□□ Microsoft Azure □□ □□□□(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

Group3□ Group1□ □□□□□□.

□□□□ Windows Defender ATP(Advanced Threat Protection)□ □□□□□. Windows Defender ATP□□ □□ □□ □□□ □□□□ □□□□.

Name	Permission	Assigned user group
Windows Defender ATP administrator (default)	View data, Alerts investigation, Active remediation actions, Manage security settings	None
Role1	View data, Alerts investigation	Group1
Role2	View data	Group2

Windows Defender ATP□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Rank	Machine group	Machine	User access
1	ATP1	Device1	Group1
Last	Ungrouped machines (default)	Device2	None

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

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
User1 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can sign in to Windows Defender Security Center.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can view Device1 in Windows Defender Security Center.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 163

□□□ □ □□

□□□□□□ Azure AD(Azure Active Directory) □ □□□□□ □□□□□□ Active Directory □□ □□ □□□□ □□□□. □□□□□□ □□ □□ □□□ □□□ □□□□□□.

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

Azure Information Protection □ □□□□□.

Azure Information Protection □□□□ Server1 □ □□ □□□□ □□□ □ □□□ □□□□ □□ □.

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

□□ □ □□:

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

Answer Area

Answer:

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

□□: [□□]

□□/□□:

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

NEW QUESTION: 164

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

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

Answer: D (LEAVE A REPLY)

□□:

https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/saf

NEW QUESTION: 165

Microsoft Intune □ □□ □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ □□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□
□.

Name	Role	Member of
User1	Cloud device administrator	Group1
User2	Intune administrator	Group2
User3	None	None

Intune □ □□□□ □□ □□□ □□ □□ □□ □□□□□.

Priority	Name	Device limit	Assigned to
1	Policy1	15	Group2
2	Policy2	10	Group1
Default	All users	5	All users

Intune □□ □□ □□ □□□□ User3 □ □□□□□.
□□ □ □□ □□ □□ □□ □□□ □□ □□□□□. □□□□ □□□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□□.

Statements

- User1 can enroll a maximum of 10 devices in Intune.
- User2 can enroll a maximum of 10 devices in Intune.
- User3 can enroll an unlimited number of devices in Intune.

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



Answer:

Statements



Yes

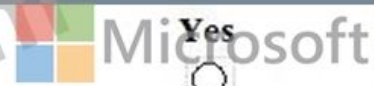
No

User1 can enroll a maximum of 10 devices in Intune.

User2 can enroll a maximum of 10 devices in Intune.

User3 can enroll an unlimited number of devices in Intune.

Statements



Yes

No

User1 can enroll a maximum of 10 devices in Intune.

User2 can enroll a maximum of 10 devices in Intune.

User3 can enroll an unlimited number of devices in Intune.

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

NEW QUESTION: 166

Microsoft Azure Active Directory(Azure AD) contoso.com Active Directory

Microsoft System Center Configuration Manager(SCCM)

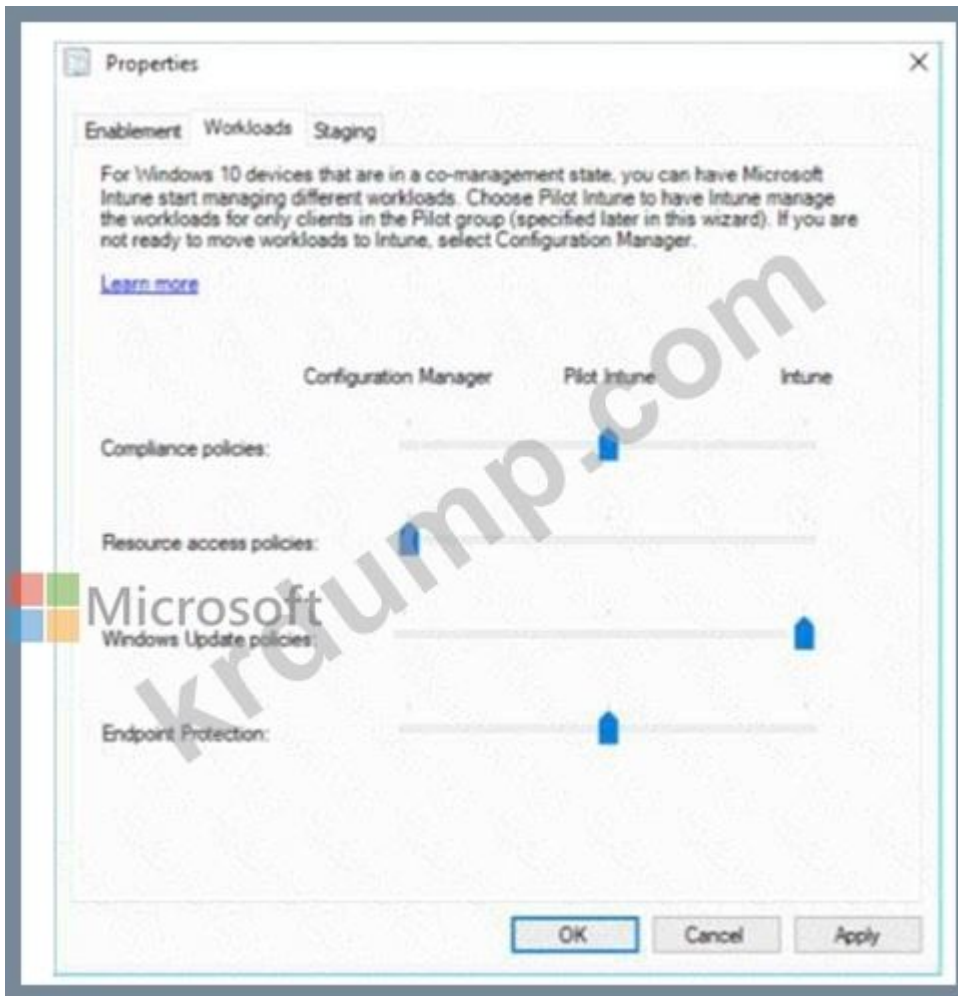
Windows 10

Name	Collection
Device1	Collection1
Device2	Collection2

Configuration Manager

* Intune

* Collection2



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

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
Microsoft Intune manages Endpoint Protection for Device2.	<input checked="" type="radio"/>	<input type="radio"/>

□□

Answer Area	Statements	Yes	No
	Microsoft Intune manages the compliance policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
	Configuration Manager manages the Windows Update policies for Device1.	<input type="radio"/>	<input checked="" type="radio"/>
	Microsoft Intune manages Endpoint Protection for Device2.	<input checked="" type="radio"/>	<input type="radio"/>

MS-101 <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps, **30%OFF Special Discount: KrDump**)

NEW QUESTION: 167

Microsoft 365 E5

Name	Role
User1	Global admin
User2	None
User3	None

Microsoft Store

Microsoft Store

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

Microsoft Store

Microsoft Store

100

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

Answer:

In Azure:

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

On the computers:

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

□□

□□□ □□□ □□□□□, □□□, □□□□□□ □□□ □□□□ □□□

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

□□:

<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-rol>

NEW QUESTION: 168

□□ □□ □□ Microsoft 365□ □□ □□□ □□□□□.

Name	Location
Policy1	OneDrive accounts
Policy2	Exchange email, Exchange public folders, Office 365 groups, OneDrive accounts, SharePoint sites

Policy1□ Policy1 □□□ □□□ □□ □□□□□□. (□□1 □□ □□□□□□.)

Decide if you want to retain content, delete it, or both

Do you want to retain content? ⓘ

Yes, I want to retain it ⓘ

For this long... 7 years

No, just delete content that's older than ⓘ

2 years

Delete the content based on when it was created ⓘ

Need more options?

Use advanced retention settings ⓘ

Back Next Microsoft

Policy2 Policy2 □□□ □□□ □□ □□□□□. (□□

Decide if you want to retain content, delete it, or both

Do you want to retain content?

Yes, I want to retain it

For this long... 4 years

Retain the content based on when it was created

Do you want us to delete it after this time?

Yes No

No, just delete content that's older than ⓘ

2 years

Need more options?

Use advanced retention settings ⓘ

Back Next Cancel

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

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
If a user creates a file in Microsoft OneDrive on January 1, 2018, users will be able to access the file on January 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2020.	<input checked="" type="radio"/>	<input type="radio"/>
If a user deletes a Microsoft OneDrive file that was created on January 1, 2018, an administrator will be able to recover the file on April 15, 2023.	<input checked="" type="radio"/>	<input type="radio"/>

<https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies#the-principles-of-retention-or->

NEW QUESTION: 169

contoso.com Active Directory

Name	IP address
Server1	192.168.1.10
Server2	192.168.2.10

File1.abc Server1 . File2.abc Server2 . App1, App2 App3

WIP(Windows Information Protection)

App2

App1

Windows

IPv4 : 192.168.1.1-192.168-1.255

File1.abc

.

1

Statements	Yes	No
You can open File1.abc in App1.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can open File1.abc in App1.	<input checked="" type="radio"/>	<input type="radio"/>
You can open File1.abc in App2.	<input checked="" type="radio"/>	<input type="radio"/>
You can open File1.abc in App3.	<input type="radio"/>	<input checked="" type="radio"/>

□□:

<https://docs.microsoft.com/en-us/windows/security/information-protection/windows-information-protection/create-wip-policy-using-intune-azure>

NEW QUESTION: 170

Azure AD(Azure Active Directory) □□□□ Microsoft 365 E5 □□□ □□□□. □□□□□ □□ □□ □□□□ □□□□□.

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

Microsoft Defender Advanced Threat Protection(Microsoft Defender ATP)□ □□□ □□□□□.

Microsoft Defender ATP□□ RBAC(□□ □□ □□□ □□)□ □□ □□□ □□□□□.

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

□□ □□□□ □□□□ □□□?

A. □□□1

B. □□□4

C. □□□2

D. □□□3

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

NEW QUESTION: 171

□□□ Microsoft 365 □□□ □□□□.

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

* Microsoft SharePoint□ 2□□ □□□□□ □□ □□

* □□□□ □□□□ □□ □□□□ □□□□□.

* □□□ □□□□ □□□
□□□ □□□□□□□?

- A. Microsoft Azure Activity Directory(Azure AD) □□ □□
- B. □□ □ □□ □□ □□□ □□
- C. Microsoft Azure Activity Directory(Azure AD) □□□
- D. □□ □ □□ □□ □□ □□ □□

Answer: A (LEAVE A REPLY)

□□/□□:
□□:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/activity-logs-overview>

NEW QUESTION: 172

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

Microsoft 365 □□□ □□□□.

□□□□ □-□□□□ □□□□□ □□□□ □□ □□□ □□□□ Microsoft SharePoint Online □
□□□ □□□□□ □□□□ □□ □□□.

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

□□□ □□□ □□□□□?

- A. □
- B. □□□

Answer: B (LEAVE A REPLY)

□□

SharePoint Online□ □□□ □□□□ IP □□ □□ □□□ □□□□ □□□□ □□□□ □□□
□ □□□□.

□□:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Onlinean>

NEW QUESTION: 173

□□□ Azure Directory(Contoso.com□□□ Azure AD0 □□□)□ □□□□ Microsoft 365 □□□
□□□□. □□□□ □□ □□ □□□ □□□□ □□□□□.

□□ □□□ □□□□ Label1□□□ □□ □□□□ □□□□□.

□□□□ 5□□ □□□□□.

5□ □□ □ □□ □□□□ □□□□ □□□□□.

Policy1□□□ □□□ □□□□ Label1 b□ □□ □□ □□□ □□□ □□□. Policy1□□ □□□
□□ □□□ □□□□□.

* 500 000 00

* 50 00 0 00 0000 0000 00

Policy1 000 000 0000 000 10 00 00 000 000 000. 0000 000 0 000 0000.

* Merger 00 000 000 0000 00000.

* OneDrive 00 0 SharePoint 000 00 00 00 000 00000.

RetentionCompliancePolicy Policy1 RestrictiveRetention \$true 00 00

Answer Area

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

Answer:

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

NEW QUESTION: 174

00 00 000 Microsoft Azure Active Directory(Azure AD) 0000 0000.

Name	Member of
User1	Group1
User2	Group2

0000 Microsoft Intune 0 00000.

00 00 00 00 000 Intune 0 0000 0000.

Name	Platform	BitLocker Drive Encryption (BitLocker)	Member of
Device1	Windows 10	Disabled	Group3
Device2	Windows 10	Disabled	Group4

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

Name	Require BitLocker	Assigned to
Policy1	Not configured	Group3
Policy2	Require	Group4

□□ □□□ □□ □□□ □□□ □□□□□.

□□ □□□ □□□ □□ □□□□□.

* □□□ □ □□: Group1

* □□□□ □: Microsoft Office 365 Exchange Online

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

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Statements

User1 can access Microsoft Exchange Online from Device1.

Yes

No

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

Answer:

Statements

User1 can access Microsoft Exchange Online from Device1.

Yes

No

User1 can access Microsoft Exchange Online from Device2.

User2 can access Microsoft Exchange Online from Device2.

□□

Statements	Yes	No
User1 can access Microsoft Exchange Online from Device1.	<input checked="" type="radio"/>	<input type="radio"/>
User1 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access Microsoft Exchange Online from Device2.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION: 175

□□□□ Windows Defender ATP(Advanced Threat Protection)□ □□□□□. Windows Defender ATP□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Rank	Machine group	Member
1	Group1	Name starts with COMP
2	Group2	Name starts with Comp And OS In Windows 10
3	Group3	OS In Windows Server 2016
Last	Ungrouped machines (default)	Not applicable

□□ □□ □□ Windows Defender ATP□ □□□□ □□□□□□.

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2016

Computer1 □ Computer2 □□□□ □□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

Computer1:

Microsoft

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2:

- Group1 only
- Group3 only
- Group1 and Group3

Answer:

Computer1:

- Group1 only
- Group2 only
- Group1 and Group2
- Ungrouped machines

Computer2:

- Group1 only
- Group3 only
- Group1 and Group3

3□□ □□□□ □ □□□□ □□□□ □□□□ Microsoft□ □□□ □□ □ □□□□? □□□□□
□□ □□□□ □□□ □□□ □□□□□□.
□□: □ □□□ □□□ 1□□ □□□ □□□□.

Seattle:	<input type="text"/>
	6 months
	18 months
	24 months
	30 months
	5 years
New York:	<input type="text"/>
	6 months
	18 months
	24 months
	30 months
	5 years

Answer:

Seattle:



New York:



□□:

<https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet> 3□ □□ □□□□:
□□□ □□□□□ 18□□ □□ □□□ □□ 9□ □□ □□□□: □□□ □□□□□ 30□□ □□
□□□

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

□□ 2, □□

□□ □□

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

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

□□ □□□ □□□□□
□ □□ □□□ □ □□ □□□ □□□□□ □□ □□□ □□□□□□. □□□ □□□ □□ □□ □
□ □□ □□□ □□□□ □□ □□□ □□□ □□□□□□. □ □□□ □□□□ □□□□ □□ □
□, □□ □□ □ □□ □□□ □□ □□□ □□□□□. □□□ □□ □□□ □□ □□ □□□ □□
□□ □□□□ □□□□□.

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

□□ □□□□ Microsoft 365□□ □□□□□□□. □ □□□□ □□□□□□ □□□□ □□□ □□
□ □□ □□ □□□□ □□□□(□: user1@us.adatum.com □□ user2#uk.ad3tum.com).

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

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

SIEM □□□□□□□□ □□ □□□□ □□□ □□□ □ □□□ □□ □□□□ □□□□□□ □□
□□□.

SharePoint □□□□ □□ □□□□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □ □□□
□□□□□.

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

□□ □□(EU) □□□ PII □□□□ □□□ □□ □ □□□ □□□□ 10□ □□ □□□□□ □□
□.

□□□□ 30□ □□□ Microsoft SharePoint Online□□ 1,000□ □□□ □□□ □□□□□□□□
□□ □□ □□□□□ □□□ □□□ □□□ □□ □□□□□.

□□ □□□□ □□□□ Microsoft 36S □□□□ □□□□ □□□□ □□□□□. □ □□□□ □□
□□ □□ □□□□ □□□□ □□□ □ □□□ □□□ □□□□ □□□ □□□□.

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

□□ □□ □□□ □□□□□ PII □□□□ □□□□□. □□ □□□ □□ □□□ □□□□ □□□
□□□ □□□. □□ □□□□ □□□□ □□□ □□ PII □□□□ □□□ □□□□ □□□ □□□
□ □□□□ □□□□ □□□□ □ □□□ □□□.

NEW QUESTION: 177

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

Cloud App Security□ SIEM(□□ □□ □ □□□ □□)□ □□□ □□□□□.

Windows Server 2016□ □□□□ □□□ SIEM □□□□□ □□□□ □□□.

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

Answer:

First action to perform:

- Install Java 8.
- Install Microsoft .NET Framework 3.5.
- Add the Windows Internal Database feature.
- Add the Setup and Boot Event Collection feature.

Second action to perform:

- Run the Set-MMagent cmdlet.
- Add the Setup and Boot Event Collection feature.
- Run the java command and specify the -jar parameter.
- Run the Install-WindowsFeature cmdlet and specify the -source parameter.

:

:

<https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-your-siem-server-with-office-365-cas>

NEW QUESTION: 178

Microsoft 365 .

Microsoft Azure ATP(Advanced Threat Protection) .

5 ?

.

ACTIONS	ANSWER AREA
Download the Azure ATP sensor setup package.	
Create a Security & Compliance threat management policy.	
Create an Azure Active Directory (Azure AD) conditional access policy.	
Install sensors.	
Create a workspace.	
Enter credentials.	
Configure the sensor settings.	

Answer:

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6

Kidump.com



□□:

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

NEW QUESTION: 181

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

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

Microsoft 365 □□□ □□□□.

□□□□ □-□□□□ □□□□□ □□□□ □□ □□□ □□□□ Microsoft SharePoint Online □ □□□ □□□□□ □□□□ □□ □□□.

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

A. □

B. □□□

Answer: B (LEAVE A REPLY)

□□

□□:

SharePoint Online□ □□□ □□□□ IP □□ □□ □□□ □□□□ □□□□ □□□□ □□□ □ □□□□.

□□:

<https://techcommunity.microsoft.com/t5/Microsoft-SharePoint-Blog/Conditional-Access-in-SharePoint-Online-and-OneDrive-for/ba-p/46678>

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

Microsoft Endpoint Manager can be used to manage mobile devices and apps. It can be used to manage iOS, Android, and Windows devices and apps. It can be used to manage apps that are installed on mobile devices. It can be used to manage apps that are installed on Windows devices. It can be used to manage apps that are installed on Windows devices. It can be used to manage apps that are installed on Windows devices.

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

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"/>

□□:

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

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

NEW QUESTION: 184

Windows Defender Advanced Threat Protection(Windows Defender ATP) can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices.

Name	Rank	Members
Group1	1	Operating system in Windows 10
Group2	2	Name ends with London
Group3	3	Operating system in Windows Server 2016
Ungrouped machines (default)	Last	Not applicable

□□ □□ □□ Windows Defender ATP can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices. It can be used to protect Windows devices.

Name	Operating system
Computer1-London	Windows 10
Server1-London	Windows Server 2016

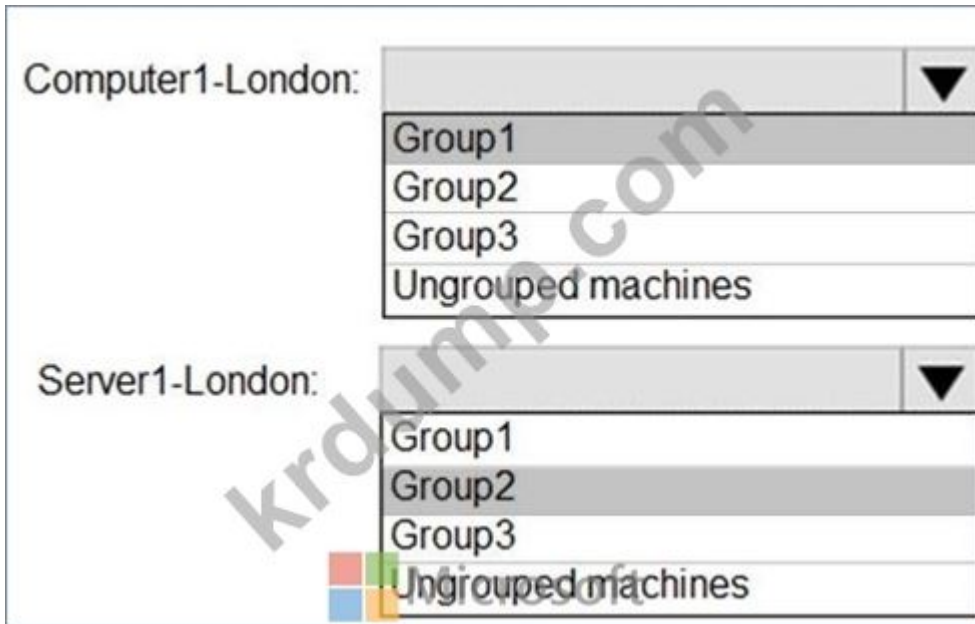
□ □□□□ □□ □□□ □□□ □□□□□? □□□□□ □□□□ □□□ □□□ □□□□□□□□.
 □□: □ □□□ □□□ 1□□ □□□ □□□□□.

The screenshot shows the Active Directory console with two objects selected: Computer1-London and Server1-London. For Computer1-London, the 'Members' list includes Group1, Group2, Group3, and Ungrouped machines. For Server1-London, the 'Members' list includes Group1, Group2, Group3, and Ungrouped machines. A watermark 'Krdump.com' is visible across the image.

Answer:

The screenshot shows the Active Directory console with two objects selected: Computer1-London and Server1-London. For Computer1-London, the 'Members' list includes Group1, Group2, Group3, and Ungrouped machines. For Server1-London, the 'Members' list includes Group1, Group2, Group3, and Ungrouped machines. In this screenshot, Group1 and Group2 are highlighted with green dashed boxes. A watermark 'Krdump.com' is visible across the image.

□□



NEW QUESTION: 185

Microsoft Office 365 □□□ □□□□.

□□ □□ □□ eDiscovery □□□ □□□□ □□□.

User	Task
User1	<ul style="list-style-type: none"> • Decrypt Microsoft Azure Rights Management (Azure RMS)-protected content. • View the eDiscovery cases created by User1. • Configure case settings. • Place content on hold.
User2	<ul style="list-style-type: none"> • View the eDiscovery cases created by User1. • Export data from Advanced eDiscovery.

□□□□ □□ □□ □□□ □□□ □□□.

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

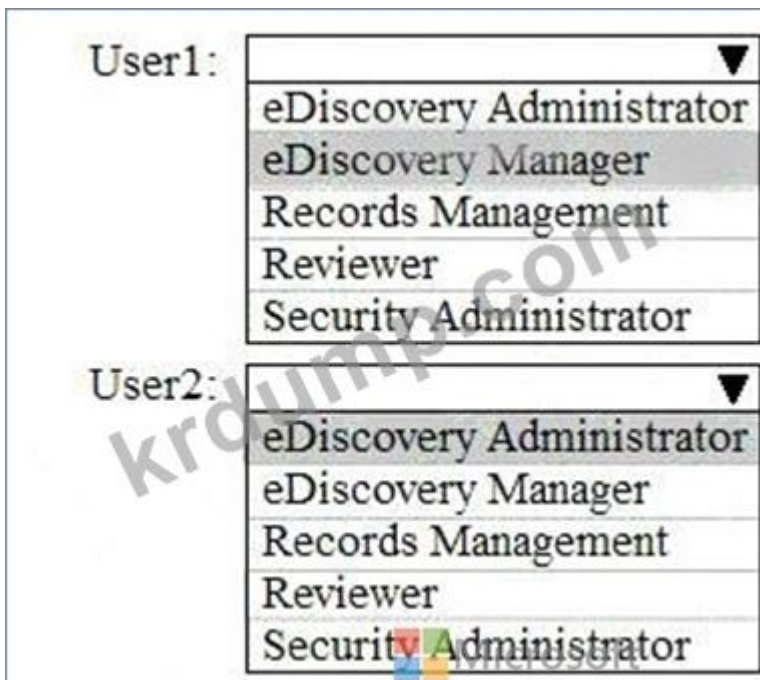
□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



□□



□□:

<https://docs.microsoft.com/en-us/office365/securitycompliance/assign-ediscovery-permissions>

NEW QUESTION: 186

contoso.com Active Directory . 100 Windows 8.1 Windows 10 Enterprise Windows 8.1 Windows 10 .

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

Answer: B (LEAVE A REPLY)

: []
/ :
:

<https://docs.microsoft.com/en-us/microsoft-365/enterprise/windows10-infrastructure>

NEW QUESTION: 187

User1 User2 Azure AD(Azure Active Directory) .
2019 9 5 (ToU) . ToU .

: 1
 : 1
 :
 :
 : 2019 10 10
 :

User1 2019 9 5 1 . User2 2019 10 5 1 .
 .
 1 ?
 : 1 .

B. SharePoint □□ □□□□ □□ □□□ □□□□.

C. □□ □ □□ □□ PowerShell□□ New-DataClassificationcmdlet□ □□□□□.

D. □□ □ □□ □□ PowerShell□□ New-DlpComplianceRulecmdlet□ □□□□□.

Answer: (SHOW ANSWER)

□□: [□□]

□□/□□:

<https://docs.microsoft.com/en-us/powershell/module/exchange/policy-and-compliance-dlp/new-dataclassification?view=exchange-ps>

NEW QUESTION: 189

□□□ □□ □□□ □□ □□□ □□□□□□□

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

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

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.	

□□:

□□:

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

NEW QUESTION: 190

Azure AD(Azure Active Directory) Microsoft Endpoint Configuration Manager .

.

Name	Platform	Configuration
Device1	Windows 10	Hybrid joined to on-premises Active Directory and Azure AD only
Device2	Windows 10	Joined to Azure AD and enrolled in Configuration Manager only
Device3	Windows 10	Enrolled in Microsoft Endpoint Manager and has the Configuration Manager agent installed only

.

.

?

- A. Device1
- B. Device2 Device3
- C. 1, 2 3
- D. Device2
- E. Device3

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

NEW QUESTION: 191

contoso.com Azure AD(Azure Active Directory) Microsoft 365 . SharePoint Online 2TB . .

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

Statements	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>

Answer:

NEW QUESTION: 192

Microsoft Intune .

Microsoft Azure Active Directory(Azure AD) .

Name	Member of
User1	Group1
User2	Group1, Group2
User3	None

Microsoft

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

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

You add User3 as a device enrollment manager in Intune.

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

☐☐: ☐ ☐☐☐ ☐☐☐ 1☐☐ ☐☐☐☐ ☐☐☐☐.

Answer Area

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

Answer:

Answer Area

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

☐☐

Answer Area

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

Name	Architecture	Memory	Applications installed
Computer1	64-bit	1 GB	App1
Computer2	32-bit	2 GB	App2

Computer3 has 8 GB of memory and is 64-bit.

Name	UpgradeDecision
App1	Ready to upgrade
App2	Review in progress

Computer3 has App1 and App2 installed. Computer3 has 8 GB of memory and is 64-bit.

8 GB of memory

64-bit architecture

App3 is installed on Computer3.

App3 has an UpgradeDecision status of Ready to upgrade.

Which of the following statements are true?

Statements: Computer1 has an UpgradeDecision status of Ready to upgrade.

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>
Computer2 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>
Computer3 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
Computer1 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input checked="" type="radio"/>
Computer2 has an UpgradeDecision status of Ready to upgrade.	<input type="radio"/>	<input checked="" type="radio"/>
Computer3 has an UpgradeDecision status of Ready to upgrade.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION: 195

Windows 10 Intune app is installed on a device.

Intune app is installed on a device. What is the status of the app?

- A. Installed
- B. Not installed
- C. Uninstallable
- D. Uninstalling

Answer: D (LEAVE A REPLY)

□□ 2, □□ □□ □□

□□ □□

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

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

□□ □□□ □□□□□

□ □□ □□□ □ □□ □□□ □□□□□ □□ □□□ □□□□□□. □□□ □□□ □□ □□ □ □□ □□□ □□□□ □□ □□□ □□□ □□□□□□. □ □□□ □□□□ □□□□ □□ □□, □□ □□ □ □□ □□□ □□ □□□ □□□□□. □□□ □□ □□□ □□ □□ □□□ □□ □□ □□□□ □□□□□.

□□ □□□

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

□□ □□□ □□□ Microsoft 365□ □□□□□□□□□□.

□□ □□□□ Microsoft 365□□ □□□□□□. □ □□□□ □□□□□□ □□□□ □□□ □□ □ □□ □□ □□□□ □□□□(□: user1@us.adatum.com □□ user2#uk.ad3tum.com).

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

□ . Datum□ □□ □□ □□(PII)□ □□□□ □□□□□□.

□□ □□

□□ □□

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

□□ □□

□ . Datum□ □□ □□□ □□ □□ □□□ □□ □□ □□□□ □□□ □□□ □□ □□□□□□.

□ . Datum□ □□□ □ □□□□ □ □□□□□ □□□ □□□□□□ □□□□.

□□ □□ □□

* □□ □□□□ □□ □□ □□□ □□□□ □□□□□□.

* SIEM □□□□□□□□ □□ □□□□ □□□ □□□ □ □□□ □□ □□□□ □□□□ □□□□ □□□□.

* SharePoint □□□□ □□ □□□□□□ □□□ □□ □□□ □□□□ □□□□ □□□ □ □□ □ □□□□□□.

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

* □□ □□(EU) □□□ PII □□□□ □□□ □□ □ □□□ □□□□ 10□ □□ □□□□□□.

* 30 Microsoft SharePoint Online 1,000 Microsoft Office 365 licenses.

* Microsoft 365 Microsoft Office 365 licenses. Microsoft Office 365 Microsoft Office 365 licenses.

* Microsoft Office 365 Microsoft Office 365 licenses. Microsoft Office 365 Microsoft Office 365 licenses. Microsoft Office 365 Microsoft Office 365 licenses. Microsoft Office 365 Microsoft Office 365 licenses.

NEW QUESTION: 196

Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security.

Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security. Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security.


Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security Microsoft Cloud App Security.

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

□□

Minimum number of data sources:

▼
1
3
6

Minimum number of log collectors:

▼
1
3
6



□□:

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

MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
 DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□
 □□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)

NEW QUESTION: 197

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

Name	Role
User1	Global admin
User2	None
User3	None

□□□□□ Microsoft Store□□ □□ □□□□ □□□□□□□□.

□□ □□ □□ □□□□□ Microsoft Store □□□ □□□□□ □□□□□□.

Name	Role
User1	None
User2	Purchaser
User3	Basic Purchaser

Can add apps to the private store: Microsoft Store
 Can assign apps from Microsoft Store for Business:
 User2 only
 User1 and User2 only
 User2 and User3 only
 User1, User2, and User3

Can add apps to the private store:  Microsoft

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:

Can assign apps from Microsoft Store for Business:

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

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

Can

Can assign apps from Microsoft Store for Business, User2 only, User1 and User2 only, User2 and User3 only, User1, User2, and User3

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	

□□:

<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-rol>

NEW QUESTION: 198

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

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



	▼
Audit log	
Data governance events	
DLP policy matches	
eDiscovery	

Filter by:

	▼
Activity	
Detail	
Item	
User agent	

Answer:

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



- Audit log
- Data governance events
- DLP policy matches
- eDiscovery

Filter by:

- Activity
- Detail
- Item
- User agent

□□:

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

NEW QUESTION: 199

Contoso.onmicrost.com□□□ Microsoft Azure Active Directory(Azure AD) □□□□ □□□□. Microsoft 365 □□□ □□□□. □□□ □□□□ □□□ Windows 10 □□□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□. □□□ □□□□ □□□?

- A. □□ □□
- B. □□□ □□ □□ □□ □□
- C. □□□ □□ □□(MDM) □□
- D. Windows □□ □□

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 200

□□ □□□ □□ DLP1□□□ □□□ □□ □□(DLP) □□□ □□□□□.

Choose the types of content to protect

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

Content contains

Any of these ▾

Sensitive info type

Match accuracy

Credit Card Number

min max
85 100 ×

Retention labels

1 year

Add ▾



Microsoft

+ Add group

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□

□□: □ □□□ □□□ 1□□ □□□ □□□□.



DLP1 cannot be applied to [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

Answer:



DLP1 cannot be applied to [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

□□

DLP1 cannot be applied to [answer choice].

- Exchange email
- SharePoint sites
- OneDrive accounts

DLP1 will be applied only to documents that have [answer choice].

- both a credit card number and the 1 year label applied
- either a credit card number or the 1 year label applied
- between 85 and 100 credit card numbers

SharePoint Online OneDrive

:

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

NEW QUESTION: 201

Microsoft 365

Microsoft 365

20

?

1

<p>ATP anti-phishing</p> <p>Protect users from phishing attacks (like impersonation and spoofing), and use safety tips to warn users about potentially harmful messages.</p>	<p>ATP safe attachments</p> <p>Protect your organization from malicious content in email attachments and files in SharePoint, OneDrive, and Teams.</p>	<p>ATP Safe Links</p> <p>Protect your users from opening and sharing malicious links in email messages and Office 2016 desktop apps.</p>
<p>Anti-spam</p> <p>Protect your organization's email from spam, including what actions to take if spam is detected.</p>	<p>DKIM</p> <p>Add DKIM (DomainKeys Identified Mail) signatures to your domains so recipients know that email messages actually came from your users.</p>	<p>Anti-malware</p> <p>Protect your organization's email from malware, including what actions to take and who to notify if malware is detected.</p>

Answer:

Create a policy to retain what you want and get rid of what you don't.

Name your label

Label settings

Review your settings

Microsoft

Review your settings

⚠ It will take up to 1 day to apply the retention policy to the locations you chose.

Name
6Months [Edit](#)

Description for admins [Edit](#)

Description for users [Edit](#)

Retention [Edit](#)
6 months
Retain and Delete
Based on when it was created

[Back](#)

[Create this label](#)

[Cancel](#)

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

Automatically apply a label to content

Choose label to auto-apply

Choose conditions

Name your policy

Locations

Review your settings

Detect content that matches this query: X

^ Conditions

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

Keyword query editor

ProjectX

□□□ □□□ □□ □□ □□ □□□□□.

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

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

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

Answer:

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"/>

□□:

□□:

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

NEW QUESTION: 205

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

User1□□□ □□□□ □□□ Azure AD(Azure Active Directory) □□□□ □□□□.

□□□□ Microsoft 365 □□□ □□□□□.

Cloud App Security □□ □□□□ □□ □□□ □□□ □□□□ □ □□□ □□□ User1

□ □□□□□□ □□□□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

□□/□□:

□□:

<https://docs.microsoft.com/en-us/cloud-app-security/manage-admins>

NEW QUESTION: 206

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

Microsoft 365 □□□ □□□□.

□□□□ □-□□□□ □□□□□ □□□□ □□ □□□ □□□□ Microsoft SharePoint Online □

□□□ □□□□□ □□□□ □□ □□□.

New DLP policy

- Choose the information to protect
- Name your policy
- Choose locations
- Policy settings

Review your settings



Review your settings

Template name Edit
U.K. Personally Identifiable Information (PII) Data

Policy name Edit
U.K. Personally Identifiable Information (PII) Data

Description Edit

Applies to content in these locations Edit
Exchange email
SharePoint sites
OneDrive accounts

Policy settings Edit
If the content contains these types of sensitive info: U.K., National Insurance Number (NINO)U.S. / U.K. Passport Number then notify people with a policy tip and email message.

If there are at least 10 instances of the same type of sensitive info, block access to the content and send an incident report with a high severity level but allow people to override.

Turn policy on after it's created? Edit
Yes

Back Create Cancel

□□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□ □ □□□ □□□□ □□□ □□□□

□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□.

□□□ □□:

<e ip="769890ae5c7c741a6e6b585472b537fc.jpg"></ e>

Answer:

Answer Area

If a user attempts to upload a document to a Microsoft SharePoint site, and the document contains one UK passport number, the document will be [answer choice].

allowed
blocked without warning
blocked, but the user can override the policy

If a user attempts to email 100 UK passport numbers to a user in the same company, the email message will be [answer choice].

allowed
blocked without warning
blocked, but the user can override the policy

□□: [□□]

□□/□□:

□□:

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

NEW QUESTION: 208

□□ □□□ □□ DLP1□□□ □□□ □□ □□(DLP) □□□ □□□□□.

Choose the types of content to protect

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

Content contains *

Any of these ▾

Sensitive info type

Match accuracy

min max

Credit Card Number

85 100

×

Retention labels

1year

×

Add ▾

+ Add group

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.

DLP1 will be applied only to documents that have [answer choice].

DLP1 will be applied only to documents that have [answer choice].

Answer:

DLP1 will be applied only to documents that have [answer choice].

DLP1 will be applied only to documents that have [answer choice].

□□

DLP1 will be applied only to documents that have [answer choice].

DLP1 will be applied only to documents that have [answer choice].

□□:

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

NEW QUESTION: 209

Microsoft 365 □□□ □□□□.

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

□□ □□□ □□ □□□□□.

10□ □□ SharePoint Online□ □□□ 5□ □□□ □□□□ □□□□ □□□ □□□□ □□□ □□□□ □□ □□□.

□□ □□□ □□ □□□?

A. Microsoft Office 365 Cloud App Security□ □□□□□□.

B. Windows Defender Advanced Threat Protection(Windows Defender ATP) □□

C. Microsoft Office 365 Analytics□ □□□□□□.

Answer: B (LEAVE A REPLY)

□□ 1, □□ □□

□□

□□ □□

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

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

□□ □□□ □□□□□

□ □□ □□□ □ □□ □□□ □□□□□ □□□ □□□□□□. □□□ □□□ □□ □□ □□ □ □□□ □□□□ □□ □□□ □□□ □□□□□□. □ □□□ □□□□ □□□□ □□ □□, □ □□ □ □□ □□□ □□ □□□ □□□□□. □□□ □□ □□□ □□ □□ □□□ □□ □□ □□□. Datum□ □□□ Microsoft 365 □□□ □□□□□□.

□□ □□□ □□□ Microsoft 365□ □□□□□□□□□□.

□□ □□□□ Microsoft 365□□ □□□□□□. □ □□□□ □□□□□□ □□□□ □□□ □□ □ □□ □□ □□□□ □□□□(□: user1@us.adatum.com □□ user2#uk.ad3tum.com).

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

A: Datum□ □□ □□ □□(PII)□ □□□□ □□□□□.

□□ □□

□□ □□

A: □□□□ □□□ □□□□. □□ □□□ Microsoft 365□ □□ User1□□□ □□□□ □□ □□ □ □□□□ □□□.

□□ □□

A: Datum□ □□□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□ □□□ □□ □□□□ □.

A: Datum□ □□□ □ □□□□ □ □□□□□ □□□ □□□□□□ □□□□.

□□ □□ □□

A: Datum□ □□□ □□ □□ □□ □□□ □□□□□.

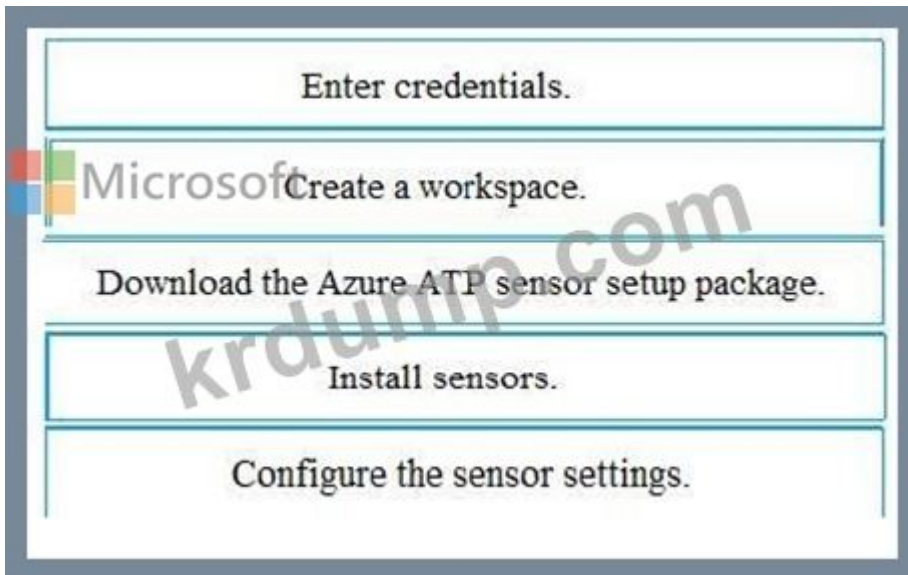
* □□ □□□□ □□ □□ □□□ □□□□ □□□□□.

*□□□ □□□ □□ SIEM □□□□□□□□ □□ □□□□ □□ □□□□ □□□□ □□□□□.

*SharePoint □□□□ □□ □□□□□□ □□□ □□ □□□ □□□□ □□□ □□□ □ □□□ □□□□□□.

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

*□□ □□(EU) □□□ PII □□□□ □□□ □□ □ □□□ □□□□ □□□□ 10□ □□ □□□□□.



□□:

<https://blog.ahasayen.com/azure-advanced-threat-protection-deployment/>

NEW QUESTION: 211

Microsoft 365 E5 □□□□ □□□□.

□□ □□ □□□ □□□□ □□ □□ □□□□ □□□□ □□□□.

* □□ □□□ □□□□ □□ □□□□ □□□□□.

* □□□ □□□ □□, □□□□ □ □□□□ □□□□□.

* □□□ □□□□ □□□□ □□ □□ □□□□□□□□ □□□□□.

□ □□ □□□ □□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □□ □

□□□ □□□□□□□□. □ □□□□ □ □, □ □ □□ □□ □□ □□□□ □□ □ □□□□□. □□

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

□□: □ □□□ □□□ 1□□ □□□ □□□□.



Answer:



MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
 DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
 □□□□□ □□□ □□□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□

□□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps, 30%OFF Special Discount: **KrDump**)

NEW QUESTION: 212

100□□ Windows 10 □□□ □□□ Microsoft 365 E5 □□□□ □□□□.

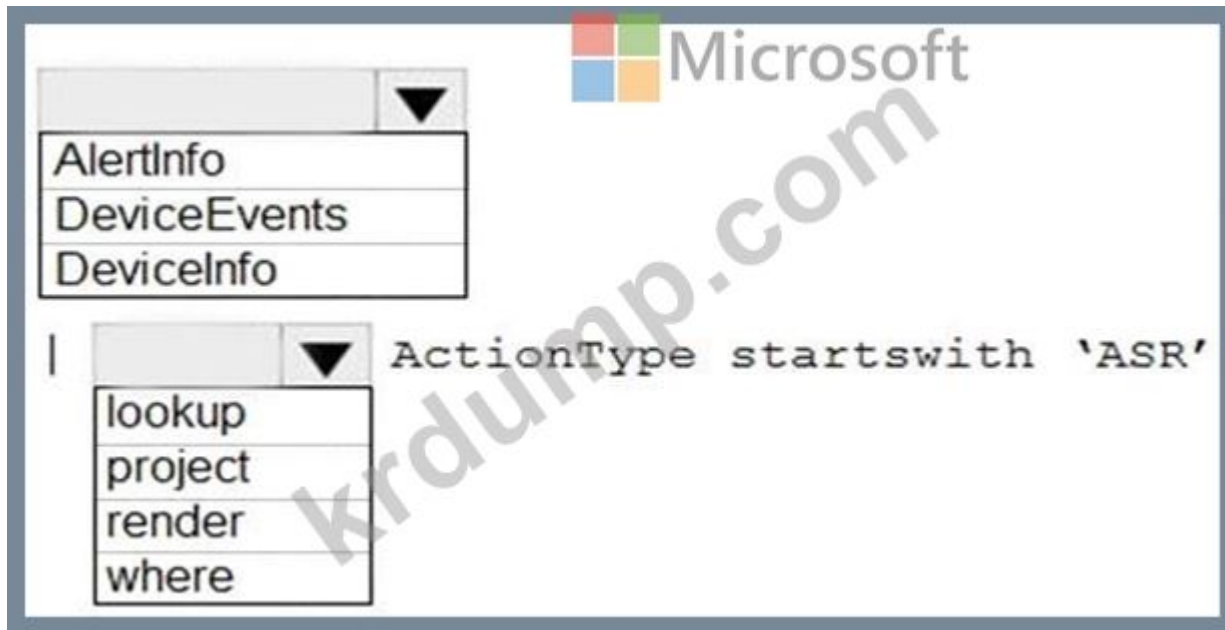
Windows 10 □□□ □□ ASR(□□ □□) □□□ □□□ □□□□□.

□□ □□□□ ASR □□□ □□□□ Log Analytics □□ □□□□ □□ □□□□ □□□□□.

□□□ □□□ □□□□ ASR □□□ □□□ □□□.

Kusto □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□□.

□□: □ □□□ □□□ 1□□ □□□ □□□□□.

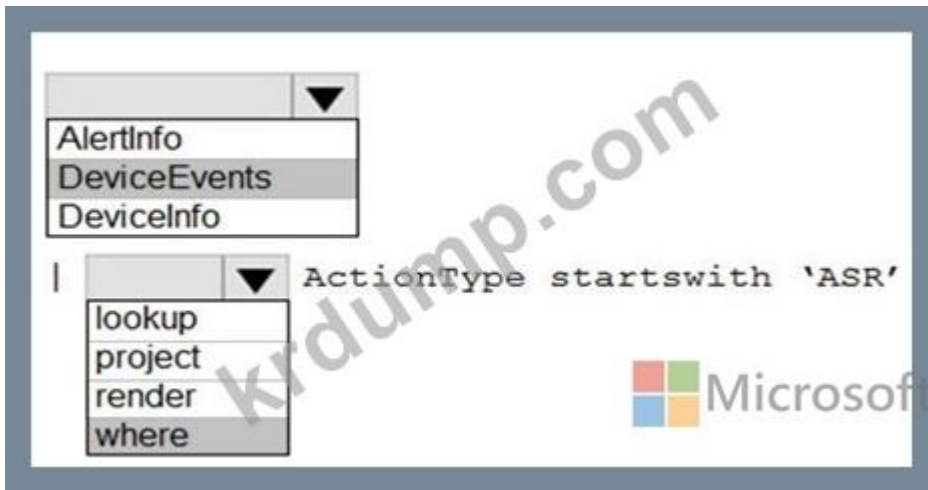


Answer:



□□

□□□ □□□ □□□□□, □□□□□□□ □□□ □□□□ □□□



□□:

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/demystifying-attack-surface-reduction->

NEW QUESTION: 213

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

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

□□□ □□ VPN □□□□ □□□□ □□□□□.
 □□□ □□ □□□ □□ □□ □□□□□?

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

Answer: A (LEAVE A REPLY)

NEW QUESTION: 214


□□□

□□□ contoso.com□□□ Azure AD(Azure Active Directory) □□□□ □□□□ Microsoft 365 □ □□ □□□□.

□ □□□ SharePoint Online □□ □□□□□□ 2TB□ □□□□ □□□□□.
 □□□□□ □□ □□ □□□ □□□□ □□□□.

Name	Type
Label1	Sensitivity label
Label2	Retention label
Label3	Azure Information Protection label

☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐☐☐☐. ☐☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐☐.
☐☐: ☐ ☐☐☐ ☐☐☐ 1☐☐ ☐☐☐ ☐☐☐☐☐.
☐☐☐ ☐☐:




Answer Area

Statements

	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input type="radio"/>	<input type="radio"/>

Answer:



Answer Area

Statements

	Yes	No
Label1 can now be used as a sensitivity label or an Azure Information Protection label.	<input checked="" type="radio"/>	<input type="radio"/>
Label2 can now be used as a retention label or an Azure Information Protection label.	<input type="radio"/>	<input checked="" type="radio"/>
Label3 can now be used as a sensitivity label or an Azure Information Protection label.	<input checked="" type="radio"/>	<input type="radio"/>

□□:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/custom-sensitive-info-types?view=o365-worldwide>

MS-101 □□ □□□ □□□□□ □□ DumpTop □□ □□□□ □□□ MS-101 □□!
DumpTop □ □□ **MS-101** □□ □□□ □□□□□□, DumpTop MS-101 □□ □□□ □□□
□□□□□ □□□ □□□□□□□. □□□□ □□□ □□□□ □□ DumpTop MS-101 □□□
□□□□□. <https://www.dumptop.com/Microsoft/MS-101-dump.html> (408 Q&As Dumps,
30%OFF Special Discount: KrDump)