Microsoft.SC-300-KR.v2026-08-29.q204

□□□□:	SC-300-KR
□□□□:	Microsoft Identity and Access Administrator (SC-300 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	204
□□:	v2026-08-29
# □□ □:	125
# □□ □□□:	2040
https://www.krdump.com/Microsoft.SC-300-KR.v2026-08-29.q204.html	

NEW QUESTION: 1
Microsoft 365 □□□ □□□□ □□□□. □□ □□□□ Microsoft Outlook 2016 □ Outlook 2013 □□□□□□ □□□□ □□□□ □□□□ □□□□.
□□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□ □□ □□□?
A. Outlook 2013 □□□□□□ □□ □□□ □□□□□ □□□□□.
B. Outlook 2013 □□□□□□ Outlook 2016□□ □□□□□□□□.
C. Exchange □□ □□□□ □□ □□□ □□□□□.
D. □□ Outlook □□□□□□ Outlook 2019□ □□□□□□□□□.
Answer: B (LEAVE A REPLY)
From October 13, 2020 onward, only these versions of Office are supported for connecting to Microsoft 365 (and Office 365) services:
Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus) Microsoft 365 Apps for business (previously named Office 365 Business) Office LTSC 2021, such as Office LTSC Professional Plus 2021 Office 2019, such as Office Professional Plus 2019 Office 2016, such as Office Standard 2016 Note:
Office 2019 and Office 2016 will be supported for connecting to Microsoft 365 (and Office 365) services until October 2023.
Note: Client software: To support tenant restrictions, client software must request tokens directly from Azure AD, so that the proxy infrastructure can intercept traffic. Browser-based Microsoft 365 applications currently support tenant restrictions, as do Office clients that use modern authentication (like OAuth 2.0).
Reference:
https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions

NEW QUESTION: 2
Microsoft Office 365 Enterprise E3 □□□□□ □□□ 2,500□□ □□□□ □□□□. □□□□□ □□ □□□□□ □□□□□.
Azure Active Directory □□ □□□ □□ □□□□□□ □□□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□□.
□□□□ □□ □□□ □□ □□□□ Office 365 Enterprise E3 □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Azure Active Directory □□ □□□ ID □□□□ □□□□
B. Set-AzureAdUser cmdlet
C. Azure Active Directory □□ □□□ □□□□ □□□□

D. Set-WindowsProductKey cmdlet
Answer: (SHOW ANSWER)
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this QUESTION 1in the exam. The QUESTION 1has two possible correct answers:
1. the Licenses blade in the Azure Active Directory admin center
2. the Set-MsolUserLicensecmdlet
Other incorrect answer options you may see on the exam include the following:
* the Identity Governance blade in the Azure Active Directory admin center
* the Set-WindowsProductKeycmdlet
* the Set-AzureAdGroupcmdlet
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

NEW QUESTION: 3
Microsoft 365 E5 □□□ □□□□.
□ □□□□ □□ □□ □□□□□ □□□□□.
□ □□□□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□?
A. Azure Active Directory □□ □□
B. Microsoft 365 Defender
C. □□□□ □ □□□ Microsoft Defender
D. Microsoft Purview □□ □□ □□
E. Microsoft 365 □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 4
□□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□□ □□□□.
- □□□
- □□□□ □□□□
- □□□ □ □□□(AWS)
- □□ □□□□ □□□(GCP)
Azure □□□ □□□□ Microsoft Entra □□ □□□ □□□□ Azure □□□□ □□□ □□□ □ □□□□.
□□ □□□ □□ □□□ □ □□ □□ □□□□ □□□□ □□□□□?
A. AWS □□
B. □□□□ □□□□ □ AWS□ □□
C. □□□□ □□□□ □ GCP □□
D. AWS □ GCP□ □□
E. □□□□ □□□□, AWS, GCP
Answer: (SHOW ANSWER)
Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities.

For example, over-privileged workload and user identities, actions, and resources across multicloud infrastructures in Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

NEW QUESTION: 5
□□□ Site1□□□ □□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Site1□ □□ Microsoft Defender for Cloud Apps □□ □□□ □□□□□ □□□.
□□ □□□ □□□ □□ □□□□ □□□?
A. □□
B. □ □□
C. □□
D. □□□ □□□
Answer: (SHOW ANSWER)
Create Microsoft Defender for Cloud Apps session policies
Microsoft Defender for Cloud Apps session policies provide granular visibility into cloud apps with real-time, session-level monitoring. Use session policies to take various actions, depending on the policy you set for a user session.
In contrast to access policies, which allow or block access completely, session policies allow access while monitoring the session. Add Conditional Access app control to your session policies to limit specific session activities.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad

NEW QUESTION: 6
Azure AD □□□□ □□□□.
App1□□□ □□□ □□□ □□□□□□ □□□□□□□ □□□□□.
□□□□ App1□ □□□ □□ □□□ □□□□□ □□ □□□ □□□□□.
□□□□ App1□ □□ □□□ □□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□ □□□.
□□□ □□ □□ □□□?
A. □□□□ □□ □□□ □□ □□□ □□□□□□.
B. □□□□ □□ □□□ □□ □□ □□□□ □□□□□□.
C. App1□ □□ □□□□ □□□□ □□ App1 □□□ □□□ □□□□□□.
D. App1□ □□ □□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
To ensure that users can request admin consent for App1 in your Azure AD tenant, you should first enable admin consent requests for the tenant.
Enabling admin consent requests allows users to initiate the process of requesting admin consent for applications that require it. By default, users do not have the ability to grant admin consent for applications. Enabling this feature ensures that users can request admin consent for App1 without having to rely on an administrator to initiate the process.

NEW QUESTION: 7
Microsoft 365 □□□□ □□□□.
□□ □□□□ □□□□□ □□□ 10 □□□□ □□□ □□□□.
□□□□□ □□□□□ □□□ □□□ □□□□ □□□□□ □□ □□□□□. □□□ □□□□□ □□□ □, □□□□□ □□□□ □□□□ □□□ □ □□ □□ □□□□□ □□□□□.
□□□ □□□ □□(MFA)□ □□□ □□□□□.
□□ □□□□ □□□□ □□□ □ □□ MFA □□ □□□ □□□□□?
A. □□□□□ Windows Hello
B. □□

C. SMS
D. Microsoft Authenticator □□ □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
Azure AD □□□□ □□□□.
□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □ □□□ □□ □□□.
□□ □□□ □□□□ □□□?
A. □□ □□
B. □□□ □ □□□ □□
C. □□ □□ □□□□
D. □□ □□ □□
Answer: D (LEAVE A REPLY)

NEW QUESTION: 9
□□□□□
□□ □□□ □□□ □□□ □□ □□□□ □□□□ □□□□ □□□ □□□□ □□□.
Answer:
To create a group that automatically includes users based on a specific property value, you need to create a Dynamic User Group.
Step 1: Sign in to the Microsoft Entra admin center.
Access the Portal
Step 2: Expand the Identity menu on the left.
Step 3: Click on Groups and then select All groups.
Step 4: Click New group at the top of the page.
Initiate New Group
Step 5: Group type: Select Security (or Microsoft 365, depending on your needs).
Configure Basic Settings
Step 6: Group name: Enter a descriptive name. [Enter Bellevue]
Step 7: Membership type: Change this from Assigned to Dynamic User.
Step 8: Click Add dynamic query under the Dynamic user members section.
Build the Membership Rule
Step 9: Choose a Property from the dropdown (e.g., department, country, jobTitle). [Choose City] Step 10: Choose an Operator. [Choose Equals] Step 11: Enter your specific value in the Value field. [Enter Bellevue] Step 12: Click Save at the top of the rule builder page Reference:
https://www.manageengine.com/microsoft-365-management-reporting/kb/how-to-add-group-members-in-entra-id.html

NEW QUESTION: 10
□□□ □□
contoso.com□ fabrikam.com□□□ □ □□ Microsoft Entra □□□□ □□□□. contoso.com□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Department	Job title	City	Member of
User1	IT	Support	Vancouver	Group1
User2	IT	Technician	Madrid	*None*
User3	HR	Consultant	Montreal	Group1

contoso.com□□ fabrikam.com□□□ □□□ □ □□□□ □□□□□ □□ □□□ □□□□□□.

- □□□ □ □□: Group1
- □□□□□ □□: □□
- □□ □□
- □□ □□ □□: □□1, □□2

□□1□ □□ □□ □□□ □□ □□□□□.

Source attribute	Operator	Clause value
department	EQUALS	IT
jobTitle	PRESENT	*Not applicable*

Filter2□ □□ □□ □□□ □□ □□□□□.

Source attribute	Operator	Clause value
city	INCLUDES	M

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 syncs to fabrikam.com.	○	○
User2 syncs to fabrikam.com.	○	○
User3 syncs to fabrikam.com.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 syncs to fabrikam.com.	○	●
User2 syncs to fabrikam.com.	●	○
User3 syncs to fabrikam.com.	○	●

Explanation:

Box 1: No

User1 is in IT department and has the job title support. Filter1 matches.

User1 is in city Vancouner, which does not have a letter M. Filter2 does not match.

User1 is not synced.

Note:

Both filter must match.

Filter1 matches if department is IT, and there is jobTitle value.

Filter2 matches any city that has the letter M in it.
In Microsoft Entra Connect Sync, the "PRESENT" operator in scoping filters specifies that the attribute must exist with any value, even if it's empty or null. This is different from EQUALS, which requires a specific value, or NOT EQUALS, which excludes a specific value. The PRESENT operator is used to ensure that an attribute exists in the object being synchronized, regardless of its actual value.
Box 2: Yes
User2 is in IT department and has the job title technician. Filter1 matches.
User2 is in city Madrid, which does not have a letter M. Filter2 matches.
User2 syncs.
Box 3: No
User3 is in HR department, so Filter1 will not match.
User3 will not sync.
Reference:
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering

NEW QUESTION: 11
□□□□□
fabrikam.com □□□□ □□□□ Microsoft Entra □□□□ □□□ □ □□□ □□ □□□.
Answer:
To restrict external invitations to a specific domain, you must configure the Collaboration restrictions allowlist within the Microsoft Entra admin center.
Step 1: Sign in to the Microsoft Entra admin center using an account with at least Global Administrator privileges.
Step 2: Navigate through the left-hand sidebar menu: Identity > External Identities > External collaboration settings.
Step 3: Scroll down to locate the Collaboration restrictions section near the bottom of the page.
Step 4: Select the radio button labeled "Allow invitations only to the specified domains (most restrictive)".
Step 5: Target the domain: Under the Target domains input field, type the exact domain name you want to allow. [Enter fabrikam.com] Note: If you need to include multiple domains, type each one on a new line.
Step 6: Apply changes by clicking the Save button at either the top or bottom of the page.
Reference:
https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list

NEW QUESTION: 12
□□ □□ 2 - □□□□ □□□□
□□
Litware, Inc.□ □□□□ Fabrikam, Inc.□ □□□ □□ □□□□□.
Litware□ □□□□ □□□□ □□□□ □□ □□□, □□ □□□ □□□ □□□□ □□□□.
□□□□ VPN □□□ □□□□ □□□□ □ □□□ □ □ □□ □□□□□.
□□ □□. □□ □□
□□□□□□ litware.com□□□ □□□ Active Directory □□□□□ □□□, □ □□□□□ litware.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. Azure AD Connect□ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□□□□ □□□□.
Litware.com□□ □□ □□□□□□ □□□ □□□□ User1□□□ □□□□ □□□□.
Litware□ Azure AD □□□□□□ □□□□ □□□□□.
Fabrikam□ fabrikam.com□□□ □□□ Azure AD □□□□ □□□□ □□□□. Fabrikam□ □□□□□ litware.com □□□□ □□□ □□□ □□□□ litware.com□ □□□□ □□□□□.
□□ □□. □□□□ □□
Litware□ □□ □□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□ □□□□. Microsoft □□□□ □ □□□ □□□ □□ □□ □□ □□□ □□□□□ □□□□.

Litware□ litware.com Azure AD □□□□ □□□ Azure □□□ □□□□ □□□□. □ □□□□ Azure Active Directory □□□□ Office 365 □□□□ □□□□ Azure Sentinel □□□□□ □□□□ □□□□. Azure Sentinel□ □ □ Azure AD □□□ □□□ □□ □□□ □□□□□.

□□ □□. □□□□□ □□

□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware□ □ □□□ □□ □□□□ □□ □□□□ □□□□. □ □□□ □□ □□□ □ VPN □□□ □□□□ Azure □□□ □□ □□□□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□□ □□□□ □ □□□ □□□□ □□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□□□.

* Azure AD □□ □□ ID □□(PIM)□ □□□□ □□ □□ □□ □□□ □□□□□.
* □□□ □□ □□□□ litware.com Azure AD □□□□ □□□□□□□ □□□□ □□□□ □□□□□.
* □□□ □□ □□□□ □ □□□ □□ □□□□□ □□□□ ID □□□ □□□□□.
* User1□ Azure AD□□ □□□□□□ □□□□□□□ □□□ □ □□□ □□□□□□.
* □□ □□ □□□ □□□□□□.

□□ □□. □□ □□

Litware□ □□ litware.com Active Directory □□□□□ LWLicenses□□ □□□ □□ □□□ □□□□□□. Litware□ LWLicenses □□ □□ □□□□ Azure AD □□□□ □□□ □□□□□ □□□. LWLicenses □□ □□ □□ □ □□□□ □□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□□ □□□.

□□□□. □□ □□□□

Litware□ Litware□ □□ Azure AD □□□ □□□ □□□□ Azure AD □□□ □□□ □□□ LWGroup1□□□ □□□ □□□□ □□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

* □□ Litware □□□□□ □□□ □□(MFA)□ □□□□□□.
* Litware □□□ □□□□□ Azure AD□ □□□ □ MFA(□□□ □□)□ □□□□ □□□ □□□□ □□□□□.
* litware.com □□□□□ □□ □□ □□ □□□ □□□□□□.
* □□□□□ □□□□□□□ □□□□ □ MFA(□□□ □□)□ □□□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□ □□□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

* □□□ □□□ □□□ □□□□ □□ Azure □□□ □ Azure AD □□□□□□□ □□ □□ □□□□ □□□□□.
* Microsoft SharePoint Online□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□.
* Azure AD□ □□□ □□□ □□□□ □□□□□□□ □□ □□ □□ □□□□ □□□□□.

□□□□. □□□□ □□□□

Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□ Microsoft Office 365 □□□ □□□ □□□ □□□ □□□□□ □□□.

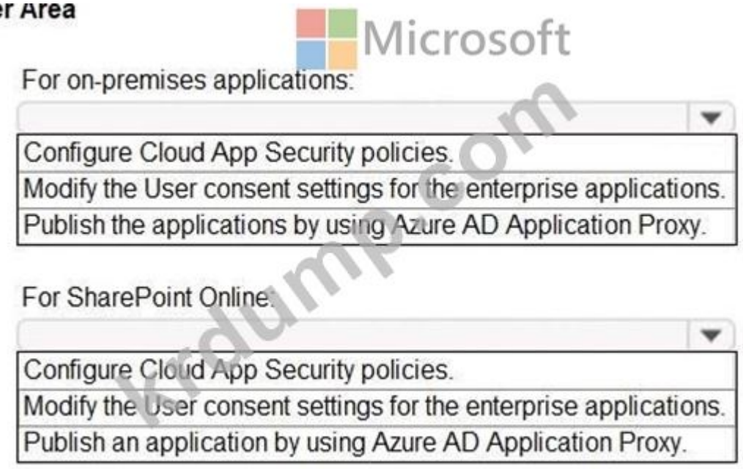
□□□ □□

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

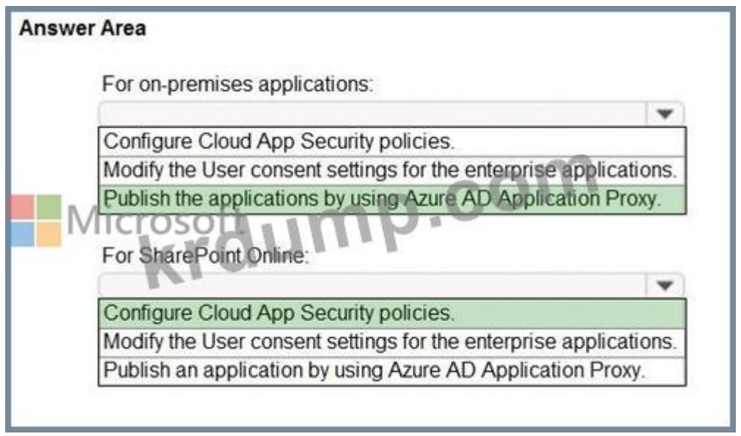
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area



Answer:



Explanation:

Configure Cloud App Security polices

Conditional Access App Control enables user app access and sessions to be monitored and controlled in real time based on access and session policies. Access and session policies are used within the Cloud App Security portal to further refine filters and set actions to be taken on a user.

Configure app-enforced settings

Conditional Access App Control uses a reverse proxy architecture and integrates with your IdP.

When integrating with Azure AD Conditional Access, you can configure apps to work with Conditional Access App Control with just a few clicks, allowing you to easily and selectively enforce access and session controls on your organization's apps based on any condition in Conditional Access.

Reference:

https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#featured-apps

https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad#how-it-works

NEW QUESTION: 13

Sub1□□□ Azure □□□ □□□□.
Microsoft Entra □□ □□ □□□□□ □□□□□.
□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. Sub1□ □□ □□ □□□ □□□□□.
B. Microsoft Entra □□□□□□ □□□□ □□□□□.
C. Azure Portal□□ □□□ □□ □□(DCR)□ □□□□.
D. Microsoft Entra □□ □□□□ □ □□□ □□□□.
E. Microsoft Entra □□ □□□□ □□□ □□□ □□□□□.
F. Microsoft Entra □□ □□□□ □□ □□□ □□□□□.
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 14
□□□ □□□□□ □□□□ □□ □□ 100% Azure □□□□ □□ □□□□□. □□ □□□□□ □□□ □□□□ □□ □□□ □□□□□□. □□ □□□□ □□□□□ □□□ □□□ □□□□□ □ □□□□□□ □ □□□ □□ □□□ □□□ □□ □□□□ □□□. Azure Active Directory□ □□□□ □□□□□ □□□□□□□ □□ □□□ □ □□□ □□□ □ □□ □□□□ □□□□□?
A. Azure Active Directory □□
B. Azure □□ □□
C. Azure Active Directory □□□□□□ □□□
D. Azure Active Directory □□□ □□□
Answer: C (LEAVE A REPLY)
Azure Active Directory Application Proxy is a service that you can deploy that will allow users that have been authenticated via Azure Active Directory to connect to applications that are hosted on- premise. This allows you to also use Azure AD features such as multi-factor authentication for connecting to on-premise applications.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy

NEW QUESTION: 15
□□□ □□
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.

Name	Member of
Admin1	Group1
Admin2	Group2
Admin3	Group1, Group2

□□□ □□□ □□□ □□ □□□ □□□□□.
- □□ □□: □□□□
- □□□ □□□: □□1
- □□ □□: □□
- □□ □□□: 2022□ 8□ 15□
□□ □□□: 2022□ 12□ 15□
Exchange □□□ □□□ □□ □□□ □□□□□.

- □□ □□: □□□□
- □□□ □□□: □□2
- □□ □□: □□
- □□ □□□: 2022□ 10□ 15□

□□ □□□: 2023□ 1□ 15□

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
On November 15, 2022, Admin1 can reset the password of Admin2.	○	○
On October 15, 2022, Admin2 signs in and can administer Exchange Online.	○	○
On September 1, 2022, Admin3 can reset the password of Admin1.	○	○

Answer:

Answer Area

Statements	Yes	No
On November 15, 2022, Admin1 can reset the password of Admin2.	○	○
On October 15, 2022, Admin2 signs in and can administer Exchange Online.	○	○
On September 1, 2022, Admin3 can reset the password of Admin1.	○	○

NEW QUESTION: 16

□□□ Microsoft Entra □□□□ □□□□ □□□□.

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

□□□ □□ □□□□ □□□?

A. □□□ □□ □□

B. □□ □□

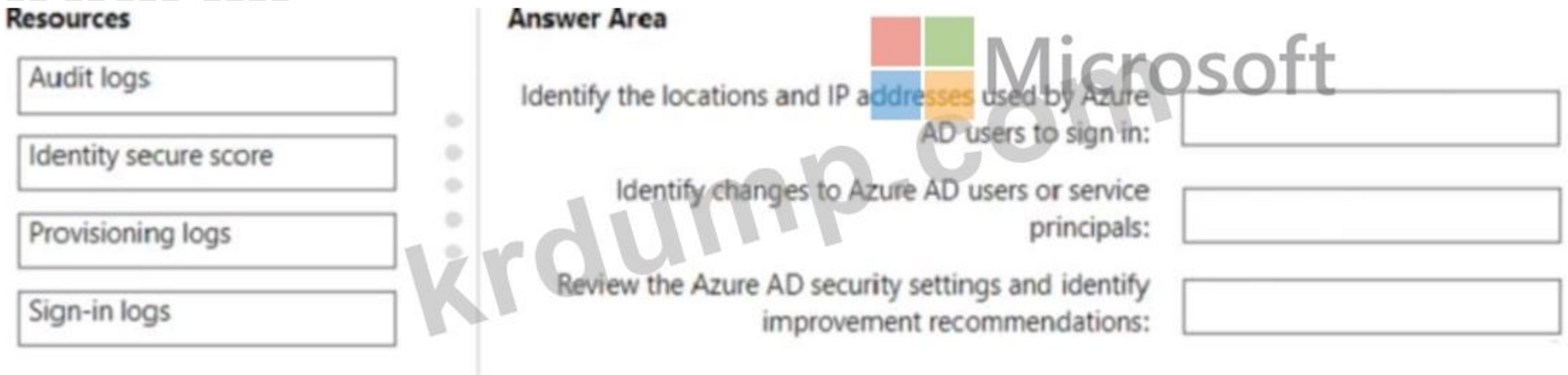
C. □□□ □□ □□

D. □ □□

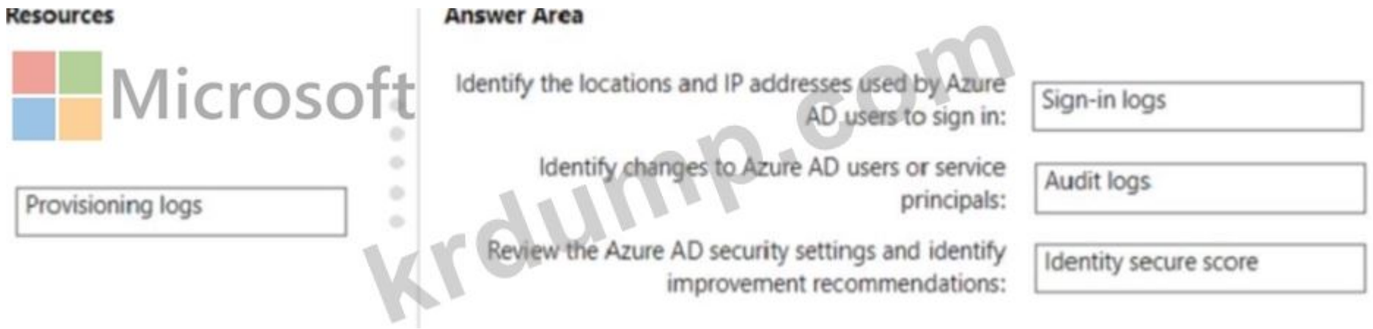
Answer: C (LEAVE A REPLY)

To let users consent to low-risk permissions but block others in Microsoft Entra, use User Consent Settings in the Microsoft Entra admin center to select "Allow user consent for apps from verified publishers for selected permissions," then define those low-risk permissions under Permission classifications, requiring admin approval for anything beyond that, especially high-risk or unverified app requests. This balances security by restricting risky requests (often flagged by risk-based step-up consent) while allowing productivity for trusted apps.
Reference:
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent

NEW QUESTION: 17
□□□ □ □□ □□
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□ □□□ □□□□ □□□.
- Azure AD □□□□ □□□□ □□ □ IP □□□ □□□□□.
□□□□□□.
- Azure AD □□ □□□ □□□□ □□ □□□ □□□□□.
□□ □□.
- Azure AD □□□ □□ □□□ □□□ □□ □□□ □□□□□.
□ □□□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□□ □□ □□ □□□ □□□□□□. □ □□□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□ □□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 18

Terms1□□□ □□ □□(ToU)□ □□□ Microsoft Entra □□□□ □□□□. Terms1□ □□□□ □□ Policy1□□□ □□□ □□□ □□□ □□□□. □□□□ Terms1□ □□□□□ Policy1□ □□□□ □□□. Policy1□ □□ □ □ □□□ □□□□ □□□?

A. □□

B. □□

C. □□

D. □□ □□□

Answer: B (LEAVE A REPLY)

To enforce Terms of Use (ToU) acceptance in a Conditional Access policy, you must configure it under the Grant section :

https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-require-terms- of-use

NEW QUESTION: 19

□□□ □□

Microsoft Entra □□□□ □□□ Azure □□□ □□□□. □□ □□□□□ User1, User2, User3□□□ □ □□ □□□□ □□□□.

□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Platform	Description
Device1	Windows 11	Microsoft Entra joined
Device2	Windows 11	*None*
Device3	Android	Microsoft Entra registered

□□□ □□ □□□ □□ □□ □□□ □□□□□.

- □□: VM1
- □□□ □□: RG1
- □□ □□: Windows Server
- Microsoft Entra ID□ □□□: □□ □□□

□□ □□ Azure □□ □□□ □□ □□□□.

User	Role	Scope
User1	Virtual Machie Local User Login	RG1
User2	Virtual Machie User Login	RG1
User3	Virtual Machie Administrator Login	Sub1

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer:

Explanation:

Box 1: No

User1 has the Virtual Machine Local User login role with scope RG1.

The role is not correct.

The Virtual Machine User Login role would be OK.

Box 2: Yes

User2 has a correct role: The Virtual Machine User Login role.

The Device is Windows 11, which is fine.

The Device does not have to been Entra joined or Entra registered.

Box 3: No

Not possible from an Android device.

Note:

Enable Microsoft Entra login for a Windows VM in Azure

To use Microsoft Entra login for a Windows VM in Azure, you must:

1. Enable the Microsoft Entra login option for the VM. [we can assume this has been configured]

2. Configure Azure role assignments for users who are authorized to sign in to the VM.

Reference:

https://learn.microsoft.com/en-us/entra/identity/devices/howto-vm-sign-in-azure-ad-windows

https://learn.microsoft.com/en-us/azure/virtual-desktop/azure-ad-joined-session-hosts

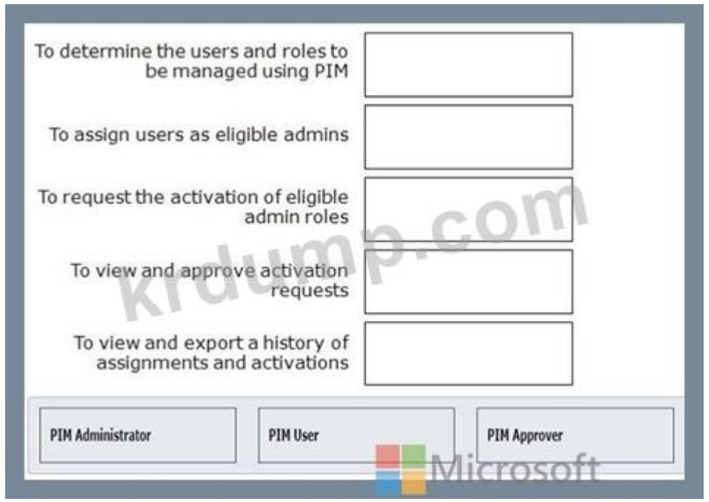
NEW QUESTION: 20

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

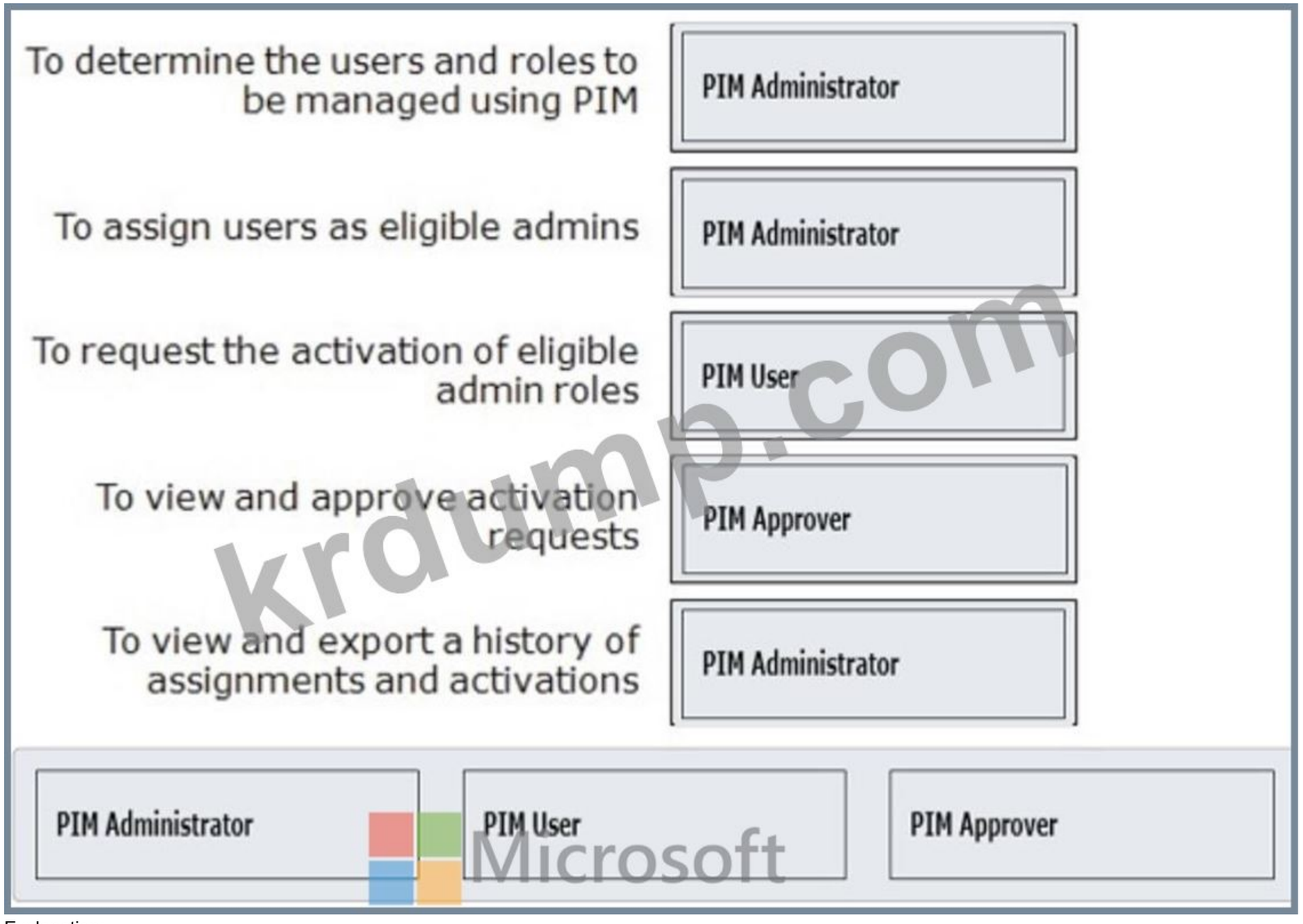
□□□□ □□ □□□□ □□□□□□□□ □□□ □ □□ □□□ '□□□'□ □□□□ □□□□.
Admin1□□□ □□□□ App1□□□ □□□ □ □□□□ □□ □□□□ □□□.
Admin1□ Azure AD□ App1□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□.
Admin1□□ □□ □□□ □□□□ □□□?
A. □□1□ □□ □□□ □□□□□□ □□□.
B. Azure AD □□□□□□ □□□.
C. Azure AD□ □□□□ □□□□□□ □□□.
D. □□1□ □□ □ □□ □□□ □□□.
Answer: B (LEAVE A REPLY)
Application Developer can create application registrations independent of the 'Users can register applications' setting.
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

NEW QUESTION: 21
□□□ Azure □□□□□ □□ □□ □□□ □□□□ □□□□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□□ □□□. □□□□ □□□ □□□□ □□□□ □□□ □□□ □□□□□ □□□□ □□□. □□ □□ □□ □ □□ □□□□ □□□?
A. □□ □□
B. □□□ □□
[□□]: Microsoft 365 □□
C. □□ □□
Answer: (SHOW ANSWER)
Dynamic groups allow administrators to set rules to populate groups that are created in Azure AD based on user attributes such as userType, department, or country/region.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/use-dynamic-groups

NEW QUESTION: 22
□□□ □ □□ □□
□□□ Azure □□□□ □□ □□□ □□□ □□□ □□□□ □□ □□ □□ ID □□(PIM)□ □□□ □□□□□.
PIM□ □□ □□□□ □ □□□□ PIM□ □□□□ □□□ □ □□□ □□□□□ □□□□□.
□□ □□ □□□ □□□□□ □□ □□□ □□ □□□ □□□□ □□□? □□□ □ □□□ □□□ □□□ □□□□□ □□□ □□□□. □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□.


To determine the users and roles to be managed using PIM
To assign users as eligible admins
To request the activation of eligible admin roles
To view and approve activation requests
To view and export a history of assignments and activations
PIM Administrator
PIM User
PIM Approver
krdump.com
Microsoft

Answer:



Explanation:

You should use the Privileged Identity Management (PIM) Administrator role to determine the users and roles to be managed using PIM. The PIM Administrator will be the person performing the initial setup of PIM and will therefore need to collect the requirements for the implementation.

You should use the PIM Administrator role to assign users as eligible admins. The PIM Administrator will determine and configure which users will have which rights within the environment. As this is an administrative task, the PIM Administrator role will be required for this.

You should use the PIM User role to request the activation of eligible admin roles. When users require elevated rights for their account, they can create a PIM activation request to be granted the requested permissions.

You should use the PIM Approver role to view and approve activation requests. When PIM requests are created, the PIM Approver will approve or deny the request for the elevated permissions.

You should use the PIM Administrator role to view and export a history of assignments and activations. The PIM Administrator can access the history to make sure compliance requirements are met.

NEW QUESTION: 23
□□□□□
Microsoft Defender for Cloud Apps□□ Microsoft SharePoint Online□ □□□ □□□ □ □□□ □□□ □□□□ □□□.
Answer:
To add Microsoft SharePoint Online as a Conditional Access App Control app, you must create a Conditional Access policy in the Microsoft Entra admin center that routes traffic to Microsoft Defender for Cloud Apps. Because SharePoint Online is a native Microsoft application, it onboards automatically to Defender for Cloud Apps as soon as a user session triggers the policy for the first time.
Follow these steps to complete the deployment:
Create the Conditional Access Policy in Microsoft Entra
Step 1: Sign in to the Microsoft Entra admin center as a Conditional Access Administrator.
Step 2: Navigate to Identity > Protection > Conditional Access.
Step 3: Select + New policy.
Step 4: Under Assignments, select Users to include your targeted users or groups.
Step 5: Under Target resources, choose Select apps, search for, and select Office 365 SharePoint Online (or Office 365 to include all core suites).
Step 6: Under Conditions > Client apps, set the toggle to Yes, check the Browser box, and click Done. (Session control only applies to interactive browser sessions).
Step 7: Under Access controls > Session, select Use Conditional Access App Control.
Step 8: Choose a policy type from the dropdown, such as Use custom policy (recommended for advanced granular rules) or Monitor only.
Step 9: Set Enable policy to On, and click Create.
Reference:
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

NEW QUESTION: 24
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
Azure Monitor□ □□□□ Azure Active Directory(Azure AD) □□ □□□ □□□ □ □□□□.
Yon□ Azure AI □□□ □□□ □□□ □□□ □□□ □□□ □□ 100□ □□ □□□□.
□□□ □□ □□□□ □□□ □□□ □□□□ □□□.
□□ □□: Azure □□□□□ □□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Data Collection Rules (DCRs) define the data collection process in Azure Monitor. DCRs specify what data should be collected, how to transform that data, and where to send that data. Some DCRs will be created and managed by Azure Monitor to collect a specific set of data to enable insights and visualizations.
Reference:
https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/data-collection-rule-overview>

NEW QUESTION: 25
Microsoft 365 □□□□ □□□□.

□□ □□□□ □□□□□ □□□□ □□□ □□□□.
□□□□□ Wi-Fi□ □□□ □□□ □□ □□□□□ □□□□ □□□ □□□□.
□□ □□□□ □□□□ □□ □□□□ □□□□ □□□ □□□ □□□ □□ □□□□□ □□□□□.
□□ □□ □□(MFA)□ □□□ □□□□□.
□□□□ □□ □□□□ □□ MFA □□ □□□ □□□ □ □□□□?
A. Microsoft Authenticator □□ □□ □□
B. □ □□□□
C. □□□□□ Windows Hello
D. □□
Answer: C (LEAVE A REPLY)
In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or PIN.
After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.
Incorrect Answers:
A: The Microsoft Authenticator app requires a mobile phone that runs Android or iOS B: An app password can be used to open an application but it cannot be used to sign in to a computer.
D: SMS requires a mobile phone
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication- methods
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello- overview

NEW QUESTION: 26
□□□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com
Microsoft 365 □□: =1122334455667788
Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 99999999
Salesforce □□ □□ □□□ □□ □□□ □□□□ □□□□ □□□□□ □□□□ □□□.
□□□ □□ □□□ □□□□ □□□.
- □□□ □□ □□□□ □□□.
- □ □□□ □□□□ □□□□ □□ □□□ □□□□ □□□.
- □□□ 5□ □□□ □□□□ □□□ □□ □□□ □□□□□.
- □□□ □□□□□ □□□□ □□ □□, □□ □□□ □□ □□□ □□□□ □□□.
□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□.
Answer:

Microsoft Entra, Microsoft Entra ID Governance, Manage guest access with access reviews

Create an access review of groups and applications in Microsoft Entra ID
Access to groups and applications for employees and guests changes over time. To reduce the risk associated with stale access assignments, administrators can use Microsoft Entra ID to create access reviews for group members or application access.

Create a single-stage access review
Scope

Step 1: Sign in to the Microsoft Entra admin center as at least an Identity Governance Administrator.

Step 2: Browse to Identity governance > Access Reviews.

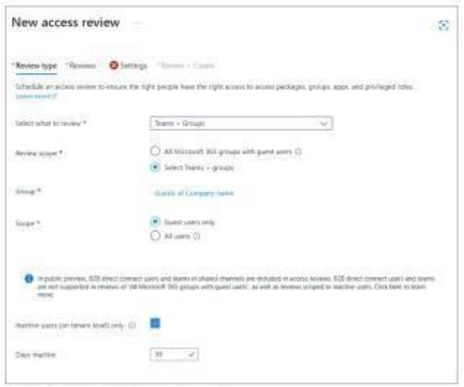
Step 3: Select New access review to create a new access review.

Step 4: In the Select what to review box, select which resource you want to review. [Select Teams + Groups]

Step 5: If you selected Teams + Groups, you have two options:

* All Microsoft 365 groups with guest users: Select this option if you want to create recurring reviews on all your guest users across all your Microsoft Teams and Microsoft 365 groups in your organization. Dynamic groups and role-assignable groups aren't included. You can also choose to exclude individual groups by selecting Select group(s) to exclude.

* Select Teams + groups: Select this option if you want to specify a finite set of teams or groups to review.



Step 6: [Select All Microsoft 365 groups with guest users]

Step 7: Now you can select a scope for the review. [Select Guest users only]: This option limits the access review to only the Microsoft Entra B2B guest users in your directory.

Step 8: Select Next: Reviews.

Next: Reviews. Single stage review

Step 9: In the Specify reviewers section, in the Select reviewers box, select either one or more people to make decisions in the access reviews. You can choose from:

Group owner(s): This option is only available when you do a review on a team or group.
Selected user(s) or groups(s)
Users review their own access
Managers of users

Step 10: [Select Managers of users]

Step 11: In the Specify recurrence of review section, specify the following selections:

Duration (in days): How long a review is open for input from reviewers.

Start date: When the series of reviews begins.

End date: When the series of reviews ends. You can specify that it Never ends. Or, you can select End on a specific date or End after number of occurrences.

Step 12: Enter For Duration (in days): 5

Step 12a: Click Select fallback reviewers, and specify Megan Bowen
Question: If the guest user does not have a manager, Megan Bowen must review the access.

Step 13: Select Next: Settings.

Step 14: In the Upon completion settings section, you can specify what happens after the review finishes.

Step 14a: Select Auto apply results to resource
Select this checkbox if you want access of denied users to be removed automatically after the review duration ends. If the option is disabled, you have to manually apply the results when the review finishes.

Step 14b: For If reviewers don't respond, select Remove access [Maybe not available, and only need to do step 14c]
Question: If the reviews are **NOT** completed within five days, access must be removed.

If reviewers don't respond: Use this option to specify what happens for users not reviewed by any reviewer within the review period. This setting doesn't affect users who were reviewed by a reviewer. The dropdown list shows the following options:

No change: Leaves a user's access unchanged.
Remove access: Removes a user's access.
Approve access: Approves a user's access.
Take recommendations: Takes the system's recommendation to deny or approve the user's continued access.

Step 14c: For Action to apply on denied guest user, select Remove user's membership from the resource.

Action to apply on denied guest users: This option is only available if the access review is scoped to include only guest users to specify what happens to guest users if they're denied either by a reviewer or by the If reviewers don't respond setting.

* Remove user's membership from the resource: This option removes a denied guest user's access to the group or application being reviewed. They can still sign in to the tenant and won't lose any other access.

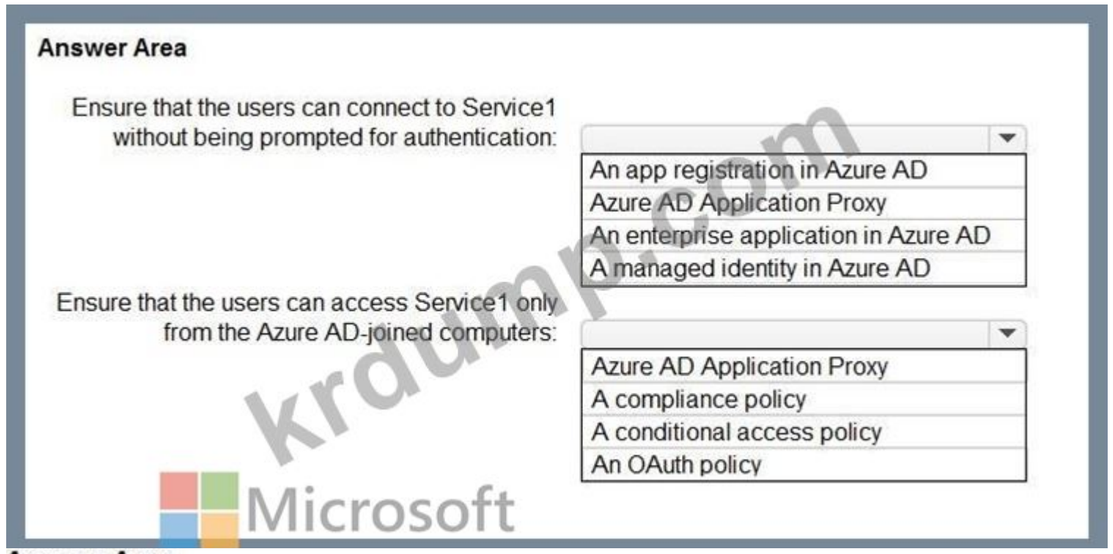
* Block user from signing-in for 30 days, then remove user from the tenant

Step 15: Select Next: Review + Create.

Step 16: Review the information and select Create.

Reference:
https://learn.microsoft.com/en-us/azure/active-directory/governance/create-access-review

NEW QUESTION: 27
□□□ □□
□□□ Microsoft 365 □□□□ □□□□ □□□□.
□□ □□□□ Windows 10□ □□□ □□□□ □□□□ □□□, □□ □□□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
□□ □□□ Service1□□□ □□ □□□□ □□□□ □□□□ □□□□. Service1□ OAuth □□□ Azure AD □□ □ □□ □□□ □□□□□. Service1□ Azure AD □□□□ □□□□ □□□□.
□□□□ □□ □□□□ □□ Service1□ □□□ □ □□□ □□ □□□□ □□□□ □□□. □ □□□□ □□□□ Azure AD□ □□□ □□□□□□ Service1□ □□□□ □ □□□ □□□□ □□, □□ □□□ □□□□□ □□□.
□ □□□□□ □□ □□ □□ □□□□□□□□□? □□□□□ □□□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer Area

Ensure that the users can connect to Service1 without being prompted for authentication:

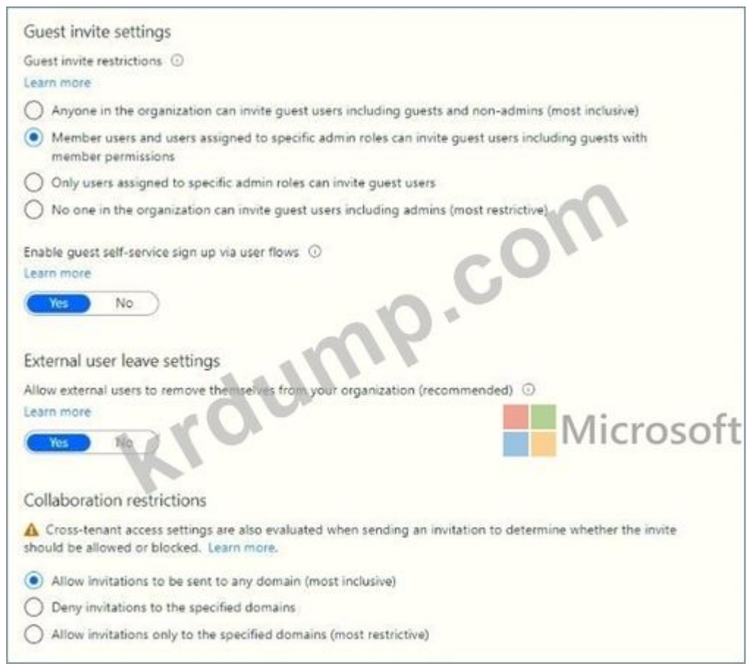
- An app registration in Azure AD
- Azure AD Application Proxy
- An enterprise application in Azure AD
- A managed identity in Azure AD

Ensure that the users can access Service1 only from the Azure AD-joined computers:

- Azure AD Application Proxy
- A compliance policy
- A conditional access policy
- An OAuth policy

Explanation:
Service1 support OAuth for Authentication & authorization, however Service1 is published in Azure AD gallery, hence we will use An enterprise application in Azure AD blade to register for SSO.
Conditional access policy - to ensure users access from Azure AD joined computers.

NEW QUESTION: 28
fabrikam.com □□□ □□□ □□□□ Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□ □□□ □□□ □□ □□□□□. (□□ □□ □□□□□□.)



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

bsmith@fabrikam.com□□□ □□□□ □□ □□ □□□ □□□□□ Microsoft SharePoint Online □□ □□□□□□ □□□□□.

Name	Email	Description
User1	User1@contoso.com	An existing guest user in fabrikam.com
User2	User2@tailspintoys.com	A guest user who has never accessed resources in fabrikam.com
User3	User3@fabrikam.com	A user in fabrikam.com

□□ □□□□□□ □□□□ □□□□□ □□□□□?

A. □□□1, □□□2, □□□3

B. □□□ 1 □□

C. □□□1 □ □□□2 □□

D. □□□2 □□

Answer: C (LEAVE A REPLY)

NEW QUESTION: 29

□□□ □□

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

□□: □□1

□□□: User1, User2

□□□: User3

2021□ 1□ 15□, □□□ □□□ □□ □□ □□ □□□ □□□□□. (□□□ □□ □□ □□□□□.)

Access reviews allow reviewers to attest to whether users still need to be in a role.

Review name * Review1

Description ⓘ

Start date * 01/15/2021

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never | End by | Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope
- ○ Guest users only
- ◉ Everyone

Group *
Group1

Reviewers

Reviewers Members (self)

Programs

Link to program
Default Business Flow

Upon completion settings

Advanced settings

Start

□□□□ □□ □□ □□□ □□ Review1 □□□ □□□□□.

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Answer:

Answer Area

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Explanation:
Box 1: No
The review end date is 14 days after the start (January 15), the end of the review cycle for the month is January 29. After that date, the review cycle will not start again until February 15.
Box 2: Yes
The user will not be removed from the group until the end of the access review period.
Box 3: No
Reviews are for Group1, which User3 is not a member of.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

NEW QUESTION: 30
Azure Active Directory(Azure AD) □□□□ □□□□.
□□ □□□ □□□□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□.
* □□□ □ □□□ □□ □□: □
* □□□□ □□□ □□ □ : 1
□□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □ □□□
B. □□□ □ □□
C. □□□ □ □□

D. □□□ □□ □ □□□ □□□ □□□

Answer: C (LEAVE A REPLY)

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks

NEW QUESTION: 31

□□□ □□

Azure Active Directory(Azure AD) □□□□ User1□□□ □□□□ □□□□.

□□□□ User1□ □□□□□.

□□ □□□□ □□□□ □□□.

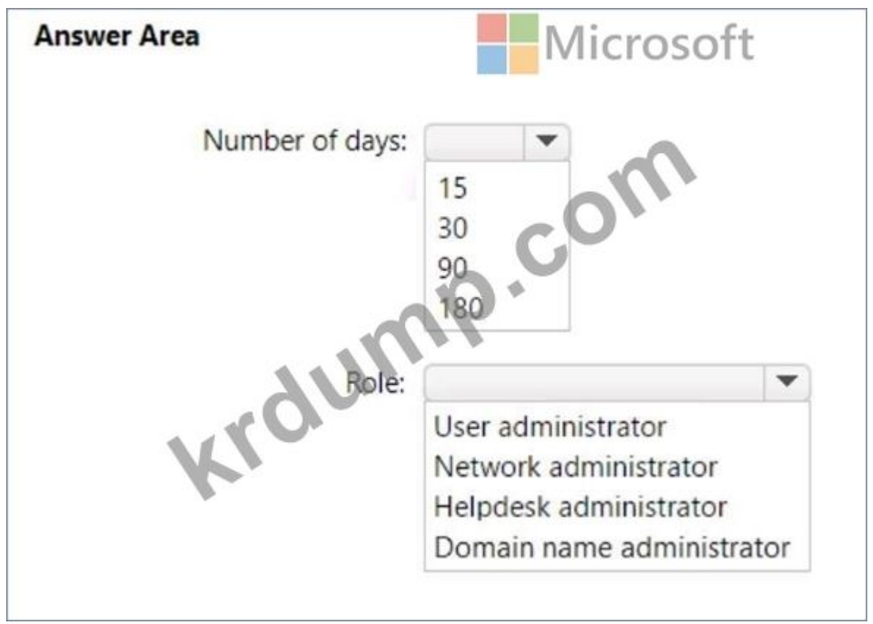
- □□□1□ □□□ □□□ □ □□□ □□□ □□□ □ □□□?

□ □□ □□□□?

- User1□ □□□□ □ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?

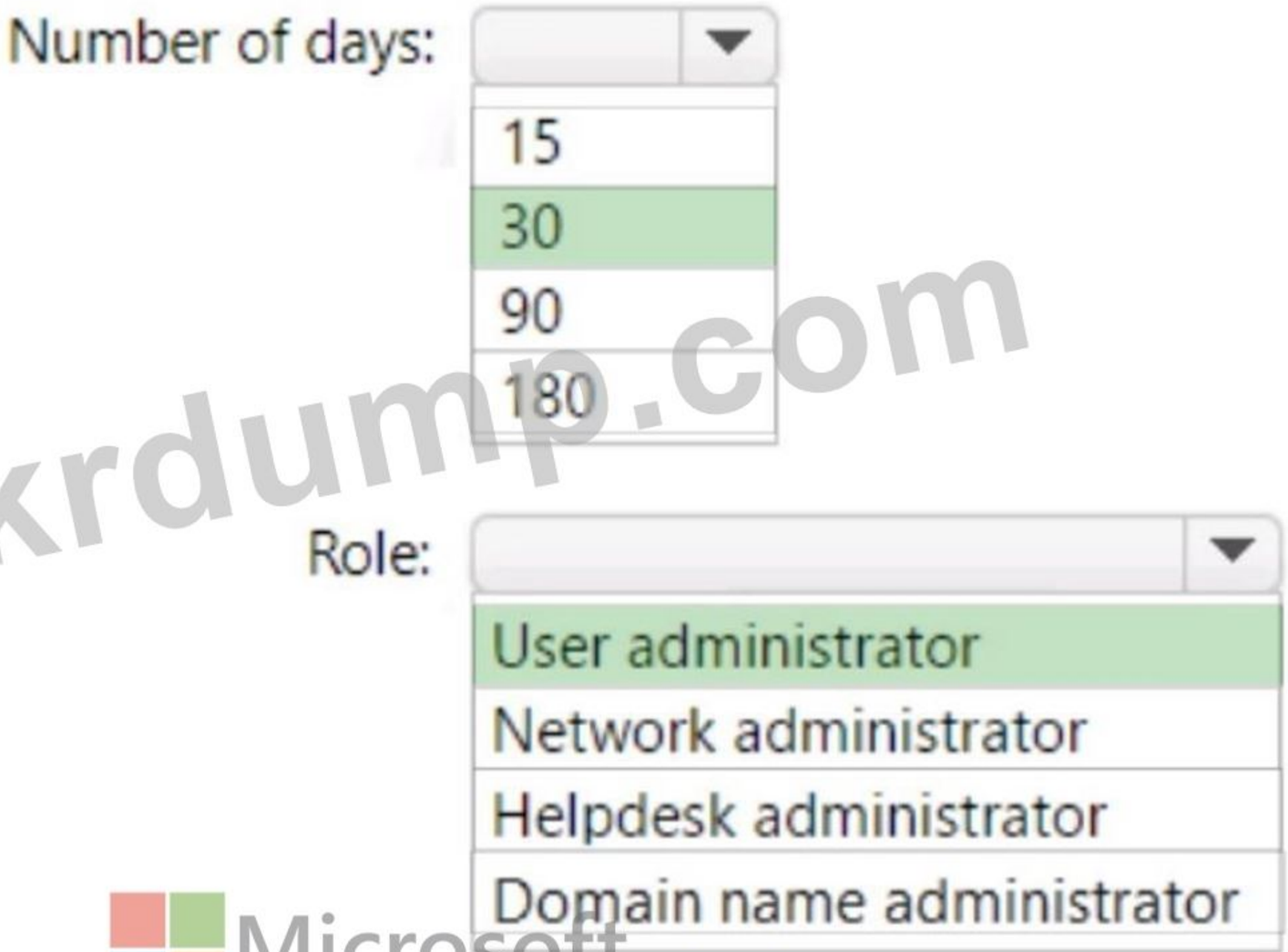
□□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.

□□: □□ □□□ 1□□□□.



Answer:

Answer Area



NEW QUESTION: 32

□□ □□ 2 - □□□□ □□□□

□□

Litware, Inc.□ □□□□ Fabrikam, Inc.□ □□□ □□ □□□□□.

Litware□ □□□□ □□□□ □□□□ □□ □□□, □□ □□□ □□□ □□□□ □□□□.

□□□□ VPN □□□ □□□□ □□□□ □ □□□ □ □ □□ □□□□□.

□□ □□. □□ □□

□□□□□□ litware.com□□□ □□□ Active Directory □□□□□ □□□, □ □□□□□ litware.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. Azure AD Connect□ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□□□□ □□□□.

Litware.com□□ □□ □□□□□□ □□□ □□□□ User1□□□ □□□□ □□□□.

Litware□ Azure AD □□□□□□ □□□□ □□□□□.

Fabrikam□ fabrikam.com□□□ □□□ Azure AD □□□□ □□□□ □□□□. Fabrikam□ □□□□□ litware.com □□□□ □□□ □□□ □□□□ litware.com□ □□□□ □□□□□.

□□ □□. □□□□ □□

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

Litware□ litware.com Azure AD □□□□ □□□ Azure □□□ □□□□ □□□□. □ □□□□ Azure Active Directory □□□□ Office 365 □□□□ □□□□ Azure Sentinel □□□□□ □□□□ □□□□. Azure Sentinel□ □ □ Azure AD □□□ □□□ □□ □□□ □□□□□.

□□ □□. □□□□□ □□

□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware□ □ □□□ □□ □□□□ □□ □□□□ □□□□. □ □□□ □□ □□□ □ VPN □□□ □□□□ Azure □□□ □□ □□□□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□□ □□□□ □ □□□ □□□□ □□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□□□.

* Azure AD □□ □□ ID □□(PIM)□ □□□□ □□ □□ □□ □□□ □□□□□.
* □□□ □□ □□□□ litware.com Azure AD □□□□ □□□□□□□ □□□□ □□□□ □□□□□.
* □□□ □□ □□□□ □ □□□ □□ □□□□□ □□□□ ID □□□ □□□□□.
* User1□ Azure AD□□ □□□□□□ □□□□□□□ □□□ □ □□□ □□□□□□.
* □□ □□ □□□ □□□□□□.

□□ □□. □□ □□

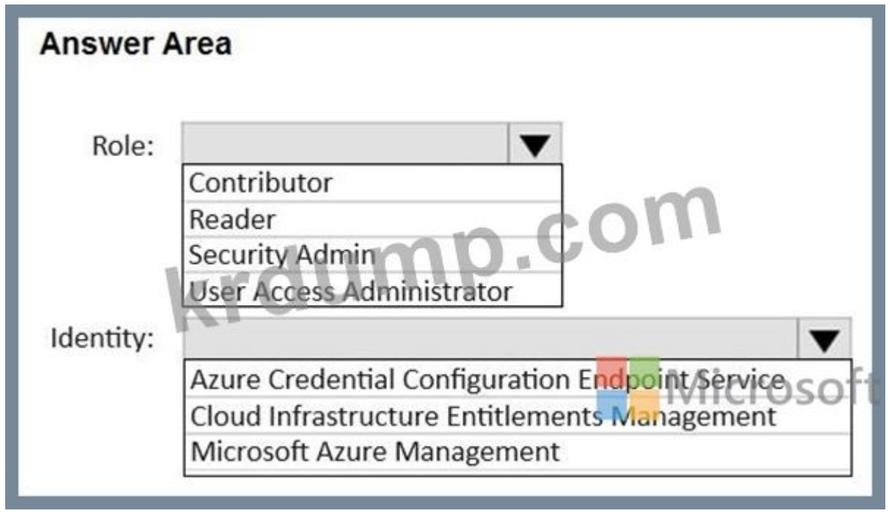
Litware□ □□ litware.com Active Directory □□□□□ LWLicenses□□ □□□ □□ □□□ □□□□□□. Litware□ LWLicenses □□ □□ □□□□ Azure AD □□□□ □□□ □□□□□ □□□. LWLicenses □□ □□ □□ □ □□□□ □□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□□ □□□.

□□□□. □□ □□□□

Litware□ Litware□ □□ Azure AD □□□ □□□ □□□□ Azure AD □□□ □□□ □□□ LWGroup1□□□ □□□ □□□□ □□□.

□□ □□. □□ □□ □□
Litware□ □□□ □□ □□ □□ □□□ □□□□□.
* □□ Litware □□□□□ □□□ □□(MFA)□ □□□□□□.
* Litware □□□ □□□□□ Azure AD□ □□□ □ MFA(□□□ □□)□ □□□□ □□□ □□□□ □□□□□.
* litware.com □□□□□ □□ □□ □□ □□□ □□□□□□.
* □□□□□ □□□□□□□ □□□□ □ MFA(□□□ □□)□ □□□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□ □□□□□.
□□ □□. □□ □□ □□
Litware□ □□□ □□ □□ □□ □□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□ Azure □□□ □ Azure AD □□□□□□□ □□ □□ □□□□ □□□□□.
* Microsoft SharePoint Online□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□.
* Azure AD□ □□□ □□□ □□□□ □□□□□□□ □□ □□ □□ □□□□ □□□□□.
□□□□. □□□□ □□□□
Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□ Microsoft Office 365 □□□ □□□ □□□ □□□ □□□□□ □□□.
ID □□□□□ □□□□ □□□□□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. □□□ □□□□□□□ □□□ □□ □□□ □□□□□.
B. □□□□□ □□□□□.
C. □□□□□ □□□□□.
D. □□□ □□□□□□□ □□ □□□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Requirement is for program which is a part of Access Reviews. Catalog is for Access Packages.
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview

NEW QUESTION: 33
□□□ □□
Sub1□□□ □□□ Azure □□□ □□□□.
Microsoft Entra □□ □□ □□□ □□□ □□□□□.
□□ □□ □□□□ Sub1□ □□ □□ □□□ □□□ □ □□□ □□ □□□.
□□□□ □□ □□ □□□ □□□ □□□.
□□ □□□ □□□□ □□, □ □□□ □□ □□□□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-controller-after-onboarding#enable-or-disable-the-controller-in-azure

NEW QUESTION: 34

□□ □□ 2 - □□□□ □□□□

□□

Litware, Inc.□ □□□□ Fabrikam, Inc.□ □□□ □□ □□□□□.

Litware□ □□□□ □□□□ □□□□ □□ □□□, □□ □□□ □□□ □□□□ □□□□.

□□□□ VPN □□□ □□□□ □□□□ □ □□□ □ □ □□ □□□□□.

□□ □□. □□ □□

□□□□□□ litware.com□□□ □□□ Active Directory □□□□□ □□□, □ □□□□□ litware.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. Azure AD Connect□ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□□□□ □□□□.

Litware.com□□ □□ □□□□□□ □□□ □□□□ User1□□□ □□□□ □□□□.

Litware□ Azure AD □□□□□□ □□□□ □□□□□.

Fabrikam□ fabrikam.com□□□ □□□ Azure AD □□□□ □□□□ □□□□. Fabrikam□ □□□□□ litware.com □□□□ □□□ □□□ □□□□ litware.com□ □□□□ □□□□□.

□□ □□. □□□□ □□

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

Litware□ litware.com Azure AD □□□□ □□□ Azure □□□ □□□□ □□□□. □ □□□□ Azure Active Directory □□□□ Office 365 □□□□ □□□□ Azure Sentinel □□□□□ □□□□ □□□□. Azure Sentinel□ □ □ Azure AD □□□ □□□ □□ □□□ □□□□□.

□□ □□. □□□□□ □□

□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware□ □ □□□ □□ □□□□ □□ □□□□ □□□□. □ □□□ □□ □□□ □ VPN □□□ □□□□ Azure □□□ □□ □□□□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□□ □□□□ □ □□□ □□□□ □□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□□□.

* Azure AD □□ □□ ID □□(PIM)□ □□□□ □□ □□ □□ □□□ □□□□□.
* □□□ □□ □□□□ litware.com Azure AD □□□□ □□□□□□□ □□□□ □□□□ □□□□□.
* □□□ □□ □□□□ □ □□□ □□ □□□□□ □□□□ ID □□□ □□□□□.
* User1□ Azure AD□□ □□□□□□ □□□□□□□ □□□ □ □□□ □□□□□□.
* □□ □□ □□□ □□□□□□.

□□ □□. □□ □□

Litware□ □□ litware.com Active Directory □□□□□ LWLicenses□□ □□□ □□ □□□ □□□□□□. Litware□ LWLicenses □□ □□ □□□□ Azure AD □□□□ □□□ □□□□□ □□□. LWLicenses □□ □□ □□ □ □□□□ □□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□□ □□□.

□□□□. □□ □□□□

Litware□ Litware□ □□ Azure AD □□□ □□□ □□□□ Azure AD □□□ □□□ □□□ LWGroup1□□□ □□□ □□□□ □□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

* □□ Litware □□□□□ □□□ □□(MFA)□ □□□□□□.
* Litware □□□ □□□□□ Azure AD□ □□□ □ MFA(□□□ □□)□ □□□□ □□□ □□□□ □□□□□.
* litware.com □□□□□ □□ □□ □□ □□□ □□□□□□.
* □□□□□ □□□□□□□ □□□□ □ MFA(□□□ □□)□ □□□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□ □□□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.

* □□□ □□□ □□□ □□□□ □□ Azure □□□ □ Azure AD □□□□□□□ □□ □□ □□□□ □□□□□.
* Microsoft SharePoint Online□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□.
* Azure AD□ □□□ □□□ □□□□ □□□□□□□ □□ □□ □□ □□□□ □□□□□.

□□□□. □□□□ □□□□

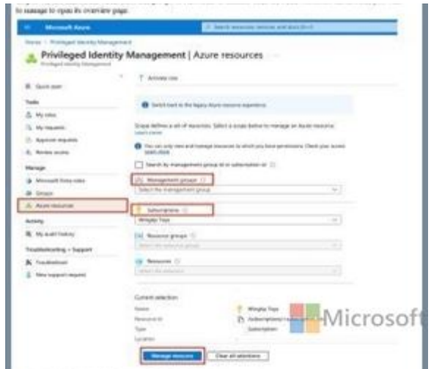
Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□ Microsoft Office 365 □□□ □□□ □□□ □□□ □□□□□ □□□.

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

□□□ □□ □□□?
A. Azure Sentinel □□ □□□ □□□ □□□□□.
B. □□ □□□ □□□□.
C. Azure Sentinel □□□ □□□□ □□□□□.
D. Azure Sentinel □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)
In order to enable these Fusion-powered attack detection scenarios, any data sources listed must be ingested using the associated Azure Sentinel data connectors.
https://docs.microsoft.com/en-us/azure/sentinel/fusion#attack-detection-scenarios

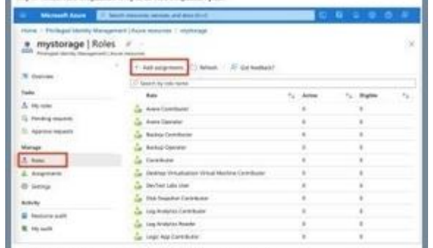
NEW QUESTION: 35
□□□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com
Microsoft 365 □□: =1122334455667788
Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 99999999
□□ □□□ □□□ □□ □□ □□□ □□ □□□□ □□□.
- Allan Deyoung□ □□ □□□ □□□ □□□□ □□□ □ □□□ □□□□.
- □□□□ □□□□ □□ □□□□ □□□ □ □□□ □□□□.
- □□ □□ □□□ □□□□□□.
□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□.
A. □□ ID □□(PIM)□□:
Christie Cline□□ □□ □□□ □□□ □□□ □□□ □□□□□□.
□□ □□□ □□ □□□ □□ □□ □□□□□ □□□□ □□, Allan Deyoung□ □□ □□□□ □□□□□□.
B. Entra ID □□□□:
Christie Cline□□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□ □ □□□ Allan Deyoung□ □□□ □□□ □□□ □□□□□.
C. Microsoft 365 □□ □□ > □□□□:
□□□□ □□□□ □□ □□□□ □□□□□.
□□ □□□□ □□□ □□□ □□□ □□□□ □□ □□□ □□□ □ □□□ □□□□.
D. Exchange □□ □□□□:
Christie□□ □□ □□ □□□ □□□□ □□ □□ □□□ □□□□□.
□□□□ □□ □□ □□ □□□ □□ □□ □□ □□□ □□□ □□□□□□.
Answer: A (LEAVE A REPLY)


to manage to open its overview page.



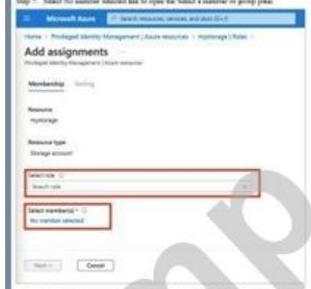
Step 4: Under Manage, select Roles to see the list of roles for Azure resources.

Step 5: Select Add assignments to open the Add assignments page.



Step 6: Select a Role you want to assign. [Here: Select the Group Administrator role]

Step 7: Select No member selected link to open the Select a member or group pane.

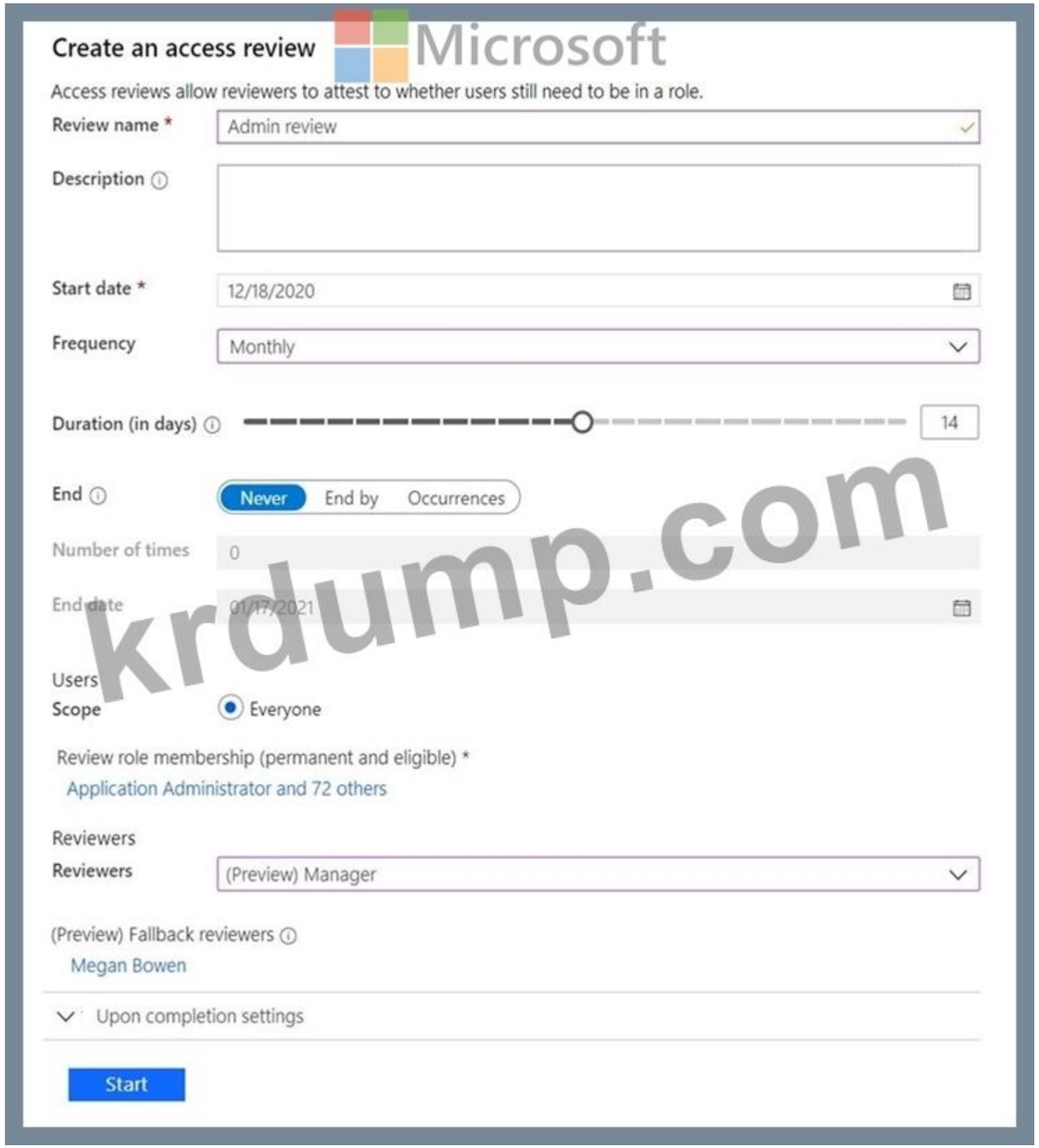


Step 8: Select a member or group you want to assign to the role and then choose Select. [Here: select Allin Deyoung]

Step 9: On the Settings tab, in the Assignment type list, select Eligible or Active. [Here: Select Active]

NEW QUESTION: 36
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Review1□□□ □□□ □□□ □□□ □□□□□. Review1□ 6□□□□ Microsoft□□ □□□□ □□□.
365 □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □ □□□□.
□□ □□□□ Review1□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□.
Review1□ □□ □□ □□□ □□□□ □□□?
A. □□
B. □□ □
C. □□□
D. □□ □□
Answer: (SHOW ANSWER)

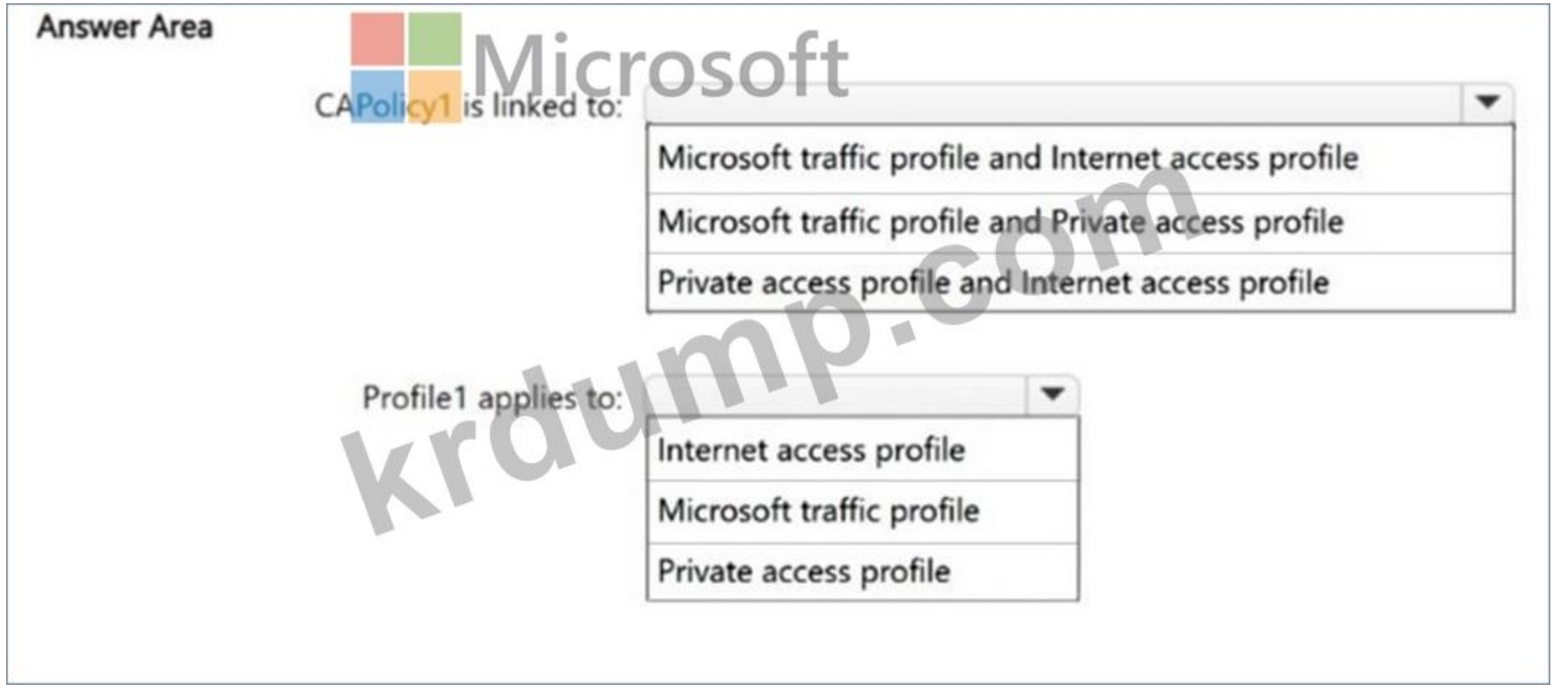
NEW QUESTION: 37
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 □□□□ □□□□.
10□ □□□ □□□ 100□□ IT □□□□ □□□□.



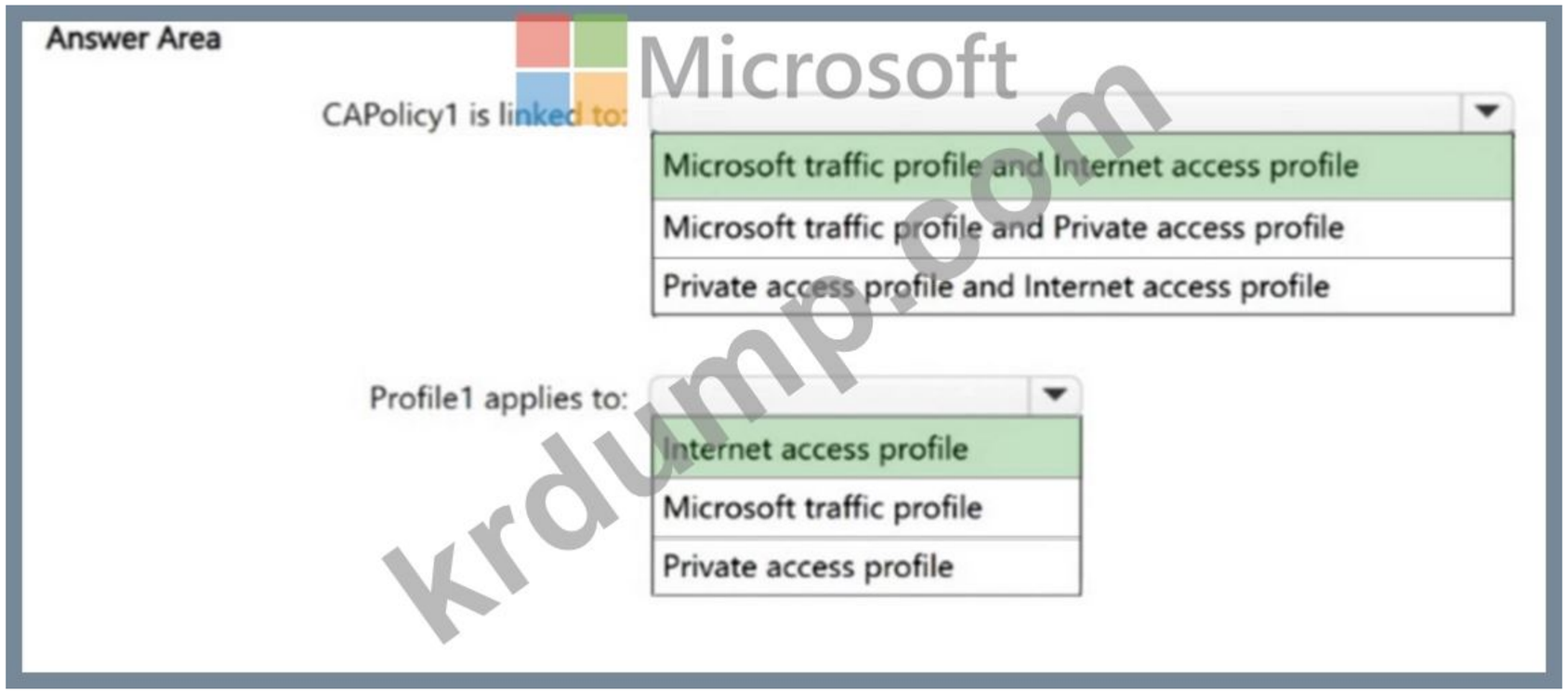
□□ □□ □□ □□□ □□ □□□□ □□□□□ □□□ □□ □□□□□.
□ □□ □□□□ □□ □□□ □□ □□□ □□□□ □□□□ □□□.
□□□: □ □□□□ □□ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)

The option of Fallback reviewer is when you set as reviewer to the manager or group owner and somehow that user is not having a manager in the directory. In those case, the fallback reviewer, which could be a department head would be the reviewer.
"Fallback reviewers are asked to do a review when the user has no manager specified in the directory or the group does not have an owner."
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

NEW QUESTION: 38
□□□ □□
□□□ 1,000□□ □□□□ □□ Microsoft Entra □□□□ □□□□ □□□□. □□ □□□□□□□ Microsoft Entra Suite □□□□□ □□□□ □□□□.
□□□ □□ □□□ □□□□□.
* □□□ □□ □□□□ □□□□□.
* Profile1□□□ □□□ □□□ □□ □□□ □□ □□□□ □□□□□.
* □□□ □□ □□□ □□□ □□□ □□□□□□.
- □□: CApolicy1
- □□ □□□: □□□ □□□ □□□ □□ □□□ □□□
□□
- □□: CApolicy2
- □□:
-- □□□ □□ □□□ □□ □□□ □□: □□□1
CAPolicy1□ □□ □□□ □□ □□□ □□□ □□ □□□□ □□□□ □□□, Profile1□ □□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 39
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□ □□□□ □□ □□□□ □□□ □□□ □□□□, □□ □□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□
B. □□□ □□□ □□
C. □□□ □□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
Sub1□□□ Azure □□□ □□, □ □□□□ RG1□□□ □□□ □□□ □□□□. RG1□□ DB1□□□ Azure Cosmos DB □□□□□□□ AKS1□□□ Azure Kubernetes Service(AKS) □□□□□ □□□□ □□□□. AKS1□ □□ ID□ □□□□□.
AKS1□ DB1□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- AKS1□ □□ ID□ □□□□ DB1□ □□□□□□ □□□□□□.
- □□ □□ □□□ □□□□□□.
AKS1□ □□ □□ ID□ □□ □□□ □□□□ □□□?
A. Sub1□ □□□ □□□ □□□□□.
B. DB1□ Azure Cosmos DB □□ □□ □□ □□(Account Reader Role)□ □□□□□.

C. RG1□ □□ Azure Cosmos DB □□□ □□ □□(Data Reader Role)□ □□□□□.
D. RG1□ □□, □□ □□(Reader) □□□ □□□□□.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 41
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□ □□□□ □□ □□ □□ □□ □□(MFA)□ □□□□□ □□□ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. □□□ □□□□ □□□□□.
B. □□□□ □□ □□ □□□ □□□□□.
C. □□ □□□□□ □□□□□.
D. □□□ □□□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
Protected actions are enforced through Conditional Access by associating specific high-impact permissions with an authentication context. The authentication context is the "tag" that Conditional Access can target for step-up requirements. You must create this authentication context first because it becomes the linkage point used later to bind the selected protected permissions to that context and build a Conditional Access policy that targets the context and requires a phishing-resistant authentication requirement (for example, the built-in Phishing- resistant MFA authentication strength). Without an authentication context in place, there's nothing to attach protected actions to and nothing specific for a Conditional Access policy to scope to for those protected permissions.

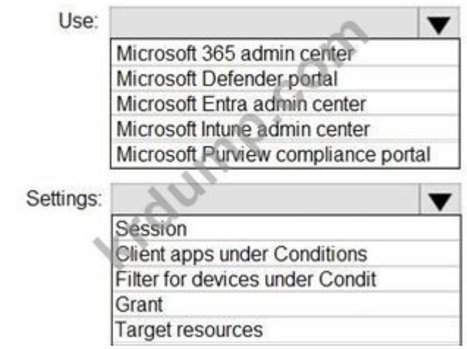
NEW QUESTION: 42
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Role
Admin1	Global Administrator
Admin2	Conditional Access Administrator
Admin3	Authentication Policy Administrator
Admin4	Global Administrator

Admin4□ "Azure □□□ □□ □□ □□ □□ □□" □□□□ □□□□ Policy1□□□ □□□ □□□ □□□ □□□□.
□□□ □□□□ □ □□ □□ □□(MFA)□ □□□□ □□ □□□□ □□□□□?
A. Admin1, Admin2, Admin3, Admin4
B. Admin2 □ Admin3□ □□
C. Admin1, Admin2, Admin3□
D. Admin1 □ Admin4□
Answer: (SHOW ANSWER)

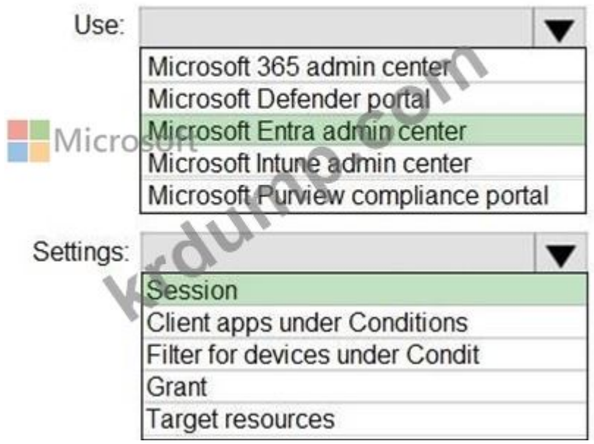
NEW QUESTION: 43
□□□ □□
□□□ Policy1□□□ □□□ □□□ □□□ □□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□ □□□ □□□□ □□□.
- Custom1□□□ □□□ □□□ □□□ □ □□□ □□□ □□ □□□ □□□□□.
- Policy1□ Custom1□ □□□□□ □□□□□.
Custom1□ □□□□□ □□□ □□□□ □□, Policy1□ □□ □□□□ □□□ □□□ □ □□□ □□□□□ □□□? □□□ □□□□□ □□ □□□□ □□□ □□□ □□□□□□. □□: □ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



Explanation:

Box 1: Microsoft Entra admin center

The "Conditional Access App Control" custom policy is created within the Microsoft Entra admin center. Specifically, you'll find it under Protection > Conditional Access > Policies. You can also access it through Entra ID > Conditional Access.

Box 2: Session

Define Session controls:

Under the "Session" section, you can enable Conditional Access App Control. This allows you to leverage Microsoft Defender for Cloud Apps for session controls and custom policies.

Reference:

https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

NEW QUESTION: 44

Azure Active Directory Premium P2 □□□□ □□□□.

Log Analytics □□ □□□ □□□□.

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

□□ □□ □□□ □□ □□□?

A. Set-AzureADTenantDetail cmdlet□ □□□□□.

B. Azure AD □□ □□□ □□□□.

C. Azure AD□ □□ □□ □□□ □□□□□.

D. Get-AzureADAuditDirectoryLogs cmdlet□ □□□□□.

Answer: C (LEAVE A REPLY)

AAD/Diagnostic Settings/Add Diagnostic Settings/Export Settings/Send to Log Analytic Workspace.

https://learn.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate- activity-logs-with-log-analytics#send-logs-to-azure-monitor

NEW QUESTION: 45

□□□ □□

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

□ □□□□ □□□ □□□□□.

User1□ □ □□ □□□□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.

User1□□ □□ □□□ □□□□ □□, User1□ □□ □□□ □□□□ □□□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

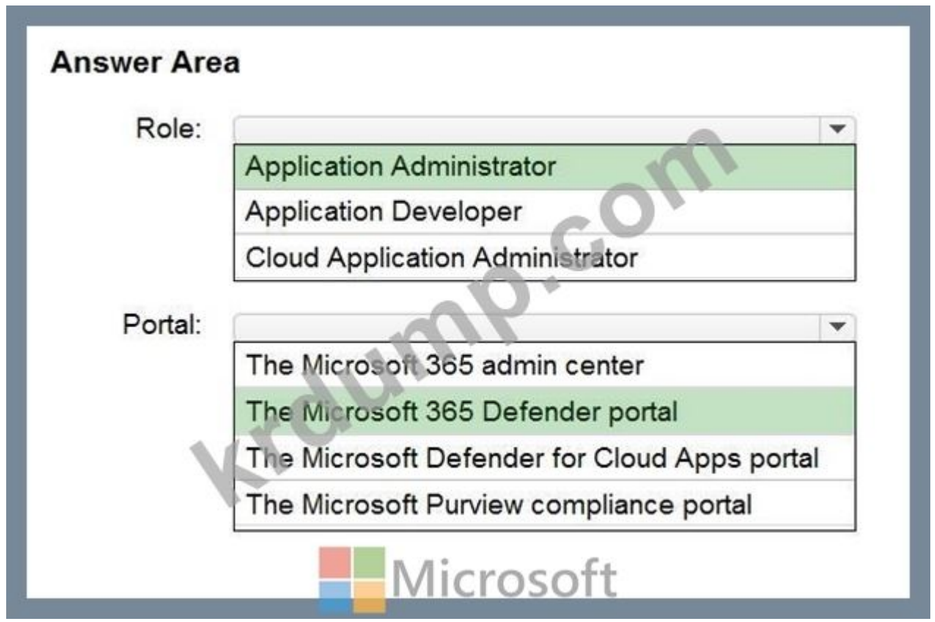
Role:

- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:

- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Answer:



Explanation:

https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles

NEW QUESTION: 46

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

* Device1□□□ □□

* User1, User2, User3, User4, User5□□ □□□ □□

* Group1, Group2, Group3, Group4, Group5□ □□□ □□

□□□ □□ □□ □□ □□□□□.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

□□ □□□ Microsoft Office 365 Enterprise E5 □□□□□ □□ □□□ □ □□□□?

A. □□1□ □□4□

B. □□1, □□2, □□3, □□4, □□5

C. Group1□ Group2□

D. □□1□

E. Group1, Group2, Group4, Group5□

Answer: C (LEAVE A REPLY)

You cannot assign licenses to group 3 because it is a device group. You cannot assign licenses to device groups.

You cannot assign licenses to group 4 and group 5. You cannot assign licenses to Microsoft 365 groups.

https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

NEW QUESTION: 47
□□□ Microsoft 365 □□□ □□□□ □□□□.
□□□□ Microsoft Edge□□ Microsoft 365 □□□ □□□□□ □□□□ □□□ □□□□□ □□□ □□ □□□□ □□□ □□□ □□□□□ □□ □□□.
Microsoft Entra □□ □□□□ □□□ □□ □□□?
A. □□□ □□□□ □□ □□ □□□ □□□□□□.
B. □□□ □□ □□□□□ □□ □□ □□□ □□□□□.
C. □□ □□□ □□□ □□□□□.
D. □□□ □□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
Configure your company branding
Language customization
Customize the sign-in experience based on browser language when users authenticate into your corporate intranet or web-based applications.
Customize the sign-in experience by browser language
You can create a personalized sign-in experience for users who sign in using a specific browser language by customizing the branding elements for that browser language. This customization overrides any configurations made to the default branding. If you don't make any changes to the elements, the default elements are displayed.
1. Sign in to the Microsoft Entra admin center as an Organizational Branding Administrator.
2. Browse to Identity > User experiences > Company branding.
3. Select Add browser language.
Reference:
https://learn.microsoft.com/en-us/entra/fundamentals/how-to-customize-branding

NEW QUESTION: 48
User1□□□ □□□□ □□□ Azure □□□ □□□□.
Azure AD □□□□ □□ □ □□ □□□ □□ □□□ □□ □□□□□.

User1□ App1□□□ □□□ ASP.NET □ □□□□□□□ □□□□□.
User1□ App1□ □□□ □ □□□ □□ □□□. □□ □□□ □□ □□ □□□ □□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□□□□ □□□
B. □□□□ □ □□ □□□
C. □□□□ □□□□□□ □□□
D. □□□□□□ □□□
Answer: A (LEAVE A REPLY)
Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability- is-disabled

NEW QUESTION: 49
□□□ □□
contoso.com□□□ □□□ Microsoft 365 □□□□ □□□□.
□□□ □□□ □□□□ □□□□□□□□.
□□□□ □□ □□ □□ □□ □□□ contoso.com□ □□□ □ □□□□.

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

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

Microsoft SharePoint Online □□□□□ □□□□ user3@adatum.com□ □□□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

Answer:

Explanation:
Box 1: Yes
Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.
Box 2. Yes
Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.
Box 3. No
Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

NEW QUESTION: 50
□□□ Azure AD □□□ □□□ □□□□ □□ □□□ □□□□□ □□□. □□ □□ □□□□ □□ □□□ □□□ □□□ □□□ □□ □□ □□ □□□□ □□ □□□ □ □□□ □□□ □□□ □□□□ □□□ □□□ □□□□ □□□. □□□ □□□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□ □□□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. Azure AD □□ □□
B. Azure AD □□ □□ ID □□
C. Azure Defender for Passwords
D. Azure AD □□□ □□

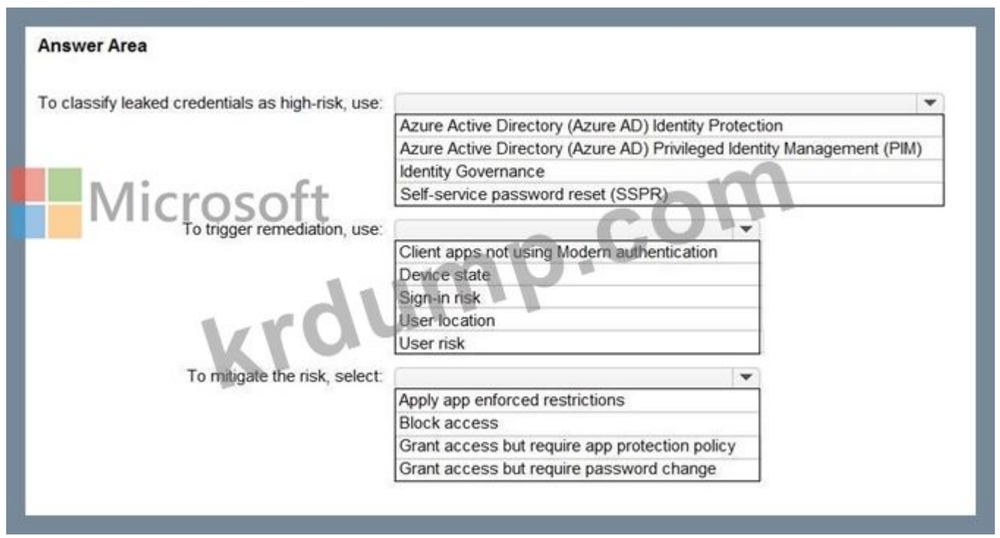
Answer: A (LEAVE A REPLY)
Azure AD Password Protection is a feature that detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization or other local entities such as sports teams.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad

NEW QUESTION: 51
Microsoft Entra □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□. Sub1□□ User1□□□ □□□□ □□□, User1□□□ Sub1 □□□ □□ □□ □□□ □□□□ □□□□.
User1□□ □□□ □□ □□□ □□ □□ □□□□ □□□□ □□□. □ □□□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□ □□□ □□□ □□ □□□?
A. □□/□□ □□□ □□ □□□ □□□□ □□□□□.
B. '□ □□' □□ □□□ □ □□□ □□□□□.
C. □□/□□ □□ □□□ □□□ □□□□□.
D. □□ □□ □□□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
There are four quick actions that can be used to manage users:
Revoke Unused Tasks
Revoke High-Risk Tasks
Revoke Delete Tasks
Assign Read-Only Status
https://learn.microsoft.com/en-us/training/permissions-management/explore-features-of-permissions-management/9-act-on-your-findings-with-remediation-tab

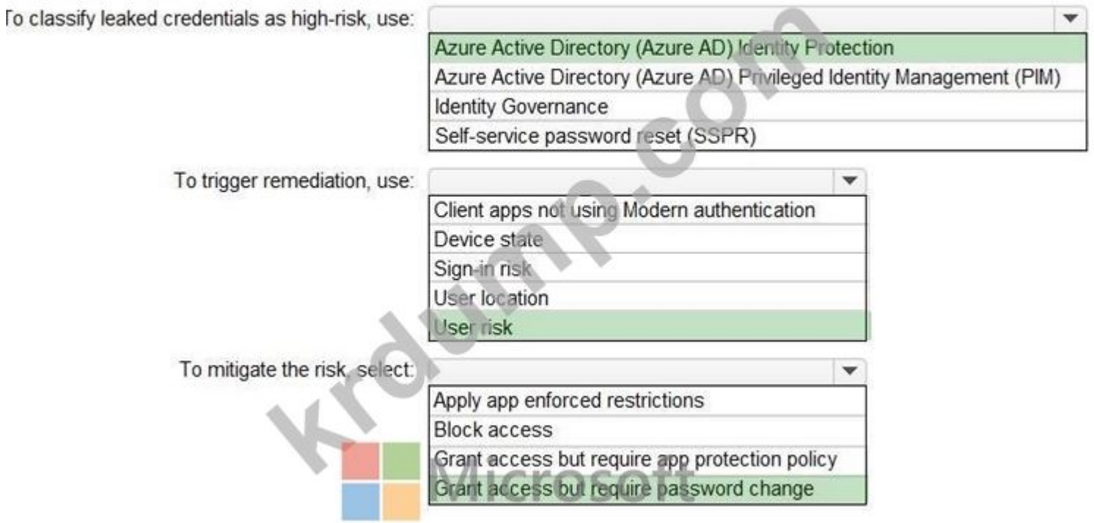
NEW QUESTION: 52
Microsoft 365 □□□□ □□□□.
□□ □□□□ □□□□□ □□□ 10 □□□□ □□□ □□□□.
□□□□□ □□□□□ □□□□ □□□ □□□□ □□□□□ □□ □□□□□. □□□ □□□□□ □□□ □, □□□□□ □□□□ □□□□ □□□ □ □□ □□ □□□□□ □□□□□.
□□□ □□□ □□(MFA)□ □□□ □□□□□.
□□ □□□□ □□□□ □□□ □ □□ MFA □□ □□□ □□□□□?
A. □□□□□ Windows Hello
B. Microsoft Authenticator □□ □□ □□
C. □□ □□
D. □ □□□□
Answer: (SHOW ANSWER)

NEW QUESTION: 53
□□□ □□
Microsoft 365 □□□□ □□□□.
□□ □□□ □□□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□ □□□ □□□□ □□□□ □□□ □□□ □□□□□.
□□□.
- □□□ □□□ □□□ □□□□ □□□□□.

- □□□ □□□□ □□ □□ □□□ □□ □□□□, □□□
□□□□ □□□□□□□ □□□ □ □□□ □□□.
□□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

NEW QUESTION: 54
□□□□ □□□□ □□ □□□ □□□ □□□□□ □ □□□□ □□□□ □□□ □□□ □□□ □□□□□.

□□ □□□□ □□□ □□□□□ □□□.
- □□□□ □□ □□□□ □□□□□□.
- □□□□ □□□ □□□ □□□□□□.
□□□ □□□□□ □□□ □□□□ □□□?
A. □□□ □□□ □□ □□□□ □□
B. Azure Active Directory(Azure AD)□ □□□ □□
C. Microsoft Defender for Cloud Apps□ □□ □□
D. Azure Active Directory(Azure AD)□ □□□ □□
Answer: (SHOW ANSWER)
The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.
Reference:
https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available

NEW QUESTION: 55
Azure □□□ □□□□ □□□□. □□ □□□□ Linux□ □□□□ VM1□□□ □□□ □□ □□□ □□□□.
VM1□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□□ Microsoft Entra□ □□□□ VM1□ □□□□ □ □□□ □□□□□□.
□□□.
- □□ □□ □□□ □□ □□□□ □□□□□ □□□□□□.
- □□□□ □□□□□ □□□□ VM1□ □□□□□ □□□□ □□□□□.
□□□□ □□□ □ □□ □ □□ □□ □□□ □□□□□? □ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□□□□□□ □□ □
B. SMS
C. □□ □□□
D. □□□□□ Windows Hello
E. FIDO2 □□ □
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 56
□□□ Site1□□□ □□□ Microsoft SharePoint Online □□□□ Group1□□□ □□□ Microsoft 365 □□□ □□□ Microsoft 365 □□□ □□□□ □□□□.
□□1□ □□□□□ 90□ □□ □□□1□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□
B. □□□ □□
C. □□□□□ □□□□
D. □□□ □□□ □□
Answer: A (LEAVE A REPLY)
For this scenario, an access package would be the most suitable. An access package in Azure Active Directory (Azure AD) entitlement management is a bundle of resources that you can give to users so they can access a set of

related resources. They can be configured to expire after a certain amount of days (in this case 90 days), after which access to the resources is automatically revoked, saving administrative effort.

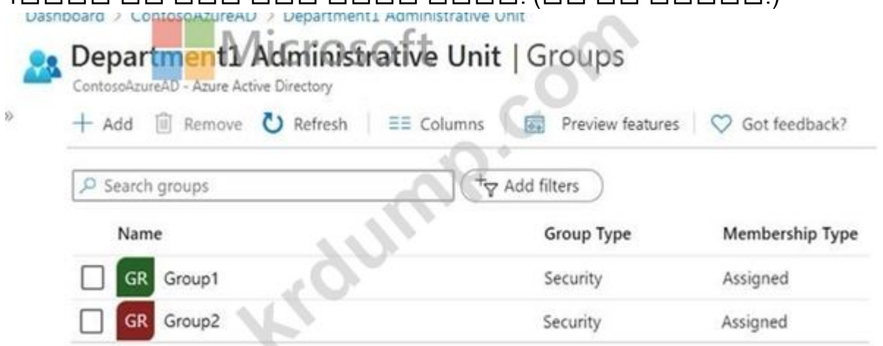
NEW QUESTION: 57

□□□ □□

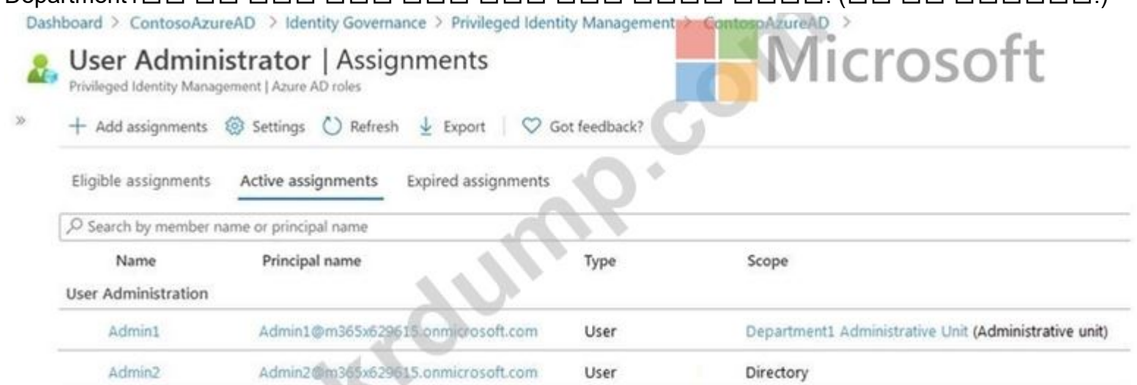
□□□ Department1□□□ □□ □□□ □□□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.

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

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



Department1□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□. (□□ □□ □□□□□□.)



□□2 □□□□ □□2 □□□□ □□□ □ □□□□. (□□2 □□ □□□□□.)

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

Explanation:
Admin1 and Admin2 are not members of Administrative group(Department1). However Admin1 has User administrator role scope for Department1 and Admin2 has User administrator role scope for the whole directory User 1 And User 2 are users of Department1 Group1(No members) and Group2(User 3 and User4 are members) are groups of Department1.
Box 1: No
Admin1 cannot reset the password for User 3 and User4 because they are part of group2.(User admin role assigned to admin unit cannot reset password of users present inside the group.
Admin1 can reset the password of User1 and User2 who are not part of any groups inside the admin unit) Box 2: Yes Admin1 can add/remove users to the GROUPS present inside the admin unit (Admin1 cannot add/remove users from USERS section) Box 3: Yes Admin2 is User admin at directory scope ,hence can reset password of any uses except the password of global admin/higher power roles

NEW QUESTION: 58
□□□ □□
Microsoft Entra □□□□□ Group1 □ Group2□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□□.

Name	Type	Member of	Description
User1	Member	Group1	*None*
User2	Guest	Group1	*None*
User3	Member	*None*	Assigned the Owner role for Group1
User4	Member	Group2	Assigned the Owner role for Group2
User5	Guest	Group2	*None*

□□2□ □□1□ □□□□□□.
□□□ □□ □□□□ □□□ □□□ □□□□□.
- □□: □□1
- □□□ □□□ □□□□□: □ + □□
- □□ □□: □ □ □□ □□
- □□: □□1
- □□ □□: □□□ □□□□ □□
- □□□ □□: □□ □□□

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User3 can perform an access review of User1.	○	○
User3 can perform an access review of User4.	○	○
User3 can perform an access review of User5.	○	○

Answer:

Answer Area

Statements	Yes	No
User3 can perform an access review of User1.	○	●
User3 can perform an access review of User4.	○	●
User3 can perform an access review of User5.	●	○

NEW QUESTION: 59
Azure AD □□□□ □□□□.
Azure AD □□ □□ ID □□(PIM)□ □□□ □□□□□.
PIM□ □□□□ □□ □□□ □□□ □ □□□?
A. □□□ □□□ □□
B. □□□ □□□ □ □□ □□□□ □□

C. □□□ □□□, □□ □□□ □ □□ □□□□ □□
D. □□ □□□, □□□ □□□, □□ □□□ □ □□ □□□□ □□
Answer: (SHOW ANSWER)
You can manage just-in-time assignments to all Microsoft Entra roles and all Azure roles using Privileged Identity Management (PIM) in Microsoft Entra ID.
https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION: 60
□□□ □□
□□□□□□ contoso.com□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. contoso.com□□ □□ □□ □□□ ID□ □□□□ □□□□.

Name	Type	Member of	In organizational unit (OU)
User1	User	Group1	OU1
User2	User	Group2	OU2
Group1	Group	*None*	OU1
Group2	Group	Group1	OU1

Microsoft Entra □□□□ User1□□□ □□□□ □□□□.
Microsoft Entra Cloud Sync□ □□□□ □□ □□□□ □□□□ □□ □□□ □□□□□.
CN=□□1,OU=OU1,DC=contoso,DC=com.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Statements	Yes	No
Contoso\User1 syncs from contoso.com to the tenant	○	○
Contoso\User2 syncs from contoso.com to the tenant.	○	○
Contoso\Group1 syncs from contoso.com to the tenant.	○	○

Answer:
Answer Area

Statements	Yes	No
Contoso\User1 syncs from contoso.com to the tenant	○	○
Contoso\User2 syncs from contoso.com to the tenant.	○	○
Contoso\Group1 syncs from contoso.com to the tenant.	○	○

Explanation:
Box 1: Yes
User1 is in Group1.
User1 is in OU1.
Note:
The filter is for Group1 and OU1.

Box 2: No
User2 is in OU2.
User2 is in Group2.
Group2 is in OU1.
Group2 is a member of Group1.
Box 3: Yes
Group1 is in OU1.
Note: You can use multiple filtering options at the same time. For example, you can use OU- based filtering to only include objects in one OU. At the same time, you can use attribute-based filtering to filter the objects further.
When you use multiple filtering methods, the filters use a logical "AND" between the filters.
Reference:
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering

NEW QUESTION: 61
□□□ storage1□□□ □□□ □□□□ □□□ □□□ Azure □□□ □□□□ □□□□.
□□ □□ □□□ □□□□ App1□□□ □□ □□□ □□□□□. □□□ □□ □□□ □□ □□ □□□□ □□ API□ □□□ □□□□.
□□ □□□ □□□ □□ □□□□ □□□ □□□□. □□ □□□□ □□ □□ □□□ □□□□ □□□.
- □□ □□□ □□□□ □□□□□.
- App1 □□□ □□ □□□ □□□ □□□ □□□ □□□□.
- □□ □□□ Azure □□□□ □□□□ □ □□□ □□□ □□□ □□□□□□.
Microsoft Entra □□
- □□□ □□□ □□□□□□.
□□ □□□ □□□ □□□□ □□□?
A. □□□ □□ □ □□□□ □□□ □□□
B. □□□ □□ □□ ID □ Azure Key Vault
C. □□□ □□ □ Azure Key Vault
D. □□□ □□ □□ ID □ □□□□ □□□ □□□
Answer: B (LEAVE A REPLY)
Azure Key Vault for the 3rd party API creds, and a user assigned managed identity for the MULTIPLE VMs to access "Azure resources by using Entra authentication".

NEW QUESTION: 62
□□□ Microsoft Defender for Cloud Apps□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□□ □□□□ □□ □3□ □□ □□□□ □□ □□□□□□.
□□ □□□ 5□□□ □□ □□□□ 200GB□ □□□□ □□□□ □□ □□ □□□□ □□□□ □□□□ □□□. □□ □□ □□□ □□□□□ □□□.
□□□ □□ □□□?
A. Microsoft Defender □□□□ □ □□ □□□ □□□□□.
B. □□□ □□ □ □□□□ □□□□ □ □□ □□□ □□□□□.

C. Microsoft Entra □□ □□□□ □□□ □□□ □□□ □□□□□.
D. □□□ □□ □ □□□□ □□□□ □ □□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)
The best action to take is to create an app discovery policy by using the New risky app template.
Perfect Alignment: The New risky app template in Microsoft Defender for Cloud Apps is specifically designed to trigger alerts and take automatic actions based on risk scores and traffic volume.
Automation: By configuring this Cloud Discovery anomaly detection policy, you can automatically tag matching discoveries as Unsanctioned.
Low Administration: Once integrated with your security appliances or Microsoft Defender for Endpoint, unsanctioned apps are blocked automatically without requiring manual administrator intervention for each app.
Reference:
https://learn.microsoft.com/en-ca/answers/questions/5876601/using-defender-for-cloud-apps-to-control-access-to

NEW QUESTION: 63
□□□ Microsoft 365 □□□ □□□□ □□□□.
Azure □□□□ App1□□□ □□□ Azure App Service □ □□ □□□□ □□□□.
Windows□ □□□□ Microsoft Intune□ □□□ □□□ □□ □ □□□□.
Intune□ □□□□ Global Secure Access □□□□□□ □□□ □□□□□.
App1□ □□ □□ □□□□ □□□□ □□□.
□□□□ □□□ □□ □□□?
A. □□□□□□ □□ □□□ □□□□□.
B. □□ □□□□ □□□□ □□□□□.
C. □□□ □□□ □□□□ □□□□□.
D. □□ □□□□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
□□□ □□
Azure □□□ Group1□□□ □□□ User1, User2□□ □ □□ □□□□ □□□□. User1□ Group1□ □□□□□□.
App1□□□ □□□ □□□ □□□□□□□ □□□□□.
App1□ □□ □□ □□□ □□□□□□ □□□□ □□□□□ □□ □□□ □□□□□.
- □□□□ □ □□□□□□□ □□ □□□ □□□ □□□ □ □□□ □□□□□□□□? □
- □□□ □□□□ □□ □□□ □□□□ □□□? □□1
- □ □□□□□□□ □□ □□ □□□ □□□□ □□ □□□ □□□ □□□?: □
- □ □□□□□□□ □□ □□ □□□ □□□ □ □□ □□□ □□□□□? □□□2
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Answer:

Explanation:
Box 1: Yes
Box 2: No
Being allowed to approve access to an application in Azure self-service application access does not automatically assign you to the application's group. While you can configure an application to have a specific group assigned to it upon approval, the approver themselves is not automatically added to that group.
Box 3: Yes
For self-service application access in Azure, approvers utilize the Microsoft Entra admin center to review and make decisions on access requests. Specifically, approvers can access the "My Access" portal within the Microsoft Entra admin center to view pending requests and either approve or deny them.
Reference:
https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/manage-self-service-access

NEW QUESTION: 65
□□□ □□
□□□ Site1□□□ □□□ Microsoft SharePoint Online □□□□ □□ □□ □□□ □□□□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

□□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Platform	Azure AD join type
Device1	Windows 11	*None*
Device2	Windows 10	Azure AD joined
Device3	Android	Azure AD registered

□□□ □□ □ □□ □□□ □□□ □□□ □□□□□.
- □□: CAPolicy1
- □□
o □□□ □□ □□□□ ID: □□1
o □□□□ □ □□ □□: Office 365 SharePoint Online
□□
□□ □□: □□□□ □□□ □□□□ □□□□□.
□□ □□: device.displayName -startsWith Device?
o □□ □□
□□: □□ □□
□□: □□□ □□□ 0□
o □□ □□□: □□
- □□: CAPolicy2
- □□
o □□□ □□ □□□□ ID: □□2
o □□□□ □ □□ □□: Office 365 SharePoint Online
o □□: □□□ □□ 0□
- □□ □□
o □□ □□: □□ □□ □□
□□ □□ □□□ □□□□□.
□□: 0□□ □□□□ □□□□□□□□.
- □□ □□□: □□
□□ □□□□ MFA□ □□□□ □□□□□ □□□ □ □□□ □□□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Statements	Yes	No
User1 can access Site1 from Device1.	○	○
User2 can access Site1 from Device2.	○	○
User3 can access Site1 from Device3.	○	○

Answer:

Statements	Yes	No
User1 can access Site1 from Device1.	○	●
User2 can access Site1 from Device2.	●	○
User3 can access Site1 from Device3.	○	●

NEW QUESTION: 66

□□□ User1□ □□ □□ □□□ □□□ □□□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

User1□ □□□ IP □□□□ □□□□□□ □□□ □ □□ □□□ □□□□ □□□□ □□□.

□□ □□□ □□□□ □□□?

A. □□□ □□

B. □□ □□ □□

C. □□ □□□□ □□

D. Microsoft 365 □□□□ □□ □□□ □□

Answer: C (LEAVE A REPLY)

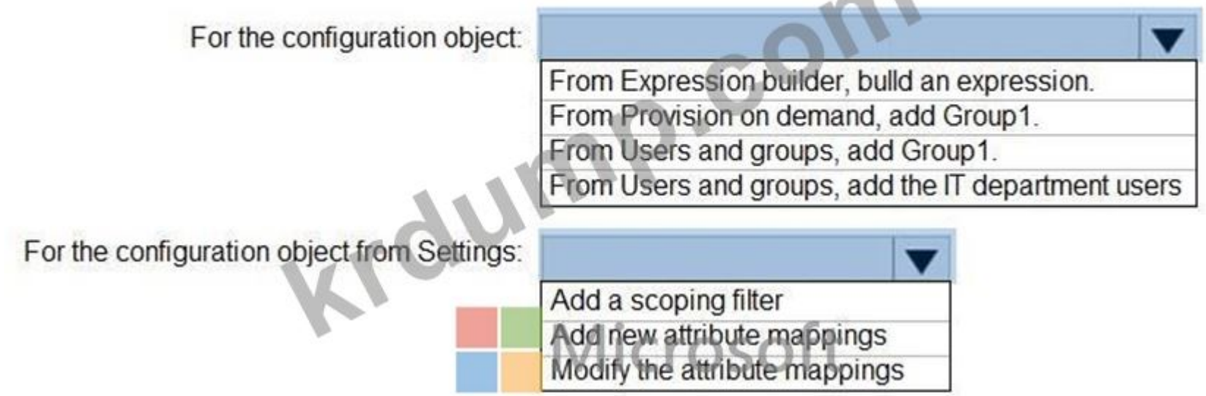
The Azure AD conditional access What if tool allows you to understand the impact of your conditional access policies on your environment. Instead of test driving your policies by performing multiple sign-ins manually, this tool enables you to evaluate a simulated sign-in of a user. The simulation estimates the impact this sign-in has on your policies and generates a simulation report. The report does not only list the applied conditional access policies but also classic policies if they exist.
Reference:
https://azure.microsoft.com/en-us/updates/azure-ad-conditional-access-what-if-tool-is-now-available

NEW QUESTION: 67
□□□ Pass4test Inc.□ □□□□ □□□□□, Azure AD □□ □□□ □□□ □□ □□□ □□□□□□. □ □□ □□□ □□□, □□ □□□, □□ □□□ □□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□ □□ □ □□ □□ □ □□ □□□ □□□□□. □□ □□ □ □□ □□ □□□ □□□□ □□□. □□ □□□□ □□ □□□ □□□□ □□□?
A. □□□□ □□□
B. □□□ □□□
C. □□ □□□
D. □□□ □□□
Answer: (SHOW ANSWER)
The Global Admin role would allow the new employee to reset passwords for all users.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator
https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

NEW QUESTION: 68
Sub1□□□ Azure □□□ □□, □ □□□□ User1□□□ □□□□ □□□□.
User1□ Sub1□ □□ Microsoft Entra □□ □□ □□□□□ □□□ □ □□□ □□ □□□. □□ □□□ □□ □□ □□□ □□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□ □□□
B. □□□ □□□ □□□
C. □□□ □□□
D. □□ □□ □□□
Answer: A (LEAVE A REPLY)

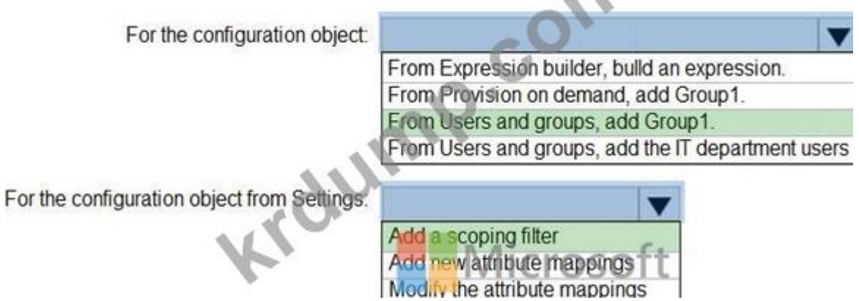
NEW QUESTION: 69
□□□ □□
contoso.com□□□ Microsoft Entra □□□□ □□, □ □□ Group1□□□ □□□ □□□□.
□□1□□ □□ IT □□ □□□ 50□□ □□ □□ □□□ 50□□ □□□□ □□□□.
□□□ □□□ □□□ fabrikam.com□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.
contoso.com□ fabrikam.com □□ □□□ □ □□□□ □□□□□.
Group1□ □□□ □□□ fabrikam.com□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- IT □□ □□□□ fabrikam.com□ □□□□ □ □□□ □□□□.
- □□□ □□□ □□□□□□.
□□□ □ □□□ □□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area



NEW QUESTION: 70

□□□ □□

Sub1□□□ □□□ Azure □□□ □□□□.

Microsoft Entra □□ □□ □□□ □□□ □□□□□.

□□ □□□□ Sub1□ □□□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□ □□□.

PowerShell □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

NEW QUESTION: 71

□□□ Microsoft Entra □□□□ □□□□ □□□□.

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

- □□□ □ □□□ □□ □□: □
- □□□□ □□□ □□ □: 1

□□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?

A. □□□ □ □□

B. □□ □□ □□□ □□□ □□□

C. □□□□□□□ □□ □□

D. FIDO2 □□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 72

□□□ □□

□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□□ 500□□ Windows 11 □□□ □□□□.

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

Policy1□□□ □□□ □□□ □□□ □□□ □□□□□.

□□ □□□ □□□□ □□□.

- Policy1□ □□ Windows □□□ □□□□□.
- Windows □□□ □□1□ □□□□□ □□□□□.

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

□□: □□ □□□ 1□□□□.

Answer Area

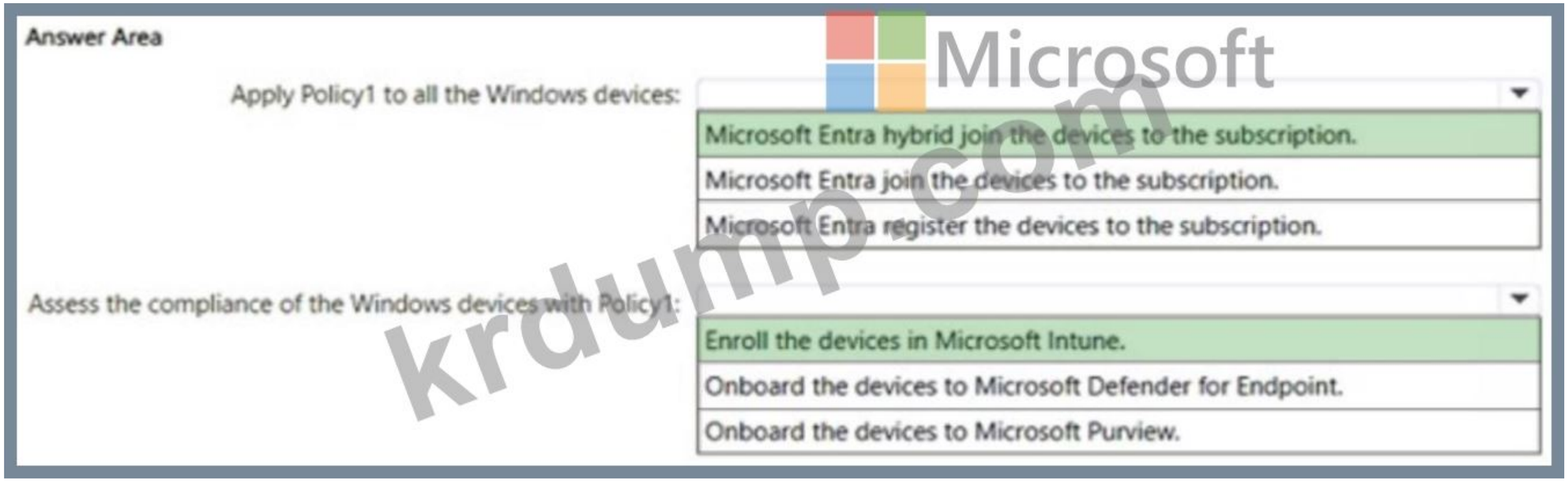
Apply Policy1 to all the Windows devices:

- Microsoft Entra hybrid join the devices to the subscription.
- Microsoft Entra join the devices to the subscription.
- Microsoft Entra register the devices to the subscription.

Assess the compliance of the Windows devices with Policy1:

- Enroll the devices in Microsoft Intune.
- Onboard the devices to Microsoft Defender for Endpoint.
- Onboard the devices to Microsoft Purview.

Answer:



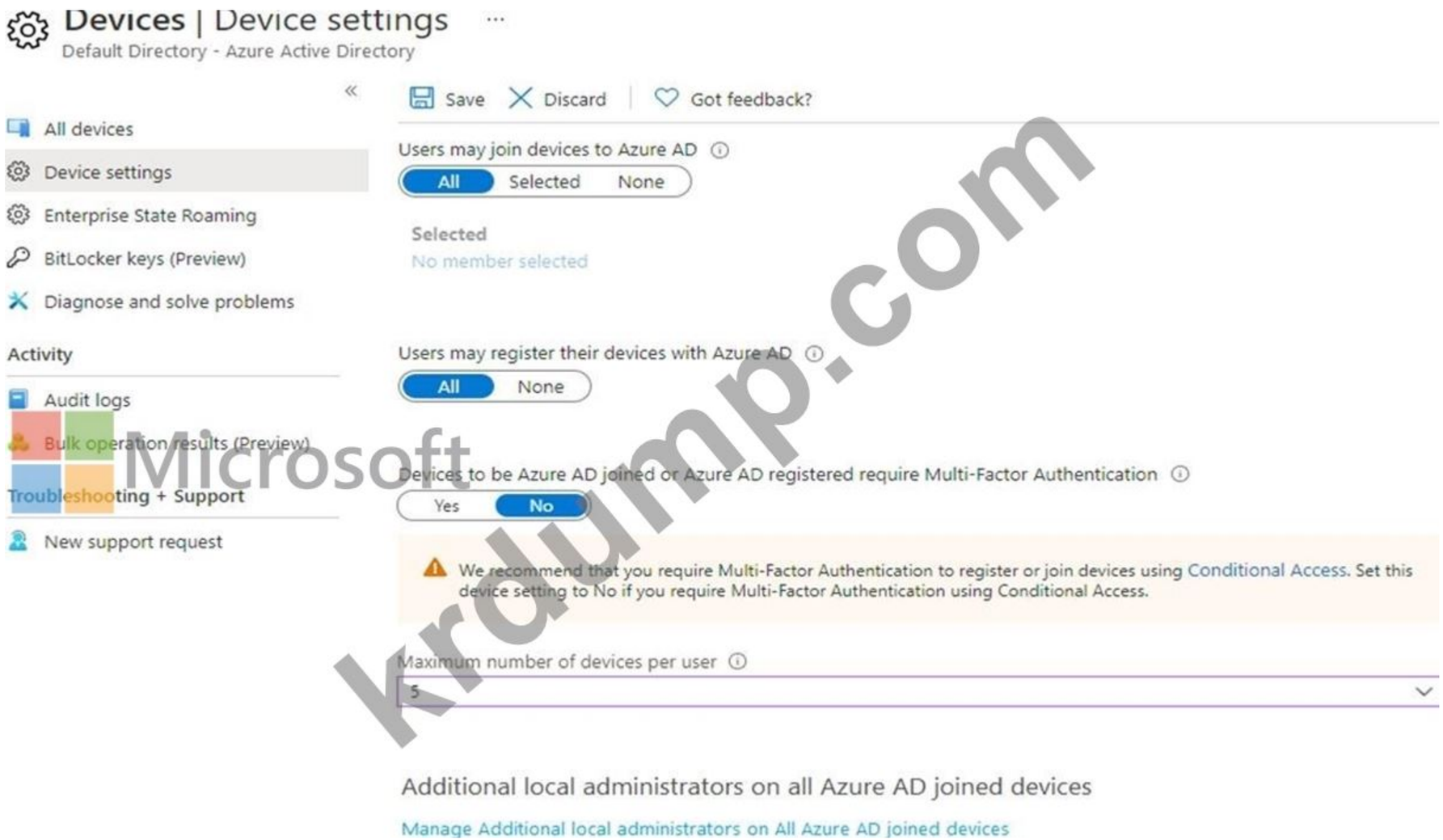
NEW QUESTION: 73

□□□ □□

Azure Active Directory Premium Plan 2 □□□□□ □□ Azure Active Directory(Azure AD) □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□□.

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	**None**

□□ □□□ □□ □□ □□□ □□□□□.



User1□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Operating system	Device identity
Device1	Windows 10	Azure AD joined
Device2	iOS	Azure AD registered
Device3	Windows 10	Azure AD registered
Device4	Android	Azure AD registered

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	○
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Azure AD.	○	●
Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.	●	○
Admin2 is a local administrator on Device3.	○	●

Explanation:

Box 1: No

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.

Box 2: Yes

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

* Global Administrator
* Cloud Device Administrator
* Global Reader
* Directory Reader

Box 3: No

Additional local administrators on Azure AD joined devices (Device is Registered not Joined) Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

NEW QUESTION: 74

Azure AD □□□□ User1□□□ □□□□ □□□□.

User1□ □□□□ □□□ □□□□ □□□ □□□ □□□□□ □□□.

User1□□ □□ □□□ □□□□ □□□?

A. □□□□□ □□□

B. □□ □□□

C. □□□□ □□□

D. □□□ □□□

Answer: D (LEAVE A REPLY)

Only User Access Admin fits in both the requirement : manage license assignments and reset user passwords.

NEW QUESTION: 75

Azure AD □□□□ □□□□.
□□□□ □ □□ □□□□ □□□ □□ □□□□□□.
□□□ □□□ □□□□□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□□ □□ □□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□□ □□□ □□□□□.
C. Microsoft Defender for Cloud Apps □□□□ □□□□ □□ □□ □□ □□□ □□□□□.
D. Microsoft Defender for Cloud Apps □□□□ □ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
□□□ □□
□□□ Azure □□□□ □□ □□ □□□ □ □□ □□ □□□ □□□□ □□□□.

Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

6□ 1□, Admin4□ □□□ □□ □□□ □□□□□.
KeyVault1□□ Certificate1□□□ □□□ □□□□ □□□□□.
- KeyVault2□□ Secret1□□□ □□□ □□ □□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	○	○
Admin2 can purge Certificate1 on June 12.	○	○
Admin3 can purge Certificate1 on June 14.	○	○

Answer:

Answer Area

Statements	Yes	No
Admin1 can recover Secret1 on June 7.	●	○
Admin2 can purge Certificate1 on June 12.	○	●
Admin3 can purge Certificate1 on June 14.	○	●

Explanation:

Box 1: Yes

Key Vault Administrator can perform all data plane operations on a key vault.

And purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.

Do not mismatch with soft-delete

Box 2: No

We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate Box 3: No We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

NEW QUESTION: 77
□□ □□ □□□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned
Group5	Microsoft 365	Dynamic User

□□ □□□ □□ □□□ □□□ □□□ □ □□□?
A. □□1□
B. □□1□ □□4□
C. Group1□ Group2□
D. Group1, Group2, Group4, Group5□
E. □□1, □□2, □□3, □□4 □ □□5
Answer: D (LEAVE A REPLY)
Technically you can create access review for Dynamic Device group (no errors/warnings during the creation), however it doesn't work and you will see a hitch "Warning - No access to review" for that access review in the list.
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

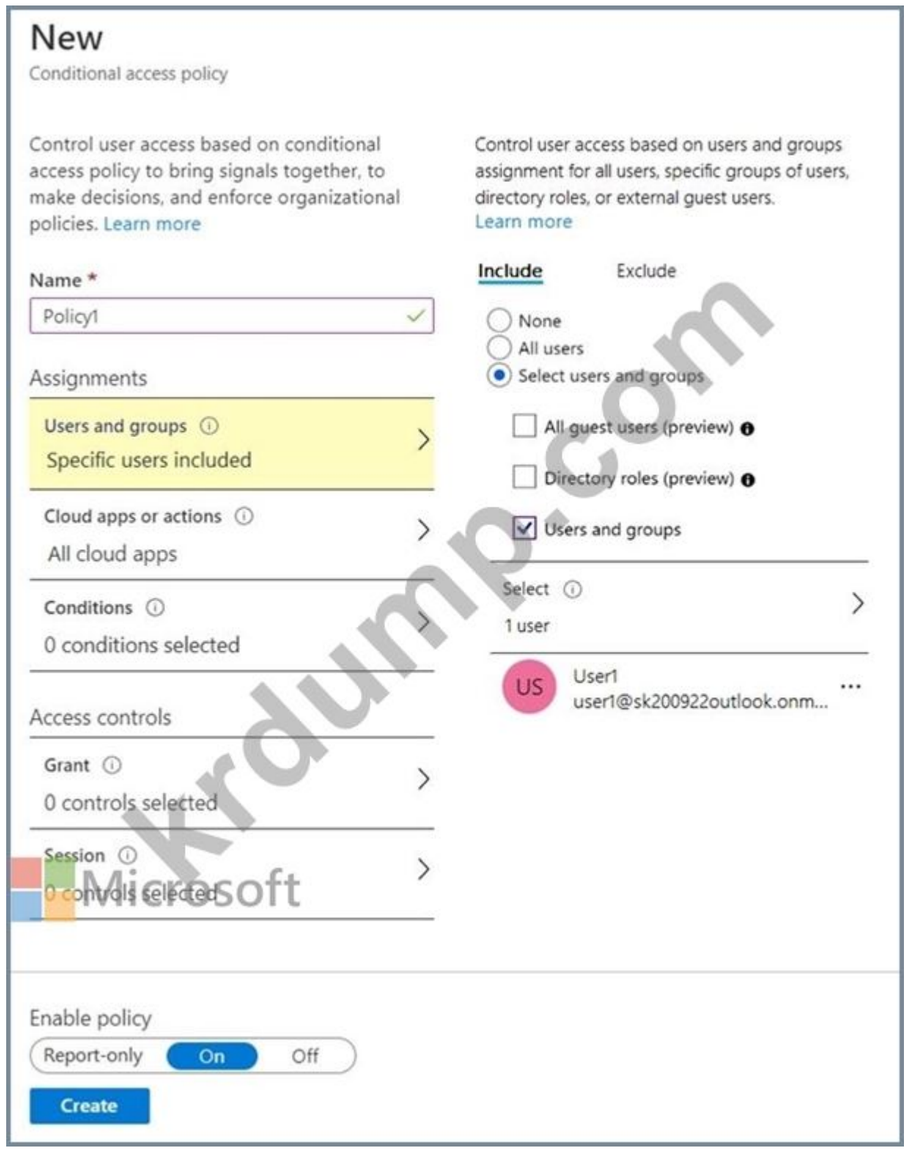
NEW QUESTION: 78
□□□ Microsoft Defender for Cloud Apps□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□ □□ □□□ □□□□□ □□ □□□□□ □□□□□ □□□□ □□□. □□, □□ □□□ □□□□□ □□□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. □□□□ □□ Defender □□□ □□□ □□□□□.
B. □□□ □□□ □□□ □□□□□.
C. Microsoft 365 Defender □□□□ Facebook□ □□ □□□ □□□□□.
D. Microsoft Intune□□ □ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 79
□□□ Microsoft Entra ID Premium □□□□□ □□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□ □□□□ □□ □□ □□(ToU)□ □□□ □□□□□.
□□□□□ □□□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. HTML
B. RTF

C. PDF □□ □□ □□□
D. DOCX
Answer: C (LEAVE A REPLY)
https://learn.microsoft.com/en-us/entra/identity/conditional-access/terms-of-use

NEW QUESTION: 80
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Microsoft Entra □□□□ □□□ Azure □□□ □□□□. □□ □□□□□ User1□□□ □□□□ □□□□.
Microsoft Entra □□ □□ □□□ □□□ □□□□□.
User1□ Azure □□□ □□ □□□ □□□ □ □□□ □□ □□□.
□□□□ □□□ □□□ □□□ □□□.
User1□□ □□ Microsoft Entra □□□ □□□□ □□□?
A. □□ □□ □□□
B. □□□ □□□
C. □□ □□□
D. □□□□□□ □□□
Answer: A (LEAVE A REPLY)
Task Least privileged role Additional roles
Tenant onboarding Permissions Management Administrator
Onboard cloud environments Permissions Management Administrator
Assign permissions in Microsoft Entra Permissions Management Permissions Management Administrator Start trial and buy Microsoft Entra Permissions Management licenses Billing Administrator
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-by-task#permissions-management

NEW QUESTION: 81
□□□ □□
Azure Active Directory(Azure AD) □□□□□ □□ □□ □□□ □□□□□□ □□□□.
□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□.


New
Conditional access policy
Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
Policy1
Assignments
Users and groups
Specific users included
Cloud apps or actions
All cloud apps
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. Learn more
Include
Exclude
None
All users
Select users and groups
All guest users (preview)
Directory roles (preview)
Users and groups
Select
1 user
US
User1
user1@sk200922outlook.onm...
Enable policy
Report-only
On
Off
Create

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

Answer Area

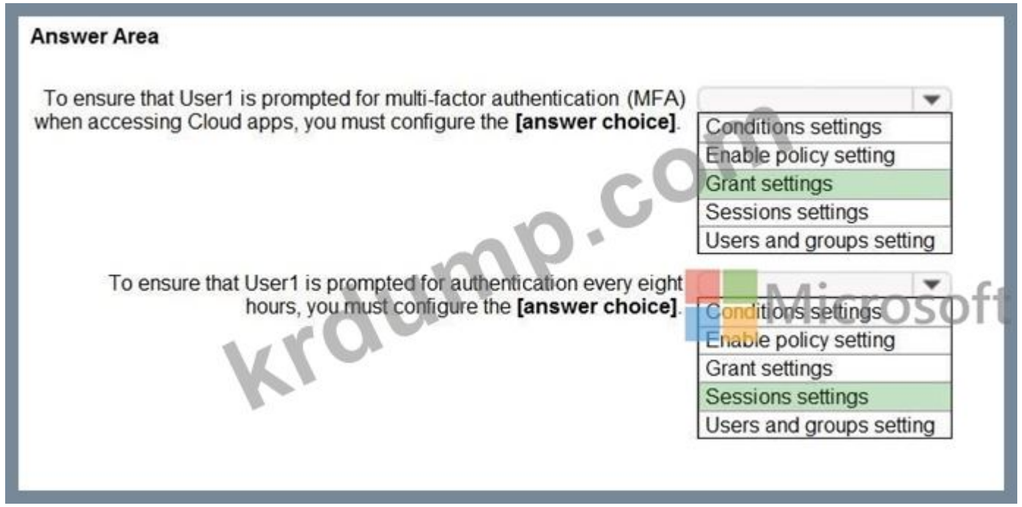
To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

To ensure that User1 is prompted for authentication every eight hours, you must configure the **[answer choice]**.

- Conditions settings
- Enable policy setting
- Grant settings
- Sessions settings
- Users and groups setting

Answer:



Explanation:

Create a Conditional Access policy

1. Under Access controls > Grant, select Grant access, Require multi-factor authentication, and select Select.
2. Confirm your settings and set Enable policy to On.
3. Select Create to create to enable your policy.

Sign-in frequency

Sign-in frequency defines the time period before a user is asked to sign in again when attempting to access a resource.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-conditions
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#sign-in-frequency

NEW QUESTION: 82
□□□ □□
RG1 □ RG2□□ □ □□ □□□ □□□ storage1□□□ □□□□ □□□ □□□ Azure □□□ □□□□.
□□ □□ □□□ □□ □□□ □□ □□□ □□□□□.

User	Role
User1	Reader
User2	Reader
User3	Reader
User4	Owner

□□ □□ □□□ □□ RG1□ □□□ □□□□□.

User	Role
User1	Reader and Data Access
User2	Contributor

□□ □□□ □□ storage1□ □□□ □□□□□.

```
1  [
2     {
3           "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
4           "Scope": "/subscriptions/7fefd66e-8694-4b54-beae-
   17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1",
5           "DisplayName": "User3",
6           "SignInName": "User3@contoso.com",
7           "RoleDefinitionName": "User Access Administrator",
8           "RoleDefinitionId": "/subscriptions/7fefd66e-8694-4b54-beae-
   17fd819d4873/providers/Microsoft/Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
9           "ObjectId": "919948b2-bc93-41a0-9562-9399576cc8f0",
10          "ObjectType": "User",
11          "RoleAssignmentDescription": "",
12          "ConditionVersion": "",
13          "Condition": ""
14    }
15 ]
```

□□ Azure □□□□□ □□□ □□□□ □□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

Box 1: Yes

User1 has the Reader role in the subscription.

The subscription includes the storage account.

User1 will have read access to the storage account.

(For RG1 User1 has the Reader and Data Access role.

User1 has no role at the storage account scope level.)

Note:

The Azure Reader role is a built-in role that grants users read-only access to view Azure resources. This means they can see information about resources, their properties, and configurations, but they cannot make any changes or modifications to those resources.

Box 2: No

User2

User2 has the Contributor role for RG1 only, but not for RG2.

User2 has the Reader role in the subscription.

User2 will not be able to create a virtual network in RG2.

Box 3: Yes

User3 has the User Access Administrator role for the storage1storage account.

The User Access Administrator role can assign roles. This role is specifically designed to manage access to Azure resources, including assigning roles to other users, groups, or service principals.

Reference:

https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

NEW QUESTION: 83

□□□ □□

□□□ contoso.com□ fabrikam.com□□□ □ □□ Microsoft Entra □□□□ □□□□ □□□□.

Contoso.com□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type
User1	Member
User2	Member
User3	Guest

Contoso.com□□ □□ □□ □□□ □□□ □□□□ □□□□.

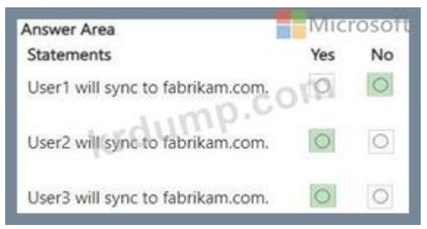
Name	Membership type	Members
Group1	Assigned	User1
Group2	Assigned	Group1, User2

contoso.com□□ fabrikam.com□□□ □□□ □ □□□□ □□□□ User3 □ Group2□ □□ □□□ □ □□□□ □□□□□□.

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer:



NEW QUESTION: 84

□□□□ □□ □□□ □□□ □□ □ □□ □□□ □□□ □□□ □□ □□□ □□□□□ □□□. Azure Identity Protection□ □□ □□□, □ □□□□ □□□ □□ □□□□□ □□□. □ □□ Identity Protection□ □□ □□ □ □ □ □□□ □□□□□, □□ □□□ □□□ □□□□ □□□□. □□ □□ □□□ □□□□ □□□. □ □□□ □□ □□ □□□ □□□□ □□□?

A. □□ □□□

B. □□□ □□□

C. □□ □□□

D. □□□□□ □□□

Answer: (SHOW ANSWER)

As this role would provide full access to Identity Protection minus the ability to reset passwords for a user.

Reference:

https://docs.microsoft.com/en-us/learn/modules/manage-azure-active-directory-identity-protection/2-review-identity-protection-basics

NEW QUESTION: 85

□□ □□ 1 - □□□ □□□□

□□

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

Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.

□□ □□. □□ □□

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

□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.

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

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□

Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.

* □□□□□□□ □□□ 365 □□□□□□ E5
* □□ □□□□ + □□
* □□□ 10 □□□□□□ E3
* □□□□ □□ 3

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

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

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

* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.

contoso.com□ □□ □□ □□□ □□□□□□ □□□□.

Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.

□□ □□. □□ □□

Contoso□ □□□ □□ □□□□ □□□□□.

* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.
* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

□□□□. □□□ □□ □□

Contoso□ □□□ □□ □□ □□□ □□□ □□□□□.

* □□ □□□ □□ □□□(SSPR)□ □□□□□.
* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.
* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□□□.
* App1□□□ □□□ □□□ □□ □□□ Azure □ □□ □□□□□. App1□ □□□□□ □□ □□□□ Azure AD □□□ □□□□ □□□□□.

* □□□ □□□ □□ □□□□ □□ Microsoft SharePoint Online □□□, □□ □ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□.
Contoso□ Adatum Corporation□□□ □□□ □□□ □□□□□. 100□□ □□□ Adatum □□□□ Adatum□□□ □□□ Active Directory □□ □□(OU)□ □□□ □□□□□. □ □□□□□ □□□ □□□□ □□□□ □□□. □□□□. □□□ □□□□
Contoso□ □□□ □□ □□ □□ □□□ □□□□□.
* □□ □□□□ AD DS□□ contoso.com Azure AD □□□□ □□□□□□ □□□.
* App1□ https://contoso.com/auth-response□ □□□□ □□□□ URI□ □□□ □□□.
* □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□.
* Fabrikam □□□□ □□□ □□□ SharePoint □□□□ □□ 90□ □□ □□ □□□ □□□ □□□.
* Azure AD□□ □□□□ □□□ □□□ □□□□□ □□□. □□ □□□ 1□ □□ □□□□ □□□.
* □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.
Log Analytics □□□□□□□ □□□□□.
□□□ □□□ □□□ □□□ □□□□ □□□.
Azure AD□□ □□□ □□□□ □□□?
A. □□ □□□
B. □□ □□
C. □□ □□□
D. □ □□
Answer: B (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/azure-monitor/logs/design-logs-deployment
https://docs.microsoft.com/en-us/security/benchmark/azure/security-control-logging-monitoring

NEW QUESTION: 86
□□ □□ □□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group3

□□ □□□□ □□ □□ □□□ □□ □□□ □□□ □ □□□□.

Method	Target	Enabled
FIDO2	Group2	Yes
Microsoft Authenticator app	Group1	Yes
SMS	Group3	Yes

□□ □□□□□ □□ □□□ □□□ □□□ □□□□□ □□□ □□□ □□□□ □□□□ □□ □□□□□□?
A. □□□ 1 □□
B. □□□2 □□
C. □□□3 □□

D. □□□1□ □□□2□ □□
E. □□□2 □ □□□3□ □□
Answer: A (LEAVE A REPLY)
Microsoft Authenticator
You can also allow your employee's phone to become a passwordless authentication method.
You may already be using the Authenticator app as a convenient multi-factor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.
The Authenticator App turns any iOS or Android phone into a strong, passwordless credential.
Users can sign in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.
FIDO2 security keys
The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.
FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign in to their resources without a username or password using an external security key or a platform key built into a device.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

NEW QUESTION: 87
□□ □□ □□□ □□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic
Group3	Microsoft 365	Assigned
Group4	Microsoft 365	Dynamic

□□□ □□ PIM(Privileged Identity Management)□ □□□□ □□□.
PIM□ □□□□ □□ □□□ □□□ □ □□□□?
A. □□1□
B. □□1□ □□2□
C. Group1□ Group3□
D. □□3□ □□4□
E. □□1. □□2. □□3. □□□ □□4
Answer: (SHOW ANSWER)
Groups in Microsoft Entra ID can be classified as either role-assignable or non-role-assignable.
Additionally, any group can be enabled or not enabled for use with Microsoft Entra Privileged Identity Management (PIM) for Groups. These are independent properties of the group. Any Microsoft Entra security group and any Microsoft 365 group (except dynamic groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. The group doesn't have to be role-assignable group to be enabled in PIM for Groups.
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/concept- pim-for-groups

NEW QUESTION: 88
Microsoft 365 □□□□ □□□□.
□□ □□□□ □□□□□ □□□ 10 □□□□ □□□ □□□□.
□□□□□ □□□□□ □□□ □□□ □□□□ □□□□□ □□ □□□□□. □□□ □□□□□ □□□ □, □□□□□ □□□□ □□□□ □□□ □ □□ □□ □□□□□ □□□□□.
□□□ □□□ □□(MFA)□ □□□ □□□□□.
□□ □□□□ □□□□ □□□ □ □□ MFA □□ □□□ □□□□□?

A. □□
B. □□□□□ Windows Hello
C. Microsoft Authenticator □□ □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
□□□ Site1□□□ □□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□ Site1□ □□ □□ □□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□ □□□ □□ □□□ □□□ □□□□ □□□□□.
□□ □□.
- 30□ □ □□□□ □□ □□□ □□□□□.
□□□ □□ □□□?
A. □□□ □□□ □□□ □□□□□.
B. □□□ □□□□ □□□□□.
C. Azure AD □□ □□ ID □□□□ □□ □□□ □□□□□.
D. Microsoft Defender for Cloud Apps □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

NEW QUESTION: 90
contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□, □□ □□□□□ Azure AD ID □□ □□□ □□□□□ □□□□.
□□□ □□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. Azure AD□□ □□□ □□□ □□□□□.
B. Azure AD □□ □□□ □□□□□.
C. □□ □□□□ □□ □□ □□□ □□ □□□(SSPR)□ □□□□□.
D. □□ □□□□ □□ □□ □□ □□(MFA)□ □□□□□.
Answer: D (LEAVE A REPLY)
To implement a sign-in risk remediation policy.
When a sign in risk policy triggers:
Azure AD MFA can be triggered, allowing to user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-risk-policies

NEW QUESTION: 91
□□□ contosri.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□□ □□□□ □□□□ □□ □□ □□ □□□□.

Name	Description
Fabrikam, Inc.	An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com
Litware, Inc.	A third-party identity provider that uses the domain names of litwareinc.com and contoso.com

□□□□ □□□ 1□ □□□□ □□ □□□ □□□ □ □□□□.
Fabrikam□ Litware□ □□□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□□.
□□□ Fabrikam □ Litware □□□□ □□□ □ □□ packaqel□□□ □□□ □□□□ □□ □□□□□.
Fabrikam □ litware□ □□□ □□□ □□□□ □□ □□□ □□ □□□□ package1□ □□□□ □□□ □□□ □□□ □ □□□□.
□□□ □□ □□□ □□ □□□ □□□□ □□□?
A. 4
B. 2
C. 1
D. 3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 92
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□□ □□ □□□(SSPR)□ □□ □□□ □□□□ □□□□□.
- □□□ □ □□□ □□ □□: □
- □□□□ □□□ □□ □: 1
□□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□ □ □□
B. □□ □□ □□□ □□□ □□□
C. □□□□□
D. Windows Hello PIN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 93
□□□□ Microsoft 365 E3 □□□□□ □□□ □□□□ 2,500□ □□□□. □□□□□ □□ □□□□□ □□□□□.
Microsoft 365 E5 □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□ □□ □□□□ □□□□□□ Microsoft 365 E3 □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Update-MgGroup cmdlet
B. Set-WindowsProductKey cmdlet
C. Set-MgUserLicense cmdlet
D. Microsoft Entra □□ □□□ □□□□ □□□□
Answer: D (LEAVE A REPLY)
The Licenses blade in the Microsoft Entra admin center lets you manage and remove direct (per- user) license assignments in bulk with minimal effort, which is the quickest way to strip the individually assigned Microsoft 365 E3 licenses after moving users to group-based E5 licensing.

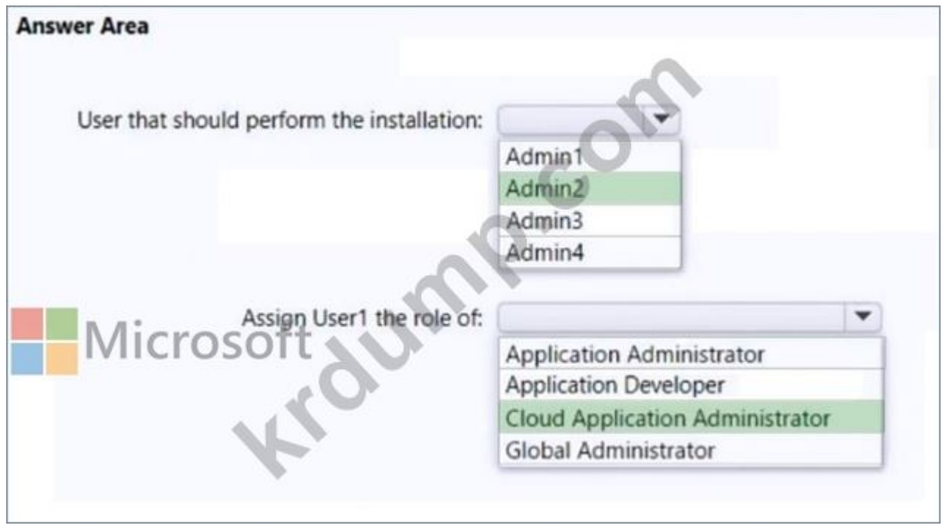
NEW QUESTION: 94
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□ □□□□ □□□.
□□ □□ □□ □□□ □□□ □□□□ □□□□□?
A. □□□□ □□□□
B. Microsoft Entra □□ □□□□□
C. □□□□ □□ □□□ □□
D. □□ IP □□
Answer: (SHOW ANSWER)

NEW QUESTION: 95
□□□ □□
□□□ □□ □□ □□□ □□□□ □□□ □□□□□ Microsoft 365 □□□ □□□□ □□□□.

Name	Role
Admin1	Global Administrator
Admin2	Application Administrator
Admin3	Cloud Application Administrator
Admin4	Application Developer
User1	None

App1□□□ □□□ □□□□□ □□ □□□ □□□□□. App1□ Azure AD□ □□□□ Azure AD □□□□□□ □□□□ □□□ □□□□.
□□□□□□ □□□ □□□ □□□ □□□□ User1□ Azure AD□ App1□ □□□ □ □□□ □□ □□□.□ □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□□□ □□□ □□□□ □□, User1□□ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer:



NEW QUESTION: 96

□□□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

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

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

Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 □□: =1122334455667788

Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□□□ □□□□: 99999999

sg-Executive □□□□ □□ □□ □□□□ □□ □□□□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □ □□□ □□□□ □□□.

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

- □ □□ □□□ □□□ □□□□□ □□ □□□□ □□□□□.

□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□.

Answer:

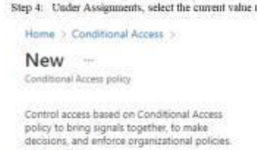
Part 1: First, create a Conditional Access policy and assign your test group of users as follows:

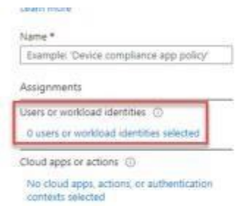
Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access, select + New policy, and then select Create new policy.

Step 3: Enter a name for the policy, such as MFA Pilot.

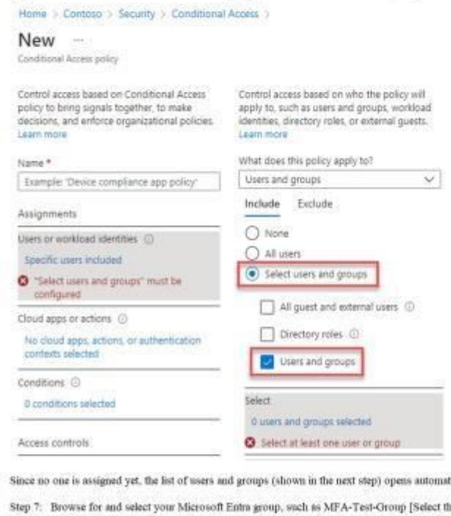
Step 4: Under Assignments, select the current value under Users or workload identities.





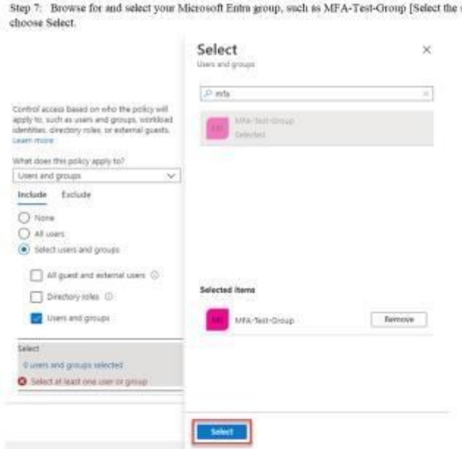
Step 5: Under What does this policy apply to?, verify that Users and groups is selected.

Step 6: Under Include, choose Select users and groups, and then select Users and groups.



Since no one is assigned yet, the list of users and groups (shown in the next step) opens automatically.

Step 7: Browse for and select your Microsoft Entra group, such as MFA-Test-Group [Select the sg-Executive group], then choose Select.



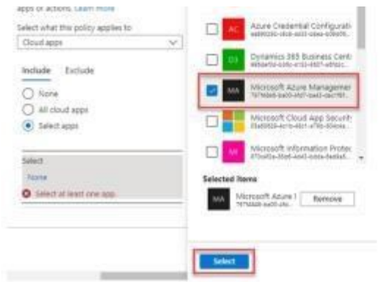
Part 2: Select applications
Configure the apps which require the conditions

Step 8: Select the current value under Cloud apps or actions, and then under Select what this policy applies to, verify that Cloud apps is selected.

Step 9: Under Include, choose Select apps.

Since no apps are yet selected, the list of apps (shown in the next step) opens automatically.

Step 10: Browse the list of available sign-in events that can be used. Then choose Select.
Choose Select apps and select the link under Select.



Step 11: On the Select page, choose Windows Azure Service Management API, and then choose Select.

Part 3: Select Conditions
Question:
The members must meet one of the following conditions:
Connect by using a device that is marked as compliant by Microsoft Intune.
Connect by using client apps that are protected by app protection policies.

Step 12: Select Conditions > Client apps to apply the policy to apps and browsers. Select Yes, and then select the checkboxes for enable Browser and Mobile apps and desktop clients.

Step 13: Under Access controls, select Grant to apply Conditional Access based on a device compliance status. Select Grant access > Intune compliant Device, and Require app protection policy, then select Require one of the selected controls.

Step 14: For Enable policy, select On, and then select Create to save your changes. By default, Enable policy is set to Report-only.

Reference:
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa
https://learn.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune-create

NEW QUESTION: 97
Active Directory □□□□ □□□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□ VPN □□□ □□□□ □□□□. VPN □□□ Azure Multi-Factor Authentication(MFA)□ □□□□ □□□□.
VPN □□□ □□ Azure MFA□ □□□□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Azure AD □□□□□□ □□□
B. Azure AD □□ □□ □□□
C. □□□□ □□ □□(NPS)
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
NPS (Network Policy and Access Service) is like a middle man between the VPN client and Azure MFA. The NPS role is installed on a domain-joined server or the domain controller and is configured to authenticate and authorize RADIUS requests from the VPN client.
The VPN should be configured to use RADIUS authentication and point to the NPS server.
The MFA NPS extension is installed anywhere but the VPN server. When a user/VPN client attempts to authenticate, it sends a RADIUS request to the NPS server through the VPN which performs the primary authentication and then triggers the NPS Extension for secondary authentication.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension-vpn

NEW QUESTION: 98
□□□ □□
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.

Name	Type
User1	Member
User2	Guest
User3	Member

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

Name	Membership type	Role assignment allowed	Members
Group1	Assigned	Yes	User1, User2
Group2	Assigned	No	User1, User3
Group3	Dynamic user	No	User2, User3

□□□ □□ □□□□ Access1□□□ □□□ □□□ □□□ □□□□□.

- □□□ □□□ □□□□□: □ + □□
- □□ □□: □□□ □□□□ □□ □□ Microsoft □□
- □□ □□: □□□ □□□□ □□
- □□□ □□: □□□□ □□□ □□ □□□ □□ □□□□□.

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

Answer Area

Statements	Yes	No
User1 can review their membership in Group1 by using Access 1.	○	○
User2 can review their membership in Group3 by using Access1.	○	○
User3 can review their membership in Group2 by using Access1.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can review their membership in Group1 by using Access 1.	○	○
User2 can review their membership in Group3 by using Access1.	○	○
User3 can review their membership in Group2 by using Access1.	○	○

Explanation:

Box 1: No

Group1 is a role-assignable group.

Role-assignable groups are not included with the 'All Microsoft 365 groups with guest users' selected.

Note: Review Scope

Option All Microsoft 365 groups with guest users:

Select this option if you want to create recurring reviews on all your guest users across all your Microsoft Teams and Microsoft 365 groups in your organization. Dynamic groups and role- assignable groups aren't included. You can also choose to exclude individual groups by selecting Select group(s) to exclude.

Box 2: No

Group3 is a dynamic group.

Dynamic groups are not included with the 'All Microsoft 365 groups with guest users' selected.

Box 3: No

Scope is guest users only

User3 is not a guest user.

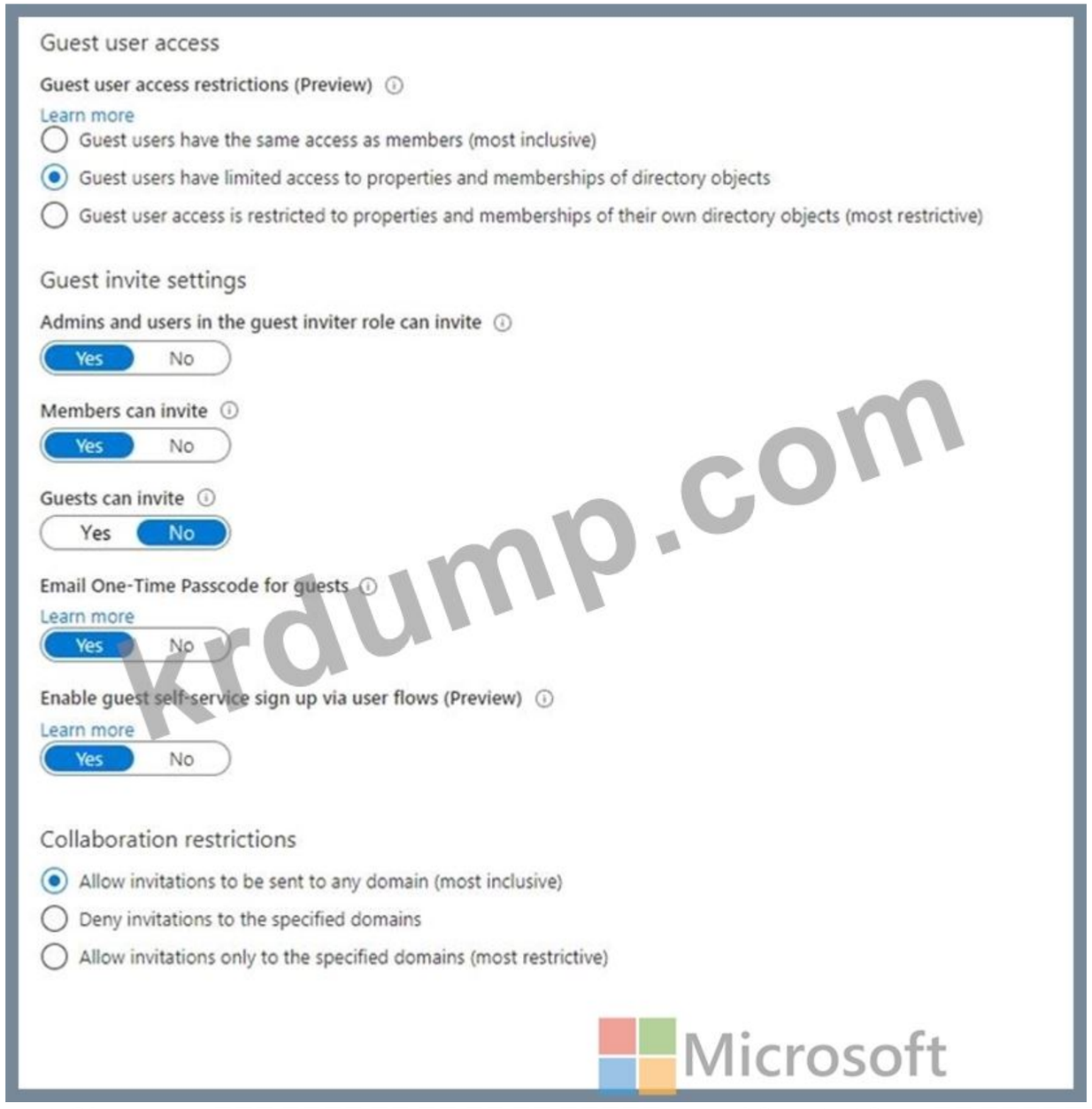
Note 2: Scope: Guest users only
Access Review scope Guest users only
Scope for the review.
*-> Guest users only: This option limits the access review to only the Microsoft Entra B2B guest users in your directory.
* Everyone: This option scopes the access review to all user objects associated with the resource.
Reference:
https://learn.microsoft.com/en-us/entra/id-governance/create-access-review

NEW QUESTION: 99
contoso.com□ fabrikam.com□□□ □ □□ Microsoft Entra □□□□ □□□□. contoso.com□□ □□ □□ □□□ ID□ □□□□ □□□□.

Name	Type
User1	User
Group1	Security group
Group2	Microsoft 365 group

contoso.com□□ fabrikam.com□□□ □□□ □ □□□□ □□□□□.
fabrikam.com□ □□□□ □□□ □□□□□?
A. □□□ 1 □□
B. User1 □ Group1□ □□
C. □□□ 1 □ □□ 2 □□
D. □□□1, □□1, □□2
Answer: A (LEAVE A REPLY)
In Microsoft Entra cross-tenant synchronization, only user objects are supported for synchronization across tenants. Groups (including security groups and Microsoft 365 groups) are not synchronized between tenants.
Given this limitation:
User1, being a user object, can be synchronized from contoso.com to fabrikam.com.
Group1 (Security group) and Group2 (Microsoft 365 group) cannot be synchronized as groups are not supported for cross-tenant sync.

NEW QUESTION: 100
fabrikam.com□□□ □□□□ □□□□ Microsoft 365 □□□□ □□□□. Azure Active Directory(Azure AD)□ □□□ □□ □□□ □□□ □□□ □□ □□□□□. (□□ □□ □□□□□.)



bsmith@fabrikam.com□□□ □□□□ □□ □□ □□ □□ □□□□□ Microsoft SharePoint Online □□ □□□□□□ □□□□□.

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

□□ □□□□□ □□□□ □□□ □□□□□?
A. User2□
B. User1□
C. User1□ User2□
D. User1, User2, User3
Answer: (SHOW ANSWER)
When the email one-time passcode feature is enabled, newly invited users who meet certain conditions will use one-time passcode authentication. Guest users who redeemed an invitation before email one-time passcode was enabled will continue to use their same authentication method.
User 1 is already a registered guest user in fabrikan.com so will not receive additional OTP.
User 2 has never accessed fabrikam.com so WILL receive OTP each time they login.
User 3 (providing email addy is not a typo) will not receive a OTP as they are a domain user.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode#when-does-a-guest-user-get-a-one-time-passcode

NEW QUESTION: 101
□□□ Microsoft Entra □□□□ □□□□ □□□□.
ID □□□ □□□□□□□ Microsoft Entra □□ □□□ □□□□ □□□.
□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□?
A. □□□□ □□□□ □□
B. □□□ □□□□□ □□
C. □□□ □□□ □□□□
D. □□ □□ □□ □□□□ □□□
Answer: (SHOW ANSWER)
Microsoft Entra workbooks use data stored in a Log Analytics workspace, so the diagnostic logs must be sent to Log Analytics to enable workbook queries and visualizations.

NEW QUESTION: 102
□□□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com
Microsoft 365 □□: =1122334455667788
Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 99999999
sg-Operations □□□ □□□□ □ □ □□□ □□□□ □, □□ □□□□□□□ □□□ '□□' □□ □□□□□ □□ □□□.
- □□□□
- □□
□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□.
Answer:

Access and session controls in Microsoft Defender for Cloud Apps work with applications from the Cloud app catalog and with custom applications.

Configure the Microsoft Entra ID integration
Use the following steps to create a Microsoft Entra Conditional Access policy that routes app sessions to Defender for Cloud Apps.
Step 1: In Microsoft Entra ID, browse to Security > Conditional Access.

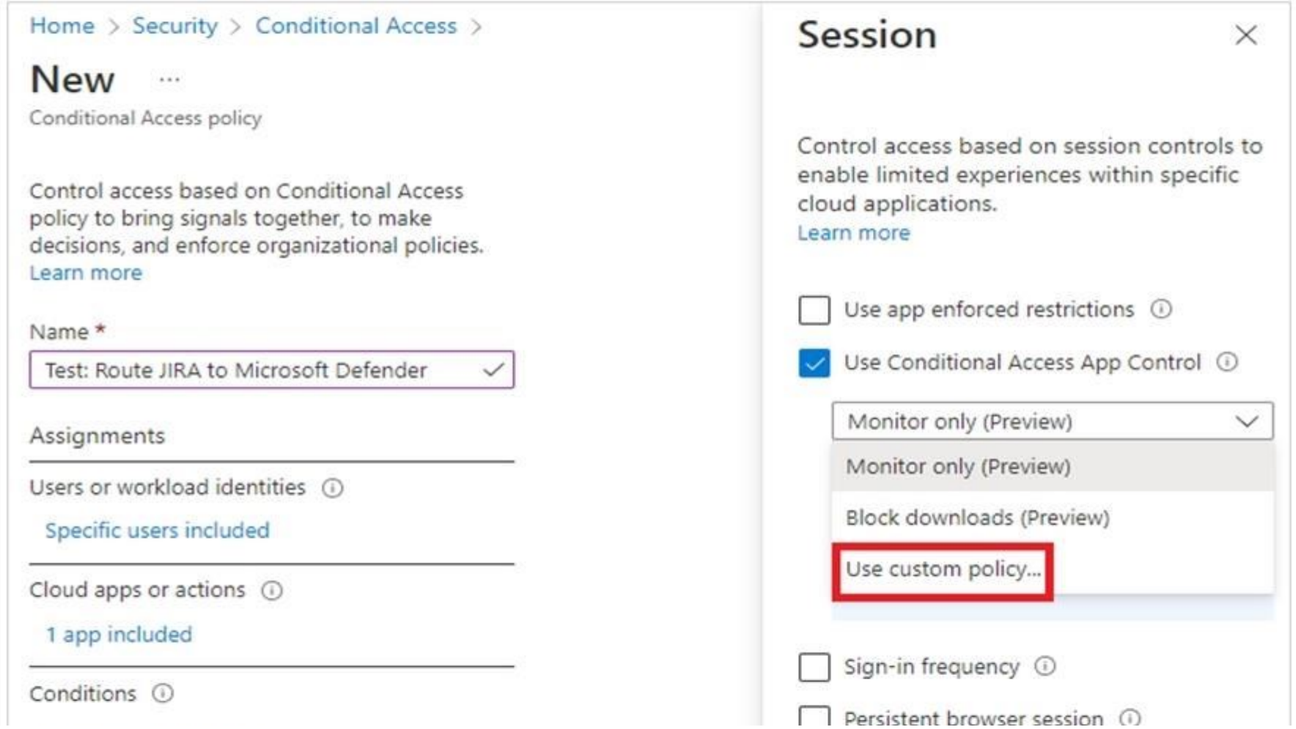
Step 2: On the Conditional Access pane, in the toolbar at the top, select New policy -> Create new policy.

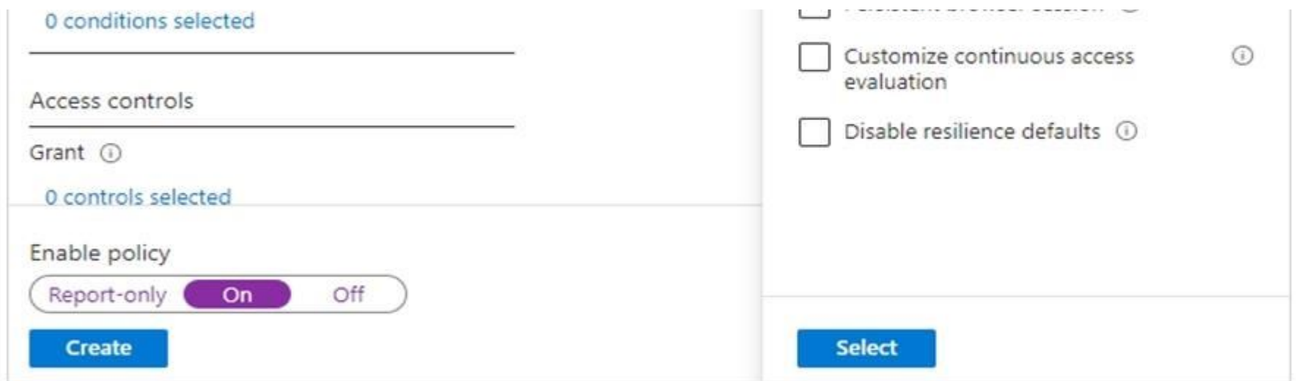
Step 3: On the New pane, in the Name textbox, enter the policy name.

Step 4: Under Assignments, select Users or workload identities and assign the users and groups that will be onboarding (initial sign-on and verification) the app. [Select the sg-Operations group]

Step 5: Under Assignments, select Cloud apps or actions and assign the apps and actions you want to control with conditional access app control. [Select the My Apps portal app]

Step 6: Under Access controls, select Session, select Use Conditional Access App Control, and choose a built-in policy (Monitor only (Preview) or Block downloads (Preview)) or Use custom policy to set an advanced policy in Defender for Cloud Apps, and then select Select. [Select Use custom policy]





Step 7: Add conditions and grant controls as required.

Step 7a: Configure the Custom policy so that it satisfies the question (Details omitted)
Question: A tab named Operations appears that contains only the following applications: LinkedIn, Box

Step 8: Set Enable policy to On and then select Create.

Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies

NEW QUESTION: 103
□□ □□ 1 - □□□ □□□□
□□
□□□ □□□□□ □□□□□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
□□ □□. □□ □□
Contoso□ □□□□□ □□□□□□ contoso.com□□□ Active Directory □□□□ □□□□.
□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.
contoso.com Active Directory □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□
Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.
* □□□□□□□ □□□ 365 □□□□□□ E5

* □□ □□□□ + □□
* □□□ 10 □□□□□□ E3
* □□□□ □□ 3

Azure AD Connect□ Azure AD□ Active Directory □□□ □□□(AD DS) □□ □□□□□. Contoso_Resources OU□ □□□□□□.

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

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

* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.

contoso.com□ □□ □□ □□□ □□□□□□ □□□□.

Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.

□□ □□. □□ □□

Contoso□ □□□ □□ □□□□ □□□□□.

* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.
* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

□□□□. □□□ □□ □□

* □□ □□□ □□ □□□(SSPR)□ □□□□□.

Contoso□ □□□□ □□ □□ □□□ □□□□ □□□□□.

* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.
* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□□□.
* App1□□□ □□□ □□□ □□ □□□ Azure □ □□ □□□□□. App1□ □□□□□ □□ □□□□ Azure AD □□□ □□□□ □□□□□.
* □□□ □□□ □□ □□□□ □□ Microsoft SharePoint Online □□□, □□ □ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□.

Contoso□ Adatum Corporation□□□ □□□ □□□ □□□□□. 100□□ □□□ Adatum □□□□ Adatum□□□ □□□ Active Directory □□ □□(OU)□ □□□ □□□□□. □ □□□□□ □□□ □□□□ □□□□ □□□.

□□□□. □□□ □□□□

Contoso□ □□□ □□ □□ □□ □□□ □□□□□.

* □□ □□□□ AD DS□□ contoso.com Azure AD □□□□ □□□□□□ □□□.
* App1□ https://contoso.com/auth-response□ □□□□ □□□□ URI□ □□□ □□□.
* □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□.
* Fabrikam □□□□ □□□ □□□ SharePoint □□□□ □□ 90□ □□ □□ □□□ □□□ □□□.
* Azure AD□□ □□□□ □□□ □□□ □□□□□ □□□. □□ □□□ 1□ □□ □□□□ □□□.
* □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.

□□

□□□ □□□ □□ □□□ □□□□ □□□.

Microsoft Entra □□□□ □□ □□ □□□ □□ □□□?

A. □□ □□

B. □□□ □□ □□

C. □□□ □□

D. □□ □□ □□

Answer: A (LEAVE A REPLY)

Issue: Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.

Configure device settings

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD. If users reach this limit, they can't add more devices until one or more of the existing devices are removed. The default value is 50. You can increase the value up to 100. If you enter a value above 100, Azure AD will set it to 100. You can also use Unlimited to enforce no limit other than existing quota limits.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

NEW QUESTION: 104

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

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

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

□□ Azure AD □□□ □□□ □□□ □□□□ 100□ □□□ □□□ □□□ □□ □□□.

□□ □□ □□□ □□ □□□□ □□□ □□□ □□ □□□.

□□ □□: Azure AD□□ □□ □□□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: B (LEAVE A REPLY)

Need to go to Azure monitor to modify action group not diagnostic settings.

NEW QUESTION: 105

□□□ □□

□□□ Microsoft Entra ID□ □□□□ Microsoft 365 □□□□ □□ □□□ □ □□□ □□□□ □□□□□.

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

Default user role permissions

Learn more

Users can register applications — No

Restrict non-admin users from creating tenants — Yes

Users can create security groups — No

Guest user access

Learn more

Guest user access restrictions

- Guest users have the same access as members (most inclusive)
- Guest users have limited access to properties and memberships of directory objects
- Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Administration center

Learn more

Restrict access to Microsoft Entra admin center — No

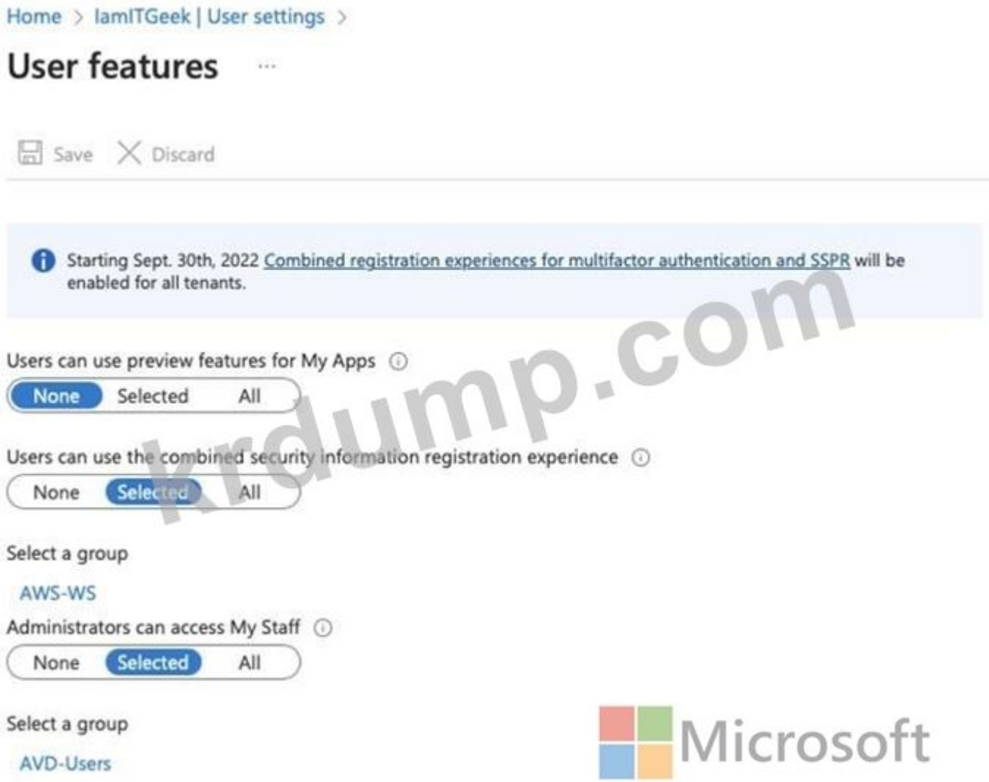
LinkedIn account connections

Learn more

Allow users to connect their work or school account with LinkedIn *

- Yes
- Selected group
- No

Allow users to connect their work or school account with LinkedIn * AWS-WS Edit



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

Username	Group Association	Requirements
User-GU-A	None	• Requires same access as UserC
UserA	AVD-Users, AWS-WS	• Should not be able to access preview features for My Apps • Needs to access LinkedIn with Microsoft Entra ID account
UserB	AVD Users	• Requires access to My Staff • Needs to be able to use the combined security information registration experience
UserC	AWS-WS	• Needs to access LinkedIn with the Microsoft Entra ID account
UserD	AVD-Users	• Should not be able to access preview features for My Apps • Needs to access LinkedIn with the Microsoft Entra ID account

□□ □□□□ □□□ □□ □□□□□□.
- □□□ GU-A(□□□ □□□)□ □□ □□ □□□ □□□ □□□□□□.
UserC□ □□□ □□ □□□ □□□□.
- □□□B□ □□ □□ □□□ □□□ □ □□□ □□□□□□.
□□ □□.
- UserD□ Microsoft □□□□ LinkedIn□ □□□ □ □□□ □□□□□□.
□□□ ID □□.
□□□□ □□ □□□ □□□□□ Microsoft Entra□□ □□□ □□□ □□□□□□ □□□. □□ □ □□□ □□ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	○	○
You need to add UserB to the AWS-WS group to allow them access to My Staff.	○	○
Only UserA and UserD can access the Combined Security Information Registration Experience.	○	○

Answer:

Statement	Yes	No
You should change Guest User access to be more inclusive to allow User-GU-A to have the same access as UserC.	○	○
You need to add UserB to the AWS-WS group to allow them access to My Staff.	○	○
Only UserA and UserD can access the Combined Security Information Registration Experience.	○	○

Explanation:
You should change Guest user access to be more inclusive to allow User-GU-A to have the same access as UserC. With the current configuration of the User Settings and User Features, as shown in the three exhibits, Guest user access is set to limit access to properties and memberships of directory objects. To allow User-GU-A to have the same access as UserC, this setting would need to change to the most inclusive setting, which is Guest users have the same access as members.
You do not need to add UserB to the AWS-WS group to allow them access to My Staff. With the current configuration of the User Settings and User Features, as shown in the three exhibits, we can see that only the AVD-Users group have been added to the setting Administrator can access My Staff option. As UserB is already a member of this group, they already have the access they need to access My Staff, and you do not need to add them to the AWS-WS group.
Not only UserA and UserD can access the Combined Security Information Registration Experience. With the current configuration of the User Settings and User Features, as shown in the three exhibit images, we can see that the AVD-Users group is selected under the Users can use the combined security information registration experience setting. In this scenario, UserA, UserB, and UserD are all in the AVD-User group.

NEW QUESTION: 106

□□□ □□

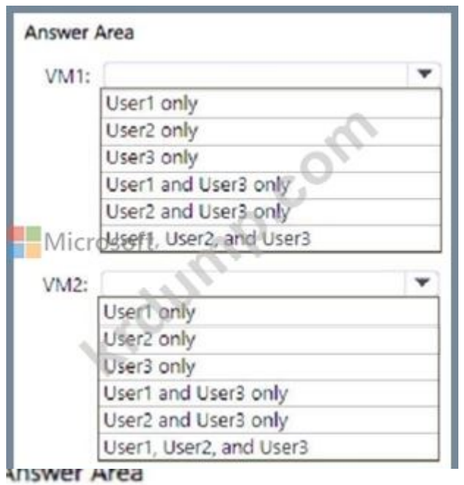
Azure □□□ RG1□□□ □□□ □□□ □□□□. RG1□□ Microsoft Entra ID □□□□ □□□□ VM1 □ VM2□□ □ □□ □□ □□□ □□□□.

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Role	Role scope
User1	Virtual Machine User Login	Subscription
User2	Virtual Machine Contributor	RG1
User3	Virtual Machine Administrator Login	VM1

VM1□□ □□ □□□□ □□□□ □ □□, VM2□□ □□ □□□□ □□□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer Area

VM1:

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

VM2:

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

NEW QUESTION: 107
□□□□ Microsoft Office 365 Enterprise E3 □□□□□ □□□ □□□□ 2,500□ □□□□. □□□□□ □□ □□□□□ □□□□□.
Microsoft Entra □□ □□□ □□ □□□□□□ □□ □□□□ □□□ □□□ Microsoft Office 365 Enterprise E5 □□□□□ □□□ □ □□□□.
□□□□ □□ □□□□ □□□□□□ Office 365 Enterprise E3 □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Entra □□ □□□ □□□□ □□□□
B. Microsoft Entra □□ □□□ □□ □□ □□□□
C. Microsoft Entra □□ □□□ ID □□□□ □□□□
D. Update-MgUser cmdlet
Answer: A (LEAVE A REPLY)
To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the "Licenses" blade in the Microsoft Entra admin center. This allows you to manage license assignments at a group level, making it easier to apply and remove licenses for multiple users simultaneously.

NEW QUESTION: 108
Azure AD □□□□ □□□□.
□□□ □□ □□□ 10□□ □□□□ □□ □□□□ □□□ □□ □□□ □□□□ □□□.
Azure AD □□ □□□□ □□□ □□□□ □□□?
A. □□ □□
B. □□□□ □□
C. □□□ □□ □□
D. □□□ □□ □□
Answer: B (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

NEW QUESTION: 109
□□□ Microsoft 365 □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

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

□□□□□ □□□ □□ □□ □□□ □□□□□.
□□ □□□ □□□ □□ □□□□ □□□□□?
A. □□□2 □□
B. User3 □□
C. □□□2 □ □□□3 □□
D. □□□3 □ □□□4□ □□

E. User1, User2, User3□ □□
F. □□□1, □□□2, □□□3, □□□4
Answer: D (LEAVE A REPLY)
Naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator.
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy#roles-and-permissions.

NEW QUESTION: 110
Microsoft 365 E5 □□□ User1□□□ □□□□ □□□□. User1□ □□ □□□□ □□□ □□□ □□□ □□□ □□□□.
User1□ □□□□□□ □□□□ □ □□□ □□□ □□□□ □□□.
User1□ □□ □□□ □□□□□□ □□□ □□□□ □□□?
A. Azure Active Directory □□ □□
B. Microsoft 365 Defender □□
C. Microsoft Defender for Cloud Apps □□
D. Microsoft 365 □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
□□□ □□
Microsoft Entra ID P2 □□□□ □□□, □ □□□□□ User1, User2, User3, User4□□ □□□ □□□□ □ □ □□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Owner	Members
Group1	User2	User1, User3, User4
Group2	User2	User2

Group2□ □□ □□ □□□ ID □□(PIM) □□□□ □□□□□□□.
□□2□ □□ □□ □□□ □□□ □□□□□.

Member	Role	Assignment type
User1	Member	Eligible
Group1	Member	Eligible
User4	Owner	Active

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Statements	Yes	No
User2 can request to become a member of Group1 by using PIM.	○	○
User3 can request to become a member of Group2 by using PIM.	○	○
User4 can request to become a member of Group2 by using PIM.	○	○

Answer:

NEW QUESTION: 112
□□□ Microsoft 365 E5 □□□ Azure □□□ □□□□ □□□□.
Azure Monitor□ □□□□ Microsoft Entra □□□ □□□ □□□ □□□□□.
Microsoft Entra□ □□ □□ □□□ □□□□ □□□.
□□□ □□□ □□□ □□□ □□□ □□□□ □□□?
A. Azure □□□ □□
B. Azure SQL □□□□□□
C. □□ □□ □□ □□
D. Azure Storage □□
Answer: C (LEAVE A REPLY)
Integrate Microsoft Entra logs with Azure Monitor logs
A Log Analytics workspace allows you to collect data based on a variety or requirements, such as geographic location of the data, subscription boundaries, or access to resources.
Note: Use the integration of Microsoft Entra activity logs and Azure Monitor to perform the following tasks:
*-> Compare your Microsoft Entra sign-in logs against security logs published by Microsoft Defender for Cloud.
* Troubleshoot performance bottlenecks on your application's sign-in page by correlating application performance data from Azure Application Insights.
* Analyze the Identity Protection risky users and risk detections logs to detect threats in your environment.
* Identify sign-ins from applications still using the Active Directory Authentication Library (ADAL) for authentication.
Reference:
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-integrate-activity-logs-with-azure-monitor-logs

NEW QUESTION: 113
□□ □□ □□□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Type	Directly assigned license
User1	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

□□ □□□ Group3□ □□□ □□□ □ □□□?
A. User2□ Group2□
B. User2, Group1, Group2□
C. User1, User2, Group1 □ Group2

D. User1□ User2□
E. User2□
Answer: (SHOW ANSWER)
In the M365 admin center, only users can be added to the mail-enabled security group.
You can only add licensed users to the group, unlicensed users won't even show up on the member select page.
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

NEW QUESTION: 114
□□ □□ 1 - □□□ □□□□
□□
□□□ □□□□□ □□□□□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
□□ □□. □□ □□
Contoso□ □□□□□ □□□□□□ contoso.com□□□ Active Directory □□□□ □□□□.
□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.
contoso.com Active Directory □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□
Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.
* □□□□□□□ □□□ 365 □□□□□□ E5
* □□ □□□□ + □□
* □□□ 10 □□□□□□ E3
* □□□□ □□ 3
Azure AD Connect□ Azure AD□ Active Directory □□□ □□□(AD DS) □□ □□□□□. Contoso_Resources OU□ □□□□□□.
□□□□□ □□□□ □□□ □□□ □□□□ □□ Microsoft 365 □□ □□□ □□□□□ □□□□□.
□□ □□□ □□□□ Microsoft 365 □□ □□□ □□□□ □□□□ □□□□□ □□□□□. □□ □□ □□□ □□□□ □□ □□□□□ □□ □□□□□ □□□□ □□□□.
* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.
contoso.com□ □□ □□ □□□ □□□□□□ □□□□.
Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.
□□ □□. □□ □□
Contoso□ □□□ □□ □□□□ □□□□□.
* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.

* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

□□□□. □□□ □□ □□

Contoso□ □□□ □□ □□ □□□ □□□ □□□□□.
* □□ □□□ □□ □□□(SSPR)□ □□□□□.
* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.
* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□□□.
* App1□□□ □□□ □□□ □□ □□□ Azure □ □□ □□□□□. App1□ □□□□□ □□ □□□□ Azure AD □□□ □□□□ □□□□□.
* □□□ □□□ □□ □□□□ □□ Microsoft SharePoint Online □□□, □□ □ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□.

Contoso□ Adatum Corporation□□□ □□□ □□□ □□□□□. 100□□ □□□ Adatum □□□□ Adatum□□□ □□□ Active Directory □□ □□(OU)□ □□□ □□□□□. □ □□□□□ □□□ □□□□ □□□□ □□□.

□□□□. □□□ □□□□

Contoso□ □□□ □□ □□ □□ □□□ □□□□□.
* □□ □□□□ AD DS□□ contoso.com Azure AD □□□□ □□□□□□ □□□.
* App1□ https://contoso.com/auth-response□ □□□□ □□□□ URI□ □□□ □□□.
* □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□.
* Fabrikam □□□□ □□□ □□□ SharePoint □□□□ □□ 90□ □□ □□ □□□ □□□ □□□.
* Azure AD□□ □□□□ □□□ □□□ □□□□□ □□□. □□ □□□ 1□ □□ □□□□ □□□.
* □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.

□□

ADatum□□ □□ □□□□□ □□□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

□□ □□□ □□□ □□□□ □□□?

A. □□ □□□ □□ □□

B. OU

C. □□ □□

D. □□ □□

Answer: A (LEAVE A REPLY)

Prompt states "License allocation for new users must be assigned automatically based on the location of the user." This would indicate a Dynamic Group with the Attribute of location to determine a License.

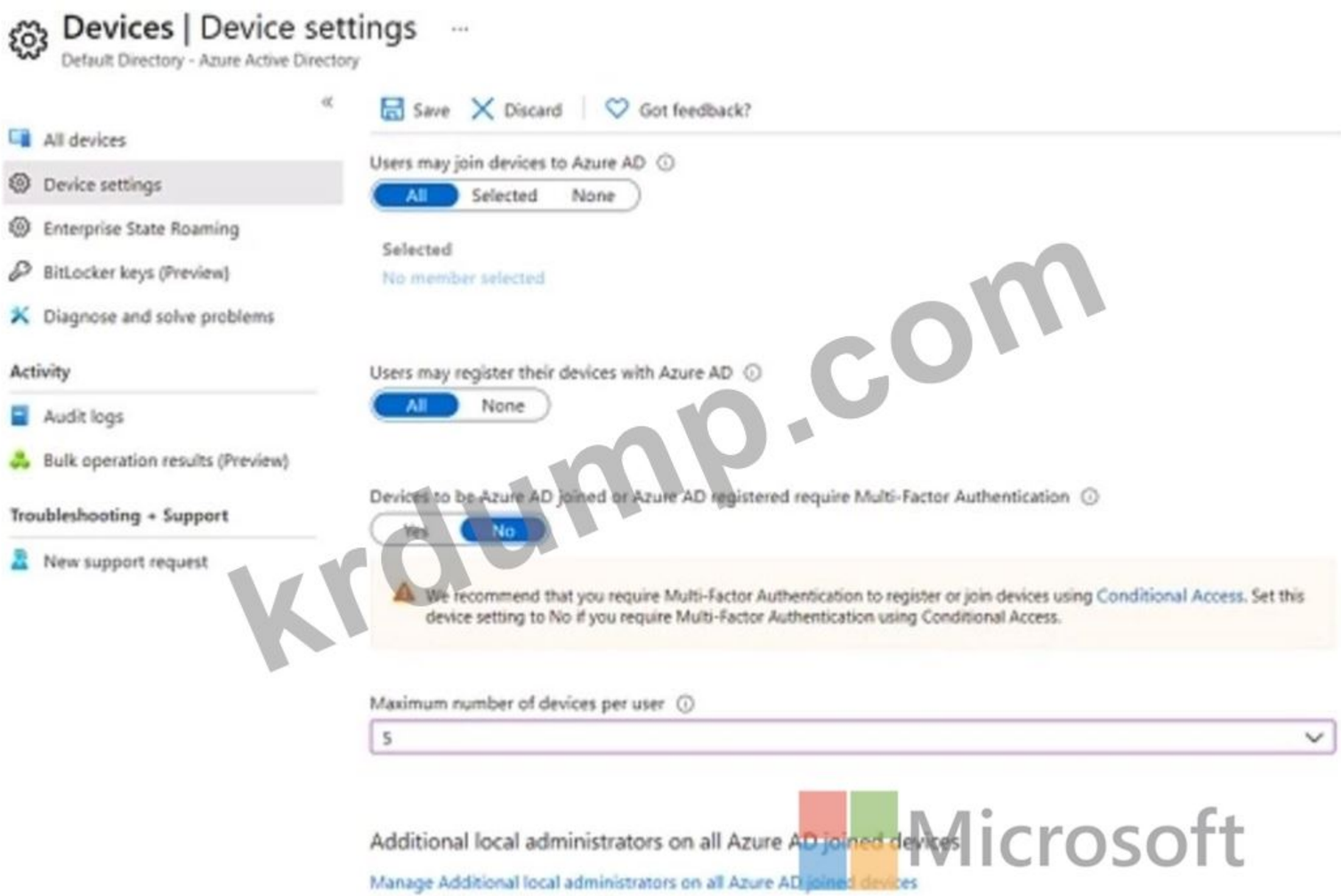
NEW QUESTION: 115

□□□ □□

Microsoft Entra ID P2 □□□ □□□ □□ Microsoft Entra □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Role
Admin1	Cloud Device Administrator
Admin2	Microsoft Entra Joined Device Local Administrator
User1	*None*

□□ □□□ □□ □□ □□□ □□□□□.



User1□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Operating system	Device identity
Device1	Windows 10	Microsoft Entra joined
Device2	iOS	Microsoft Entra registered
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	○
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	●
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	●	○
Admin2 is a local administrator on Device3.	○	●

NEW QUESTION: 116

□□□ □□

Azure □□□ □□□□ □□□□.

Role1□ Role2□□ □□□ □□□ □□ □□□ □ □ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

- □□ 1□ □□□ □□□□ Azure Container Apps □□□□□ □□□□□ □□□ □ □□□□.
- □□ 2□ □□□ □□□□ □□□ □□□□ □□ □□□ □□□ □ □□□□.

□□.

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

□□: □□ □□□ 1□□□□.

Answer Area

Role1:

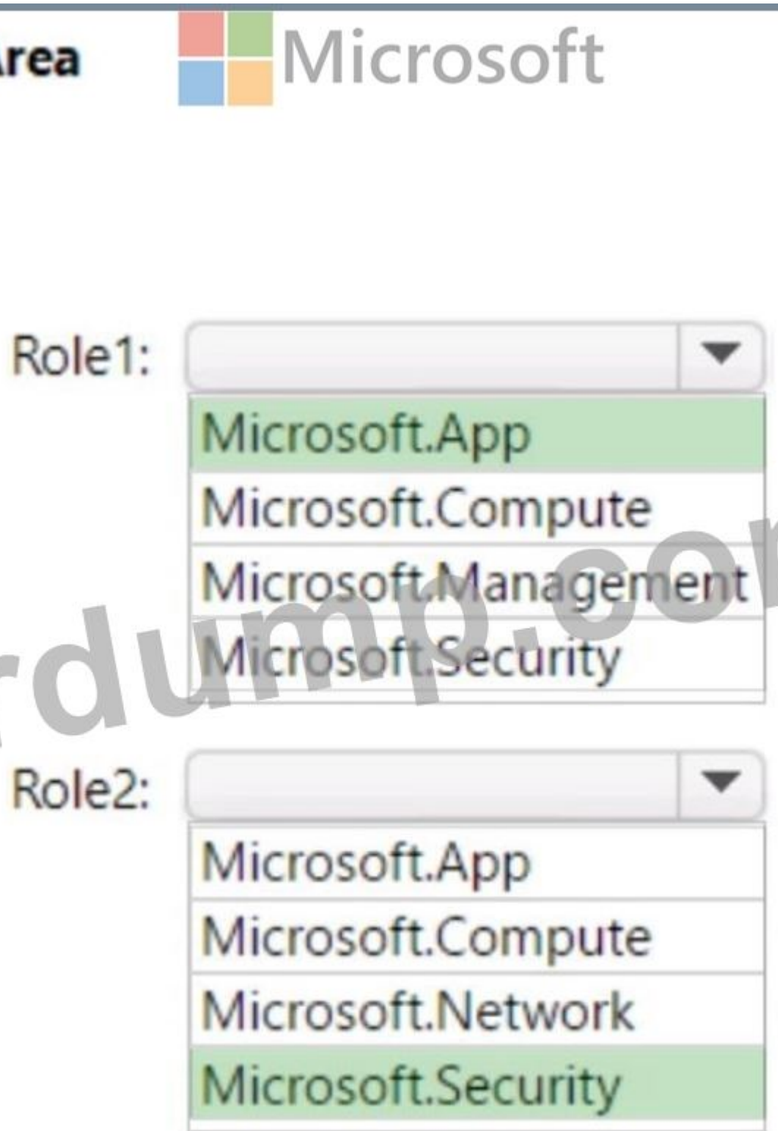
- Microsoft.App
- Microsoft.Compute
- Microsoft.Management
- Microsoft.Security

Role2:

- Microsoft.App
- Microsoft.Compute
- Microsoft.Network
- Microsoft.Security

Answer:

Answer Area



Explanation:

Role1: Microsoft.App

https://learn.microsoft.com/en-us/azure/container-apps/quickstart-portal#prerequisites Role2: Microsoft.Security

https://learn.microsoft.com/en-ie/rest/api/defenderforcloud/adaptive-network-hardenings/enforce?tabs=HTTP

NEW QUESTION: 117

□□□ □□

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

Name	Type	Role
User1	User	Helpdesk Administrator
User2	User	Conditional Access Administrator
Group1	Group	Global Administrator
Group2	Group	Exchange Administrator
App1	Registered app	Authentication Administrator

□□□□ □□ □□ □□□□ □□□□□□□.

□□ □□ □□□ Azure □□□□ □□□□□.

Name	Type	Role
Managed1	Managed identity	Owner
Managed2	Managed identity	Cloud Application Administrator
SPrincipal1	Service principal	Security Operator

Microsoft Entra Insights□□ □□ □□□ □□□ □□□ □□□ □□□□ □□ ID□ □□□□, □□□ □□□ □□□ □□□ □□□ □□□□ □□ ID□ □□□□□?

Answer:

NEW QUESTION: 118

□□□ □□

Sub1□ Sub2□□ □ □□ Azure □□□ Microsoft Entra □□□□ □□□□ □□□□. □□ □□□□□ Group1, Group2, Group3□□□ □ □□ □□□ □□□□.

□□□□ □□ □□ □□□ □□□□ □□□□□.

Name	Type	Subscription
VM1	Virtual machine	Sub1
VM2	Virtual machine	Sub2
Automation1	Azure Automation account	Sub2

□□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

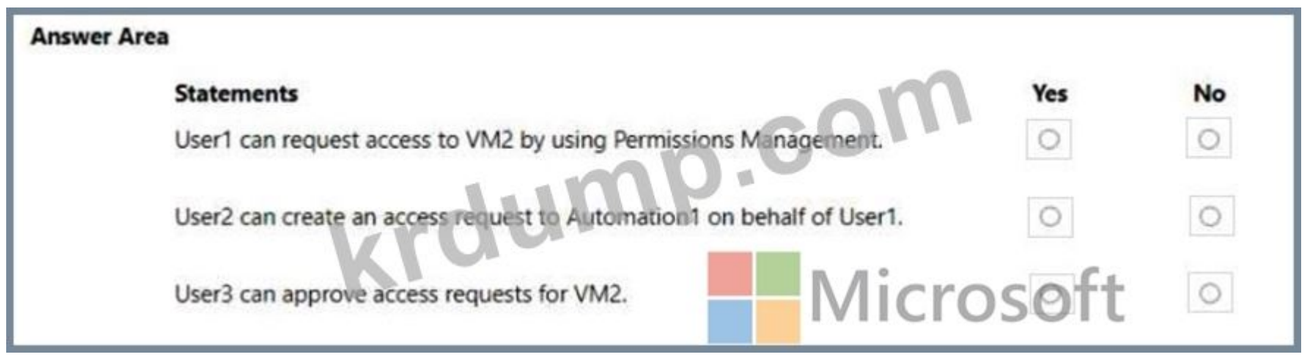
Name	Member of
User1	Group1
User2	Group2, Group3
User3	Group3

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

Name	Roles	Authorization System Name	Requestor for Other Identities
Group1	Viewer	Sub1	*None*
Group2	Controller	Sub2	User1
Group3	Approver	All Current and Future	*None*

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

No - User1 is part of the group that can request access to sub1, not sub2 No - User1 can request access to Sub1 on behalf of other identities, not user2 Yes - User3's group can approve access requests for all subscriptions

NEW QUESTION: 119

□□□ Microsoft Sentinel□ □□ □□ □□ □□□ □□ □□□□□ □□□ □□□□□. Microsoft Sentinel□ □□□□ □□ □□□□ □ □□ □□□ □□□□□?

A. Azure AD Premium P1 □□□□

B. □□ □□ □□ □□

C. Azure AD Premium P2 □□□□

D. Azure Key Vault

Answer: (SHOW ANSWER)

As having a configured Log Analytics Workspace is a prerequisite before begging to ingest data into Microsoft Sentinel.

Reference:

https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard#:~:text=%20Enable%20Azure%20Sentinel%20%201%20Sign%20in,support%20the%20moving%20of%20that%20workspace...%20See%20More

NEW QUESTION: 120

□□□ □□

□□□ Group1, Group2, Group3□□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Role	Member of
User1	Global Administrator	Group1
User2	*None*	Group2
User3	Global Reader	Group2, Group3

CA1□□□ □□□ □□□ □□□ □□□ □□□ □□□ □□ □□□ □□□□□.
- □□□
- □□□□
-- □□□ □ □□: Group1
- □□
-- □□□ □ □□: Group2
-- □□□□ □□: □□ □□□
- □□ □□
-- □□ □□: □□ □□□□ □
- □□ □□
-- □□ □□: □□□ □□ □□
CA2□□ □□□ □□□ □□□ □□□ □□□ □□□ □□ □□□ □□□□□.
- □□□
- □□□□
-- □□□ □ □□: Group2
- □□
-- □□□ □ □□: Group3
- □□ □□
-- □□ □□: □□ □□□□ □
-- □□: □□ □□
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online.	○	○
User2 will be prevented from signing in to Microsoft SharePoint Online.	○	○
User3 will be prevented from signing in to Microsoft SharePoint Online.	○	○

Answer:

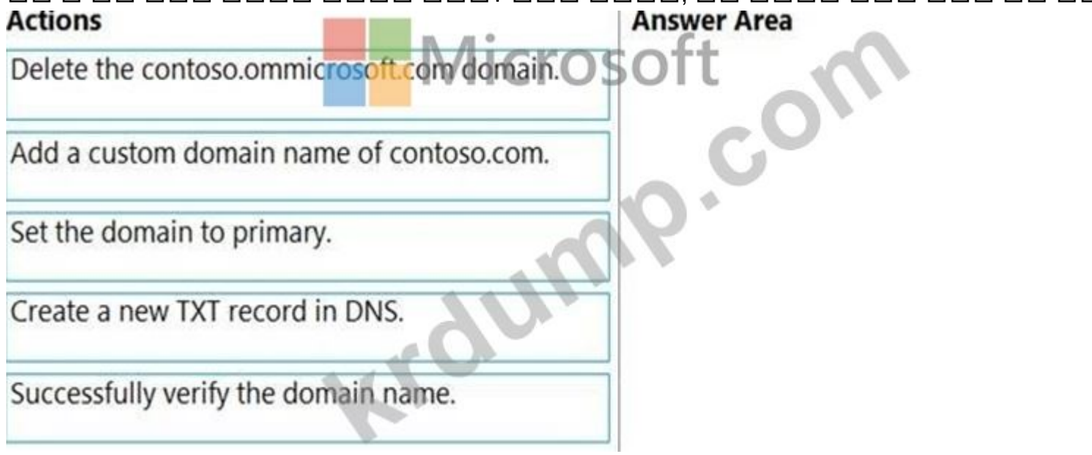
Answer Area

Statements	Yes	No
User1 will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online.	○	○
User2 will be prevented from signing in to Microsoft SharePoint Online.	○	○
User3 will be prevented from signing in to Microsoft SharePoint Online.	○	○

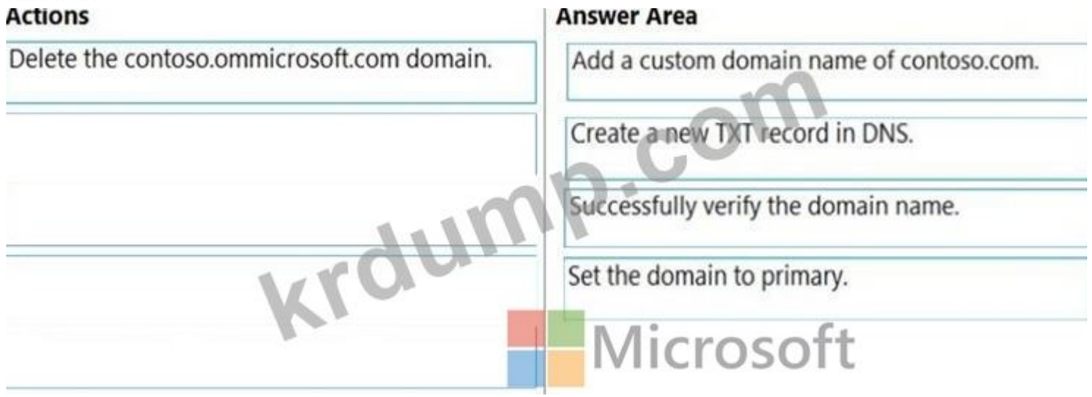
Explanation:
Box 1: No
User1 is Global Administrator.
User1 is member of Group1.
CA1 includes Group1.
CA1 excludes Global Adminstrators.
The exclusion takes precedence.
CA1 will not be applied to User1.
CA2 does not apply to User1 or Group1, only to Group2 and Group3.
User1 will NOT be prompted for multifactor authentication (MFA).
Note: In Azure Conditional Access policies, exclusion takes precedence over inclusion. This means that if a user is a member of both an included group and an excluded group, the exclusion policy will apply, denying them access or requiring different conditions.
Note 2: When no Azure Conditional Access policies are matched for a user, the user is granted access to the resource without any additional access controls or authentication requirements.
Essentially, it's treated as a normal sign-in. Conditional Access policies don't have a default deny policy, meaning if no policy applies, the user's access is not restricted.
Box 2: Yes
User2 has no role.
User2 is member of Group2.
CA1 excludes Group2.
CA1 will not be applied to User2.
CA2 includes Group2.
CA2 block access to all cloud apps.
CA2 will block access for user to Microsoft SharePoint Online.
Box 3: No
(User3 is Global Reader.)
User3 is member of Group2 and Group3.
CA1 excludes Group2.
CA1 will not be applied to User3.
CA2 includes Group2, and excluded Group3.
The exclusion takes precedence.
CA2 will not be applied to User3.
No Conditional Access policy will be applied to User3.
User3 will not be prevented from signing in to Microsoft SharePoint Online.

Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-users-groups
https://learn.microsoft.com/en-us/answers/questions/1004659/how-multiple-conditional-access-policies-are-appli

NEW QUESTION: 121
□□□ □ □□ □□
contoso.onmicrosoft.com □□□ □□□ □□□□ □ Microsoft 365 □□□□ □□□□.
□□□ □□□ □□□□□ contoso.com□□□ □□□ □□□□□.
□□□ Microsoft 365 □□□□ □□ □□□ □□□□ contoso.com□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□ □□□□, □□ □□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:
https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide

NEW QUESTION: 122

□□□ □□

□□□ Group1□ Group2□□ □ □□ □□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□□ □□□□□.

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

□□□ □□ □□□ □□□ □□□ □□□□□.

□□: □□1

□□□:

o □□: □□1

□□ □□: □□2

□□ □□□:

□□ □□: □□ □□□□ □

□□□□:

o □□ □□ □□: □□□ □□ □□

□□:

o □□□□ □□ □□ □□: □□ □□□□ □□

□□: □□2

□□□:

o □□ □□:

- □□□□ □□: □□ □□□

- □□□ □ □□: User3

□□ □□: □□2

□□ □□□:

□□ □□: □□ □□□□ □

□□:

□□□ □□:

- □□□ □□: 2□□

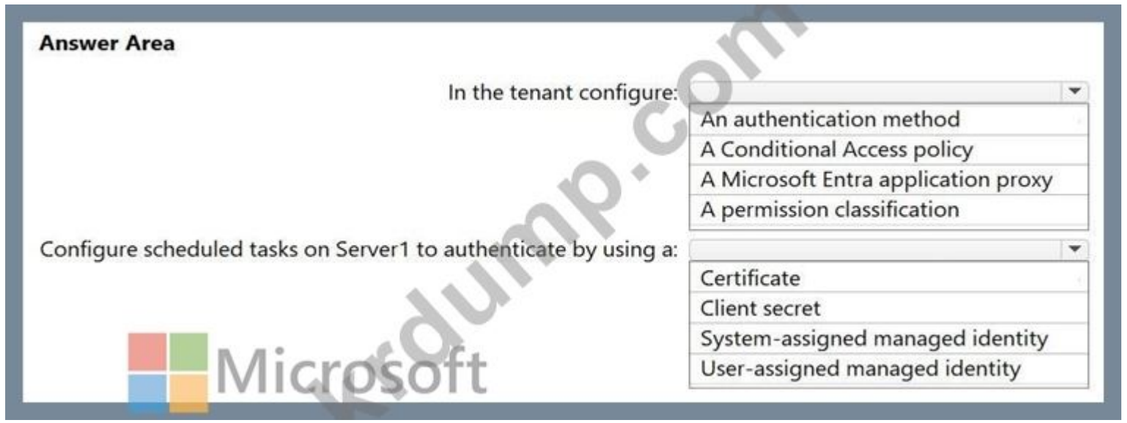
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□

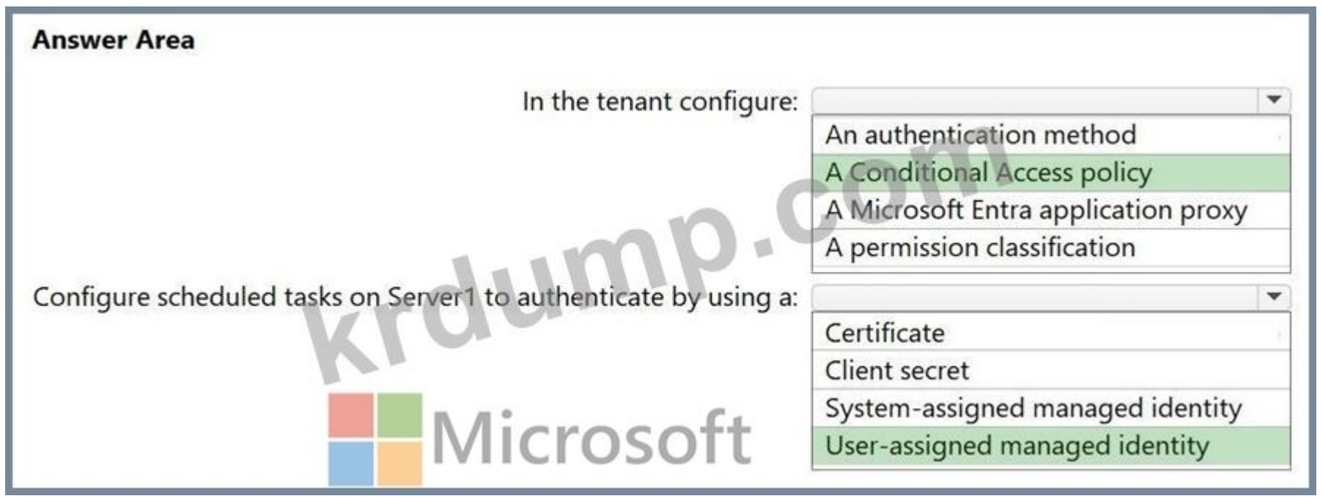
Answer:

NEW QUESTION: 123
□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
User1□ Microsoft Entra □□□ □□ □□□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□□
B. □□ □□ □□ □□□
C. □□□ □□ □□□
D. ID □□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 124
□□□ □□□ □□□□ □□□□□, □□□□ □□ □□ □□ □□ □ □□ □□ □□□ □□□□ □□□. □ □□□ □□□□ □□ □ □□□□?
A. Microsoft Entra □□□ □□
B. Microsoft Entra □□ □□
C. Azure □□□
D. □□□□□□□ □□□ □□ □□□ □□□
Answer: A (LEAVE A REPLY)
The Microsoft Entra Sign-in logs will show you all sign-in events and whether those events were successful or failed.
Reference:
https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-sign-ins
NEW QUESTION: 125
□□□ □□
Windows Server□ □□□□ Server1□□□ □□□ □□□□□ □□□ □□□□.
Microsoft Entra □□□□ App1□□□ □ □□□ □□□□. App1□□ Microsoft Graph □□□□□□ □□□ □□□□.
App1□ □□□□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- App1□ □□ □□□□□□□ □□ □□□□ □□□.
- App1□ □□ □□□ □□□□ □□□□□ □ □□□.
- Server1□ □□□□ □□ □□□ □□□ □□□ □ □□□ □□□.
App1□ □□□□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: A Conditional Access policy

To restrict access to a Microsoft Entra app registration with Microsoft Graph application permissions to only the corporate network, Conditional Access policies are used. These policies allow administrators to define rules based on various conditions, including network location, to control access to resources.

Box 2: User-assigned managed identity

It is possible to use a managed identity to configure non-interactive scheduled tasks on an on- premises server to authenticate with an application that has Microsoft Graph application permissions within a Microsoft Entra tenant. This involves leveraging a user-assigned managed identity, granting it the necessary permissions to access Microsoft Graph, and then configuring the scheduled task to utilize that identity for authentication.

Reference:

https://learn.microsoft.com/en-us/graph/migrate-azure-ad-graph-configure-permissions

https://docs.azure.cn/en-us/app-service/configure-authentication-provider-aad

NEW QUESTION: 126

□□□ □□

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

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

Assignment

SETTING	STATE
Allow permanent eligible assignment	No
Expire eligible assignments after	15 day(s)
Allow permanent active assignment	No
Expire active assignments after	1 month(s)
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	No

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

Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a **[answer choice]**.

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

Answer:

Answer Area

A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**.

- 8 hours
- 15 days
- 1 month

Before an eligible user can perform a task that requires the User administrator role, the activation must be approved by a **[answer choice]**.

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- privileged role administrator only

Explanation:
Select at least one approver. If no specific approvers are selected, Privileged Role Administrators and Global Administrators become the default approvers.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

NEW QUESTION: 127
□□□ □□
□□□ Microsoft 36S □□□□ □□□□ □□□□.
□□□ □□ □□□ □□□ HighRiskCountries□□ □□□ □□□ □□□□□.
□□□□ □□ □□□□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area Microsoft

Configure HighRiskCountries by using:

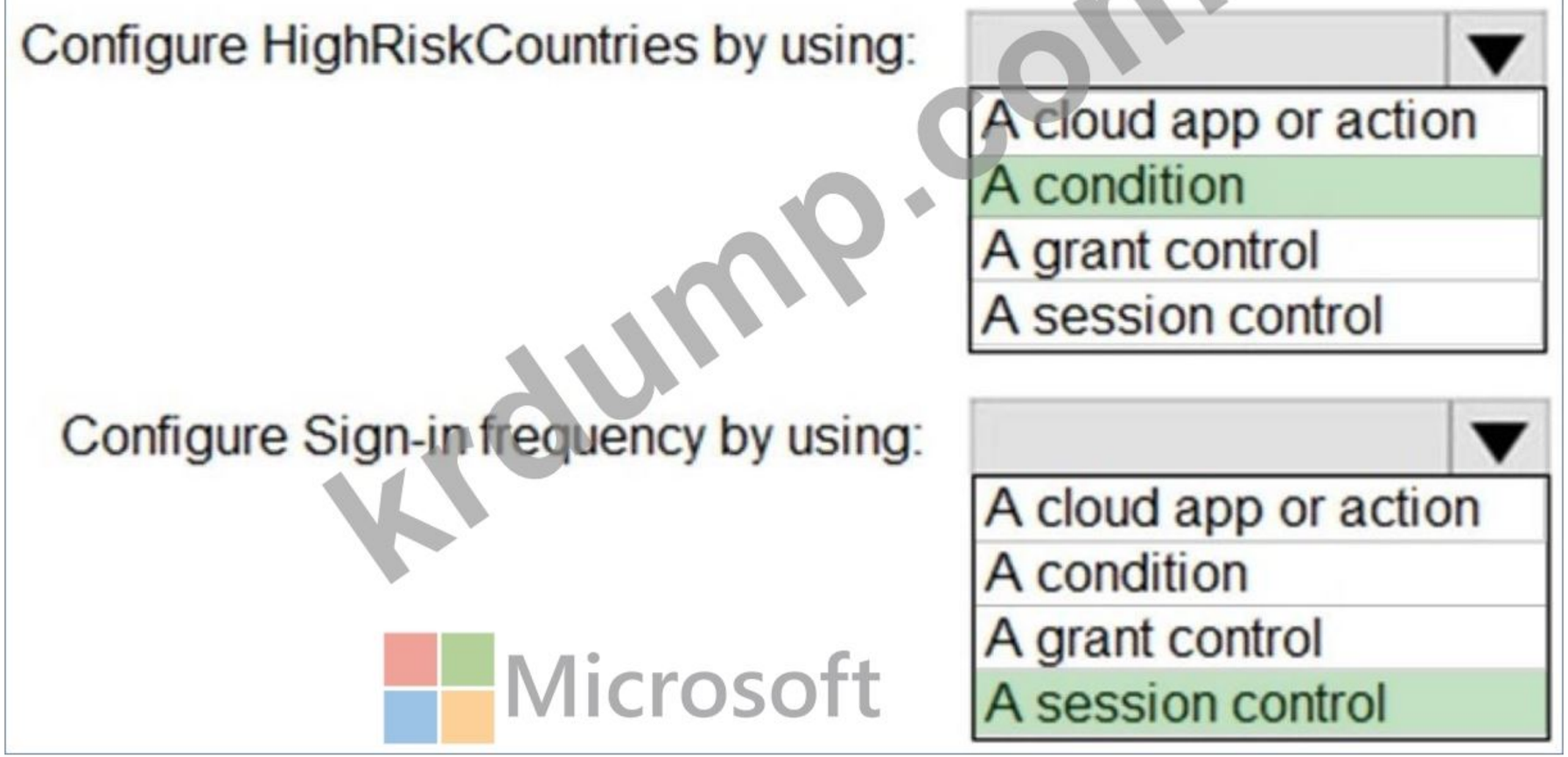
- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Answer:

Answer Area



Explanation:

Reference:

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

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

NEW QUESTION: 128

□□□□ Microsoft Office 365 Enterprise E3 □□□□□ □□□ □□□□ 2,500□ □□□□. □□□□□ □□ □□□□□ □□□□□.

Azure Active Directory □□ □□□ □□ □□□□□□ □□□□□ Microsoft 365 Enterprise E5 □□□□□ □□□□□.

□□□□ □□ □□□□ □□□□□□ Office 365 Enterprise E3 □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Azure Active Directory □□ □□□ □□ □□ □□□□
B. Set-AzureAdUsercmdlet
C. Azure Active Directory □□ □□□ □□ □□□□
D. Set-MsolUserLicensecmdlet
Answer: (SHOW ANSWER)
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this QUESTION 1in the exam. The QUESTION 1has two possible correct answers:
3. the Licenses blade in the Azure Active Directory admin center
4. the Set-MsolUserLicensecmdlet
Other incorrect answer options you may see on the exam include the following:
* the Identity Governance blade in the Azure Active Directory admin center
* the Set-WindowsProductKeycmdlet
* the Set-AzureAdGroupcmdlet
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

NEW QUESTION: 129
□□□ □□
□□□ □□ □□ □□□ ID□ □□□□ Microsoft Entra □□□□ □□□□ □□□□.

Name	Type	Member of
User1	User	Group1
Managed2	Managed identity	Group1
User3	User	Group2
User4	User	*None*

□□1□ □□□ □□ □□□ □□□ □□□□.
- □□□: User1, User4
- □□□: User1, Managed2, Group2
□□□ □□ □□□□ □□□ □□□ □□□□□.
- □□: □□1
- □□ □□: □ □ □□ □□
- □□: □□1
- □□ □□: □□ □□□
- □□□ □□: □□ □□□
□□ □□□ □□□ □□□□ □□ □□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
User1 can perform an access review for User1.	○	○
User1 can perform an access review for Managed2.	○	○
User1 can perform an access review for User3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can perform an access review for User1.	○	○
User1 can perform an access review for Managed2.	○	○
User1 can perform an access review for User3.	○	○

NEW QUESTION: 130

□□□ □ □□ □□

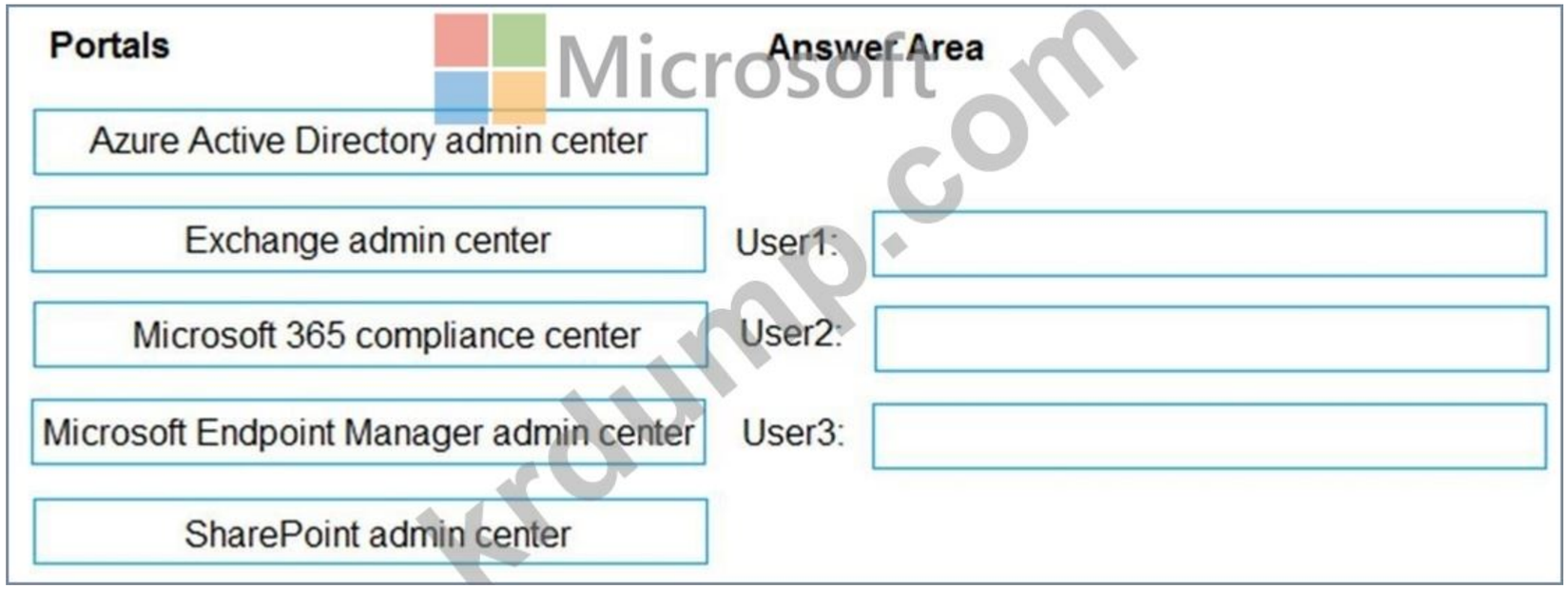
□□□ User1, User2, User3□□□ □□□ □□□ 3□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.

□□ □□ □□□ □□ □□□□ □□□□ □□□.

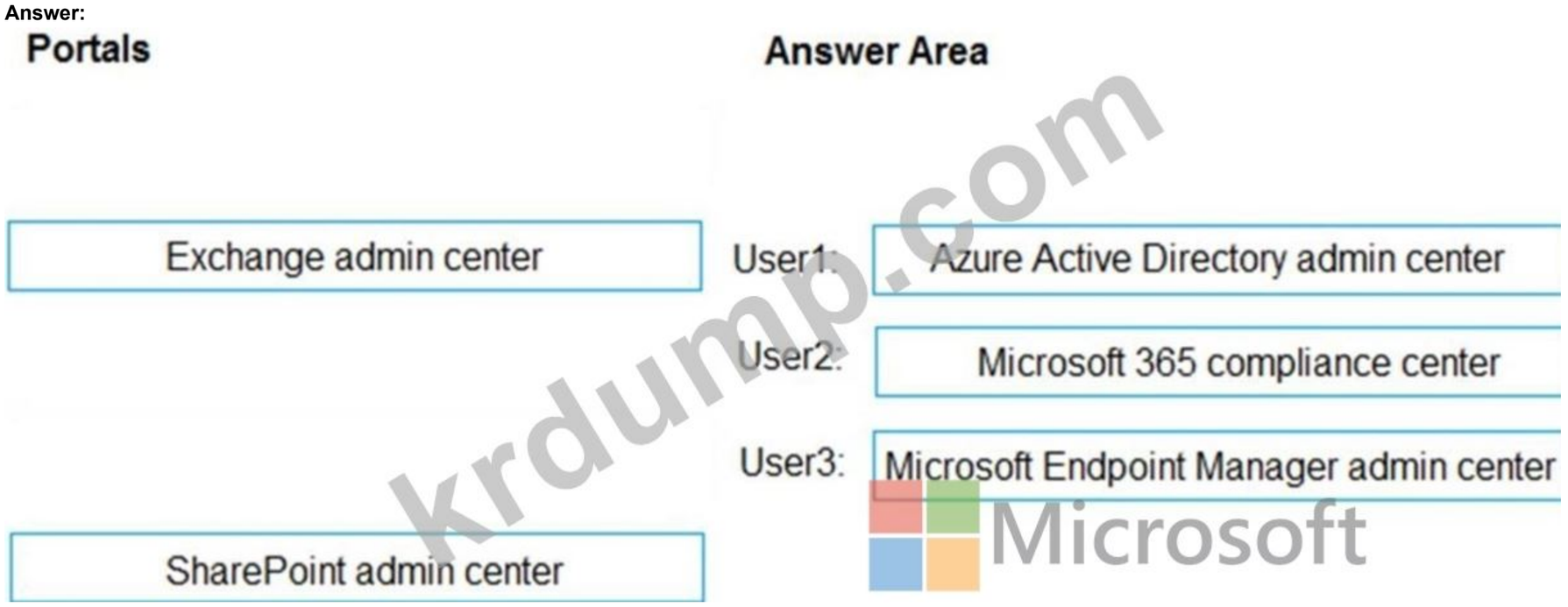
User	Configuration
User1	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

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

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

User 1: Azure Active Directory Admin Center

User 2: Microsoft Purview admin center (legacy Microsoft Compliance Admin center) These roles came from Exchange, Microsoft is not enforcing the roles permission from Exchange, Microsoft is recommending using Microsoft Purview Admin center. I believe this answer is too old.

it could be true years ago, however, Microsoft today is with MS purview to assign these roles.
Record management and Quarantine role are known as SCC (security and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.
User 3: Microsoft Endpoint Manager Admin Center
You will see these two roles in the endpoint admin center.

NEW QUESTION: 131
□□□ □□
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□, □□ □□□□□ User1□□□ □□□□ □□□□.
User1□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

2020□ 11□ 5□, □□□ contoso.com□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.
- □□: Terms1
- □□ □□: Contoso □□ □□
- □□□□ □□ □□□ □□□□□ □□: □□
- □□ □□□□ □□□□ □□□ □□□: □□
- □□ □□: □□
- □□□: 2020□ 12□ 10□□□
- □□: □□

2020□ 11□ 15□, User1□ Device3□□ Terms1□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	○	○
On December 11, 2020, User1 can accept Terms1 on Device2.	○	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
On November 20, 2020, User1 can accept Terms1 on Device1.	○	○
On December 11, 2020, User1 can accept Terms1 on Device2.	○	○
On December 7, 2020, User1 can accept Terms1 on Device3.	○	○

Explanation:
Box 1: Yes
Because User1 has not yet accepted the terms on Device1.
Box 2: Yes
Because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.
Box 3: No
Because User1 has already accepted the terms on Device3. The terms do not expire until December 10th and then monthly after that.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

NEW QUESTION: 132
□□ □□ □□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Usage location	Department	Job title
User1	United States	Sales	Associate
User2	Finland	Sales	SalesRep
User3	Australia	Sales	Manager

□□ □□□ □□□ □□□□ □□ □□ □□□ □□□□□.
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep") □□ □□□□□ □□□ □□□□□?
A. □□□ 1 □□
B. □□□2 □□
C. □□□3 □□
D. □□□1□ □□□2□ □□
E. User1 □ User3□ □□
F. □□□1, □□□2, □□□3
Answer: (SHOW ANSWER)
user.usageLocation -in ["US","AU"] == User 1 & User 3
-and (user.department -eq "Sales") == User 1 & User 3
-and -not (user.jobTitle -eq "Manager") == User 1

-or (user. jobTitle -eq "SalesRep")

NEW QUESTION: 133

□□ □□ 2 - □□□□ □□□□

□□

Litware, Inc.□ □□□□ Fabrikam, Inc.□ □□□ □□ □□□□□.

Litware□ □□□□ □□□□ □□□□ □□ □□□, □□ □□□ □□□ □□□□ □□□□.

□□□□ VPN □□□ □□□□ □□□□ □ □□□ □ □ □□ □□□□□.

□□ □□. □□ □□

□□□□□□ litware.com□□□ □□□ Active Directory □□□□□ □□□, □ □□□□□ litware.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. Azure AD Connect□ □□□□ □□□ □□ □□ □□ □□ □□□□ □□□□□□ □□□□.

Litware.com□□ □□ □□□□□□ □□□ □□□□ User1□□□ □□□□ □□□□.

Litware□ Azure AD □□□□□□ □□□□ □□□□□.

Fabrikam□ fabrikam.com□□□ □□□ Azure AD □□□□ □□□□ □□□□. Fabrikam□ □□□□□ litware.com □□□□ □□□ □□□ □□□□ litware.com□ □□□□ □□□□□.

□□ □□. □□□□ □□

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

Litware□ litware.com Azure AD □□□□ □□□ Azure □□□ □□□□ □□□□. □ □□□□ Azure Active Directory □□□□ Office 365 □□□□ □□□□ Azure Sentinel □□□□□ □□□□ □□□□. Azure Sentinel□ □ □ Azure AD □□□ □□□ □□ □□□ □□□□□.

□□ □□. □□□□□ □□

□□□□□ □□□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litware□ □ □□□ □□ □□□□ □□ □□□□ □□□□. □ □□□ □□ □□□ □ VPN □□□ □□□□ Azure □□□ □□ □□□□□ □□□□□. □□ □□□□□ □□□ □□□□□ □□□□ □□□□ □ □□□ □□□□ □□□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□□ □□□□□.

* Azure AD □□ □□ ID □□(PIM)□ □□□□ □□ □□ □□ □□□ □□□□□.

* □□□ □□ □□□□ litware.com Azure AD □□□□ □□□□□□□ □□□□ □□□□ □□□□□.

* □□□ □□ □□□□ □ □□□ □□ □□□□□ □□□□ ID □□□ □□□□□.

* User1□ Azure AD□□ □□□□□□ □□□□□□□ □□□ □ □□□ □□□□□□.

* □□ □□ □□□ □□□□□□.

□□ □□. □□ □□

Litware□ □□ litware.com Active Directory □□□□□ LWLicenses□□ □□□ □□ □□□ □□□□□□. Litware□ LWLicenses □□ □□ □□□□ Azure AD □□□□ □□□ □□□□□ □□□. LWLicenses □□ □□ □□ □ □□□□ □□ □□□□□ □□□ Microsoft 365 □□□ □□□□ □□□□□ □□□.

□□□□. □□ □□□□

Litware□ Litware□ □□ Azure AD □□□ □□□ □□□□ Azure AD □□□ □□□ □□□ LWGroup1□□□ □□□ □□□□ □□□.

□□ □□. □□ □□ □□

Litware□ □□□ □□ □□ □□ □□□ □□□□□.
* □□ Litware □□□□□ □□□ □□(MFA)□ □□□□□□.
* Litware □□□ □□□□□ Azure AD□ □□□ □ MFA(□□□ □□)□ □□□□ □□□ □□□□ □□□□□.
* litware.com □□□□□ □□ □□ □□ □□□ □□□□□□.
* □□□□□ □□□□□□□ □□□□ □ MFA(□□□ □□)□ □□□□□□.
* □□□ □□□ □□ □□□ □□□□ □□□□ □□□□□.
□□ □□. □□ □□ □□
Litware□ □□□ □□ □□ □□ □□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□ Azure □□□ □ Azure AD □□□□□□□ □□ □□ □□□□ □□□□□.
* Microsoft SharePoint Online□ □□ □□ □□ □□□ □□□□ □□□ □□□ □□□ □□□□□.
* Azure AD□ □□□ □□□ □□□□ □□□□□□□ □□ □□ □□ □□□□ □□□□□.
□□□□. □□□□ □□□□
Litware□ Azure Sentinel□ Fusion □□□ □□□□ □□□□□ Azure AD □□□□ □□□□□ Microsoft Office 365 □□□ □□□ □□□ □□□ □□□□□ □□□.
□□□ □□
□□ □□ □□□ □□□□□ Azure AD□□ □ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

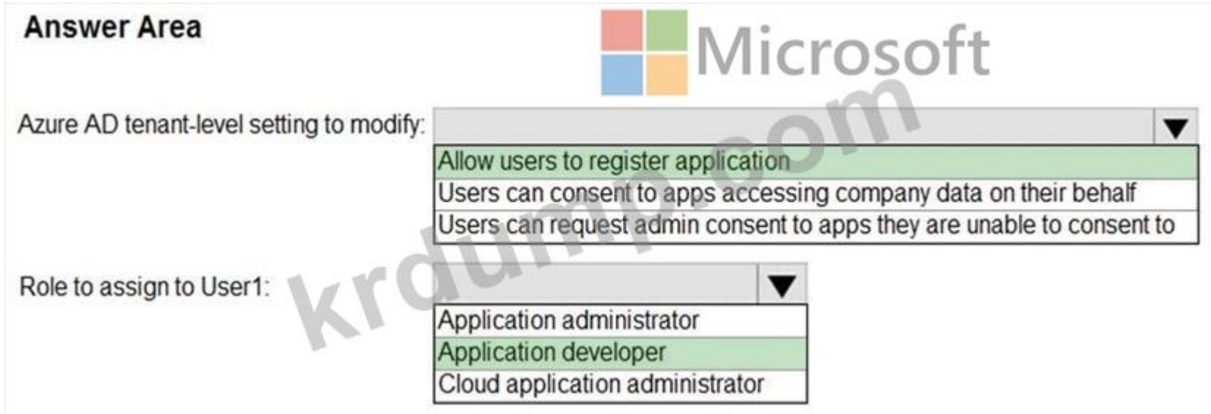
Azure AD tenant-level setting to modify:

- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- Application developer
- Cloud application administrator

Answer:



Explanation:

1: Requirements for delegation clearly says " Prevent users to register applications"

2: User1 would need App Developer to register an app in tenant using "principle of least privilege"

https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

NEW QUESTION: 134

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

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

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

User1□□□ □□□ □□□□ □□□□□.

User1□ Identity Secure Score □□ □□□ □□□ □□□□□ □ □□□ □□ □□□.

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

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read-and-write-roles

NEW QUESTION: 135

contoso.com□□□ Microsoft Entra □□□□ □□□, □ □□□□□ App1□□□ □□□□□□ □□□□□□□ □□□□.

□□□□□ user1@outlook.com □□ □□□ □□□□□.

□□□□□□ App1□ □□ □□ □□□ □□□ □ □□□ □□ □□□. □□□□□ user1@outlook.com□□ □□□ □ □□□ □□□.

□□□ □□ □□□?

A. Microsoft Entra Connect □□□□ □□□□□.

B. contoso.com□ □□□ □□ □□□ □□□ □□□□□.

C. Microsoft Entra □□□□□□ □□□□ □□□□□.

D. New-MgInvitationcmdlet□ □□□□□.

Answer: D (LEAVE A REPLY)

* Create a guest user account in contoso.com.
* Run the New-AzureADMSInvitation cmdlet. [For Microsoft Active Directory]
* Run the New-MgInvitationcmdlet. [For Microsoft Entra]
Note:
* New-AzureADMSInvitation
This cmdlet is used to invite a new external user to your directory.
* New-MgInvitation
Microsoft.Graph.Identity.SignIns
Use this API to create a new invitation or reset the redemption status for a guest user who already redeemed their invitation. Invitation adds an external user to the organization Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

NEW QUESTION: 136
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
App1□□□ □□□ □□ SaaS(Software as a Service) □□ □□□ □□□□□.
App1□ Microsoft Defender for Cloud Apps□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. Microsoft Entra □□ □□□□ □□□ □□ □□□□ □□□□□.
B. Microsoft Entra □□ □□□□ App1□ □□ □□ □□□(SSO)□ □□□□□.
C. Microsoft Defender □□□□ OAuth □ □□□ □□□□□.
D. Microsoft Defender □□□□ □□□□ □□□ □□□□□.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 137
□□□ □ □□ □□
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Description
User1	User	*Not applicable*
User2	User	*Not applicable*
Vault1	Azure Key Vault	Contains a secret named Secret1
Vault2	Azure Key Vault	Contains a secret named Secret2
Secret1	Secret	Stored in Vault1
Secret2	Secret	Stored in Vault2

□ □□ □□□□ □□ □□ □□□ ID □□(PIM)□ □□□□□.
PIM□ □□□□ □□ □□□ □□□ □□□□ □□□.
- User1□ Secret1□ □□ □□□□□ □ □□□ □□□□□□.
- User2□ □□□ □□ □□□ □□□ □□ □ □□□ □□□□□□.

□□2.
□□□□ □□ □□ □□□ □□□ □□□.
□ □□□□□ □□ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□ □□ □□□ □□ □□□□□ □□□□□□. □ □□ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □ □□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.

Authorization methods

- The GET Secret Permissions Access Policy permission
- The Key Vault Secrets Officer RBAC role
- The Key Vault Reader RBAC role
- The Key Vault Secrets User RBAC role
- The LIST Secret Permissions Access Policy permission
- The SET Secret Permissions Access Policy permission

Answer Area

User1:

User2:

Answer:

Authorization methods

- The GET Secret Permissions Access Policy permission
- The Key Vault Reader RBAC role
- The LIST Secret Permissions Access Policy permission
- The SET Secret Permissions Access Policy permission

Answer Area

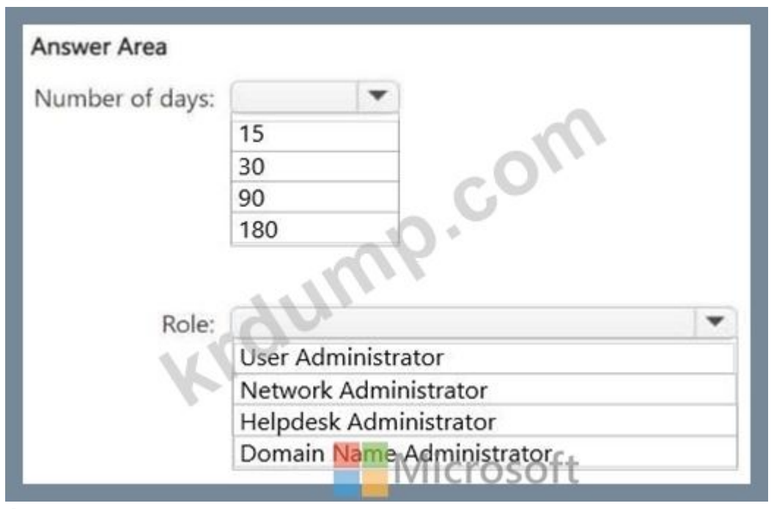
User1: The Key Vault Secrets Officer RBAC role

User2: The Key Vault Secrets User RBAC role

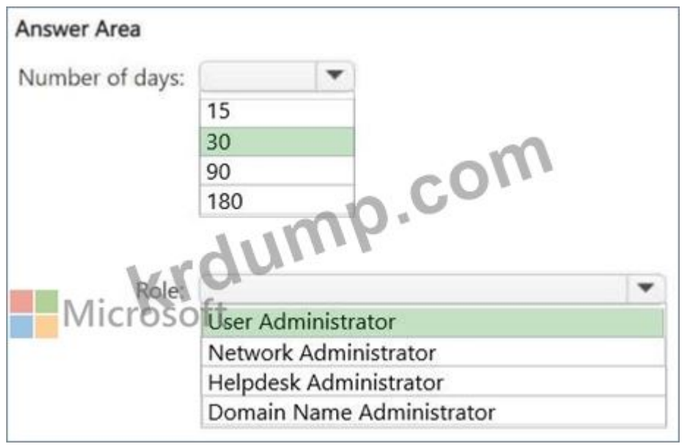
NEW QUESTION: 138
Microsoft 365 □□□□ □□□□.
Microsoft Entra ID□□□ □□ □□□ □□□□□.

□□ □□□ □□□ □□□□ □□□ □ □□□□ □□□ □ □□□ □□ □□□. □□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Defender for Cloud Apps□ □□□ □□
B. Microsoft Entra ID□ □□□ □□□ □□
C. Microsoft Intune □□ □□
D. Microsoft Intune□ □□ □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 139
□□□ □□
Microsoft Entra □□□□ User1□□□ □□□□ □□□□.
□□□□ User1□ □□□□□.
□□ □□□□ □□□□ □□□.
- □□ □□ □□ □ □□□ □□□ □ □□□?
User1 □□□ □□□□□□□□?
- User1□ □□□□ □ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?
□□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Box 1: 30

In Microsoft Entra ID (formerly Azure AD), deleted users can be restored within a period of 30 days. After this 30-day period, the account is permanently deleted and cannot be recovered.

Box 2: User Administrator

The User Administrator role is the least privileged role that has the permissions required to restore deleted user accounts in Microsoft Entra ID. Other roles, like Network Administrator or Domain Name Administrator, do not have the necessary permissions to manage user accounts.

NEW QUESTION: 140

□□ □□ 1 - □□□ □□□□

□□

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

Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.

□□ □□. □□ □□

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

□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.

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

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□

Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.

* □□□□□□□ □□□ 365 □□□□□□ E5

* □□ □□□□ + □□

* □□□ 10 □□□□□□ E3
* □□□□ □□ 3

Azure AD Connect□ Azure AD□ Active Directory □□□ □□□(AD DS) □□ □□□□□. Contoso_Resources OU□ □□□□□□.

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

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

* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.

contoso.com□ □□ □□ □□□ □□□□□□ □□□□.

Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.

□□ □□. □□ □□

Contoso□ □□□ □□ □□□□ □□□□□.

* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.
* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

□□□□. □□□ □□ □□

Contoso□ □□□ □□ □□ □□□ □□□ □□□□□.

* □□ □□□ □□ □□□(SSPR)□ □□□□□.
* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.
* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□□□.
* App1□□□ □□□ □□□ □□ □□□ Azure □ □□ □□□□□. App1□ □□□□□ □□ □□□□ Azure AD □□□ □□□□ □□□□□.
* □□□ □□□ □□ □□□□ □□ Microsoft SharePoint Online □□□, □□ □ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□.

Contoso□ Adatum Corporation□□□ □□□ □□□ □□□□□. 100□□ □□□ Adatum □□□□ Adatum□□□ □□□ Active Directory □□ □□(OU)□ □□□ □□□□□. □ □□□□□ □□□ □□□□ □□□□ □□□.

□□□□. □□□ □□□□

Contoso□ □□□ □□ □□ □□ □□□ □□□□□.

* □□ □□□□ AD DS□□ contoso.com Azure AD □□□□ □□□□□□ □□□.
* App1□ https://contoso.com/auth-response□ □□□□ □□□□ URI□ □□□ □□□.
* □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□.
* Fabrikam □□□□ □□□ □□□ SharePoint □□□□ □□ 90□ □□ □□ □□□ □□□ □□□.
* Azure AD□□ □□□□ □□□ □□□ □□□□□ □□□. □□ □□□ 1□ □□ □□□□ □□□.
* □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.

□□

ADatum □□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.

□□□ □□ □□□?

A. Microsoft Entra Connect □□□□□ □□□ □□ □□□ □□□ □□□□□.

B. PowerShell□□ Set-ADSyncScheduler□ □□□□□.

C. PowerShell□□ Start-ADSyncSyncCycle□ □□□□□.

D. Microsoft Entra Connect □□□□□ □□□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#filtering-options
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-whatis#azure-ad-connect-sync-topics

NEW QUESTION: 141
□□ □□ □□□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

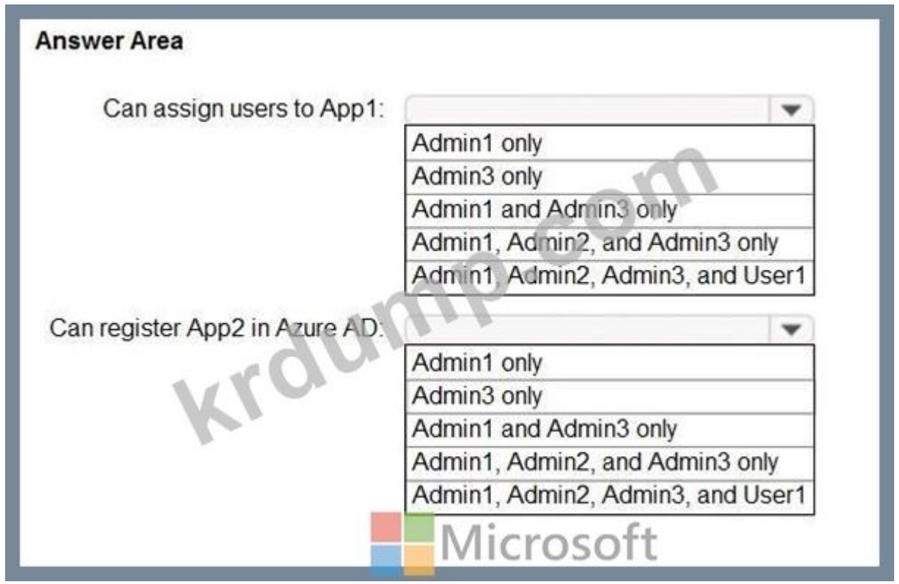
Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Azure AD □□□ □□ Azure AD □□ □□ ID □□(PIM)□□ □□ □□□ □□□ □ □□ □□□ □□□□□?
A. User1, Guest1, Identity1
B. User1 □ Guest1□ □□
C. □□□ 1 □□
D. User1 □ Identity1□ □□
Answer: B (LEAVE A REPLY)
You cannot assign service principals as eligible to Azure AD roles, Azure roles, and Privileged Access groups but you can grant a time limited active assignment to all three.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

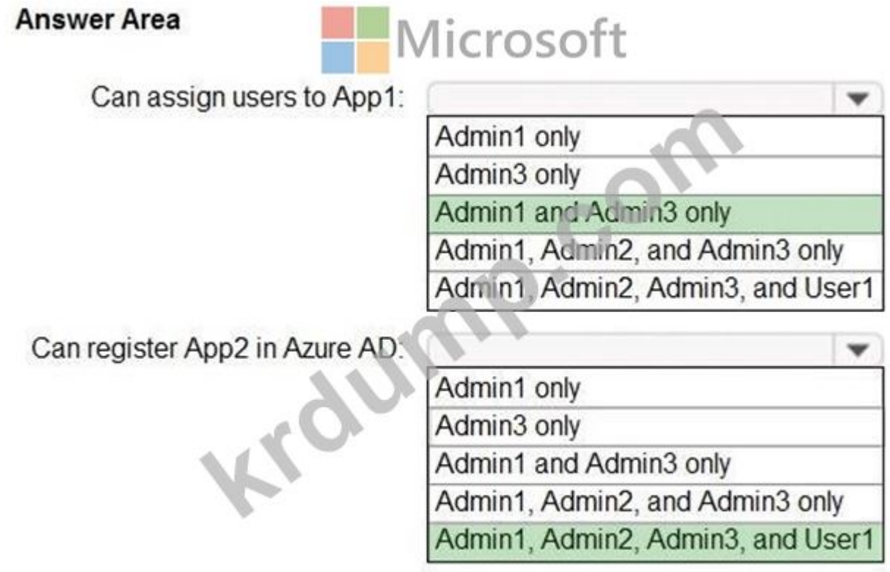
NEW QUESTION: 142
□□□ □□
□□ □ □□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

App1□ App2□□ □ □□ □□□□ □□ □□□□□□. □□□ □□□□ Azure AD□ App1□ □□□□□.
App1□ □□□□ □□□ □ □□ □□□ Azure AD□ App2□ □□□ □ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Only administrators (Admin1 - Application Administrator & Admin3 - Cloud application administrator) can manage/configure apps.

Name: Cloud application administrator

Description: Users in this role can add, manage, and configure enterprise applications, app registrations but will not be able to configure or manage on-premises like app proxy.

Azure AD - User settings - App registration: default is Yes (If this option is set to yes, then non- admin users may register custom-developed applications for use within this directory.)

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

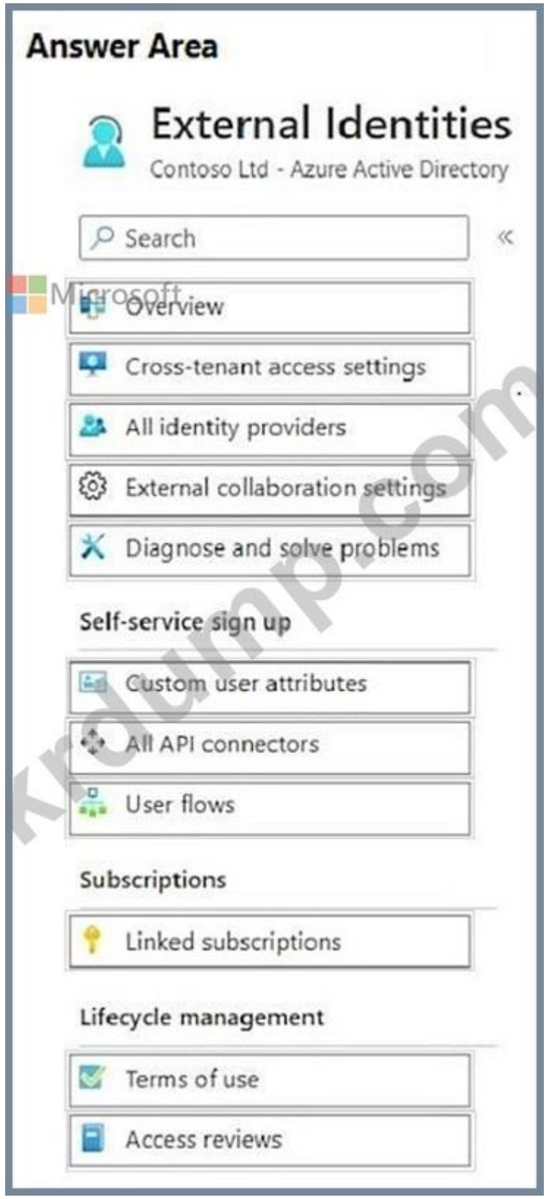
NEW QUESTION: 143
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□, □□ □□□ □□ □□□ □□□□ □□□□.
Amazon Web Services(AWS) □□, Google Workspace □□, GitHub □□□ □□□□.
Azure □□□ □□□□ Microsoft 365 Defender□ □□□□□□.
□□□□ □□ Microsoft Defender□ □□□□ OAuth □□ □□□ □□□□□ □ □□□ □□□□ □□□.
□□□: Microsoft 365 Defender □□□□ Google Workspace □ □□□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: A (LEAVE A REPLY)
Microsoft Defender for Cloud Apps is now part of Microsoft 365 Defender, which correlates signals from across the Microsoft Defender suite and provides incident-level detection, investigation, and powerful response capabilities.
For more information, see Microsoft Defender for Cloud Apps in Microsoft 365 Defender.
https://learn.microsoft.com/en-us/defender-cloud-apps/manage-app-permissions

NEW QUESTION: 144
□□□□ Microsoft Office 365 Enterprise E3 □□□□□ □□□ □□□□ 2,500□ □□□□. □□□□□ □□ □□□□□ □□□□□.
Microsoft Entra □□ □□□ □□ □□□□□□ □□ □□□□ □□□ □□□ Microsoft Office 365 Enterprise E5 □□□□□ □□□ □ □□□□.
□□□□ □□ □□□□ □□□□□□ Office 365 Enterprise E3 □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Set-MgUserLicense cmdlet
B. Microsoft Entra □□ □□□ ID □□□□ □□□□
C. Microsoft Entra □□ □□□ □□ □□□□
D. Update-MgGroup cmdlet
Answer: A (LEAVE A REPLY)
The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.
Note:
There are several versions of this QUESTION 1in the exam. The QUESTION 1has two possible correct answers:
the Licenses blade in the Azure Active Directory admin center
the Set-MsolUserLicensecmdlet
Other incorrect answer options you may see on the exam include the following:
the Identity Governance blade in the Azure Active Directory admin center
the Set-WindowsProductKeycmdlet
the Set-AzureAdGroupcmdlet
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0
NEW QUESTION: 145

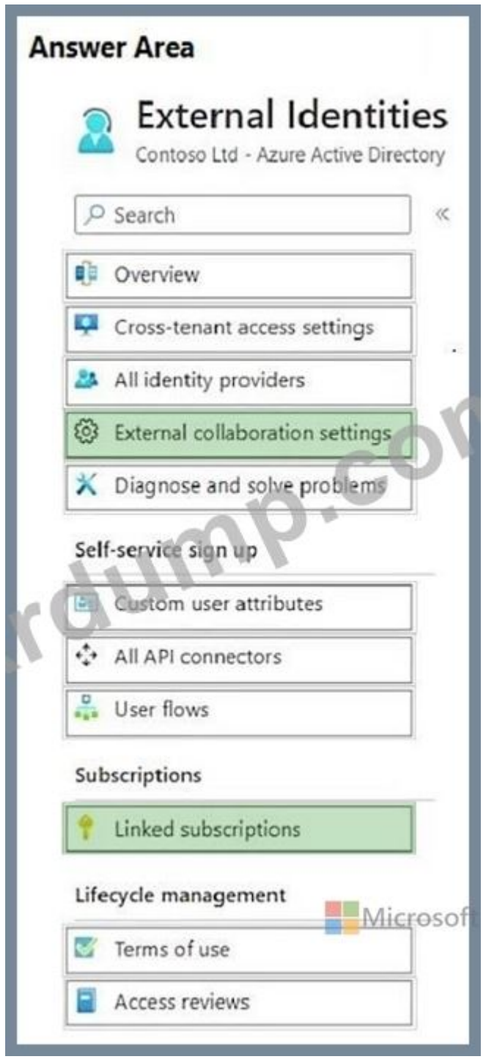
Azure AD □□□□ □□□□.
□□ □□ □□□□ □□□.
□□ □□ □□ □□□ □□□ □□□□ □□□□□?
A. □□□□ □□□□
B. □□ IP □□
C. □□□□ □□ □□□ □□
D. Azure AD □□ □□□□□
Answer: (SHOW ANSWER)
Sign-in Risk policies cover:
- Anonymous IP address
- Additional Risk detected
- Admin confirmed user compromised
- Anomalous token
- Atypical travel
- Azure AD threat intelligence
- Impossible travel
- Malicious IP
- Malware linked IP
- Mass Access to sensitive files
- New country
- Password spray
- Suspicious browser
- Suspicious inbox forwarding
- Suspicious inbox manipulation rules
- token issuer anomaly
- Unfamiliar sign-in properties
User risk policies cover:
- Additional risk detected
- Anomalous user activity
- Azure AD threat intelligence
- Leaked credentials
- Possible attempt to access Primary Refresh Token (PRT)
https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity- protection-risks

NEW QUESTION: 146
□□□ □□
Azure AD □□□□ □□□□.
□□□ □□ □□ ID □□□ □□□□ □□□.
- B2B □□
- □□ □□ □□□(MAU) □□ □□ □□
□□ □ □□ □□□ □□□□ □□□? □□□ □□□□□ □□□□ □□□□□.

□□: □□ □□□ 1□□□□.


Answer Area
External Identities
Contoso Ltd - Azure Active Directory
Search
Overview
Cross-tenant access settings
All identity providers
External collaboration settings
Diagnose and solve problems
Self-service sign up
Custom user attributes
All API connectors
User flows
Subscriptions
Linked subscriptions
Lifecycle management
Terms of use
Access reviews

Answer:



NEW QUESTION: 147
□□□ Azure AD □□□□ □□□□□ □□□.
□□□□ □□ □□□□□ □□□□□ □□ □□(MFA) □□□ □□□□□?
A. Microsoft □□□
B. □□
C. □□□□
D. □□□ OTP
Answer: A (LEAVE A REPLY)
Security defaults users are required to register for and use multifactor authentication using the Microsoft Authenticator app using notifications. Users might use verification codes from the Microsoft Authenticator app but can only register using the notification option. Users can also use any third party application using OATH TOTP to generate codes.

https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults#authentication-methods

NEW QUESTION: 148
contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
Fabrikam, Inc.□□ □□□□ □□□□□ □□□ □□ □□□ □□□□ □□ □□ □□ □□□ □□□□□. Fabrikam□ fabrikam.com□□□ □□□□ □□□□□.
Fabrikam □□□□ □ □□ □□□□ □□□□ □□ □□ □□□□□ □□□□ □□□□□ □□□.
□□ □□□ □□□□ □□□.
- □□ □□□□ □ □□□□ □□□ □□: □□□
- □□ □□□ □□: □
- □ □□□□□□ □□ □□□□ □□□□□□□ □□: 90□
ID □□□□ □□□□□□ □□□ □□□□ □□□?
A. □□□ □□□
B. □□ □□ □□
C. □□□□
D. □□□ □□
Answer: (SHOW ANSWER)
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users

NEW QUESTION: 149
□□ □□ 1 - □□□ □□□□
□□
□□□ □□□□□ □□□□□ □□□ □□ □□□ □□□□ □□□ □ □□□ □□□□□.
Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
□□ □□. □□ □□
Contoso□ □□□□□ □□□□□□ contoso.com□□□ Active Directory □□□□ □□□□.
□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.
contoso.com Active Directory □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□
Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.
* □□□□□□□ □□□ 365 □□□□□□ E5
* □□ □□□□ + □□
* □□□ 10 □□□□□□ E3
* □□□□ □□ 3

Azure AD Connect□ Azure AD□ Active Directory □□□ □□□(AD DS) □□ □□□□□. Contoso_Resources OU□ □□□□□□.
□□□□□ □□□□ □□□ □□□ □□□□ □□ Microsoft 365 □□ □□□ □□□□□ □□□□□.
□□ □□□ □□□□ Microsoft 365 □□ □□□ □□□□ □□□□ □□□□□ □□□□□. □□ □□ □□□ □□□□ □□ □□□□□ □□ □□□□□ □□□□ □□□□.
* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.
contoso.com□ □□ □□ □□□ □□□□□□ □□□□.
Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.
□□ □□. □□ □□
Contoso□ □□□ □□ □□□□ □□□□□.
* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.
* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.
□□□□. □□□ □□ □□
Contoso□ □□□ □□ □□ □□□ □□□ □□□□□.
* □□ □□□ □□ □□□(SSPR)□ □□□□□.
* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.
* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□□ □□□ □□□ □□□□□ □□□ □□□□□ □□□□□ □□□ □□□□□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.
□□
□□□ □□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□□□ □□□.
□□ □□□ □□ □□ □ □□ □□□ □□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.
A. □□□ □ □□□ □□ □□□ □□□□□.
B. □□□ □ □□ □□ □□ □□□ □□□□□.
C. □□ □ □□ □□ □□□ □□□□□.
D. □□ □□□ □□□□ □□□□□.

E. □□ □□□ □□□□ □□□□□.

Answer: (SHOW ANSWER)

Scenario: Configure the User administrator role to require justification and approval to activate.

Require justification.

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the Require justification on activation box.

To require justification need assignment to be Eligible instead of Active.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings

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

NEW QUESTION: 150

□□□ □□

Azure □□□ □□□□ □□□□.

□□ □□□□ □□□ □□ □□ □□□□□ □□□□ Catalog1□□□ □□□□□ □□ □□□□□.

Catalog1□ □□□□□ □□□ □□ □□□□ □□, □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

Answer:

Answer Area

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-logic-apps-integration

NEW QUESTION: 151

□□ □□ 1 - □□□ □□□□

□□

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

Contoso□ Fabrikam, Inc.□□ □□□ □□□□□ □□ □□□□. Fabrikam□ fabrikam.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.

□□ □□. □□ □□

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

□□ □□□□□ Contoso_Resources□□ □□ □□(OU)□ □□□□. Contoso_Resources OU□□ □□ □□□□ □□□□ □□□□ □□□□.

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

Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

□□ □□. Microsoft 365/Azure □□

Contoso□ contoso.com□□□ Azure AD □□□□ □□□□ □□□, □□ □□□□□ □□□ □□ □□□□□ □□□□ □□□□.

* □□□□□□□ □□□ 365 □□□□□□ E5
* □□ □□□□ + □□
* □□□ 10 □□□□□□ E3
* □□□□ □□ 3

Azure AD Connect□ Azure AD□ Active Directory □□□ □□□(AD DS) □□ □□□□□. Contoso_Resources OU□ □□□□□□.

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

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

* □□ □□□ □□□□□□ Microsoft 365 □□ □□□ □□□□□ □□□□ □□□□□.
* □□□ □□□ □□□□□ Yammer Enterprise □□□□□ □□□□ □□ □□□□□.

contoso.com□ □□ □□ □□□ □□□□□□ □□□□.

Contoso□ □□□ □□□ □□□□ □□ Azure AD □□ □□ ID □□(PIM)□ □□□□□.

□□ □□. □□ □□

Contoso□ □□□ □□ □□□□ □□□□□.

* □□ □□ □□□□□ □□□□ □□ Microsoft 365 □□□□□ □□□ □□□□□ □□□ □ □□□□.
* □□□ □□□□□ □ Contoso □□□□□ □□ □□ □□□□ □□ □□□ □□□□ □□□□ □□ □□□□□ □□□□□□.
* □□□□□ □□□□ □□ Microsoft 365 □□□ □ □□ □□ □□ □ □□□ □□□ □□□ □□□□ □ □□ □□ □□□ □□□□□.
* □□ □□□□□ □□□□ □□□ □□□ □□ □□ □□□ □□□ □□□ □□□□ □□□ □□□ □ □□□□.
* Azure AD□□ □□ □□□ □□□□ Log Analytics □□□ □□□□□ □□□□ □□ □□□□ □□□□□.

□□□□. □□□ □□ □□

Contoso□ □□□ □□ □□ □□□ □□□ □□□□□.

* □□ □□□ □□ □□□(SSPR)□ □□□□□.
* Azure Monitor□ □□□□ Azure □□ □□ □□□ □□□□□.
* □□□□ □□ □□□□ □□□□ □□ □□□□ □□□ □□□□□□.

* Fabrikam □□□□□ □□□□ □□ □□□ □□□□ □□□□□.
* □□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□□□□.
* App1□□□ □□□ □□□ □□ □□□ Azure □ □□ □□□□□. App1□ □□□□□ □□ □□□□ Azure AD □□□ □□□□ □□□□□.
* □□□ □□□ □□ □□□□ □□ Microsoft SharePoint Online □□□, □□ □ □□ □□ □□□ □□□ □□□□ □□ □□ □□□□□ □□□□□□.

Contoso□ Adatum Corporation□□□ □□□ □□□ □□□□□. 100□□ □□□ Adatum □□□□ Adatum□□□ □□□ Active Directory □□ □□(OU)□ □□□ □□□□□. □ □□□□□ □□□ □□□□ □□□□ □□□.

□□□□. □□□ □□□□

Contoso□ □□□ □□ □□ □□ □□□ □□□□□.

* □□ □□□□ AD DS□□ contoso.com Azure AD □□□□ □□□□□□ □□□.
* App1□ https://contoso.com/auth-response□ □□□□ □□□□ URI□ □□□ □□□.
* □□ □□□□ □□ □□□□ □□□ □□□□ □□□ □□□□ □□□□ □□□□□ □□□.
* Fabrikam □□□□ □□□ □□□ SharePoint □□□□ □□ 90□ □□ □□ □□□ □□□ □□□.
* Azure AD□□ □□□□ □□□ □□□ □□□□□ □□□. □□ □□□ 1□ □□ □□□□ □□□.
* □□□□□ □□□□ □□□ □□ □□□□ □□□□ □□□□ □□□□□ □□□ □ □□□ □□□.
* □□□□ □□□ □□□□□ □□□□ □□ □□, □□□□ □□□□□ □□□□□ □□□□□ □□□.

□□

□□□ □□□ □□ □□□ □□□□ □□□.

Azure AD □□□□ □□ □□□ □□ □□□?

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

Answer: D (LEAVE A REPLY)

You can add enable 'Guest Inviter' role. But you cannot enable self-service role for 'Office 365' apps. So far, that is only available for apps you build.

Reference:

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration-settings-configure#configure-settings-in-the-portal

https://learn.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-user-flow#enable-self-service-sign-up-for-your-tenant

NEW QUESTION: 152

□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

□□ □□□□ □□ □□ □□ □□□ □□□ □ □□□?

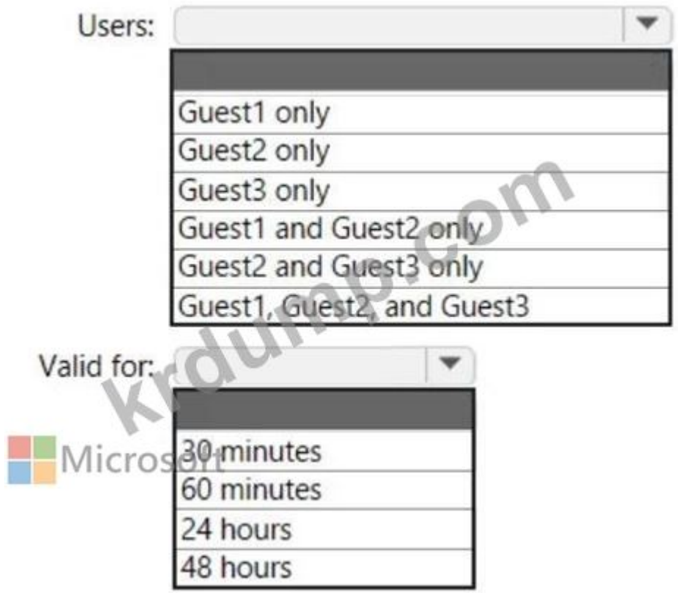
A. □□1, □□1 □ □□□□ □□
B. □□1□ □□
C. □□1, □1, □□□ □ □□1
D. □□ 1 □ □□□ □□
Answer: C (LEAVE A REPLY)
Access reviews require an Azure AD Premium P2 license.
Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.
Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

NEW QUESTION: 153
□□□ □□□ □□□ □□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□ □□ □□ □□ □ □□□ □□(SIEM) □□□□ □□□□ □□□ □□□ □□□□ □□□ □□□□□.
□□ □□□ □□□□ Azure AD □□□ □□□□□□ □□□. □□ □□□□ □□□ □□□ □□ □□ □□□ □□□□ □□□ □□□.
Azure AD□□ □□□ □□□□ □□□?
A. CSV □□□ □□ □□
B. CSV □□□ □□□ □□
C. JSON □□□ □□ □□
D. JSON □□□ □□□ □□
Answer: C (LEAVE A REPLY)
You can also choose to download the filtered data, up to 250,000 records, by selecting the Download button. You can download the logs in either CSV or JSON format.
You can use the JSON transform feature in the Power Query Editor in Excel to split each property in the JSON object in the AuditData column into multiple columns so that each property has its own column.
https://docs.microsoft.com/en-us/microsoft-365/compliance/export-view-audit-log-records?view=o365-worldwide

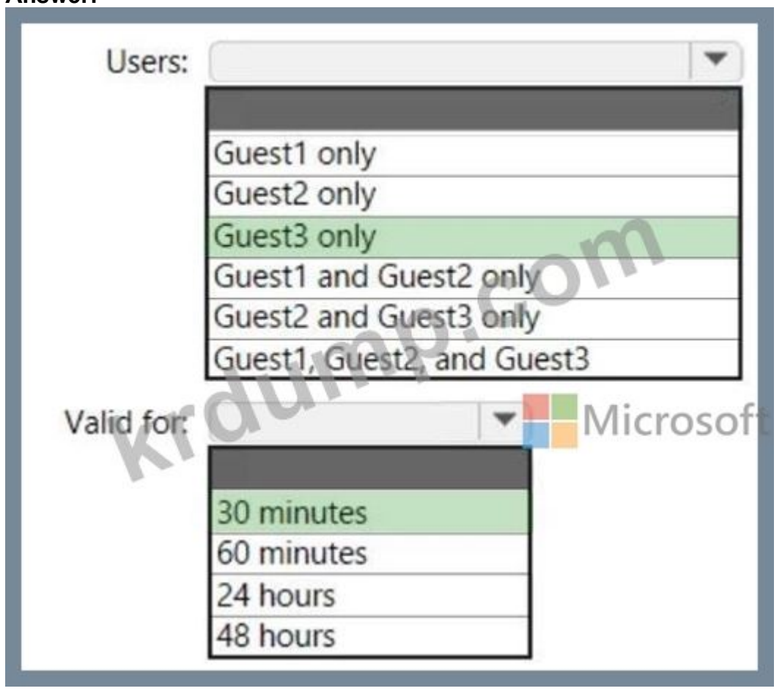
NEW QUESTION: 154
□□□ □□
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□, □□ □□□□ □□□□ □□□ □□□ □□ □□□ '□'□ □□ □□□□.
□□ □□ □□ □□ □□□ □□□□ □□□□□.

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

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



Answer:



Explanation:

Box 1: Guest3 only

When does a guest user get a one-time passcode?

When a guest user redeems an invitation or uses a link to a resource that has been shared with them, they'll receive a one-time passcode if:

They don't have an Azure AD account
They don't have a Microsoft account
The inviting tenant didn't set up federation with social (like Google) or other identity providers.
Box 2: 30 minutes
One-time passcodes are valid for 30 minutes. After 30 minutes, that specific one-time passcode is no longer valid, and the user must request a new one. User sessions expire after 24 hours.
After that time, the guest user receives a new passcode when they access the resource. Session expiration provides added security, especially when a guest user leaves their company or no longer needs access.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

NEW QUESTION: 155
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Active Directory □□□□□ □□□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
Active Directory□□ □□□ □□□ □□□□□ □□□□ □□□□□ □□□□ □□ 30□ □□ Azure AD□ □□□ □ □□□ □□ □□ □□□□□.
Active Directory□□ □□□ □□□ □□□□□□ □□ □□□ □□□ Azure AD□ □□□□ □□□ □□ □□□□ □□□.
□□□: □□□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Password writeback is a feature of Azure AD Connect which ensures that when a password changes in Azure AD (password change, self-service password reset, or an administrative change to a user password) it is written back to the local AD - if they meet the on-premises AD password policy.
Technically, a password write-back operation is a password "reset" action. Password writeback removes the need to set up an on-premises solution for users to reset their password. It all happens in real time, and so users are notified immediately if their password could not be reset or changed for any reason.
Reference:
https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html

NEW QUESTION: 156
□□□ □□ □□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
- Devie1□□□ □□□ □□
- □□□ □□□ User1, User2, User3, User4, User5□□□.
- □□1, □□2, □□3, □□4, □□5□□ □□□ □□ □□
□□□ □□ □□ □□□ □□ □□□□□.

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Assigned	User5

Microsoft 365 Enterprise E5 □□□□□ Group1□ □□□□ □ □□ □□□□□ □□□□□?

A. 0
B. 2
C. 3
D. 4
Answer: B (LEAVE A REPLY)
Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced#limitations-and-known-issues

NEW QUESTION: 157
Microsoft Entra □□□□ □□□ Azure □□□ □□□□. □□ □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Type	Membership type	Security enabled	Role assignment allowed
Group1	Security	Assigned	Yes	No
Group2	Security	Assigned	Yes	Yes
Group3	Microsoft 365	Assigned	Yes	Yes
Group4	Microsoft 365	Assigned	No	No

□□ □□ ID □□(PIM)□ □□□□ □□ □□□ □□□ □ □□□□?
A. □□2□ □□
B. □□1 □ □□2□ □□
C. □□2 □ □□4□ □□
D. □□1, □□2, □□3□ □□
E. □□1, □□2, □□3, □□4
Answer: (SHOW ANSWER)
* Group1 - Yes
Group1 is security enabled, role assignment is not allowed.
Group1 can be managed.
All security enabled groups can be manged by PIM.
Note: Groups in Microsoft Entra ID can be classified as either role-assignable or non-role- assignable. Additionally, any group can be enabled or not enabled for use with Microsoft Entra Privileged Identity Management (PIM) for Groups. These are independent properties of the group.
Any Microsoft Entra security group and any Microsoft 365 group (except dynamic membership groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. The group doesn't have to be role-assignable group to be enabled in PIM for Groups.
* Group2 - Yes
Group2 is security enabled, role assignment is allowed.
Group2 can be managed.
All security enabled groups can be manged by PIM.
* Group 3 - Yes
Group3 is security enabled, role assignment is allowed.
Group3 can be managed.
All security enabled groups can be manged by PIM.
* Group4 - No

Group4 is not security enabled.
Reference:
https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/concept-pim-for-groups

NEW QUESTION: 158
□□□□□
□□□ □□ □□ □□□ □□ □□□ □□□□□□.
□□□ □□□ □□□□□ □□□ □□□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□.
□□□□□ □□□□□ '□□□□ □□' □□□ □□□ □□ □□□ '□□□□'□ □□□□□.
Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com
Microsoft 365 □□: =1122334455667788
Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.
□□ □□□ □□ □□ □□□□□ □□□□□.
□□□ □□□□: 99999999
Microsoft Entra Identity Protection□ □□ □□ □□□ □□ □□□□ □□□.
- □□□□ □□ □ □□□ □□(MFA)□ □□□ □□□□□.
- □□□ □□□ □□□ □□ □□□□□ □□□ □□□□□.
□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□□.
Answer:

Microsoft Entra Identity Protection multi-factor authentication (MFA) for any sign-ins at the high risk level

Enable sign-in risk policy for MFA
Most users have a normal behavior that can be tracked. When they fall outside of this norm, it could be risky to allow them to successfully sign in. Instead, you might want to block that user, or ask them to perform a multifactor authentication. If the user successfully completes the MFA challenge, you can consider it a valid sign-in attempt and grant access to the application or service.

To enable this policy, complete the following steps:

Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select New policy.

Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

Step 5: Under Assignments, select Users or workload identities
Step 5a: Under Include, select All users.
Step 5b: Under Exclude, select Users and groups and choose your organization's emergency access or break-glass accounts.
[Select Mod Administrator]

Step 6: Under Cloud apps or actions > Include, select All cloud apps.

Step 7: Under Conditions > Sign-in risk, set Configure to Yes. Under Select the sign-in risk level this policy will apply to.
a. Select High.
b. Select Done.

Step 8: Under Access controls > Grant.
a. Select Grant access, Require multifactor authentication.
b. Select Select.

Step 9: Under Session. [Skip, do not need to specify sign-in frequency]

Step 10: Confirm your settings and set Enable policy to On.

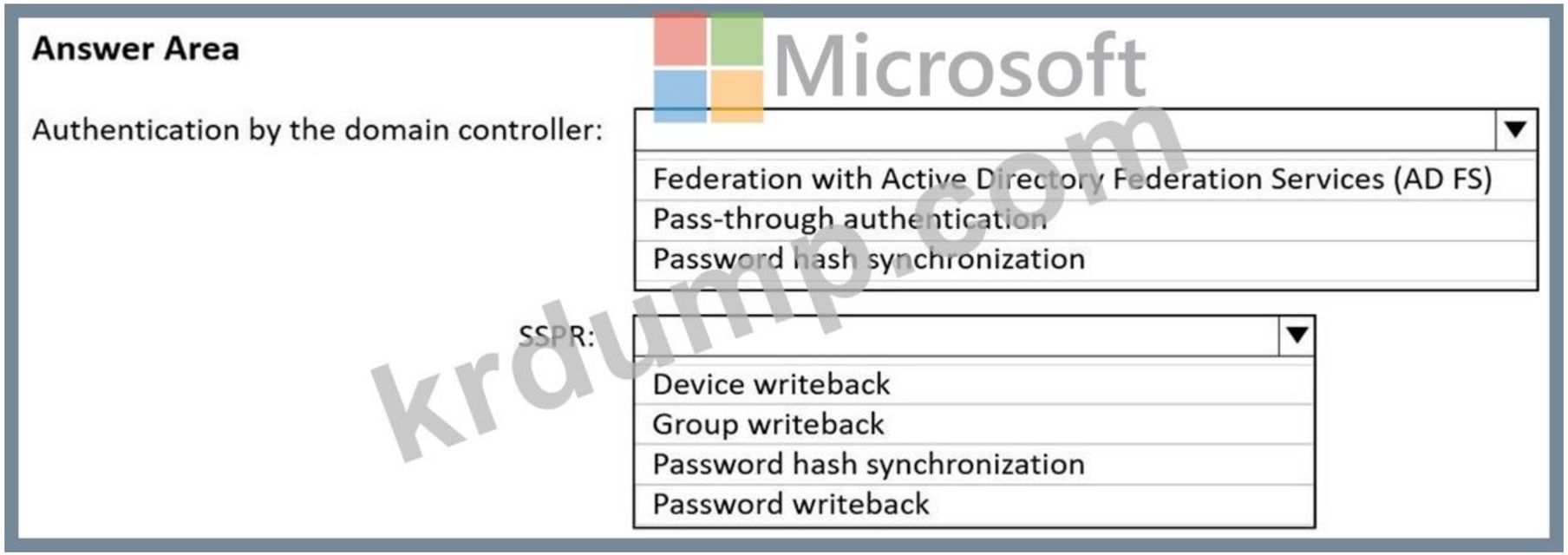
Step 11: Select Create to create to enable your policy.

Note: Use risk detections for user sign-ins to trigger Microsoft Entra multifactor authentication or password changes
To protect your users, you can configure risk-based Microsoft Entra Conditional Access policies that automatically respond to risky behaviors. These policies can automatically block a sign-in attempt or require extra action, such as require a secure password change or prompting for Microsoft Entra multifactor authentication. These policies work with existing Microsoft Entra Conditional Access policies as an extra layer of protection for your organization. Users might never trigger a risky behavior in one of these policies, but your organization is protected if an attempt to compromise your security is made.

Reference:
https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-risk-based-sspr-mfa

NEW QUESTION: 159

□□□ □□
□□□□□ □□□□□□□ Azure AD Connect□ □□□□ Azure AD □□□□ □□□□□ Active Directory □□□□ □□□□.
Azure AD Connect□ □□ □□ □□□ □□ □□□□ □□□.
- Azure AD□ □□ □□□ □□□□ Active Directory□ □□ □□□□□ □□□.
□□□□ □□□ □□□□.
- Active Directory □□□ □□□□ Azure AD □□ □□□□ □□□ □ □□□ □□□.
□□□ □□ □□□(SSPR).
□ □□ □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

NEW QUESTION: 160

Azure □□□ storage1□□□ □□□□ □□□ WebApp1□□□ □ □□ □□□□. WebApp1□ □□□ □□ □□ ID□ □□□□□.

WebApp1□ □□□□□ □□□ □□ ID□ □□□□ storage1□ □□□ □□ □ □ □□□ □□ □□□.

Azure □□□□ storage1□ □□ □□ □□□ □□□□ □□□?

A. □□□ □□

B. □□ □□□ □□(SAS)

C. □□□ □□(IAM) □□

D. □□ □□ □□

E. □□□ □

Answer: C (LEAVE A REPLY)

In the Azure portal, go into your storage account to grant your web app access. Select Access control (IAM) in the left pane, and then select Role assignments. You'll see a list of who has access to the storage account. Now you want to add a role assignment to a robot, the app service that needs access to the storage account. Select Add > Add role assignment to open the Add role assignment page.

https://learn.microsoft.com/en-us/entra/identity-platform/multi-service-web-app-access-storage?tabs=azure-portal%2Cprogramming-language-csharp#grant-access-to-the-storage- account

NEW QUESTION: 161

□□□ □ □□ □□

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

□□ □□□ □□□□ □□□.

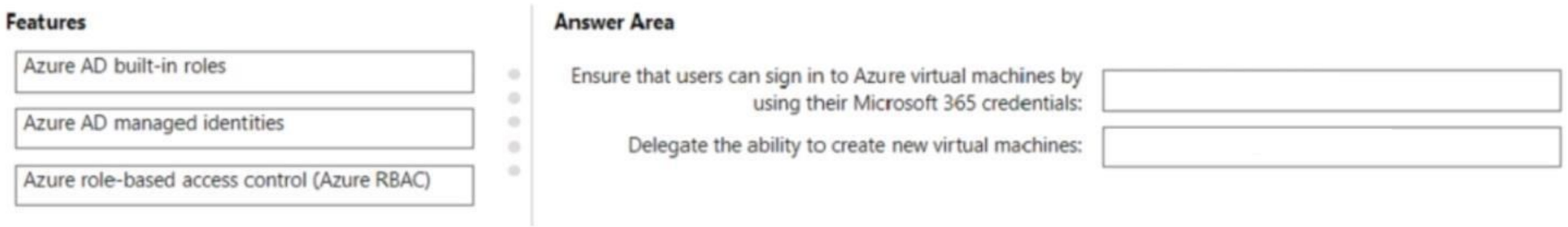
- □□□□ Azure □□ □□□ □□□□ □ □□□ □□□□□.

Microsoft 365 □□ □□.

- □□□ □□ □□□ □□□ □ □□ □□□ □□□□□.

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

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows#configure-role-assignments-for-the-vm

NEW QUESTION: 162

□□□□□

□□□ □□ □□ □□□ □□ □□□ □□□□□□.

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

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

Microsoft 365 □□□ □□: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 □□: =1122334455667788

Microsoft 365 □□□ □□□□□□ □□□ □□□□ □□□ Ctrl+K□ □□ □ □□□□ □□□ □□□ □□ □□□□□.

□□ □□□ □□ □□ □□□□□ □□□□□.

□□□ □□□□: 99999999

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

App1□ Microsoft Entra ID□ □□□□ □□□. □□□ □□□□ https//app1.contoso.com URI□ □□□□□□□ □□□.

□ □□□ □□□□□ □□ □□□ □□□ □□□□□□□.

Answer:

Register an application with the Microsoft identity platform
Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around. Once created, the application object can't be moved between different tenants.

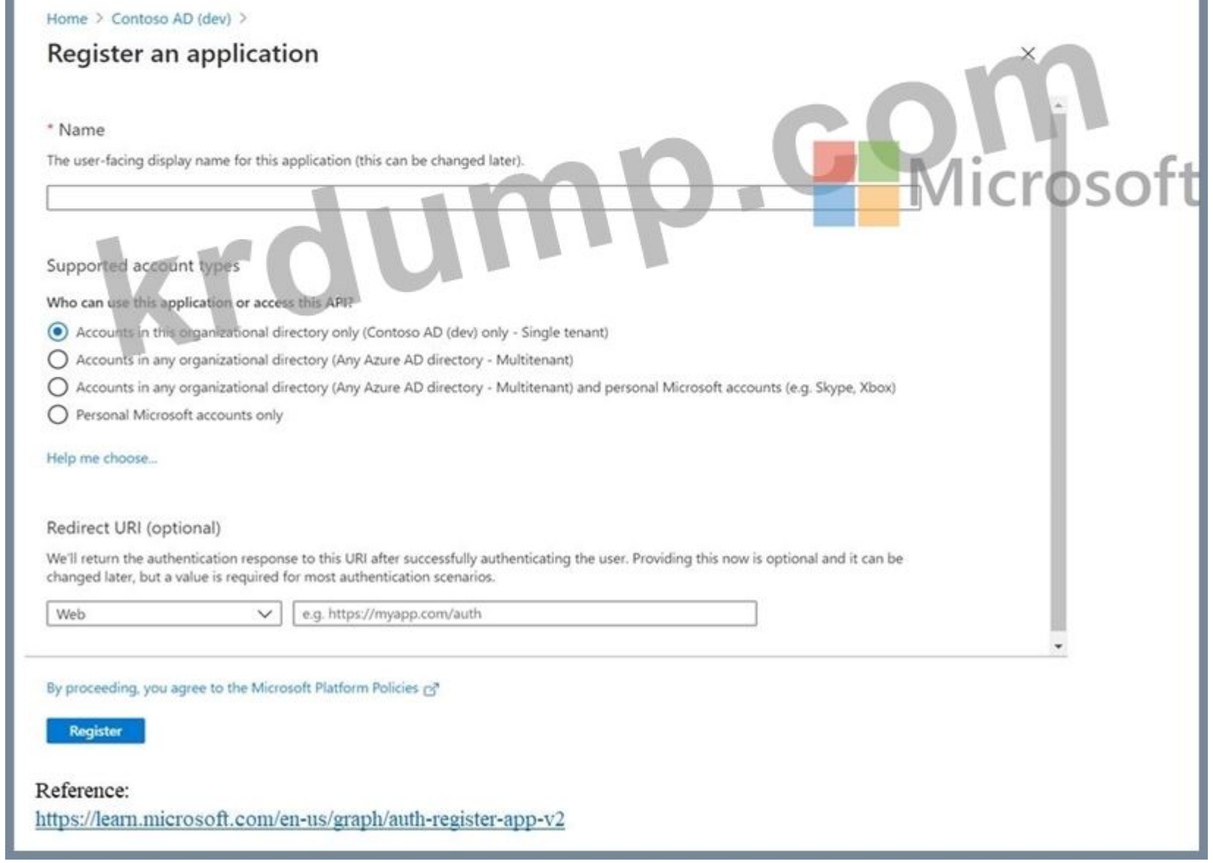
Specify who can use the application in the Supported account types section.
Step 1: Sign in to the Microsoft Entra admin center.

Step 2: If you have access to multiple tenants, use the Settings icon in the top menu to switch to the tenant in which you want to register the application from the Directories + subscriptions menu.

Step 3: Browse to Identity > Applications > App registrations and select New registration.

Step 4: Enter a display Name for your application. [Here: App1]

Step 5: Specify who can use the application in the Supported account types section.
Step 6: Redirect URI (optional). [Here: https//app1.contoso.com]
Step 7: Select Register to complete the initial app registration.



Reference:
https://learn.microsoft.com/en-us/graph/auth-register-app-v2

NEW QUESTION: 163
□□□ □□

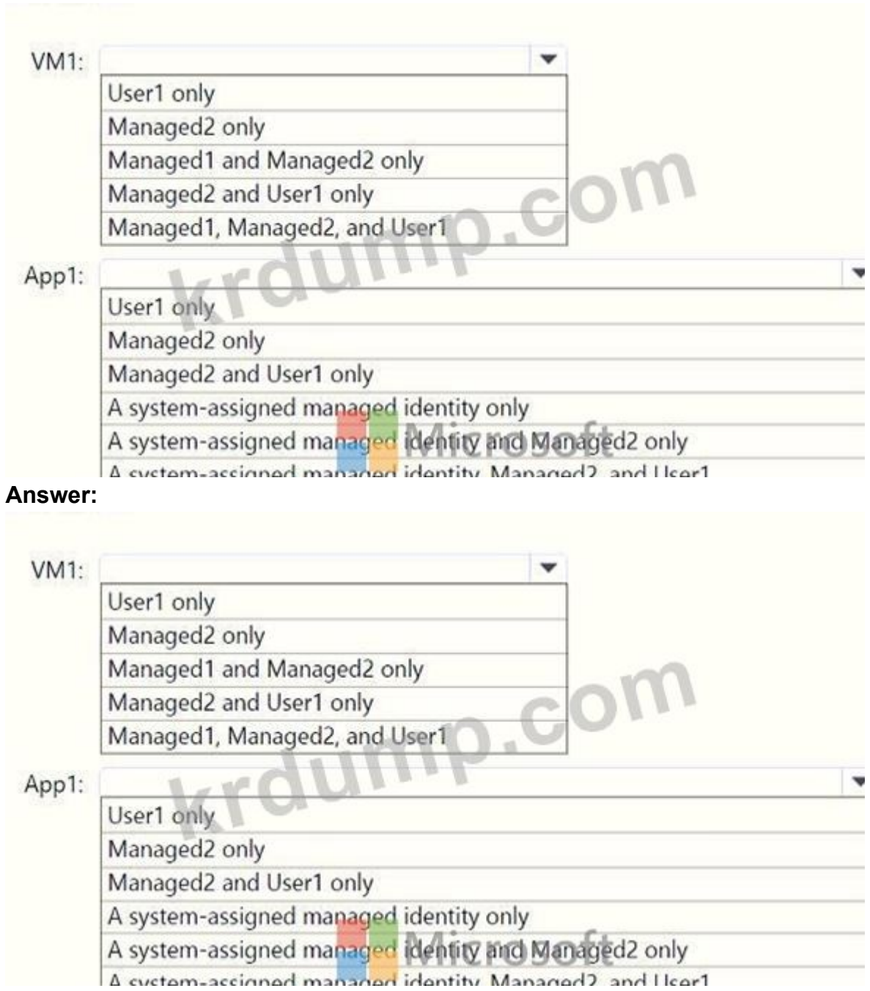
□□□ Azure □□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

Microsoft Entra□ User1□□□ □□□ □□□□ □□□□□.

VM1□ App1□ □□ ID□ □□□ □ □□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.



Answer:

NEW QUESTION: 164

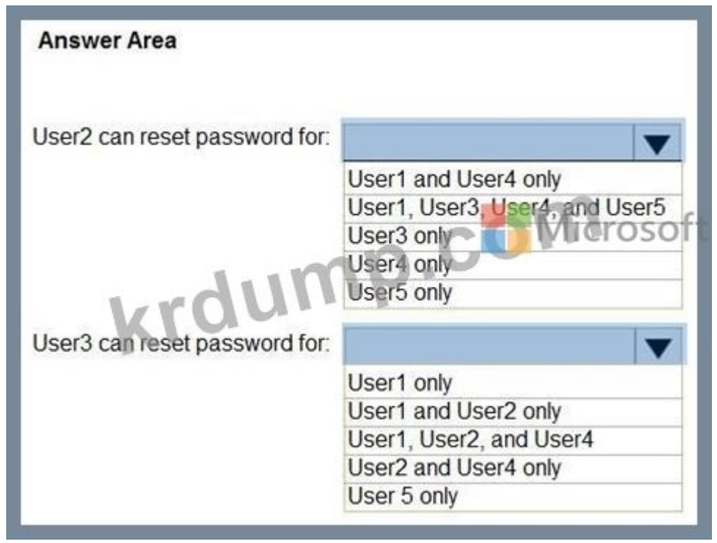
□□□ □□

□□□ AU1 □ AU2□□ □ □□ □□ □□□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

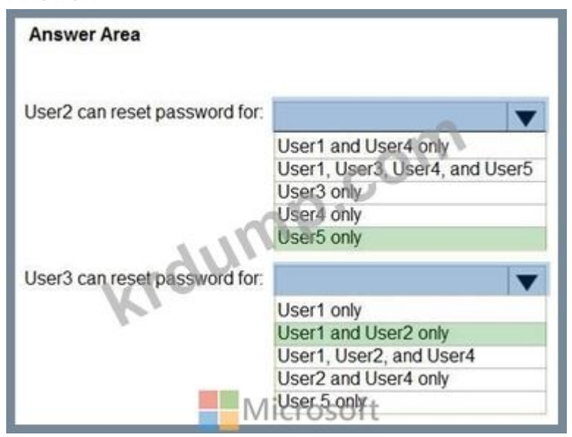
□□ □□ □□□ □□ 5□□ □□□□ □□□□□.

Name	Administrative unit	Role	Role scope
User1	AU2	Global Administrator	None
User2	AU2	Helpdesk Administrator	AU1
User3	AU1	Privileged Authentication Administrator	AU2
User4	AU1	Helpdesk Administrator	AU1
User5	AU1	None	None

User2□ User3□ □□ □□□□ □□□□□ □□□□ □ □□□□? □□□ □□□□□ □□□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:



NEW QUESTION: 165
□□□ □□□□ Microsoft 365 □□□□ □□□□.
□ □□□□ 300□□ □□□□ □□ □□□□ □□□□. □□□□□ □□□□ □□□□ □□□□ □□□□ □□ □□ □□□□ □□□ □ □□□□. □□□ □□□□ □□ □□□ □□ □□□□ □□□□□.

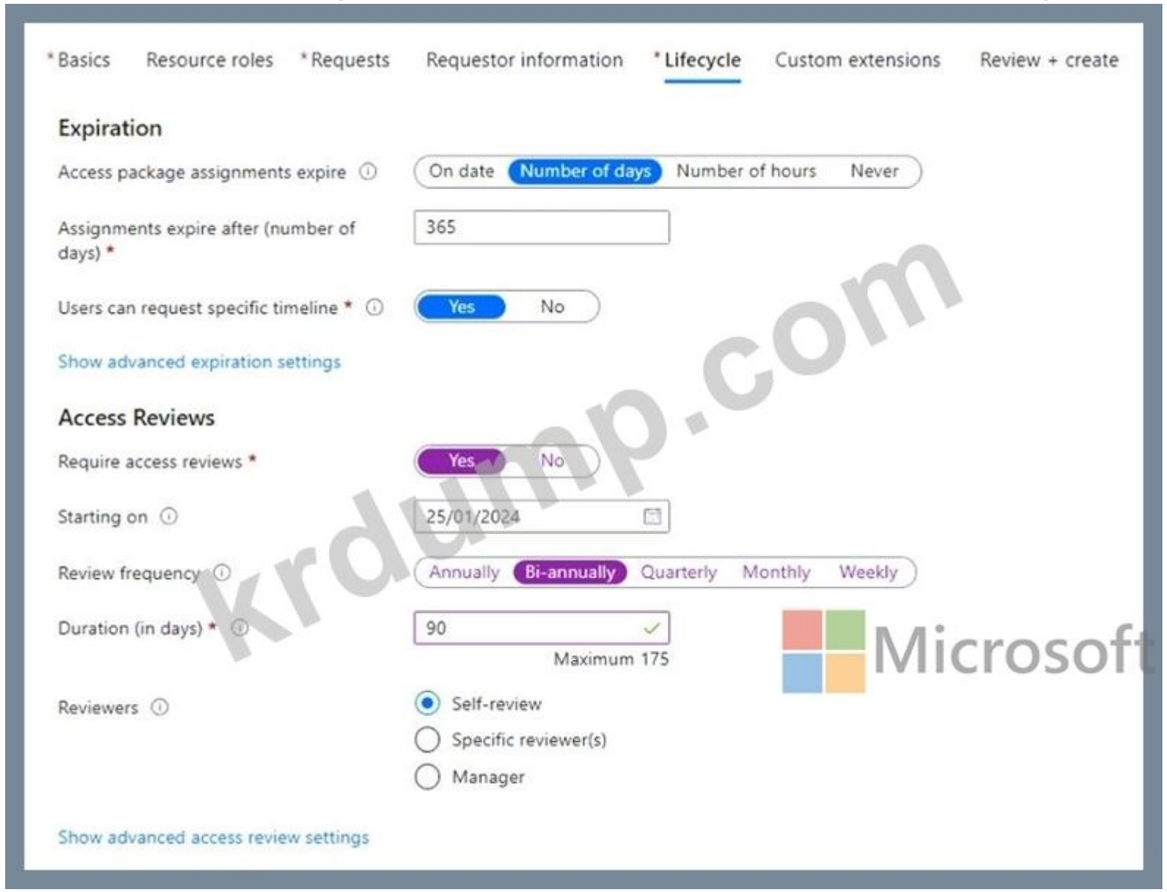
□□□ □□□□ □□□□ □□□□ □□□□ □□ □□□□ □□□□.
□□□ □□□□ Microsoft□ □□□□ □ □□ □□ □□(MFA)□ □□□□ □□□.
365
□□□.
□□□□ □□□ □□□□ □□□?
A. □□□ □□□□ □□
B. Microsoft Authenticator □
C. Windows Hello for Business □□
D. FIDO2 □□
Answer: (SHOW ANSWER)
FIDO2 security device (biometrics, PIN, and NFC)
User can access device based on organization controls and authenticate based on PIN, biometrics using devices such as USB security keys and NFC-enabled smartcards, keys, or wearables.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication- passwordless

NEW QUESTION: 166
□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
User1□ Azure AD □□□ □□ □□□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□ □□□
C. □□□ □□□
D. □□□ □□□ □□□
Answer: C (LEAVE A REPLY)
To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review#prerequisites

NEW QUESTION: 167
□□□ □□□ Microsoft 365 E5 □□□ App1□□□ □□ □□□□□□.
App1□ □□ Microsoft Defender for Cloud Apps □□□ □□□ □□□□ □□□.
□□□□ □□ □□□ □□ □□□?
A. □ □□ □□□ □□□□□ □□□ □□□ □□□ □□□□□.
B. App1□ □□ □□ □□□ □□□□□.
C. □□□ □□□ □ □□□ □□□□□ □□□ □□□ □□□ □□□□□.
D. App1□ □□ API □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 168
Microsoft Defender for Cloud Apps□ □□□□ Microsoft 365 □□□ □□□□ □□□□.
□□□ □□□ □□□□ □□□□ □□ □□ □□ □ □□□□.
□□ □□ □□ □□□ □□□□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □ □□ □□
C. OAuth □ □□
D. □□□□□ □□ □□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 169
Microsoft Entra □□□□ Package1□□□ □□□ □□□□ User1□□□ □□□□ □□□□. Package1□ □□ □□□ □□ □□□□ □□□□.



User1□ Package1□ □□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□ □□□.
User1□□ □□ □□□ □□□□ □□□?

A. □□ □□ □□ □□□
B. □□ ID □□□ □□□
C. ID □□ □□□
D. □□ □□□
Answer: C (LEAVE A REPLY)
Correct:
* Identity Governance Administrator
* User administrator
Check catalog for resources
If you need to add resources to an access package, you should check whether the resources you need are available in the access package's catalog. I' you're an access'package manager, you can't add resour'es to a catalog, even if you own them. You're restricte' to using the resources available in the catalog.
Prerequisite role: Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager.
In the Azure portal, select Azure Active Directory and then select Identity Governance.
In the left menu, select Catalog and then open the catalog.
In the left menu, select Resources to see the list of resources in this catalog.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources

NEW QUESTION: 170
□□□ □□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□.
□□ □□□□ Microsoft Entra Connect Sync□ □□□□ Microsoft 365 □□□ □□□□□□.
300□□ □ □□□□ □□□ □□□□□. □□□ □□ □□□ Microsoft Excel □□□□□□□ □□□□ □□□□.
□□□ □□ □□□□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
- □□□□ Microsoft 365□ □□□□ □□□□ □ □□□ □□□.
□□.
- □□□□ □□□□□□ □□ □□□□ □□□ □ □□□ □□□.
□□□.
- □□□ □□□ □□□□□□ □□□.
□□□□ □□ PowerShell cmdlet□ □□□□ □□□?
A. New-MgUser □ Get-Content
B. Set-MgUser □ Import-CSV
C. Set-ADUser □ Get-Content
D. New-ADUser □ Import-CSV
Answer: (SHOW ANSWER)
The two PowerShell cmdlets that should be used are Import-Csv and New-ADUser.
Import-Csv: Since the spreadsheet is saved as a Microsoft Excel document, you must first save it as a .csv file. This cmdlet imports the data from the CSV file into custom PowerShell objects so that the script can systematically loop through the 500 records.
New-ADUser: This cmdlet automates the creation of the user accounts in your on-premises Active Directory Domain Services (AD DS) environment.
Reference:
https://www.starwindsoftware.com/blog/creating-bulk-user-accounts-ad-via-powershell/

NEW QUESTION: 171
□□□ User1□ Vault1□□□ Azure □ □□ □□ □□□ □□□ Azure □□□ □□□□.
User1□ Vault1□ □□□ □□□, □ □ □□ □□□ □□□□□□ □□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □ □□ □□ □□□
B. □ □□ □□□ □□□
C. □ □□ □□
D. □ □□ □□□ □□□
Answer: (SHOW ANSWER)
The Key Vault Reader role is the minimum user role required to read the metadata of certificates, keys, and secrets stored in an Azure Key Vault. This role allows users to view the properties and attributes of these objects, but not to access their actual contents.
Reference:
https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide

NEW QUESTION: 172
□□□ Microsoft 365 E5 □□□□ □□□□.
□□□□ □□□ IP □□□□ Microsoft 365 □□□ □□□□ □□ □□ □□ □□(MFA)□ □□□□□ □□□□ □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□ □□
B. □□□ □□ □□
C. MFA □□ □□
Answer: (SHOW ANSWER)
Examples for Sign-In Risk:
- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

NEW QUESTION: 173
Microsoft Exchange □□□□ contoso.com□□□ SMTP □□ □□□ □□□□ □□□□.
□□ □□□□ Microsoft Entra □□ □□□ □□□ □□ contoso.com □□□ □□□ □□□□□.
□□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□ □□ □□□ □□□ □□ □□□.
contoso.com Microsoft Entra □□□□□ □□□□ Microsoft 365 □□□□ □□ □□□□ □□□□ □□ □□□ □□□ □□□□ □□□□ □□□□ □□□.
□□ PowerShell cmdlet□ □□□□ □□□?
A. □□□□-MgPolicyAuthorizationPolicy
B. MgDomain □□□□
C. Update-MgPolicyPermissionGrantPolicyExclude
D. MgDomainFederationConfiguration □□□□
Answer: A (LEAVE A REPLY)
Use the "Update-MgPolicyAuthorizationPolicy" cmdlet with the

"AllowedToSignUpEmailBasedSubscriptions" parameter set to False.
https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup

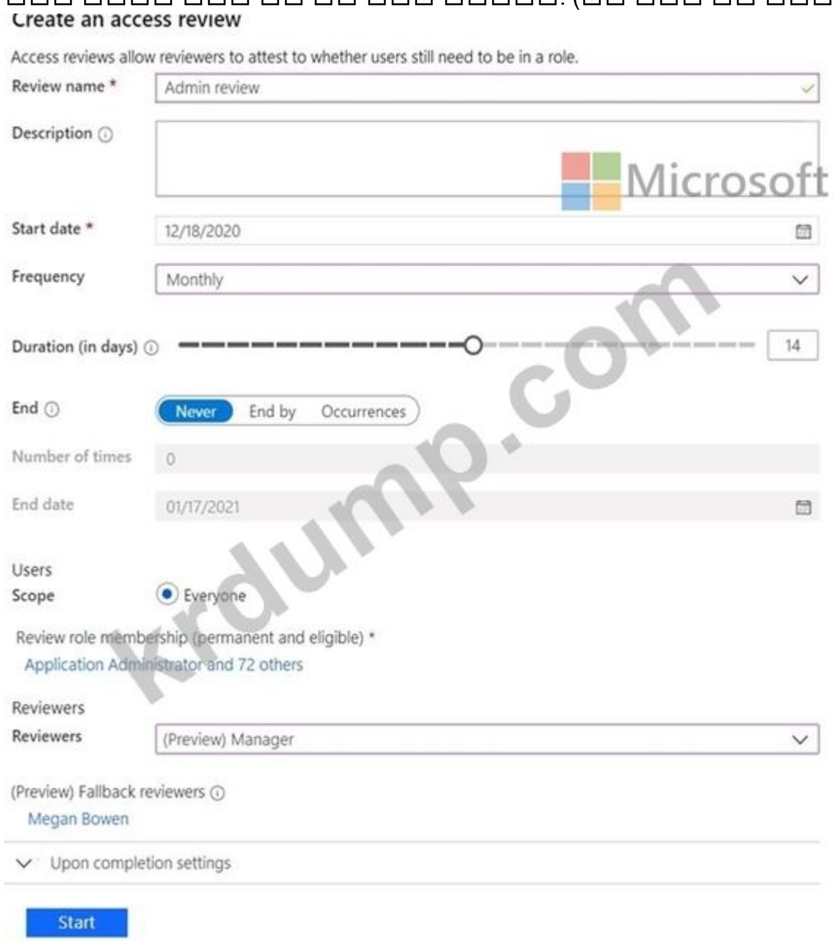
NEW QUESTION: 174
contoso.com□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
Azure AD □□ ID □□ □□□ □□ □□ □□□ □(MAU)□ □□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□
B. □□ □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)
To take advantage of MAU billing, your Azure AD tenant must be linked to an Azure subscription.
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing#what-do-i-need-to-do

NEW QUESTION: 175
□□□□□□ contoso.com□□□ Active Directory □□□□□ □□□□ □□□, □ □□□□□ Azure AD Connect□ □□□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□.
extensionAttribute15 □□□ NoSync□ □□□ □□□□ □□□□ □□□□ □□□.
Azure AD Connect□□ □□□ □□ □□□?
A. Windows Azure Active Directory □□□□ □□ □□□□ □□□ □□□ □□□□.
B. □□ □□□□ □□ □□□□ □□□□□.
C. Active Directory □□□ □□□ □□□□ □□ □□□□ □□□ □□□ □□□□.
D. □□□□ □□ □□□□ □□□□□.
Answer: (SHOW ANSWER)
You create an inbound rule because information is taken from Active Directory to Metaverse object.
Reference:
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these

NEW QUESTION: 176
Azure AD Privileged Identity Management(PIM)□ □□□□ Azure □□□ □□□□.
□□□□ □□□□□□ □□□ □□□ □□□ □□□□ □□□□ □□□.
Privileged Identity Management □□□□ □□ □□□□□ □□□□ □□□?
A. Azure AD □□
B. □□□ □□ □□□ □□
C. Azure □□□
D. □□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 177
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.

□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
Microsoft 365 □□□□ □□□□.
□□□□ 10□□ □□□ □□□ 100□□ IT □□□□ □□□□.
□□□ □□□□ □□□ □□ □□ □□□ □□□□□. (□□ □□□ □□ □□□□□.)



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

A. □

B. □□□

Answer: B (LEAVE A REPLY)

Each access review would still send review approval to Megan as no manager has been set for the user accounts under review.
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

NEW QUESTION: 178

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

Answer:

To automate this membership review, you must configure a Microsoft Entra ID Access Review through the Microsoft Entra admin center.

Step 1: Navigate to the Microsoft Entra admin center.

Open Access Reviews

Step 2: Expand the Identity Governance menu.

Step 3: Click on Access reviews.

Step 4: Select New access review.

Step 5: Select Teams + Groups for the review type.

Configure Scope

Step 6: Choose Select teams + groups.

Step 7: Find and select your specific group. [Select Project Falcon]

Step 8: Set scope to All users.

Step 9: Select Multi-stage review if needed, or leave it off for a standard single-stage review.

[Leave it as a standard single-stage review]

Step 10: Set quarterly Schedule

Step 11: Set the Frequency to Quarterly.

Step 12: Define a Duration (e.g., 14 days) for users to respond.

Step 13: Choose an End date or set it to Never to run indefinitely. [Choose Never] Step 14: Set the Select reviewers dropdown to Users review their own access. This forces the group members to self-attest.

Assign Reviewers

Step 15: Expand the Upon completion settings section.

Configure Automatic Removal

Step 16: Check the box for Auto apply results to resource.

Step 17: Set If reviewers don't respond to Remove access.

Step 18: Advanced settings allow you to enable Notifications and Reminders.

Finalize and Create

Step 19: Click Review + Create.

Step 20: Provide a Review name and description.

Step 21: Click Create to activate.

Reference:

https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-perform-roles-and-resource-roles-review

NEW QUESTION: 179

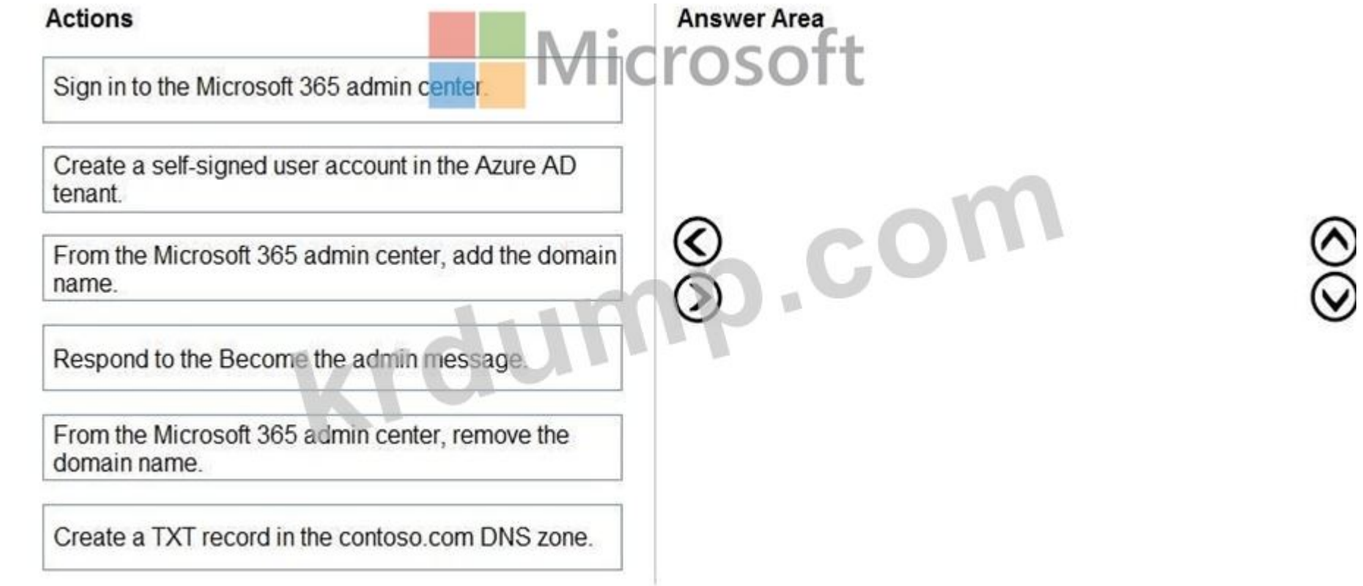
□□□ □ □□ □□

□□□ contoso.com□□□ SMTP □□ □□□ □□□□ □□□□□ Microsoft Exchange □□□ □□□□ □□□□.

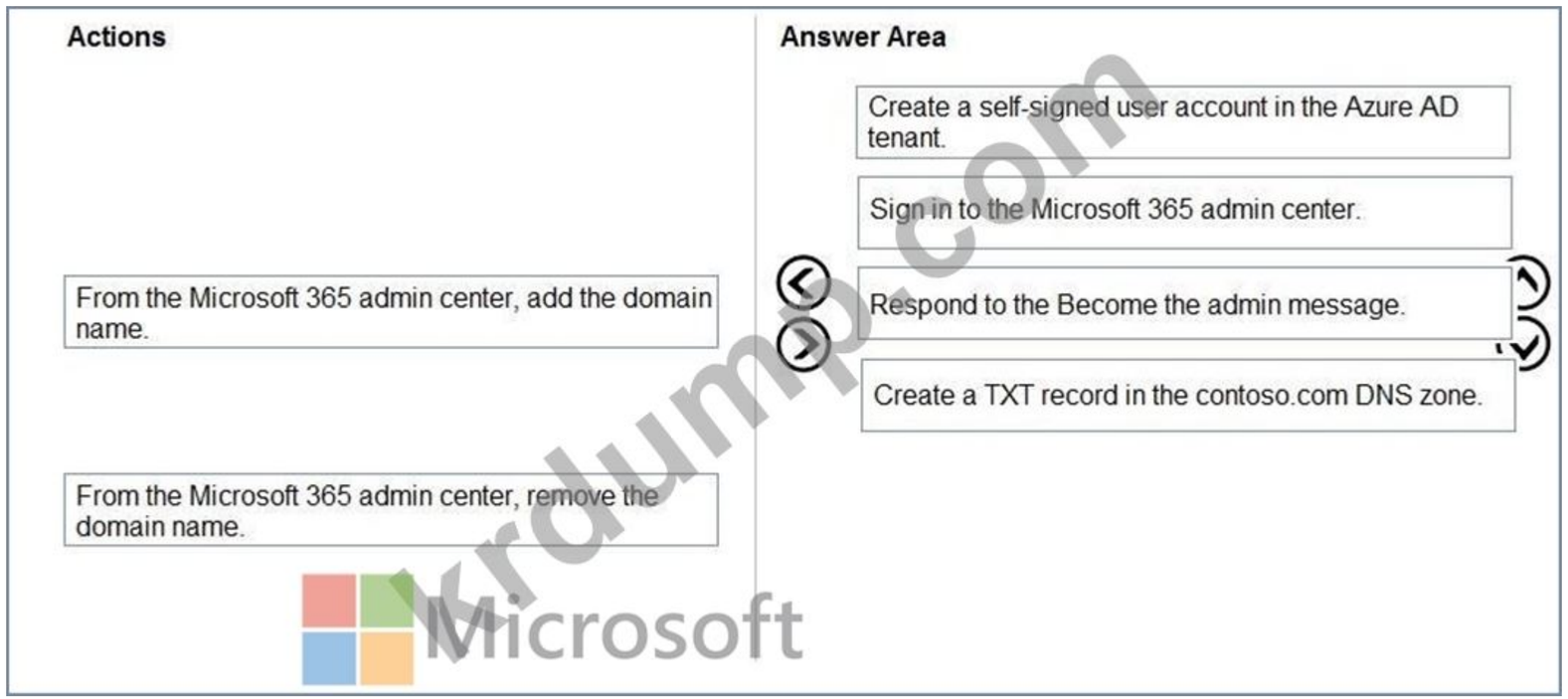
□□□□□ Microsoft 365 □□□□ □□ □□□□ □□□ □ □□□ □□□ □□□□ □□ □□□□□□.

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

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



Answer:



Explanation:

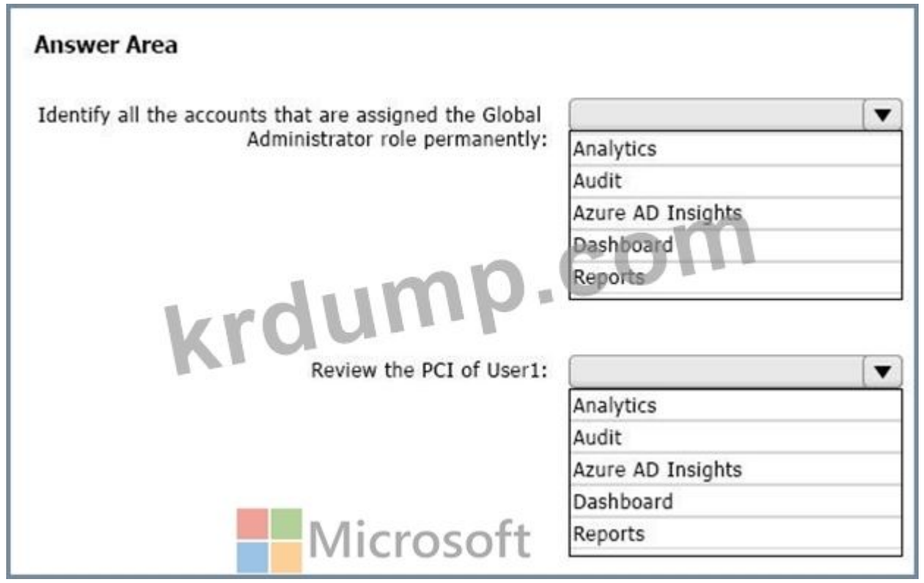
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

NEW QUESTION: 180
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □□□ □ □ □□□ □ □□□, □□□ □□ □□ □□ □ □□□□.
□ □□□□ □□□ □□□ □□□ □□ □□□□ □□□ □ □□□□. □□□ □ □□□□ □□ □□□ □□□□ □□□□.
Microsoft 365 □□□□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□ □ □□□ □□(MFA)□ □□ Microsoft Authenticator □□ □□□□ □□□.
□□ □□□□ □□□ □□□ □□□□ □□□□□ Microsoft Authenticator □□□ MFA(□□□ □□) □□□□ □□□□□□ □□□□□□.
□□□□ □□□ □□□□ □□ MFA □□□ □□□ □□ □□□□ □□ □□□□ □□□□ □□□.
□□ □□: Azure □□□□ □□□ □□(MFA)□ □□ □□□ □□/□□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
You need to configure the fraud alert settings.
Fraud alert setting literally has an option to configure it to automatically block.
To enable and configure fraud alerts, complete the following steps:
1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#fraud-alert

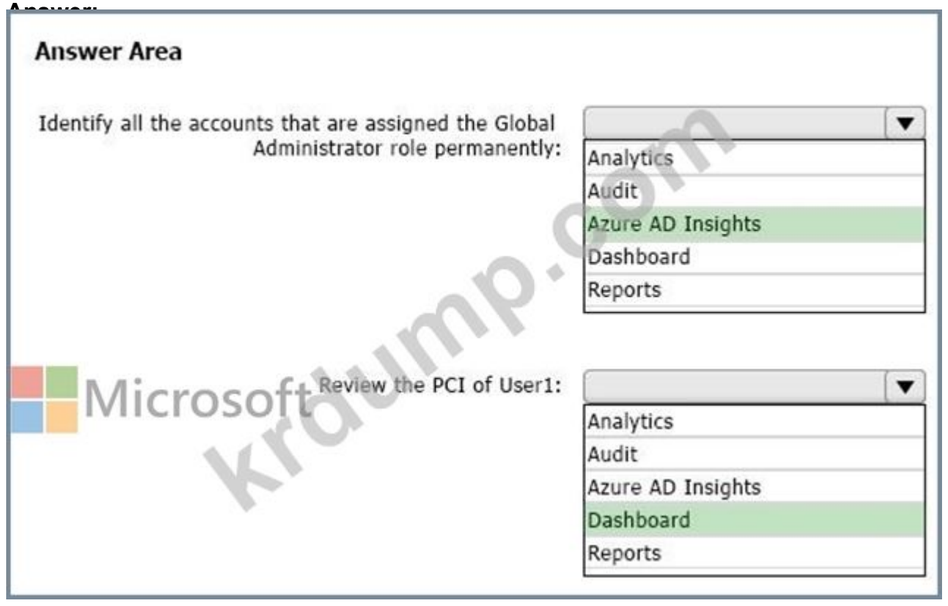
NEW QUESTION: 181
RG1□□□ □□□ □□□ User1, User2, User3, User4□□ □ □□ □□□□ □□□□ Azure □□□ □□□□. RG1□ □□ □□ □□□ □□□□□ □□□ □□□□□.
* User1: □□
* User2: □□□
* User3: □□□□ Blob □□□ □□
* User4: □□ □□ □□□
□□ □□ □□□ □□(ABAC) □□□ □□□□ □□□□. □□ □□□□ □□□ ABAC □□□ □□□□□?
A. □□□1
B. □□□2
C. □□□3
D. □□□4
Answer: C (LEAVE A REPLY)

NEW QUESTION: 182
□□□ □□

User1□□□ □□□□ □□□ Azure □□□ □□□□.
Microsoft Entra □□ □□ □□□ □□□□□□.
□□ □□□ □□□□ □□□.
- □□□ □□□□ □□□ □□ □□□ □□□□□.
□□□□□□.
- User1□ □□ □□ □□(PCI)□ □□□□□□.
□□ □□□□ □ □□□ □□ □□ □□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.



Answer:



NEW QUESTION: 183
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□, □ □□□□ App1□□□ Azure AD □□□□□□ □□□□□□□ □□□□ □□□□.
□□□□ user1@outlook.com□ □□ □□□ □□□□□.
□□□□□ App1□ □□ □□□ □□□ □□□ □ □□□ □□□□ □□□. □□□□ user1@outlook.com□□ □□□ □ □□□ □□□.
□□□ □□ □□□?
A. New-AzureADMSInvitation cmdlet□ □□□□□.
B. □□ □□ □□□ □□□□□.
C. WS-Fed ID □□□□ □□□□□.
D. Azure AD Connect□ □□□□□.
Answer: A (LEAVE A REPLY)
By default, all users in your organization, including B2B collaboration guest users, can invite external users to B2B collaboration. If you want to limit the ability to send invitations, you can turn invitations on or off for everyone, or limit invitations to certain roles.
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-collaboration- settings-configure

NEW QUESTION: 184
Azure Active Directory(Azure AD) □□□□ □□□□.
□□□ □□□ □□□□□ □ □□□ □□ 25□□ □□ □□□□ □□□.
□□□ □□□ □□□□ □□□ □□□□□?
A. displayName, identityIssuer, usageLocation □ userType
B. accountEnabled, givenName, surname □ userPrincipalName
C. accountEnabled, displayName, userPrincipalName □ passwordProfile
D. accountEnabled, passwordProfile, usageLocation □ userPrincipalName
Answer: (SHOW ANSWER)
Name [displayName] -> Required
User name [userPrincipalName] -> Required
Initial password [passwordProfile] -> Required,
Block sign in (Yes/No) [accountEnabled] -> Required
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-bulk-add

NEW QUESTION: 185
□□□ User1□ RG1, RG2□□ □ □□ □□□ □□□ □□□ Azure □□□ □□□□.
User1□ □□ □□□ □□□ □ □□□ □□□□ □□□.
- □□ □□□ □□□□□.
- □□ □□□ □□□□□□.
- RG1□□□ □□ □□□ □□□□□□.
- RG1□□□ □□□□ □□□ □□□□□.
□□ □□ □□ □□(RBAC)□ □□□ □□ □□ □□ □□ □ □□□□?
A. 1
B. 2
C. 3
D. 4

Answer: C (LEAVE A REPLY)
Assign User1 the "Reader" role at the subscription level to view all resources.
Assign User1 the "Virtual Machine Contributor" role at the RG1 level to restart virtual machines and create virtual machines in RG1 only.
Assign User1 the "Storage Account Contributor" role at the RG1 level to create storage accounts in RG1 only.

NEW QUESTION: 186
□□□ Microsoft 365 □□□□ □□□□ □□ □□□ □□□□ contoso.com□ □□□□□ □□□□□.
□□□ □□□ □□□ □□□□ Microsoft 365 □□□□ □□ □□□□ □□□ □ □□□ □□□□ □□□.
□□□ □□ □□ □□□?
A. Azure AD □□□□ □□ □□ □□□ □□□□□.
B. □□□ □□ □□□ □□□□□□□.
C. □□ □□ □□□ □□□□□□□.
D. □□ □□ □□(MFA) □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 187
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

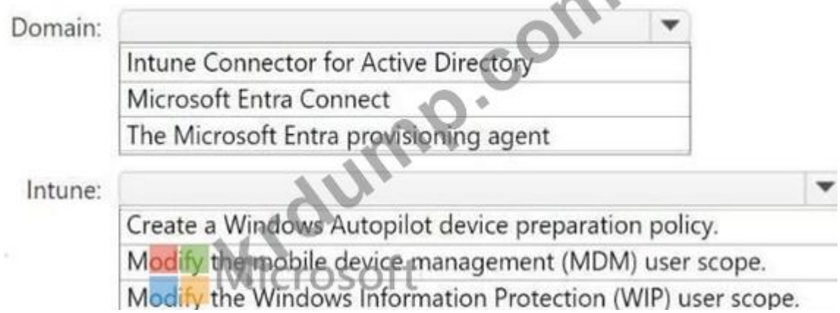
Name	Role
User1	User Administrator
User2	Password Administrator
User3	Security Reader
User4	User

□□ □□□□ □□ SSPR(□□ □□□ □□□□ □□□)□ □□□□□ SSPR□ □□ □□□ □□□ □□ □□□□ □□□□□ □□□□□.
□□ □□□□ □□□□□ □□□□ □ □□ □□□ □□□□ □□□?
A. User4□
B. User3□ User4□
C. User1□ User4□
D. User1, User3, User4□
E. User1, User2, User3, User4
Answer: (SHOW ANSWER)
Basically, some administrative roles, by design can only use strong, two-gate password reset policy, regardles of SSPR settings.
User Administrator and Password Administrator will be always forced to use two methods and cannot use security questions.
Securiry Reader and User will use whatever is set under SSPR, so security questions in this case.
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr- policy#administrator-reset-policy-differences

NEW QUESTION: 188
□□□ □□
□□□□□ □□□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□□ Windows 11□ □□□□ □□□□ □□□□ □□□□.

□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
□□□□□ □□□ □□□□□ □□□□ Microsoft Intune□ □□□ □□□□□.
□□□□ □□□□ □ □□□□□□ Intune□□ □□□□ □ □□□ □□□□ □□□.
□□ □□□ □□□ □□□□ □□□? □□□□□ □□□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area



Answer:

Answer Area

Explanation:
Box 1: The Intune Connector for Active Directory
Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot Intune connector server requirements
* The Intune Connector for Active Directory must be installed on a computer that's running Windows Server 2016 or later with .NET Framework version 4.7.2 or later.
* The server hosting the Intune Connector must have access to the Internet and Active Directory.
Box 2: Modify the mobile device management (MDM) User scope
Set up Windows automatic MDM enrollment
1. Sign in to the Azure portal and select Microsoft Entra ID.
2. In the left hand pane, select Manage | Mobility (MDM and WIP) > Microsoft Intune.
3. Make sure users who deploy Microsoft Entra joined devices by using Intune and Windows are members of a group included in MDM User scope.
4. Use the default values in the MDM Terms of use URL, MDM Discovery URL, and MDM Compliance URL boxes, and then select Save.
Reference:
https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid

NEW QUESTION: 189

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

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

□□ □□□□ □ □□□ □□□ □ □□□□.

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

□□ □□□□ □□ □□□ □□□ □□□□ □□□□.

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

A. □□□1

B. □□□2

C. □□□3

D. □□□4

Answer: (SHOW ANSWER)

User2 is the only one who has access to Application.write for the calendar.

NEW QUESTION: 190

□□□ □□

Azure Active Directory(Azure AD) □□□□ App1□□□ □□□ Azure □ □□ □□□□.

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

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

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

□ □□ □□□ □□ Azure Active Directory □□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.

□□: □□ □□□ 1□□□□.

Answer Area

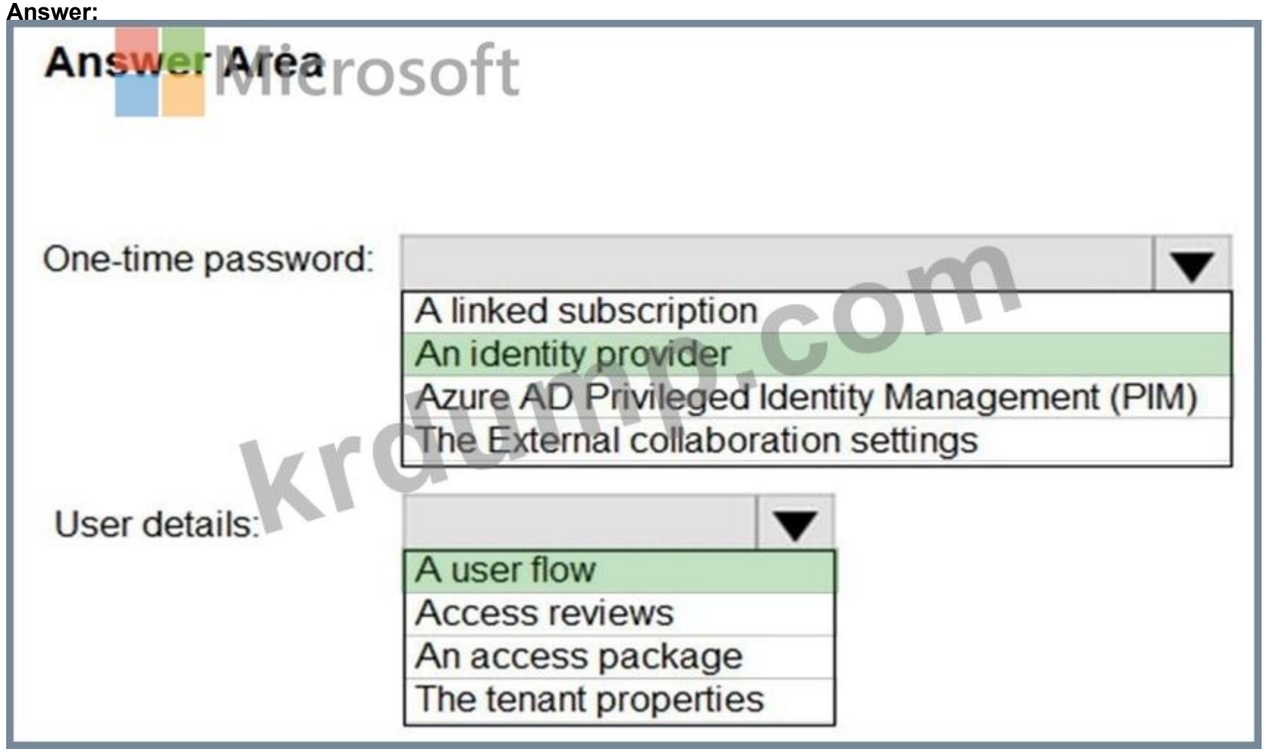
One-time password:

- A linked subscription
- An identity provider
- Azure AD Privileged Identity Management (PIM)
- The External collaboration settings

User details:

- A user flow
- Access reviews
- An access package
- The tenant properties

Answer:



Explanation:

Box 1: Identity Provider
First you'll enable self-service sign-up for your tenant and federate with the identity providers you want to allow external users to use for sign-in.
Box 2: User Flow
Then you'll create and customize the sign-up user flow and assign your applications to it.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/identity-providers
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/self-service-sign-up-overview

NEW QUESTION: 191
□□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Review1□□□ □□□ □□□ □□□ □□□□□. Review1□ 6□□□□ Microsoft□□ □□□□ □□□.
365 □□ □□□□ □□□ □□□□ □□ □□□ □□□ □□□ □ □□□□.
□□ □□□□ Review1□ □□□□ □□□□ □□ □□ □□□ □□□□ □□□□ □□□□□ □□ □□□.
Review1□ □□ □□ □□□ □□□□ □□□?
A. □□□
B. □□
C. □□ □□
D. □□ □□ □
Answer: (SHOW ANSWER)
* When completed
* Upon completion settings
Incorrect:
* Advanced settings
* General
* Reviewers
* Scheduling
Note: See step 5 below.
Ask guests to review their need for access, in general
In some organizations, guests might not be aware of their group memberships.
1. Create a security group in Microsoft Entra ID with the guests as members, if a suitable group doesn't already exist.
2. To create a' access review for that group, select the reviewers to be the members themselves.
3. Ask each guest to review their own membership. By default, each guest who accepted an invitation receives an email from Microsoft Entra ID with a link to the access review in your organization's access panel.
4. After the reviewers give input, stop the access review.
5. You can automatically delete the guest users Microsoft Entra B2B accounts as part of an access review when you're configuring an Access review for Select Team + Groups. This option isn't available for All Microsoft 365 groups with guest users.

To do so, select Auto apply results to resource as this will automatically remove the user from the resource. If reviewer don't respond should be set to Remove access and Action to apply on denied guest users should also be set to Block from signing in for 30 days then remove user from the tenant.

Reference:
https://learn.microsoft.com/en-us/entra/id-governance/manage-guest-access-with-access-reviews

NEW QUESTION: 192

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

Name	Group
User1	Group1
User2	Group1
User3	Group2
User4	Group2
User5	*None*

Au1□□□ □□ □□□ □□□□. Group1, User2, User3□ Au1□ □□□□□□.

User5□□□ Au1□ □□ □□□ □□□ □□□ □□□□□□□.

User5□ □□ □□□□ □□□□□ □□□□ □ □□□?

A. □□□1, □□□2, □□□3

B. □□□1□ □□□2□ □□

C. □□□3 □ □□□4 □□

D. □□□2 □ □□□3□ □□
Answer: D (LEAVE A REPLY)
Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but not the members of the group. In other words, an administrator scoped to the administrative unit can manage properties of the group, such as group name or membership, but they cannot manage properties of the users or devices within that group (unless those users and devices are separately added as members of the administrative unit).
https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units

NEW QUESTION: 193
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □□ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.
Amazon Web Services(AWS) □□, Google Workspace □□, GitHub □□□ □□□□. Azure □□□ □□□□ Microsoft 365 Defender□ □□□□□□.
□□□□ □□ Microsoft Defender□ □□□□ OAuth □□ □□□ □□□□□ □ □□□ □□□□ □□□.
□□□: Microsoft 365 Defender □□□□ GitHub □ □□□□ □□□□□. □□□□ □□□ □□□ □ □□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
Adding the GitHub app connector to Microsoft Defender for Cloud Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

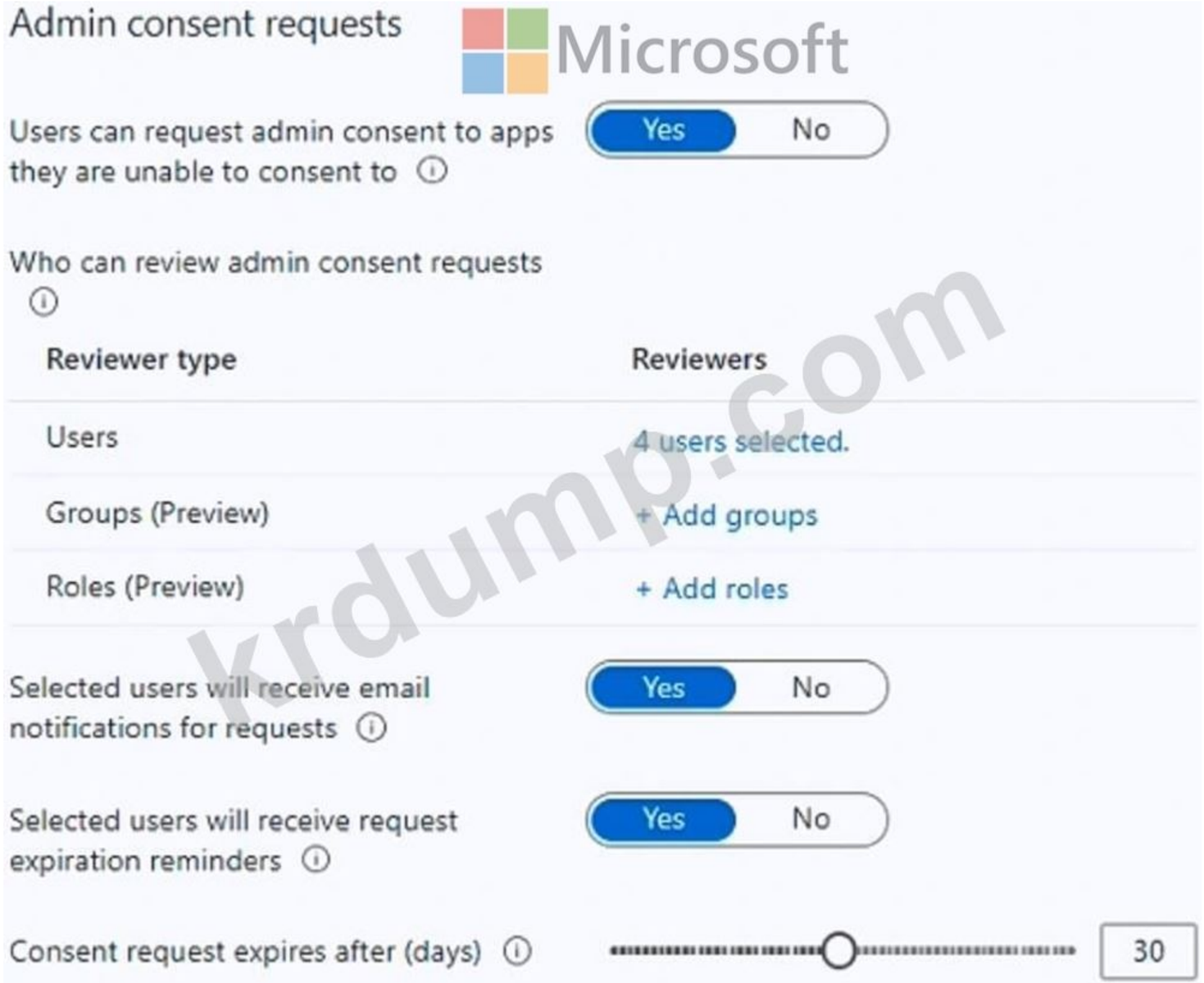
NEW QUESTION: 194
□ □□□ □□□□□ Active Directory□ Microsoft Entra ID□ □□ □□□□ □□□□□ □□□ □□□□□□. IT □□□□ □□□□□ □□□□□□ □□□□□ □□□ □□□ □ □□ □□□□□ □□ □□ □□□□□□.
Active Directory□ Microsoft Entra ID□ □□□□□ □□□ □□□□ □□□.
□ □□□ □□□□ □□ □□ □□ □□ □ □□ □□□□□?
A. □□□□□□ Microsoft Entra ID □□ □□□□ □□□ □□□□□□.
B. Microsoft Entra Connect □□□ □□□ □□□□□
C. Microsoft Entra Connect Health □□□ □□□ □□□□□
D. □□□ □□□□ □□ □□□□ □□□□□□.
Answer: C (LEAVE A REPLY)
You should check the Microsoft Entra Connect Health sync status as the very first step to troubleshoot the issue. Microsoft Entra Connect Health is a feature of Microsoft Entra ID that allows you to monitor and troubleshoot the directory synchronization between your on-premises Active Directory and Microsoft Entra ID. To do this, you would check the Microsoft Entra Connect Health dashboard seeing as it provides real-time monitoring and alerting for the synchronization service, including the status of the sync engine, the number of objects synced, and any errors that may have occurred. By checking the Microsoft Entra Connect Health dashboard and identifying the root cause of the issue, the IT administrator can then take the appropriate steps to resolve the issue and re-establish the sync between on-premises Active Directory and Microsoft Entra ID.
Your first step should not be to check the Event Viewer for error messages. The very first step to troubleshoot the issue with Microsoft Entra Connect should be to check Microsoft Entra Connect Health sync status in a centralized dashboard to identify the root cause of the issue. Only after this first step should you check the event log on the server running the Microsoft Entra Connect to see if there are any relevant events or errors that may be related to the syncing issue.
You should not check the Microsoft Entra Connect sync configuration as the very first step to troubleshoot the issue. Verifying the Microsoft Entra Connect sync configuration is one of the next steps during the troubleshooting. In this step you should check the Microsoft Entra Connect sync service and ensure that it is running and configured correctly. If the service is stopped, the administrator should start it again and check the configuration to ensure that it is correct.
You should not check the network connectivity between the on-premises and Microsoft Entra ID as the very first step to troubleshoot the issue. The first step is to identify the root cause of the issue. If the issue is related to network connectivity, the administrator should check the network connection between the on-premises and Microsoft Entra ID environments to ensure that there is no problem with it, such as a firewall restriction.

NEW QUESTION: 195
Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□□□ □□□ □□□□□□ Microsoft Exchange Online□ □□□ □ □□□ □□□□ □□□□.
□□□□ □□ □□ □□□□□ □□□□ □□□ □□□□□□□□ Exchange□ □□□ □ □□□ □□ □□□.
□□□ □□□□ □□□?
A. Microsoft Defender for Cloud Apps□ OAuth □□
B. Azure Active Directory(Azure AD)□ □□□ □□□ □□
C. Microsoft Endpoint Manager□ □□ □□ □□
D. Microsoft Endpoint Manager□ □□□□□□ □□ □□□
Answer: B (LEAVE A REPLY)
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

NEW QUESTION: 196
□□ □□ □□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	None

Azure AD□ App1□□□ □□□□□□ □□□□□□□ □□□□ User1□ App1□ □□□□ □□□□□.
App1□ □□□□□ Azure AD□ □□□□□ □□ □□□ □□□ □□□□□.
□□ □□□ □□ □□□ □□ □□ □□□ □□□□□.



Admin1, Admin2, Admin3 □ '□□□'□ □□□□ □□□□□□□.
□□ □□□□ □□□ □□ □□□ □□□□ □□□ □ □□□□?

A. □□□1 □□

B. □□□1, □□□2, □□□3□ □□

C. □□□1, □□□2 □ □□□1□ □□

D. □□□1 □ □□□2 □□

E. Admin1, Admin2, Admin3 □ User1

Answer: (SHOW ANSWER)
To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

NEW QUESTION: 197
□□□ □□
□□□ Azure □□□□ □□□ □□ □□ □□□ □□□□ □□□□.
- □□: V1
- Azure □□: □□ □□
- □□□□□ □□□ □□ ID: □□ □ □
□□ □□ □□□ □□ ID□ □□□□□.

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

□□□ □□ □□□ □□□□□.
- Managed1□ V1□ □□□□□.
- □□ □□ □□□ RG1□□□ □□□ □□□ □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	○	○
You can assign Managed3 to V1.	○	○
You can assign VM1 the Owner role for RG1.	○	○

Answer:

Answer Area

Statements	Yes	No
You can assign Managed2 to V1.	○	○
You can assign Managed3 to V1.	○	○
You can assign VM1 the Owner role for RG1.	○	○

Explanation:

You can use user assigned managed identities in more than one Azure region.

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq#can-the-same-managed-identity-be-used-across-multiple- regions

NEW QUESTION: 198

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

Name	Role
User1	None
User2	None
Admin1	Application administrator
Admin2	Authentication administrator

□□□ □□□□□□□ □□□ □□□ □□□ □□ □□□ □□□□.

- □□□□ □□ □□□ □□□□ □□ □□□□ □□□□ □□ □□□ □ □□□□: □□□
- □□□□ □□□ □□□ □□□ □□ □□□□ □□ □□ □□□ □□□ □ □□□□: □□□
- □□□□ □□□ □□□ □ □□ □□ □□ □□□ □□□ □□□ □ □□□□: □
- □□□ □□ □□□ □□□ □ □□ □□□: Admin2, User2

User1□ □□ □□□ □□□ □□□ □□□ □□ □□□□□ □□□□□.

□□ □□□□ □□□ □□□ □ □□□?

A. □□□1

B. □□□2

C. □□□1

D. □□□2

Answer: C (LEAVE A REPLY)

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

NEW QUESTION: 199

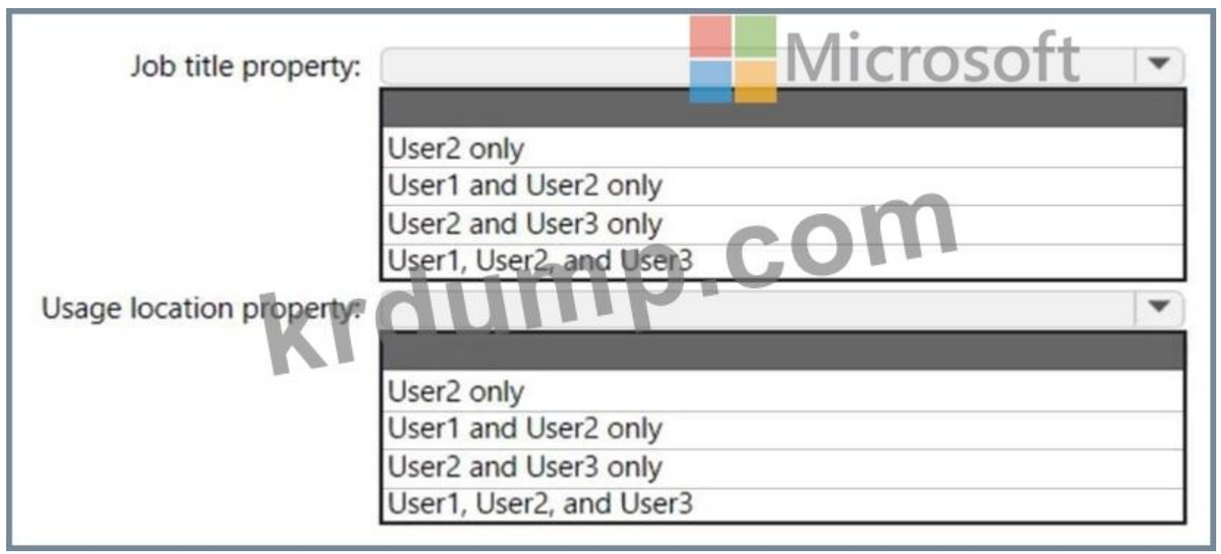
□□□ □□

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

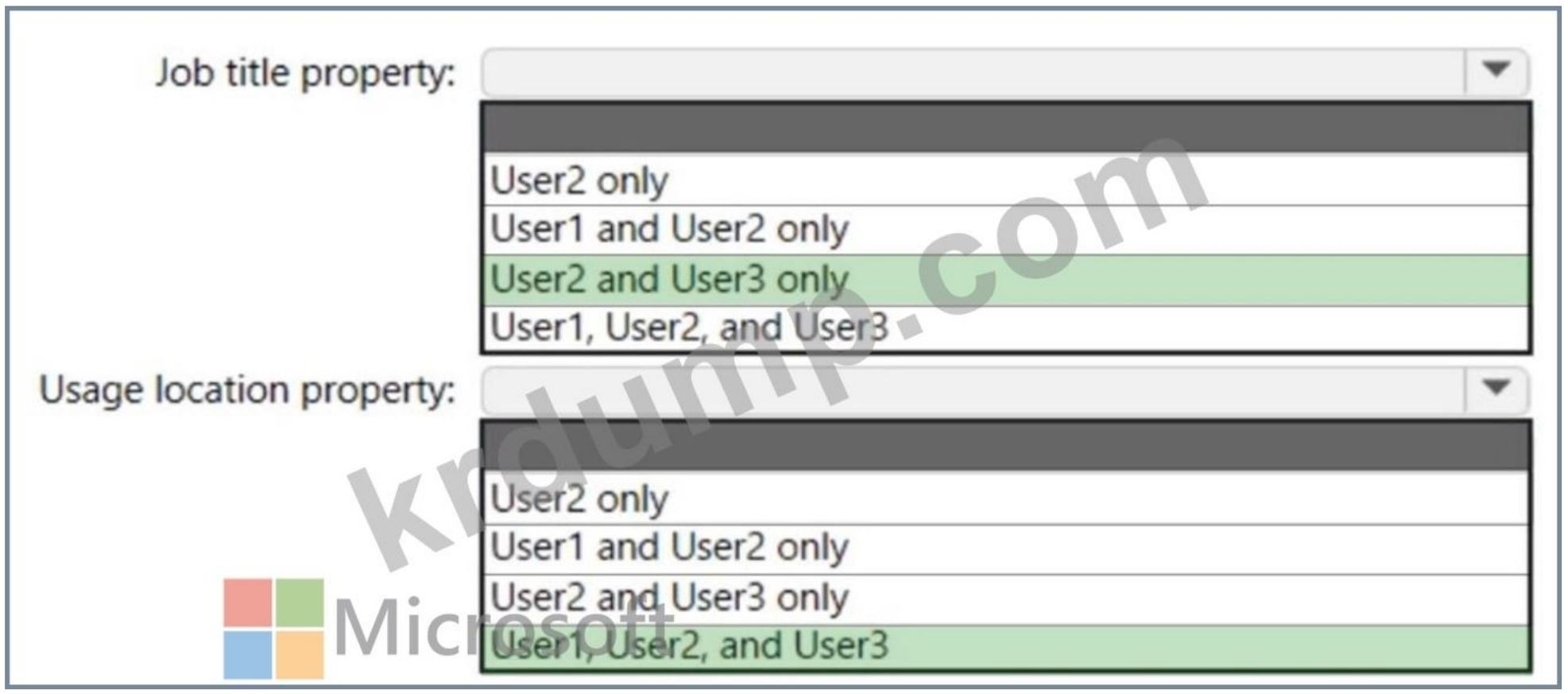
Name	User type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

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

□□: □□ □□□ 1□□□□.



Answer:



Explanation:
Box 1: User2 and User3 only
Job title property for directory synched users cannot be updated from Azure AD.
Box 2: User1, User2, and User3
Invite users with Azure Active Directory B2B collaboration, Update user's name and usage location.
To assign a license, the invited user's Usage location must be specified. Admins can update the invited user's profile on the Azure portal.
1. Go to Azure Active Directory > Users and groups > All users. If you don't see the newly created user, refresh the page.
2. Click on the invited user, and then click Profile.
3. Update First name, Last name, and Usage location.
4. Click Save, and then close the Profile blade.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-profile-azure-portal
https://docs.microsoft.com/en-us/power-platform/admin/invite-users-azure-active-directory-b2b-collaboration#update-users-name-and-usage-location

NEW QUESTION: 200
Azure Active Directory(Azure AD) □□□□ □□□□.
□□ □□□ □□ □□□(SSPR)□ □□ □□□ □□□□ □□□□□.

- □□□ □ □□□ □□ □□: □
- □□□□ □□□ □□ □: 1

□□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?

A. □□□□□

B. □□□ □ □□

C. □□□ □ □□

D. □□ □□ □□□ □□□ □□□

Answer: B (LEAVE A REPLY)

When using a mobile app as a method for password reset, like the Microsoft Authenticator app, the following considerations apply:

- When administrators require one method be used to reset a password, verification code is the only option available.
- When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.

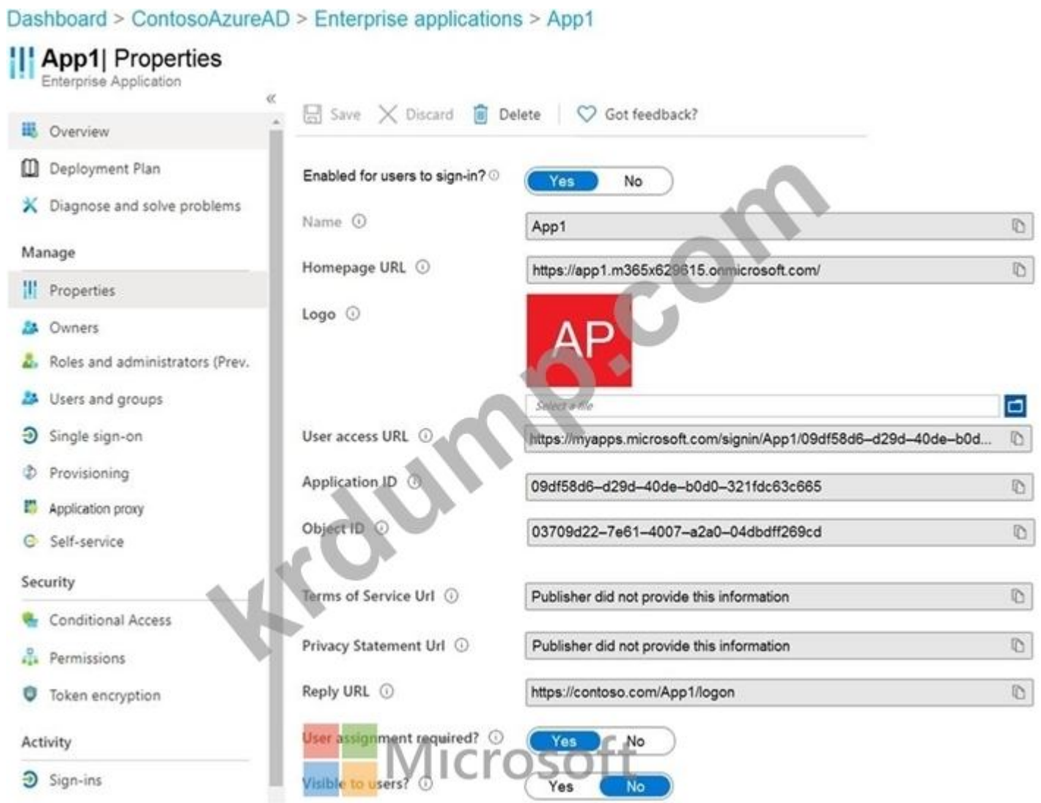
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr

NEW QUESTION: 201

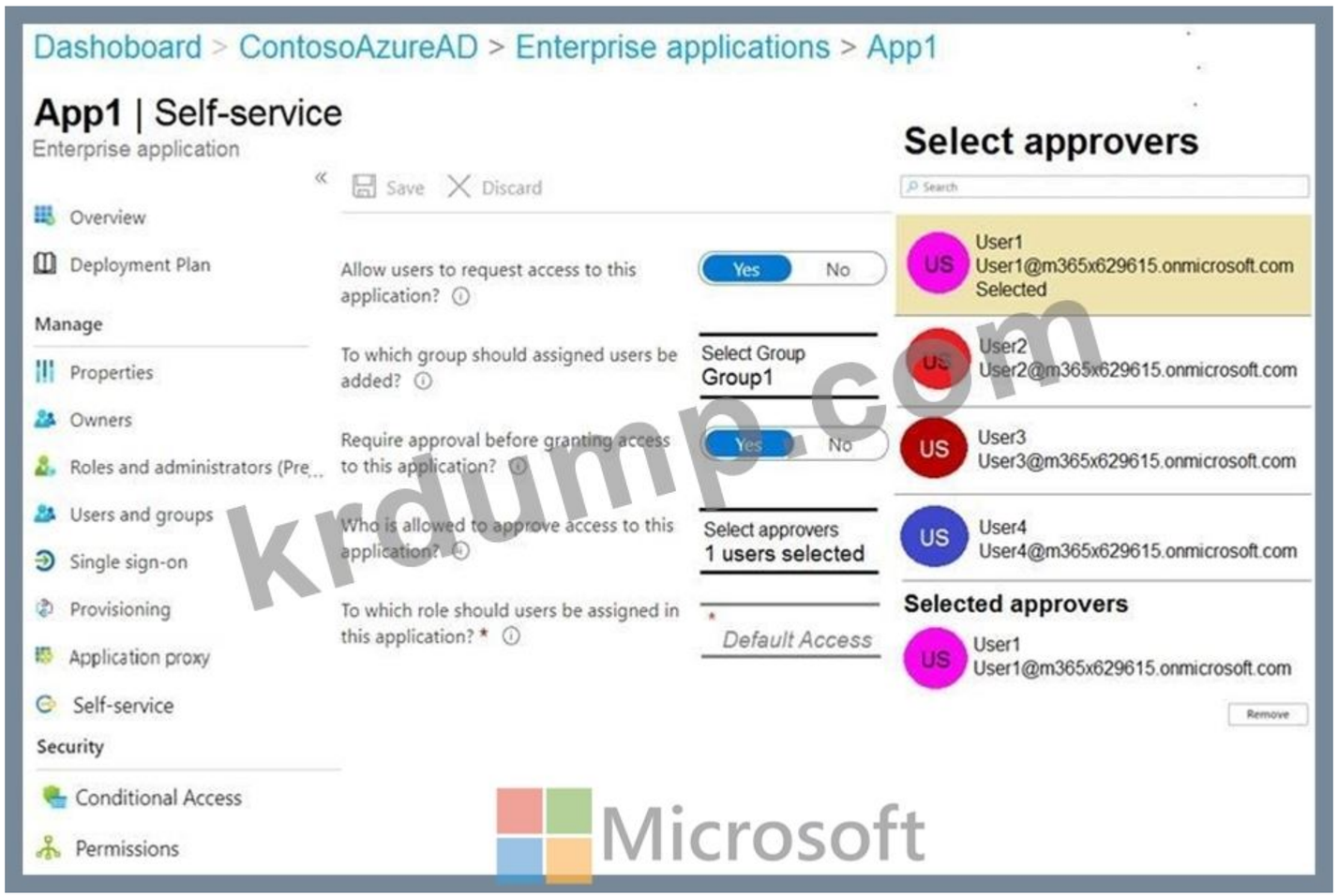
□□□ □□

Group1 □□□ □□ Group1□□□ □□□ □□□ Microsoft 365 □□□□ □□□□. (Group1 □□ □□□□□.)

App1 □□ □□□ □□□ □□□ App1□□□ □□□ □□□□□□ □□□□□□□ □□□□□. (App1 □□ □□ □□□□□□.)



App1 □□ □□□ □□□ App1 □□ □□□ □□□ □□ □□□□□. (App1 □□ □□□ □□ □□□□□.)


Dashoboard > ContosoAzureAD > Enterprise applications > App1
App1 | Self-service
Enterprise application
Save
Discard
Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators (Pre...
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Allow users to request access to this application?
Yes
No
To which group should assigned users be added?
Select Group
Group1
Require approval before granting access to this application?
Yes
No
Who is allowed to approve access to this application?
Select approvers
1 users selected
To which role should users be assigned in this application? *
Default Access
Select approvers
Search
US
User1
User1@m365x629615.onmicrosoft.com
Selected
User2
User2@m365x629615.onmicrosoft.com
US
User3
User3@m365x629615.onmicrosoft.com
US
User4
User4@m365x629615.onmicrosoft.com
US
Selected approvers
US
User1
User1@m365x629615.onmicrosoft.com
Remove
Microsoft

□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.

□□: □□ □□□ 1□□□□.


Answer Area
Microsoft
Statements
Yes
No
The members of Group3 can access App1 without first being approved by User1.
After you configure self-service for App1, the owner of Group1 is User1.
App1 appears in the Microsoft Office 365 app launcher of User4.

Answer:

Explanation:
Box 1: No
Only direct members will have access. Approved users will be added to Group 1.
Box 2: Yes
The approver will automatically become owner of the Group 1 after self service is configured.
Box 3: No
Visible to users is NO. So no one will be able to see the app.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

NEW QUESTION: 202
Microsoft 365 E5 □□□ □□□□ □□□, □ □□□□ Site1□□□ Microsoft SharePoint Online □□□□ Team1□□□ Microsoft Teams □□ □□□□ □□□□. □□, Group1, Group2, Group3, Group4, Group5□□ □□□ □ □ □□□ 5□ □□□□.
Site1□ Team1□ □□ □□□ □□□□ □□□□ □□□.
- □□3□ □□□□ □□□1□ □□ □□ □□□ □□□ □ □□□ □□□.
- □□1□ □□□□ □□□1□ □1□ □□ □□ □□□ □□□ □ □□□ □□□.
- □□4□ □□□□ □□□1□ □1□ □□ □□ □□□ □□□ □ □□□ □□□.
- □□2□ □□□□ □□□ □□□□ □□□ □ □□□ □□□.
□□1 □□□□□ □□□□□.
- □□ □□□□ □□□ □□□□ □□□ □ □□□ □□□.
□□3 □ □□4 □□□□ □□□□□.

□□□ □ □□ □□□ □□□□ □□□□ □□□?

A. 2

B. 3

C. 4

D. 5

Answer: B (LEAVE A REPLY)

Three access packages needed.

* Members of Group3 must be able to request access to Site1 only. [One access package for Site1 named X1]

* Members of Group1 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X2]

* Members of Group4 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X3]

* Only members of Group2 must be able to approve access package requests from Group1 members. [Add Group2 as approver for X2]

* Only members of Group5 must be able to approve access package requests from Group3 and Group4 members. [Add Group5 as approver for X1 and for X3] Reference:

https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-first

NEW QUESTION: 203

□□□ □□

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

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

□□ □□ □□ □□ □□□□ □□□□ □ □□□□.

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

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

* □□: □□1

* □□□ □ □□ □□□ □□: □□

IPv4 □□: 10.10.0.0/16 -

MFA□ 193.17.17.0/24□ □□□ □ □□ IP □□ □□□ □□□□□.

* □□: CAPolicy1

* □□

- □□□ □□ □□□□ ID: □□1

- □□□□ □ □□ □□: □□ □□□□ □

* □□

- □□: □□ □□□ □ □□ □□

* □□ □□

- □□□□

- □□ □□ □□: □□□ □□ □□

- □□: 0□□ □□□□ □□□

* □□ □□□: □□
□□ □ □□□ □□, □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□□.
□□: □□ □□□ 1□□□□.

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	○
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	○	○
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	○	○

Answer:

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	●
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	●	○
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	○	●

Explanation:
Box 1: No
User1 will not be prompted for MFA because user not in CA scope and MFA is disabled.
Box 2: Yes
User2's source IP is 10.10.1.160, the public IP of which is in the range of 20.93.15.0/24, which isn't a trusted MFA range. Besides, User2 is a per-user MFA-enforced user. Therefore, User2 will be prompted for MFA.
Box 3: No
The public IP address of 192.168.1.20 is in the space of 193.17.17.0/24, which is an MFA-trusted IP range. Although user2 is a per-user MFA-enforced user, it won't be prompted for MFA.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

NEW QUESTION: 204
□□ □□ □□ □□ Azure □□□□ □□□ □ □□□□.

Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

RG1□ □□ □□□ □□□ □□ ID□ □□□ □ □□□□?

A. □□□ 1 □□

B. User1, VM1 □ App1□ □□

C. User1, Group1, VM1, App1

D. User1 □ Group1□ □□

E. User1 □ VM1 □□

Answer: C (LEAVE A REPLY)