Microsoft.SC-300-KR.v2026-06-08.q173

□□□□:	SC-300-KR
□□□□:	Microsoft Identity and Access Administrator (SC-300 Korean Version)
□□□:	Microsoft
□□ □□ □□□:	173
□□:	v2026-06-08
# □□ □:	106
# □□ □□□:	1730
https://www.krdump.com/Microsoft.SC-300-KR.v2026-06-08.q173.html	

NEW QUESTION: 1
Microsoft 36S □□□ □□□□. □ □□□□ Microsoft Outlook 2016 □ Outlook 2013 □□□□□□ □□□□ □□□□ □□□□ □□□□. □□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □ □□. □□ □□ □□ □ □□ □□□□□?
A. Outlook 2013 □□□□□□ Outlook 2016□□ □□□□□□□□.
B. Outlook 2013 □□□□□□ □□□□ □□ □□□ □□□□□.
C. □□ Outlook □□□□□□ Outlook 2019□ □□□□□□□□.
D. Exchange □□ □□□□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Tenant Restrictions in Microsoft 365 are designed to prevent users from accessing external tenants while allowing access to approved tenants. According to the SC-300 exam material and Microsoft's Tenant Restrictions documentation, only modern authentication-capable clients (OAuth 2.0) can enforce tenant restrictions.
Outlook 2013 by default uses basic authentication, which does not support tenant restrictions. Outlook
2016 (and later versions) use modern authentication, making them compatible.
Microsoft Documentation: "Tenant restrictions require modern authentication to enforce access control.
Legacy clients like Outlook 2013 must be upgraded to Outlook 2016 or newer."

NEW QUESTION: 2
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□□□ □□□ □□□□□□□ □□ □□ □□ □□□ □□□□ □□□□ □□□□ □□□. □□, □□□□ □□□□ □□ □□ □□□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□
C. □□□ □□ □□
D. □ □□
Answer: (SHOW ANSWER)

NEW QUESTION: 3
□□□□□□ Azure Active Directory(Azure AD) □□□□ □□□□□ □-□□□□ Active Directory □□□□ □□□□ □□□□.

□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Source	Member of
Group1	Cloud	Group3
Group2	Active Directory domain	None
Group3	Cloud	None

□□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group3
User3	Yes	Group2

□□ □□ □□□ □□ □□□ □□□ □□□□□.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

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

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group1 if the user does not respond to the review request.	○	○
User2 will be removed automatically from Group3 if the user does not respond to the review request.	○	○
User3 will be removed automatically from Group2 if the user does not respond to the review request.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 will be removed automatically from Group1 if the user does not respond to the review request.	○	○
User2 will be removed automatically from Group3 if the user does not respond to the review request.	○	○
User3 will be removed automatically from Group2 if the user does not respond to the review request.	○	○

Explanation:

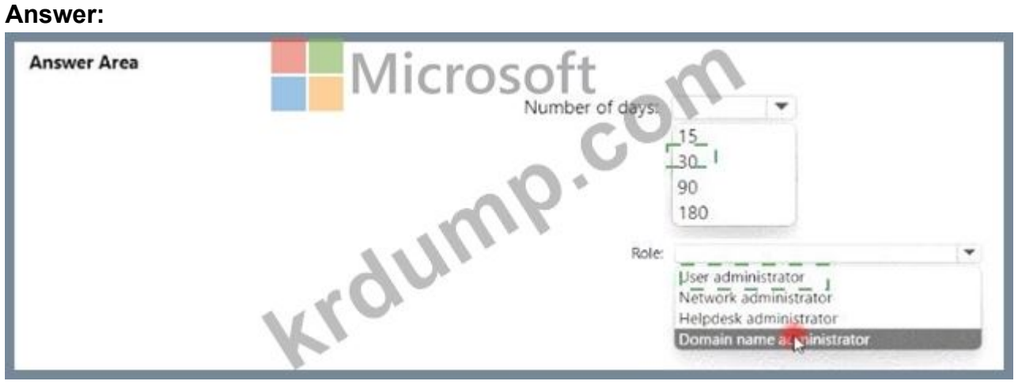
Answer Area

Statements	Yes	No
User1 will be removed automatically from Group1 if the user does not respond to the review request.	●	○
User2 will be removed automatically from Group3 if the user does not respond to the review request.	●	○
User3 will be removed automatically from Group2 if the user does not respond to the review request.	○	●

NEW QUESTION: 4
□□ 1
□□ □□ □□(MFA)□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* Sg-Finance □□ □□□□□ MFA □□□ □□□□□.
* □□□ □□□ MFA□ □□□□ □□ □□□□□.
* □□□ □□□ □□□ □□□□ □□ □□□□ □□□□□.
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To deploy Multi-Factor Authentication (MFA) for only the members of the Sg-Finance group, excluding Debra Berger, and without using a Conditional Access policy, you can follow these steps:
Open the Microsoft Entra admin center:
Sign in as a Security Administrator or Global Administrator.
Navigate to MFA settings:
Go to Users > Active users.
On the Active users page, select Multi-factor authentication.
Manage user settings:
Find and select the Sg-Finance group.
Enable MFA for this group by setting the requirement status to Enabled.
Exclude a user from MFA:
In the Multi-factor authentication page, search for Debra Berger.
Set her MFA status to Disabled to exclude her from MFA registration.
Verify the configuration:
Ensure that all members of the Sg-Finance group have MFA enabled except for Debra Berger.
Communicate the change:
Inform the Sg-Finance group members about the MFA requirement and provide instructions on how to register for MFA.
Monitor the setup:
Check the sign-in logs to confirm that MFA is being prompted for the Sg-Finance group members and not for Debra Berger.

NEW QUESTION: 5
User1□□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ User1□ □□□□□.
□□ □□□ □□□□ □□□.
* User1□ □□□ □□□ □ □□ □□ □□□ □□□ □ □□□?
* User1□ □□□□ □ □□□ □ □□ □□ □□□ □□ □□□ □□□□□?
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□. □□: □□ □□□ 1□□□□.

Answer:



Explanation:

As per the Microsoft Identity and Access Administrator (SC-300) official study guide, and confirmed by Microsoft Learn documentation on "Restore a deleted user in Azure Active Directory", when a user account is deleted from Azure Active Directory (Azure AD), it is not permanently removed immediately. Instead, the deleted user object is retained in a " soft-deleted " state for 30 days. During this retention period, administrators can restore the user account, including its associated group memberships and licenses. After 30 days, the user object is permanently deleted and cannot be recovered.

From the Microsoft documentation:

"When a user is deleted, the account is retained in a deleted state for up to 30 days. You can restore the user within this period using the Azure portal, PowerShell, or Microsoft Graph." Regarding the minimum role required, the same documentation and SC-300 guide state that the User Administrator role is the least privileged built-in Azure AD role that can manage users - including restoring deleted accounts. Higher roles, such as Global Administrator, also have this capability, but the principle of least privilege applies.

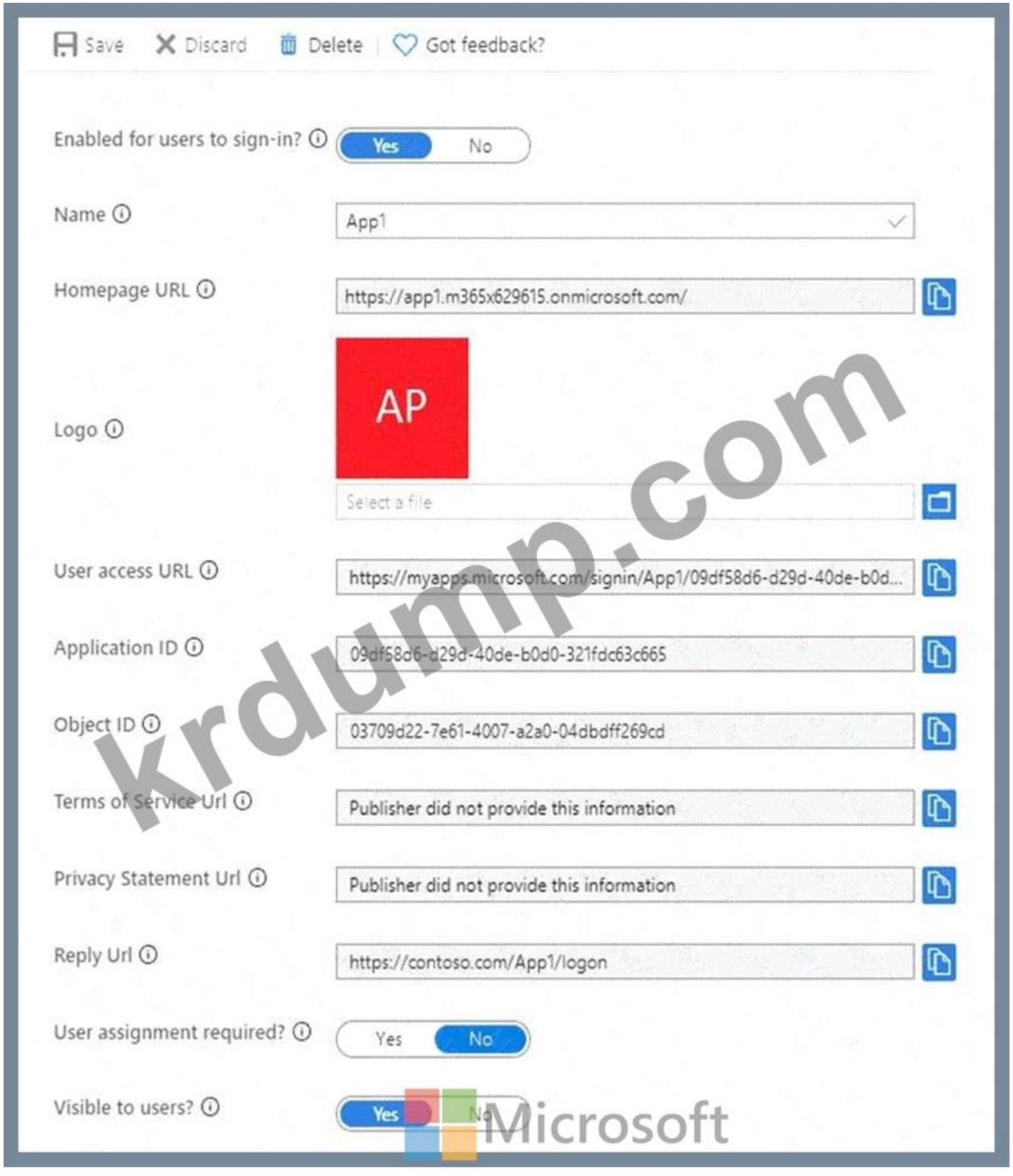
"The User Administrator role can create, update, delete, and restore user accounts and reset passwords for non- administrators." Therefore, the correct configuration is:

* Number of days: 30
* Role: User Administrator

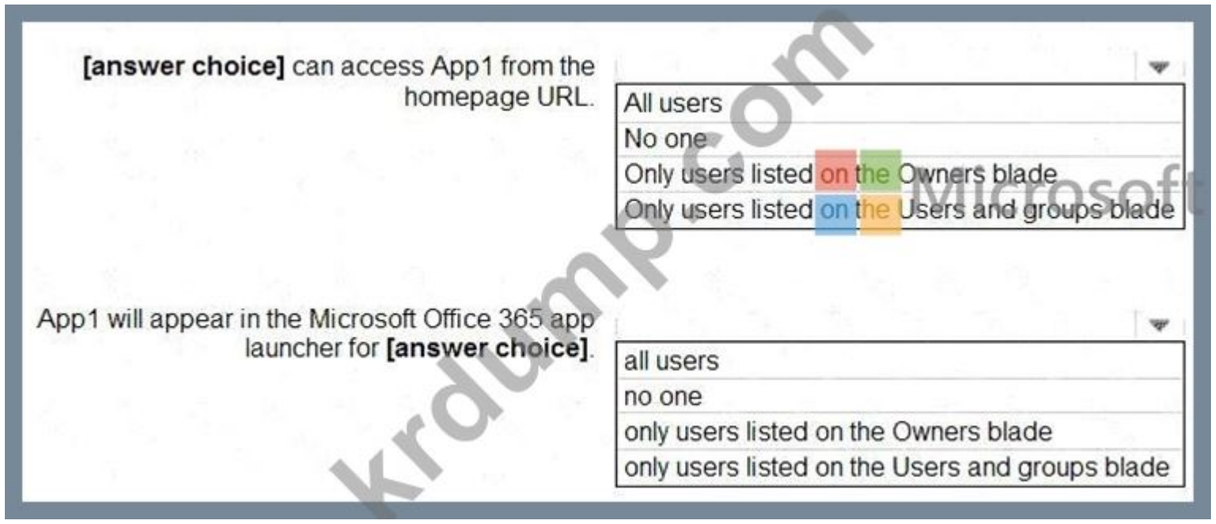
NEW QUESTION: 6

Azure Active Directory(Azure AD)□ □□□ App1□□□ □□□ □□ □□□□ □□ □□□□.

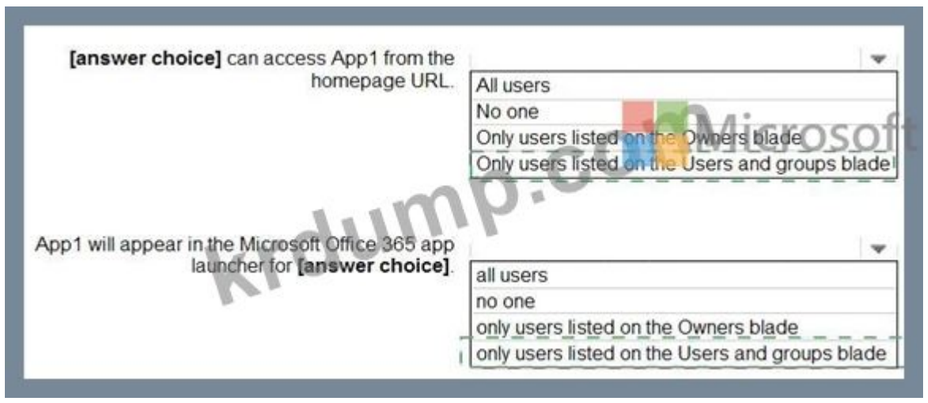
App1□ □□ □□□ □□ □□□□□.



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

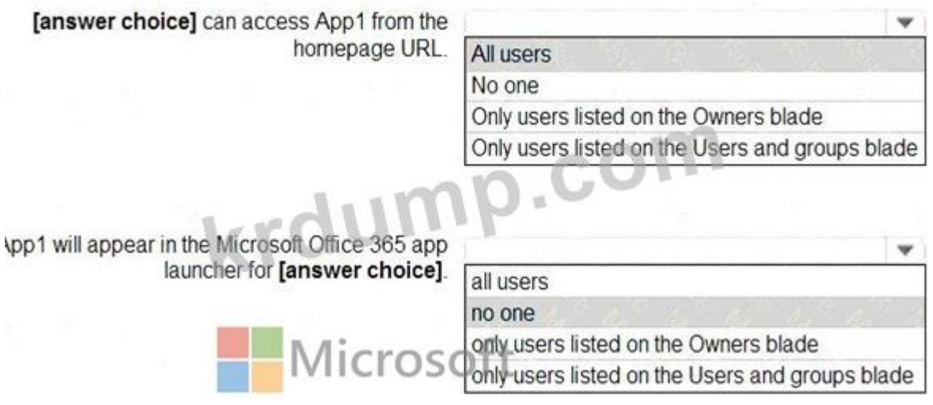


Answer:



Explanation:

< [answer choice] can access App1 from the homepage URL: # Only users listed on the Users and groups blade App1 will appear in the Microsoft Office 365 app launcher for [answer choice]: # Only users listed on the Users and groups blade



According to Microsoft's official documentation and the SC-300: Microsoft Identity and Access Administrator study guide, when you register and configure an enterprise application in Azure Active Directory, two specific settings directly influence user visibility and access:
* User assignment required?
* If this option is set to Yes, Azure AD requires users to be explicitly assigned to the app before they can sign in.
* Only users or groups listed on the Users and groups blade (app assignments) will have access.
* This means that even if the application is visible in Azure AD, users not assigned to it cannot authenticate or launch it.
* Visible to users?
* If set to Yes, the app appears in the Microsoft 365 app launcher (also known as the My Apps portal).
* However, when "User assignment required" is Yes, the visibility is limited only to those who are assigned to the app.
From the exhibit:
* "User assignment required?" = Yes
* "Visible to users?" = Yes
This configuration implies:
* Only assigned users (those listed on the Users and groups blade) can sign in to App1 via the homepage URL.
* App1 will appear in the Microsoft 365 app launcher (My Apps portal) only for those same assigned users.
As per Microsoft Learn documentation ("Manage enterprise apps in Azure AD"):
"When User assignment required is set to Yes, only users assigned to the application can access it. If Visible to users is also Yes, the application will appear in My Apps for those assigned users."

NEW QUESTION: 7
□□□ □□□□□ □□□□ □□□□ □□ MFA □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□ IP □□ □□□ □□ □□□ □□
B. □□ IP □□ □□□ □□ □□□ □□
C. □□ IP □□ □□□ □□ □□□ □ □□ IP
D. □□ IP □□ □□□ □□ □□□ □ □□ IP
Answer: B (LEAVE A REPLY)
SC-300 emphasizes using Conditional Access with named locations to scope MFA-especially to exclude trusted corporate egress IPs . The materials state that administrators can define named locations by public IP ranges and "mark them as trusted" for policy exceptions. This aligns with the requirement: enforce MFA for all users, but exempt users authenticating from the Boston office. Because Azure AD evaluates the client's public egress address, private RFC1918 ranges are never seen by Azure AD on the internet, so defining private IP ranges would not work. Likewise, the legacy "Trusted IPs" setting belongs to the old per-user MFA service settings; SC-300 guidance prefers Conditional Access named locations for modern MFA deployments and for combining with other conditions (apps, platforms, user risk, locations). Implementing the Boston office as a named location using its public egress IP range(s), and marking it trusted, lets you exclude that location from the tenant-wide MFA policy while still meeting the broader requirement to enforce MFA for everyone else and for on-prem apps published via Azure AD Application Proxy. In short: define Boston's public IP as a named location and use it in your Conditional Access policy exclusion to satisfy the exemption precisely and securely.
Topic 3, A Datum CorpOverview
A Datum Corporation is a consulting company in Montreal.
A Datum recently acquired a Vancouver-based company named Litware, Inc.
A Datum Environment
The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
A Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS dom ain by using Azure AD Connect A Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.

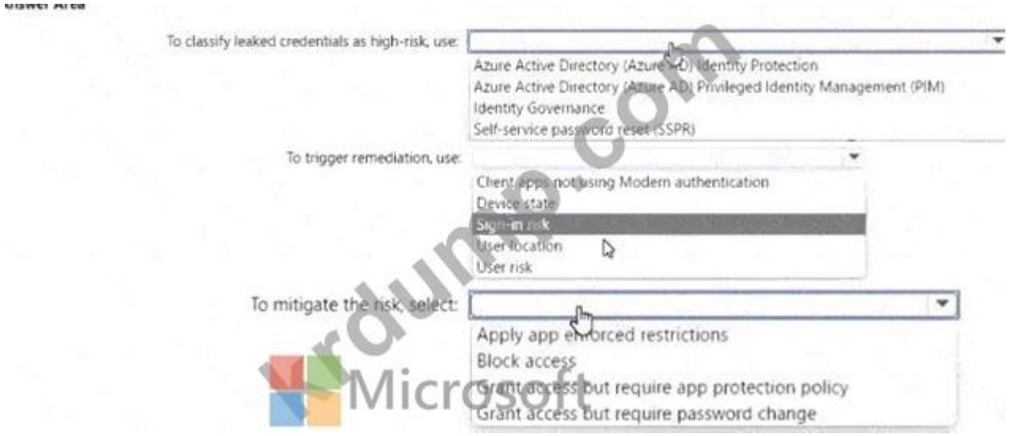
Problem Statements
A Datum identifies the foll owing issues:
* Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device li mit.
* A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address,
* When you attempt to assign the Device Administrators role To IT_ Group1, the group does NOT appear in the selection list.
* Anyone in the organization can invite guest users, including other guests and non-administrators.
* The helpdesk spends too much time resetting user passwords.
* Users currently use only passwords for authentication.
Requirements
A Datum plans to implement the following changes;
* Configure self-service password reset {SSPR}.
* Configure multi-factor authentication (MFA) for all users.
* Configure an access review for an access package named Package1.
* Require admin approval for application access to organizational data.
* Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
* Ensure that only users that are assigned specific admin roles can invite guest users.
* Increase th e maximum number of devices that can be joined or registered to Azure AD to 10.
Technical Requirements
A Datum identifies the following technical requirements:
* Users assigned the User administrator role must be able to request permission to use the rol e when needed for up to one year.
* Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
* Users must provide one authentication method to reset their password by using SSPR. Available method s must include:
* Email
* Phone
* Security questions
* The Microsoft Authenticator app
* Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
* The principle of least privilege must be used.

NEW QUESTION: 8
Microsoft 365 □□□□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□ □ □□ □□ □□(MFA)□ □□ Microsoft Authenticator □□ □□□□ □□□.
□□ □□□□ □□□ □□□ □□ □□□□□ Microsoft Authenticator □□□ MFA □□□□ □□□□ □□□□□□.
□□□□ □□□ □□□□ □□ MFA □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□.
□□ □□: Azure Portal□□ □□ □□ □□(MFA)□ □□ □□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)

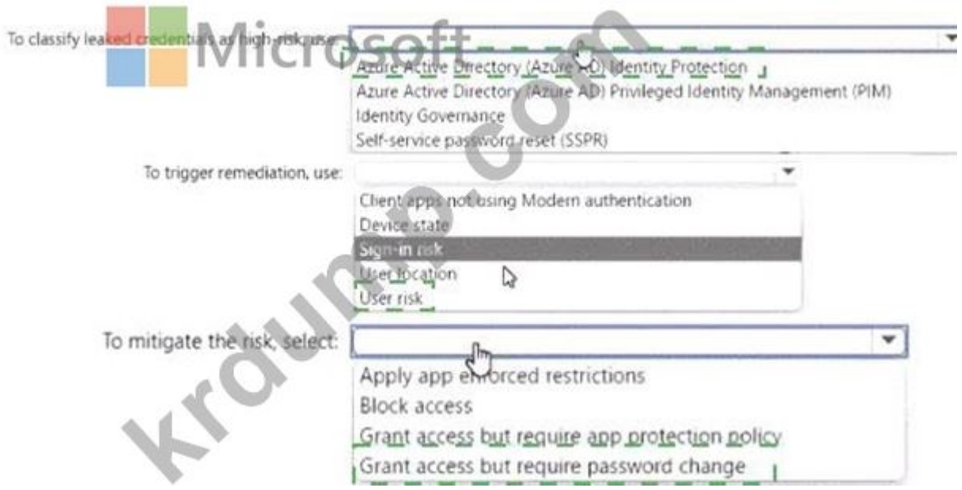
Azure AD MFA Fraud alert is explicitly documented in the SC-300 content as the control to combat push- bombing. The documentation explains: "Enable Fraud alert so users can report unexpected MFA prompts; when configured to block the user , Azure AD marks the user as blocked automatically upon the fraud report.
" It also notes: "The block remains in effect (default 90 days) until an administrator unblocks the user." This directly satisfies the requirement to automatically block users when they report that they did not initiate the sign-in. Other MFA configurations-such as account lockout thresholds-address repeated denial scenarios and rate-limiting but do not trigger an immediate block as a result of a user's fraud report. Configuring Fraud alert therefore meets the goal exactly, aligning with SC-300's best-practice guidance for protecting users from unsolicited MFA prompts.

NEW QUESTION: 9
User1□□□ □□□□ Microsoft Defender for Cloud Apps □□□ □□□□□□ □□ □□ □□□□ □□□□□.
□□□ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□□ □□
C. □□ □□
D. □□□□□ □□
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Entra ID (Azure AD) documentation , sign-in logs are the primary source for diagnosing and troubleshooting authentication and access issues for Azure AD-integrated services, including Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) .
The sign-in logs record all user authentication attempts - successful and failed - along with critical d etails such as:
* User identity (User Principal Name)
* Application name (in this case, "Microsoft Cloud App Security" or "Microsoft Defender for Cloud Apps")
* IP address and device details
* Conditional Access policy outcomes
* Failure reasons (e.g., MFA requireme nt, denied by Conditional Access, invalid token, etc.) These logs can be accessed directly from the Microsoft Entra admin center # Monitoring # Sign-in logs .
They allow administrators to quickly identify why a user was unable to access a specific cloud ser vice , without needing to configure or collect extra data sources.
Other log types do not fit this scenario:
* Audit logs record changes (e.g., policy updates, role assignments) but not authentication attempts.
* Provisioning logs track synchronization and prov isioning events from connected applications.
* Log Analytics is a log aggregation workspace; it's not the first-line diagnostic tool and requires extra configuration.
Hence, to identify the cause of User1's access error with minimal administrative effort , th e correct choice is sign-in logs .

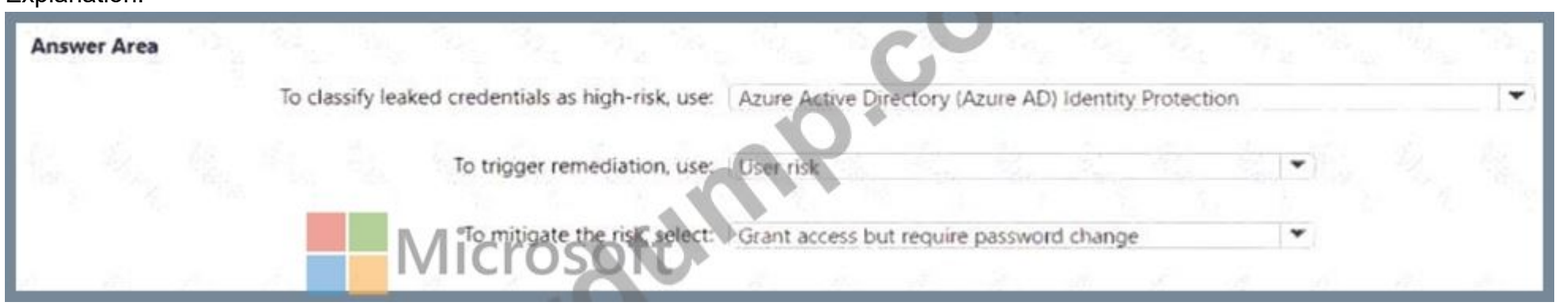
NEW QUESTION: 10
Microsoft 365 □□□□ □□□□.
□□ □□□ □□□ □□□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ □□□ □□□ □□□□ □□□□ □□ □□.
* □□□□ □□□ □□□□ □□□□□.
* □□□□ □□□□□□□ □□ □□□□ □ □□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□□□.
□□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:



According to Microsoft's SC-300 Study Guide , Exam Ref SC-300: Microsoft Identity and Access Administrator , and the Azure AD Identity Protection documentation , leaked credentials and risky sign-ins are detected and managed through Azure AD Identity Protection. This service identifies, categorizes, and automates the mitigation of risks related to user and sign-in behavior.

* Classify leaked credentials as high-risk:

* Azure AD Identity Protection automatically flags users as high-risk if their credentials appear in public or dark web breach data. Microsoft continuously monitors leaked credentials and matches them against Azure AD user accounts.

* The guide states: "Azure AD Identity Protection detects when user credentials are found on public credential dumps and flags those users as high-risk."

* Trigger remediation:

* The appropriate signal to trigger a policy response for leaked credentials is User risk, not sign-in risk.
* User risk evaluates the likelihood that a user's identity has been compromised, while sign-in risk deals with suspicious conditions during authentication.
* From Microsoft's documentation: "User risk policy is used to automatically remediate leaked credentials by requiring the user to change their password."
* Mitigate the risk:
* To mitigate the risk while still allowing access, the best practice is to grant access but require a password change . This satisfies the requirement to "immediately enforce a control" without fully blocking the user.
* The SC-300 study materials confirm: "When user risk is high, organizations can configure policies to allow sign-in but require a password change to remediate risk."

NEW QUESTION: 11
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
Microsoft Entra Internet Access□ □□□□□. □□ □□□□ Microsoft Entra Internet Access□ □□□ □ □□□?
A. User1□
B. User2only
C. User3only
D. User1□ User2□
E. User1, User2, User3
Answer: D (LEAVE A REPLY)
In Microsoft Entra Internet Access and Private Access, administrative permissions are controlled through specific Microsoft Entra roles. The SC-300 exam content (module "Manage Microsoft Entra Global Secure Access") identifies that management of Global Secure Access features requires either of these roles:
* Global Administrator, or
* Network Access Administrator
These roles can configure, deploy, and manage settings for both Microsoft Entra Internet Access and Microsoft Entra Private Access in the Microsoft Entra admin center.
From Microsoft Learn:
"To configure and manage Microsoft Entra Internet Access or Private Access, you must be assigned either the Global Administrator or the Network Access Administrator role." Thus, if:
* User1 = Global Administrator
* User2 = Network Access Administrator
* User3 = (Any other role)
Then only User1 and User2 can manage Microsoft Entra Internet Access.

NEW QUESTION: 12
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
Azure AD B2B(□□ □) □□ □□□□ □□□□ □□□ □□□□□.
□□ □□□□ □□ □ □□ □ □□ □□□□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□. □□: □ □□□ 1□□□□.
A. □□□ □□
B. □□□□ URL
C. □□□ □□
D. □□□
E. □□□□
Answer: A,B (LEAVE A REPLY)
In Azure AD B2B bulk invitations, the portal and CSV workflow require two core fields: the external user's email address and the Invite Redirect URL that determines where the guest is sent to redeem the invitation.

The study guide notes that the bulk invite template "must include the guest's email address" and that "InviteRedirectUrl is required to define the post-invite redemption target (such as MyApps or a specific app)." Usernames and passwords are not supplied for B2B guests because "guest accounts authenticate with their home identity provider," and there is no shared key involved in the invitation. Therefore, the only mandatory parameters to successfully process a bulk B2B invite are the email address of each guest and the redirection URL used during invitation redemption.

NEW QUESTION: 13
I-.Group1 □□□ □□□□ □□□. □□ □□□ □□ □□□?
A. IT □□ 1 □□□ □□ □□□□□.
B. IT-Group1□ □□□ □□□ □□ □□□ □□□□□.
C. IT_Group1□ □□□□ □□□□□.
D. IT-Group1□ □□□ □□□ □□ □□□□ □□□□□.
Answer: A (LEAVE A REPLY)
Assigning built-in directory roles (like Device Administrators) to a group requires a role-assignable group.
The SC-300 documentation explains: "You can assign Azure AD roles to a cloud security group by creating the group with the setting 'Azure AD roles can be assigned to the group.'" It further emphasizes: "This attribute is immutable; you must decide at creation time. You cannot convert an existing group to be role- assignable later." When a standard security group is not created as role-assignable, it will not appear in the picker when attempting to assign a directory role-exactly the behavior observed: "groups that aren't role- assignable cannot be selected for Azure AD role assignments." Therefore, the first step is to recreate IT_Group1 as a role-assignable security group (often called an "eligible for role assignment" group) and then assign the Device Administrators role to that group. Changing membership types (Dynamic User or Dynamic Device) or adding owners does not convert an existing group into a role-assignable one and thus would not resolve the issue.

NEW QUESTION: 14
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Role
Admin1	Cloud Application Administrator
Admin2	Application Administrator
Admin3	Security Administrator
User1	None

App1□□□ □□□□□□ □□□□□□□ Microsoft Entra ID□ □□□□ User!□ App1□ □□□□ □□□□□.
App1□ □□□□□ Microsoft Entra ID□ □□□□□ □□ □□□ □□□ □□□□□.
□□ □□□ □□ □□□ □□ □□ □□□ □□□□□.

Admin1, Admin2, Admin3, □□□ User1□ □□□□ □□□□□□□. □□□ □□ □□□ □□□□ □□□ □ □□ □□□□ □□□□□?
A. Admin1□

B. Admin1 ☐ Admin2☐
C. Admin1, Admin2 ☐ Admin3☐
D. Admin1, Admin2, User1☐
E. Admin1, Admin2, Admin3 ☐ User1
Answer: C (LEAVE A REPLY)
When an application requires admin consent to access Microsoft Entra ID data, and you have enabled "Users can request admin consent to apps they are unable to consent to", Microsoft Entra allows specific users or roles to act as reviewers who can review and approve or deny those requests.
In this scenario:
* The Admin consent requests feature is enabled.
* Admin1, Admin2, Admin3, and User1 were added as reviewers.
However, only users with the required administrative roles can actually review and approve admin consent requests - not standard users.
According to the Microsoft SC-300 study guide and Microsoft Learn documentation ("Configure the admin consent workflow"), the roles that can review and approve admin consent requests include:
* Global Administrator
* Cloud Application Administrator
* Application Administrator
The Security Administrator role can view and audit permissions but cannot approve consent requests, and regular users (with no admin role) cannot perform any action in this workflow.
Applying this to the question:
* Admin1 (Cloud Application Administrator) # # Can approve requests.
* Admin2 (Application Administrator) # # Can approve requests.
* Admin3 (Security Administrator) # # Can review (depending on Entra configuration; Security Administrator has partial consent visibility for security-sensitive apps).
* User1 (None) # # Cannot review or approve because they lack an admin role.
Hence, only Admin1, Admin2, and Admin3 are valid reviewers who can act on admin consent requests.

NEW QUESTION: 15
☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐ 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. User1☐
B. User2☐
C. User3☐
D. User1☐ User2☐
E. User1☐ User3☐
F. User1, User2, User3
Answer: (SHOW ANSWER)
Dynamic Azure AD groups use membership rules written against user attributes (for example, user.

department , user.jobTitle , user.country , user.usageLocation). The SC-300 materials show operators such as
-eq, -contains, -startsWith, and logical -and/-or to build precise targeting. In this scenario, the provided rule syntax evaluates users in the Sales department whose jobTitle contains "Sales" (for example, "SalesRep").
From the data: User1 has job title Associate (does not contain "Sales"); User2 has job title SalesRep (contains
"Sales"); User3 has job title Manager (does not contain "Sales"). Because department for all three is Sales, the discriminating condition is the job title match. Therefore, only User2 satisfies the rule and will be added to the dynamic group. The SC-300 guide emphasizes validating rules with the "Preview membership results" tool to confirm which users are included before enforcing at scale.

NEW QUESTION: 16
□□□ Group1 □ Group2□□ □ □□ □□□ □□ □□ □□□ □□□□ □□□□ Microsoft 365 E5 □□□ □□□□ □□□□.

Name	Department	Member of
User1	Marketing	Group1
User2	Marketing	Group2
User3	HR	Group1

□□2□ □□1□ □□□□□□.
fabrikam.com□□□ □□□ □□□□ □□□ □ □□□□ □□□□□ □□ □□□ □□□□□□.
* □□□□□ □□: □□
* □□□ □ □□: □□ 1
* □□□ □□□□ □□ □□: 500
* □□: □□□ □□□ □ □□□ □□□
* □□ □□ □□□ □□□□ □□□□□
□□□ □ □□□ □□□□ □□□□□ □□□ □□□□ □□□□□. □□ □ □□□ □□ □□□ □□□□ '□'□ □□□□, □□□ □□□ '□□□'□ □□□□□.
□□: □□ □□□ 1□□□□.
Answer Area

Statements	Yes	No
User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○
User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○
User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○

Answer:
Answer Area

Statements	Yes	No
User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○
User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○
User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com.	○	○

Explanation:

NEW QUESTION: 17
Microsoft 365 E5 □□□ □□□□.
Review1□□□ □□□ □□□ □□□ □□□□. Review1□ Microsoft 365 □□ □□□□ 6□□□□ □□ □□□ □□ □□□ □□□ □□□□ □□□□□ □□□□□.
□□ □□□□ Review1□ □□□□ □□□□ □□ □□, □□□ □□□□ □□□□ □□□□□ □□ □□□.
Review1□ □□ □□ □□□ □□□□ □□□?
A. □□□
B. □□ □□
C. □□
D. □□ □□ □
Answer: D (LEAVE A REPLY)
In Microsoft Entra Access Reviews, the "Upon completion settings" determine what happens after a review cycle ends - especially what happens when reviewers fail to take action. To automatically remove guest users who were not reviewed (or whose memberships were not approved), you must configure the "If reviewers don't respond" option under the Upon completion settings to "Remove access." The Reviewers and General sections define who conducts reviews and their frequency, while Advanced settings provide notifications and reminders.
From SC-300 content:
"You can specify actions upon completion, such as removing users not reviewed, keeping access unchanged, or approving all. The 'Upon completion settings' section controls this behavior."

NEW QUESTION: 18
□□□□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□□□ □□□□□.
Azure Active Dilatory(Azure AD)□ MyApp1□□□ □ □□□□□□ □□□□□□□ □□□□ MyApp1□ □□ SSO(Single Sign-On)□ □□□□□.
MyApp1□ □□ □□□□ □□ □□□ □□□□ □□□?
A. □□□□□
B. □□□□□
C. □□ □ □□□
D. □□□□□□ □□□
Answer: A (LEAVE A REPLY)

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and the Microsoft Learn module "Manage Enterprise Applications in Azure AD", when an organization requires that users request access before being allowed to use a corporate application, the correct configuration is to enable Self-service application access.
In Azure AD, the Self-service settings under an enterprise application allow administrators to specify whether users can request access to the app, who can approve those requests, and whether approvals are automatic or manual. This feature integrates directly with Azure AD Entitlement Management, enabling governance controls around who can request and access applications.
The documentation states:
"To allow users to request access to an enterprise application, you must enable self-service application access and configure the request and approval workflow." By contrast:
* Provisioning (Option B) is used for automatic account lifecycle management within the app, not for user access requests.
* Roles and administrators (Option C) deals with administrative delegation, not access requests.
* Application Proxy (Option D) is for enabling secure remote access to on-premises apps, not access workflows.
Therefore, enabling and configuring the Self-service settings is the required step to meet the requirement that users must request access before using MyApp1.

NEW QUESTION: 19
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

□□ □□□ □□□ □□□ □□ □□□ □□□□.
* □□:
o □□: □□ 1
o □□: □□2
* □□□ □□ □□ □□
* □□ □□:
o □□□ □□: □□□□ □□ □□
□□□□ □□□□ □□□□ □□□ □□ □□□ □□ □□ □□ □□□□□.

User	Risk level
User1	High
User2	Medium
User3	High

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

Answer Area

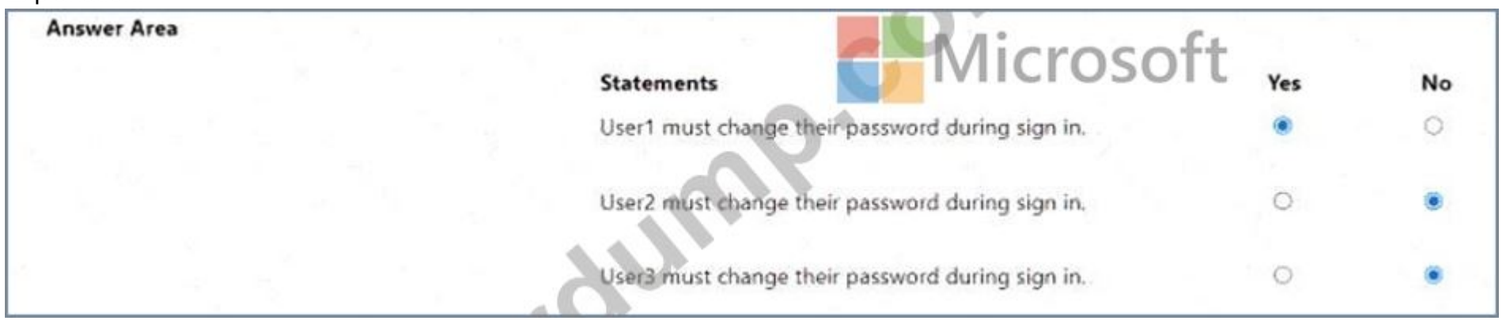
Statements	Yes	No
User1 must change their password during sign in.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

Explanation:



This scenario is based on the Microsoft Entra (Azure AD) Identity Protection feature, which is a major topic in the SC-300: Microsoft Identity and Access Administrator exam. According to the official study guide and Microsoft documentation:

"A user risk pol icy in Microsoft Entra ID is used to detect when a user account is at risk and to enforce remediation actions, such as requiring the user to change their password on the next sign-in."

* Assignments:
* Include: Group1
* Exclude: Group2
* Sign-in risk: Medium and above
* Access control: Require password change

Given Policy Settings: User Details: User

Group Membership

Risk Level

User1

Group1

High

User2

Group2

Medium

User3

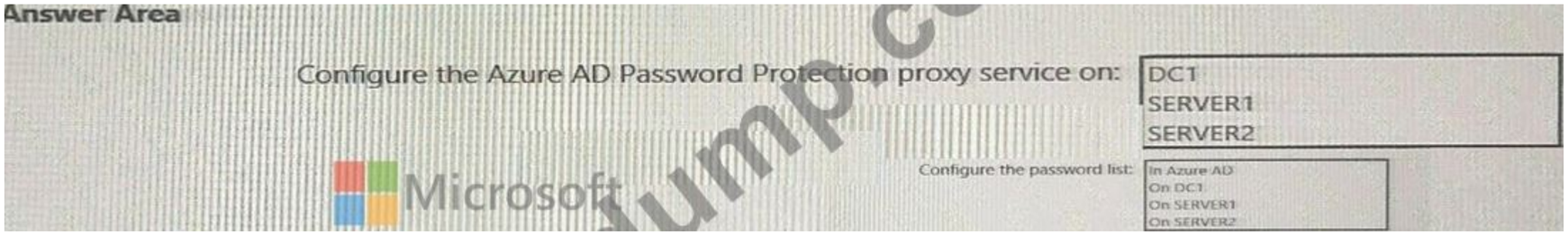
Group1, Group2

High

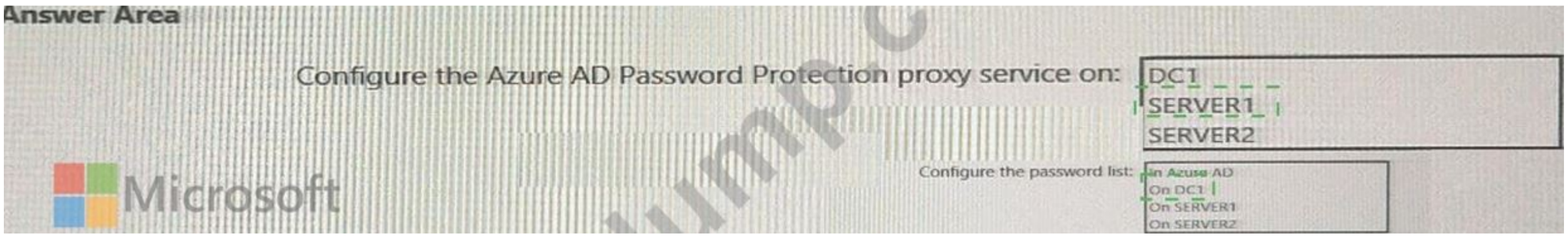
* User1:
* Included in Group1 (policy applies).
* Not a member of Group2 (not excluded).
* Risk level = High, which is # Medium, meeting policy threshold. # User1 must change their password.

* User2:
* Member of Group2 (excluded).
* Even though their risk level is Medium, exclusion overrides inclusion. # User2 will not be prompted to change their password.
* User3:
* Member of both Group1 (included) and Group2 (excluded).
* Exclusion always takes precedence in Microsoft Entra conditional access and risk policies. # User3 will not be required to change their password.
Analysis:
Official Microsoft SC-300 Source Excerpt: From the Microsoft Identity and Access Administrator Study Guide (Exam Ref SC-300) and Microsoft Learn ("Configure and manage user risk policies"):
"When a user is included in both the include and exclude assignments of a pol icy, the exclude setting takes precedence. Risk policies can enforce password change for users with detected risk levels that meet or exceed the configured threshold."

NEW QUESTION: 20
□□ □□ □□□ □□□□□ □□□□ □□□ □□□□ □□□.
DC1□ Azure AD □□ □□ DC □□□□□ □□□□□.
□□□□ □□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
Server1
On DC1
Azure AD Password Protection has two components: the DC agent (installed on domain controllers) and the proxy service (installed on one or more member servers). The SC-300 materials and Microsoft Identity Governance guidance explain that the proxy service is required when domain controllers do not have direct internet access. The proxy retrieves the password protection policy and custom banned password list from Azure AD over outbound HTTPS and makes it available to DC agents. The documentation further states that you should deploy at least one proxy per forest and two for high availability, and that domain controllers do not need internet connectivity when a proxy is deployed. In this scenario, DCs are explicitly blocked from internet access, so the proxy must be placed on member servers. Both SERVER1 (Application Proxy connector) and SERVER2 (Azure AD Connect) are domain-joined member servers with internet connectivity and are appropriate locations for the AzureADPasswordProtectionProxy service; selecting both provides the recommended redundancy. The custom banned password list is configured in Azure AD at the tenant level (as part of Azure AD

Password Protection settings), not on individual servers. Once configured, the policy and list are downloaded by the proxy and enforced by the DC agent during password set or change operations, satisfying the requirement to implement a banned password list for the litware.com forest.

NEW QUESTION: 21
Microsoft Entra □□□□ □□□□.
□□ □□□ □□□□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□.
□□□ □ □□□ □□ □□: □
□□□□ □□□ □□ □: 1
□□□□ □□□ □ □□ □□□ □□ □□□ □□□□□?
A. □□□□□
B. □□□ □ □□
C. FIDO2 □□ □□
D. Windows Hello PIN
Answer: B (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra ID self-service password reset (SSPR) settings and the available authentication methods, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Self-Service Password Reset (SSPR) in Microsoft Entra ID:
Self-service password reset (SSPR) allows users to reset their passwords without administrator intervention, improving security and reducing helpdesk workload.
The settings provided are:
Require users to register when signing in: Yes- U sers must register their authentication methods (e.g., phone number, email, security questions) the first time they sign in. This ensures they have methods available for SSPR.
Number of methods required to reset: 1- Users must verify their identity using o ne authentication method to reset their password. This is the minimum number of methods required, meaning users must have at least one method registered, and they will use one method during the reset process.
Available Authentication Methods for SSPR:
Micr osoft Entra ID SSPR supports a specific set of authentication methods that users can use to verify their identity during a password reset. These methods are configured by the administrator in the Microsoft Entra admin center under " Password reset " settings .
The default authentication methods available for SSPR include:
Email:Users receive a code sent to an alternate email address.
Mobile phone (SMS):Users receive a code via SMS to their registered mobile phone.
Mobile app code:Users use a code generated by the Microsoft Authenticator app (or another compatible authenticator app).
Mobile app notification:Users receive a push notification in the Microsoft Authenticator app to approve the reset.
Security questions:Users answer predefined security questions they set up during registration.
Important Note:Methods like smartcards, FIDO2 security tokens, and Windows Hello are not supported for SSPR. These methods are typically used for authentication during sign-in (e.g., MFA or passwordless sign- in), not for the SS PR process.
Analysis of the Options:
A). A smartcard:
Smartcards are a form of certificate-based authentication often used for sign-in to Windows devices or VPNs.
They require a physical card and a reader, and they are typically used for primary authenticat ion, not for SSPR.
Microsoft Entra ID SSPR does not support smartcards as an authentication method for password reset.
Smartcards are not listed as an available method in the SSPR configuration settings.

Conclusion:This is incorrect.
B). A mobile app code:
A mobile app code refers to a time-based one-time password (TOTP) generated by an authenticator app, such as the Microsoft Authenticator app.
This is a supported method for SSPR in Microsoft Entra ID. Users can register the Microsoft Authenticator app (or another compatible app) and use the generated code to verify their identity during a password reset.
Since the setting " Number of methods required to reset: 1 " means only one method is needed, a mobile app code is a valid option if the user has registered it.
Conclusion:This is correct.
C). An FIDO2 security token:
FIDO2 security tokens (e.g., YubiKey) are hardware-based security keys that support passwordless authentication in Microsoft Entra ID. They are part of Microsoft's passwordless authentication stra tegy and can be used for sign-in.
However, FIDO2 security tokens are not supported for SSPR. The SSPR process does not allow users to verify their identity using a FIDO2 security key because the reset process is designed to work with simpler, more accessib le methods like email, SMS, or app-based codes.
Conclusion:This is incorrect.
D). A Windows Hello PIN:
Windows Hello PIN is a device-specific authentication method used to sign in to Windows devices. It is part of Windows Hello, which also includes biometric authentication (e.g., facial recognition, fingerprint).
Windows Hello PIN is not supported for SSPR in Microsoft Entra ID. The SSPR process occurs in a web- based portal (e.g., aka.ms/sspr) and does not integrate with device-specific authenticatio n methods like Windows Hello. Additionally, Windows Hello PIN is tied to a specific device, whereas SSPR is designed to be device-agnostic.
Conclusion:This is incorrect.
Additional Considerations:
The setting " Require users to register when signing in: Yes " ensures that users have at least one authentication method registered. However, the question does not specify which methods are enabled by the administrator. In Microsoft Entra ID, the default enabled methods for SSPR typically include email, mobile phon e (SMS), mobile app code, and mobile app notification. Security questions may also be enabled but are less common due to security concerns.
If the administrator has disabled certain methods (e.g., mobile app code), the answer could change. However, the que stion does not indicate any such restrictions, so we assume the default methods are available.
The " Number of methods required to reset: 1 " setting means users only need to use one method to reset their password, but they may have multiple methods registered. The question asks for a " valid authentication method available to users, " so we need to identify a method that SSPR supports.
Conclusion:Based on the SSPR settings and the supported authentication methods in Microsoft Entra ID:
A mobile app cod e (option B) is a valid authentication method for SSPR, as it is supported by default and aligns with the configuration.
Smartcards, FIDO2 security tokens, and Windows Hello PIN are not supported for SSPR.Therefore, the correct answer isB.
References:
Micr osoft Entra ID documentation: " Self-service password reset authentication methods " (Microsoft Learn:
https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication- methods) Microsoft Entra ID documentation: " Configure self-service password reset " (Microsoft Learn:https://learn.
microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers SSPR configuration and supported authe ntication methods.

NEW QUESTION: 22
Microsoft 365 E5 □□□ □□□□.
Microsoft Entra □□□□ □□□ Azure □□□ □□□□. □□ □□□□ User1□□□ □□□□ □□□□.
Microsoft Entra □□ □□□ □□□ □□□□□.
User1□ □□ □□□ Azure □□□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□□.

User1□□ □□ Microsoft Entra □□□ □□□□ □□□?

A. □□ □□□

B. □□□□□□ □□□

C. □□ □□ □□□

D. □□□ □□□

Answer: C (LEAVE A REPLY)

In Microsoft Entra Permissions Management (formerly CloudKnox), the Permissions Management Administrator role provides the least-privilege rights necessary to onboard cloud environments such as Azure subscriptions, AWS accounts, or GCP projects. This role allows users to configure data collection and onboard environme nts without granting global administrative access.

The Global Administrator role could also perform onboarding but exceeds the least-privilege requirement.

Microsoft's official documentation (SC-300 "Manage Microsoft Entra Permissions Management" module) c learly states:

"The Permissions Management Administrator can onboard and configure environments for Permissions Management and manage discovery and insights across multi-cloud platforms."

NEW QUESTION: 23

Windows Server□ □□□□ Server!□□ □□□□□ □□□ □□□□.

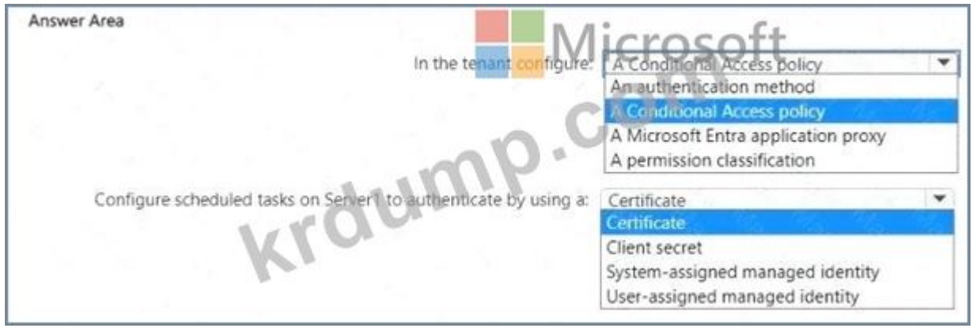
App1□□□ □ □□□ □□□□ Microsoft Entra □□□□ □□□□. App1□□ Microsoft Graph □□□□□□ □□□ □□□□.

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

* App1□ □□ □□□□□□□ □□□ □ □□□ □□□.
* App1□ □□ □□□ □□ □□□□ □□□□ □ □□□.
* □□ 1□ □□□□ □□ □□□ App1□ □□□ □ □□□ □□□.

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

□□: □□ □□□ 1□□□□.



Answer:

Explanation:

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn documentation ("Implement app registration and authentication with Microsoft Entra ID") , when configuring app registrations and securing non-interactive service applications (like scheduled tasks), two key elements must be addressed - secure authentication and conditional access enforcement.

Step 1: Secure App Access from the Corporate Network To ensure App1 is accessible only from the corporate network, you must configure a Conditional Access policy in Microsoft Entra ID. Conditional Access policies allow you to restrict access to applications based on conditions such as:

* User or workload identity
* Location (e.g., trusted IP ranges or corporate networks)
* Device compliance and sign-in risk

As Microsoft documentation states:

"Conditional Access policies can restrict access to specific applications based on location, risk, or device status. Use named locations to allow access only from your trusted network." Therefore, a Conditional Access policy is required to meet the first requirement.

Step 2: Secure Authentication for Non-Interactive Tasks For non-interactive scheduled tasks running on an on- premises server (Server1) that need to authenticate to App1 using application permissions, credentials must be securely stored. Storing plain-text secrets (like passwords or client secrets) violates security best practices.

Microsoft recommends using certificates for application authentication because certificates are securely stored and provide higher security than secrets.

From the SC-300 material and Microsoft Learn:

"When registering applications that use non-interactive authentication, use a certificate-based credential instead of a client secret. Certificates are more secure and meet compliance requirements for secure app authentication." This approach also ensures that Server1's scheduled tasks can authenticate silently using the private key of the certificate.

NEW QUESTION: 24

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

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

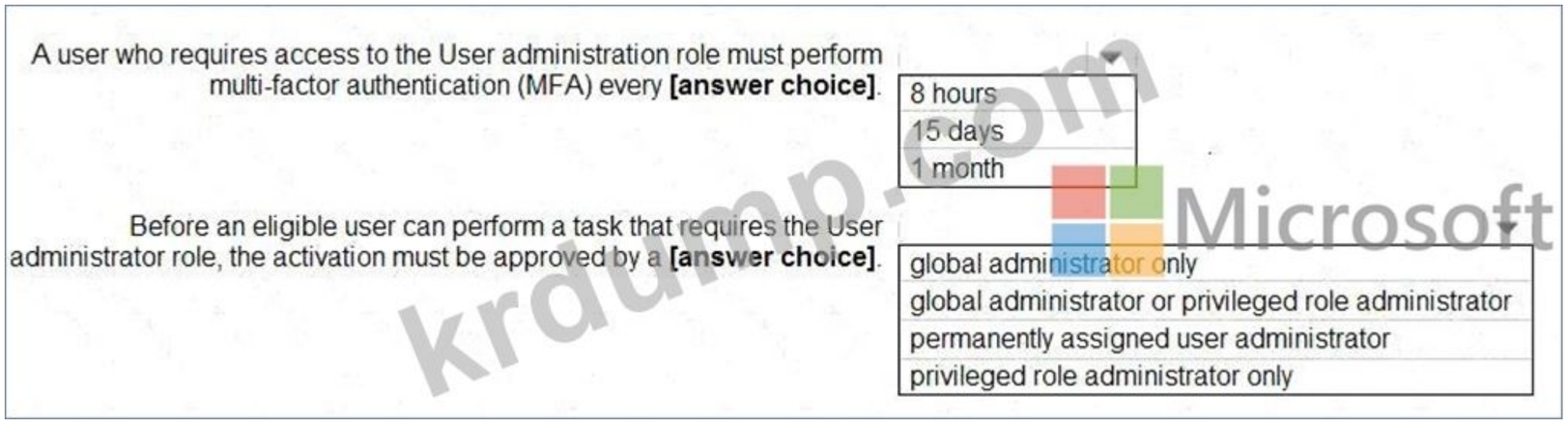
Activation

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

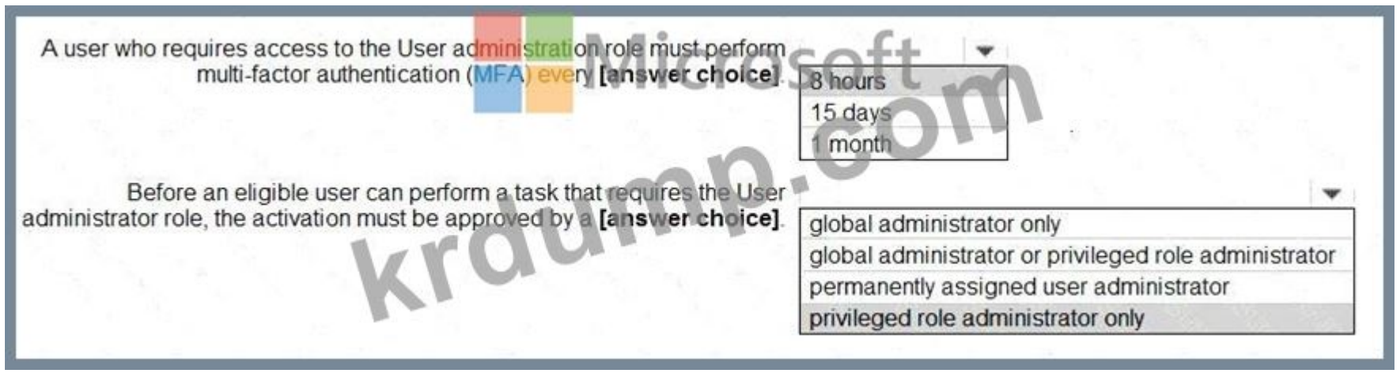
Assignment

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:



In Azure AD Privileged Identity Management (PIM), MFA can be enforced at role activation. The setting "On activation, require Azure MFA: Yes" means a user must complete MFA each time they activate the role.

Because the "Activation maximum duration (hours)" is 8 hours, any user who needs the User Administrator role beyond that window must re-activate the role and therefore perform MFA again. The study guide explains: "Requiring MFA on activation ensures strong verification at the moment privileges are elevated." It also states: "Activation maximum duration controls how long the user holds the role before needing to re- activate." For approvals, the role settings show "Require approval to activate: Yes" and "Approvers: None." PIM behavior for Azure AD roles is that "if no approver list is configured for a role, activation requests are routed to Privileged Role Administrators and Global Administrators." The exam materials emphasize: "Privileged Role Administrator manages role settings, including approval workflows, and can approve eligible activations; Global Administrator also has approval capability when no explicit approvers are defined." Therefore, the correct selections are 8 hours for MFA (per activation window) and global administrator or privileged role administrator as the approver when none are explicitly assigned.

NEW QUESTION: 25

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

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

tenan1□□ □□□ □□ □□ □□□ □□□□□.

□□ □□□□ □□ □□□ □□□ □□□□?

A. User2□

B. User3only
C. User2☐ User3☐
D. User3 ☐ User4☐
E. User1, User2, User3☐
F. User1, User2, User3, User4
Answer: D (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and the Microsoft Learn
- "Manage Microsoft 365 Groups naming policies" documentation, group naming policies in Azure Active Directory (now Microsoft Entra ID) apply to end users who create Microsoft 365 groups, but do not apply to administrators who have roles that allow them to override naming restrictions.
The policy defines conventions such as prefixes, suffixes, blocked words, and enforced naming rules.
However, certain administrative roles are exempt from this policy to allow organizational management and automation processes. The exempt roles are:
* Global Administrator
* User Administrator
These two roles can create Microsoft 365 groups without the naming policy constraints. Other users - including Groups Administrator and users without administrative roles - are subject to the naming policy when creating groups.
From the official documentation:
"Naming policies apply to all users who create groups, except for global administrators and user administrators. These roles can create groups that bypass the naming policy restrictions." Applying this rule:
* User1 (Global Administrator) - exempt
* User2 (User Administrator) - exempt
* User3 (Groups Administrator) - affected by the policy
* User4 (no role) - affected by the policy

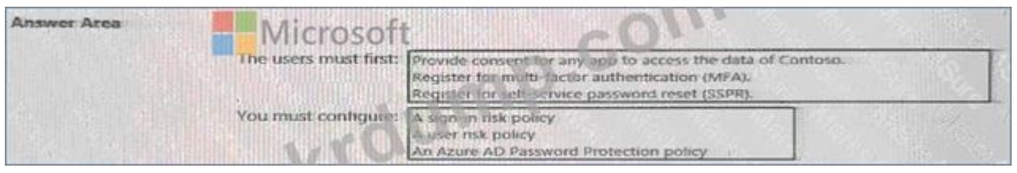
NEW QUESTION: 26
☐☐: ☐ ☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐ ☐☐☐☐☐. ☐ ☐☐☐☐ ☐ ☐☐☐☐ ☐☐☐ ☐☐☐ ☐☐☐ ☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐ ☐☐☐☐. ☐☐ ☐☐ ☐☐☐☐ ☐ ☐ ☐☐☐ ☐☐☐ ☐ ☐ ☐ ☐☐, ☐☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐ ☐☐☐☐.
☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐ ☐☐☐☐. ☐☐☐ ☐☐☐ ☐☐☐ ☐☐ ☐☐☐ ☐☐☐☐ ☐☐☐☐.
Active Directory ☐☐☐☐☐ ☐☐☐☐☐ Azure Active Directory(Azure AD) ☐☐☐☐ ☐☐☐☐.
Active Directory☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐☐☐☐ ☐☐☐☐ ☐☐ 30☐ ☐☐ Azure AD☐ ☐☐☐ ☐ ☐☐☐ ☐☐ ☐☐ ☐☐☐☐☐.
Active Directory☐☐ ☐☐☐ ☐☐☐ ☐☐☐☐☐☐ ☐☐ ☐☐☐ ☐☐☐ Azure AD☐ ☐☐☐☐ ☐☐☐ ☐☐ ☐☐☐☐ ☐☐☐.
☐☐ ☐☐: ☐☐☐☐ ☐☐☐ ☐☐☐☐☐.
☐☐☐ ☐☐☐ ☐☐☐☐☐?
A. ☐
B. ☐☐☐
Answer: A (LEAVE A REPLY)
Implementing Pass-through Authentication (PTA) ensures that Azure AD delegates the authentication process directly to the on-premises Active Directory in real-time. When a user signs in, Azure AD routes the authentication request through a secure channel to the on-premises Authentication Agent, which verifies credentials against AD.
If a user account is disabled in Active Directory, authentication immediately fails because the request is validated directly against the on-premises domain controllers - there's no delay or dependency on synchronization intervals.
From Microsoft documentation (SC-300 official guide):
"Pass-through Authentication provides real-time authentication directly against on-premises Active Directory.
If an account is disabled on-premises, authentication requests are denied immediately." Thus, enabling PTA satisfies the requirement for immediate blocking of disabled accounts.

Correct Answer: A. Yes

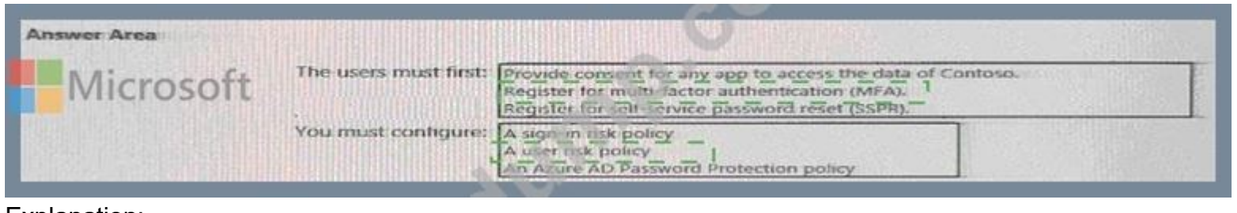
NEW QUESTION: 27
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□, □ □□□□ □□□ □□□ Microsoft 365 E5 □□□ □□□□□□. □□□□□ □□ □□ □□□ Microsoft Entra □□□□ □ □□□□ □□ □□□. □□ □□□ □□□□ □□□?
A. □□□□ □□
B. Microsoft Entra Seamless Single Sign-on(Microsoft Entra Seamless SSO)
C. □□□□ □□ □□□
D. Microsoft Entra □□□□ □□□
Answer: (SHOW ANSWER)

NEW QUESTION: 28
Microsoft 365 E3 □□□□□ □□□ □□□□ 2,500□ □□□□. □□□□□ □□ □□□□□ □□□□□. Microsoft Entra □□ □□□ □□ □□□□□□ □□ □□□□ □□□ □□□ Microsoft 365 E5 □□□ □□ □□□□□□. □□ □□□□ □□ □□□□ □□□□□ □□□ Microsoft 365 E3 □□□□□ □□□□ □□□. □□ □□□ □□□□ □□□?
A. Set-WindowsProductKey cmdlet
B. Microsoft Entra □□ □□□ □□□□ □□□□
C. Microsoft Entra □□ □□□ ID □□□□ □□□□
D. Microsoft 365 □□ □□□ □□□□ □□
Answer: B (LEAVE A REPLY)

NEW QUESTION: 29
□□□ □□ □□□ □□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□.
□□□□ □□ □□ □□ □ □□ □□□□, □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
The users must first: Register for multi-factor authentication (MFA)
You must configure: A user risk policy
According to Microsoft SC-300 official learning materials and Exam Ref SC-300: Microsoft Identity and Access Administrator, when the requirement is to address the probability that user identities were compromised, the appropriate feature is Azure AD Identity Protection. Identity Protection detects risky sign- ins and risky users through continuous analysis of login behavior, location, device, and credential exposure signals.

Two types of policies can be created:
* Sign-in risk policy - Triggers actions based on suspicious sign-in behavior (for example, unfamiliar location).
* User risk policy - Triggers actions when the user's overall identity is deemed at risk (for example, compromised credentials).
The documentation specifies:
"When user risk is detected, the policy can require the user to change their password to remediate the risk.
Users must first be registered for MFA to perform secure password change operations." Therefore, before the user risk policy can be enforced, users must be enrolled in multi-factor authentication (MFA). MFA is used during the remediation step (password change) to verify the user's identity securely.
Thus, to meet the requirement for "the probability that user identities were compromised," you configure a user risk policy in Azure AD Identity Protection, and ensure that users first register for MFA so that they can complete password change or verification flows when risks are detected.

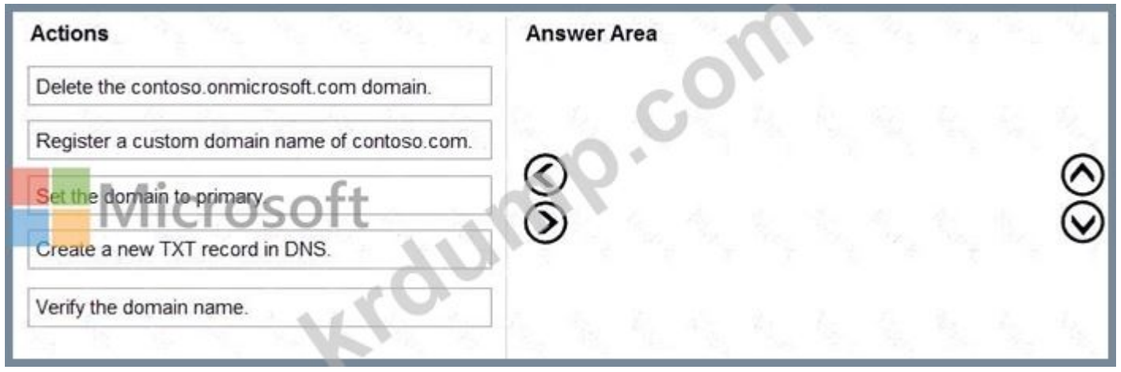
NEW QUESTION: 30
Active Directory □□□□ □□□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□□ □□□□□□ □□□□□ Active Directory □□□□ □□□□ VPN □□□ □□□□ □□□□. VPN □□□ Azure Multi-Factor Authentication(MFA)□ □□□□ □□□□.
VPN □□□ □□ Azure MFA□ □□□□ □□□□ □□□□ □□□.
□□□□□ □□□ □□□□ □□□?
A. Azure AD □□□□□□ □□□
B. Azure AD □□ □□ □□□
C. □□□□ □□ □□(NPS)
D. □□□□ □□ □□□
Answer: C (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Exam Study Guide and Microsoft Learn module "Implement and manage hybrid identity with Azure AD Connect" , when a VPN solution authenticates users through an on-premises Active Directory and does not natively support Azure MFA, the correct method is to integrate Azure MFA using the Network Policy Server (NPS) extension for Azure MFA.
The NPS extension acts as an intermediary between the VPN server and Azure AD. The VPN server sends authentication requests to the NPS server. The NPS server validates the credentials against the on-premises Active Directory, and then the NPS extension triggers the Azure MFA challenge for secondary authentication.
Microsoft documentation states:
"To enable Azure Multi-Factor Authentication for on-pre mises resources such as VPNs, RD Gateway, and other services using RADIUS authentication, you must install the Azure MFA extension for the Network Policy Server (NPS)." Therefore, the correct recommendation is to deploy and configure NPS on-premises, install the Azure MFA NPS Extension, and configure the VPN server to forward RADIUS requests to NPS.

NEW QUESTION: 31
ADatum □□□ □□□ □□□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. PowerShell□□ Set-ADSyncScheduler□ □□□□□.
B. PowerShell□□ Start-ADSyncSyncCycle□ □□□□□.
C. Microsoft Azure Active Directory Connect □□□□□ □□□ □□□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
The SC-300 coverage of Azure AD Connect explains that when you need to bring in a new set of on-premises users or change what is synchronized (for example, adding an additional domain/OU such as ADatum or adjusting filtering), you reopen the Azure AD Connect wizard and choose "Customize synchronization options." The guide notes that this path lets you "modify directory/OU filtering, add or remove forests, and enable optional sync features" so that only the intended users are synchronized. It contrasts with operational commands: Start-ADSyncSyncCycle merely triggers an immediate delta/full sync of the

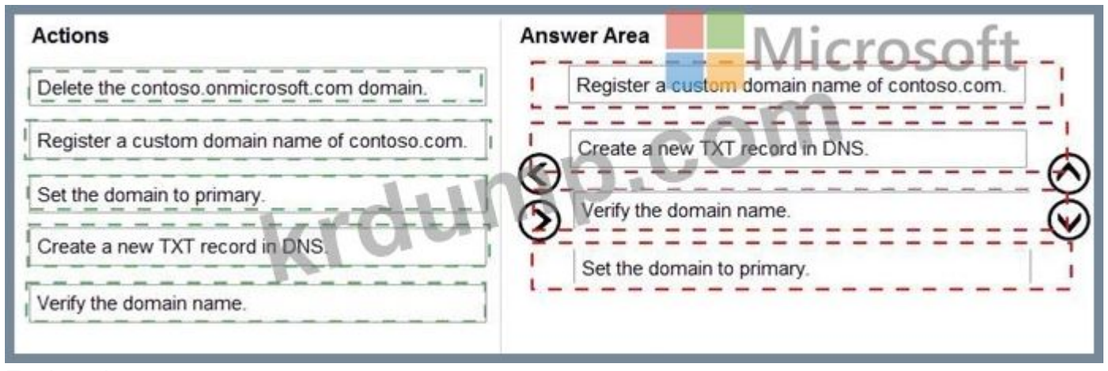
current configuration; Set-ADSyncScheduler changes the sync cadence or pause/resume behavior; and "Change user sign-in" alters the authentication method (e.g., PHS vs. PTA) but does not control scoping of which users are synced. To meet a requirement to sync the ADatum users according to technical constraints (such as OU
/domain selection or feature toggles), you must first configure the scope by running the wizard and selecting Customize synchronization options, then perform/allow a sync cycle to bring those users into Azure AD as defined.

NEW QUESTION: 32
Site1□□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□. □□□□ Site1□□ 1□□ 50□□ □□ □□□ □□□□□□ □□ □□□ □□□ □□□.
Microsoft Defender for Cloud Apps □□□□ □□ □□□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□ □□
C. □□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
To detect and get alerts when a user downloads a large number of files in a short period of time (for example, more than 50 files within one minute) in Microsoft SharePoint Online , you must configure an Activity policy in Microsoft Defender for Cloud Apps (MCAS) .
* Activity policies monitor specific user actions (upload, download, delete, share, etc.) and can trigger alerts based on thresholds or frequency.
* Anomaly detection policies detect behavioral anomalies automatically (not threshold-based).
* Session policies apply real-time controls during sessions (e.g., block download).
* File policies monitor or classify files at rest.
From Microsoft's documentation:
"Activity policies let you monitor specific activities in your cloud apps and define actions or alerts when certain criteria are met, such as excessive downloads or mass deletions." Thus, for detecting a user who downloads more than 50 files in one minute - an Activity policy is required.

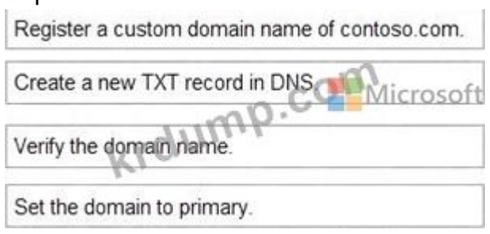
NEW QUESTION: 33
contoso.onmicrosoft.com□□□ □□□ □□□ □□□□ □□□ Microsoft 365 □□□□ □□□□.
□□□ □□□□□ contoso.com□□□ □□□ □□□□□.
□□□ Microsoft 365 □□□□ □□ □□ □□□ □□□□ contoso.com□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation under "Add and configure custom domains in Microsoft 365", when an organization acquires a new Microsoft 365 tenant, it starts with a default domain such as contoso.onmicrosoft.com . To use a friendly and company-branded domain like contoso.com for email and user principal names (UPNs), administrators must follow a specific sequence of steps to integrate the custom domain into Azure AD
/Microsoft 365.

Step 1 - Register a custom domain name of contoso.com First, register the custom domain in Azure Active Directory. This action adds contoso.com to your tenant and prepares Microsoft 365 to validate ownership.

Step 2 - Create a new TXT record in DNS After adding the domain, Microsoft 365 provides a TXT record to add to your DNS zone (at your registrar or DNS host). This record proves that your organization owns the domain.

Step 3 - Verify the domain name Once the TXT record is published and propagated, return to the Microsoft
365 admin center or use PowerShell to verify the domain. This step confirms domain ownership and completes the domain setup.

Step 4 - Set the domain to primary Finally, after verification, set contoso.com as the primary domain. Doing this ensures that all newly created users automatically receive user principal names (email addresses) ending in @contoso.com .

Microsoft documentation states:

"After verifying ownership of the custom domain, you can set it as the default (primary) domain for new users in Microsoft 365."

NEW QUESTION: 34
Microsoft 365 □□□ □□□□.
□□□□ □□□□□□ □□□□□□□ □□□ □□□□ □□ □□ □□□ □□□ □ □□□ □□ □□□. □□□□ □□□□ □□□□□ □□□ □□□ □□ □□□□ □□□ □ □□□ □□ □□□.
□□ □□□ □□□□ □□□?
A. □□ □□□
B. □□□ □□ □□
C. □□ □□
D. ID □□ □□
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation ("Configure how end-users consent to applications"), application consent management in Microsoft Entra ID is governed by the Admin consent settings under Enterprise applications # Consent and permissions # User consent settings.
By default, users can grant delegated permissions to apps, but organizations often need to restrict which permissions users may consent to - for example, allowing consent only to low-impact permissions like User.
Read (basic profile information).
Microsoft Documentation Reference:
"In the Admin consent settings, you can control how end users grant consent to applications. You can limit user consent to low-risk permissions, such as permissions that only allow apps to access the user's basic profile data." The configuration steps outlined in Microsoft's official SC-300 training materials are:
* In the Entra admin center, go to Enterprise applications # Consent and permissions # User consent settings.
* Under User consent for applications, choose Allow user consent for apps from verified publishers for selected permissions (recommended).
* Under Select permissions to allow, specify User.Read and User.ReadBasic.All, which correspond to User.Read and User.Read profile delegated permissions.
This ensures that users can only consent to applications accessing their basic profile data and no additional permissions beyond what's explicitly approved.
Why not the other options:
* A. Security defaults: Controls basic security policies (e.g., MFA, legacy authentication) - unrelated to app consent.
* C. Permission classifications: Used for labeling permission risk levels but doesn't enforce consent behavior.
* D. Identity Protection settings: Related to risky user or sign-in detections, not app consent control.

NEW QUESTION: 35
□□ □□ □□ □□ □□□ □□□ □□□ User1□□□ □□□□ □□□ 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 □□□□ □□□□ □□□ □ User1□ □□ □□□ □□□□ □□□□ □□□.
□□ □□□ □□□□ □□□?
A. □□□ □□
B. □□ □□ □□
C. What If □□
D. Microsoft 365 □□□□ □□ □□□ □□
Answer: C (LEAVE A REPLY)

According to Microsoft Entra Conditional Access documentation and the SC-300 study guide, the What If tool in Azure AD is specifically designed to simulate Conditional Access policy results for a given user scenario. It allows administrators to input details such as user identity, location (IP address), device state, and application to determine which Conditional Access policies would apply before actual enforcement.
From Microsoft documentation:
"The What If tool allows admins to simulate a sign-in event for a specific user and evaluate which Conditional Access policies will be applied or excluded." Other options do not serve this function:
* Access Reviews: Used for periodic access validation, not policy simulation.
* Identity Secure Score: Provides improvement recommendations, not policy evaluation.
* Microsoft 365 network connectivity test tool: Tests network connectivity, not policy application.

NEW QUESTION: 36
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)
Attribute-Based Access Control (ABAC) in Azure enhances role-based access control (RBAC) by adding conditions based on attributes of the user, resource, or environment.
Currently, ABAC is supported only for Azure Storage (Blob and Queue) when used with the appropriate data plane roles, such as Storage Blob Data Reader, Storage Blob Data Contributor, or Storage Blob Data Owner.
In the scenario:
* User1 (Reader) and User2 (Contributor) are assigned management plane roles, not ABAC-supported data roles.
* User3 (Storage Blob Data Reader) is assigned a data plane role, which supports ABAC.
* User4 (Virtual Machine Contributor) also has a management plane role.
Therefore, only User3's role supports ABAC.
Microsoft documentation confirms:
"ABAC is currently supported for Azure Storage when using Azure RBAC roles such as Storage Blob Data Reader or Contributor. ABAC allows conditions on user or resource attributes for fine-grained access."

NEW QUESTION: 37
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

Name	Role
User1	*None*
User2	Privileged Authentication Administrator
User3	Global Administrator

Azure AD Privileged Identity Management(PIM)□□ □□ □□□ □□ □□□ □□□ □□□ □□□□□.

Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

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

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.	○	○
User2 can approve all activation requests for the Global Administrator role.	○	○
User2 and User3 can edit the Global Administrator role assignment.	○	○

Answer:

Explanation:

In Azure AD Privileged Identity Management (PIM), the activation settings shown for the Global Administrator role include "On activation, require Azure MFA: Yes." The SC-300 materials describe that when this flag is enabled, "eligible users must complete MFA during role activation." Therefore, User1, who is eligible for Global Administrator, must satisfy MFA at activation time.

The exhibit also shows "Require approval to activate: No (Approvers: None)." Per the exam guide, "if approvals are not required, no approver action is taken; users activate directly after satisfying policy (e.g., MFA, just ification)." Consequently, there are no activation requests to approve, so User2 cannot approve all activation requests (there are none).

Regarding who can change role assignments, the guide states that "only Global Administrator or Privileged Role Adminis trator (Role Management Administrator) can add, remove, or update Azure AD role assignments in PIM." Privileged Authentication Administrator focuses on authentication method and MFA settings and does not grant role-assignment management. Thus, User2 (Privileged Authentication Administrator) cannot edit the assignment, while User3 (Global Administrator) can; since the statement claims both can edit, the correct evaluation is No.

NEW QUESTION: 38

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

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 10	Microsoft Entra joined
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

Microsoft Entra Private Access□ □□□□□ □□□. □□□□ □□□ Global Secure Access □□□□□□ □□□□□. □□ □□□□ Private Access□ □□□ □ □□□□?

A. Device2□ Device4□

B. Device2□

C. Device1, Device2, Device3□

D. Device1□

E. Device1, Device2, Device3, Device4

Answer: (SHOW ANSWER)

NEW QUESTION: 39

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

Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

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

□□□ □□□□ □□□?

A. Microsoft 365 Defender □□

B. Microsoft 365 □□ □□

C. Microsoft Entra □□ □□

D. Microsoft Purview □□ □□ □□

Answer: (SHOW ANSWER)

To compare and analyze role permissions of multiple users within an Azure AD tenant, the correct and most efficient tool is the Microsoft Entra admin center.

According to the Microsoft Identity and Access Administrator Study Guide and Microsoft Entra documentation, the Entra admin center provides the Roles and Administrators blade where administrators can:

* View all directory roles.

* Compare role permissions and assignments.

* See which users have which roles and what each role allows.

The guide clarifies:

"Administrators can use the Entra admin center to view and compare role definitions and assigned members without using additional portals or manual PowerShell scripts." The other options serve different purposes:

* Microsoft 365 Defender portal focuses on security incidents and threat management.

* Microsoft 365 admin center handles licensing and user management but not detailed role comparison.

* Microsoft Purview compliance portal deals with compliance, data governance, and auditing.

NEW QUESTION: 40

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

Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

Azure Portal□ □□□□ Role3□□□ □□□ □□ Azure □□ □□□ □□□□ □□□. Role3□ □□ □□□ □□ □□□ □□□□□. □□ □□□ □□□□ Role3□ □□ □ □□□□?

A. Role2□

B. □□ □□ Azure □□ □□□

C. □□ □□ Azure □□ □□ □ Role2□ □□

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

E. Role1, Role2 □□ □□ Azure □□ □□ □ □□ □□ Azure AD □□

Answer: C (LEAVE A REPLY)

In Azure RBAC, when creating a custom role through the Azure portal, you can only clone from existing roles of the same scope type. Since Role3 is an Azure subscription-level custom role, it can be cloned only from subscription-level roles-either built-in subscription roles (like Owner, Contributor, Reader) or other custom subscription roles.

Azure AD roles (directory roles) cannot be cloned to create subscription roles because they operate at a completely different control plane (Azure AD vs Azure Resource Manager).

Thus, from the given table:

* Role1 = Azure AD role # cannot be cloned.
* Role2 = Azure subscription role # can be cloned.
Therefore, the correct option is C

NEW QUESTION: 41
User1□□□ □□□□ □□□ Microsoft 365 □□□ □□□□.
User1□ Azure AD □□□ □□ □□□ □□□ □□□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□ □□ □□□
B. □□□□ □□□ □□
C. □□□ □□□
D. □□□ □□□ □□□
Answer: D (LEAVE A REPLY)
The question asks which role allows a user to create access reviews for Azure AD roles using the principle of least privilege.
* Privileged Role Administrator can manage all role assignments and access reviews, but it has more privileges than needed.
* Identity Governance Administrator manages entitlement management and access packages, not Azure AD roles directly.
* User Administrator can manage users but not access reviews for roles.
* # User Access Administrator is the correct least-privilege role, as it allows management of access reviews related to Azure AD roles and role-assignable groups.
From Microsoft Documentation (SC-300 Exam Guide):
"The User Access Administrator role allows management of access reviews and permissions for Azure AD roles and resources using the least-privileged approach."

NEW QUESTION: 42
Azure AD □□□□ App1□□□ .NET □□□ □□□□.
Azure AD □□□ □□ App1□ □□□□ □□□.
App1□ □□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□ ID
C. □□□ □□
D. □□□□ URI
Answer: (SHOW ANSWER)
When registering an application in Azure Active Directory (Azure AD) for authentication, one of the key configuration items is the redirect URI. According to Microsoft Identity Platform Documentation and the SC-
300 official study guide , the redirect URI (or reply URL) specifies where Azure AD should send the authorization code or access token after a successful sign-in.
The guide explains:
"During app registration, Azure AD requires a redirect URI to identify where authentication responses are sent. For web apps, this must be a valid HTTPS endpoint where your app listens for responses from the Azure AD authorization endpoint." In contrast:
* The executable name, bundle ID, and package name are identifiers relevant to desktop or mobile app packaging and are not part of Azure AD web app registration configuration.
* Only the redirect URI ensures proper return of authentication tokens in OAuth 2.0 and OpenID Connect flows.
Thus, when registering a .NET web app (App1) for Azure AD authentication, you must configure the redirect URI to handle token responses securely.

NEW QUESTION: 43

□□ □□ □□□ □□□ □□□ 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: D (LEAVE A REPLY)

Azure AD supports several group types with different membership rules. For Microsoft 365 groups, "group nesting isn't supported; only user identities can be members." For mail-enabled security groups used in Azure AD/Exchange Online, the SC-300 materials emphasize that only user objects are supported as members when managed in Azure AD, while "Microsoft 365 groups can't be added to other groups." Security groups are commonly nestable for access scenarios, but the mail-enabled security group membership experience in Azure AD limits member selection to users; thus you cannot add Group1 (security group) or Group2 (Microsoft 365 group) as members of Group3 (mail-enabled security group). Licensing assignments shown in the table are irrelevant to membership eligibility. Consequently, the only valid members you can add to Group3 are the user objects - User1 and User2.

NEW QUESTION: 44

Azure □□□ □□□□.

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

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

□□: □□ □□□ 1□□□□.

Answer:

First create: # An Azure Automation account

* Distribute Catalog1 by using: # An access package

According to the Microsoft SC-300 study guide and Microsoft Entra Identity Governance documentation, when creating custom extensions for Entitlement Management catalogs, the extensions must be hosted in an Azure Automation account. This automation account provides the execution environment for scripts or runbooks that perform external actions when certain events occur, such as user assignments or access removals.

Entitlement Management in Microsoft Entra (formerly Azure AD) allows administrators to automate user access lifecycle processes through access packages. These packages are distributed to internal or external users and define which resources (applications, groups, teams, or SharePoint sites) they can request access to

- all under a governance framework.

* First create an Azure Automation account

* To use a custom extension in a catalog, Microsoft Entra requires an Azure Automation account.

* The automation account hosts runbooks (PowerShell scripts or actions) that execute when access package events trigger (e.g., user request approval, role assignment, or removal).

* The automation account acts as the backend engine for entitlement management extensions.

Step-by-Step Breakdown: As per Microsoft documentation:

"To add a custom extension to an access package, create an Azure Automation account that contains the runbook to handle the automation triggered by access lifecycle events."

* Distribute Catalog1 by using an access package

* Once the catalog (Catalog1) and custom extension are configured, access to the resources in that catalog is granted through access packages.

* Each access package defines eligibility, approval workflows, and access duration for users.
* Access packages serve as the distribution mechanism of catalogs - users request access through them, and the catalog defines what access is granted.
From Microsoft SC-300 content:
"In Entitlement Management, catalogs define available resources, while access packages define who can request them and under what conditions. Access packages are the method of distributing access in a catalog."

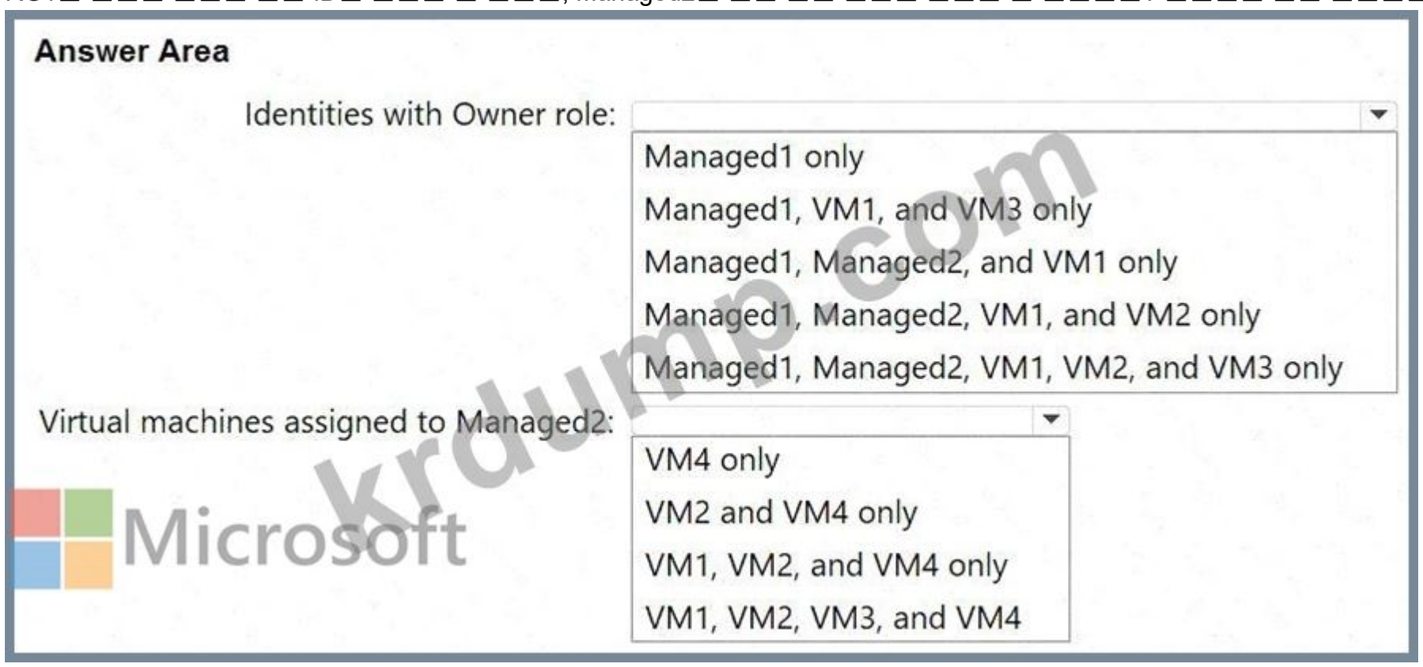
NEW QUESTION: 45
□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type	Location
RG1	Resource group	East US
Managed1	Managed identity	East US
Managed2	Managed identity	West US

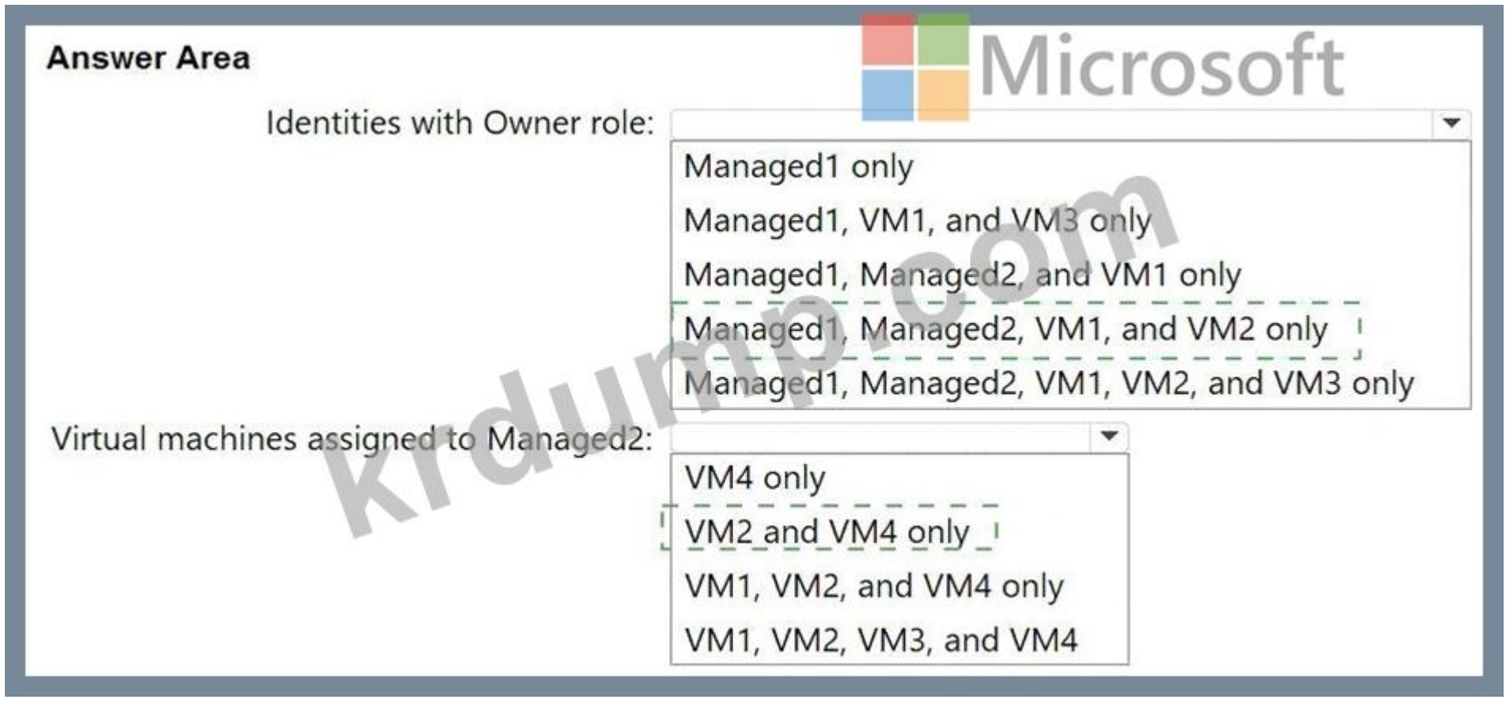
□□□□ □□ □□ □□□ □□ □□□ □□□□ □□□□.

Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VM3	East US	Managed1
VM4	West US	None

RG1□ □□□ □□□ □□ ID□ □□□ □ □□□, Managed2□ □□ □□ □□□ □□□ □ □□□□? □□□□ □□ □□□□ □□□ □□□ □□□□□. □□: □□□ 1□□□□.



Answer:



Explanation:

Identities with Owner role: Managed1, Managed2, VM1, and VM2 only

Virtual machines assigned to Managed2: VM2 and VM4 only

In Azure RBAC, role assignments can be made to Azure AD security principals , including managed identities (user-assigned and system-assigned) . The SC-300 learning path on Identity Governance and Privileged Access, and the Exam Ref coverage of Azure RBAC, explain that a system-assigned managed identity is a service principal tied to a single resource, and you can assign RBAC at any scope (subscription, resource group, or resource) to that identity. A user-assigned managed identity is an independent Azure resource with its own service principal; it can also be granted roles at the resource group scope. Therefore, the assignable principals for RG1 include the two user-assigned identities (Managed1 , Managed2) and the two VMs that have system-assigned identities (VM1 , VM2). VM3 does not present a system-assigned identity; its access is represented by Managed1 .

For attaching a user-assigned identity to a virtual machine, SC-300 materials note that the identity and the target resource must be in the same region (often phrased as "user-assigned identities are regional; the identity and the resource must share a region"). Since Managed2 is in West US , it can be associated only with West US VMs-here, VM2 and VM4 .

NEW QUESTION: 46

□□ 2

Salesforce □□ □□□□ □ □□ □□□ □□□□ □□□□ □□□□□ □□□□ □□□. □□□ □□ □□ □□□ □□□□ □□□.

* □□□ □□ □□□□□ □□□.
* □ □□□ □□□□ □□□□ □□□□ □□□□ □□□.
* □□□ 5□ □□□ □□□□ □□□ □□ □□□ □□□□□.
* □□□ □□□□□ □□□□ □□ □□, Megan Bowen□ □□□□ □□□□ □□□.

Answer:

See the Explanation for the complete step by step solution.

Explanation:

To implement a process for reviewing guest users' access to the Salesforce app with the specified requirements, you can use Microsoft Entra's Identity Governance access reviews feature. Here's a step-by-step guide:
Assign the appropriate role:
Ensure you have one of the following roles: Global Administrator, User Administrator, or Identity Governance Administrator1.
Navigate to Identity Governance:
Sign in to the Microsoft Entra admin center.
Go toIdentity governance>Access reviews1.
Create a new access review:
Select New access review.
Choose the Salesforce app to review guest user access1.
Configure the review settings:
Set the frequency of the review to monthly.
Define thedurationof the review period to5 days1.
Determine the reviewers:
Assign the manager of each guest user as the reviewer.
If a guest user does not have a manager, assignMegan Bowenas the reviewer1.
Automate the removal process:
Configure settings toautomatically remove accessif the review is not completed within the specified time frame1.
Monitor and enforce compliance:
Regularly check the access review results to ensure compliance with the review policy1.
Communicate the process:
Inform all stakeholders about the new review process and provide guidance on how to complete the reviews.
By following these steps, you can ensure that guest users' access to the Salesforce app is reviewed monthly, with managers being responsible for the review, and access is removed if the review is not completed in time.

NEW QUESTION: 47
Azure Active Directory(Azure AD) □□□□ □□□□.
□□□ □□□ □□□□ □□□□□ Azure AD □□□ □□□ □□□□ □□□.
Azure AD□ □□□ □□□ □□□□ □□ □□ □□□□□?
A. 14□
B. 30□
C. 90□
D. 365□
Answer: A (**LEAVE A REPLY**)

In Azure AD Monitoring and Reporting documentation and the SC-300 Study Guide (Module: Monitor and report on identity and access) , sign-in logs in Azure Active Directory are retained for a default duration of 14 days.
The sign-in logs contain information about user sign-in activity, including application usage, conditional access policies, and multi-factor authentication details. These logs are accessible through the Azure portal # Azure Active Directory # Sign-ins, or programmatically via Microsoft Graph.
Microsoft specifies:
"Azure AD stores sign-in activity for 14 days by default. For longer retention, you must integrate with Azure Monitor (Log Analytics), Azure Storage, or Event Hub." This 14-day retention limit applies to tenants without additional premium log retention solutions.

NEW QUESTION: 48
Azure Active Directory(Azure AD) □□□□ □□□□.
□□ □□ □□□□ □□□.
□□ □□ □□ □□□ □□□ □□□□ □□□□□?
A. □□□□ □□
B. □□ IP □□
C. □□□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
SC-300 distinguishes user risk from sign-in risk. The text defines: "User risk is the probability that an identity is compromised," and lists its core detections, including " Leaked credentials detected on public or dark-web sources." By comparison, impossible/anomalous travel and anonymous IP are cited as sign-in risk detections:
"Sign-in risk is calculated per authentication event using detections such as impossible travel, atypical travel, and anonymous IP address ." Therefore, among the options, only leaked credentials is a user risk detection type; the others are sign-in risk indicators used at authentication time. SC-300 also ties user risk to Identity Protection policies that can require password change or block access when a user's credentials are suspected to be compromised.

NEW QUESTION: 49
Azure □□, Google Cloud Platform(GCP) □□, Amazon Web Services(AWS) □□□ □□□□.
□□ □□□□□ □□ □□□ □□□ □□□ □□□ □ □□ □□□□ □□□□ □□□. □ □□□□ □□ □□□ □□□□□ □□□. □□□□□ □□□ □□□□ □□□?
A. Microsoft Sentinel
B. □□□□ □□ Microsoft Defender
C. Microsoft Entra ID □□
D. Microsoft Access □□ □□
Answer: D (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) study materials and Microsoft Learn module: "Manage permissions across multicloud environments" , Microsoft Entra Permissions Management is the dedicated solution for unified Cloud Infrastructure Entitlement Management (CIEM)
. It enables organizations to discover, remediate, and continuously monitor permission risks across Azure , AWS , and Google Cloud Platform (GCP) environments.
Entra Permissions Management automatically integrates with multicloud environments through read-only connectors, allowing you to assess permissions, identify excessive privilege assignments, and recommend least-privilege configurations. It provides a Permissions Creep Index (PCI) score that quantifies risk, helping administrators maintain a principle of least privilege across all platforms - while minimizing manual effort through automated analysis and unified dashboards.
In contrast, Microsoft Defender for Cloud Apps focuses on app discovery and data protection, not infrastructure entitlement management. Microsoft Entra ID Protection monitors risky sign-ins and identities only within Entra ID, while Microsoft Sentinel provides security information and event management (SIEM) but does not evaluate privilege assignments directly.
Therefore, the verified recommendation from the official Microsoft documentation is to use Microsoft Entra Permissions Management for unified, automated privilege risk assessment across Azure, AWS, and GCP.

Correct Answer: D. Microsoft Entra Permissions Management

NEW QUESTION: 50
Microsoft Entra □□□□ □□□□.
□□□□ □□ □□□ □□□ □□□ □□□□ □□□.
□□□ □□□ □□ □□□ □□□ □□□□ □□□□□?
A. 30□
B. 60□
C. 90□
D. 180□
Answer: C (LEAVE A REPLY)
According to the Microsoft Entra ID Protection section of the SC-300 Study Guide and the official Microsoft documentation on risk detections and retention , Microsoft Entra ID stores risky user activity and detections for 90 days . This includes logs of risky users, risky sign-ins, and risk detections identified by machine learning models and heuristic signals.
The retention period of 90 days ensures administrators can analyze user risk patterns, investigate compromised accounts, and implement mitigations such as Conditional Access or user risk policies. After 90 days, these logs are automatically purged unless exported to a SIEM such as Microsoft Sentinel for extended retention.
Microsoft Learn states:
"Identity Protection retains data for 90 days. Administrators can view risk detections, risky users, and risky sign-ins in the portal or query them using Microsoft Graph."

NEW QUESTION: 51
□□□□ Microsoft 565 ES □□□ □□□□□□.
User1□□□ □□□□□ □□ □□□ □□□ □□□□□□□.
User1□ Microsoft Defender for Cloud Apps □□ □□□ □□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□□ □□□□□□ □□□ □□□ □□□□ □□□□□.
B. User1□□ Cloud App Security □□□ □□□ □□□□□.
C. □□□ □□□ □□□ □□□ □ □□ □□ □□□ □□□□□.
D. □□□ □□□ □□□ □□□ □□□ □□□ □ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)

NEW QUESTION: 52
User1□□□ □□□□ □□□ Azure □□□ □□□□. □□ □□ □□□ □□□□ □□□.
* User1□ □□ □□□ □□ □□□□ □□□□ □□ □□□□□.
* User1□ □□□□□□ □□□ □□□ □□□ □ □□□ □□□□□.
* User2□ □□ □□□ □ □□□ □□□□□.
* □□ □□□ □□□ □□□□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□□□□ □□□
B. □□□□ □□□□□□ □□□
C. □□□ □□ □□□
D. □□□□□□ □□□
Answer: (SHOW ANSWER)

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn documentation on Azure AD roles and permissions , the Cloud Application Administrator role provides privileges to manage applications while enforcing the principle of least privilege.
The scenario requires:
* Preventing User1 from being added as an owner of newly registered apps.
* Allowing User1 to manage Application Proxy settings (used for publishing on-premises apps through Azure AD).
* Allowing User2 to register new applications.
* Application Administrator: Can create and manage all app registrations and enterprise apps, and can add owners - too permissive for this requirement.
* Cloud Application Administrator: Can manage applications, including Application Proxy settings, but cannot assign application owners or grant broad permissions.
* Application Developer: Can only register and manage own applications.
* Service Support Administrator: Provides service health access - not relevant here.
Role Comparison (from Microsoft documentation): Thus, to let User1 manage Application Proxy and prevent assigning ownership of new apps, Cloud Application Administrator is the correct and least-privileged choice.

NEW QUESTION: 53
□□□ Microsoft Entra □□□□ □□□□ □□□□.
□□ □□ □□□□ □□□□ □□□□ □□□□ □□□ □ □□□ □□ □□□.
□□ □□□ □□□□ □□□?
A. □□□ □ □□□ □□
B. □□ □□ □□
C. □□ □□
D. □□ ID □□□□
Answer: B (LEAVE A REPLY)
According to the Microsoft Entra External Identities module within the SC-300 curriculum, control over which external domains can be invited as guest users is managed under External collaboration settings i n the Entra admin center.
Administrators can specify "Allow invitations only to the specified domains" and list approved domains.
This ensures that guest invitations can only be sent to trusted business partners while blocking all others.
Cross-tenant access settings control authentication and access policies between trusted tenants, not invitation restrictions. Linked subscriptions and identity providers manage billing and authentication federation but do not control guest invitations.
Therefore, to re strict guest invitations to specific external domains, you must configure the External collaboration settings in Microsoft Entra ID.

NEW QUESTION: 54
□□□□□□ Microsoft Entra Connect□ □□□□ Microsoft Entra □□□□ □□□□□ contoso.com□□□ □+□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□ □□ □□□□ □□ □□ □□□□.

Name	User principal name (UPN)	Proxy addresses
User1	user1@contoso.com	smtp: user1@contoso.com smtp: sales@contoso.com
User2	user2@contoso.com	smtp: user2@contoso.com smtp: user.2@contoso.com smtp: service@contoso.com

Active Directory □□□ □ □□□□□ □□ □□□□ □□□□□.
* □□ : User3

* UPN: user3@contoso.com
* □□□ □□: smtp: user3@contoso.com, smtp: sales@contoso.com

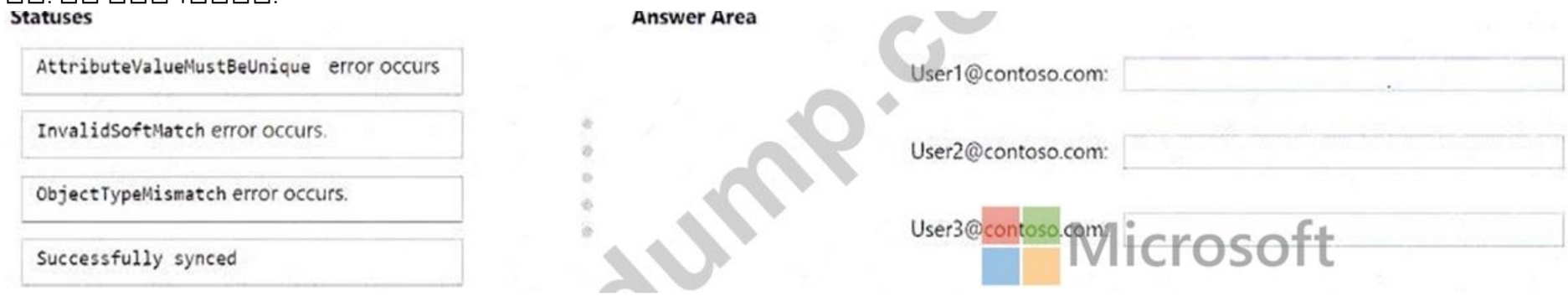
Active Directory □□□ □ □□□□□ □□ □□ □□□ □□ □ □□□□ proxyAddresses □□□ □□□□□□□.

Name	Proxy address
User1	smtp: admin@contoso.com
User2	smtp: sales@contoso.com

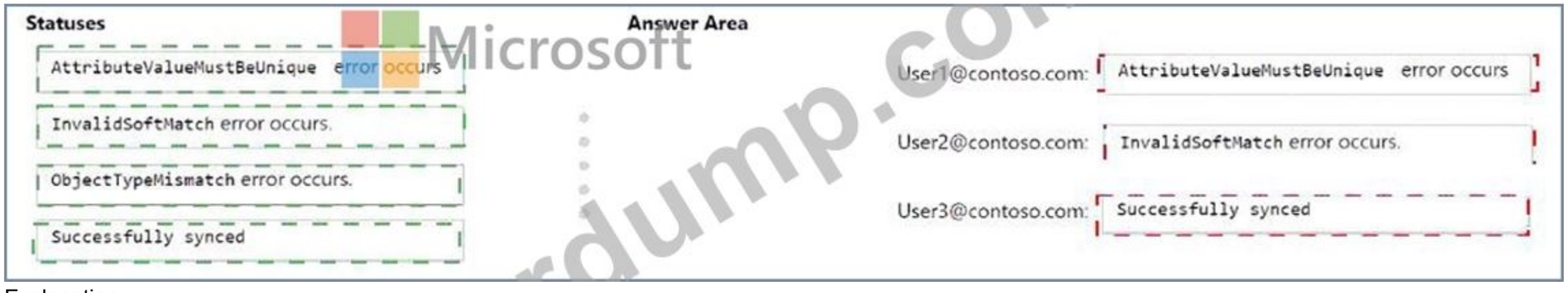
□□ □□□□ □□□□□.

Microsoft Entra Connect □□□□ □ □□□□□ □□ □□□ □□□ □□□□□? □□ □□□□ □□ □□□ □□ □□□□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □ □□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

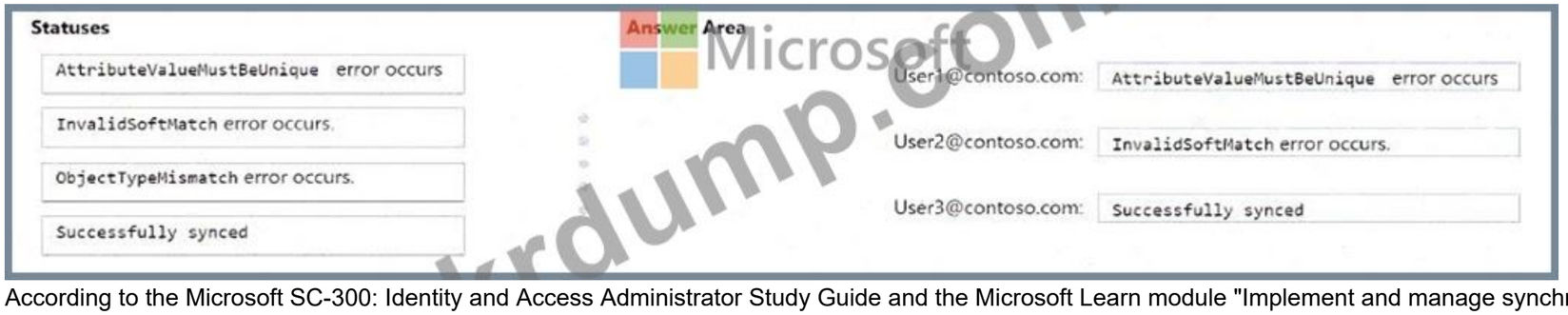
□□: □□ □□□ 1□□□□.



Answer:



Explanation:



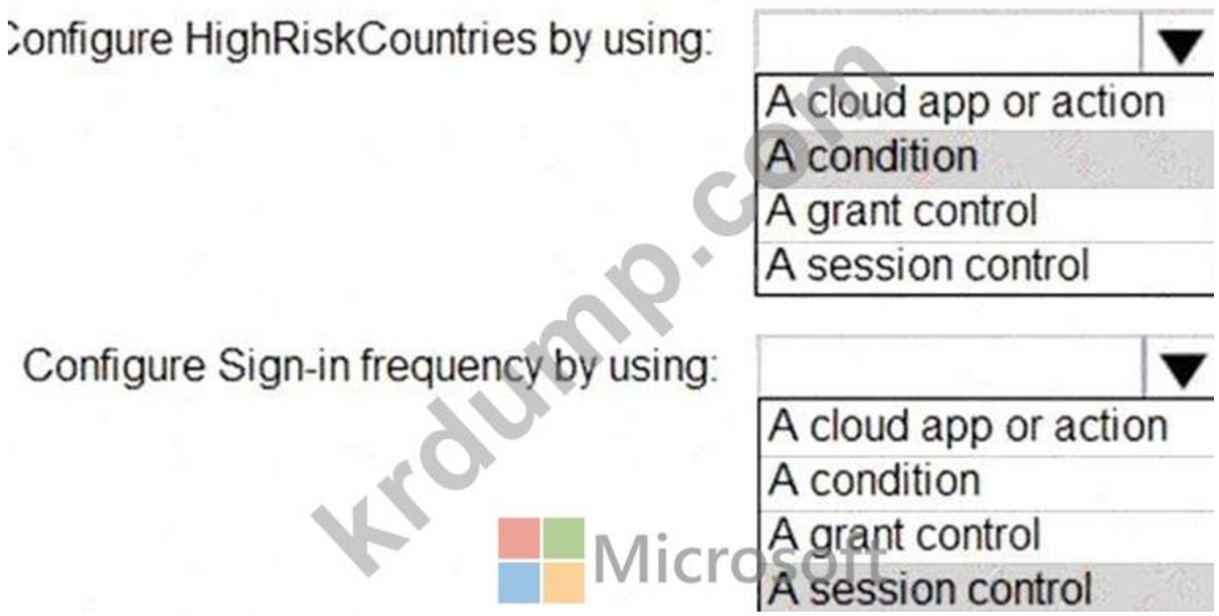
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Implement and manage synchronization with Microsoft Entra Connect", when Microsoft Entra Connect synchronizes user objects between on-premises Active Directory (AD) and Microsoft Entra ID (formerly Azure AD), each user must have unique proxyAddresses attributes across the directory.

The proxyAddresses attribute represents all the email aliases (SMTP addresses) associated with a user. The synchronization process verifies these values to ensure they are not duplicated among multiple user objects. If two or more objects in AD share the same SMTP address, the synchronization process generates an error, typically reported as a "Duplicate Attribute" conflict.
In the provided scenario:
* User1 (proxyAddresses: user1@contoso.com, sales@contoso.com)
* User2 (proxyAddresses: user2@contoso.com, user.2@contoso.com, service@contoso.com)
* User3 (proxyAddresses: user3@contoso.com, sales@contoso.com)
After updating the proxy addresses:
* User1 # admin@contoso.com
* User2 # sales@contoso.com
Because sales@contoso.com is now used by both User2 and User3, the sync process detects a duplicate SMTP address. This causes synchronization errors for User2 and User1 if any other duplicates exist. User3, with unique attributes, synchronizes successfully.
The SC-300 reference under "Manage synchronization errors using Microsoft Entra Connect Health" confirms:
"If two or more objects contain the same value for attributes marked as unique (such as proxyAddresses or userPrincipalName), Microsoft Entra Connect synchronization fails for those objects until the conflict is resolved."

NEW QUESTION: 55
Microsoft 36S □□□□ □□□□.
□□□ □□ □□□ □□□ HighRiskCountries□□ □□□ □□□ □□□□.
□□□□ □□ □□□□ □□□□ □□ □□□□ □□ □□□ □□□ □ □□ □□□ □□□□ □□□.
□□□ □□□ □□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:



According to the Microsoft SC-300: Identi ty and Access Administrator Study Guide and the Microsoft Learn module "Implement Conditional Access Policies," the Azure AD Conditional Access engine uses a structured framework that consists of conditions, grant controls, and session controls.

1# # Configure HighRiskCountries by using A condition In Conditional Access, conditions define the circumstances under which a policy applies. Named locations (such as HighRiskCountries) are part of the Locations condition. When configuring a Conditional Access policy, administrators can include or exclude sign-ins based on IP address ranges, country/region, or named locations.

Microsoft documentation states: "You can define named locations to specify IP ranges or countries/regions and use them as conditions in your C onditional Access policies." Thus, HighRiskCountries should be configured as a condition within the policy to target sign-ins from those regions.

2# # Configure Sign-in frequency by using A session control Session controls in Conditional Access determine how sessions behave after a user successfully signs in. The Sign-in frequency setting controls how often users must reauthenticate, effectively limiting the duration of their authentication session.

Microsoft Learn reference: "Session controls, such as sig n-in frequency and persistent browser session, enable administrators to enforce how often users must reauthenticate." Therefore, to restrict how long a user can remain authenticated when signing in from high-risk countries, you configure Sign-in frequency as a session control.

Final Correct Answers:

* HighRiskCountries: A condition
* Sign-in frequency: A session control

NEW QUESTION: 56

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

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

Admin4□ "Azure □□□ □□ □□ □□ □□ □□" □□□□ □□□□ Policy1□□□ □□□ □□□ □□□ □□□□.
□□□ □□□□ □ □□ □□ □□(MFA)□ □□□□ □□ □□□□ □□□□□?

A. Admin1 □ Admin4□
B. Admin1, Admin2, Admin3□
C. Admin2 □ Admin3□ □□
D. Admin1, Admin2, Admin3, Admin4
Answer: (SHOW ANSWER)

NEW QUESTION: 57
conto.so.com□□□ Azure Active Directory(Azure AD) □□□□ □□□, □ □□□□ Azure AD Identity Protection□ □□□□□ □□□□. □□□□ □□□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?

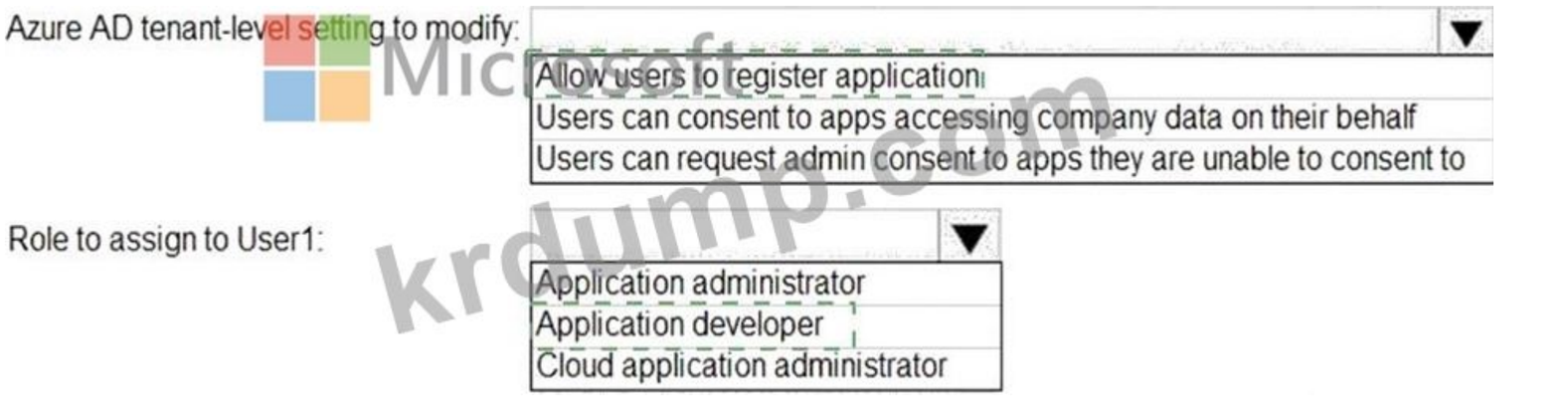
A. Azure AD□□ □□□ □□□ □□□□□.
B. Azure AD □□ □□□ □□□□□.
C. □□ □□□□ □□ □□ □□ □□(MFA)□ □□□□□.
D. □□ □□□□ □□ □□ □□□ □□□□ □□□(SSPR)□ □□□□□.
Answer: C (LEAVE A REPLY)
Azure AD Identity Protection helps detect risky sign-ins and risky users. To mitigate these risks without blocking user access, Microsoft recommends configuring sign-in risk policies to enforce MFA rather than block sign-ins.
From the SC-300 documentation:
"When you want to remediate sign-in risk without blocking users, configure a Conditional Access or Identity Protection policy to require MFA when a risky sign-in is detected." This approach allows users to verify their identity and continue to sign in securely, rather than being blocked outright.
Hence, to implement sign-in risk remediation without blocking users, the first step is to enable and enforce MFA for all users so that users can self-remediate risky sign-ins.

NEW QUESTION: 58
□□ □□ □□□ □□□□□ Azure AD□□ □ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□□□: □□□ □□□ □□□ 1□□ □□□□□.

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

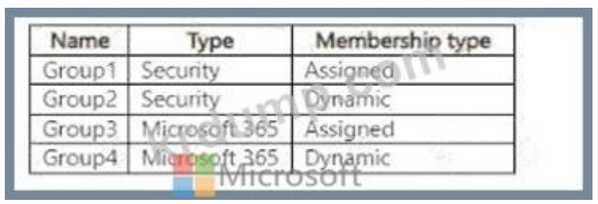
Answer:



Explanation:

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

NEW QUESTION: 59
□□ □□ □□□ □□□ □□□ Microsoft Entra □□□□ □□□□.

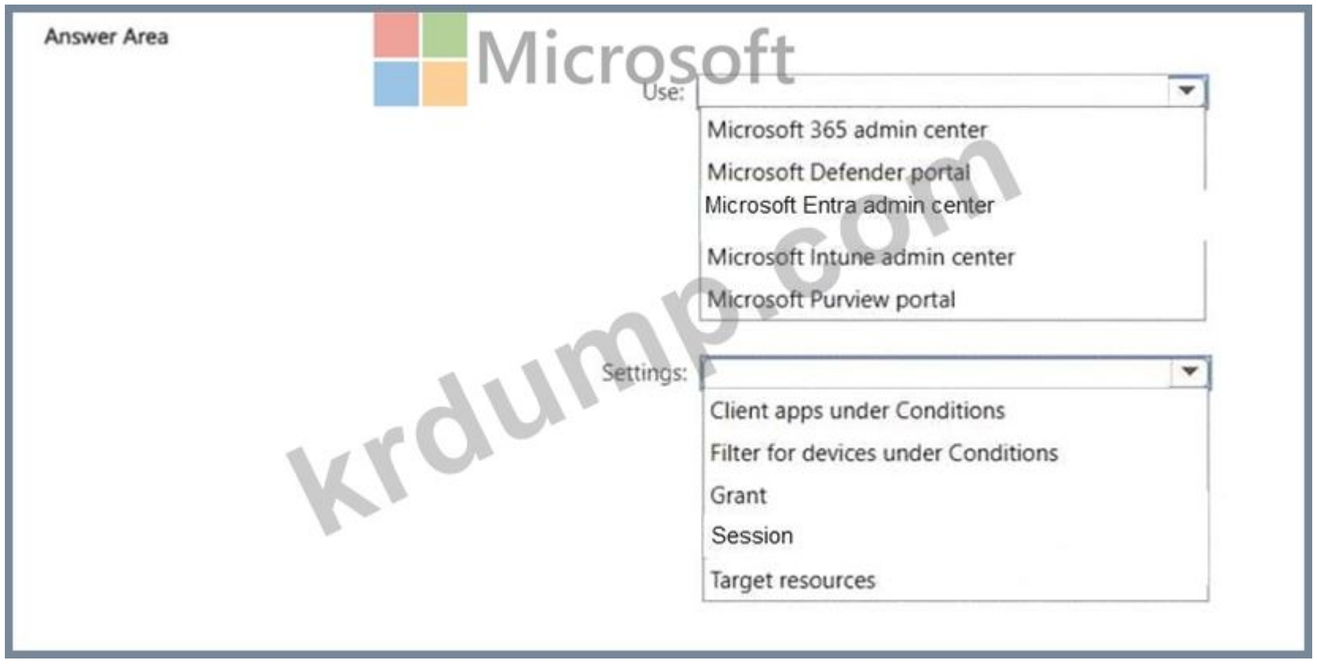


Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic
Group3	Microsoft 365	Assigned
Group4	Microsoft 365	Dynamic

□□□ □□ PIM(Privileged Identity Management)□ □□□□ □□□.
PIM□ □□□□ □□ □□□ □□□ □ □□□□?
A. □□1□
B. □□1□ □□2□
C. Group1□ Group3□
D. □□3□ □□4□
E. □□1. □□2. □□3. □□□ □□4
Answer: (SHOW ANSWER)

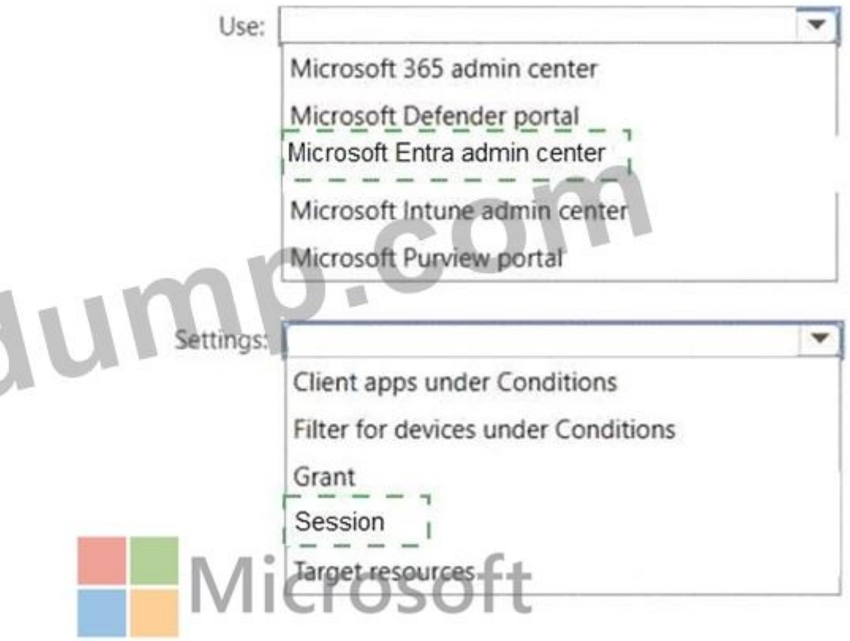
Privileged Identity Management (PIM) for groups in Microsoft Entra ID can only be applied to eligible assignment groups, specifically security groups and Microsoft 365 groups that have a membership type of Assigned. According to Microsoft documentation ("Manage Privileged Access Groups in PIM"), only assigned groups can be enabled for PIM. Dynamic groups are not supported for PIM because their memberships are automatically managed based on rules, and PIM requires manual activation and approval for eligible roles or memberships.
From the official study guide and Microsoft Learn module "Implement Privileged Identity Management (PIM) for Groups":
"Only groups with an Assigned membership type can be managed in Privileged Identity Management.
Dynamic membership groups cannot be enabled for privileged access."
Therefore, among the listed groups:
* Group1 (Security, Assigned) # Supported
* Group2 (Security, Dynamic) # Not supported
* Group3 (Microsoft 365, Assigned) # Supported
* Group4 (Microsoft 365, Dynamic) # Not supported
# Correct Answer: C. Group1 and Group3 only

NEW QUESTION: 60
Microsoft 365 E5 □□□ Policy1□□□ □□□ □□□ □□□ □□□□. □□ □□□ □□□□ □□□.
* Custom1□□□ □□□ □□□ □□□ □ □□□ □□□ □□ □□□ □□□□□.
* Custom1□ □□□□□ □□□ □□□□□!
Custom1□ □□□□□ □□□ □□□□ □□, □□□ □□ □□□□ □□□ □□□ □ □□□ □□□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Answer Area



Explanation:

Answer Area

NEW QUESTION: 61

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

Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1□ Group1□ □□□□□□.

□□ □□□ □□□ □□□ □□□ □□□□□.

□□□ □□: Teams + Groups

□□: □□ □□□

□□: □□1

□□□: □□□□ □□□ □□□□ □□□□□.

□□ □□□□ User3□ □□ □□ □□□ □□□ □ □□□?
A. User1□
B. User3□
C. User1□ User2□
D. User1, User2, User3
Answer: (SHOW ANSWER)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on the Microsoft Entra access review settings and the principles outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Access Review Settings:
What to review: Teams + GroupsThis indicates that the access review is evaluating memberships in Teams and Groups within the Microsoft Entra tenant. Since the group specified is Group1, the review focuses on Group1 membership.
Scope: All usersThe scope defines who is being reviewed. "All users" in this

NEW QUESTION: 62
□□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.

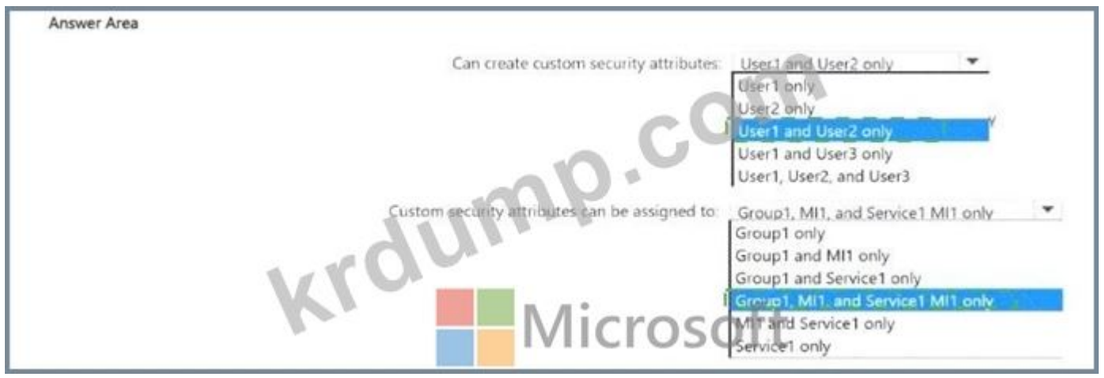
Name	Microsoft Entra role
User1	Global Administrator
User2	Attribute Definition Administrator
User3	Security Administrator

□□□□ □□ □□ □□□ □□□ □□□□□.

Name	Type
Group1	Security group
Service1	Service principal
MI1	Managed identity

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

Answer:



Explanation:

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation ("Manage and use custom security attributes in Microsoft Entra ID") , custom security attributes allow administrators to define key-value pairs that can be applied to various Microsoft Entra objects. These attributes can be used for fine-grained access control, app governance, and conditional policies.

Who can create custom security attributes:

Custom security attributes can only be created and managed by users assigned either of these roles:

* Global Administrator
* Attribute Definition Administrator

The Security Administrator role does not have the permissions required to create or modify attribute schema definitions.

Hence, from the table:

* User1 (Global Administrator) #
* User2 (Attribute Definition Administrator) #
* User3 (Security Administrator) #

Therefore, User1 and User2 only can create custom security attributes.

To which identities can custom security attributes be assigned:
As per Microsoft documentation:
"Custom security attributes can be assigned to supported Microsoft Entra objects, including users, groups, service principals, and managed identities." This means attributes can be attached to:
* Group objects (Group1) #
* Managed identities (MI1) #
* Service principals (Service1) #
Thus, the correct assignable identities are Group1, MI1, and Service1 only.

NEW QUESTION: 63
□□□ □□ □□ □□□ □□□□ □□□ Microsoft Entra □□□□ □□□□ □□□□.

Name	Role
Admin1	Global Administrator
Admin2	Attribute Assignment Administrator
User1	User

□□ □□□□ □□ □□ □□□ □□□ □□□□□.

Name	Type
Group1	Security group
Service1	Service principal

Custom1□□□ □□ □□□ □□□, □ □□□□ □□ □□ □□□ □□□ □□ □□ □□□ □□□□ □□□□.

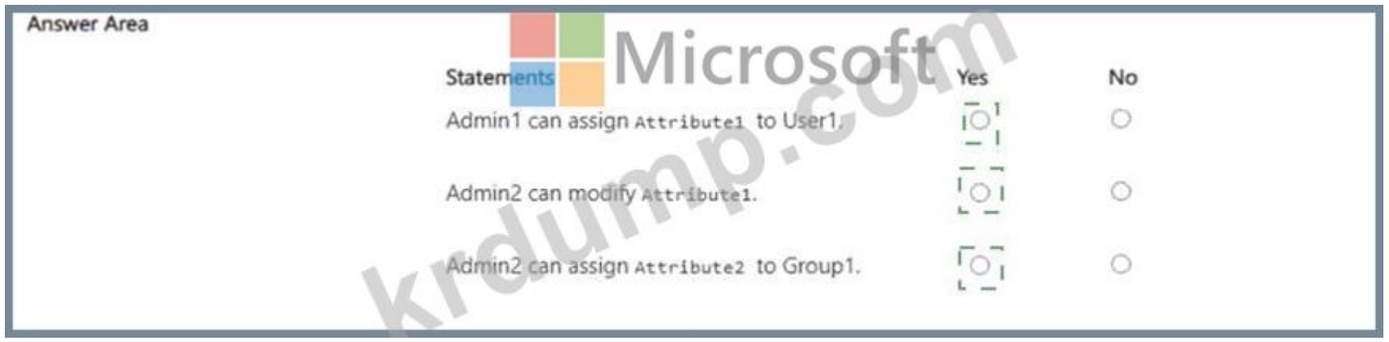
Name	Type
Attribute1	String
Attribute2	Integer

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

Answer Area

Statements	Yes	No
Admin1 can assign `Attribute1` to User1.	○	○
Admin2 can modify `Attribute1`.	○	○
Admin2 can assign `Attribute2` to Group1.	○	○

Answer:



Explanation:

NEW QUESTION: 64

Microsoft 365 □□□□ □□□□.

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

□□ □□ □□□ □□ □□□?

A. Get-AzureADAuditDirectoryLogs cmdlet□ □□□□□.

B. Azure AD □□ □□□ □□□□.

C. Set-AzureADTenantDetail cmdlet□ □□□□□.

D. Azure AD□ □□ □□ □□□ □□□□□.

Answer: (SHOW ANSWER)

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and Microsoft Learn module: "Monitor and troubleshoot Azure Active Directory", to integrate Azure Active Directory audit logs with Azure Monitor, Log Analytics, or Event Hubs, you must first configure Diagnostic settings in Azure AD.

Azure AD logs - including Audit Logs and Sign-in Logs - are stored natively within Azure AD for a limited retention period (14-30 days, depending on license). However, to analyze these logs over time, perform custom queries, or integrate them with monitoring or SIEM solutions, administrators must send them to Azure Monitor logs, Azure Storage, or Event Hubs.

The official documentation explicitly states:

"To send Azure AD logs to Azure Monitor, create a diagnostic setting in Azure Active Directory. From there, select which log categories (AuditLogs, SignInLogs, or NonInteractiveUserSignInLogs) you want to send to a Log Analytics workspace, Event Hub, or storage account." Steps outlined in the study guide and Microsoft Learn:

* Sign in to the Azure portal as a Global Administrator.
* Navigate to Azure Active Directory # Diagnostic settings.
* Select Add diagnostic setting.
* Choose the log categories (e.g., AuditLogs, SignInLogs).
* Select a destination - for instance, a Log Analytics workspace (for Azure Monitor integration).

This configuration is required before Azure Monitor can query or visualize Azure AD audit data.

NEW QUESTION: 65
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)
According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn module "Manage External Identities" , when granting external users (such as contractors) access to Azure AD resources, the recommended method is to invite them as guest users (B2B collaboration users) into your Azure AD tenant.
The New-AzureADMSInvitation cmdlet is the PowerShell command used to create an Azure AD B2B guest invitation. It sends an invitation to an external user (such as user1@outlook.com) and, upon acceptance, creates a corresponding guest user account in the tenant (for example, user1_outlook.com#EXT#@contoso.
com). This account can then be assigned to enterprise applications like App1.
From Microsoft documentation:
"To provide external users access to resources in your organization, invite them as guests using Azure AD B2B collaboration. You can do this by running the New-AzureADMSInvitation cmdlet or via the Azure portal."
* B. Configure the External collaboration settings: These settings define collaboration policies (who can invite guests, restrictions, etc.) but do not invite users themselves.
* C. Add a WS-Fed identity provider: This is used to federate another identity provider (e.g., ADFS or another Azure AD tenant), not to onboard an individual external user.
* D. Implement Azure AD Connect: This tool synchronizes on-premises directories with Azure AD; it's not relevant for external users from Outlook.com.
Why not the other options: # Correct Answer: A. Run the New-AzureADMSInvitation cmdlet.

NEW QUESTION: 66
Site1□□□ Microsoft SharePoint Online □□□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.
□□□□ □□ □□ □□□ □□□ □□□ □□□□.
□□ □ □□ □□□ □□□ □□□ □□□□.
* □□: CAPolicy1
* □□
o □□□ □□ □□ ID: □□ 1
o □□□□ □ □□ □□: Office 365 SharePoint Online
o □□
#□□ □□: □□□□ □□□□ □□ □□
#□□ □□: device.displayName - "Device*"□ □□
o □□ □□
#Grant: □□ □□
#□□: 0□□ □□□□ □□□□□□□.
o □□ □□□: □□
* □□: CAPolicy2
* □□

o □□□ □□ □□ ID: □□2
o □□□□ □ □□ □□: Office 365 SharePoint Online
o □□: 0□ □□□ □□□
* □□ □□
o □□ □□: □□□ □□ □□
#□□ □□ □□
o □□:
0□□ □□□□ □□□□□□□
* □□ □□□: □□
□□ □□□□ MFA□ □□□□ □□□□□ □□□ □ □□□ □□□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

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

Answer:

Answer Area

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

Explanation:

Answer Area

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

NEW QUESTION: 67
□□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□ □□□□. □□ Fabrikam, Inc.□□ □□□□ □□□□ □□□□ □□□□.
Fabrikam□ Azure AD□ □□□□ fabrikam.com□ litwareinc.com□□□ □ □□ □□□ □□□ □□□ □□□□ □□□□. □ □□□ □□ □□ Fabrikam □□□ □□□ □□□□□.
Fabrikam□ □□□□ □□□ □ □□ package1□□□ □□□ □□□ □□□□ □□ □□□□□.
Fabrikam□ □□ □□□ □□□ □□□□.
□□□1□ fabrikam.com □□□ □□□ □□ □□□□ □□□ □ □□□ □□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□□□: □□□ □□□ □□□ 1□□ □□□□□.

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Answer:

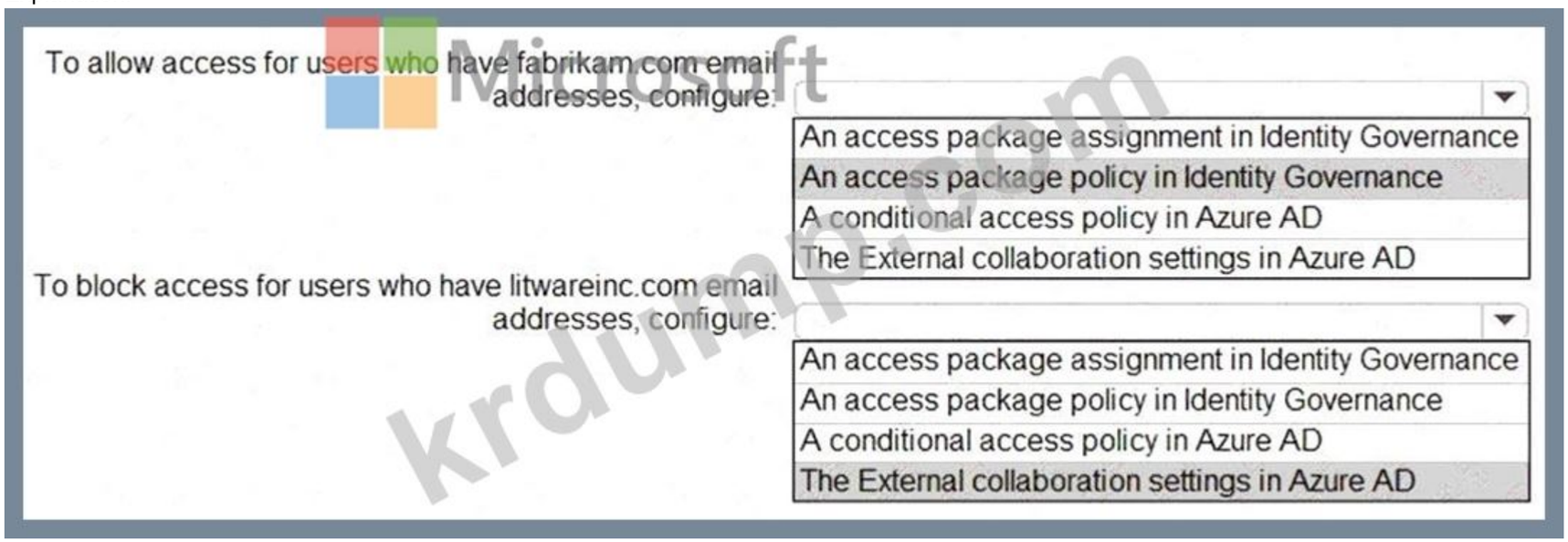
To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

Explanation:



According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Microsoft Learn's official training on "Manage entitlement management in Azure AD Identity Governance", connected organizations and access package policies determine who can request access packages.

When creating an access package for external users, administrators define connected organizations and then specify who from those organizations is allowed to request access. This configuration is managed through access package policies within Identity Governance. Each policy defines the requestors (users from specific domains or organizations) and approval settings.

To allow access for users who have @fabrikam.com email addresses, the correct step is to configure an access package policy in Identity Governance, specifying that only users whose domain matches fabrikam.com can request access.

However, since Fabrikam also owns another domain (litwareinc.com), and you want to block those users from accessing the package, this restriction cannot be configured solely through the access package policy.

The Microsoft documentation clarifies that to block specific external domains from collaborating or being invited into the tenant, administrators must use the External collaboration settings in Azure AD. These settings allow tenant administrators to define which external domains are allowed or denied for guest invitations.
Thus:
* To allow fabrikam.com # configure Access package policy in Identity Governance (to specify who can request the package).
* To block litwareinc.com # configure External collaboration settings in Azure AD (to block invitations or collaboration from that domain).

NEW QUESTION: 68
Azure □□□ □□□□.
Microsoft Entra □□ □□□ □□□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□ □ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□□.
□□ □□ □□□ □□□□ □□ □□□ □□□□ □□□?
A. □□
B. □□□
C. □□□
D. □□□ □□□ □□□
Answer: D (LEAVE A REPLY)
Microsoft Entra Permissions Management (formerly CloudKnox) integrates with Azure subscriptions via a service principal that must read and write role assignments to analyze and right-size permissions. The User Access Administrator role provides this ability without full ownership privileges.
The SC-300 guide explicitly notes that to allow automatic monitoring and remediation of permissions, "the Permissions Management service principal must have the User Access Administrator role on the target subscription or management group to modify and create RBAC assignments." Reader (A) and Contributor (B) roles cannot manage RBAC permissions, while Owner (C) grants unnecessary broad control, violating the principle of least privilege.

NEW QUESTION: 69
App1□ □□ □□□ □□ □□□ □□ □□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. Microsoft Endpoint Manager□ □□□ □□
B. Microsoft Endpoint Manager□ □ □□ □□
C. Azure AD□ □ □□
D. Azure AD □□□□□□ □□□
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Publish on-premises apps for remote access using Azure AD Application Proxy", Azure AD Application Proxy enables secure remote access to internal, on-premises web applications without requiring VPN access.
In the scenario, App1 is an on-premises application hosted within the Litware network, and the technical requirements specify that it must be securely accessible to both internal and external users - including Fabrikam guest accounts - through Azure AD authentication.
Microsoft's official documentation states:
"Azure AD Application Proxy provides se cure remote access to on-premises web applications, integrating with Azure AD for single sign-on (SSO) and conditional access policies." Given that the environment already includes a server (SERVER1) running the Azure AD Application Proxy connector, and that Litware wants to enforce Azure AD Conditional Access and MFA for App1, Azure AD Application Proxy is the correct implementation.
The other options are not suitable:
* A. Policy set in Microsoft Endpoint Manager: Used for device compliance and app management, not for publishing on-premises apps.
* B. App configuration policy in Endpoint Manager: Used for mobile app configuration (e.g., MAM policies), not for access publishing.
* C. App registration in Azure AD: Used for modern cloud or SaaS apps integration, but App1 is on- premises and needs proxy access.

answer: D. Azure AD Application Proxy
Topic 2, Litware, IncOverview
Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a V PN connection.
Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash s ynchronization disabled.
Litware.com contains a user named User1 who oversees all application development. Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litw are.com by using gu est accounts in the litware.com tenant.
Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices in Microsoft Cloud App Security are enabled.
Litware has an Azure s ubscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector.
Azure Sentinel currently collects the Azure AD sign-ins logs and au dit logs.
On-premises Environment
The on-premises network contains the severs shown in the following table.

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

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Delegation Requirements
Litware identifies the following delegation requirements:
* Delegate the management of privileged roles by using Azure AD Pri vileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant-
* Use custom catalogs and custom programs for Identity Governance.
* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.
Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft
365 group that he appropriate license assigned.
Management Requirement
Litware wants to create a group named LWGroup1 will conta in all the Azure AD user accountsfor Litware but exclude all the Azure AD guest accounts.
Authentication Requirements

Litware identifies the following authentication requirements:
* Implement multi-factor authentication (MFA) for all Litware users.
* Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
* Implement a banned password list for the litware.com forest.
* Enforce MFA when accessing on-premises applications.
* Automatically detect and remediate externally leaked credentials
Access Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

NEW QUESTION: 70
Microsoft Entra □□□□ □□□□.
□□ □□□□ □□ □□□ □□□□ □□□ □□ □□□.

Name	Description
Office staff	Contains Windows 11 devices that are Microsoft Entra joined
Contractors	Contains Windows 11 devices that are Microsoft Entra registered
Frontline workers	Contains Windows 11 Enterprise multi-session remote desktops that are Microsoft Entra joined
Senior managers	Contains Windows 11 single-session hosts that are Microsoft Entra joined
Developers	Contains Windows 365 devices that are Microsoft Entra joined

Global Secure Access□ □□□□ □□□.
□□ □□□ Global Secure Access □□□□□□ □□□ □ □□□?
A. □□□, □□□ □□ □ □□ □□□□ □□
B. □□□, □□□, □□ □□□, □□□ □□, □□ □□□
C. □□□ □ □□□ □□□
D. □□ □□□ □ □□ □□□□ □□
Answer: D (LEAVE A REPLY)

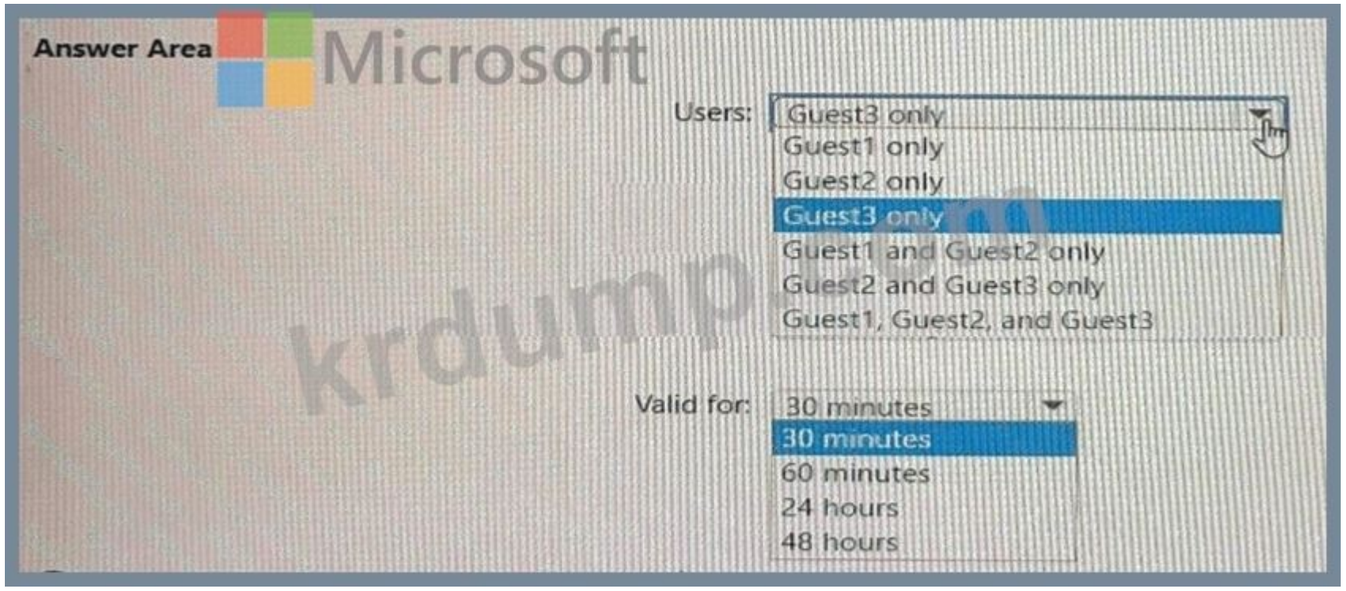
NEW QUESTION: 71
VM1□□□ □□ □□□ Vault1□□□ Azure □ □□ □□ □□□ □□□ Azure □□□ □□□□. VM1□□ □□□□□ □□□ □□ ID□ □□□□. VM1□ Vault 1□ □□□ □□ □□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□. □□ □□□ □□ □□□?
A. Vault1□ □□ □□□ □□□ □□□ □□□□□.
B. Vault1□ □□ □□ □□ □□
C. VM1□ □□□□ □□□ □□ ID□ □□□□□.
D. VM1□ Azure □□□ □□□□□.
Answer: D (LEAVE A REPLY)
To ensure VM1 can retrieve the values of secrets stored in Vault1 while minimizing administrative effort, you should assign an Azure role to VM1 .
1. Managed Identities and Key Vault Access: VM1 has a system-assigned managed identity . This identity acts as a Service Principal in Microsoft Entra ID (formerly Azure AD). To access Key Vault secrets, this identity must be granted permissions on the Key Vault.
2. Permission Models (RBAC vs. Access Policies): Azure Key Vault supports two permission models:

* Azure role-based access control (Azure RBAC): The recommended, modern authorization system. It allows you to mana ge access to Key Vault keys, secrets, and certificates centrally using Azure IAM (Identity and Access Management), just like other Azure resources. It provides fine-grained access control and integrates with PIM (Privileged Identity Management).
* Vault acce ss policy: The legacy model where permissions are defined within the Key Vault ' s own " Access policies " blade.
3. Why " Assign an Azure role " (Option D) is the Correct First Step:
* Minimizing Administrative Effort: Using Azure RBAC is the recommended best pra ctice for minimizing effort because it unifies access management across Azure resources.
* The Action: To grant the required access (reading secrets) under the RBAC model, you must assign a specific role to the managed identity. The appropriate role is Key V ault Secrets User , which grants permission to read secret contents (Get and List operations) without granting administrative privileges (adhering to Least Privilege).
* Scenario Analysis: While older Key Vaults defaulted to Access Policies, new vaults and th e " minimize effort " requirement point towards the RBAC model. Option A (" Configure the Resource access settings ") is vague and likely refers to the " Access configuration " or " Access policies " blade, but " Assign an Azure role " is the definitive action to gr ant access in the modern RBAC workflow. If the vault were in Access Policy mode, one would typically " Add an access policy, " but that specific option is not listed, reinforcing that RBAC (Option D) is the intended path.
Documentation Extract:
" Azure RBAC is an authorization system built on Azure Resource Manager that provides centralized access management of Azure resources... The Azure RBAC model allows users to set permissions on different scope levels... To grant access to a specific user, group, or app lication... assign a role. For example, the Key Vault Secrets User role allows a user to read secret contents. " (Source: Microsoft Learn - Provide access to Key Vault keys, certificates, and secrets with an Azure role-based access control)

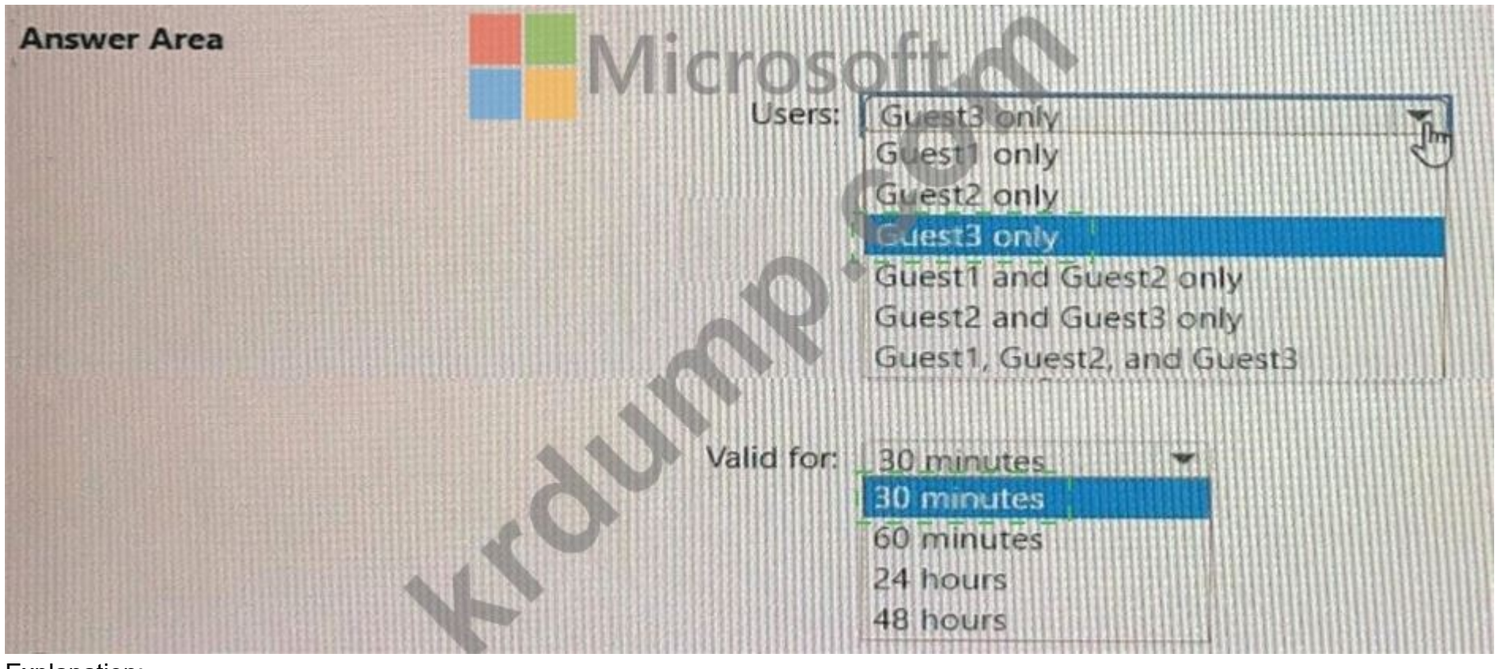
NEW QUESTION: 72
contoso.com□□□ Azure AD □□□□ □□, □□□□ □□ □□□ □□□ □□□ □□ □□□□ □□□□.
□□ □□ □□□ □□□ □□□□ □□□□□.

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

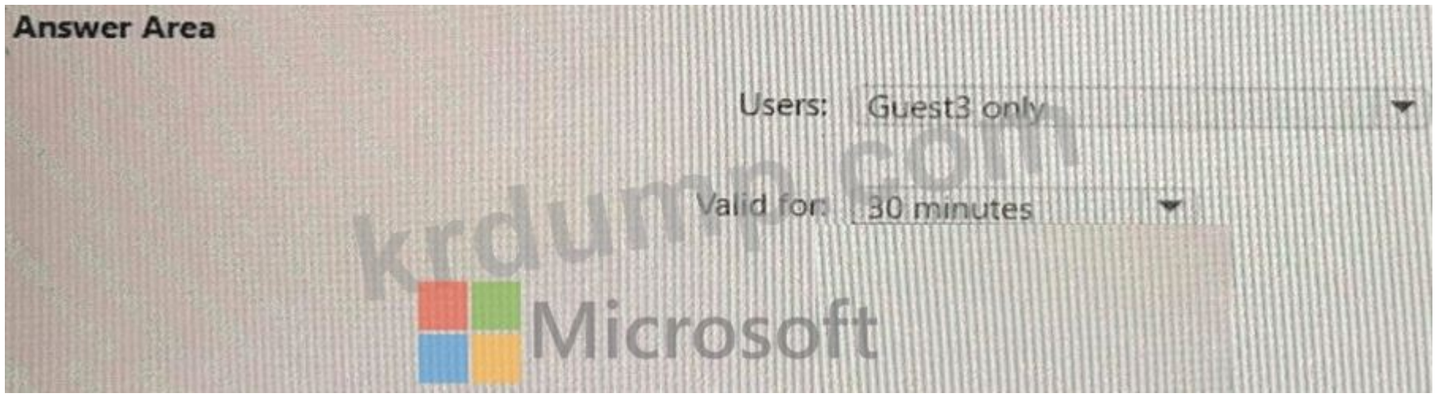
□□ □□□□□ □□□ □□□ □□□□, □□□ □□□ □□□□ □□□□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:



According to the Microsoft SC-300 Study Guide, Exam Ref SC-300, and Microsoft Entra (Azure AD B2B collaboration) documentation, when a guest is invited to an Azure AD tenant and the setting "Email one-time passcode for guests" is enabled, Azure AD determines the authentication method based on the guest's account type.

Here's how the logic applies:

* Guest1 (adatum.com - Azure AD account)
* Because adatum.com is an Azure AD-managed domain, Guest1 will authenticate using their own organization's Azure AD credentials.
* The guest sign-in will federate to their home tenant, and therefore no one-time passcode (OTP) is sent.
* Guest2 (outlook.com - Microsoft account)
* A user with an @outlook.com email has a Microsoft account (MSA).
* Microsoft accounts can authenticate directly via Microsoft's identity system.
* Hence, no one-time passcode is sent - the user signs in using their Microsoft account credentials.
* Guest3 (gmail.com - Personal Google account)
* A @gmail.com address is not a Microsoft account and not linked to any Azure AD tenant by default.
* In this case, because the tenant's setting "Email one-time passcode for guests" is enabled, Azure AD automatically sends a one-time passcode (OTP) to the guest's email address for authentication.
* The Microsoft documentation specifies that the OTP is valid for 30 minutes and is single-use.

After expiration, a new code is issued upon the next authentication attempt.

This is confirmed in Microsoft's official Entra ID documentation:

"When the Email one-time passcode for guests setting is enabled, guests who do not have an Azure AD or Microsoft account will authenticate using a one-time passcode that is valid for 30 minutes."

NEW QUESTION: 73

Microsoft 365 □□□□ □□□□.

Azure Active Directory {Azure AD} □□□□ □□□□□ Active Directory □□□□ □□□□.

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

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

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

□□□ □□□□□ □□□ □□□□ □□□?

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

B. Azure AD□ □□□□□□ □□□□□□

C. Azure AD□□ □□ □□□

D. Azure Monitor□ Application Insights

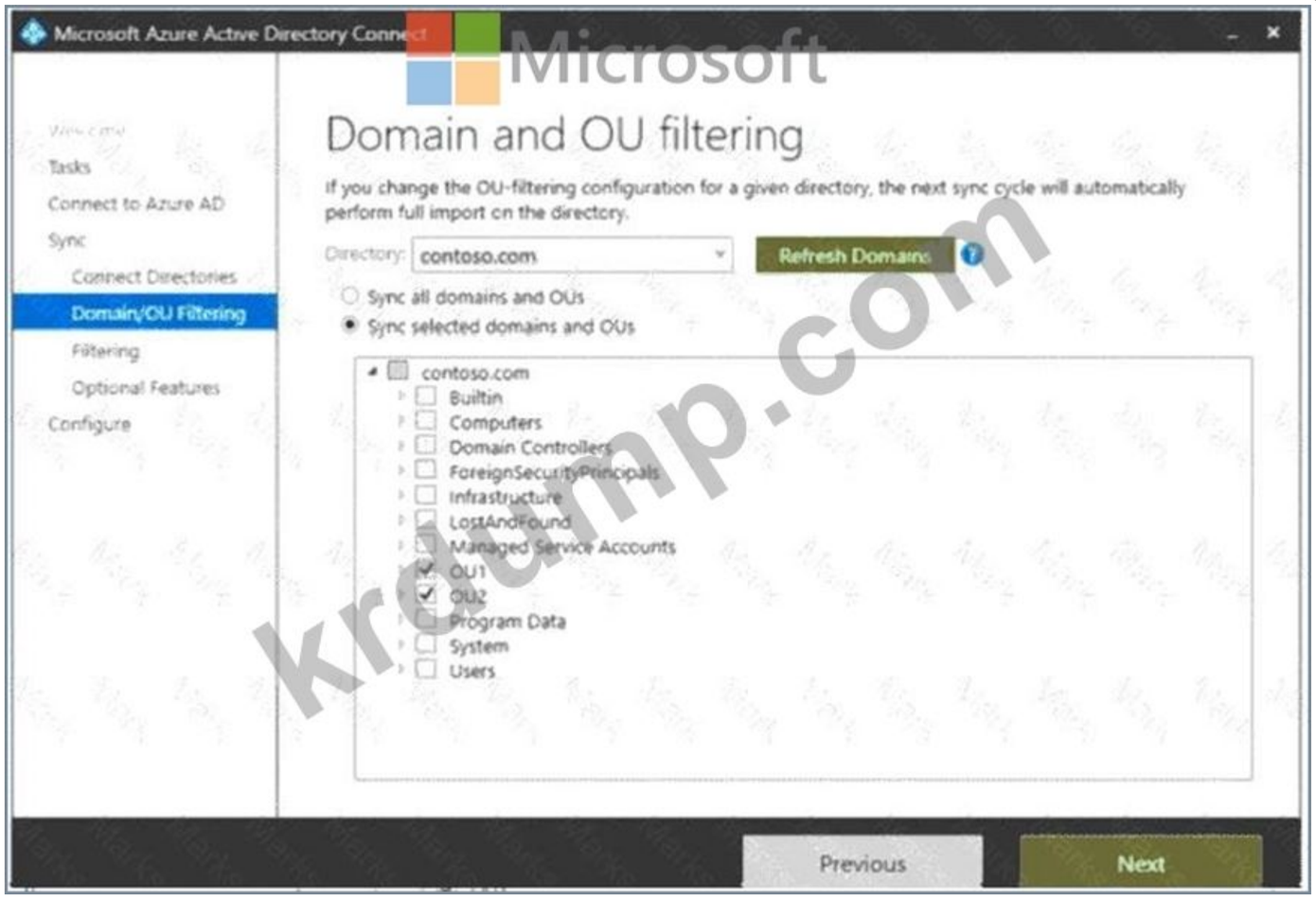
Answer: (SHOW ANSWER)

The Cloud App Discovery feature in Microsoft Defender for Cloud Apps (formerly Cloud App Security) is designed to identify and analyze shadow IT-applications being accessed by users that are not managed by IT.
By importing firewall or proxy logs, Defender for Cloud Apps can automatically detect unmanaged external SaaS applications and the users accessing them. The study guide specifically states:
"Cloud App Discovery analyzes traffic logs from your firewalls and proxies to identify cloud applications used by your organization and provides visibility into usage and risk levels." Therefore, to identify unmanaged external apps and the users accessing them using firewall logs, Cloud App Discovery is the correct Microsoft tool.

NEW QUESTION: 74
□□□□□ contoso.com□□□ □-□□□□ Active Directory □□□□ □□□□. □ □□□□□ □□ □□ □□ □□ □□□ □□□□ □□□□.

Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

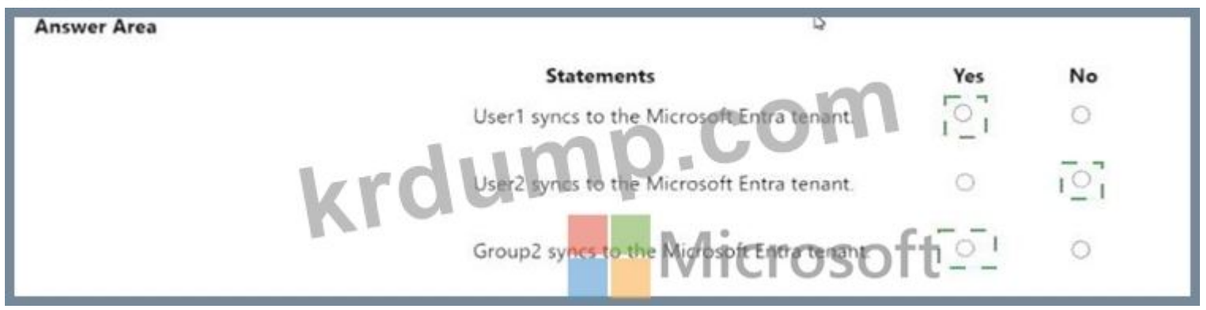
Microsoft Entra Connect□ □□□□□. □□□ □ OU □□□ □□□ □□□ □□ □□□ □ OU □□□ □□□ □□□□□. (□□□ □ OU □□□ □□ □□□□□.)



"□□□ □ □□ □□□" □□□ □□□ □□ "□□□ □ □□ □□□" □□□ □□□□□. ("□□□ □ □□ □□□" □□ □□□□□.) □□ □ □□□ □□, □□□□ □□ "□"□ □□□□, □□□ □□□ "□□ □"□ □□□□□.

□□: □□ □□□ 1□□□□.

Answer:



Explanation:

< User1 syncs to th e Microsoft Entra tenant: Yes

User2 syncs to the Microsoft Entra tenant: No

Group2 syncs to the Microsoft Entra tenant: Yes

NEW QUESTION: 75

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

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

□□□□ □□ □□□ □□ □□□□□□ Office 365 Enterprise E3 □□□□□ □□□□ □□□.

□□□ □□□□ □□□?

A. Set -KindohsProductKcy cmdlct

B. Update-MgGroup cmdlet

C. Set-HgUserLicense cmdlet

D. Update-MgUser cmdlet

Answer: C (LEAVE A REPLY)

In this scenario, users already have Office 365 E3 licenses assigned individually, and you've now assigned Microsoft 365 E5 licenses through a group-based license assignment. The goal is to remove the E3 licenses from each user with the least administrative effort.

The SC-300 study guide and Microsoft documentation on "Manage license assignment in Azure AD" explain that when licenses are assigned both individually and through groups, the group assignment does not automatically remove the direct user-assigned licenses. To remove the individually assigned license programmatically, the Set-MgUserLicense cmdlet (Microsoft Graph PowerShell) is used.

The documentation states:

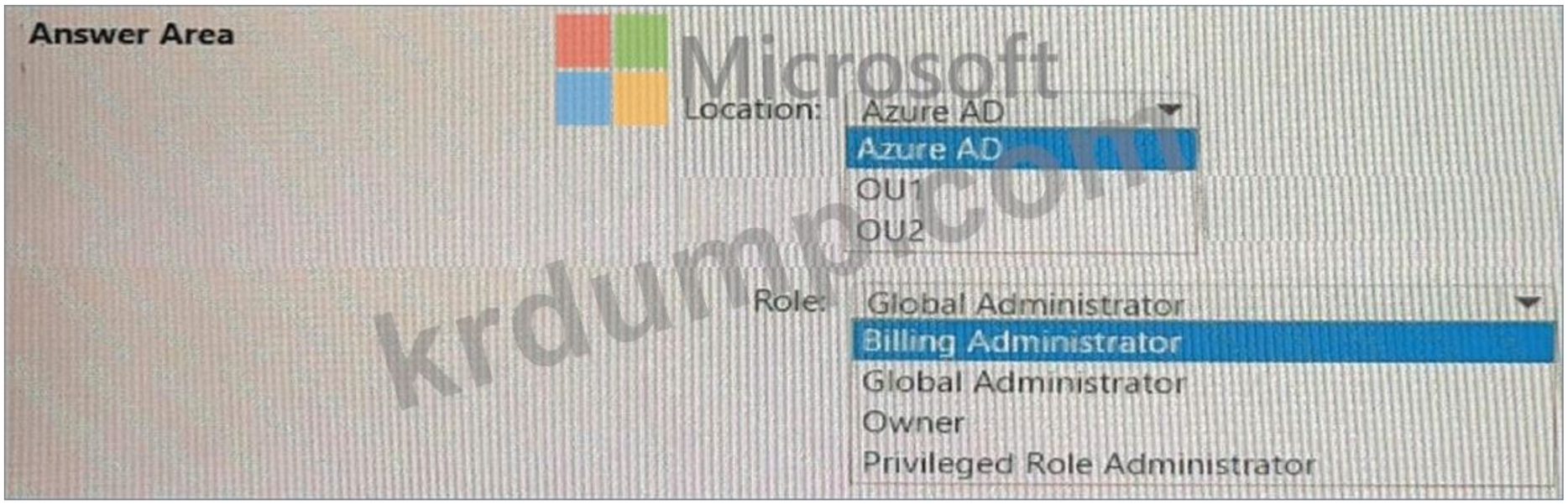
"Use the Set-MgUserLicense cmdlet to add or remove product licenses for users. You can specify the license plan to remove using the -RemoveLicenses parameter." Example: Set-MgUserLicense -UserId user@domain.com -RemoveLicenses " O365_ENTER PRISE_E3 "
* A. the Set-KindohsProductKcy cmdlet: This is not a valid Microsoft 365 or Graph cmdlet (appears to be a distractor).
* B. the Update-MgGroup cmdlet: Used to modify group properties - not for managing user licenses.
* D. the Update-MgUser cmdlet: Updates user object attributes (e.g., display name) but cannot assign or remove licenses.
Why not the other options: # Correct Answer: C. the Set-MgUserLicense cmdlet.

NEW QUESTION: 76
□□□□ □□ Yammer□ Microsoft Defender□ □□□□ Microsoft 365 ES □□□ □□□□.
□□□□ □□ □□□□ □□□□ Yammer□ □□□□□ □□ □□□□ □□□.
□□□□ □ □□□ Microsoft Defender□□ □□□ □□ □□□?
A. □□□ □□□ □□□□.
B. □□ □□□ □□□□.
C. □□□□ □□ □□.
D. □□ □□ □□□ □□□□□.
Answer: A (LEAVE A REPLY)
Defender for Cloud Apps (MCAS) provides Access policies to control sign-in and session access to sanctioned apps based on conditions such as user, device, and location. SC-300 notes that access policies can allow, block, or require additional controls and are evaluated at sign-in, making them appropriate to prevent logons from risky or specific locations. In contrast, Activity policies alert on or govern in-app actions (downloads, sharing) after sign-in, and Anomaly detection policies use heuristics to surface suspicious behavior, not enforce blocking. "Unsanctioning" an app merely flags it and can integrate with firewall/proxy tagging; it does not directly enforce a conditional sign-in block. Therefore, to block Yammer sign-ins from high-risk locations, you create an Access policy in Defender for Cloud Apps targeting Yammer with a condition for the designated high-risk locations and set the action to Block (or require step-up).

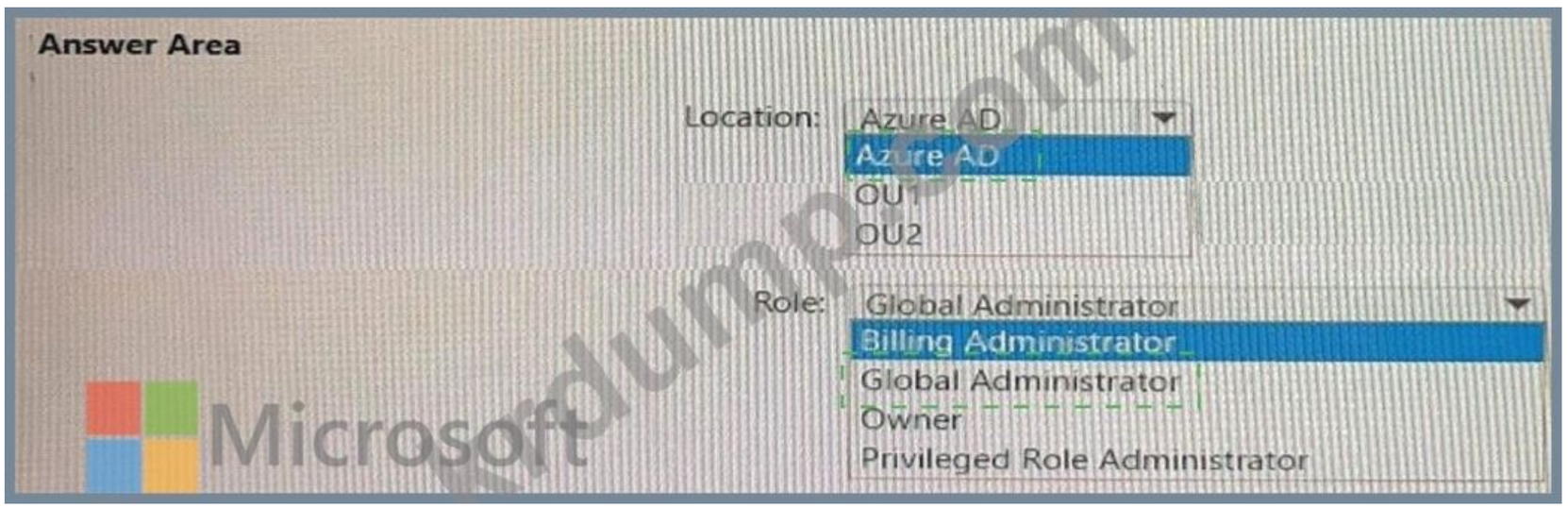
NEW QUESTION: 77
□□□□□□ Azure AD □□□□ □□□□□ □-□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□ □□□□. AD DS □□□□□ □□ □□ □□ □□ □□ □□(OU)□ □□□□ □□□□.

Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

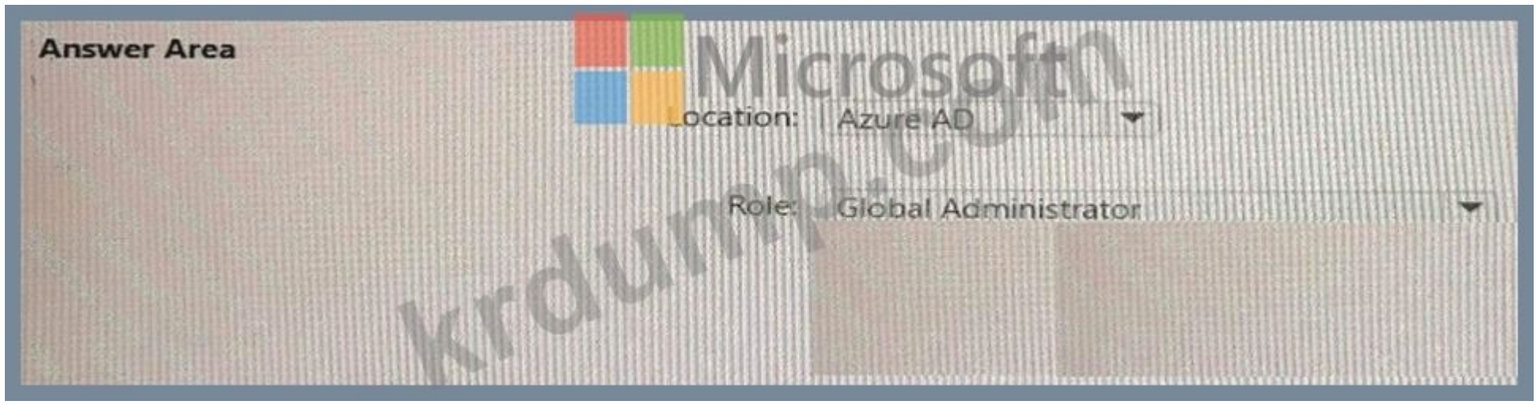
BreakGlass□□ □□□ □□□□ □□□ □□□ □□□□ □□□.
BreakGlass□ □□□ □□□□ □□, BreakGlass□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Entra ID documentation , a break-glass account (also known as an emergency access account) is a cloud-only account that must not depend on any on-premises identity infrastructure, such as Active Directory synchronization or conditional access.

* Location: The break-glass account must be created directly in Azure AD (cloud-only) - not in an on- premises Organizational Unit (OU1 or OU2).
* OU1 syncs with Azure AD, meaning if on-premises synchronization fails or the domain controller is unavailable, accounts in OU1 might not authenticate.
* OU2 doesn't sync at all, so creating the account there wouldn't provide Azure AD access.

Therefore, the only resilient option is Azure AD (cloud-only) to ensure access even if directory sync or on-premises systems are unavailable.

* Role: Microsoft recommends assigning the Global Administrator role to break-glass accounts. This ensures full tenant recovery capability in emergencies such as Conditional Access lockouts or MFA misconfiguration.
* The Billing Administrator or Privileged Role Administrator roles don't provide sufficient rights to recover access or modify Conditional Access settings.
* The Global Administrator role has full control over all Azure AD resources and configuration settings.

Reasoning: Microsoft documentation states:

"Create at least two cloud-only emergency access accounts with the Global Administrator role. These accounts must be excl uded from Conditional Access policies and protected with strong authentication methods."

NEW QUESTION: 78

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

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

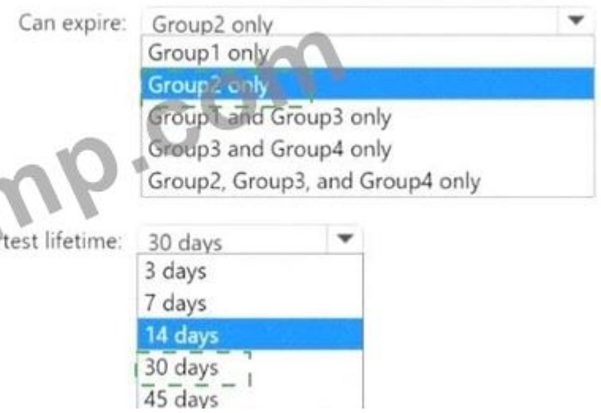
□□□ □□ □□□ □□□ □□□□□.

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

□□: □□ □□□ 1□□□□.

Answer:

Answer Area



Explanation:

Answer Area

According to the Microsoft SC-300 Study Guide and Microsoft Learn module: "Manage Microsoft 365 group lifecycles", group expiration policies in Microsoft Entra ID apply only to Microsoft 365 groups (formerly Office 365 groups).

Group expiration is part of lifecycle management for Microsoft 365 services and helps ensure that unused groups are automatically deleted after a defined period unless renewed by the owner.

From the table:

* Group1 (Security) # Cannot be set to expire.
* Group2 (Microsoft 365) # Can be set to expire.
* Group3 (Mail-enabled security) # Cannot be set to expire.

* Group4 (Distribution) # Cannot be set to expire.
Therefore, Group2 only can have an expiration policy applied.
Regarding group lifetime, the Exam Ref SC-300 and Microsoft documentation confirm that the minimum (shortest) group lifetime that can be configured for Microsoft 365 group expiration policies is 30 days.
Microsoft Learn states:
"The group lifetime can be set to 30, 60, 90, 180, or 365 days. The minimum allowed is 30 days." This ensures group owners have sufficient time to renew or manage expiring groups before automatic deletion.

NEW QUESTION: 79
□□ 6
Sg-Executive □□□□ □□ □□ □□□□□ □□ □□ □□□ □□□□ □□□. □□□□ □□ □□ □ □□□ □□□□ □□□.
* Microsoft Intune□□ □□□ □□ □□□ □□□ □□□ □□□□ □□□□□.
* □ □□ □□□□ □□□□ □□□□□ □□ □□□□ □□□□□.
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To implement additional security checks for the Sg-Executive group members before they canaccess any company apps, you can use Conditional Access policies in Microsoft Entra. Here's a step-by-step guide:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Security Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Name the policy appropriately, such as "Sg-Executive Security Checks".
Assign the policy to the Sg-Executive group:
Under Assignments, select Users and groups.
Choose Select users and groups and then Groups.
Search for and select the Sg-Executive group.
Define the application control conditions:
Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.
Set the device compliance requirement:
Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.
Set the app protection policy requirement:
Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.
Configure the access controls:
Under Access controls > Grant, select Grant access.
Choose Require device to be marked as compliant and Require approved client app.
Ensure that the option Require one of the selected controls is enabled.
Enable the policy:
Set Enable policy to On.
Review and save the policy:
Review all settings to ensure they meet the requirements.

Click Create to save and implement the policy.
By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app.
This enhances the security posture of your organization by enforcing stricter access controls for executive- level users.

NEW QUESTION: 80
Microsoft Entra ID Premium □□□□□ □□□□ Microsoft Entra □□□□ □□□□.
□□□□ □□ □□ □□(ToU)□ □□□ □□□□□.
□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□□ □□□□ □□□?
A. HTML
B. RTF
C. PDF
D. DOCX
Answer: (SHOW ANSWER)
The Microsoft Entra Terms of Use (ToU) documentation included in the SC-300 curriculum specifies that only PDF files are supported when uploading terms of use documents.
Microsoft Entra ID Premium licenses are required to configure Terms of Use, and when administrators create a new ToU, the upload field explicitly accepts a PDF document format. The PDF ensures consistent formatting across devices and preserves the legal structure of compliance statements.
The guide states:
"The terms of use document must be a PDF file. This en sures consistency in presentation and prevents tampering." Therefore, acceptable format: PDF only - formats such as HTML, DOCX, or RTF are not supported.

NEW QUESTION: 81
□□□□□□ □□□□□ Active Directory □□□ □□□(AD DS) □□□□ □□□□. □ □□□□ Microsoft Entra Connect Sync□ □□□□ Microsoft 365 □□□ □□□□□□.
300□□ □ □□□□ □□□ □□□□□. □□□ □□ □□□ Microsoft Excel □□□□□□□ □□□□ □□□□. □□□ □□□ □□□□□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
* □□□□ Microsoft 365 □□□ □□□□ □□□□ □ □□□ □□□.
* □□□□ □□□□□ □□□□□ □□□□ □□□ □ □□□ □□□.
□□□□ □□□ □□□□□□ □□□.
□□□□ □□ PowerShell cmdlet□ □□□□ □□□?
A. Set-ADUser □ Get-Content
B. New-MgUser □ Get-Content
C. Set-HgUser □ Import-CSV
D. New-ADUser □ Import-CSV
Answer: (SHOW ANSWER)

NEW QUESTION: 82
User1□□□ □□□□ □□□ Azure □□□ □□□□. □ □□□ Microsoft Entra □□ □□□ □□□□ □□□□. User!□□ □□ □□□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □ □□□.
* □□ □□□ □□□ □□□□.
* □□□ □□□ □□□□□□.
□□ □□ □□□ □□ □□□?

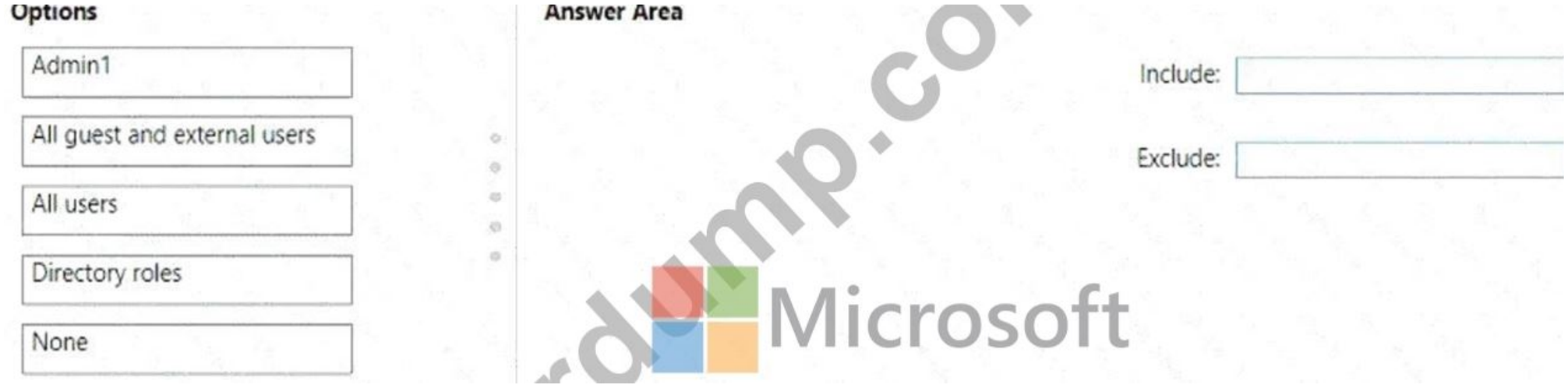
A. Microsoft Entra □□ □□□□ □□ □□□ □□□□.
B. □□ □□□ □□/□□ □□□ □□ □□□ □□□□ □□□□.
C. Microsoft Entra □□ □□□□ User1□□ □□□ □□□□□.
D. □□ □□□ □ □□ □□ □□□ □ □□□ □□□□.
Answer: C (LEAVE A REPLY)
When onboarding to Microsoft Entra Permissions Management (a CIEM solution), before a user can perform any functions inside Permissions Management, that user must be granted an appropriate Permissions Management role in the Entra tenant. The principle of least privilege dictates that you grant only the minimal role necessary (for example, a Permissions Management Approver , Viewer , or Controller). The SC-300 study materials and Microsoft's documentation emphasize that administrative access must begin by assigning roles within Entra ID.
Creating a security group (option A) is a useful organizational practice but doesn't itself grant the user permissions inside Permissions Management.
Creating a role/policy template (option B) is about defining permission scopes and is not a first step to allow a user access.
Creating a request in My Requests (option D) presupposes that User1 already has some entitlement to make requests (i.e. some role), which they don't yet.
Therefore, the first action is to assign a Permissions Management role to User1 from the Entra admin center, thus giving them appropriate access while adhering to least privilege.

NEW QUESTION: 83
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
Azure AD □□ ID □□□ □□ □□ □□□(MAU)□ □□□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□□ □□
D. □□ □□
Answer: C (LEAVE A REPLY)
Azure AD External Identities (B2B) uses Monthly Active Users (MAU) billing. The SC-300 content explains that to enable MAU-based pricing, the Azure AD tenant must be linked to an Azure subscription so that usage can be metered and billed. The configuration is performed in Azure AD # External Identities # All settings # Linked subscription , where administrators associate the tenant with a subscription and resource group. Only after this association do External Identities sign-ins count against MAU rather than per- user licenses. Access reviews (A) and terms of use (B) are governance features that do not affect billing. User flows (D) are specific to Azure AD B2C and are unrelated to enabling MAU billing for B2B External Identities. The study guide highlights: "To use MAU billing for External Identities, link your Azure AD tenant to an Azure subscription so guest usage is charged per monthly active user." Therefore, the correct prerequisite to ensure MAU billing is configuring a linked subscription .

NEW QUESTION: 84
Microsoft Entra □□ □□□ □□□□ Sub1□□□ Azure □□□ □□□□. Sub1□□ User1□□□ □□□□ □□□□. User1□□□ Sub1 □□□□ □□ □□□ □□□□□.
User1□□ □□□ □□ □□□ □□ □□ □□□□ □□□ □□□. □ □□□□ □□ □□□ □□□□□ □□□.
□□ □□□ □□ □□□ □□□ □□ □□□?
A. □□/□□ □□ □□□ □□□ □□□□.
B. □ □□ □□ □□□ □ □□□ □□□□.
C. □□ □□ □□□ □□ □□□ □□□□□.
D. □□/□□ □□□ □□ □□□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
Within the Remediation tab of Microsoft Entra Permissions Management, the Permissions subtab allows you to view, filter, and manage the permissions directly assigned to identities. It supports operations such as Read
, Update , and Delete on granted permissions.

If you need to change a user's permissions (for example, reduce all of User1's permissions to read-only), the quick action capability in the Permissions subtab is the most efficient method. Using the quick action, you can right-size, remove, or adjust permissions for a user in bulk across their assigned permissions. This is less administrative effort than creating new roles or templates The Roles/Policies subtab (option A) deals with role definitions (CRUD operations), not directly editing a given user's permissions.
The My Requests subtab (option B) is for requesting elevated permissions, not for bulk modifying existing assignments.
The Role/Policy Template tab (option D) is for defining templates; using them is less direct and more overhead when you already have assignments to adjust.
Hence, the correct and minimal-effort choice is to use the quick action in the Permissions subtab of the Remediation tab to change User1's permissions to read-only.

NEW QUESTION: 85
Admin1□□□ □□□□ □□□ Azure AD □□□□ □□□□.
Admin1□ □□□ □□□□ □□□□ □□ □□ □□ □□□□ □□□□ □□□ □□□ □□□ □□□ □□□□.
□□ □□□ □□□□□ □□□□□ □□□□ □□□ □□□□□? □□□□ □□□ □□□ □□ □□□ □□□□□□. □ □□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Official Study Guide and Microsoft Learn - Manage Conditional Access policies module, when an administrator creates a Conditional Access policy using the built-in Require password change for high-risk users template, the policy is automatically pre-configured with specific include and exclude assignments.

By default, this template targets "All users" in the tenant because the policy is designed to detect and remediate risky sign-ins or compromised accounts across the entire directory. However, since Azure AD B2B guest accounts and external users often have limited sign-in scopes and cannot be subjected to organization- specific password policies, Microsoft's security baseline specifically excludes all guest and external users by default.

The intent behind this default configuration is to apply the password change requirement to internal users while avoiding unnecessary enforcement on guest identities that do not manage credentials within the host tenant.

From the Microsoft Learn - Conditional Access policy templates documentation:

"When you create a policy from the Require password change for high-risk users template, the policy is configured to include all users and exclude all guest and external users by default."

NEW QUESTION: 86

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

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

Microsoft 365 ES □□□ □□□□.

User1□□□ □□□□ □□□□□.

User1□ ID □□ □□ □□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□.

□□ □□: □□ □□□ □□ User1□ □□□□□.

□□□ □□□ □□□□□?

A. □

B. □□□

Answer: A (LEAVE A REPLY)

The Security Operator role is part of Microsoft's tiered security roles designed to allow operational security tasks while limiting full administrative privileges.

Per Microsoft Learn ("Permissions in the Mic rosoft 365 Defender portal" and SC-300 Study Guide):

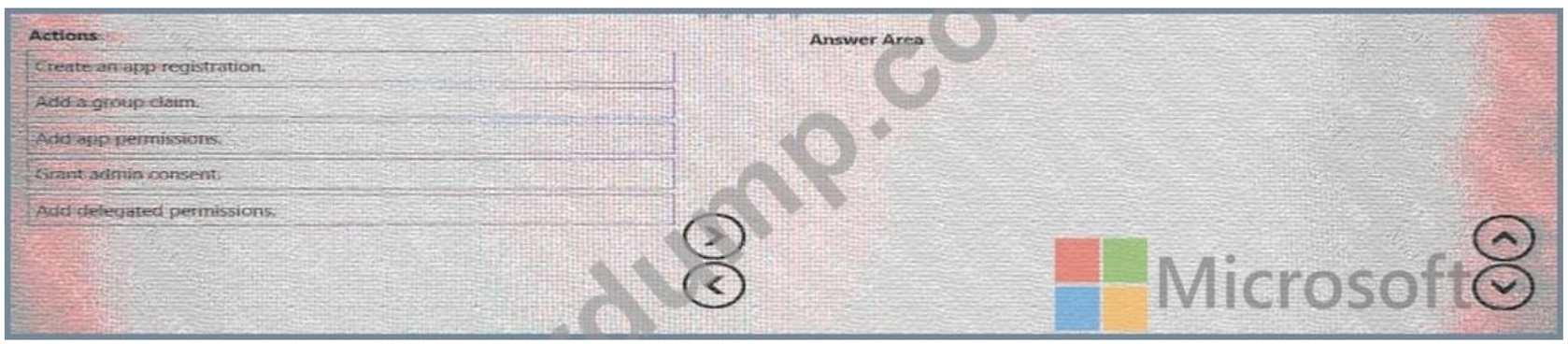
"Security Operators can view, investigate, and take actions on security recommendations, alerts, and improvement actions in Microsoft Secure Score." The Security Operator role can update the status of Secure Score improvement actions, making it the appropriate and least-privileged choice for this scenario.

NEW QUESTION: 87

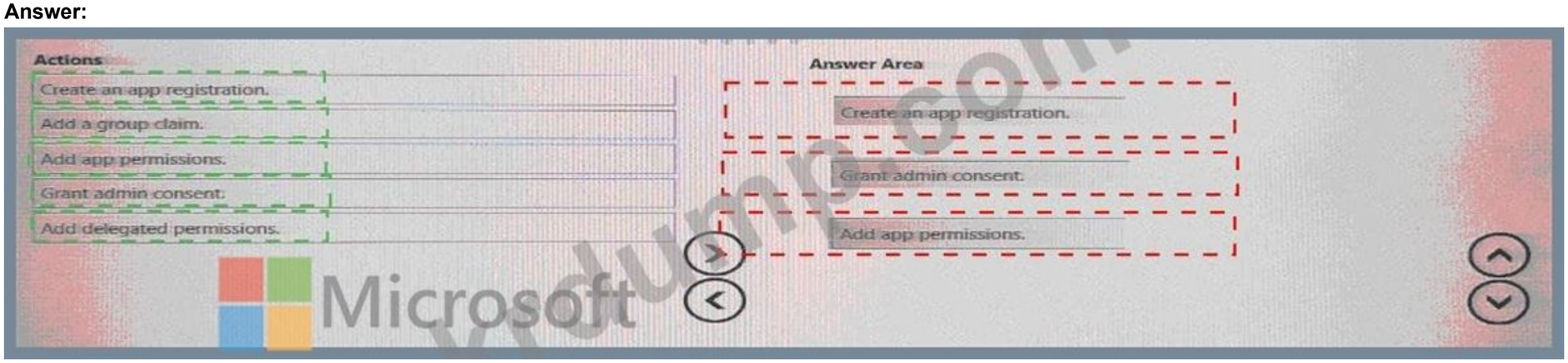
□□□ □□□□ contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□□□.

□ □□□ App1□□□ □ □□□□ □□□□ □□□□.

App1□ Microsoft Graph□ □□□□ contoso.com□ □□□□ □□□□ □□ □ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and manage enterprise applications," when developing an application that needs to access Microsoft Graph or other protected APIs on behalf of an organization, you must perform several configuration steps within Azure Active Directory (Azure AD).

Step 1 - Create an app registration:

Every application that requires access to Microsoft Graph must be registered in Azure AD. The registration process establishes an identity for the app and generates an Application (client) ID and a directory (tenant) ID.

This is done in Azure portal # Azure Active Directory # App registrations # New registration . This enables Azure AD to issue tokens to the app.

Step 2 - Add app permissions:

After registration, you must configure permissions under API permissions in the app's registration settings.

For server-to-server access (no user sign-in), Application permissions are used; for delegated access (on behalf of a user), Delegated permissions are added. In this case, since App1 will read directory data from Microsoft Graph, you assign the Microsoft Graph # Directory.Read.All permission.
Step 3 - Grant admin consent:
Application permissions require admin consent before the app can access directory data. An Azure AD administrator must grant these permissions by selecting "Grant admin consent for contoso.com." This allows the app to use the permissions organization-wide.
From Microsoft's documentation:
"To enable an application to call Microsoft Graph, register the app, configure required API permissions, and grant admin consent for those permissions."
Correct Answer Order:
* Create an app registration
* Add app permissions
* Grant admin consent

NEW QUESTION: 88
Sub1□□□ Azure □□□ □□□□.
Microsoft Entra □□ □□□ □□□ □□□□□.
□□ □□□ Sub1□ □□□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□ □□□.
PowerShell □□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

In Microsoft Entra Permissions Management (formerly CloudKnox), onboarding an Azure subscription requires granting the Permissions Management service principal the minimum rights needed to discover identities, roles, and permissions across that subscription. The SC-300 materials emphasize the principle of least privilege for onboarding: assign Reader at the subscription scope so the service can inventory resources and permissions without the ability to change them. After onboarding, if you want automated remediation/right-sizing, you can additionally grant User Access Administrator (or perform changes manually), but that elevation is not required merely to onboard and collect data.
Accordingly, you complete the PowerShell by creating an RBAC assignment for the application (service principal) at the subscription scope using New-AzRoleAssignment and specifying -RoleDefinitionName Reader . Creating a new custom role (New-AzRoleDefinition) is unnecessary, and New-AzTag is unrelated to RBAC. Choosing Owner or Contributor would ex ceed the access required for onboarding and violate least-privilege guidance. The correct, minimal configuration is therefore: assign Reader to the Permissions Management application at the /subscriptions/ < SubscriptionId > scope using New-AzRoleAssignment .

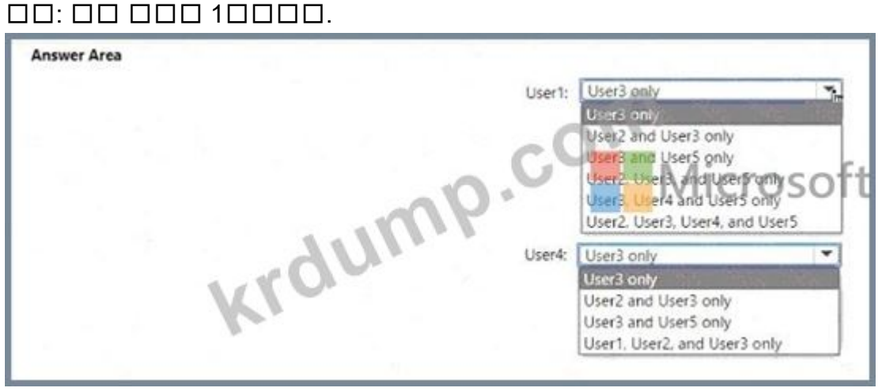
NEW QUESTION: 89
□□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

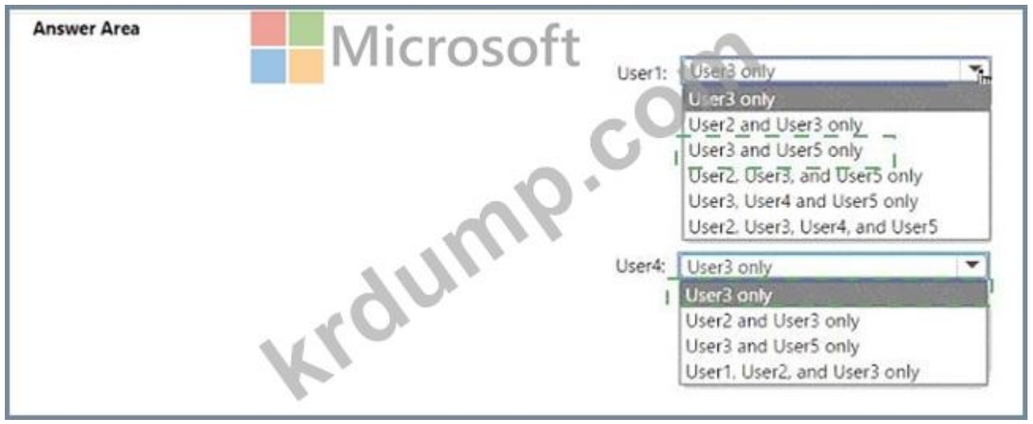
□□□□□□ □□ □□ □□□ □□□ □□□□□.

User	Role	Role scope
User1	Password Administrator	Organization
User2	Global Reader	Organization
User3	*None*	*Not applicable*
User4	Password Administrator	AU1
User5	*None*	*Not applicable*

User1□ User4□ □□ □□□□ □□□□□ □□□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

User

Can Reset Passwords For

User1

User3 and User5 only

User4

User3 only

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Learn documentation on role-based access control (RBAC) and administrative units (AUs) , the scope of administrative privileges determines which users an administrator can manage.

Role Review:

* Password Administrator (Organization scope): Can reset passwords for non-administrators and users with lesser pri vileges across the entire organization. They cannot reset passwords for Global Administrators or users with equal/higher roles.
* Global Reader (Organization scope): Read-only access-cannot perform administrative actions (including password resets).
* Password Administrator (Scoped to AU1): Can reset passwords for users within AU1 who are non- administrators and whose roles are less privileged than their own.

User

Role

Scope

Members in Administrative Unit

User1

Password Administrator

Organization

AU1

User2

Global Reader

Organization

AU1

User3

None

N/A

AU1

User4
Password Administrator
AU1
AU2
User5
None
N/A
None
Step 1 - For User1 (Org-scoped Password Administrator): User1's permissions apply organization-wide, allowing resets for:
* Users without admin roles, including those in or outside any AU.
* Cannot reset passwords for users with equal or higher roles (e.g., Global Reader, Password Administrator).
# Therefore, User1 can reset passwords for:
* User3 (no role, AU1)
* User4 (Password Administrator in AU2) - # cannot reset equal role
* User5 (no role, no AU) #
Final for User1 # User3 and User5 only
Step 2 - For User4 (AU1-scoped Password Administrator): User4's permissions apply only within AU1 and to users with lesser privileges.
Within AU1:
* User1 (Org Password Admin) - # higher privilege
* User2 (Global Reader) - # higher privilege
* User3 (no role) - # can reset
Final for User4 # User3 only

NEW QUESTION: 90
Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□□□ □□□ □□□□□□ Microsoft Exchange Online□ □□□ □ □□□ □□□□ □□□□.
□□□□ □□ □□ □□□□□ □□□□ □□□ □□□□□□□□ Exchange Online□ □□□ □ □□□ □□ □□□.
□□□ □□□□ □□□?
A. □□□□ □□ Microsoft Defender OAuth □□
B. Microsoft Intune □ □□ □□
C. Microsoft Intune □□ □□ □□
D. Microsoft Entra □□□ □□□ □□
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide, the enforcement of Modern Authentication for Microsoft 365 services such as Exchange Online is achieved through Conditional Access policies. Conditional Access allows you to block legacy authentication protocols (such as POP, IMAP, SMTP, and MAPI over HTTP) that use Basic Authentication, and require Modern Authentication (OAuth 2.0) instead.
Microsoft Learn explains that you can configure a policy that "blocks access requests using legacy authentication clients" under Conditions # Client apps and select "Other clients (legacy authentication clients)" to enforce Modern Authentication. Defender for Cloud Apps OAuth policies and Intune app
/compliance policies do not control authentication protocols at the tenant level.

NEW QUESTION: 91

Microsoft Entra □□□□ □□□□.
□□□□ □□ □□ □□□□ □□□□□ □□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□(MFA) □□□ □□□□ □□□□ □□□□□ □□ □□□.
□□□□ □□ □ □□ □□ □□□ □□□□ □□□? □□□ □□ □□□ □□□□ □□□□□.
A. □□□□□ Windows Hello
B. FID02 □□ □
C. □□□ □□ □□(□□ □□)
D. □□ □□
E. □□
F. □□□ OTP
G. □□□ □□ □□(□□ □□)
H. Microsoft □□□
Answer: A,B,C (LEAVE A REPLY)
According to Microsoft's identity and access documentation for Conditional Access and phishing-resistant MFA, phishing-resistant MFA methods are those that cannot be socially engineered or replayed. These are Windows Hello for Business, FIDO2 security keys, and certificate-based authentication (CBA) when configured for multi-factor (e.g., smart card with PIN + certificate).
The SC-300 materials highlight that these are the only methods that fully meet NIST AAL3 phishing resistance requirements. Voice calls, SMS, email OTP, and Microsoft Authenticator are not phishing-resistant because they can be intercepted or phished.
Therefore, when building a Conditional Access policy to secure administrative access, you must allow only phishing-resistant methods to meet Microsoft's best practice.

NEW QUESTION: 92
Azure □□□ □□□□.
Azure AD □□□ Log Analytics □□ □□□□ □□□□□.
□□□ □□□□ □□□□ □□□ □□ □□□□□ □□□□ □□□.
□□□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.

Answer:

```
SigninLogs
| where ResultType == 0
|  login_count = count() by Identity
```

extend
print
project
render
summarize

```
|  columnchart
```

extend
print
project
render
summarize

Explanation:
Box 1 =
SigninLogs
| where ResultType == 0
| summarize login_count = count() by identity
| render piechart
This query retrieves the sign-in logs, filters the successful sign-ins,summarizesthe count of sign-ins per user, and renders the result as a pie chart.
Box 2 = Render
In Microsoft Entra ID (Azure AD), the SigninLogs table in Azure Monitor Logs (Log Analytics workspace) contains data about user sign-ins. When you want to query and graphically display the number of sign-ins per user, you use Kusto Query Language (KQL) - the same language that powers Log Analytics, Azure Monitor, and Microsoft Sentinel.
The correct syntax must first aggregate the data and then visualize it:
* where ResultType == 0 filters for successful sign-ins (since 0 indicates success).
* summarize login_count = count() by Identity aggregates (counts) all sign-in events per user (Identity field). The summarize operator in KQL is specifically used to group and aggregate data.

* render columnchart graphically displays the summarized results as a column chart. The render operator is used to visualize query output in supported formats such as timechart, piechart, or columnchart.
Therefore, the correct operators to fill in are:
* First blank: summarize
* Second blank: render
According to the Microsoft SC-300 Study Guide and Microsoft Learn module "Query and visualize sign-in logs with Kusto Query Language", the recommended method to display sign-in frequency per user is:
"Use the summarize operator to aggregate sign-in counts by user, followed by render to visualize results."
Final Query Answer:
SigninLogs
| where ResultType == 0
| summarize login_count = count() by Identity
| render columnchart

NEW QUESTION: 93
Microsoft 365 E5 □□□ □□□□.
□□□□ □□ □□□□ □□ □□□ □□□□ □□□□□□ □□□□□.
□□ □□ □□□ □□□□ 20□ □□□ □□□□ □□□ □□ □□□□□ □□□ □□□□ □□□.
□□□□ □□ Microsoft Defender □□□□ □□ □□□ □□□ □□□□ □□□?
A. □□ □□ □□
B. OAuth □ □□
C. □□ □□
D. □□ □□
Answer: (SHOW ANSWER)
According to Microsoft Defender for Cloud Apps documentation and the SC-300 study guide, an OAuth app policy monitors third-party applications that request access to Microsoft 365 data through Microsoft Graph API permissions. These apps can request delegated or application permissions. When an app is authorized by many users and requests high permissions such as Calendars.ReadWrite , it can introduce security risks.
Defender for Cloud Apps allows administrators to create OAuth app policies to generate alerts when an app:
* Requires high permissions (e.g., read/write to mailboxes, calendars, or files).
* Is authorized by more than a specified number of users (for example, more than 20).
This matches the requirement in the question exactly. Other policy types (anomaly detection, access, or activity) monitor user or session behavior, not app consent behavior.
As per Microsoft's documentation:
"Use OAuth app policies to detect risky OAuth apps, monitor application permissions, and alert when apps are authorized by an unusual number of users or request excessive permissions."

NEW QUESTION: 94
□□ □□ □□□ 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, Giup2

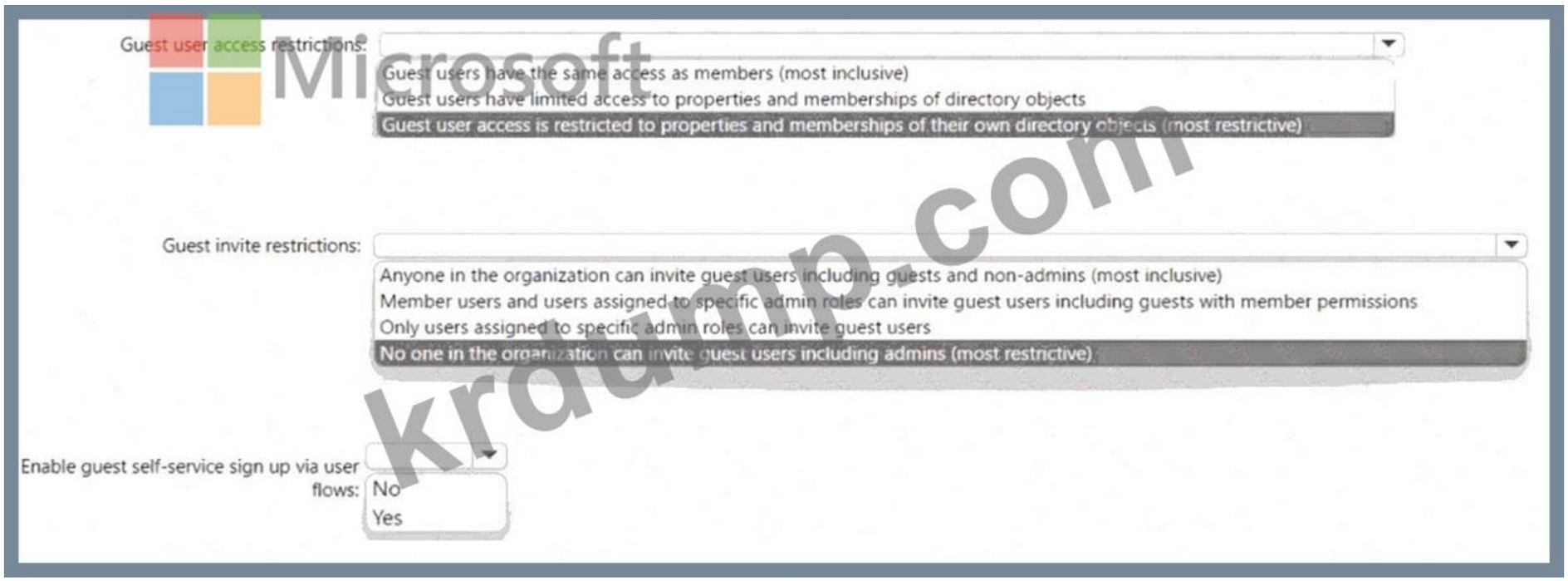
□□ □□□ □□□ □□□ □□□ □□□□□.
* □□ : □□1
* □□ □□: □ □ □□ □□
* □□ : □□1
* □□□□ : □□ □□□
* □□□ □□: □□ □□□
□□ □□□: □□□ □□□□ □□□□□.

Answer:

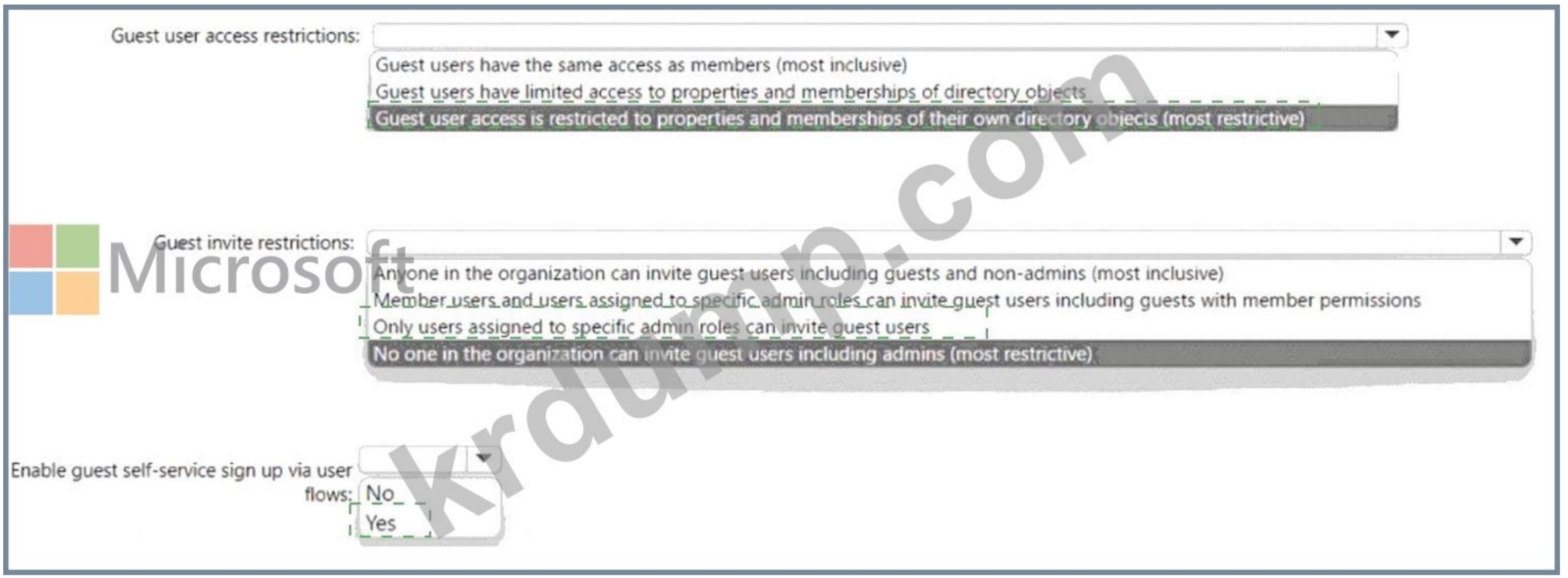
Explanation:
User1 can perform an access review for User1: No
User1 can perform an access review for Managed2: Yes
User1 can perform an access review for User3: Yes
In this scenario, an access review named Review1 has been configured for Group1, with the following conditions:
* Review scope: Teams + Groups
* Group: Group1
* Scope: All users
* Reviewers: Group owner(s)
* Fallback reviewers: None
From the configuration, the reviewers of the access review are the owners of Group1 - namely User1 and User4. Therefore, both of these users are authorized to review all members of Group1.
Group1 includes the following members:
* User1 (User, also owner)
* Managed2 (Managed identity)
* Group2 (which includes User3)
Since the scope is set to All users, it includes both internal and external members. However, the SC-300 materials emphasize that reviewers cannot review their own access; Microsoft Learn states: "Reviewers cannot approve or deny their own access in an access review, even if they are members of the group under review." Therefore:
* User1 cannot review themselves # No

* User1 can review Managed2 # Yes, because Managed2 is a member of Group1
* User1 can review User3 # Yes, because User3 is a member of Group2, and Group2 is itself a member of Group1, meaning User3's membership is indirectly part of the review scope This behavior aligns with SC-300 guidance that nested group members are included when the review scope is
"All users," and reviewers (owners) can assess all included members except themselves.

NEW QUESTION: 95
User1□□□ □□□□ □□□ Azure AD □□□□ □□□□. User1□□□ □□□ □□□ □□□ □□□□□□□.
□□ □□ □□□ □□□□□ □□□□ □□ □□ □□ □□□ □□□□ □□□.
*□□□ □□□□ □□ □□□ □□□ □□□□ □□ □□□□□ □□□.
*□□□ □□□□ User1□ □□□ □□ □□□□ □□□□ □□□□ □ □□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.



Answer:



Explanation:

According to the Microsoft SC-300 Study Guide, Exam Ref SC-300, and Microsoft Entra External Collaboration (B2B) documentation, the configuration of External collaboration settings in Azure AD determines how guest users can access directory data and who can invite them into the tenant.

Let's analyze each requirement in context:

Requirement 1: "Guest users must be prevented from querying staff email addresses." To achieve this, Azure AD provides the setting Guest user access restrictions, which defines what a guest can see in the directory. The most restrictive setting ensures that guest users can only see their own profile details and no other users or groups.

Therefore, select:

"Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)." This prevents guests from discovering internal directory data such as email addresses of staff members or group memberships.

Requirement 2: "Guest users must be able to access the tenant only if they are invited by User1." User1 has the User Administrator role. This role is included among the "specific admin roles" allowed to invite guest users when the setting is configured appropriately.

To meet the requirement that only User1 (or other admins) can invite guests, you must configure:

"Only users assigned to specific admin roles can invite guest users." This restricts invitation privileges to admin roles (such as Global Administrator, User Administrator, etc.) and prevents ordinary users or guests from inviting others.

Requirement 3: "Guests should not be able to self-enroll."

Azure AD B2B allows self-service sign-up through user flows (Identity Experience Framework). Enabling this feature would let external users sign up themselves - which violates the condition that guests must be invited by User1 only.

Therefore, set Enable guest self-service sign-up via user flows = No.

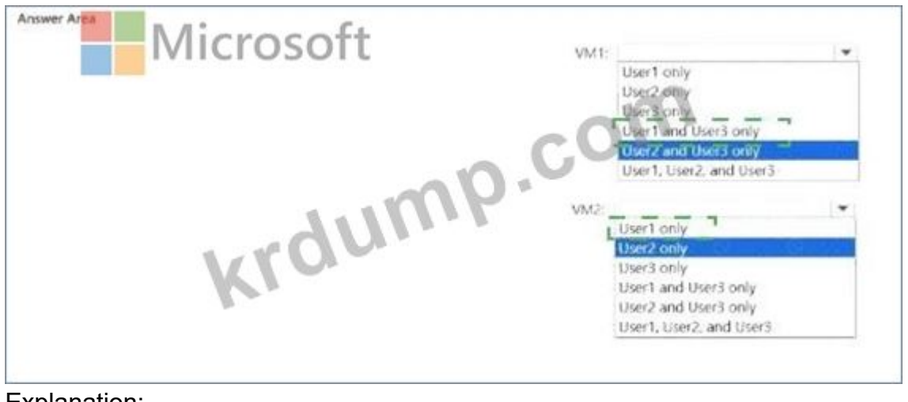
Final Configuration Summary: Setting
Value
Guest user access restrictions
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive) Guest invite restrictions Only users assigned to specific admin roles can invite guest users Enable guest self-service sign-up via user flows No
Microsoft Official Documentation Reference (SC-300 Content):
"To prevent guests from seeing other users in the directory, configure guest user access restrictions to 'most restrictive.' To control who can invite guests, use the setting that limits invitations to users with admin roles.
To disallow self-service guest access, disable user flows for external sign-up."

NEW QUESTION: 96
RG1□□□ □□□ □□□ □□□ Azure □□□ □□□, RG1□□ Microsoft □□ 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□ □□□□ □ □□, □□ □□□□ VM□ □□□□ □ □□□? □□□□□ □□ □□□□ □□ □□□ □□□□□. □□:
□□□ □□ □□□ □□□ 1□□ □□□□□.
□□ □□□□ VM1□ □□□□ □ □□, □□ □□□□ VM2□ □□□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:



Explanation:

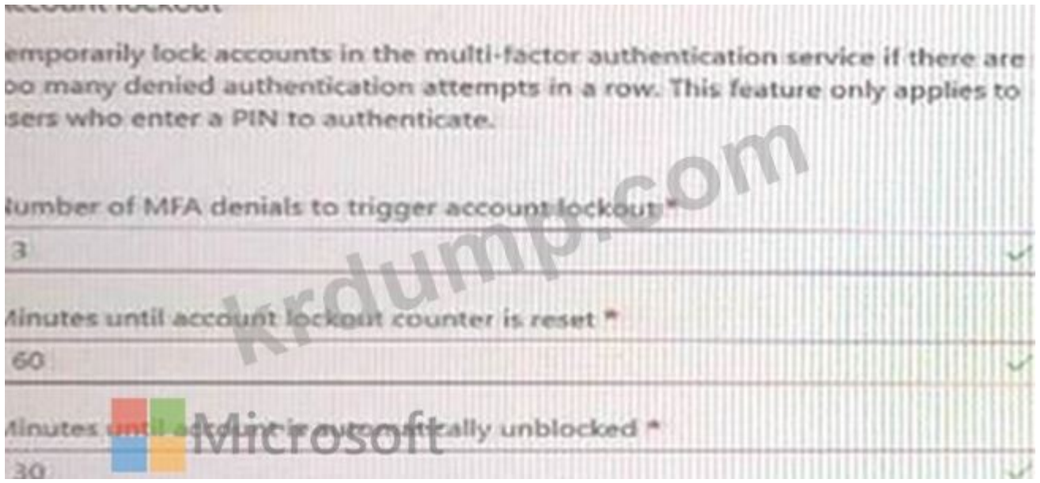
In Microsoft Entra ID-based sign-in to Azure VMs, the right to sign in is granted by the Azure RBAC data- plane roles Virtual Machine User Login and Virtual Machine Administrator Login. The SC-300 study materials state that these roles are "used to log in to a virtual machine with Azure AD credentials" and that scope inheritance applies: "RBAC permissions assigned at a higher scope (subscription, resource group) flow down to child resources." The guidance further clarifies the difference: "Virtual Machine User Login allows standard user login" while "Virtual Machine Administrator Login allows administrator login." By contrast, management roles such as Virtual Machine Contributor "manage virtual machines but do not grant sign-in rights." Applying this to the scenario: User1 has Virtual Machine User Login at the subscription scope, therefore the permission is inherited by RG1, VM1, and VM2, allowing User1 to sign in to both VMs. User3 holds Virtual Machine Administrator Login scoped to VM1, which authorizes sign-in only to VM1 (administrator level) and does not apply to VM2. User2 has Virtual Machine Contributor at RG1; this provides management capabilities (start/stop, configure) but no sign-in permission, so User2 cannot sign in to either VM.
Therefore, the correct selections are VM1: User1 and User3 only and VM2: User1 only.

NEW QUESTION: 97
Microsoft 365 E5 □□□ Azure □□□ □□□□. Azure Monitor□ □□□□ Microsoft Entra □□□ □□□ □□□ □□□□□. Microsoft Entra□ □□ □□ □□□ □□□□ □□□. □□□ □□□ □□ □□ □ □□ □□□□ □□□?
A. Log Analytics □□ □□
B. Azure □□□ □□
C. Azure SQL □□□□□
D. Azure Storage □□
Answer: A (LEAVE A REPLY)

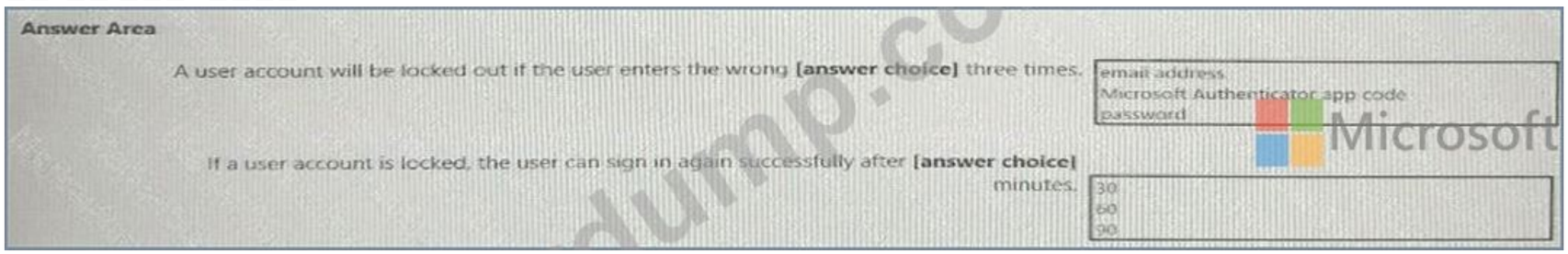
NEW QUESTION: 98
□□□ □□ □□□ □□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□?
A. Azure AD Connect□□ PingFederate□ □□□□ □□□□□□ □□□□□□.
B. Azure AD □□ □□□ □□□□□.
C. Azure AD Connect□□ □□ □□ □□□□ □□□□□□.
D. Azure AD□□ □□ □□ □□□ □□□□□.
Answer: C (LEAVE A REPLY)
In SC-300, Azure AD Identity Protection is the prescribed control to "automatically detect and remediate externally leaked credentials." That specific user risk-Leaked credentials-relies on Microsoft comparing known breached username/password pairs with what Azure AD can evaluate. The study materials explain that Identity Protection "detects leaked credentials when Microsoft finds a match with the user's current credentials," and also note that password hash synchronization (PHS) can be enabled even if your sign-in method is Pass-through Authentication or federation. A common exam call-out is that without PHS, Azure AD has no hash to compare, so the leaked-credential signal is unavailable. Enabling PHS (you can keep PTA as the active sign-in method) allows Identity Protection to raise user risk and enforce policy actions such as require password change or block access. By contrast, Azure AD Password Protection addresses banned/weak passwords at change time, not breached-credential telemetry; federation choices (e.g., PingFederate) don't deliver the leaked-credential signal; and authentication method policy controls how users perform MFA (e.g., methods) rather than whether leaked credentials are detected.
Therefore, to meet the requirement to
"automatically detect and remediate externally leaked credentials," the minimum correct step is to enable password hash synchronization while retaining PTA-exactly as recommended in SC-300 guidance.

NEW QUESTION: 99
□□□ User1□□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
User1□ Microsoft Entra □□□ □□ □□□ □□□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
User1□□ □□ □□□ □□□□ □□□?
A. □□□ □□□
B. ID □□ □□□
C. □□ □□ □□ □□□
D. □□□ □□□ □□□
Answer: C (LEAVE A REPLY)

NEW QUESTION: 100
□□ □□ □□(MFA)□ □□□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□□ □□ □□□ □□ □□ □□□ □□ □□□□□.



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



Answer:

Explanation:

According to the Microsoft SC-300: Identity and Access Administrator Official Study Guide and Microsoft Learn module "Configure Azure AD Multi-Factor Authentication settings", the Ac count Lockout settings in Azure AD MFA define how the service reacts to repeated failed MFA verification attempts.

From the exhibit:

* Number of MFA denials to trigger account lockout: 3
* Minutes until account lockout counter is reset: 60
* Minutes until account is automatically unblocked: 30

1. Lockout trigger type:

The lockout applies to MFA denials - specifically, failed verification attempts using methods such as the Microsoft Authenticator app (OTP code) or phone call verification. It does not apply to incorrect usernames or passwords, as those are handled by Azure AD sign-in risk policies.

The official Microsoft documentation states:

"Account lockout in Azure AD Multi-Factor Authentication occurs after the configured number of denied MFA verification attempts. T his setting applies to users entering an incorrect PIN or app verification code." Therefore, after three incorrect Microsoft Authenticator app codes, the account is temporarily locked.

2. Lockout duration:

The setting "Minutes until account is automatically unblocked: 30" means that once an account is locked due to too many failed MFA attempts, it will automatically unlock after 30 minutes without administrator intervention.

This aligns with Microsoft's MFA service behavior:

"When the account lockout threshold is reached, the account remains locked for the configured duration before being automatically unlocked."

Final Correct Answers:

* Wrong input type causing lockout: Microsoft Authenticator app code
* Unlock duration: 30 minutes

NEW QUESTION: 101

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

□□□ Fabrikam, Inc.□□ □□□ □□□□□ □□□ □□□□ □□□□ □□ □□ □□□ □□□□□. Fabrikam□ fabrikam.com□□□ □□□□ □□□□□.

□ □□ □□□□ □□□□ □□□ Fabrikam □□□□ □□□□□ □□□□ □□□□ □□□.

□□ □□□ □□□□ □□□.

□□ □□□□ □ □□□□□ □□□□□ □□ □□□□□: □□□

□□ □□□ □□: □

□ □□□□□□ □□ □□□□ □□□□ □ □ □: 90

Identity Governance □□□□□□ □□□ □□□□ □□□?

A. □□□ □□□

B. □□ □□ □□

C. □□□□

D. □□□ □□ □□
Answer: (SHOW ANSWER)
According to Microsoft's SC-300 Exam Guide and Microsoft Learn module: Manage Identity Governance in Azure AD , the removal and lifecycle management of external users (B2B guests) within Azure Active Directory's Entitlement Management are configured through Entitlement management settings under the Identity Governance blade.
In scenarios where external partners (such as Fabrikam) are granted access via access pack ages , administrators can define lifecycle settings to ensure that when access is no longer required, the users are automatically removed from the directory. The Entitlement Management directory settings control two specific parameters:
* Block external user from signing in to this directory - determines whether external users can still sign in after access expiration.
* Remove external user - enables automatic deletion of the guest account after a specified number of days.
* Number of days before removing external user - defines the delay period (in this case, 90 days).
Microsoft documentation states:
"To automatically remove external users from your directory after access expires, configure the Entitlement management settings. You can set whether to block sign-in and specify how many days after access expiration the user should be removed."

NEW QUESTION: 102
Microsoft 365 □□□□ □□□□.
□□ □□ □□□ □□□□ □□□ □□□□□□ Microsoft Exchange Online□ □□□ □ □□□□.
□□□□ □□ □□ □□□□□ □□□□ □□□ □□□□□□ □□□□ Exchange□ □□□ □ □□□ □□ □□□.
□□□ □□□□ □□□?
Modern □□□ □□□□ □□□.
A. Microsoft Endpoint Manager□ □□ □□ □□
B. Azure Active Directory(Azure AD)□ □□□ □□□ □□
C. Microsoft Endpoint Manager□ □□□□□□ □□ □□□
D. Microsoft Cloud App Security□ OAuth □□
Answer: B (LEAVE A REPLY)
In Microsoft 365, Basic authentication is an outdated protocol that sends credentials in plain text and does not support MFA. To enforce Modern authentication (OAuth 2.0), which is required for stronger identity protection and token-based access, administrators must block legacy authentication using Conditional Access policies in Azure AD.
According to the SC-300 study guide and Microsoft Learn module "Implement Conditional Access policies" , this can be achieved by:
* Creating a Conditional Access policy in Azure AD.
* Targeting the Exchange Online cloud app.
* Setting the condition Client apps # Other clients (legacy authentication) to block access.
Modern authentication clients (like Outlook 2016+, Outlook on the web, and Outlook mobile) use secure OAuth tokens that comply with Conditional Access requirements (such as MFA, device compliance, or trusted location).
Compliance policies or application control profiles in Microsoft Endpoint Manager do not manage authentication protocols, and Microsoft Cloud App Security OAuth policies govern third-party app permissions, not Exchange connectivity.
Therefore, the correct approach to ensure only Modern authentication clients can connect is to enforce this through a Conditional Access policy in Azure AD.

NEW QUESTION: 103
□□□ Azure AD □□□□ □□□□□ □□□.
□□□□ □□ □□□□□ □□□□□ □□ □□(MFA) □□□ □□□□□?
A. Microsoft □□□
B. □□

C. □□□□
D. □□□ OTP
Answer: (SHOW ANSWER)
In a new Azure AD (now Microsoft Entra ID) tenant, the default multifactor authentication (MFA) method tha t is automatically enabled is Microsoft Authenticator .
As per the Microsoft Learn module: Implement and manage Microsoft Entra multifactor authentication and Exam Ref SC-300 , the Microsoft Authenticator app is the default and recommended method because it provides the strongest and most phishing-resistant form of MFA compared to SMS or voice calls.
The guide states:
"New Azure AD tenants have Microsoft Authenticator app enabled by default as the primary method for MFA registration and verification. Users are prompted to register the app when MFA is enforced through security defaults or Conditional Access." Other methods such as SMS , voice call , and email OTP are optional and must be explicitly enabled by an administrator.

NEW QUESTION: 104
□□ 4
□□ □□□□ □□□ □□□ □□ □□□ □□□ □□ □□□ □ □□□ □□ □□□. □□□□ □□ □□□ □□□ □□ □□□ □ □□□ □□ □□□.
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To ensure that all users can consent to apps that require permission to read their user profile and prevent them from consenting to apps that require any other permissions, you can configure the user consent settings in the Microsoft Entra admin center. Here's how you can do it:
Sign in as a Global Administrator:
Access the Microsoft Entra admin center with Global Administrator privileges.
Navigate to user consent settings:
Go toIdentity>Applications>Enterprise applications>Consent and permissions>User consent settings1.
Configure the consent settings:
Under User consent for applications, select the option that allows users to consent to apps that only require permission to read their user profile.
Ensure that all other permissions are set to require administrator consent, thus preventing users from consenting to apps that require additional permissions1.
Save the settings:
After configuring the consent settings, select Save to apply the changes.
By following these steps, you will have configured the system to allow user consent for apps that need to read the user profile while blocking consent for apps that require additional permissions. This setup helps maintain user autonomy where appropriate while safeguarding against unauthorized access to broader permissions.

NEW QUESTION: 105
contoso.com□□□ Azure Active Directory(Azure AD) □□□□ □□, □ □□□□ User1□□□ □□□□ □□□□.
User1□ □□ □□ □□□ □□□ □□□ □□□□.
2020□ 11□ 5□□ □□ □□□ □□ contoso.com□□ □□ □□□ □□□ □□□□□.
□□: Terms1
□□ □□: Contoso □□ □□
□□□□□ □□ □□ □□ □□: □□
□□ □□□□ □□□ □□ □□: □□
□□ □□: □□
□□□: 2020□ 12□ 10□□□
□□: □□

2020□ 11□ 15□, □□□ 1□ □□ 3□□ □□ 1□ □□□□□.
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□□ □□□□ 1□□□□.

Answer:

Device1 on Nov 16, 2020: Yes
Device3 on Dec 15, 2020: Yes
Device3 on Nov 20, 2020: No
According to Microsoft's official documentation and SC-300: Identity and Access Administrator Study Guide (Identity Governance and Compliance section) , Terms of Use (ToU) in Azure Ac tive Directory are managed under Conditional Access policies and enforce user acknowledgment before granting access to resources.
Key configuration settings from the scenario:
* Require users to expand the t erms of use: On # Users must open the document before accepting.
* Require users to consent on every device: On # Each device requires a separate acceptance (consent stored per device).
* Expire consents: On
* Expire starting on: December 10, 2020
* Frequency: Mon thly # Users must reaccept terms every month after initial consent.
Given that:
* Terms1 was created on November 5, 2020 .
* User1 accepted the terms on November 15, 2020 on Device3 only.
* Acceptance is per device, meaning Device1 and Device2 do not yet have acceptance recorded.
Therefore:
* On November 16, 2020 (next day) , when User1 signs in from Device1 , they must accept Terms1 # Yes .
* The terms expire monthly starting December 10, 2020 , so by December 15, 2020 , User1 must reaccept the terms on Device3 # Yes .
* November 20, 2020 is still within the same month of initial acceptance (November 15), and terms have not expired yet # No , reacceptance is not required that soon.
This aligns with Microsoft documentation excerpt:
"When 'Require users to consent on every de vice' is enabled, each unique device sign-in requires separate consent. When expiration is configured, users must reaccept terms based on the defined frequency starting from the specified date."

NEW QUESTION: 106

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□□ □□□□□.

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:

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.	○	○

Explanation:

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.	○	○

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 t o 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.
Based on the Microsoft SC-300: Id entity and Access Administrator Study Guide and Microsoft Learn module "Manage external collaboration settings in Azure AD", Azure Active Directory provides granular control over external collaboration through External collaboration settings and Collaboration restrictions. These settings control which external domains can receive guest invitations.
1# # Collaboration Restrictions Setting The configuration in the exhibit shows:
"Allow invitations only to the specified domains (most restrictive)"
Target Domain: Outlook.com
This means invitations can only be sent to users whose email domains are explicitly listed (in this case, Outlook.com). Any other external domain (like fabrikam.com or adatum.com) is not permitted to receive or accept invitations.
2# # Evaluating Each User User1@outlook.com
* Domain Outlook.com is listed under allowed domains.
* Although the invitation was initially not accepted , since the domain is allowed, User1 can accept the invitation and gain access. # Answer: Yes User2@fabrikam.com
* The domain fabrikam.com is not listed in the allowed domains list.
* However, this user already accepted the invitation before the restriction was configured.
* Once a guest has accepted the invitation, they are an existing guest object in Azure AD and retain access unless explicitly removed. # Answer: Yes User3@adatum.com
* Domain adatum.com is not listed under allowed domains.
* Therefore, this user cannot receive or accept new invitations for collaboration resources like SharePoint Online. # Answer: No Summary from Microsoft documentation:
"When collaboration restrictions are set to allow invitations only to specified domains, invitations to all other domains are blocked. Existing guest users who have already accepted invitations remain unaffected." (Source: Mic rosoft Learn - Configure external collaboration settings in Azure AD)

NEW QUESTION: 107
□□ □□□ 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. User1□
B. User1□ Group1□

C. User1 □ VW1□
D. User1, VM1 □ App1□
E. User1, Group1, Vm1 □ App1
Answer: (SHOW ANSWER)
Azure RBAC roles on a scope (subscription, resource group, resource) can be assigned to Azure AD security principals: users , groups , and service principals (which includes enterprise applications and managed identities). The SC-300 content states: "RBAC roles can be assigned to users, groups, and applications (service principals), including system-assigned managed identities created for Azure resources." In the table, User1 (user), Group1 (security group), VM1 (a VM with system-assigned managed identity), and App1 (an enterprise application service principal) are all valid principals. Therefore, all four can be assigned the Contributor role at the RG1 scope. This enables least-privilege delegation to workloads (VM1/App1) and to people (User1/Group1) without granting broader directory roles.

NEW QUESTION: 108
□□□ 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 □□□□ □□□ □ □□ packaqe1□□□ □□□ □□□ □□□□ □□ □□□□□.
Fabrikam□ litware□ □□ □□□ □□□ □□□□ □□ □□□□ package1□ □□□□ □□□□ □□□ □ □□□ □□ □□□.
□□□ □□□□ □ □□□□ □□□ □□□ □□□□□?
A. 1
B. 2
C. 3
D. 4
Answer: (SHOW ANSWER)
According to the official Microsoft SC-300: Microsoft Identity and Access Administrator St udy Guide and Exam Ref SC-300 textbook, when configuring Entitlement Management in Azure AD Identity Governance
, connected organizations are used to define which external directories or domains are allowed to request access to specific access packages. A c onnected organization represents a single external organization whose users can be invited as guests (B2B collaboration users) or allowed to request access packages.
Each connected organization is identified by its verified domain names. For example, if yo u have two separate companies, Fabrikam, Inc. and Litware, Inc. , and they each have distinct verified domains - fabrikam.com, adatum.com (for Fabrikam), and litwareinc.com, contoso.com (for Litware) - they must each be configured as separate connected orga nizations because connected organizations are defined at the organization level, not per domain.
Even though each organization may have multiple verified domains, the configuration treats all of an organization's verified domains as part of the same connec ted organization. Therefore, to allow users from both Fabrikam and Litware to request access to Package1 , you must create two connected organizations - one for Fabrikam and one for Litware.
This behavior is confirmed in Microsoft documentation and training modules under "Manage connected organizations" in Azure AD Entitlement Management, which states that "each external organization that requires access must have its own connected organization entry, regardless of how many domains it owns."

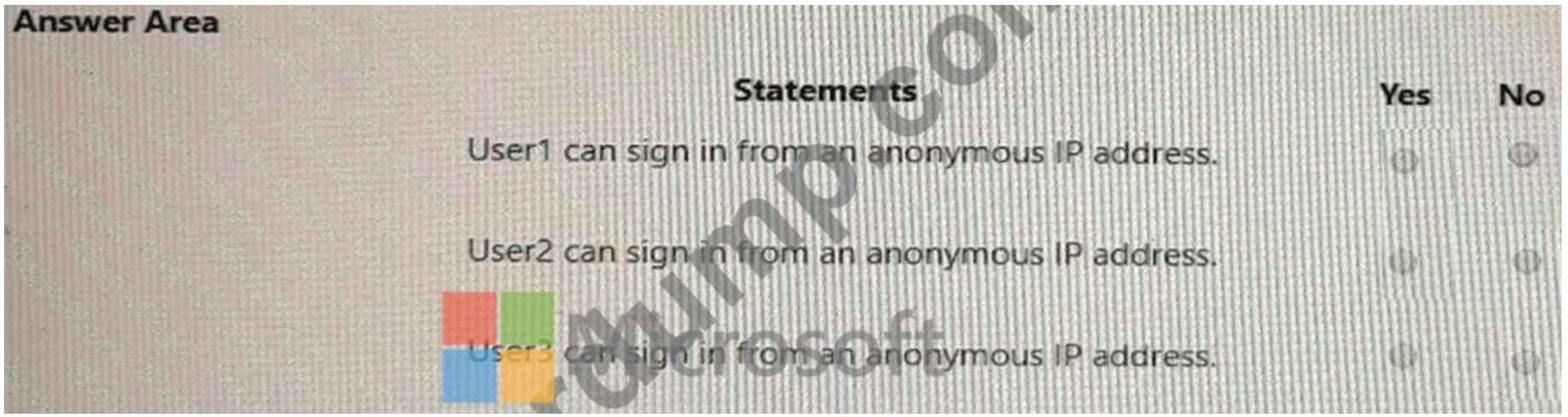
NEW QUESTION: 109
Azure AD □□□□ □□□□.
□□ □□ □□□□ □□□.
□□ □□ □□ □□□ □□□ □□□□ □□□□□?

A. □□□□ □□□□
B. □□ IP □□
C. □□□□ □□ □□□ □□
D. Azure AD □□ □□□□□
Answer: D (LEAVE A REPLY)
In Azure AD Identity Protection, risk detections are classified into sign-in risks and user risks . According to Microsoft's SC-300 Study Guide and Identity Protection documentation , a user risk represents the probability that an account has been compromised . Microsoft aggregates multiple sign-in signals and applies its threat intelligence algorithms to determine whether a user's identity may be at risk.
Among the listed options, Password spray , Anonymous IP address , and Unfamiliar sign-in properties are sign-in risk detections , while Azure AD threat intelligence is the only type classified as a user risk detection
.
Microsoft Docs states: "User risk detections are generated by Azure AD threat intelligence when Microsoft detects that user credentials appear to be compromised."

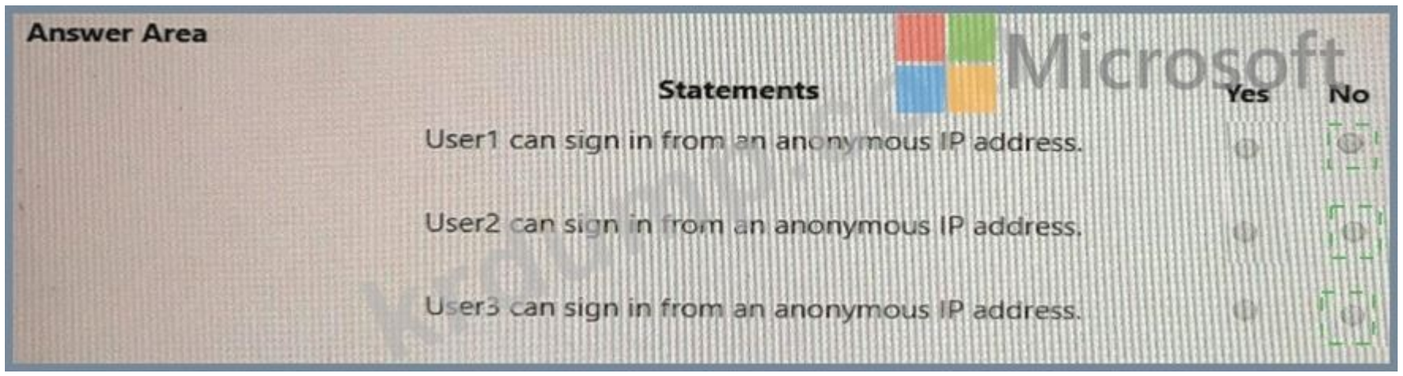
NEW QUESTION: 110
□□ □□ □□□ □□□□ □□□ Azure AD □□□□ □□□□.

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

Azure AD Identity Protection□□□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
* □□:
o □□□: □□1
o □□□ □□: □□ □□
* □□□:
o □□: □□ □□
* □□ □□: □□
Azure AD Identity Protection□□□ □□ □□□ □□□ □□□ □□ □□□ □□□□□.
* □□:
o □□□: □□2
o □□□ □□: □□ □□
* □□□:
o □□: □□ □□ □□ □□
* □□□ □□□□□.
□□ □□:
□□:
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:

User1 can sign in from an anonymous IP address: No

User2 can sign in from an anonymous IP address: No

User3 can sign in from an anonymous IP address: No

According to the Microsoft SC-300 Study Guide, Exam Ref SC-300, and Microsoft Entra Conditional Access and Identity Protection documentation, when multiple conditional access (CA) and risk policies are active, Azure AD evaluates them collectively, and if any applicable policy denies access, the user is blocked.

Let's break down the setup:

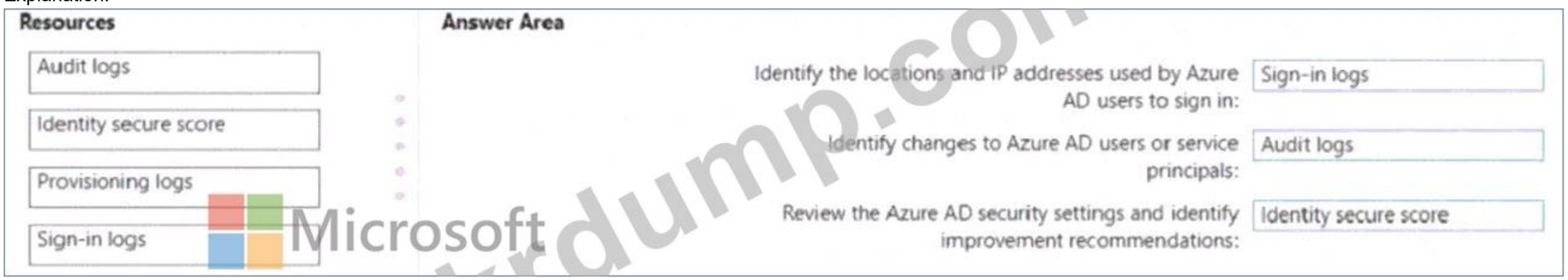
* User risk policy
* Applies to Group1
* User risk: Low and above
* Access: Block access
* Enforced: On
* Sign-in risk policy
* Applies to Group2
* Sign-in risk: Low and above
* Access: Require MFA
* Enforced: On
* CAPolicy1: Users connect from a trusted IP address (Status: On)

* CAPolicy2: Users' devices are marked as compliant (Status: On)
* CAPolicy3: Sign-in risk is low (Report-only # not enforced)
Identity Protection policies configured: Conditional Access Policies configured:
User Analysis: User
Member of
MFA Status
Applicable Policies
Result
User1
Group1
Enabled but never used
User risk policy # Block access if risk # Low
Cannot sign in (blocked by user risk policy).
User2
Group2
Disabled
Sign-in risk policy # Require MFA
Cannot complete sign-in (MFA required but disabled).
User3
Group1, Group2
Enforced and used
Both policies apply # Block access (user risk policy takes precedence)
Blocked (since one policy enforces deny).
Additionally, CAPolicy1 (trusted IP) denies anonymous IP addresses because anonymous IPs are not trusted or registered - Azure marks such attempts as "risky sign-ins." Thus, regardless of MFA capability, no user can sign in from an anonymous IP address.

NEW QUESTION: 111
Microsoft 365 E5 □□□ □□□□. □□ □□□ □□□□ □□□.
* Azure AD □□□□ □□□□□ □ □□□□ □□ □ IP □□ □□
* Azure AD □□ □□□ □□□□ □□ □□ □□□ □□□□□.
* Azure AD □□□ □□ □□□ □□□ □□ □□□ □□□□□.
□ □□□ □□□ □□□□ □□□? □□□□ □□□ □□□□ □□□ □□ □□□ □□□ □□□□.
□ □□□□ □ □, □□ □ □□ □□ □□□□ □□ □ □□□□. □□□□ □□□ □ □□□ □□ □□□ □□□□□□ □□□□□ □ □□ □□□□.

Answer:

Explanation:



According to the Microsoft SC-300 Study Guide and official Microsoft Learn modules "Monitor and maintain Azure AD" and "Implement and manage identity governance", different log types and reports within Azure Active Directory provide distinct insights for security and compliance management.

* Sign-in logs: The Sign-in logs provide detailed information on authentication attempts in Azure AD, including user identity, application accessed, authentication status, IP address, and geographical location. These logs help identify unusual sign-in patterns or possible compromise by tracking where and from which IP addresses users are accessing resources. The SC-300 documentation states:

"Sign-in logs in Azure AD enable administrators to analyze user authentication attempts, track IPs, and review sign-in locations to detect anomalies and secure identities."

* Audit logs: The Audit logs record changes within Azure AD, such as user creation, role assignments, application registration, or service principal modifications. These logs allow administrators to trace "who did what and when," which is essential for compliance auditing and operational transparency.

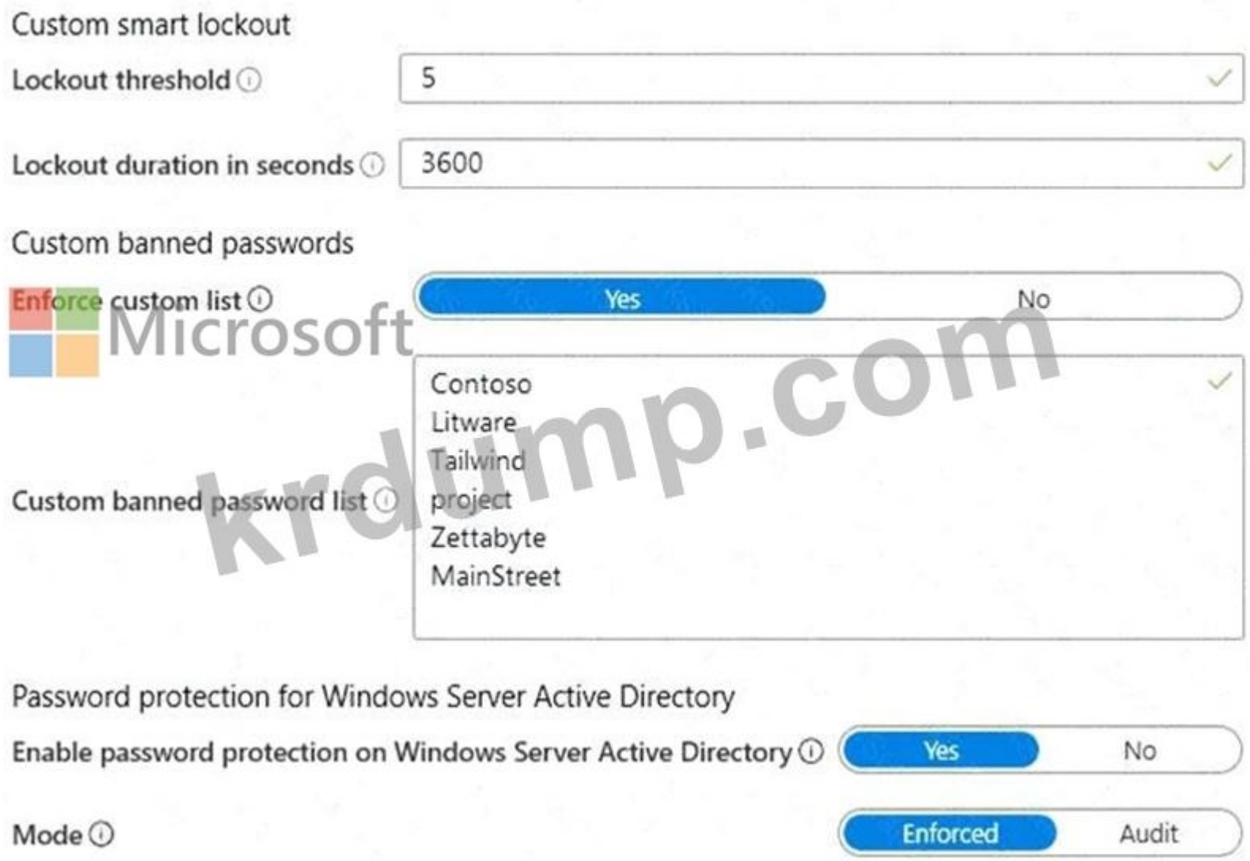
"Audit logs in Azure AD capture directory-level changes, including updates to users, groups, applications, and service principals."

* Identity Secure Score: The Identity Secure Score in Microsoft Entra (formerly Azure AD) provides a security posture assessment for your organization's identity configuration. It offers improvement recommendations to strengthen protection, including MFA enforcement, Conditional Access, and privileged identity management.

"Identity Secure Score helps organizations assess their security configuration against Microsoft best practices and provides actionable improvement recommendations."

NEW QUESTION: 112

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



□□ □□□□□ □□□□ □□□□:

* □□□□ □□ @ □
* T@ilw1nd
* C0nt0s0

□□ □□□□□ □□□□□?

A. Pr0jectlitw@re □ T@ilw1nd□

B. C0nt0s0□

C. C0nt0s0, Pr0jectlitw@re, □□□ T@ilw1nd

D. C0nt0s0 □ T@ilw1nd□

E. C0nt0s0 □ Pr0jectlitw@re□

Answer: (SHOW ANSWER)

Azure AD Password Protection combines a global banned password dictionary with any custom banned password list and applies fuzzy matching (norm alizing case, detecting common char acter substitutions, and splitting words) to block weak variants. In the exhibit, custom enforcement is enabled and the list contains:

Contoso , Litware , Tailwind , and project (plus others). The SC-300 content describes th at if a user attempts a password containing or derived from these terms, even with substitutions like 0 for o or @ for a , it will be rejected.

* C0nt0s0 # matches Contoso via character substitution # blocked .
* Pr0jectlitw@re # includes project and litware wit h substitutions # blocked .

* T@ilw1nd # matches Tailwind with common substitutions # blocked . With custom list enforcement turned on, all three candidate passwords are rejected.

NEW QUESTION: 113
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□□ □□□ □ □□ □□ □□□□ □□□ □ □□□□. □□ □□□ □□ □□□ □□□□ □□□□.
Microsoft 365 E5 □□□ □□□□.
User1□□□ □□□□ □□□□□.
User1□ ID □□ □□ □□ □□□ □□□ □□□□□ □ □□□ □□□□ □□□.
□□ □□: User1□□ □□□ □□□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: (SHOW ANSWER)
Expla nation:
The User Administrator role allows management of user accounts, licenses, and group memberships within Azure AD but does not grant access to security configurations, Secure Score dashboards, or improvement actions.
According to Microsoft's Secure Score documentation:
"Only users with Global Administrator, Security Administrator, or Security Reader roles can access Microsoft Secure Score. To modify improvement action statuses, the user must be a Security Administrator or Global Administrator." Therefore, a User Administrator cannot update Secure Score improvement actions.

NEW QUESTION: 114
Microsoft 365 E5 □□□ □□□□.
□□□□ □□ Microsoft Defender □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□□ □□ Microsoft Defender □□□□ □□□ □□□□□ □□□□□.
B. Microsoft Defender for Cloud Apps □□□□ □ □□□/□□ □□□ □□□□□.
C. Azure Active Directory □□ □□□□ □□□ □□□ □□□ □□□□.
D. Microsoft Defender for Cloud Apps □□□□ □□ □□□□ □□□□.
Answer: C (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide , Exam Ref SC-300
, and Microsoft Defender for Cloud Apps (MDCA) documentation , a session policy in Defender for Cloud Apps (formerly Microsoft Cloud App Security) is used to monitor and control user sessions in real time. These policies provide granular session-level access controls such as limiting downloads, blocking uploads, or monitoring user activity in SaaS applications integrated with Defender for Cloud Apps.
However, before a session policy can function, the Conditional Access App Control feature must be enabled. This integration connects Azure Active Directory (Azure AD) with Microsoft Defender for Cloud Apps , allowing session control to be enforced through Conditional Access policies .
The SC-300 official training content under "Implement and configure Microsoft Defender for Cloud Apps" states:
"To apply session controls using Microsoft Defender for Cloud Apps, you must first configure a Conditional Access policy in Azure AD that routes user sessions to Defender for Cloud Apps for inspection. Only after this step can you define a session policy within the Defender for Cloud Apps portal." Thus, the correct first step is to create a Conditional Access policy in Azure AD that uses the Use Conditional Access App Control option. This action establishes the required connection path so that session control policies in Defender for Cloud Apps can take effect.

NEW QUESTION: 115

Azure Monitor□ □□□□ Azure Active Directory(Azure AD) □□ □□□ □□□□□.
□□ Azure AI □□□ □□□ □□□ □□ □□□ □□□ 100□ □□ □□□□.
□□ □□ □□□ □□ □□□□ □□□ □□□ □□ □□□.
□□□: Azure Monitor□□ □□□ □□ □□□ □□□□.
□□□ □□□ □□□□□?

A. □

B. □□□

Answer: (SHOW ANSWER)

A Data Collection Rule (DCR) in Azure Monitor defines what data is collected , where it's sent , and how it's transformed before ingestion. It controls log and metric collection , not alert notifications .
Creating or editing a DCR does not change who receives alerts. It only changes the data ingestion pipeline for monitoring and analytics.
Since the goal is to redirect alert emails to a new administrator, modifying or creating a DCR will not achieve that.

NEW QUESTION: 116

□ □□ □□ □□(VM1 □ VM2)□ □□□ Azure SQL □□□ □□□□(SQL1)□ □□□ Azure □□□ □□□□.
VM1□ VM2□ SQL1□□ □□□□ □□□ □ □□□ □□ □□□. □□, □□ □□□ □□□□□ □□□□ □□□□ □□□.
□□□ □□ □□□□ □□□?

A. □□□□ ID

B. □□□

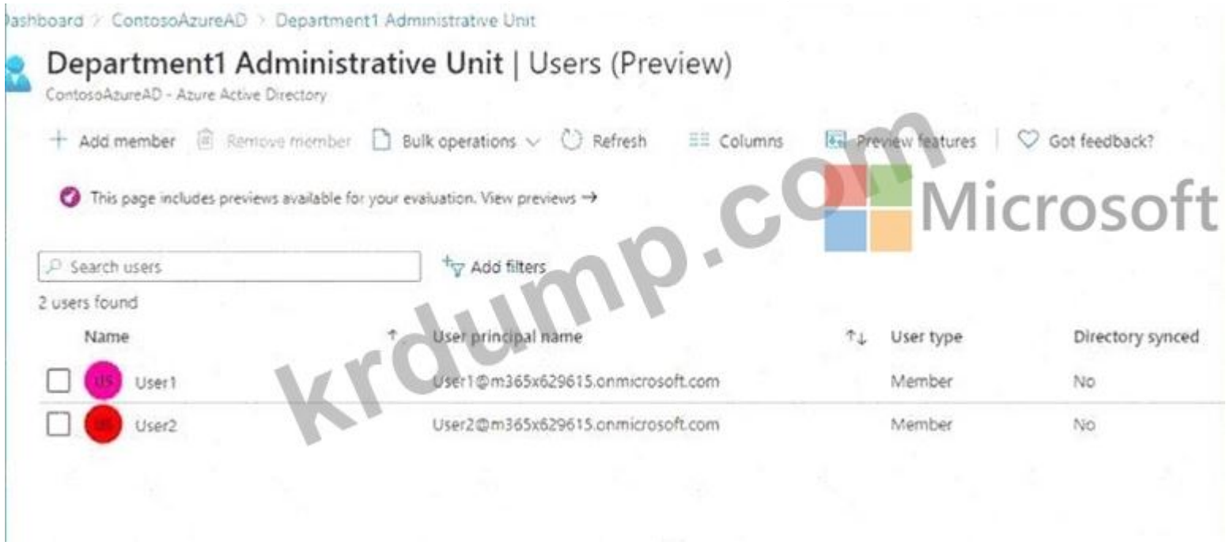
C. □□ □□□ □□(SAS) □□

D. Microsoft Entra □□□ □□

Answer: A (LEAVE A REPLY)

NEW QUESTION: 117

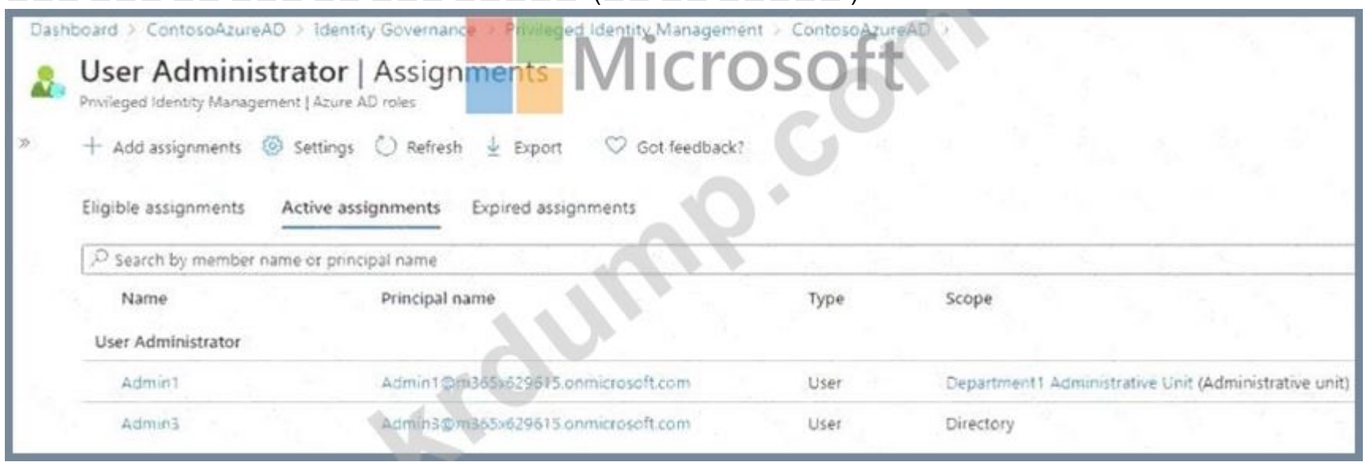
Group3□□□ □□□ Department1□□□ □□ □□□ □□□□ Microsoft Entra □□□□ □□□□.
□□□ □□□□ □□□ □□□ □□□□□. (□□□ □□ □□□□□.)



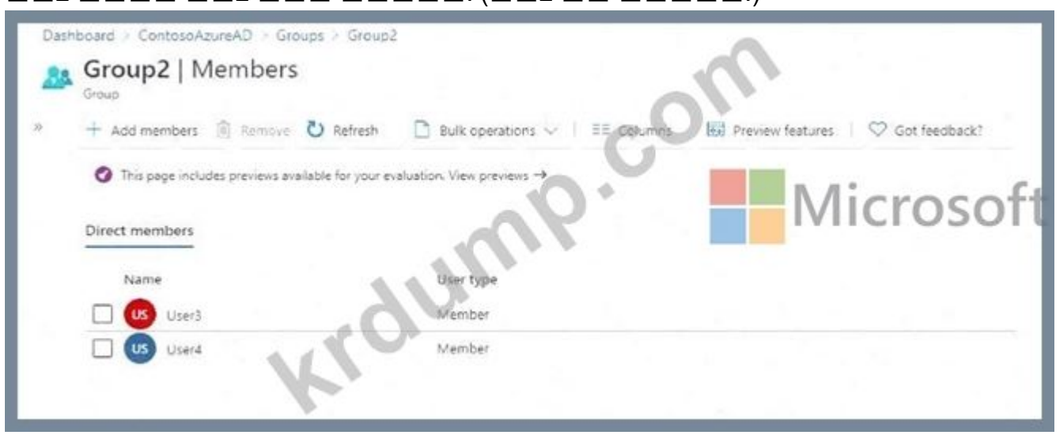
Department1□□ □□ □□□ □□□ □□□ □□□□(□□ □□ □□□□□.)


Department1 Administrative Unit | Groups
ContosoAzureAD - Azure Active Directory
Add
Remove
Refresh
Columns
Preview features
Got feedback?
Search groups
Add filters
Name
Group Type
Membership Type
Group1
Security
Assigned
Group2
Security
Assigned

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


Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD
User Administrator | Assignments
Privileged Identity Management | Azure AD roles
Add assignments
Settings
Refresh
Export
Got feedback?
Eligible assignments
Active assignments
Expired assignments
Search by member name or principal name
Name
Principal name
Type
Scope
User Administrator
Admin1
Admin1@m365x629615.onmicrosoft.com
User
Department1 Administrative Unit (Administrative unit)
Admin3
Admin3@m365x629615.onmicrosoft.com
User
Directory

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


Dashboard > ContosoAzureAD > Groups > Group2
Group2 | Members
Group
Add members
Remove
Refresh
Bulk operations
Columns
Preview features
Got feedback?
This page includes previews available for your evaluation. View previews
Direct members
Name
User type
User3
Member
User4
Member

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

Answer:

Explanation:

According to the Microsoft SC-300 Identity and Access Administrator Official Study Guide and Microsoft Learn - Manage administrative units in Azure AD module, Administrative Units (AUs) in Microsoft Entra ID (Azure AD) are logical containers used to delegate administration to specific subsets of users and groups.

The User Administrator role can perform specific actions within the scope to which it is assigned. In this scenario:

* Admin1 is assigned the User Administrator role scoped to the Department1 Administrative Unit, meaning Admin1 can only manage users and groups within that administrative unit.
* User3 and User4 belong to Group2, but Group2 members are not part of Department1's listed users (only User1 and User2 are). Therefore, Admin1 cannot reset the passwords of User3 or User4.
* Additionally, Admin1 cannot add User1 to Group3 because Group3 is not included in Department1's administrative scope. The administrator can only modify group memberships for groups within their AU.
* Admin3 is assigned the User Administrator role at the directory (tenant-wide) scope, granting full privileges over all users and groups in the tenant. Therefore, Admin3 can reset User1's password since the scope includes all users in the directory.

Microsoft documentation explicitly states:

"An administrative unit-scoped role grants the ability to manage only those users and groups within the administrative unit. Directory-scoped roles grant management across the entire tenant."

NEW QUESTION: 118

User1□□□ □□□□ Vault1□□□ Azure Key Vault□ □□□ Azure □□□ □□□□.

User1□ Vault1□ □□□ □□□, □ □ □□□ □□□□□□ □□ □ □□□ □□ □□□. □□□□ □□ □□ □□□ □□□ □□□.

User1□□ □□ □□□ □□□□ □□□?

A. Key Vault □□□ □□□

B. □ □□ □□□ □□□

C. □ □□ □□

D. Key Vault Secrets ☐☐☐

Answer: C (LEAVE A REPLY)

Comprehensive and Detailed In-Depth Explanation:

Let's break this down step by step based on Azure Key Vault roles, permissions, and the principle of least privilege, as outlined in Microsoft Identity and Access Administrator documentation.

Understanding Azure Key Vault and the Requirement:

Azure Key Vault is a service that securely stores and manages cryptographic keys, secrets, and certificates. It uses role-based access control (RBAC) to manage permissions for users, groups, and applications.

The question requires that User1 canread the metadataof certificates, keys, and secrets in Vault1. In Azure Key Vault, "metadata" refers to the properties of these objects (e.g., name, creation date, expiration date), not the actual content (e.g., the secret value, key value, or certificate private key).

The solution must follow theprinciple of least privilege, meaning User1 should be granted the minimum permissions necessary to perform the task, without access to unnecessary actions (e.g., modifying or deleting objects).

Azure Key Vault RBAC Roles and Permissions:

Azure Key Vault supports built-in RBAC roles that define specific permissions for managing keys, secrets, and certificates. Let's examine each role in the options:

Key Vault Crypto User:

This role allows a user to perform cryptographic operations using keys (e.g., encrypt, decrypt, sign, verify) and to read key metadata.

Permissions include: Microsoft.KeyVault/vaults/keys/read (read key metadata) and cryptographicoperations like encrypt, decrypt, etc.

However, this role does not grant permissions to read metadata for secrets or certificates, and it includes cryptographic operation permissions, which are not needed for the task.

Key Vault Crypto Officer:

This role is designed for managing keys and performing cryptographic operations. It includes permissions to create, delete, update, and read keys, as well as perform cryptographic operations.

Permissions include: Microsoft.KeyVault/vaults/keys/* (full control over keys).

This role does not grant access to secrets or certificates and provides more permissions than needed (e.g., create, delete), violating the principle of least privilege.

Key Vault Reader:

This role provides read-only access to the metadata of all objects in the Key Vault (keys, secrets, and certificates).

Permissions include: Microsoft.KeyVault/vaults/read (read vault properties) and Microsoft.KeyVault/vaults/*
/read (read metadata for keys, secrets, and certificates).

Importantly, this role does not allow access to the actual content of the objects (e.g., the secret value, key value, or certificate private key), only the metadata. It also does not allow write operations (e.g., create, update, delete).

This aligns perfectly with the requirement to "read the metadata" and follows the principle of least privilege.

Key Vault Secrets User:

This role allows a user to read the content of secrets (not just metadata) and perform operations like getting the secret value.

Permissions include: Microsoft.KeyVault/vaults/secrets/get (read secret values) and Microsoft.KeyVault
/vaults/secrets/read (read secret metadata).

This role does not grant access to keys or certificates, and it provides more access than needed (reading the secret value, not just metadata), violating the principle of least privilege.

Applying the Principle of Least Privilege:

The task requires User1 to read the metadata of certificates, keys, and secrets, but not to access their content or perform any write operations.

Key Vault Readeris the most appropriate role because:

It grants read-only access to the metadata of all objects (keys, secrets, certificates).

It does not allow access to the content of the objects (e.g., secret values), which is not required.

It does not allow write operations (e.g., create, delete), adhering to the principle of least privilege.

The other roles either provide too much access (e.g., Key Vault Crypto Officer, Key Vault Secrets User) or do not cover all required objects (e.g., Key Vault Crypto User, Key Vault Secrets User).

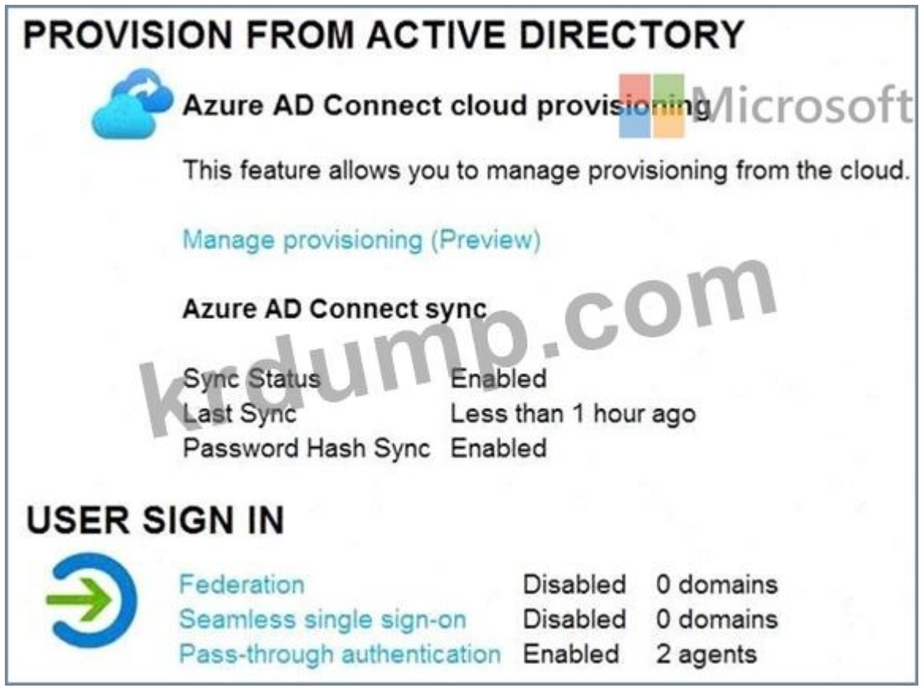
Analysis of the Options:

A). Key Vault Crypto User:
Incorrect. This role only allows reading key metadata and performing cryptographic operations, but it does not provide access to secrets or certificates metadata. It also grants unnecessarycryptographic permissions.
B). Key Vault Crypto Officer:
Incorrect. This role provides full control over keys, which is far more than needed, and does not grant access to secrets or certificates metadata.
C). Key Vault Reader:
Correct. This role provides read-only access to the metadata of keys, secrets, and certificates, exactly matching the requirement while following the principle of least privilege.
D). Key Vault Secrets User:
Incorrect. This role allows reading secret values (not just metadata) and does not provide access to keys or certificates metadata. It grants more access than needed.
Additional Considerations:
If the question had asked for User1 to read the content of secrets (not just metadata), the Key Vault Secrets User role might be considered, but it still wouldn't cover keys and certificates.
Custom RBAC roles could be created to fine-tune permissions, but the question asks for a built-in role, and Key Vault Reader is the best fit.
The question does not specify whether User1 needs to perform other actions (e.g., cryptographic operations, managing the vault). If additional permissions were needed, a combination of roles or a custom role might be required, but the principle of least privilege guides us to the minimal role.
Conclusion:To ensure User1 can read the metadata of certificates, keys, and secrets in Vault1 while following the principle of least privilege, theKey Vault Readerrole should be assigned. This role provides the exact permissions needed without granting unnecessary access. Therefore, the correct answer isC.
References:
Azure Key Vault documentation: "Azure Key Vault RBAC roles" (Microsoft Learn:https://learn.microsoft.
com/en-us/azure/key-vault/general/rbac-guide)
Azure Key Vault documentation: "Secure access to a key vault" (Microsoft Learn:https://learn.microsoft.com
/en-us/azure/key-vault/general/secure-your-key-vault)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Azure Key Vault access control and the principle of least privilege.

NEW QUESTION: 119
□□□ □□□□□□ Azure Active Directory(Azure AD) □□□□ □□□□□ □□□□□ Active Directory □□□□ □□□□ □□□□. □□□□□ □□ □□ □□□ □□□□ □□□□ □□□□.

Name	Type	Directory synced
User1	User	No
User2	User	Yes
User3	Guest	No

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



□□□□□ □□□□□ □□□□□□ □□□ □□□□□□.

□□ □□□□ Azure AD□ □□□□ □ □□□?

A. User1□ User3□

B. User1□

C. User1, User2, User3

D. User1□ User2□

Answer: C (LEAVE A REPLY)

The exhibit shows Password Hash Synchronization (PHS) enabled and Pass-through Authentication (PTA) enabled. The SC-300 materials clarify that when both PTA and PHS are enabled, Azure AD can fall back to PHS if PTA agents become unavailable. The guidance states that PHS can serve as a backup sign-in method to ensure continuity during on-premises connectivity failures. In this scenario, on-premises connectivity to the internet is lost, so PTA agents cannot process sign-ins. Because PHS is enabled, synchronized users can still authenticate in Azure AD using their synced password hashes.

* User1 is a cloud-only user and authenticates directly in Azure AD-unaffected by on-premises outages.
* User2 is directory-synced; with PTA down, sign-in falls back to PHS, allowing access as long as the hash is present.
* User3 is a guest; guests authenticate in their home directory/IdP, independent of your on-premises environment, so they can still sign in.Therefore, during the outage, all three users (User1, User2, and User3) can sign in to Azure AD, satisfying the behavior described in the SC-300 documentation regarding PHS backup for PTA and guest sign-in independence.

NEW QUESTION: 120

contoso.com□□□ Microsoft Entra □□□□ □□, □ □□□□□ Appl□□□ □□□□□□ □□□□□□□ □□□□ □□□□.

□□□□ user1@outlook.com□ □□ □□□ □□□□□.

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

□□□ □□ □□□?

A. New-Mguser cmdlet□ □□□□□.

B. New-MgInvitation cmdlet□ □□□□□.

C. □□ □□ □□ □□

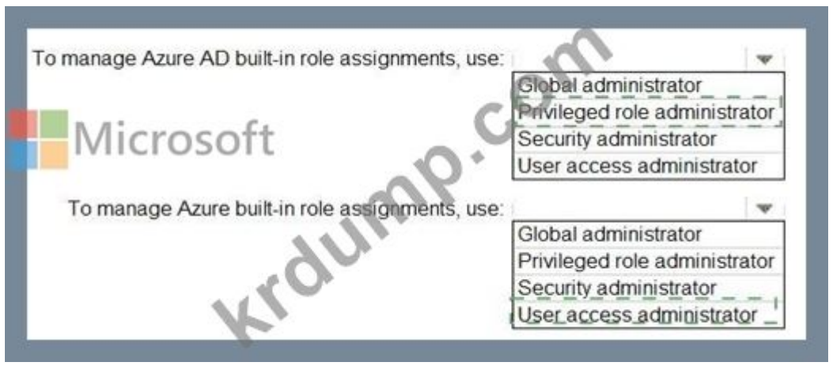
D. Microsoft Entra Connect □□□□ □□□□□.
Answer: (SHOW ANSWER)
When granting external users (such as contractors) access to Microsoft Entra resources like enterprise applications, the correct method is to invite them as guest users.
The Microsoft SC-300 Study Guide states:
"To collaborate with external users who authenticate using their existing accounts (e.g., Outlook.com, Gmail, or another Entra tenant), you must invite them as guest users using the Microsoft Graph API or the New- MgInvitation PowerShell cmdlet." In this scenario, the contractor uses user1@outlook.com, which is a personal Microsoft account. The New- MgInvitation cmdlet creates a guest user in the tenant that links to their external identity for authentication.

NEW QUESTION: 121
Sub1□□□ Azure □□□ □□□□.
Microsoft Entra □□ □□ □□□□□ □□□□□.
□□ □□□ □□□□ □□□.
□□ □ □□ □□□ □□□□ □□□? □ □□□ □□□□ □□□ □□□□□.
□□□□: □□ □□□ 1□□□□.
A. Microsoft Entra □□□□□□ □□□□ □□□□□.
B. Microsoft Entra □□ □□□□ □□□ □□□ □□□□□.
C. Sub1□ □□ □□ □□□ □□□□□.
D. Microsoft Entra □□ □□□□ □□ □□□ □□□□□.
E. Microsoft Entra □□ □□□□ □ □□□ □□□□.
F. Azure Portal□□ □□□ □□ □□(DCR)□ □□□□.
Answer: B,C (LEAVE A REPLY)
According to the official Microsoft SC-300 Study Guide and Microsoft Entra Permissions Management documentation , onboarding Microsoft Entra Permissions Management (formerly CloudKnox) involves two key setup tasks:
* Configuring Data Collection - After purchasing the license, you must connect your Azure subscription (s) to Permissions Management so it can inventory identities, roles, and permissions. This is done from the Microsoft Entra Permissions Management portal, where you enable data collection for each connected cloud environment (Azure, AWS, GCP). This process deploys the required collector identity (service principal) and defines the scope for data gathering.
* Creating Role Assignments - Permissions Management requires proper authorization to read role assignments, permissions, and activity data. You must create a role assignment at the subscription level (Sub1) using a least-privilege role (for example, Reader or CloudKnox Service Principal Role) for the Permissions Management application service principal. This ensures it can scan Azure resources for permission analysis.
Microsoft documentation confirms:
"To onboard Azure subscriptions, assign the CloudKnox service principal a Reader role on each subscription, and configure data collection from within Microsoft Entra Permissions Management."

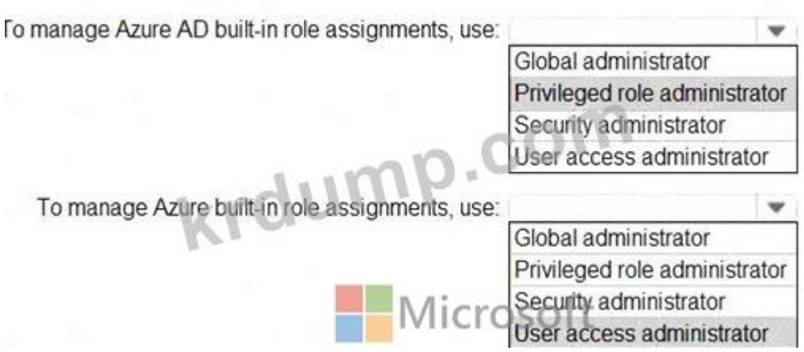
NEW QUESTION: 122
□□ □□ □□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.

□□□□: □□□ □□□ □□□ 1□□ □□□□□.

Answer:



Explanation:



According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn modules "Implement and manage Azure AD roles" and "Implement Privileged Identity Management (PIM)" , there is a clear distinction between Azure AD built-in roles and Azure (resource-based) built-in roles.

* Azure AD built-in roles govern directory-level access - such as managing users, groups, enterprise apps, or security settings in Azure Active Directory (Entra ID). The Privileged Role Administrator role allows the user to manage role assignments for directory roles in Azure AD, including activating roles through PIM. The Global Administrator also has this capability, but the Privileged Role Administrator is the least privilege role that meets the delegation requirement - aligning with the principle of least privilege stated in the scenario. As the documentation notes:

"Privileged Role Administrator manages role assignments in Azure AD, including the ability to activate and assign role s through Azure AD Privileged Identity Management."

* Azure built-in roles, on the other hand, are used to control access at the Azure resource level - for subscriptions, resource groups, and individual resources. The role responsible for managing these assignments is the User Access Administrator. This role can grant or revoke access to Azure resources by managing role assignments within Azure RBAC (Role-Based Access Control). The Microsoft documentation states:
"User Access Administrator allows management o f user access to Azure resources. It can assign roles in Azure RBAC for resources, subscriptions, and management groups." Therefore:
To manage Azure AD built-in role assignments # Privileged role administrator
To manage Azure built-in role assignments # User access administrator This approach satisfies the delegation requirement mentioned in the scenario by assigning the least-privileged roles necessary for each type of role management task.

NEW QUESTION: 123
Azure Active Directory(Azure AD) □□□□ □□□□.
□□□□ □□, □□□□ □□□□□□□ □□□ □ □□□□. '□□□'□ □□□□□.
Admin1□□□ □□□□ App1□□□ □□□ □□□□ □□ □□□□ □□□.
Admin1□ App1□ Azure AD□ □□□ □ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
Admin1□□ □□ □□□ □□□□ □□□?
A. Azure AD□ □□□□□□ □□□
B. □□1□ □□ □ □□ □□□ □□□
C. Subscription1□ □□□ □□□□□□ □□□
D. Azure AD□ □□□□ □□□□□□ □□□
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Learn module "Manage application registrations in Azure AD," the ability to register applications in Azure Active Directory is controlled by the tenant-level setting "Users can register applications" found under User settings
App registrations .
When this setting is set to No, only specific roles with app registration permissions can create or manage app registrations. To follow the principle of least privilege, the appropriate role should grant only the ability to register applications - not broader administrative capabilities.
The roles with permissions related to application registration include:
Application Developer - allows users to register and manage applications they own. This role is specifically designed for users who need to create app registrations when the tenant setting is disabled.
Cloud Application Administrator and Application Administrator - provide broader privileges, including managing all applications, credentials, and permissions, which exceed the minimum needed for this scenario.
Managed Application Contributor and App Configuration Data Owner - are Azure resource-level roles and have no relevance to Azure AD application registration.
From Microsoft documentation:
"If 'Users can register applications' is set to No, assign the Application Developer role to users who need to register apps." Therefore, to allow Admin1 to register App1 while adhering to the principle of least privilege, assign the Application Developer role.

NEW QUESTION: 124
Microsoft 365 E5 □□□ □□□□.
□□□□ Global Secure Access □□□□□□ □□□ □□□□□ □□ □□□□ □□□□ □ □□□ □□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□□□□ □□□□□.
B. □□□ □□□ □□□□ □□ □□□ □□□□□□.
C. □□□ □□□ □□□ □□□□.

D. □□□ □□ □□□ □□□ □□□□□□.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 125

□□ □□ □□□ □□□□ □□□ Azure □□□ □□□□.

Name	Type	Description
User1	User	None
User2	User	None
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

□□□□□ PIM(Privileged Identity Management)□ □□□□□.

PIM□ □□□□ □□ □□□ □□□ □□□□ □□□.

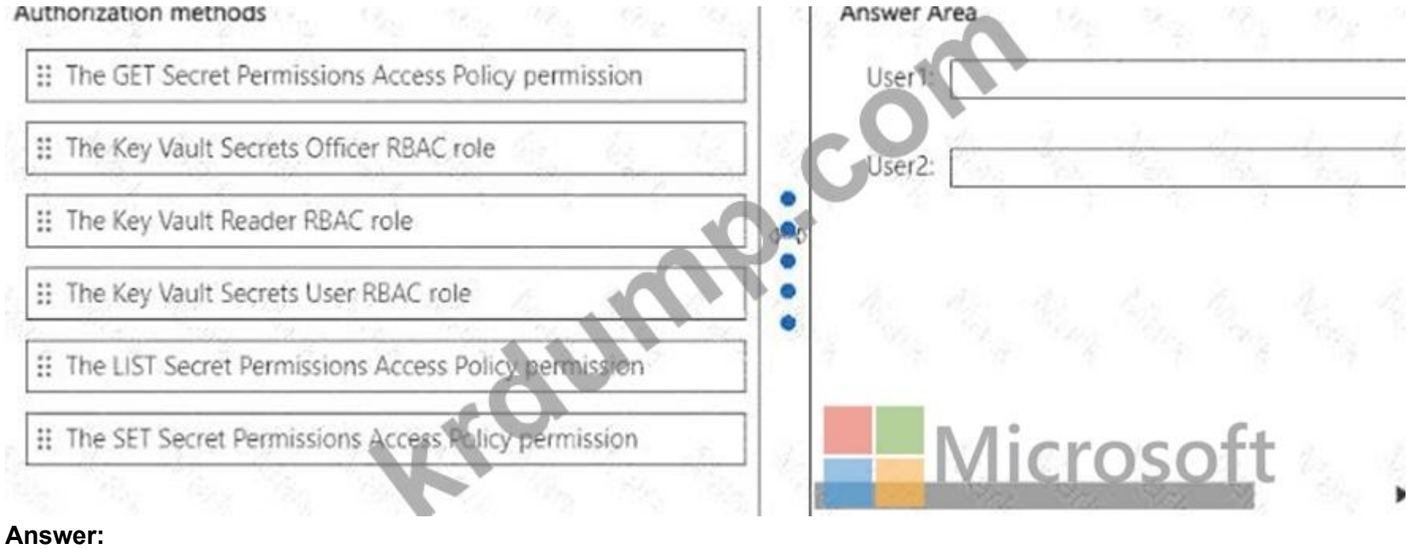
* User1□ Secret1□ □□ □□□□□ □ □□□ □□□□□.

* User2□ Vault2□ □□□ □□□ □□□ □□ □ □□□ □□□□□.

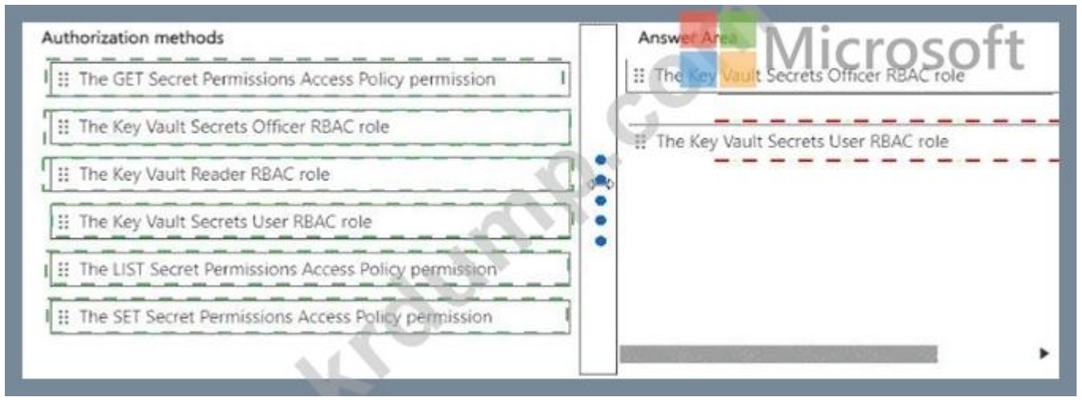
□□□□ □□ □□□ □□□ □□□ □□□.

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

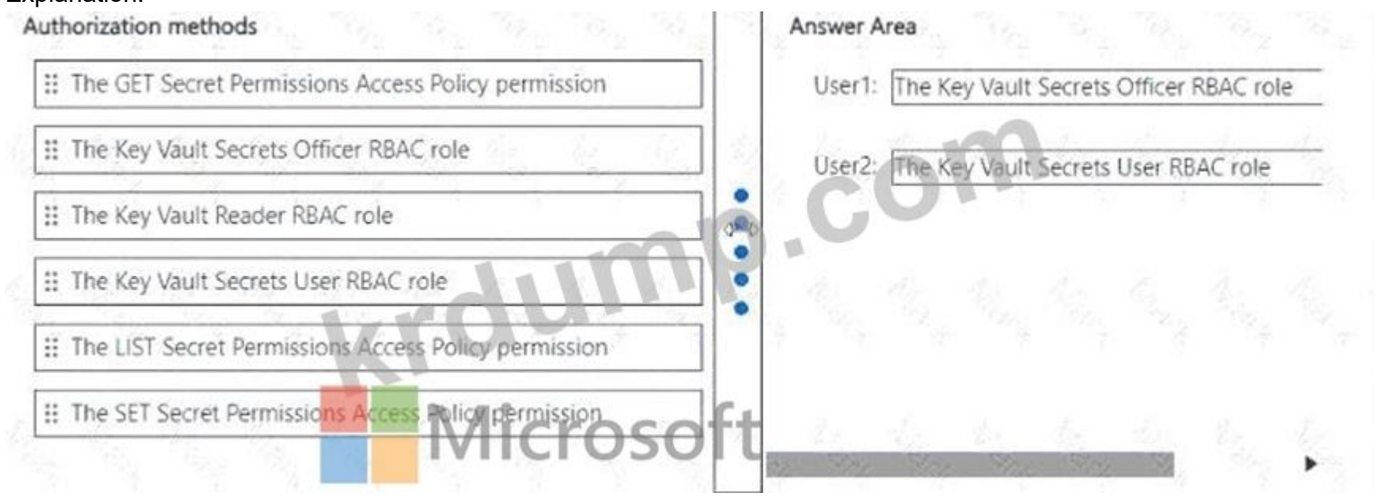
□□: □□ □□□ 1□□□□.



Answer:



Explanation:



In the SC-300 materials on Microsoft Entra PIM for Azure resources and Azure Key Vault authorization, you' re guided to use Azure RBAC (data-plane roles)-not legacy access policies-when you need time-bound, approvable, least-privilege access managed through PIM. The guide explains that PIM can make users Eligible or Active for Azure resource roles and that Key Vault provides specific data actions via built-in RBAC roles. For secrets, the roles are scoped to a vault (and can be further restricted by resource scope) and are purpose-built:

* Key Vault Secrets Officer - described as allowing a user to "create, read, update, and delete secrets" without granting key or certificate permissions. This precisely satisfies User1's requirement to read and update Secret1 while keeping scope limited to secrets (least privilege compared to broader Owner
/Contributor).
* Key Vault Secrets User - documented to "read secret contents" only. This matches User2's requirement to read the contents of the secrets stored in Vault2 while preventing modification or management actions.

The SC-300 coverage stresses that RBAC roles for Key Vault separate permissions for keys, secrets, and certificates, enabling least privilege and PIM governance (eligible/activation, approvals, MFA, and just-in- time) for access to sensitive data.

NEW QUESTION: 126

User1, User2, User3□□□ □ □□ □□□□ □□□ 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□□ □□□□□.

Portals

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

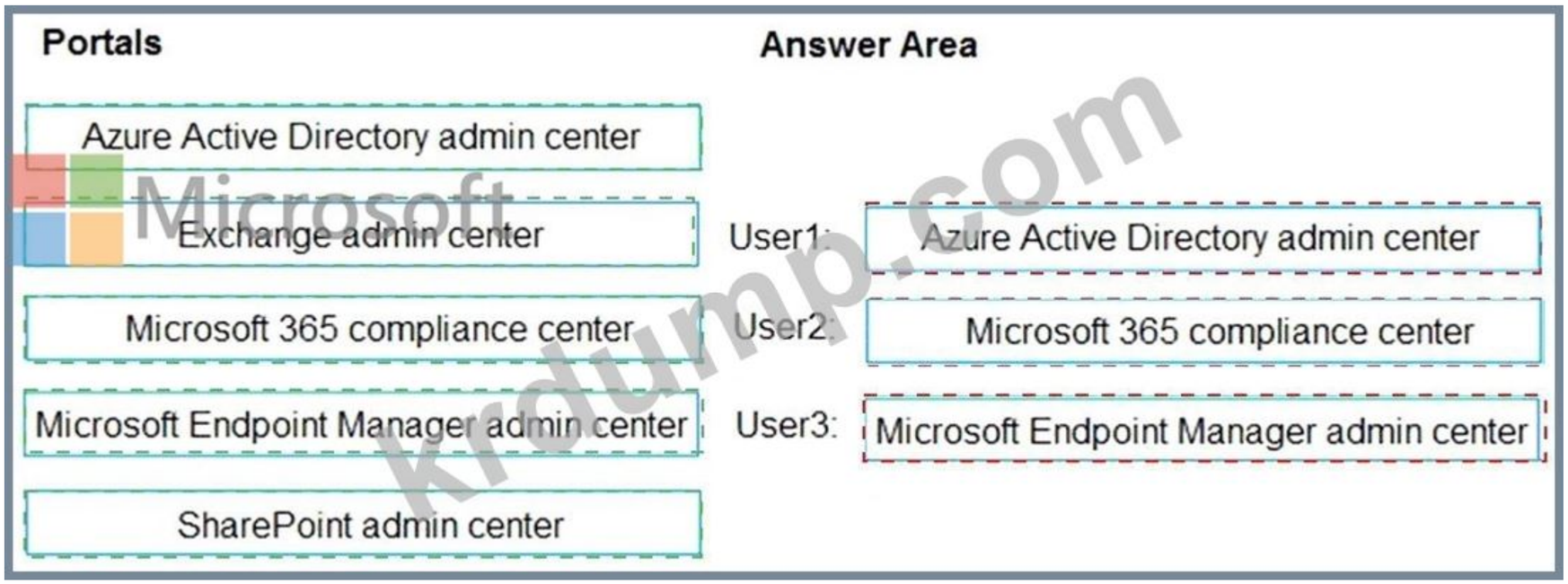
Answer Area

User1:

User2:

User3:

Answer:



Explanation:

User

Portal to Use

User1

Azure Active Directory admin center

User2

Microsoft 365 compliance center

User3

Microsoft Endpoint Manager admin center

This question tests your knowledge of Microsoft 365 administrative roles and their associated management portals, as defined in the Microsoft Identity and Access Administrator (SC-300) Exam Study Guide and Microsoft Learn's "Manage identity and access in Microsoft Entra ID and Microsoft 365" module.

Let's analyze each user and the roles assigned:

* Roles:
* User Administrator
* Device Administrator
* Identity Governance Administrator

User1 These are all Azure AD-based roles.

* The User Administrator role allows the management of users, groups, and password resets in Azure AD.
* The Device Administrator role applies to Azure AD joined devices.
* The Identity Governance Administrator manages Access Reviews, Entitlement Management, and Terms of Use, all of which are under Azure AD Identity Governance.

According to Microsoft documentation:

"User, Device, and Identity Governance Administrators perform their management tasks in the Azure Active Directory admin center." Portal: Azure Active Directory admin center

* Roles:
* Records Management

* Quarantine Administrator
User2 These are Microsoft Purview compliance roles, used for managing retention policies, data lifecycle management, and quarantine of messages/files.
Both are managed through the Microsoft 365 compliance center (previously known as the Security & Compliance Center). Microsoft documentation:
"Records Management and Quarantine Administrator roles allow access to compliance features such as data retention, auditing, and message quarantine, all of which are configured from the Microsoft 365 compliance center." Portal: Microsoft 365 compliance center
* Roles:
* Endpoint Security Manager
* Intune Role Administrator
User3 These roles are directly tied to Microsoft Endpoint Manager (Intune).
* The Endpoint Security Manager configures device compliance, security baselines, and endpoint protection.
* The Intune Role Administrator manages Intune roles and permissions.
Microsoft documentation:
"Administrators managing Intune roles and endpoint security policies use the Microsoft Endpoint Manager admin center (https://endpoint.microsoft.com)." Portal: Microsoft Endpoint Manager admin center

NEW QUESTION: 127
Microsoft Entra □□□□ □□□□.
□ □□□□ □□ □□□□ □□□ □□□ □□□□ □□□□□□ □□□ □□□ □□□ □□□□□ □□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□ □□□ □□
B. □□□ □□ □□
C. □□□ □□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)
Per Microsoft SC-300 Exam Ref and Microsoft Learn module: Implement Continuous Access Evaluation (CAE) , continuous access evaluation is configured and enforced thr ough Conditional Access policies . CAE enables near real-time enforcement of access decisions based on user or session changes such as account disablement, password reset, or location change - without waiting for token expiration. To apply CAE for specific user groups or roles (e.g., Application Administrators), administrators must create or edit a Conditional Access policy and ensure Continuous Access Evaluation is enabled for relevant cloud apps.
Settings like Admin consent , Sign-in risk policy , and Access reviews serve different functions and do not enable continuous enforcement.
Thus, to configure CAE and assign it to Application Administrators, you must use a Conditional Access policy .

NEW QUESTION: 128
□□□ □□□□ User 1□□□ □□□□ □□□ Microsoft Entra □□□□ □□□□.
□ □□□□ □□□□ □□□□ □ □□ □□□ □□□□.
□□□ □□□ □□□□ □□□ □ □□□ User1□□ □□□ □□□□ □□□.
□□ □□ □□□ □□□□ □□□?
A. □□ □□
B. Microsoft 365 □□
C. □□ □□
D. □□□ □□
Answer: (SHOW ANSWER)

The Microsoft SC-300 Exam Ref and Microsoft Learn module: "Manage administrative units" specify that administrative units (AUs) are used to delegate administrative permissions over subsets of users or groups within an Entra tenant.
In this scenario, the goal is to allow User1 to manage only the users in the marketing department. The correct approach is to create an administrative unit (AU) for the marketing department and then assign User1 an appropriate role (for example, User Administrator) scoped to that AU.
Microsoft 365 groups, management groups, and resource groups serve different purposes:
* Microsoft 365 groups are for collaboration.
* Management groups organize Azure subscriptions.
* Resource groups group Azure resources.
Only administrative units in Entra ID provide delegated role-based administration for user subsets.

NEW QUESTION: 129
Contoso□□ Azure AD □□□□ □□□, □□□□ Terms1□□□ □□ □□(ToU)□ □□□ □□□□ □□□□ □□□□. Contoso □□□□ Fabrikam□□□ □□ □□□ □□□□□. Fabrikam □□□□ □□□ □□□□ □□□□□ Terms1□ □□□□ □□□.
□□ □□□□ □□1□ □□□□□, □□□□□ □□□□ □□□.
□□□ □□□□ □□□?
A. □□□□□ □□
B. □□ □ □□□ □□□
C. □□□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)
When users accept or decline a Terms of Use (ToU) in Azure AD, these actions are recorded in the audit logs.
The Microsoft Identity and Access Administrator documentation specifies that audit logs capture "Terms of use acceptance records" including who accepted, who declined, timestamp, and version of the ToU accepted.
The other options are incorrect because:
* Provisioning logs capture provisioning events (not ToU).
* Usage and Insights reports provide activity metrics, not compliance actions.
* Sign-in logs capture authentication activity but not ToU acceptance.
Therefore, to identify which users accepted or declined Terms1, you should use the Audit logs in Azure AD.

NEW QUESTION: 130
□□ 9
Sg-Operations □□□ □□□□ My Apps □□□ □□□□ □□ □□□□□□□ □□□ Operations□□ □□ □□□□□ □□□□ □□□.
* □□□
* □□
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To ensure that users in the Sg-Operations group see a tab named "Operations" containing only LinkedIn and Box applications in the My Apps portal, you can create a collection with these specific applications.
Here's how to do it:
Sign in to the Microsoft Entra admin center:
Make sure you have one of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.

Navigate to App launchers:
Go to Identity > Applications > Enterprise applications.
Under Manage, select App launchers.
Create a new collection:
Click on New collection.
Enter "Operations" as the Name for the collection.
Provide a Description if necessary.
Add applications to the collection:
Select the Applications tab within the new collection.
Click on + Add application.
Search for and select LinkedIn and Box applications.
Click Add to include them in the collection.
Assign the collection to the Sg-Operations group:
Select the Users and groups tab.
Click on + Add users and groups.
Search for and select the Sg-Operations group.
Click Select to assign the collection to the group.
Review and create the collection:
Select Review + Create to check the configuration.
If everything is correct, click Create to finalize the collection.
By following these steps, when users in the Sg-Operations group visit the My Apps portal, they will see a new tab named "Operations" that contains only the LinkedIn and Box applications1.
Please note that to create collections on the My Apps portal, you need a Microsoft Entra ID P1 or P2 license1.

NEW QUESTION: 131
contoso.com□ SMTP □□ □□□ □□□□ Microsoft Exchange □□□ □□□□.
□□ □□□□ contoso.com □□□ □□□ □□□□ Azure Active Directory(Azure AD)□ □□ □□□□ □□□□□.
□□ □□□ □□□□ □□□ Azure AD □□□□ □□ □□□ □□□ □□□ □□□□.
Microsoft 365 □□□□ □□ □□□□ □□□□□ □□□□ contoso.com Azure AD □□□□□ □□□ □□□ □□□ □□ □□□□ □□□.
□□ PowerShell cmdlet□ □□□□ □□□?
A. Set-MsolCompanySettings
B. Set-MsolDomainFederationSettings
C. □□□□-MsolfederatedDomain
D. Set-MsolDomain
Answer: (SHOW ANSWER)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn content under "Manage Azure AD tenants and configure tenant properties", self-service sign-up (also known as viral sign-up) allows users to create accounts in an existing Azure AD tenant using an email domain associated with that tenant. This feature lets external or ungoverned users create identities if it is not explicitly disabled, which can cause unauthorized account creation in the organization's namespace.
To stop users from performing self-service sign-ups using the organization's verified domain (e.g., contoso.
com), administrators must disable the AllowEmailVerifiedUsers setting in Azure Active Directory using PowerShell. This configuration change prevents users from automatically creating accounts with the organization's domain when registering for Microsoft 365 or other Azure services.
The cmdlet used to configure tenant-level settings like this is Set-MsolCompanySettings from the MSOnline module.

The specific PowerShell command would be:
Set-MsolCompanySettings -AllowEmailVerifiedUsers $false
This command disables self-service sign-up for email-verified users, ensuring that only administrators can create accounts in the tenant.
Other cmdlets in the options serve different purposes:
* Set-MsolDomainFederationSettings - Used for configuring federation settings for a domain.
* Update-MsolFederatedDomain - Used to update or repair federation trust settings.
* Set-MsolDomain - Used to configure domain-specific properties (e.g., authentication type).
As per Microsoft's official documentation:
"To prevent users from self-service sign-up using your organization's verified domain, set AllowEmailVerifiedUsers to $false using Set-MsolCompanySettings."

NEW QUESTION: 132
Azure □□□ □□□□. □ □□□□ Windows Server□ □□□□ □□ □□ 50□□ □□□□ □□□□.
□□ □□□ □□ Microsoft Entra □□□□ □□□□□□.
□□□□□ Microsoft Entra □□ □□□ □□□□ □□ □□□ □□□□ □ □□□ □□□□□.
□□□□ □□ □□□ □□□□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□ □□□ https://enterpriseregistration.windows.net□ □□□□ □ □□□ □□□□□.
B. □□ □□ □□ □□□ □□□□□.
C. Microsoft Entra □□ □□□□ □□ □□□ □□ □□□ □□□□□.
D. OpenSSH□ □□ SSH □□□□□ □□□ □□□□□□.
Answer: (SHOW ANSWER)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation on "Enable Microsoft Entra login for Windows Server and Windows virtual machines in Azure", successful sign-in to Azure VMs using Microsoft Entra (formerly Azure AD) credentials requires network connectivity to specific Microsoft identity endpoints. One of the most critical endpoints is https://enterpriseregistration.windows.net , which is used during the device registration and Microsoft Entra Join process.
When you enable Microsoft Entra login for Azure VMs, each VM must register itself as a device in the directory to allow authentication using Entra credentials. If the VM cannot reach the enterprise registration service, the registration fails, meaning the VM will not appear as a valid device in Entra ID. Consequently, users attempting to log in with their Entra credentials will encounter sign-in errors because the system cannot validate their device trust and user token against the identity service.
Microsoft documentation explicitly states:
"To enable Microsoft Entra sign-in to Windows VMs in Azure, the VM must be able to communicate with Microsoft Entra endpoints, including https://enterpriseregistration.windows.net , to complete device registration." Options B, C, and D are unrelated to initial configuration issues. Revoking refresh tokens or deleting device registrations would not resolve connectivity or registration failures. SSH support (option D) is applicable to Linux VMs, not Windows.

NEW QUESTION: 133
Microsoft 365 □□□□ □□□□.
□□ □□□□ Windows 10□ □□□□ □□□□ □□□ □□□□. □□□□ □□□□ □□ □□□□ Azure Active Directory(Azure AD)□ □□□□ □□□□. □□ □□□□ □□□ □□□□ Azure AD□□ □□ □□ □□□□.
□□□ □□ □□□□□ Microsoft SharePoint Online□ □□□□ □□□□ □□□ □□□□□□□ □□□□□ □□ □□□□ □□□. □□ □□□□ □□□□□□ □ □□□.
□□ □□□ □□□ □□□□ □□□?
A. Microsoft Office 365 □□□□ □□□ □□□ Microsoft Cloud App Security □□ □□
B. □□ □□□ □□□ Azure AD □□□ □□□ □□
C. □□□□□ □ □□□ □□□ Azure AD □□□ □□□ □□

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

Answer: B (LEAVE A REPLY)

SC-300 teaches using Conditional Access session controls with SharePoint and OneDrive to protect data on unmanaged devices. The documentation states: "Session controls allow limiting the experience within cloud apps, including Use app enforced restrictions to apply SharePoint Online policies like block download on unmanaged devices." It defines unmanaged as devices that are "not compliant or not hybrid Azure AD joined." The scenario requires blocking download/sync only for user-owned (registered) devices, while allowing access for company-owned (joined/compliant) devices-precisely what session controls achieve.

Activity or app-discovery policies in Microsoft Defender for Cloud Apps (MCAS) are not required here, and client apps conditions target protocol types rather than shaping in-app actions. Therefore, create a Conditional Access policy targeting SharePoint Online, scope to devices that are not compliant or not hybrid joined, and set Session # Use app enforced restrictions (or Sign-in frequency + Conditional Access App Control) to block download, satisfying the SC-300 guidance for selective data exfiltration protection.

NEW QUESTION: 134

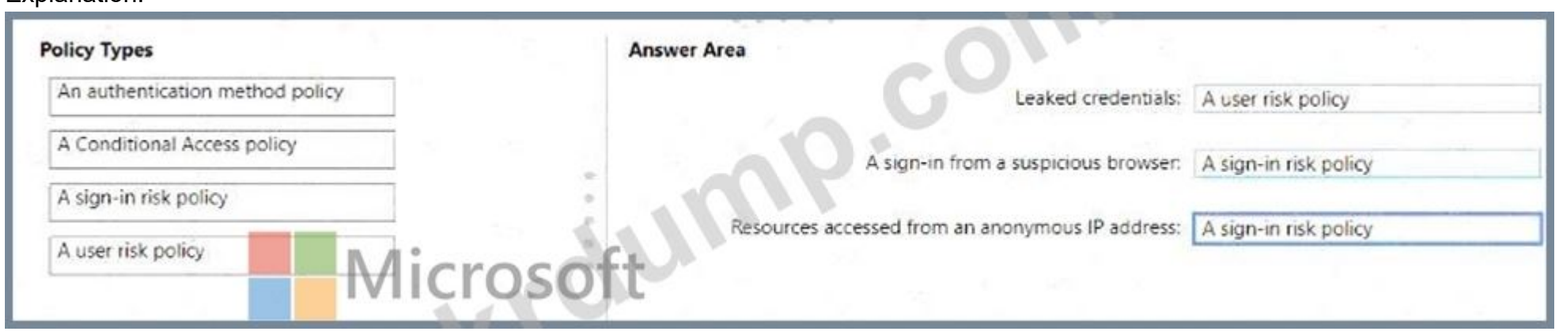
□□□ □□ □□ □□□ □□□□ □□□.

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

□□: □□ □□□ 1□□□□.

Answer:

Explanation:



According to the Microsoft SC-300: Identity and Access Administrator official study guide and the Microsoft Learn "Implement and manage Azure AD Identity Protection" module, Azure AD Identity Protection detects two primary categories of risks: user risks and sign-in risks.
* User Risk Policy: A user risk represents the probability that a user ' s identity (credentials) has been compromised. Examples of user risk signals include leaked credentials , unusual sign-ins from different geographies , or sign-ins from infected devices . The Exam Ref SC-300 specifically lists "leaked credentials detected on the dark web or other compromised repositories" as the main trigger for a user risk policy. Such a policy can automatically force password change or enforce MFA to remediate the threat.
* Sign-in Risk Policy: A sign-in risk reflects the likelihood that a specific authentication attempt is not performed by the legitimate user. Sign-in risk is based on context, such as sign-ins from suspicious browsers , anonymous IP addresses (like TOR networks) , or impossible travel sce narios . The SC-300 documentation highlights these examples as conditions best handled with a sign-in risk policy, where conditional access can block or require MFA for the risky sign-in attempt.
Therefore:
* Leaked credentials are addressed through a User Risk Policy, since the account itself is compromised.
* Sign-ins from suspicious browsers and access from anonymous IP addresses are handled through Sign- in Risk Policies, as they relate to risky sessions rather than compromised identities.

NEW QUESTION: 135
□□□ Site1□□□ □□□ Microsoft SharePoint Online □□□□ □□□ Microsoft 365 E5 □□□ □□□□ □□□□.
Site1□ PDF □□□ □□□□□□.
Sitel□□ □□□□ □□□ □□ □□□□ □□□□ □□ □□□.
Microsoft Defender for Cloud Apps □□□□ □□ □□□ □□□ □□□□ □□□?
A. □□ □□
B. □□ □□
C. □□ □□
D. □□ □□
Answer: D (LEAVE A REPLY)
In Microsoft Defender for Cloud Apps (MCAS), a Session policy is used to monitor and control user activities in real time when accessing cloud resources through Conditional Access App Control.
The requirement states:
"Prevent users from printing PDF files directly from SharePoint Online." This requires controlling a user's session behavior (e.g., download, print, copy) within a web session - not just detecting or auditing it afterward. According to Microsoft's Identity and Access Administrator training materials:
"Session policies enable real-time monitoring and control of user sessions, allowing you to restrict activities such as printing, downloading, or copying content." By configuring a session policy, administrators can apply real-time controls to prevent printing within SharePoint or Teams sessions while allowing normal view access.
Other options:
* File policy controls data at rest (e.g., classifying or sharing files).
* Activity policy detects historical actions.
* Access policy controls conditions for app access, not user actions.

NEW QUESTION: 136
□□ □□ □□□ □□□ □□ □□□ □□□□□ □-□□□□ □□□□□□ □ SharePoint Online □□□ □□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□□□: □□□ □□□ □□□ 1□□ □□□□□.

For on-premises applications:

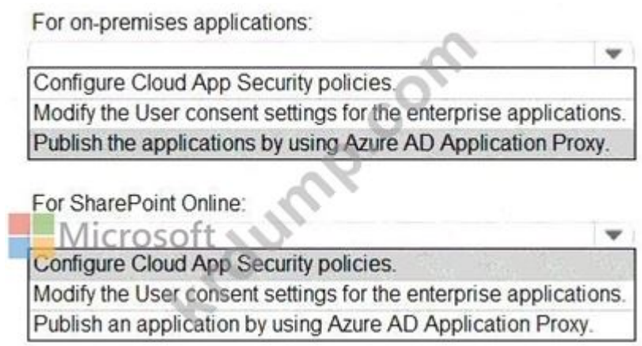
Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

Configure Cloud App Security policies.
Modify the User consent settings for the enterprise applications.
Publish an application by using Azure AD Application Proxy.

Answer:

Explanation:

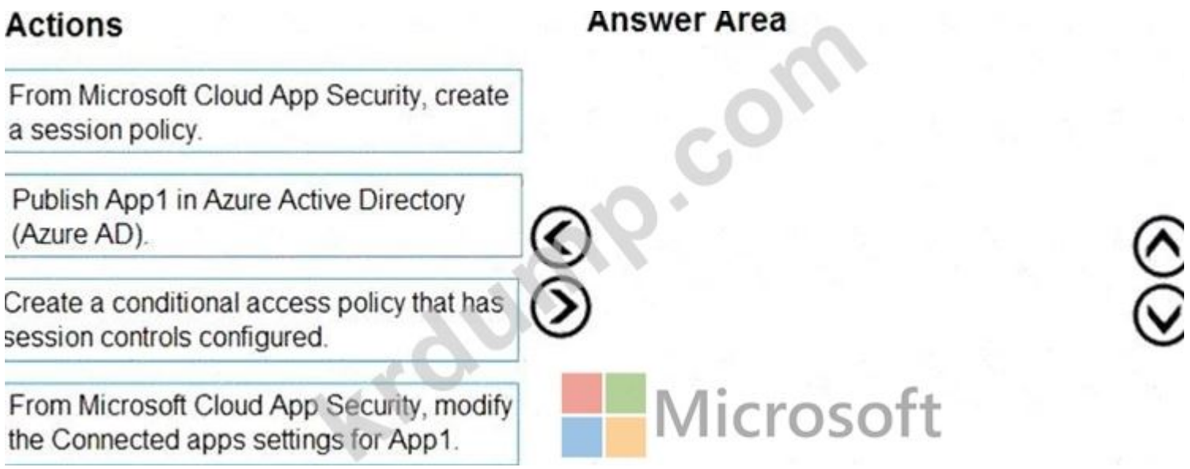


SC-300 materials stress that to enforce modern controls (like MFA) on on-premises apps, you must front them with Azure AD so Conditional Access can evaluate sign-ins. The documentation states that Azure AD Application Proxy " provides secure remote access to on-premises applications " and that apps published through it can have " Conditional Access policies, including multifactor authentication " applied at sign- in. In other words, once the legacy app is published by Application Proxy, Azure AD sits in the path, enabling you to meet the requirement to enforce MFA when accessing on-premises applications and to combine it with your location-based exemptions.

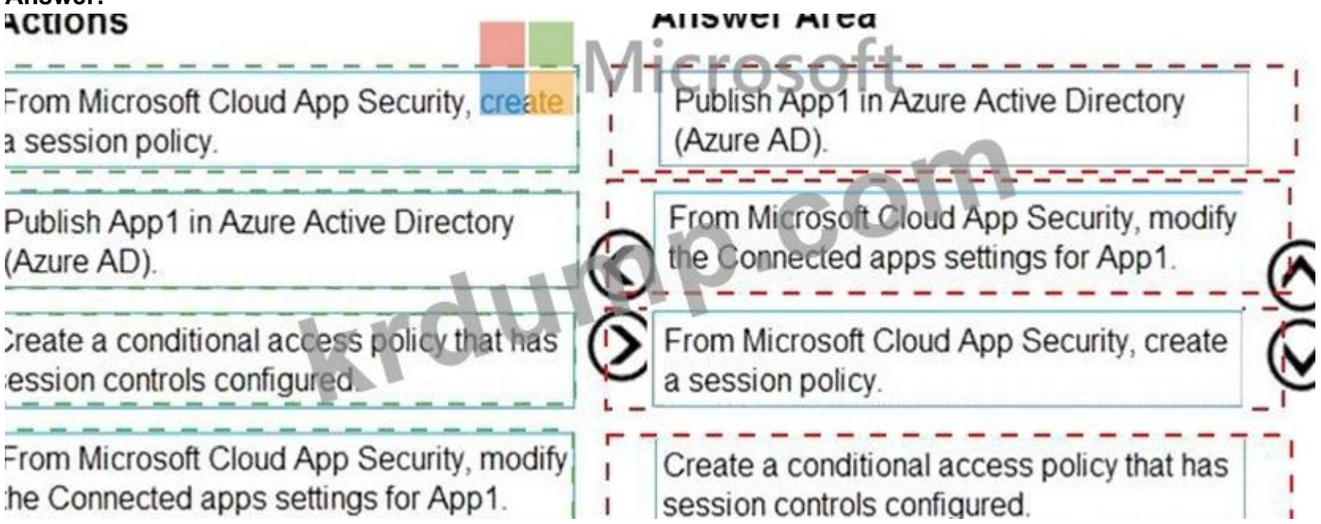
For SharePoint Online restrictions, SC-300 points to Microsoft Cloud App Security (Defender for Cloud Apps) for real-time governance: you can create session policies that " control and limit activities in real time " and, for SharePoint Online and other Microsoft 365 apps, " monitor user sessions and block download, cut, copy, and print " when conditions (device state, risk, or location) warrant it. Since the scenario already has anomaly detections enabled, configuring Cloud App Security policies aligns directly with the requirement to place access restrictions on SharePoint Online without altering tenant-wide consent settings. Thus, publish on-prem apps with Application Proxy to bring them under Conditional Access (for MFA), and use Cloud App Security policies to enforce SharePoint Online session and download controls.

NEW QUESTION: 137
□□□ □□ Azure Active Directory(Azure AD) Privileged Identity Management(PIM)□ □□□□□.
PIM□ □□□ □□□□ □□ □□ IT □□□ □□□ 15□ □□□□ □□ □□ □□□ □□□ □□□ □□ □□ □□□□□.
IT □□ □□□□ □□□ □□ □□ □□□ □□□ □□□□ □ □□□ □□ □□□.
□□ □□□ □□ □□□ □□ □□□ □□□□ □□□?
A. □□ □□ □□ □□□□ □□□ □□□ □□□□□.
B. □□ □□ □□ □□□□ □□ □□ □□
C. □□□ □□ □□ □□
D. □□□□□ □□ □□
Answer: D (LEAVE A REPLY)
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and the Microsoft Learn module "Configure Azure AD Privileged Identity Management (PIM)", Azure AD PIM provides two types of role assignments: Active and Eligible.
An Active assignment means the user permanently holds the role with immediate access. An Eligible assignment means the user can activate the role only when needed, after providing justification or approval. This follows the least privilege principle by reducing exposure to high-privilege roles.
The official documentation states:
"Users assigned as eligible must activate their role when they need to perform privileged tasks. This ensures that administrative privileges are granted only for a limited time and when necessary." Because all IT users currently have permanent Security Administrator roles, the correct remediation is to change their assignment type from Active to Eligible so they can activate it only when required. Options A and B relate to expiration settings but do not convert the assignment type.

NEW QUESTION: 138
Microsoft 365 E5 □□□□ □□□□.
App1□□□ □□□□ □□ □□□□□.
Microsoft Cloud App Security□ □□□□ App1□ □□□ □□ □□ □□□□□ □□□□□ □□□.
□□ □ □□ □□□ □□□□ □□□□ □□□? □□□□ □□ □□□□ □□ □□□ □□ □□□□ □□ □□□ □□□□ □□□□□.



Answer:



Explanation:

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and official Microsoft Defender for Cloud Apps documentation (formerly Microsoft Cloud App Security, or MCAS), enabling real-time session-level monitoring-known as session control-requires a structured integration between Azure AD Conditional Access and Microsoft Cloud App Security (MCAS).

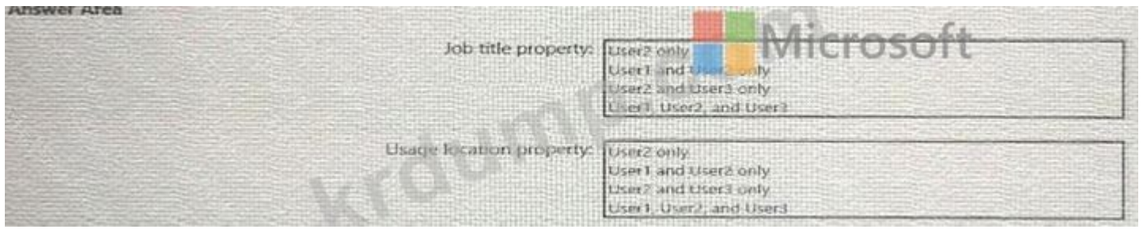
Here's the correct sequence and rationale:

* Publish App1 in Azure ADThe app must first be registered or published in Azure Active Directory so that it can participate in Conditional Access and App Control integration. Without Azure AD integration, Cloud App Security cannot monitor or enforce policies on the app's traffic.
* Create a Conditional Access Policy with Session ControlsIn Azure AD Conditional Access, you define the conditions (users, apps, risk levels) and set Session controls # Use Conditional Access App Control (Monitor only / Block download). This links Azure AD sign-in events to MCAS for real-time monitoring.
* Modify the Connected Apps Settings in Cloud App SecurityIn Microsoft Cloud App Security, navigate to Connected apps > Conditional Access App Control apps and ensure that App1 is connected. This ensures traffic from Azure AD sign-ins can be intercepted for session-level monitoring.
* Create a Session Policy in Cloud App SecurityFinally, you configure a Session Policy (e.g., monitor file downloads, block uploads, restrict copy/paste, etc.) within Cloud App Security. The session policy enforces the desired controls and visibility in real time when users interact with App1.
This order aligns with Microsoft Learn guidance:
"To monitor user sessions in real time, integrate the app with Azure AD Conditional Access, configure session control, connect the app in Microsoft Cloud App Security, and create session policies."
Final Order:
* Publish App1 in Azure AD
* Create a Conditional Access policy with session controls
* Modify Connected apps settings for App1 in Cloud App Security
* Create a Session policy in Cloud App Security

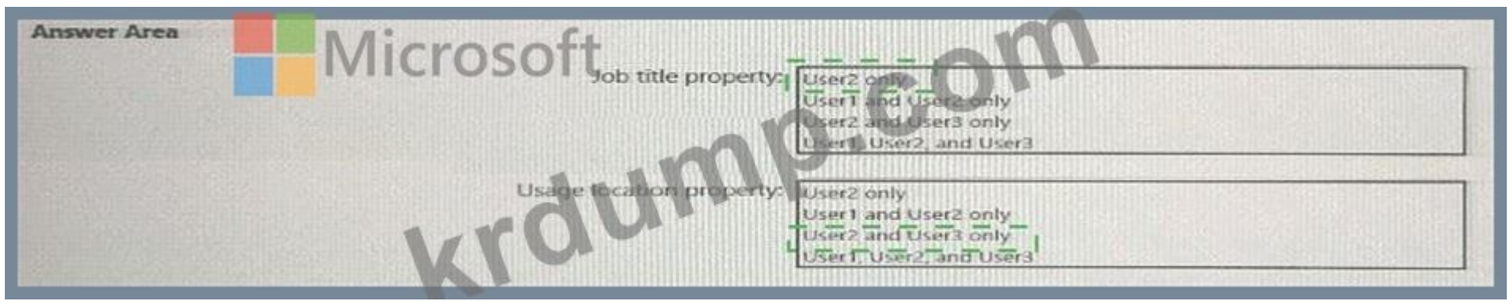
NEW QUESTION: 139
□□ □□ □□□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

Azure AD□□ □□ □□□□ □□ □□ □□□ □□ □□ □□□ □□□ □ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:



Explanation:
< Job title property: # User2 only
Usage location property: # User2 and User3 only

According to the Microsoft SC-300: Microsoft Identity and Access Administrator Study Guide and Micro soft Learn documentation on Azure Active Directory user management, the ability to modify user attributes such as Job title and Usage location depends on whether the user is:
* Directory-synced (from on-premises Active Directory), or
* Cloud-only (created directly in Azure AD), or
* Guest (external B2B user)
Here's the explanation for each scenario based on the user table provided:
Name
Type
Directory Synced
User1
Member
Yes
User2
Member
No
User3
Guest
No
* The Job title attribute is read-only for users synchronized from on-premises Active Directory. For directory-synced users like User1, the attribute must be managed in on-premises AD and synchronized via Azure AD Connect.
* For cloud-only users (like User2) and guest users (like User3), the attribute can be modified in Azure AD. However, Microsoft restricts certain profile fields, including Job title, for guest users unless they are given specific permissions.
# Job title property # Therefore, only User2 (a cloud-only member) can have the Job title property configured directly in Azure AD.
* The Usage location property determines licensing restrictions (for example, Microsoft 365 services available by country).
* This property is editable for cloud-only users (User2) and guest users (User3).
* For directory-synced users (User1), the value is controlled from on-premises AD, and cannot be modified in Azure AD.
# Usage location property # Therefore, User2 and User3 can have the Usage location property configured in Azure AD.
* Job title property: User2 only
* Usage location property: User2 and User3 only
# Final Answers:
Reference (Microsoft Official Documentation Extracts):
"For synchronized users, attribute values such as Job title and Department are managed in the on-premises Active Directory and cannot be edited in Azure AD."
"Usage location must be specified in Azure AD for cloud-only and guest users to assign licenses correctly."

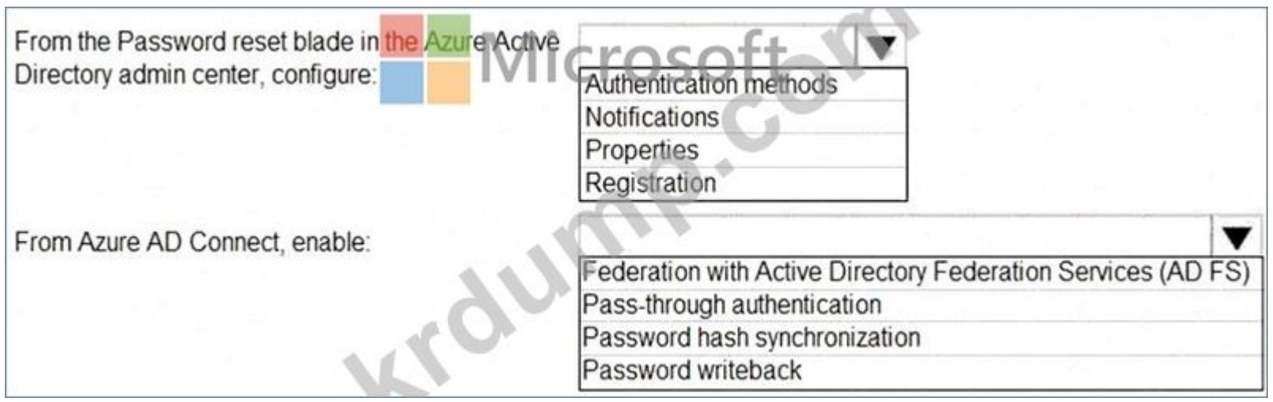
NEW QUESTION: 140
db1□□□ Azure SQL □□□□□□□ □□□ Azure □□□ □□□□.
App1□ □□□□ □□□□ □□□□□ □□ □□□ □□□□ App1□□□ Azure App Service □□□ □□□□□.
App1□ db1□ □□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□ □□□ App1□□□ □□□ □ □□□ □□□.
* □□□ □□□ □□□□□ □□□.
□□ □□□ □□□□ □□□□ □□□?

A. □□□□ □□□ □□ ID
B. Azure AD □□□ □□
C. SQL Server □□
D. □□□□□ □□□ □□ ID
Answer: D (LEAVE A REPLY)
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation on Managed Identities for Azure Resources , the recommended and most secure method for an Azure resource (like an App Service) to access another Azure resource (such as an Azure SQL Database) is through Managed Identities.
Managed identities allow Azure services to authenticate securely to other Azure services that support Azure AD authentication, without requiring the use of credentials stored in code, configuration files, or key vaults.
There are two types of managed identities:
* System-assigned managed identity
* Created and tied directly to the lifecycle of a specific Azure resource (e.g., App Service).
* When the resource (App1) is deleted, the identity is automatically deleted as well.
* Best suited when a single resource requires authentication to access another Azure service.
* User-assigned managed identity
* Created as an independent Azure resource.
* Can be assigned to multiple services and managed separately.
* Useful for scenarios requiring shared identity or cross-service authentication management.
* App1 (Azure App Service) must access db1 (Azure SQL Database).
* Credentials should be available only to App1, meaning other resources should not share or reuse the identity.
* Administrative effort should be minimized, implying automatic management of credentials and lifecycle.
Scenario Analysis: Hence, a system-assigned managed identity is the best solution because it meets all three conditions:
* No manual credential management (Azure handles authentication token issuance automatically).
* The identity exists only for App1 (it's unique to that resource).
* Simplified lifecycle - identity is created and deleted automatically with App1.
# Official Microsoft Documentation (aligned with SC-300 exam objectives):
"System-assigned managed identities are ideal for scenarios where a single Azure resource requires access to another Azure service and you want Azure to automatically manage the identity's lifecycle."
"Managed identities eliminate the need for developers to manage credentials in code or configuration files."

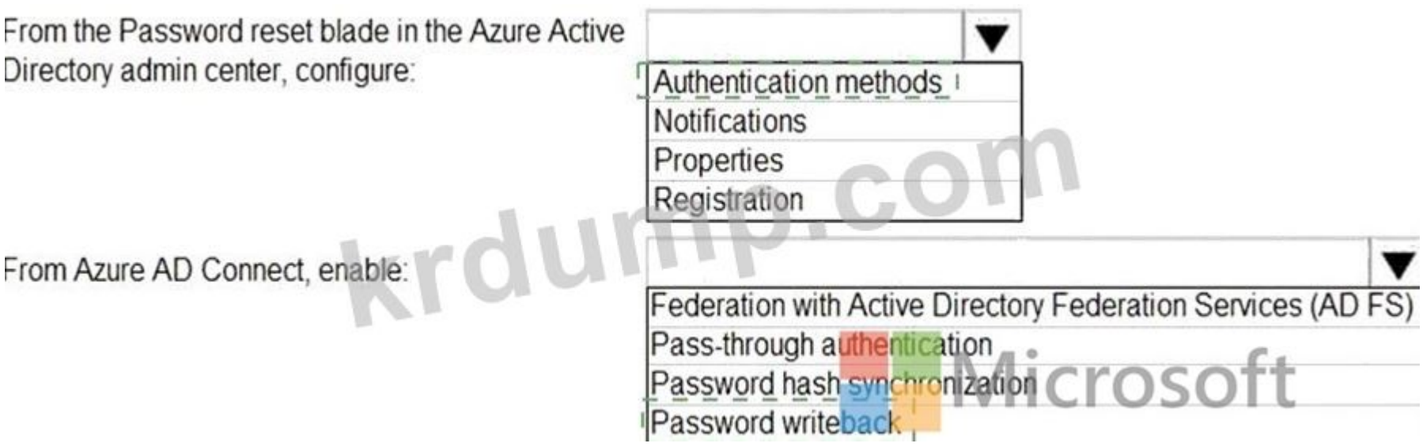
NEW QUESTION: 141
Identity Governance□ □□□□ □□□□□□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. □□□□□□ □□□□□□□ □□ □□□ □□ □□□ □□□□□.
B. □□□□□ □□□□.
C. □□□□□ □□□□.
D. □□□□□□ □□□□□□□ □□ □□□ □□ □□ □□□ □□□□□.
Answer: (SHOW ANSWER)
In Azure AD Identity Governance, application access granted through Entitlement management is organized around catalogs and access packages. The SC-300 study materials explain that "a catalog is a container for resources and access packages" and that you must add your enterprise applications (or the groups tied to those apps) to a catalog before you can build access packages that users can request. Creating the catalog first enables you to place only the required resources in scope and to delegate day-to-day ownership: "catalog owners can manage the resources and access packages within their catalog without being tenant-wide admins," satisfying the delegation requirement to use custom catalogs and least privilege. After the catalog exists, you create one or more access packages that include the

application (or groups) and policies that control who can request, how they are approved, and for how long. Identity Governance then lets you track access package assignments and review who has the app over time. By contrast, programs are used to group and report on governance initiatives (for example, collections of access reviews) rather than to onboard application resources; and modifying user/admin consent settings affects app consent behavior, not the lifecycle tracking of assignments. Therefore, the correct first step to track application access assignments while meeting the delegation requirements is to create a catalog.

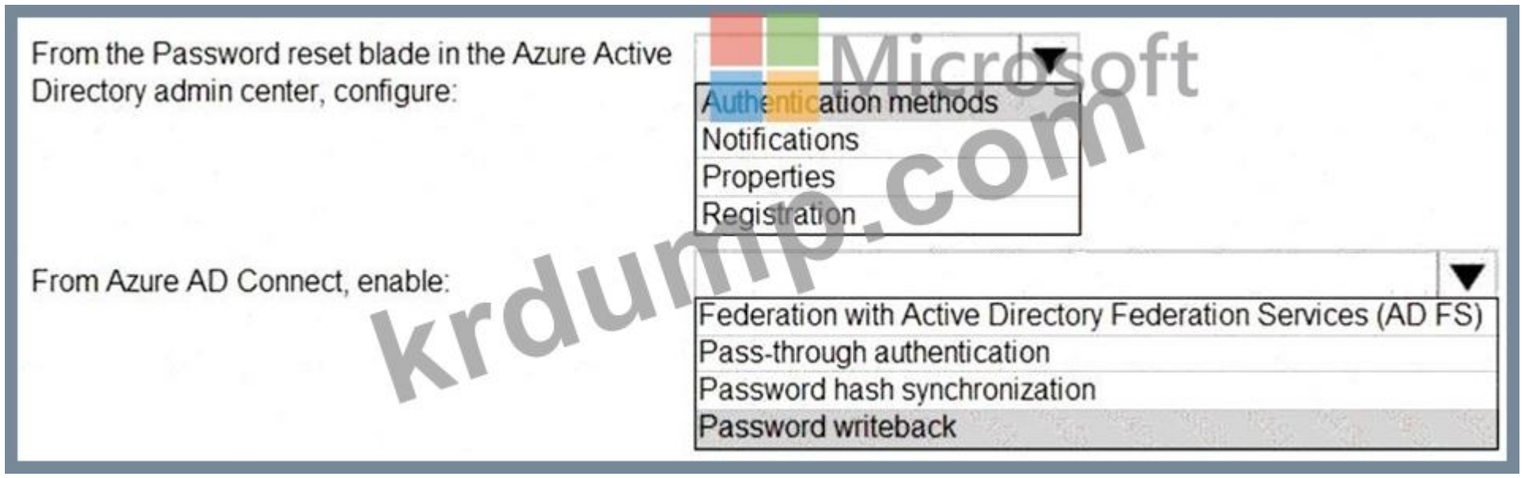
NEW QUESTION: 142
Microsoft 365 □□□□ adatum.com□□□ Active Directory □□□□ □□□□.
Azure AD Connect□ Express □□□ □□□□ □□□□□.
□□ □□ □□□ □□□□□ □□ □□□ □□□□ □□□(SSPR)□ □□□□ □□□.
□□□□ □□□□□ □□□□ □ □□□ □ □□□ □□□□□ □□ □□□ □□ □□ 3□□ □□□□ □□□□ □□□□□.
□□□□□ □□□□ □□□ □□□□ □□□□ □□□ □□ □□□□□ □□□□□ □□□.
□□□ □□ □□□? □□□□□ □□ □□□□ □□□ □□□□ □□□□□.
□□□□: □□□ □□□ □□□ 1□□ □□□□□.



Answer:



Explanation:



According to the official Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn documentation on "Implement and manage self-service password reset (SSPR)", configuration of SSPR requires settings in both Azure AD and Azure AD Connect.

* Azure AD Configuration (Password reset blade):In the Azure AD admin center, the Password reset blade includes three primary sections: Properties, Authentication methods, and Registration.
* The Authentication methods section determines which verification methods users can use when resetting their password.
* To meet the requirement that users must respond to a mobile app notification or answer three security questions, you must configure these under Authentication methods.Microsoft documentation explicitly states:

"In the Authentication methods section of the Password reset settings, choose which methods users can use, such as mobile app notification, email, or security questions."

* Azure AD Connect Configuration:When users reset their password in Azure AD or on-premises, synchronization must occur both ways to ensure passwords remain consistent.
* Enabling Password writeback in Azure AD Connect allows password changes made in Azure AD (such as through SSPR) to be written back to the on-premises Active Directory.The study guide confirms: "Password writeback enables users who change or reset their password in Azure AD to have that new password written back to their on-premises Active Directory." Therefore, to meet both requirements - user verification via mobile app or security questions and password synchronization between cloud and on-premises - the correct configuration is:
* From the Password reset blade: Authentication methods
* From Azure AD Connect: Password writeback

NEW QUESTION: 143

□□ □□ □□□ □□□ □□□ 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: (SHOW ANSWER)

The SC-300 official study guide and Microsoft Learn: Manage Access Reviews confirm that Access Reviews in Azure AD can target user-based groups, Azure AD roles, and enterprise applications. However, dynamic device groups are not supported for access reviews.

NEW QUESTION: 144
Microsoft Entra □□□□ □□□□.
□□□ □□ □□ 10□□ □□□□ □□□ □□ □□□ □□□□ □□□. Microsoft Entra □□ □□□□ □□□ □□□□ □□□?
A. □□□ □□ □□
B. □□ □□
C. □□ □□
D. □□□ □□ □□
Answer: (SHOW ANSWER)
According to the Microsoft SC-300 Study Guide and Microsoft Learn module: "Implement and manage smart lockout and password protection" , Smart Lockout is a feature of Microsoft Entra Password Protection that helps prevent brute-force attacks by locking out accounts after repeated failed sign-in attempts.
The configuration for Smart Lockout includes two primary settings:
* Lockout threshold - the number of failed sign-ins before locking the account.
* Lockout duration - how long the account remains locked before another attempt is allowed.
These settings are managed under Password protection in the Entra admin center, not under user or sign-in risk policies (those are part of Identity Protection) or authentication strengths.
By configuring the lockout threshold to 10 failed sign-ins, you meet the requirement.

NEW QUESTION: 145
□□ □□ □□ □□ □□□□ □□□ Azure □□□ □□□□.

Name	Type
VM1	Virtual machine
App1	Azure App Service
Vault1	Azure Key Vault
storage1	Storage account

□□ □□ □□□ □□(ABAC)□ □□□□ □□□□ □□ □□□ □□□□ □□□.
□□ □□□□ □□□ □□□ □ □□□?
A. Vault1
B. VM1
C. App1
D. storage 1
Answer: D (LEAVE A REPLY)
According to Microsoft Learn: "Configure Attribute-Based Access Control (ABAC) for Azure resources", ABAC allows you to assign access permissions based on resource attributes and user attributes (claims). Currently, ABAC is available for Azure Storage (Blob and Queue) and Azure Key Vault (limited preview for specific scenarios). However, the generally available and supported ABAC implementation as per SC-300 and Azure documentation is for Azure Storage accounts.
This means that you can use ABAC in storage1 to grant fine-grained access (for example, based on object tags or user department claims) while resources like VM1, App1, and Vault1 still rely on traditional RBAC (role-based access control).

NEW QUESTION: 146
□□□ □□□ □□□ □□ □□□ □□ □□□ □□□□ □□□.

□□□ □□ □□□?
A. □□ □□□ □□□□□.
B. □□ □□ □□
C. □□□ □□□ □□□□□.
D. □□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
In Azure AD Privileged Identity Management (PIM) for Azure AD roles, the exam materials describe that you tailor how a role (for example, User administrator) is used by editing its Role settings. These settings control activation behavior, including require multi-factor authentication, justification, approval, assignment
/activation durations, and notifications. The guide states that administrators can "configure activation requirements and time-bound eligibility on a per-role basis" and "enforce approval workflows and MFA at activation." Access reviews are used to periodically verify who still needs a role, but they do not implement the operational changes to how the role is activated. Active assignments simply shows and changes who currently holds active/eligible assignments; it does not set policy for the role's activation behavior.
Administrative units scope certain directory tasks, but they are not how you change PIM activation/approval
/MFA requirements. Therefore, to meet planned changes for the User administrator role (such as least privilege activation with approval, justification, and MFA), you update PIM # Azure AD roles # User administrator # Role settings. This aligns with the SC-300 objective to "configure PIM settings and policies for Azure AD roles," ensuring governance by policy rather than ad-hoc assignment.

NEW QUESTION: 147
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□ □□□□ □□□ □□□ □□□□□□ Facebook□ □□□□□ □□□□ □□□. □□□□ □□ □□□ □□□□□ □□□.
□□ □□ □□□ □□ □□□?
A. Microsoft Defender for Cloud Apps □□□□ □□□□ □□ Facebook.
B. Microsoft Endpoint Manager□□ □ □□ □□□ □□□□.
C. □□□□ □ □□□ □□□ □□ Defender□ □□□□.
D. □□□ □□□ □□□ □□□□.
Answer: C (LEAVE A REPLY)
The question asks how to identify which users access Facebook from their devices and browsers using Microsoft Defender for Cloud Apps (MCAS), with minimal administrative effort.
Here's the breakdown:
* Objective: Identify users who access Facebook (a cloud app).
* Tool: Microsoft Defender for Cloud Apps.
* Requirement: Visibility, not control - i.e., detect and report.
To achieve this, the appropriate first step is to create an Access Policy in Defender for Cloud Apps.
An Access Policy allows you to monitor and control real-time session access to cloud apps based on user, device, location, and app usage. It can:
* Detect when a user signs into or uses specific apps (like Facebook).
* Log and alert administrators automatically.
* Require no endpoint or Conditional Access configuration - satisfying the "minimize administrative effort" requirement.
From Microsoft Defender for Cloud Apps documentation:
"Access policies enable monitoring of app access patterns and can trigger alerts when users sign in to or access specific sanctioned or unsanctioned cloud applications." Other options explained:
* (A) Unsanctioning Facebook marks it as disallowed, but does not identify users accessing it.
* (B) App configuration policies in Intune control mobile device settings, not cloud app access.
* (D) Conditional Access policies can block or require conditions for Facebook access but do not report who accessed it.

NEW QUESTION: 148

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

In Microsoft Defender for Cloud Apps, app connectors integrate third-party services (such as Google Workspace, AWS, and GitHub) with Microsoft 365 Defender to enable activity monitoring, OAuth app analysis, and governance actions.

According to the Defender for Cloud Apps Integration Guide and the SC-300 Study Guide (Identity Governance and Compliance) , connecting Google Workspace through the app connector allows the system to collect OAuth authentication data, login attempts, and pe rmissions granted by third-party apps that use OAuth 2.0 within that ecosystem.

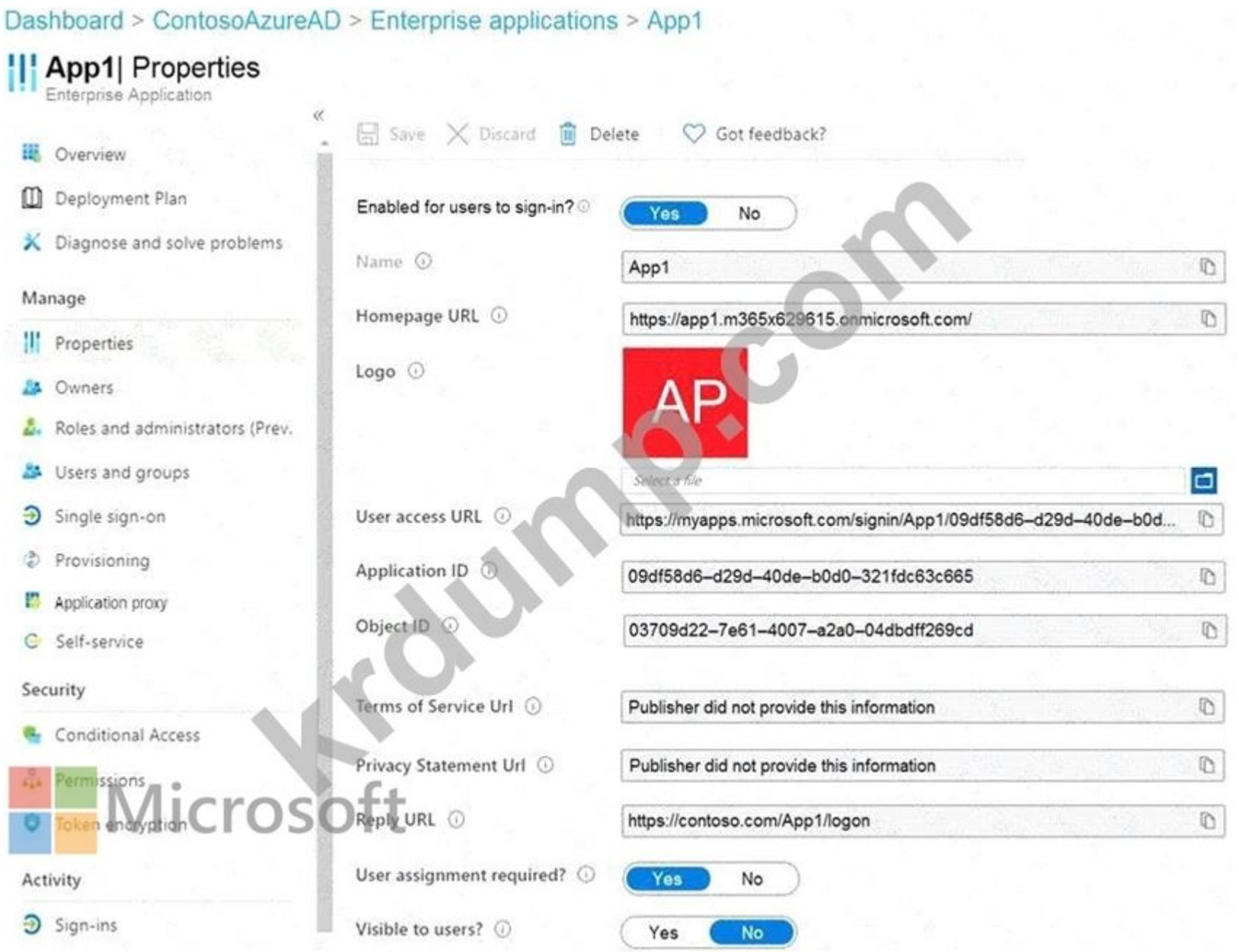
The documentation states:

"Defender for Cloud Apps integrates with connected apps such as Google Workspace, AWS, and others to detect suspicious OAuth applications and monitor app permission grants." Since the goal is to monitor OAuth authentication requests and Google Workspace is one of the connected sources , this solution meets the goal.

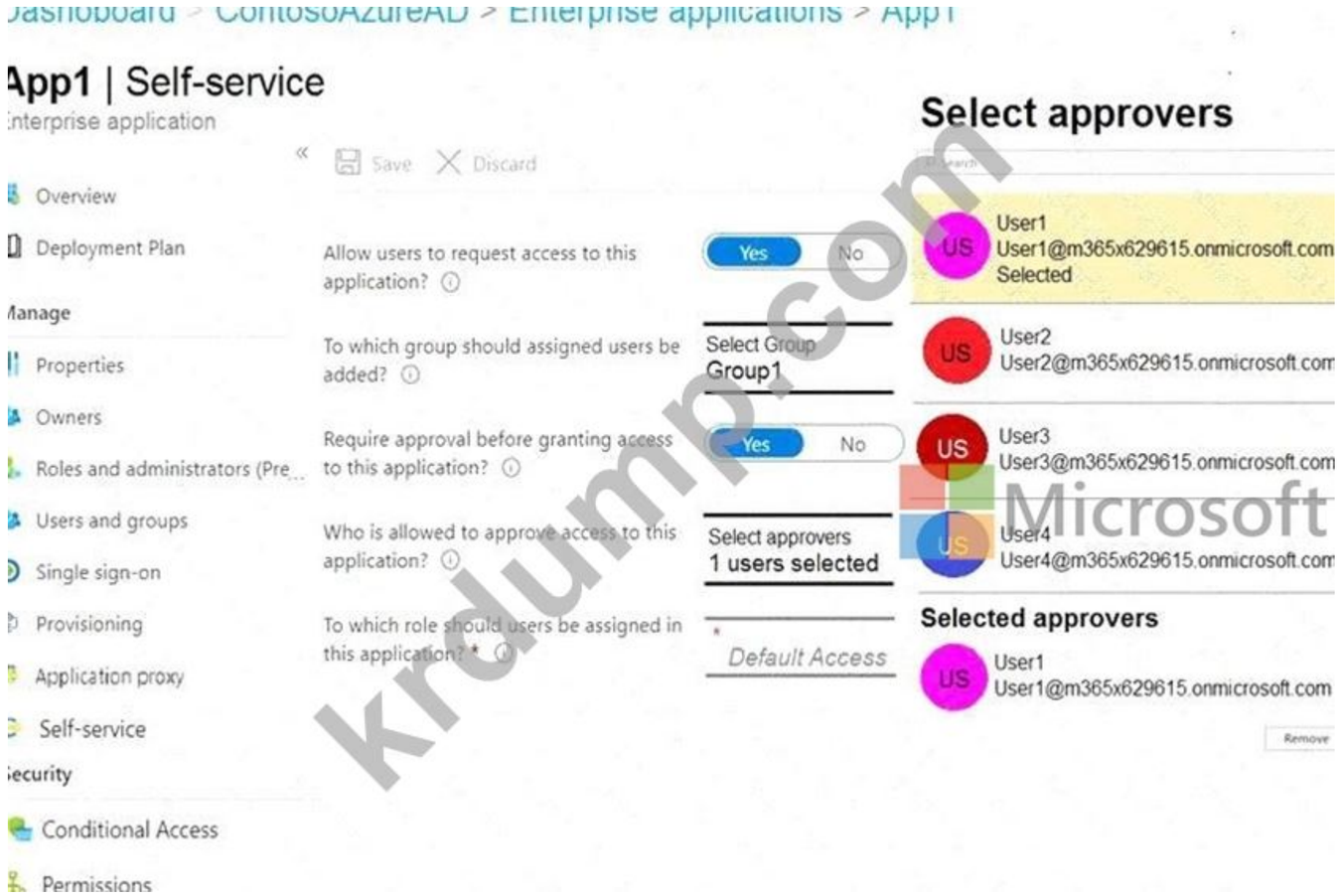
NEW QUESTION: 149

□□1 □□□ □□□ □□□ □□1□□□ □□□ □□□□ Microsoft 365 □□□□ □□□□. (□□1 □□ □□□□□.)

App1 □□ □□□ □□□ □□□ App1□□□ □□□ □□□□□□ □□□□□□□ □□□□. (App1 □□ □□ □□□□□.)



App1 □□ □□□ □□□ □□□ □□ App1□ □□ □□ □□□□ □□□□□. (App1 □□ □□□ □□ □□□□□.)



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

Answer Area

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:

No

No

Yes

a) When you assign a group to an application, only users in the group will have access. The assignment does not cascade to nested groups.

b) Tested in lab, existing owners will be replaced. Also direct assignment (resource owner) is path of least privilege. (replicated in test) c) Application setting ' visible to users ' is set to No, then no users see this application on their My Apps portal and O365 launcher.

Reference

According to the Microsoft SC-300: Identity and Access Administrator Study Guide, Azure AD Enterprise Application Self-service configuration determines how users can request access, who approves it, and whether access is automatically granted. Let's analyze each statement based on the exhibits:

* Members of Group3 can access App1 without approval from User1 - NO In the Group1 exhibit, Group1 contains User1, User4, and Group3 . In the App1 Self-Service exhibit, it shows that "Require approval before granting access" is set to Yes, and User1 is designated as the approver. Therefore, even though Group3 members might indirectly be part of Group1, access requests to App1 must still be approved by User1 before being granted.

* After configuring self-service, the owner of Group1 is User1 - NO The PowerShell command Get- AzureADGroupOwner clearly shows that Admin (not User1) is the owner of Group1. Configuring self- service for an application does not change group ownership; it only defines how access requests are handled. Ownership of Group1 remains with Admin.

* App1 appears in the Microsoft 365 app launcher of User4 - YES In the App1 Properties exhibit, the

"User assignment required" setting is set to Yes. This means only assigned users (directly or via groups) can see and access the application. Since Group1 is configured as the target group for user assignment and User4 is a member of Group1, User4 will see App1 in their Office 365 app launcher after assignment approval.

This logic follows Microsoft Learn documentation:

"When a user is assigned to an enterprise application (either directly or through group membership), the application appears in the user ' s Office 365 app launcher once access is granted."

NEW QUESTION: 150

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

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

□□□□□ □□ □□ □□□ □□□ □□□□.

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

□□ A□ □□ B□ □□ □□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□□□: □□□ □□□ □□□ 1□□ □□□□□.

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Answer:

GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Explanation:

< GroupA: # User1, Group1, Group2, and Group3 only

GroupB: # User1, Group1, Group2, and Group4 only

According to the Microsoft Identity and Access Administrator (SC-300) Official Study Guide and the Microsoft Learn module "Manage groups in Azure Active Directory", group nesting rules in Azure AD depend on group type and membership type.

* GroupA is a Security group with an Assigned membership type.
* In Azure AD, security groups (whether assigned, dynamic user, or dynamic device) can contain users, devices, and other security groups as members.
* However, Microsoft 365 groups cannot be added to a security group because Microsoft 365 groups include collaborative services (SharePoint, Teams, Planner) that rely on unique membership and ownership models.

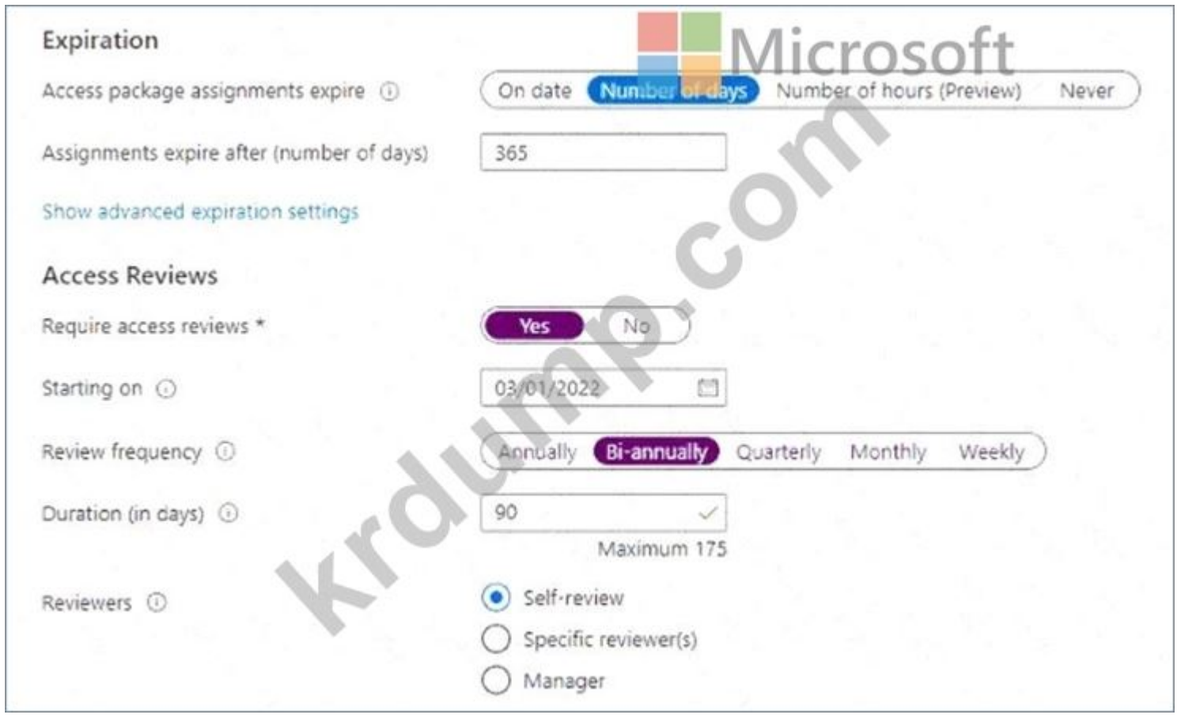
Therefore, GroupA (security group) can include:
* User1 (user) #
* Group1 (security - assigned) #
* Group2 (security - dynamic user) #
* Group3 (security - dynamic device) #
* # Group4 (Microsoft 365 group) - not allowed in a security group.
# Correct composition for GroupA: User1, Group1, Group2, and Group3 only.
* GroupB is a Microsoft 365 group with an Assigned membership type.
* Microsoft 365 groups can include users and security groups as members, but cannot include other Microsoft 365 groups (nested Microsoft 365 groups are not supported).
* So GroupB can include:
* User1 (user) #
* Group1 (security - assigned) #
* Group2 (security - dynamic user) #
* # Group3 (dynamic device) - device groups can't be members of M365 groups.
* Group4 (Microsoft 365 group) # - nesting M365 groups is not supported.
# Correct composition for GroupB: User1, Group1, Group2, and Group4 only.

NEW QUESTION: 151
Microsoft Entra □□□□ □□□□.
□□□□ □□ □□ □□□ □□ □□□ □□ □□□□□□.
□□□ □□□ □□□□□□□ □□ □□ □□□□□ □□□□ □□□. □□□ □□ □□□?
A. Microsoft Defender □□□□ Cloud Discovery □□ □□ □□□ □□□□.
B. Microsoft Entra □□ □□□□ □□□ □□ □□□ □□□□□.
C. Microsoft Defender □□□□ □ □□□□ □□□□□.
D. Microsoft Entra □□ □□□□ □□□ □□□ □□□□□.
Answer: B (LEAVE A REPLY)
When many new enterprise applications appear in a Microsoft Entra tenant, it typically means that users are granting consent for apps to access organizational data. To control this behavior, administrators can use the Admin consent workflow, found in Microsoft Entra ID # Enterprise applications # Consent and permissions # Admin consent settings.
Microsoft documentation explains:
"The admin consent workflow allows users to request access to applications that require admin consent, providing administrators with visibility and control over which apps get access to organizational data."
Enabling this workflow ensures that any new enterprise app requesting permissions beyond user-level consent must go through an approval process where an administrator can review and grant or deny access.
Options A and C refer to Defender for Cloud Apps, which detects and monitors discovered applications but does not enforce approval workflows. Option D (Access review) is used to periodically review user access, not app consent approval.

NEW QUESTION: 152
Microsoft 365 □□□□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□ □ □□ □□ □□(MFA)□ □□ Microsoft Authenticator □□ □□□□ □□□.
□□ □□□□ □□□ □□□ □□ □□□□□ Microsoft Authenticator □□□ MFA □□□□ □□□□ □□□□□□.
□□□□ □□□ □□□□ □□ MFA □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□.
□□ □□: Azure Portal□□ □□ □□ □□(MFA)□ □□ □□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
In SC-300, the mitigation for unsolicited MFA prompts (push fatigue) is Fraud alert on Azure AD MFA. The materials state that administrators can "allow users to report suspicious MFA prompts and automatically block the user when they select Report fraud in Mi crosoft Authenticator." By contrast, Account lockout settings are designed to "temporarily lock an account after a configurable number of consecutive MFA denials to thwart brute-force attempts," and they do not initiate an automatic block tied to a user's fraud report. The study guide further clarifies that fraud alerts "can automatically block the user for a specified period (default 90 days) when a fraudulent attempt is reported," which is precisely the behavior required in the scenario. Therefore, merely configuring Account lockout settings will not meet the goal of automatically blocking users when they report an unsolicited prompt.

NEW QUESTION: 153
□□□□ □□ □□□□□□ □□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.
□ □ □□□□ □□ □□ □□□□□□ □□□□□ □□□.
□□□ □□□□ □□□?
A. □□
B. □□□
C. □□ □□
D. □□ □□
Answer: B (LEAVE A REPLY)
Reference:
According to the Microsoft SC-300: Identity and Access Administrator Study Guide and the Microsoft Entra (Azure AD) Enterprise Applications documentation , the My Apps portal (https://myapps.
microsoft.com) allows users to access all applications assigned to them. To improve organization and user experience, administrators can group related applications into collections .
A collection is a logical grouping of enterprise applications that appears as a category in the My Apps portal.
Administrators use this feature to simplify navigation for users-e.g., grouping HR, Finance, or Sales applications.
The documentation states:
"Administrators can create and assign application collections to help users find their apps faster in the My Apps portal. Collections appear as tabs that group related applications." Other options in the question are incorrect:
Tags are not used in the My Apps portal; they are used mainly for resource organization in Azure Resource Manager.
Naming policies apply to groups, not apps.
Dynamic groups manage group membership, not My Apps portal organization.

NEW QUESTION: 154
Package1□□□ □□□ □□□□ User1□□□ □□□□ □□□ Azure AD □□□□ □□□□.
□□□1□ □□ □□□ □□ □□□□□.



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

A. □□□ □□ □□ □□□
B. □□□ □□□
C. □□ ID □□□ □□□
D. □□ □□□
Answer: (SHOW ANSWER)
This question refers to Azure AD Entitlement Management under Identity Governance . The goal is to let User1 modify the review frequency (i.e., Access Reviews) for an existing access package named Package1
, following the principle of least privilege .
In Azure AD, the ability to create and manage access packages, catalogs, and access reviews is granted through certain admini strative roles:
* Global Administrator and Identity Governance Administrator - Full control over all Identity Governance settings.
* Catalog Owner or Access Package Manager - Manage access packages and settings within a catalog.
* User Administrator - Can config ure access reviews and manage users, groups, and limited governance settings.
* Privileged Role Administrator , Security Administrator , and External Identity Provider Administrator - Have no direct control over access review settings in Entitlement Management.
From Microsoft documentation ("Azure AD Entitlement Management Delegation and Roles"):
"A user administrator can manage access reviews and entitlement management settings for the directory and assigned catalogs, including adjusting the review f requency or review settings." Thus, to modify the Access Review configuration (frequency, reviewers, etc.) in Package1 , the User Administrator role provides the minimum necessary privilege without granting excessive permissions like Identity Governance Adm inistrator or Global Administrator.

NEW QUESTION: 155
□□□ □□□□ □□ □□ □□ □□ □□□□ □□□ 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: C (LEAVE A REPLY)

Microsoft Graph permissions can be of two types: Delegated and Application.

* Delegated permissions require a signed-in user and can access only that user's data.

* Application permissions are used by background services or daemons to access data across the organization without user consent if the app is granted admin consent.

In the scenario:

* App1 (User1) uses Delegated # can access only the user's data.

* App2 (User2) uses Delegated and Application (Calendars.ReadWrite) # can create appointments across all users. However, User2 has no role to grant consent for application-level permissions.

* App3 (User3, User4) uses Application (Calendars.Read) # only read, not write permissions.

Since User3 is an Exchange administrator, they have the authority to grant admin consent to an application.

Although App3 only has "Read," the Exchange administrator can manage calendar data organization-wide and can create appointments using Exchange management tools.

Hence, as per Microsoft's permissions model and SC-300 guidance, User3 is the only user who has both role and access capabilities to create appointments in every user's calendar.

NEW QUESTION: 156

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

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

User1□ □□□ □□□□□□ □□□ □□ □□□?

A. □□□□ □ □□□ Microsoft Defender

B. Microsoft 365 □□ □□

C. Azure Active Directory □□ □□

D. Microsoft 365 Defender □□

Answer: C (LEAVE A REPLY)

User1 is eligible for the Application Administrator role and needs to configure an Application Proxy connector group. Application Proxy is an Azure AD feature used to publish on-premises applications securely.

To activate the eligible role, User1 must perform a Privileged Identity Management (PIM) activation within the Azure AD admin center.

From Microsoft Documentation:

"Privileged Identity Management (PIM) role activations are performed in the Azure AD admin center under Azure AD # Privileged Identity Management # My roles." Activation steps are not available through Microsoft 365 or Defender portals.

NEW QUESTION: 157
Windows □□ Linux□ □□□□ □□□□□ □□□ □□ □ □□□□.
Microsoft 365 E5 □□□ □□□□.
Microsoft Entra Internet Access□ □□□□□.
□□ □□ □□□ □□ □□ □□□□□ □□□ Global Secure Access□ □□ □□□ □□□□ □□□□□□ □□□□ □□□.
Microsoft Entra □□ □□□□ □□□ □□ □□□?
A. Global Secure Access □□□□□□ □□□□□.
B. □□ □□□□□ □□□□□.
C. □□□ □□□ □□□ □□□□.
D. □□□ □□□□ □□□□.
Answer: A (LEAVE A REPLY)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Entra Internet Access, Global Secure Access, and the requirements for routing internet traffic from on-premises devices, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Scenario and Requirements:
On-premises devices running Windows or Linux:The devices are located in an on-premises environment (e.g., a corporate office or branch) and run either Windows or Linux operating systems.
Microsoft 365 E5 subscription:This subscription includes Microsoft Entra ID P2 and Microsoft Entra Internet Access, which are part of the Global Secure Access suite. This provides the necessary licensing for the solution.
Microsoft Entra Internet Access:This is a Secure Web Gateway (SWG) solution that securesinternet and SaaS app access by routing traffic through Microsoft's Security Service Edge (SSE) for policy evaluation (e.g., web content filtering, Conditional Access).
Requirement:All on-premises devices must route their internet traffic through Global Secure Access for security policy evaluation. Global Secure Access is the unified framework for Microsoft Entra Internet Access and Microsoft Entra Private Access, providing a centralized way to manage network traffic security.
How Global Secure Access Routes Internet Traffic:
Global Secure Access can route internet traffic in two primary ways:
Global Secure Access Client:This client is installed on individual devices (e.g., Windows, macOS, Android, iOS) and routes traffic from the device to Microsoft's SSE for policy evaluation. The client is user-aware and integrates with Microsoft Entra ID for identity-based policies.
Remote Network:This method creates an IPsec tunnel between an on-premises network (e.g., a branch office) and Microsoft's SSE. All internet-bound traffic from devices in the network is routed through the tunnel for security policy evaluation, without requiring a client on each device.
The question involvesmultiple on-premises devicesrunning Windows or Linux, which suggests a network- level solution may be more practical than installing a client on each device, especially since Linux support for the Global Secure Access client is limited.

NEW QUESTION: 158
App1□□□ □□□ □□ □□□ Azure □□□ □□□□.
App1□ □□□ □□□ □□□□ □□□. □□□□ □□ □□ □□□ □□□□ □□□.
* □□□ □□□ □□□ □□□□□.
* □□□ □□□□ □□□□□.
* □□□ □□□ □□□□□□.
□□□ □□□□ □□□?

A. □□□ □ □□□
B. □□□ □□
C. □□□ □□
D. □□ □□
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
□□ 8
Microsoft Entra ID□ □□□ □ □□ □□□□ □□□ □□ □□□□□ □□□□ □□□□ □□ □□□.
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To prevent all users from using legacy authentication protocols when authenticating to Microsoft Entra ID, you can create a Conditional Access policy that blocks legacy authentication. Here's how to do it:
Sign in to the Microsoft Entra admin center:
Ensure you have the role of Global Administrator or Conditional Access Administrator.
Navigate to Conditional Access:
Go to Security > Conditional Access.
Create a new policy:
Select + New policy.
Give your policy a name that reflects its purpose, like "Block Legacy Auth".
Set users and groups:
Under Assignments, select Users or workload identities.
Under Include, select All users.
Under Exclude, select Users and groups and choose any accounts that must maintain the ability to use legacy authentication.It's recommended to exclude at least one account to prevent lockout1.
Target resources:
Under Cloud apps or actions, select All cloud apps.
Set conditions:
Under Conditions > Client apps, set Configure to Yes.
Check only the boxes for Exchange ActiveSync clients and Other clients.
Configure access controls:
Under Access controls > Grant, select Block access.
Enable policy:
Confirm your settings and set Enable policy to Report-only initially to understand the impact.
After confirming the settings using report-only mode, you can move theEnable policytoggle fromReport- onlytoOn2.
By following these steps, you will block legacy authentication protocols for all users, enhancing the security posture of your organization by requiring modern authentication methods. Remember to monitor the impact of this policy and adjust as necessary to ensure business continuity.

NEW QUESTION: 160
□□: □ □□□ □□□ □□□□□ □□□□ □□□ □□ □ □□□□□. □ □□□□ □ □□□□ □□□ □□□ □□□ □ □□ □□□ □□□□ □□□□ □□□□. □□ □□ □□□□ □ □ □□□ □□□ □ □ □ □□, □□ □□□□ □□□ □□ □ □□□□.
□ □□□ □□□ □□ □□□ □□ □□□ □ □□□□. □□□ □□□ □□□ □□ □□□ □□□□ □□□□.

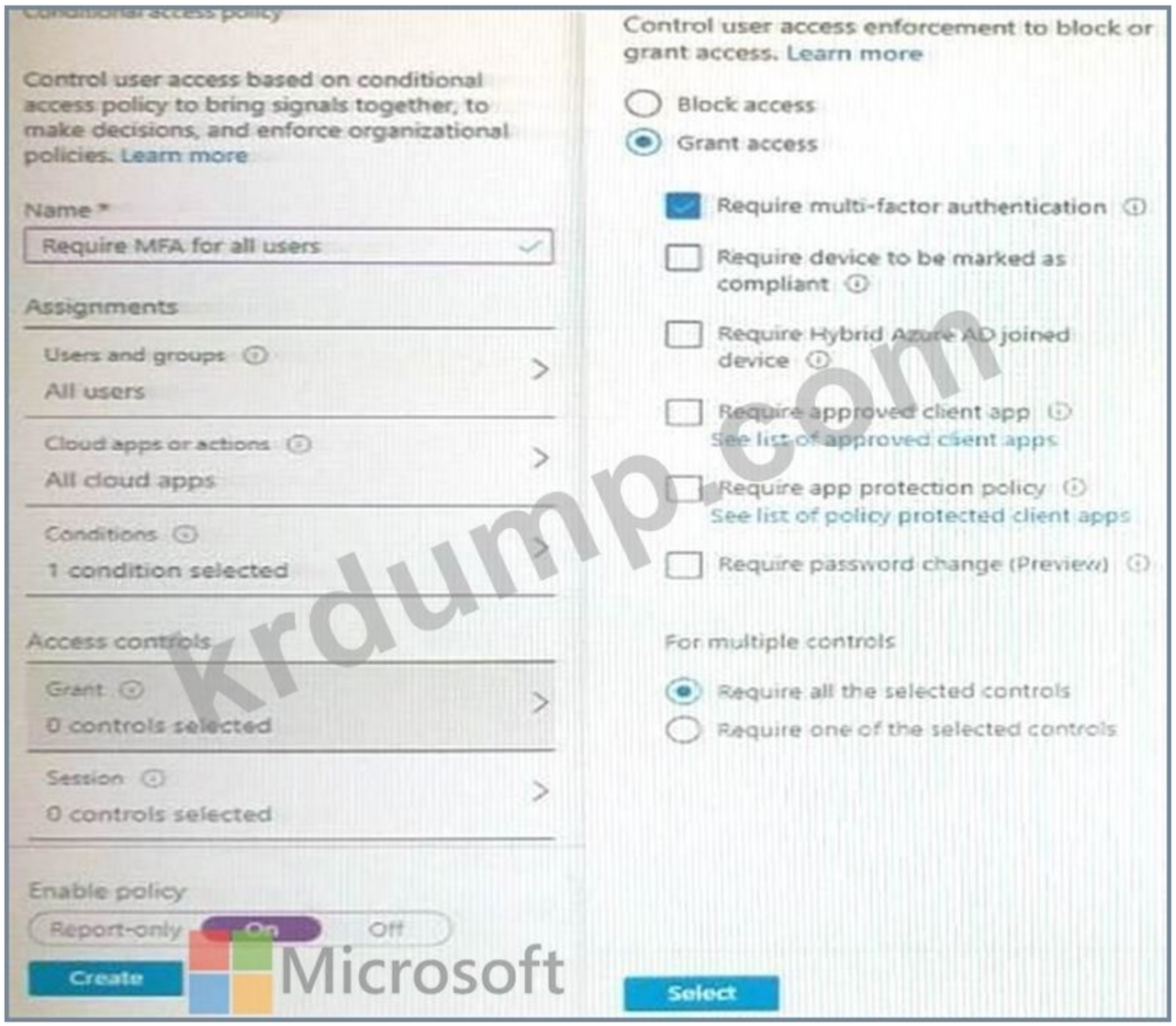
Microsoft 365 □□□□ □□□□.
□□ □□□□ Microsoft 365 □□□□ □□□□ □ □□ □□ □□(MFA)□ □□ Microsoft Authenticator □□ □□□□ □□□.
□□ □□□□ □□□ □□□ □□ □□□□□ Microsoft Authenticator □□□ MFA □□□□ □□□□ □□□□□□.
□□□□ □□□ □□□□ □□ MFA □□□ □□□□ □□ □□□□ □□□□ □□□□ □□□.
□□ □□: Azure Portal□□ □□ □□ □□(MFA)□ □□ □□ □□□ □□□□□.
□□□ □□□ □□□□□?
A. □
B. □□□
Answer: B (LEAVE A REPLY)
E xplanation:
In the SC-300 materials covering Azure AD MFA configuration, Microsoft distinguishes between Notifications (which control whether the Microsoft Authenticator sends push prompts) and Fraud alert settings (which determine what happens when a user reports an unexpected prompt). The study guide notes that notifications "enable push approvals to the app," but this does not take action when a user reports a suspicious prompt. To satisfy the requirement "block the users automatically when they report an MFA request they didn't initiate," you must use Fraud alert options. The documentation states that administrators can "allow users to submit fraud alerts" and "block users who report fraud" so that "reported accounts are immediately blocked until an administrator unblocks them." These options are part of the tenant's MFA service settings, not the Notifications section. In other words, simply configuring Notifications won't automatically block users who tap Report in Microsoft Authenticator; you must explicitly enable the setting to block users upon fraud reports. Therefore, the proposed solution-changing Notifications settings-does not meet the goal. The correct approach is to enable Fraud alert and select Block users who report fraud, ensuring automatic protection when users report unexpected MFA prompts.

NEW QUESTION: 161
□□□□ □□ □□□ □□□ □□□□ □ □□□□ □□□□ □□□ □□□ □□□ □□□□.
□□ □□□□ □□□ □□□□□ □□□.
* □□□□ □□ □□□□ □□□□□□.
* □□□□ □□□ □□□ □□□□□.
□□□□ □□□□□ □□□ □□□□ □□□?
A. □□□ □□□ What If □□
B. Azure AD□ □□□ □□
C. Azure AD□□ □□ □□□
D. □□□□ □□ Microsoft Defender□ □□ □□
Answer: (SHOW ANSWER)
The Conditional Access What If tool is designed to simulate sign-ins under various conditions to test Conditional Access policies without performing real sign-ins . Microsoft's SC-300 guide specifies that this tool is essential for validating the effect of a policy based on user, location, device, or risk l evel.
In this case, the administrator wants to test a policy that blocks access when a high-severity sign-in alert (sign-in risk) occurs and when a user signs in from another country . These scenarios are based on risk and location conditions-both supported in the What If tool simulation.
Microsoft Learn: "Use the What If tool to simulate sign-ins and verify whether a specific Conditional Access policy will be applied."

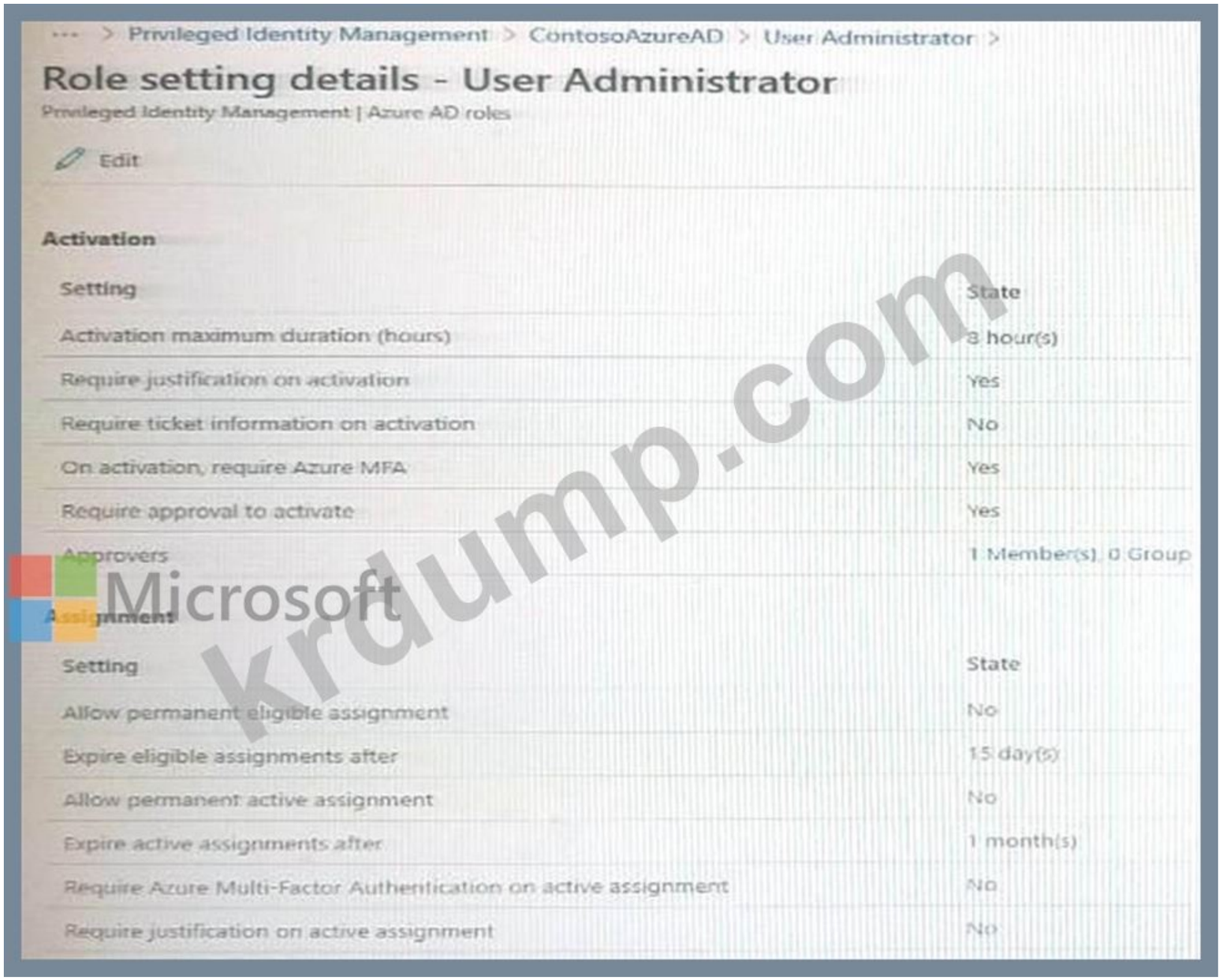
NEW QUESTION: 162
storage1□□□ □□□ □□□ WebApp1□□□ □□□ □□□ Azure □□□ □□□□. WebApp1□ □□□□□ □□□ □□ ID□ □□□□□.
□□□□□ □□□ □□ ID□ □□□□ WebApp1□ storage1□□ □□□ □□ □ □ □□□ □□□□ □□□.
Azure Portal□□ storage1□ □□ □□□ □□□□ □□□?
A. □□ □□ □□
B. □□□ □□(1AM) □□

C. □□ □□□ □□(SAS)
D. □□□ □□
E. □□□ □
Answer: B (LEAVE A REPLY)
Per Microsoft SC-300 official study guide and Microsoft Learn module "Manage identities using managed identities" , when a web app uses a system-assigned managed identity , Azure automatically creates a service principal representing that identity within Microsoft Entra ID.
To grant the managed identity permission to read and write files in an Azure Storage account, you must configure role-based access control (RBAC) permissions via the Access control (IAM) blade in the Azure portal. Specifically, you would assign roles such as Storage Blob Data Contributor or Storage Blob Data Reader to the managed identity at the appropriate resource scope (e.g., storage account or container).
Other options like SAS tokens , access keys , or File share settings rely on key-based or manual authentication methods, which contradict the principle of least privilege and managed identity automation.
Access control (IAM) ensures secure, identity-based access through Azure AD.
Correct Answer: B. the Access control (IAM) settings

NEW QUESTION: 163
Microsoft 365 □□□□ □□□□.
□□□ □□□ □□ □□□ □□□ □□ □□□ □□□ □□□ □□□□□. (□□□ □□□ □□ □□ □□□□□.)


Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
Require MFA for all users
Assignments
Users and groups
All users
Cloud apps or actions
All cloud apps
Conditions
1 condition selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
Report-only
On
Off
Create
Control user access enforcement to block or grant access. Learn more
Block access
Grant access
Require multi-factor authentication
Require device to be marked as compliant
Require Hybrid Azure AD joined device
Require approved client app
See list of approved client apps
Require app protection policy
See list of policy protected client apps
Require password change (Preview)
For multiple controls
Require all the selected controls
Require one of the selected controls
Select

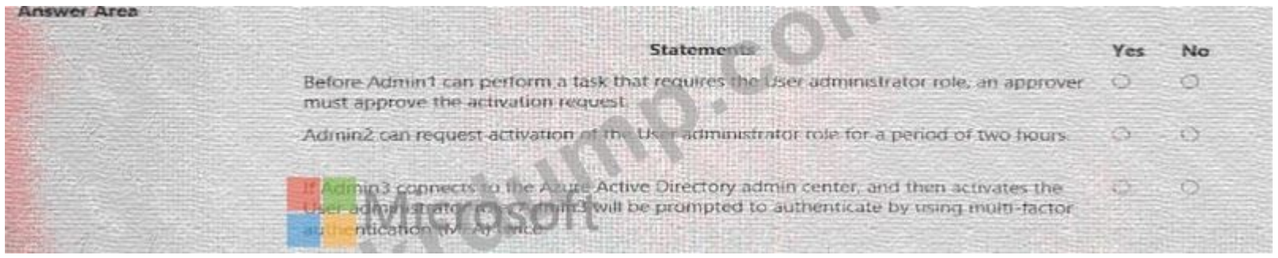
□□ □□ □□ □□ □□ □□□ □□ □□□ □□□ □□ □□□ □ □ □□□□. (□□ □□ □□ □□ □□ □□□□□.)


Privileged Identity Management > ContosoAzureAD > User Administrator >
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
1 Member(s), 0 Group
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

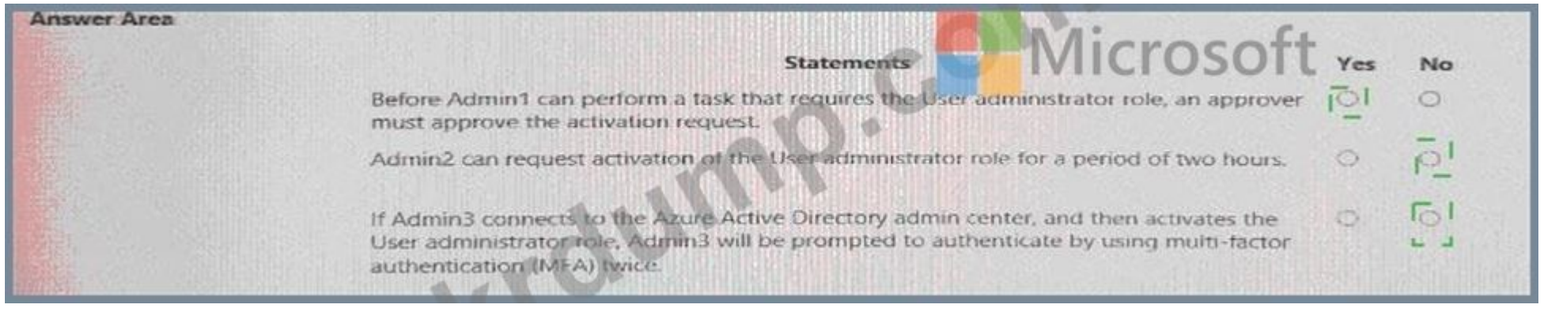
□□ □□ □□ □□□ □□ □□□ □□□ □□ □□□ □ □ □□□□. (□□ □□ □□ □□□□□.)

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

□□: □□ □□□ 1□□□□.



Answer:



Explanation:

Statement

Answer

1. Before Admin1 can perform a task that requires the User Administrator role, an approver must approve the activation request.

Yes

2. Admin2 can request activation of the User Administrator role for a period of two hours.

No

3. If Admin3 connects to the Azure Active Directory admin c enter, and then activates the User Administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice.

Based on Microsoft's SC-300 Identity and Access Administrator Study Guide , Microsoft Learn module

"Manage Azure AD roles by using Privileged Identity Management (PIM)" , and Exam Ref SC-300 , the following logic applies:

* Approval requirement (Admin1) - In the Role setting details image, Require approval to activate is set to Yes, and one approver is listed. This means before any user (e.g., Admin1) can activate the User Administrator role, approval must be granted. Therefore, Admin1 must have the activation request approved before performing any User Administrator tasks. # (Yes)

* Activation duration (Admin2) - The configuration shows Activation maximum duration (hours): 8 hours . This defines the maximum allowed time a user can remain active after role activation. Admin2 can activate for up to 8 hours, not 2 hours unless specifically limited during activation. Hence, the statement claiming Admin2 can activate for "two hours" is incorrect. # (No)
* MFA enforcement (Admin3) - Two relevant controls exist:
* Conditional Access policy requiring MFA for all users.
* PIM role setting On activation, require Azure MFA = Yes.
According to Microsoft documentation, when both Conditional Access and PIM MFA enforcement apply, Azure AD intelligently avoids redundant prompts by honoring a single valid MFA session token. This means Admin3 would only be prompted once for MFA, even though both mechanisms require it. # (No) Therefore, as verified by official Microsoft materials and SC-300 documentation:

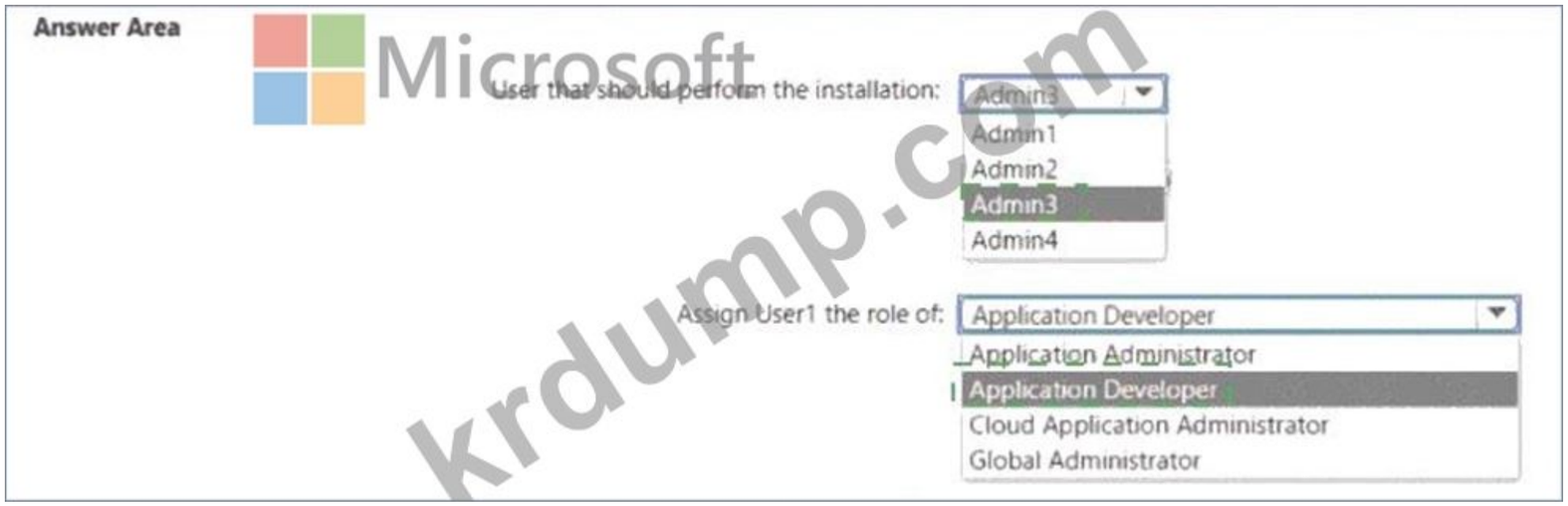
NEW QUESTION: 164
□□ □□ □□□ □□□□ □□□ □□□□□ Microsoft 365 □□□ □□□□.

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

□+□□□□ □1□ □□□ □□□□□. □1□ Azure AD□ □□□□ Azure AD □□□□□□ □□□□ □□□□□.
□□□□□□ □□□ □□□ □□□ □□□□ User1□ Azure AD□ App1□ □□□ □ □□□ □□ □□□. □ □□□□ □□ □□ □□□ □□□□ □□□.
□□ □□□□ □□□ □□□□ □□, Users1□□□ □□ □□□ □□□□ □□□? □□ □□□□ □□□ □□□ □□□□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer Area

Answer:



Explanation:

According to the Microsoft SC-300: Identity and Access Administrator Study Guide and Microsoft Learn module "Implement and manage Application Proxy for on-premises apps" , Azure AD Application Proxy requires that the connector installation be performed by a user with either the Global Administrator or Application Administrator or Cloud Application Administrator role.

Part 1 - User that should perform the installation The Application Proxy connector must be installed by a user who can register and manage applications in Azure AD. The documentation specifies that both Application Administrator and Cloud Application Administrator roles can perform Application Proxy connector installation. Since the question requires adherence to the principle of least privilege, Admin3 (Cloud Application Administrator) is the most appropriate user - because this role grants the required permissions without the broader rights of the Global Administrator.

"Cloud Application Administrator can create, manage, and delegate enterprise applications and Application Proxy connectors, without tenant-wide permissions."

Therefore, Admin3 should perform the installation.

Part 2 - Role for User1 After the connector is installed, User1 needs to register App1 in Azure AD. The role required to register and configure application registrations is the Application Developer role.

According to Microsoft documentation:

"Users assigned the Application Developer role can register applications in Azure AD and manage app registrat ions they own." This role is the least privileged role that allows creating new application registrations, unlike Application Administrator or Cloud Application Administrator, which can manage all apps tenant-wide.

Therefore, assign User1 the role of Application Developer.

NEW QUESTION: 165

Azure AD □□□□ □□□□.

App1□□□ □□□ □□□□□□ □□□□□□□ □□□□□.

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

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

□□ □□ □□□ □□ □□□?

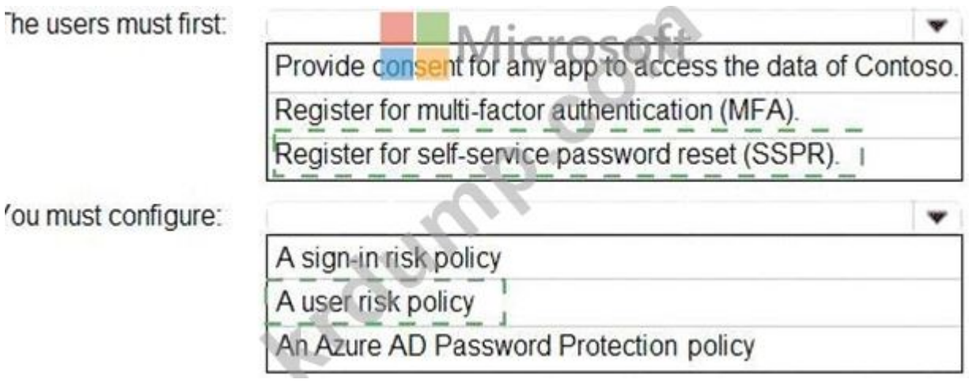
A. □□□□ □□ □□□ □□ □□□ □□□□□□.
B. □□□□ □□ □□□ □□ □□□ □□□□ □□□□□.
C. App1□ □□ □□□□ App1□ □□□□ □□ □□□ □□□ □□□□□.
D. Appl□ □□ □□□ □□□ □□□ □□□□.
Answer: A (LEAVE A REPLY)
Azure AD (Entra ID) allows administrators to control how users request permission for applications that require admin consent. By default, only administrators can grant such consent.
According to the SC-300 Study Guide (Identity Management & Governance) and Microsoft Entra Documentation, the least privileged and compliant method to enable user-driven admin consent requests is to:
* Enable admin consent requests in the tenant.
* Designate one or more reviewers (optional) to handle these requests.
Once enabled, users who encounter an app that needs admin consent can submit a request for approval instead of being blocked. This ensures controlled delegation without globally granting broad permissions to all apps.
"Enable admin consent requests in Azure AD to allow users to request approval for apps that need tenant- wide permissions, ensuring least privilege and administrator oversight."

NEW QUESTION: 166
□□ □□□□ □□ □□□□□□ □□□□ □□ □□□ □□ □□□ □□□□ □□□. □□□ □□□□ □□□?
A. □□ □□
B. □□□ □□ □□
C. □□□ □□□
D. □□□□□□ □□□
Answer: (SHOW ANSWER)
The requirement is:
"Require admin approval for application access to organizational data." According to the Microsoft SC-300 exam guide and Microsoft documentation on "Configure consent settings for applications", Azure AD provides User consent settings under Enterprise applications # Consent and permissions to control how applications can request permissions to access organizational data.
By default, users can consent to allow apps to access organizational data on their behalf, which can create security risks. To ensure tighter control, administrators can:
* Disable user consent entirely, or
* Require admin consent workflow so that when users try to grant an app access, it must first be approved by an administrator.
The SC-300 study materials explicitly describe:
"To require administrator approval before an app can access organizational data, configure the User consent settings to use the admin consent workflow." This aligns perfectly with the stated requirement - to ensure admin approval is required before apps gain access to organizational data.
Other options are incorrect:
* Authentication methods manage MFA and SSPR, not app consent.
* Access packages are part of Identity Governance for resource access, not app consent.
* Application Proxy publishes on-premises apps, not related to app consent permissions.

NEW QUESTION: 167

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

Answer:



Explanation:

According to the Microsoft Identity and Access Administrator (SC-300) official study guide and Microsoft Learn module "Implement and manage user risk policies", the scenario where "users must be forced to change their password if there is a probability that their identity was compromised" directly maps to the Azure AD Identity Protection "User risk policy." In Azure AD Identity Protection, user risk represents the likelihood that an account's credentials have been compromised. When Azure AD detects a high user risk (for example, leaked credentials, atypical sign-in behavior, or sign-ins from unfamiliar locations), the User Risk Policy can be configured to automatically block access or require the user to reset their password upon the next sign-in.

Before a user can reset their password or complete remediation, they must have a registered authentication method (for password reset and MFA). Therefore, users must first register for multi-factor authentication (MFA) - this registration enables the authentication methods (like phone number or authenticator app) that are also used during password reset verification.

The SC-300 documentation specifically highlights:

"To enforce a password change when a user's identity risk is high, the user must be registered for MFA, and a user risk policy must be configured to require password change." Thus, the correct configuration is:

* Users must first register for MFA - to ensure they have verified methods available.
* Configure a user risk policy - to automatically trigger password reset upon detection of compromised credentials.

Correct Answers:

* Users must first: Register for multi-factor authentication (MFA).
* You must configure: A user risk policy.

NEW QUESTION: 168
□□□□ □□ Microsoft Defender□ □□□□ Microsoft 365 E5 □□□ □□□□.
□□□ □□ □ □□□ □□□ □□□□□.
□□□ □□□ □□□□ □□ □□ □□□□ □□□.
Microsoft 365 Defender □□□□ □□□ □□ □□□?
A. □□□ □ □□□ □□□□.
B. □□□ Cloud Discovery □□□□ □□□□.
C. OAuth □□□ □□□ □□□ □□□□□.
D. □□□□ □ □□□□□ □□□□□.
Answer: (SHOW ANSWER)
According to the Microsoft Identity and Access Administra tor (SC-300) Study Guide and Microsoft Learn module: "Discover and manage shadow IT" within Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security) , the Cloud app catalog is the authoritative reference database that contains detailed risk assessments of thousands of cloud applications discovered within your organization. Each application in the cloud app catalog is automatically evaluated against a large set of security and compliance criteria - over 80 risk factors including authenticatio n requirements , encryption standards , data ownership , regulatory compliance , and certifications . This catalog helps administrators identify which discovered or sanctioned applications do not require user authentication , which is a critical factor when eval uating application risk posture.
From the Microsoft 365 Defender portal , administrators can open Defender for Cloud Apps # Cloud Discovery # Cloud app catalog . Within this interface, you can filter and sort apps by authentication type , specifically reviewi ng those listed with "No authentication" or "Not supported" . This allows quick identification of unsecured or unauthenticated apps that could pose risks to enterprise data and identity protection.
Microsoft's documentation emphasizes:
"The Cloud app catalo g provides detailed information about each discovered application, including whether the app supports user authentication and what authentication methods are required." Options A and B (queries and reports) are used for analyzing discovered app traffic data, not intrinsic app properties. Option C (OAuth policy) monitors app permissions, not authentication requirements.

NEW QUESTION: 169
Microsoft 365 □□□□ □□□□.
Azure Active Directory(Azure AD) □□□□ □□□□□ Active Directory □□□□ □□□□□□. □□□□□ □□ □□ □□□ □□□ □□□□ □□□□.

Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

□□□ □□□□□ □□□□ □□□ □ □□□□.
Server1□ Server2□ Azure AD □□ □□□ □□□□□.
Windows Server 2019□ □□□□ Server4□□ □ □□□ □□□□□.
□□ □□□ □□□ □□□□□□ Azure AD □□ □□□ □□ □□□□□ □□□□ □□□.
Server4□ □□□ □□□□ □□□?
A. Azure AD □□
B. Azure AD □□□□□□ □□□
C. □□□□ □□ □□ □□□(PCNS)
D. Azure AD □□ □□ □□□ □□□
Answer: D (LEAVE A REPLY)
According to the Microsoft SC-300 official exam reference and Microsoft's official documentation, Azure AD Password Protection provides password policy enforcement and banned password protectio n for both cloud and on-premises environments.

The solution requires two primary components:
* Domain Controllers (DC Agents) - enforce password policies within the domain.
* Proxy Service (Azure AD Password Protection Proxy) - communicates with Azure AD to download the latest password policies and banned password lists and then shares them with the DC agents.
In the scenario, Server1 and Server2 are domain controllers that already have Azure AD Password Protection installed but cannot communicate with the in ternet directly. That means they rely on the proxy service running on a separate server to connect securely to Azure AD.
To ensure high availability, Microsoft recommends deploying at least two proxy servers . This ensures continuous synchronization of the password policy even if one proxy fails.
From the Microsoft documentation:
"For redundancy, deploy at least two proxy servers. The proxy service retrieves the global and custom banned password lists from Azure AD and replicates them to all domain controlle rs running the DC agent." Thus, installing the Azure AD Password Protection proxy service on Server4 ensures service continuity if one of the proxy servers fails.

NEW QUESTION: 170
□□ □□ □□ □□ □□□□ □□□ contoso.com□□□ Azure AD □□□□ □□□□.
Admin 1□□□ □□□□ □□□□.

Name	Description
Au1	Administrative unit
CAPolicy1	Conditional Access policy
Package1	Access package

□□□□ contoso.com□ □□ □□ □□□□ □□□□ □ □□□ □□□□ □□□.
□□ □□ □□□ □□ □□□?
A. ID □□□□□ □□□□□.
B. □□□1□ □□□□□.
C. CAPolicy1□ □□□□□.
D. Admin1□□ Au1□ □□ □□□ □□□ □□□□□.
Answer: (SHOW ANSWER)
To enable Security defaults for contoso.com, you should first sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator. Then, browse to Azure Active Directory > Properties and select Manage security defaults. Set the Enable security defaults toggle to Yes and select Save.
After that, you can assign Admin1 the Identity Administrator role for Au1 to enable them to manage security defaults for the tenant.
https://practical365.com/what-are-azure-ad-security-defaults-and-should-you-use-them/

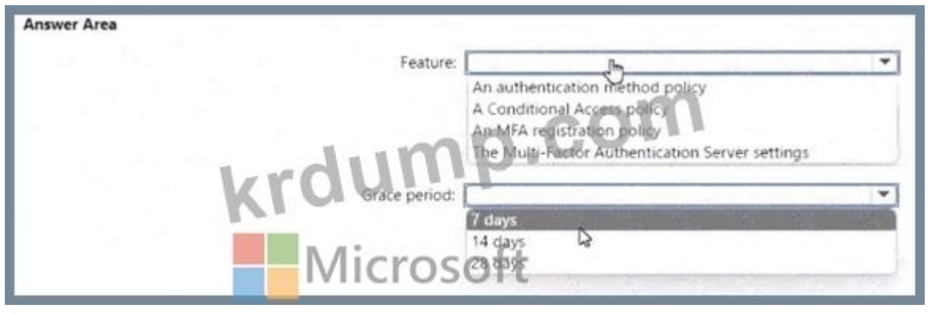
NEW QUESTION: 171
□□ □□ □□ □□ □□□□ □□□ Azure Active Directory(Azure AD) □□□□ □□□□.

Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1□ Group1□ □□□□□□.
□□ □□□ □□□ □□□ □□□ □□□□.
* □□□ □□□: □□ □□
* □□ : □□ □□
* □□ : □□1
* □□□ : □□(□□)

□□ □□□□ User3□ □□ □□ □□□ □□□ □ □□□□?
A. User1, User2, User3
B. User3□
C. User1□
D. User1□ User2□
Answer: B (LEAVE A REPLY)
Based on the Microsoft SC-300: Identity and Access Administrator Official Study Guide and Microsoft Learn module "Manage access reviews in Azure AD" , when creating an access review with the setting Reviewers: Members (self) , each user who is a member of the target group is only allowed to review their own access , not the access of others.
Here's how the logic applies in this scenario:
* The scope of the access review is set to Everyone , meaning both internal members and external (guest) users within Group1 will be included in the review.
* The reviewers option is configured as Members (self) - this setting instructs Azure AD to send review tasks to each user so they can attest to their own need for continued group membership.
* Therefore, User3 (a Guest user) will receive the review task to confirm or deny their own access to Group1.
* User1 and User2 , though they are members and User1 is the group owner, wi ll not review User3's access because "Members (self)" does not delegate review authority to other members or owners - it only applies to individual self-assessment.
Microsoft documentation explicitly clarifies:
"When you select Members (self) as the review er type, each user reviews only their own access. Owners or administrators do not approve or deny access on their behalf." Hence, in this scenario, only User3 can perform the access review for their own membership in Group1.

NEW QUESTION: 172
□□□ □□ □□□ □□□□ MFA□ □□ □□□ □□ □□□ □□□□ □□□.
□□ □□□ □□□□ □□, □□□□ □□□ □□□□ □□□ □□□ □ □□□? □□□□□ □□ □□□□ □□□ □□□ □□□□□.
□□: □□ □□□ 1□□□□.



Answer:

Explanation:
Feature: An MFA registration policy

Grace period: 14 days
According to the Microsoft Identity and Access Administrator (SC-300) Study Guide and Microsoft Learn documentation under "Plan, implement, and manage multifactor authentication (MFA)" , when an organization wants to require users to register for multi-factor authentication methods (such as Microsoft Authenticator, phone number, or email), this is managed through the MFA registration policy within Azure AD Identity Protection.
This feature is called "Combined security information registration" or MFA registration policy, and it allows administrators to enforce users to register for MFA and Self-Service Password Reset (SSPR). The policy defines which users are required to register and sets a grace period - the amount of time a user can postpone registration after first being prompted.
From the Microsoft official exam reference:
"The MFA registration policy allows users to postpone registration for a defined grace period. The default and maximum supported value is 14 days." During the grace period, users can skip the registration prompt but will be reminded every time they sign in until they complete registration or the grace period expires. Once the 14-day period ends, users must register their authentication methods before accessing resources.
Therefore, based on Microsoft's SC-300 study materials and Azure AD documentation:
* The correct feature used to enforce this is An MFA registration policy.
* The standard and maximum grace period before users must complete registration is 14 days.

NEW QUESTION: 173
Group1□ Group2□□ □ □□□ □□ □□ □□□ □□□□ □□□ Microsoft 365 E5 □□□ □□□□.

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

□□□□ □□ □□□ □□□ □□□ □□□ □□□ □□□□ □□□□.
* □□: Policy1
□□ □□□
* □□□□
* □□ □□□□ □
* □□ □□
* □□□□
* □□ □□ □□
□□ □ □□□ □□, □□□ □□□□□ '□'□ □□□□□. □□□ □□□ '□□□'□ □□□□□.
□□: □□ □□□ 1□□□□.

Answer:

Explanation:

User1 must use multifactor authen tication (MFA) when signing in to Microsoft 365 apps. = Yes User2 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. = Yes User3 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. = No Compr ehensive and Detailed Explanation with all Microsoft SC-300: Identity and Access Administrator documents : = In Conditional Access, enforcement is determined by Assignments # Users or workload identities (which specify who the policy applies to) and Target resources (which specify what apps/resources are protected). When a policy's Grant control is set to Require multifactor authentication , all identities included in the policy's user assignment scope must perform MFA when accessing the targeted resources. B eing a member of multiple groups does not weaken enforcement; if a user is in any included group, the policy applies.

Conversely, users not included in the policy's user assignment scope are not prompted by that policy, even if they hold privileged roles. Holding the Global Administrator role does not automatically force MFA unless the tenant uses Security defaults or a Conditional Access policy targets that admin account or its group.

Applying this to the scenario: Policy1 targets All cloud apps (so the ap ps side is universal), and-given the group context-its user assignment is scoped to Group1 . User1 (Group1) and User2 (Group1 and Group2) are both in scope and therefore must perform MFA. User3 is only in Group2 ; since Group2 is not within the policy's user assignment, Policy1 does not apply to User3, despite the Global Administrator role. Hence:

Yes for User1, Yes for User2, and No for User3.