Microsoft.SC-300.v2023-10-26.q85

Exam Code:	SC-300
Exam Name:	Microsoft Identity and Access Administrator
Certification Provider:	Microsoft
Free Question Number:	85
Version:	v2023-10-26
# of views:	940
# of Questions views:	850
https://www.freepdfdumps.com/Microsoft.SC-300.v2023-10-26.q85.html	

NEW QUESTION: 1
You need to locate licenses to the A. Datum users. The solution must need the technical requirements.
Which type of object should you create?
A. An OU
B. A Dynamo User security group
C. An administrative unit
D. A distribution group
Answer: C (LEAVE A REPLY)

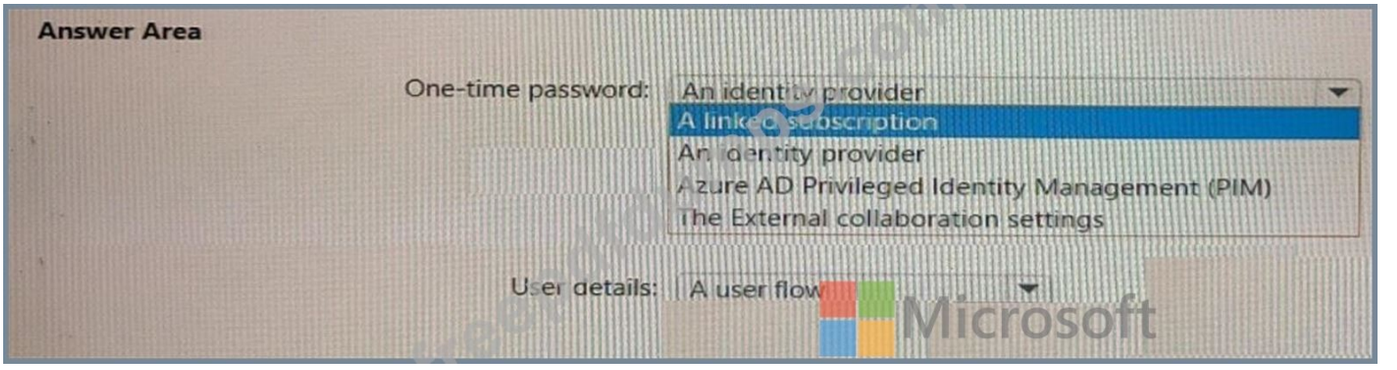
NEW QUESTION: 2
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

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

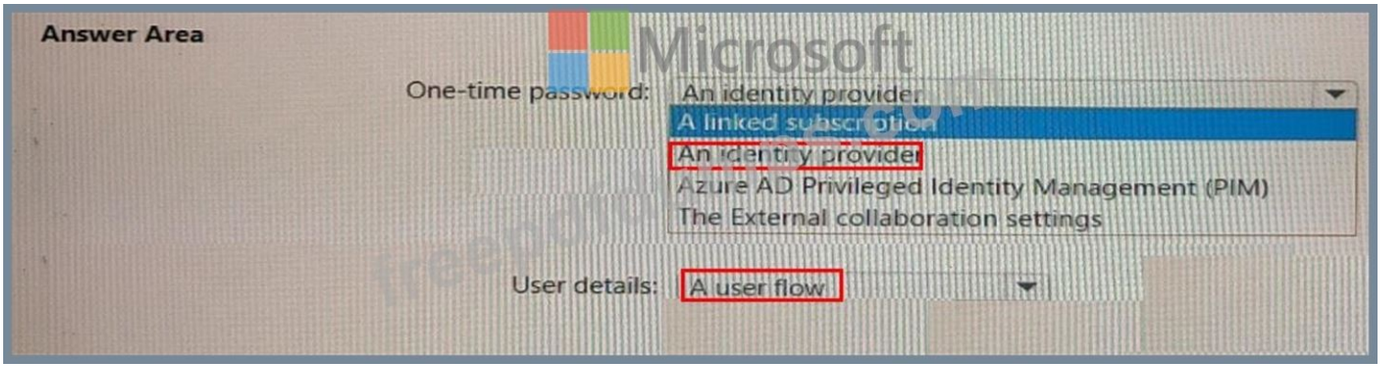
In Azure AD. you add a new enterprise application named Appl. Which groups can you assign to App1?
A. Group3 only
B. Group1 and Group2 only
C. Group1 only
D. Group1 and Group4
E. Group2 only
Answer: A (LEAVE A REPLY)

NEW QUESTION: 3

You have an Azure AD tenant and an Azure web app named App1.
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:
* Guest users must be able to sign up by using a one-time password.
* The users must provide their first name, last name, city, and email address during the sign-up process.
What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer are a.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 4
You need to implement the planned changes for litware.com. What should you configure?
A. staging mode in Azure AD Connect for the litware.com domain
B. Azure AD Connect to include the litware.com domain
C. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5
You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?
A. the Device settings
B. the User settings
C. the Access reviews settings
D. Security defaults

Answer: A (LEAVE A REPLY)

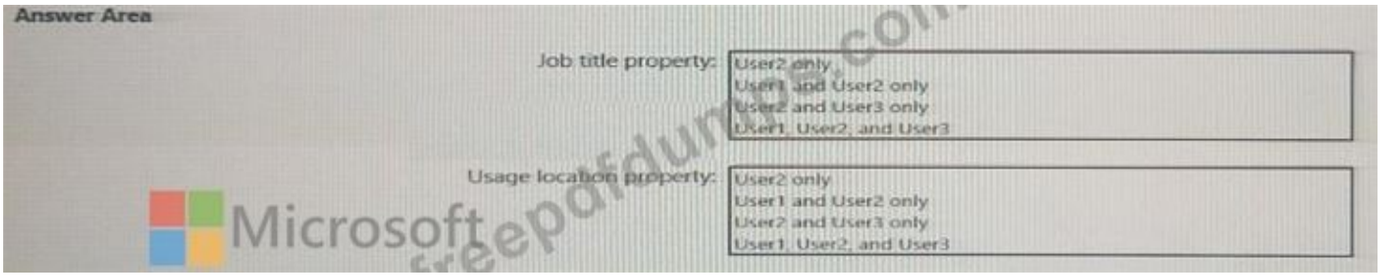
NEW QUESTION: 6

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

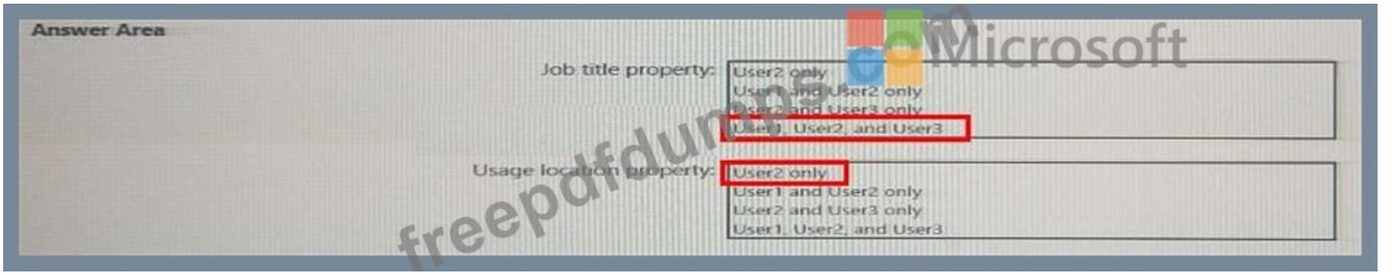
Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

For which users can you configure the Job title property and the Usage location property in Azure AD? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 7

You have an Azure subscription that contains the key vaults shown in the following table.

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

The subscription contains the users shown in the following table.

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

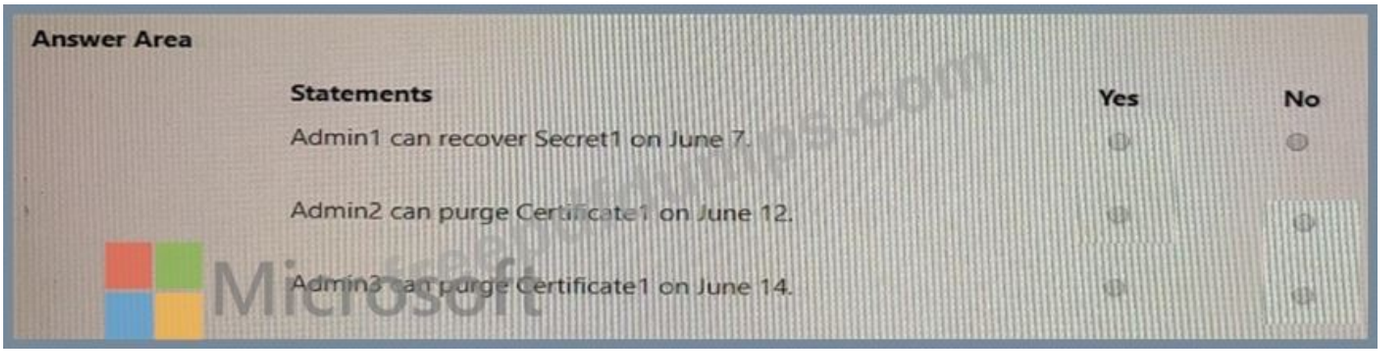
On June1, Admin4 performs the following actions:

* Deletes a certificate named Certificate! from Key Vault1

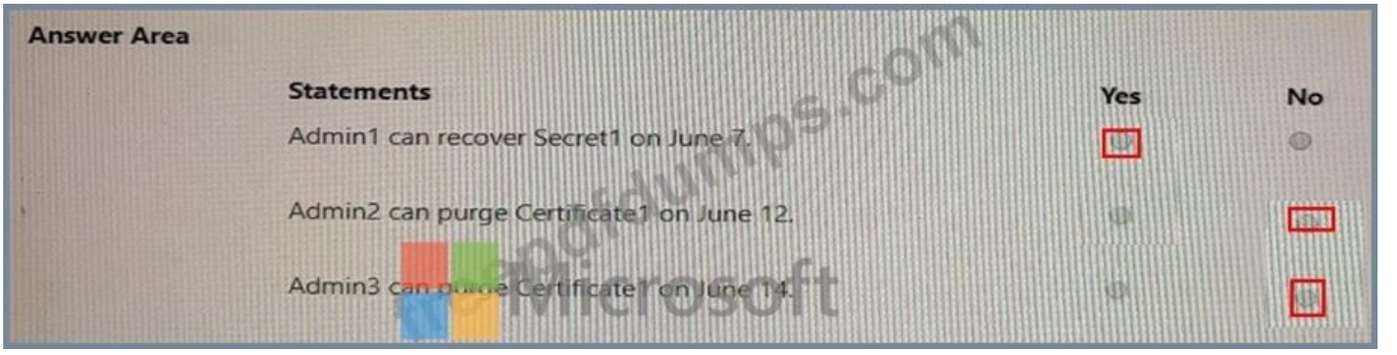
* Deletes a secret named Secret1 from KeyVault2

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

NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 8

Your network contains an Active Directory forest named contoso.com that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com by using Azure AD Connect.

You need to prevent the synchronization of users who have the extensionAttribute15 attribute set to NoSync.

What should you do in Azure AD Connect?

A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.

B. Configure a Full Import run profile.

C. Create an inbound synchronization rule for the Active Directory Domain Services connector.

D. Configure an Export run profile.

Answer: C (LEAVE A REPLY)

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration

NEW QUESTION: 9

You need to resolve the issue of I-.Group1. What should you do first?

A. Change Membership type of IT-Group1 to Dynamic User

B. Change Membership type of IT-Group1 to Dynamic Device

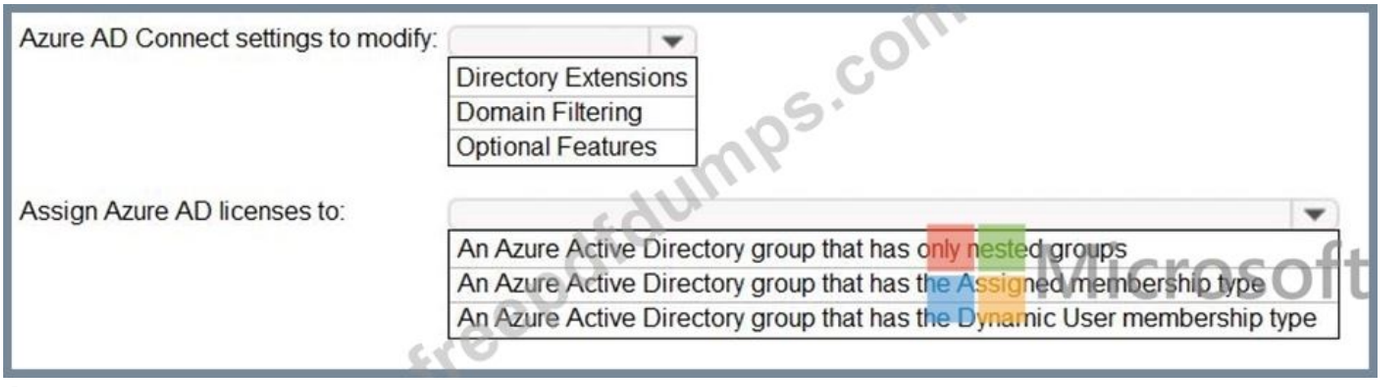
C. Add an owner to IT_Group1.

D. Recreate the IT-Group 1 group.

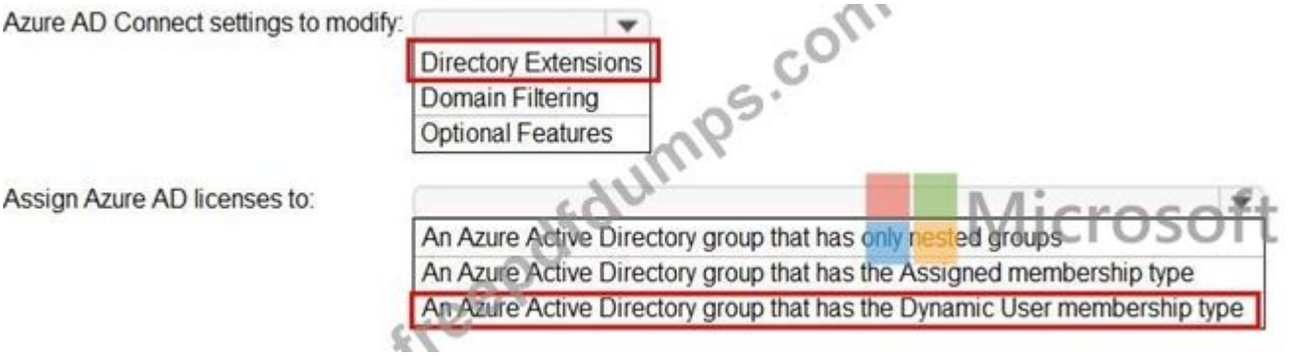
Answer: D (LEAVE A REPLY)

NEW QUESTION: 10
You have a Microsoft 365 tenant.
The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.
Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.
You plan to manage access to external applications by using Azure AD.
You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.
What should you use to gather the information?
A. Application Insights in Azure Monitor
B. access reviews in Azure AD
C. Cloud App Discovery in Microsoft Cloud App Security
D. enterprise applications in Azure AD
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery-reports#using-traffic-logs-for-cloud-discovery

NEW QUESTION: 11
You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

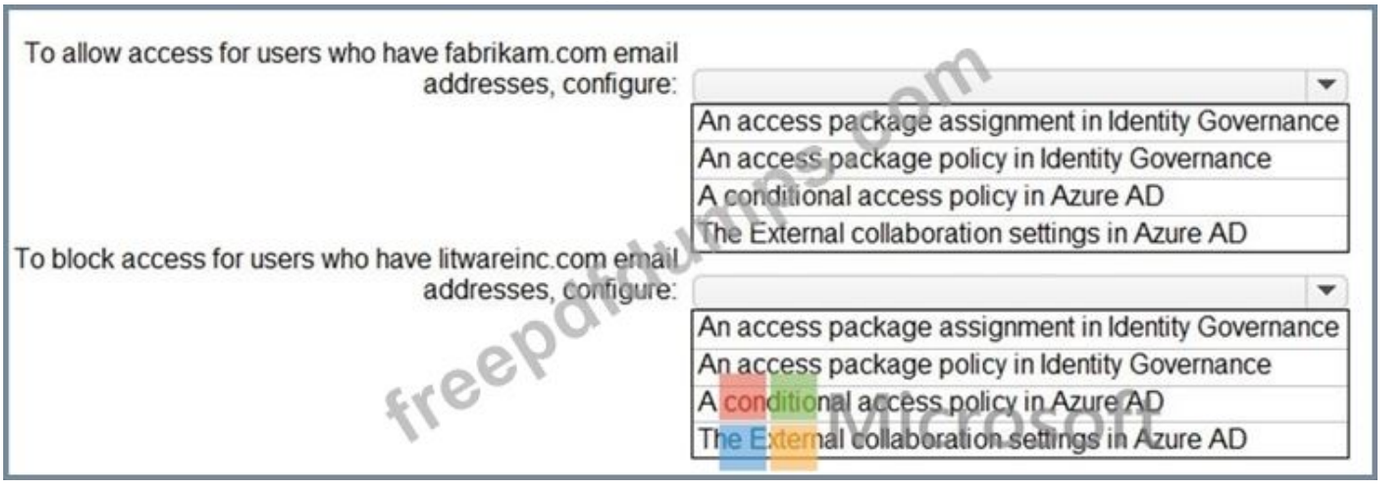


NEW QUESTION: 12
You have an Azure Active Directory (Azure AD) tenant that contains the objects shown in the following table.

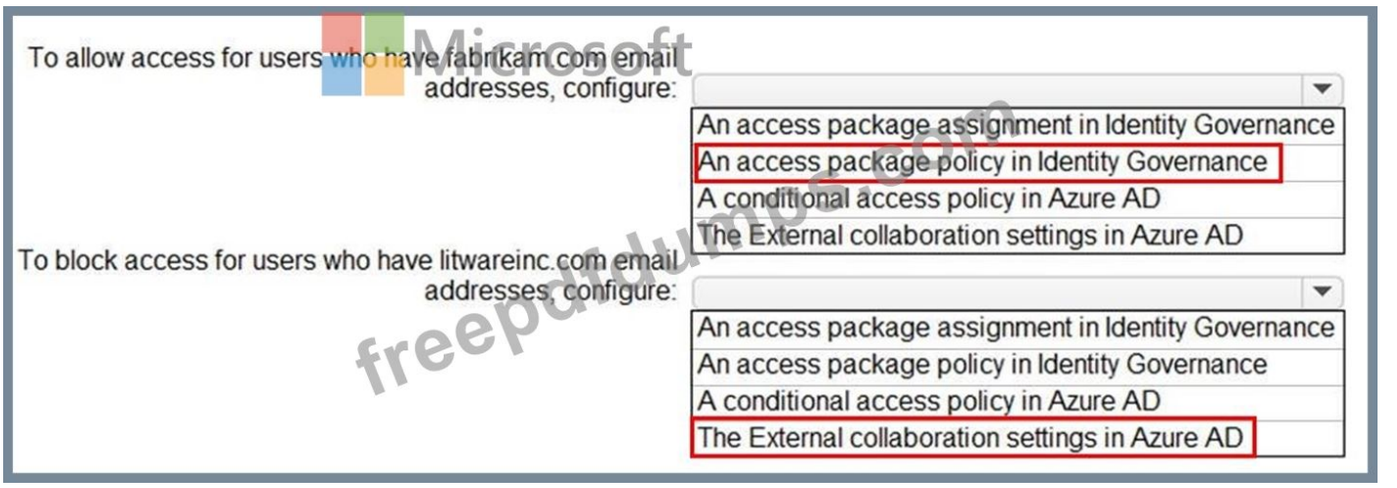
Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Which objects can you add as eligible in Azure Privileged identity Management (PIM) for an Azure AD role?
A. User1 only
B. User1 and Identity1 only
C. User1. Guest1, and Identity
D. User1 and Guest1 only
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

NEW QUESTION: 13
Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.
Fabrikam uses Azure AD and has two verified domain names of fabrikam.com and litwareinc.com. Both domain names are used for Fabrikam email addresses.
You plan to create an access package named package1 that will be accessible only to the users at Fabrikam.
You create a connected organization for Fabrikam.
You need to ensure that the package1 will be accessible only to users who have fabrikam.com email addresses.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

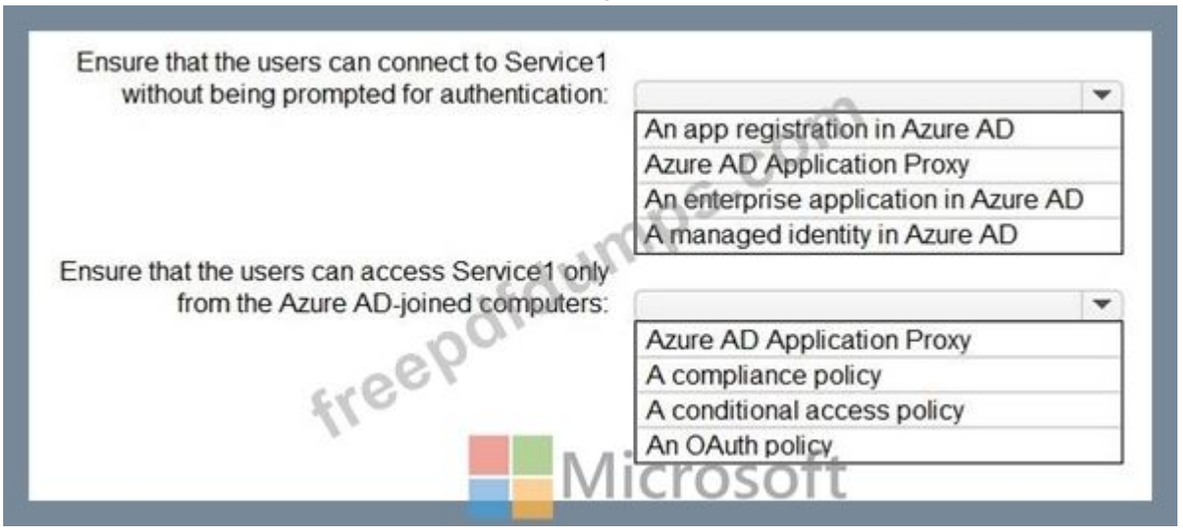


Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

NEW QUESTION: 14
Your company has a Microsoft 365 tenant.
All users have computers that run Windows 10 and are joined to the Azure Active Directory (Azure AD) tenant.
The company subscribes to a third-party cloud service named Service1. Service1 supports Azure AD authentication and authorization based on OAuth. Service1 is published to the Azure AD gallery.
You need to recommend a solution to ensure that the users can connect to Service1 without being prompted for authentication. The solution must ensure that the users can access Service1 only from Azure AD-joined computers. The solution must minimize administrative effort.
What should you recommend for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

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

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

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

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

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

NEW QUESTION: 15
Your company has an Azure AD tenant that contains the users shown in the following table.

Name	Role
User1	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

You have the app registrations shown in the following table.

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 company policy prevents changes to user permissions.
Which user can create appointments in the calendar of each user at the company?
A. User1
B. User2
C. User4

D. User3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.
You need to ensure that users can request access to Site. the solution must meet the following requirements.
* Automatically approve requests from users based on their group membership.
* Automatically remove the access after 30 days
What should you do?
A. Create a Microsoft Defender for Cloud Apps access policy.
B. Create an access package.
C. Configure Role settings in Azure AD Privileged Identity Management.
D. Create a Conditional Access policy.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 17
You have an Azure Active Directory (Azure AD) tenant named conto.so.com that has Azure AD Identity Protection enabled. You need to Implement a sign-in risk remediation policy without blocking access.
What should you do first?
A. Configure access reviews in Azure AD.
B. Enforce Azure AD Password Protection.
C. implement multi-factor authentication (MFA) for all users.
D. Configure self-service password reset (SSPR) for all users.
Answer: C (LEAVE A REPLY)
MFA and SSPR are both required. However, MFA is required first.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

NEW QUESTION: 18

You have a Microsoft 365 tenant that has 5,000 users. One hundred of the users are executives. The executives have a dedicated support team.

You need to ensure that the support team can reset passwords and manage multi-factor authentication (MFA) settings for only the executives. The solution must use the principle of least privilege.

Which object type and Azure Active Directory (Azure AD) role should you use? To answer, select the appropriate options in the answer area.

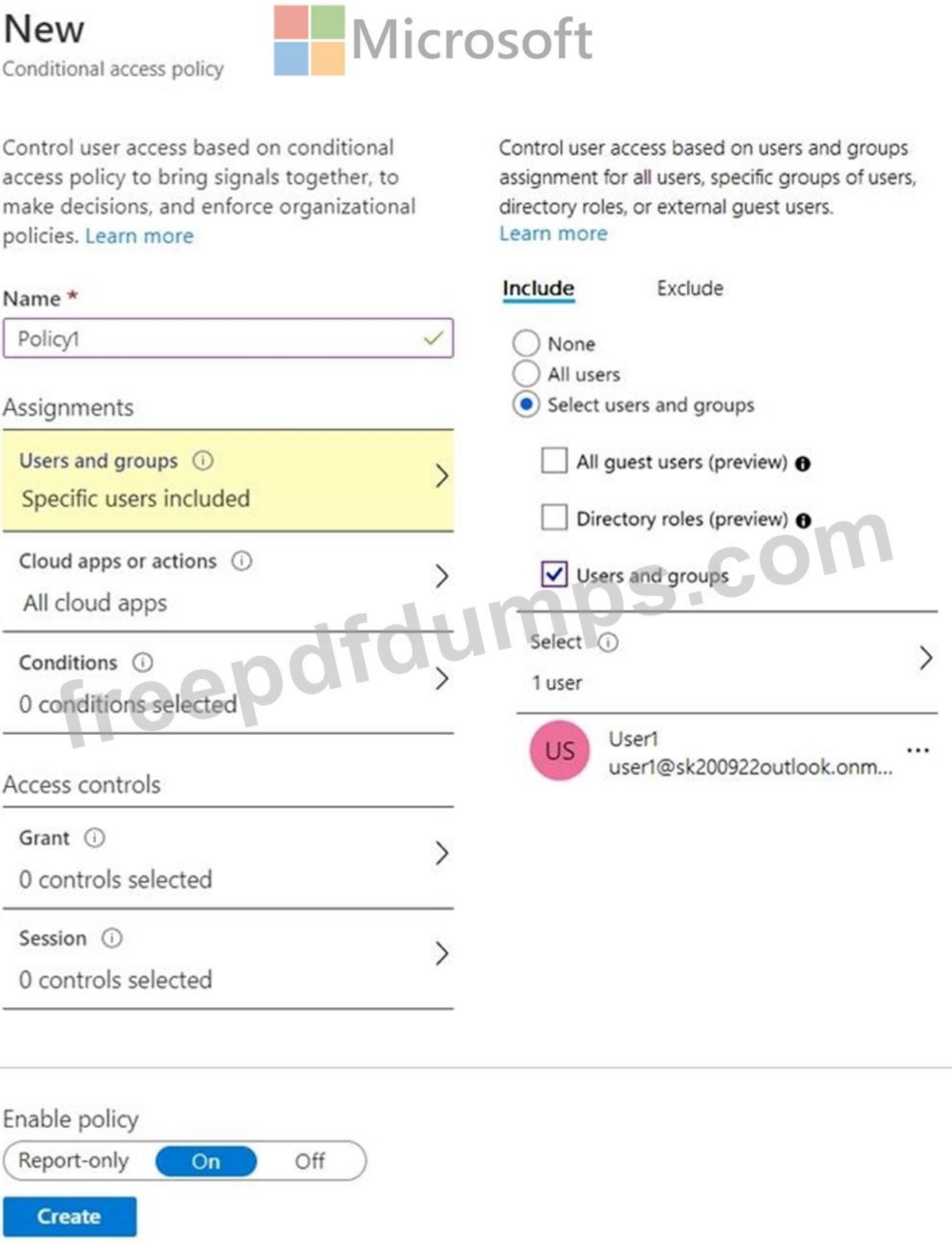
NOTE: Each correct selection is worth one point.

Answer:

NEW QUESTION: 19

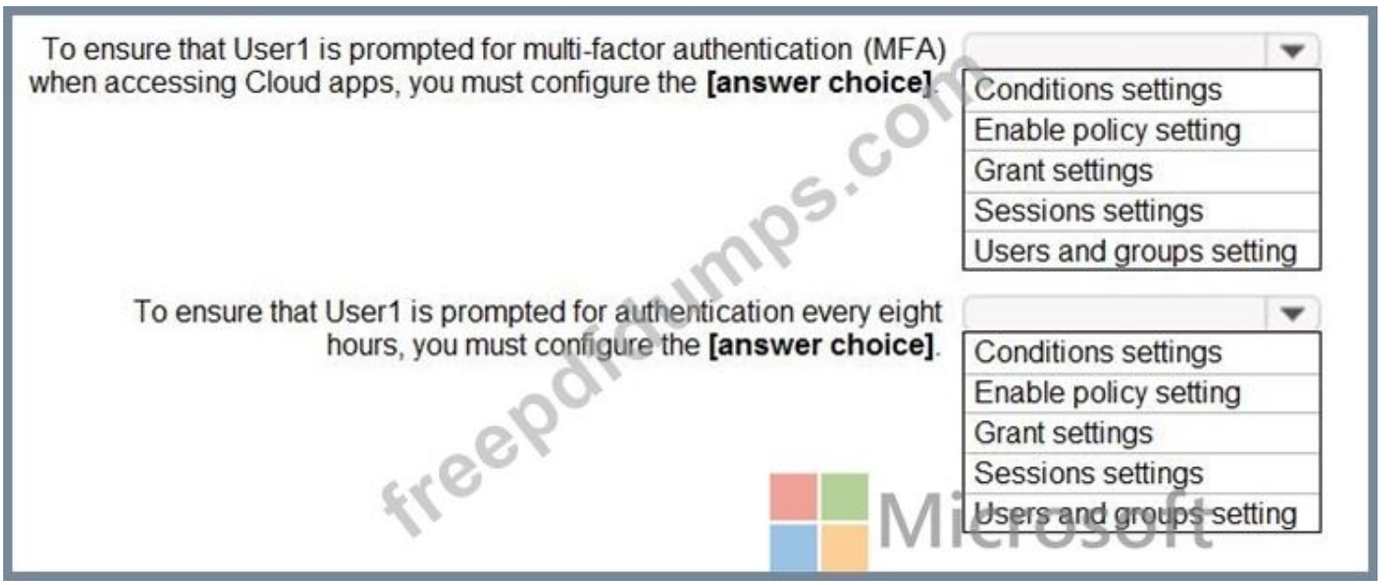
You have an Azure Active Directory (Azure AD) tenant that has Security defaults disabled.

You are creating a conditional access policy as shown in the following exhibit.

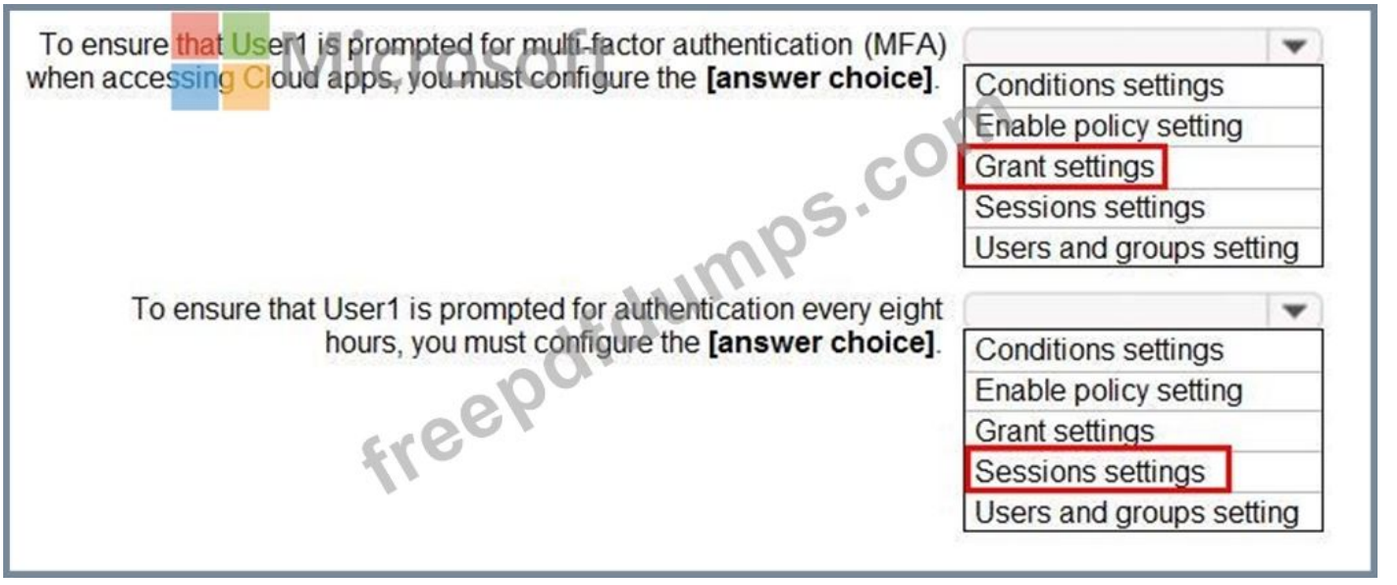


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:



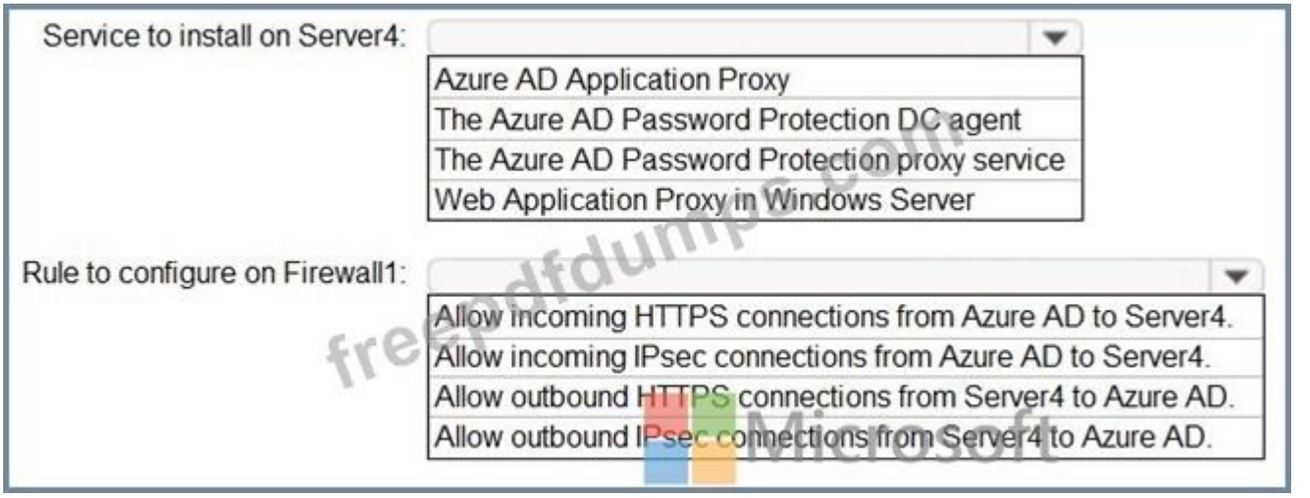
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa

NEW QUESTION: 20

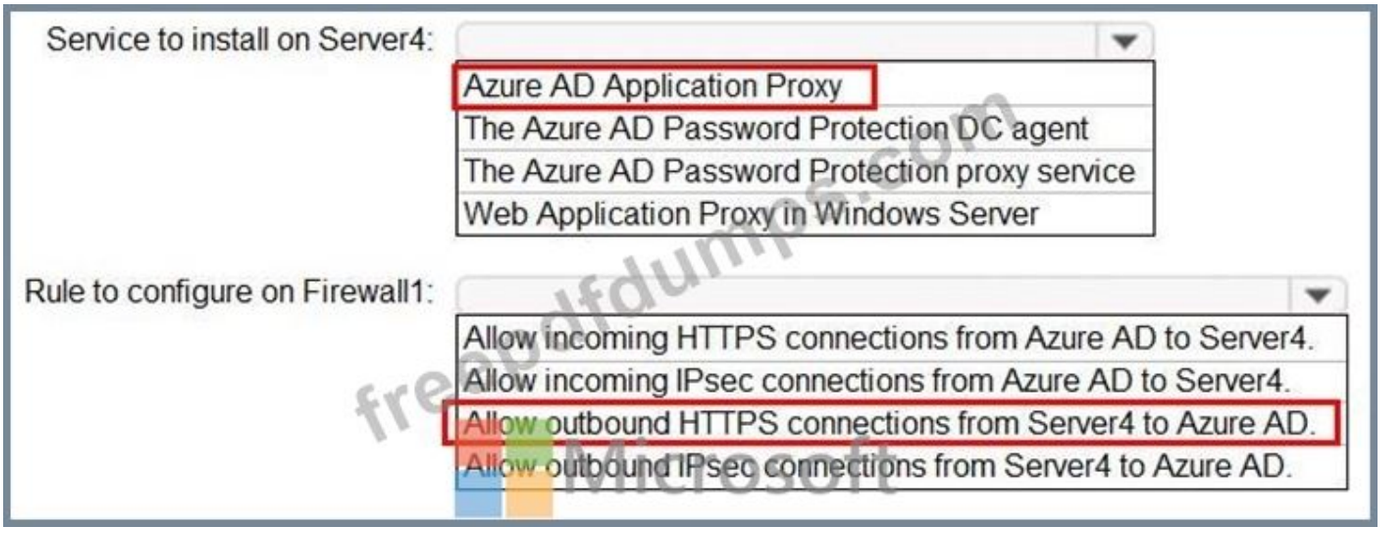
You have an on-premises datacenter that contains the hosts shown in the following table.

Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows Server 2019
Firewall1	Hardware firewall connected to the internet that blocks all traffic unless explicitly allowed

You have an Azure Active Directory (Azure AD) tenant that syncs to the Active Directory forest.
Multi-factor authentication (MFA) is enforced for Azure AD.
You need to ensure that you can publish App1 to Azure AD users.
What should you configure on Server and Firewall1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

NEW QUESTION: 21
You create a new Microsoft 365 E5 tenant.
You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).
What should you configure?
A. a sign-in risk policy
B. a user risk policy
C. an MFA registration policy
Answer: A (LEAVE A REPLY)

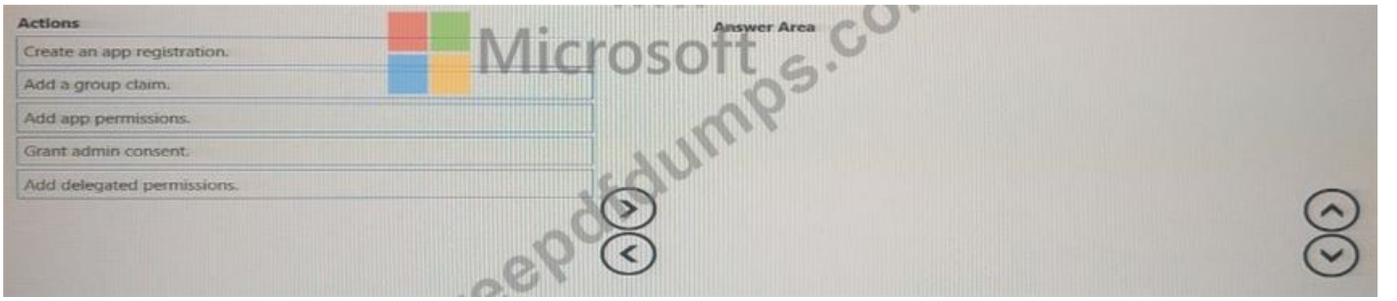
NEW QUESTION: 22

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

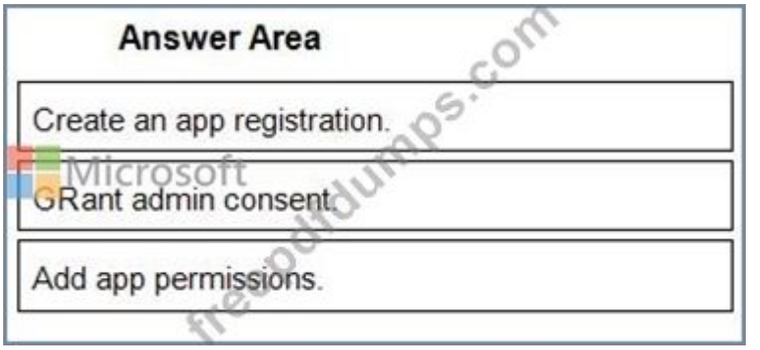
The company is developing a web service named App1.

You need to ensure that App1 can use Microsoft Graph to read directory data in contoso.com.

Which three actions should yon perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them In the correct order.



Answer:



1 - Create an app registration.

2 - GRant admin consent.

3 - Add app permissions.

Reference:

https://docs.microsoft.com/en-us/graph/auth/auth-concepts

NEW QUESTION: 23

You have an Azure AD tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

You have the locations shown in the following table.

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

The tenant contains a named location that Das the following configurations:

* Name: location1

* Mark as trusted location: Enabled

* IPv4 range: 10.10.0.0/16

MFA has a trusted iPad dress range of 193.17.17.0/24.

You have a Conditional Access policy that has the following settings:

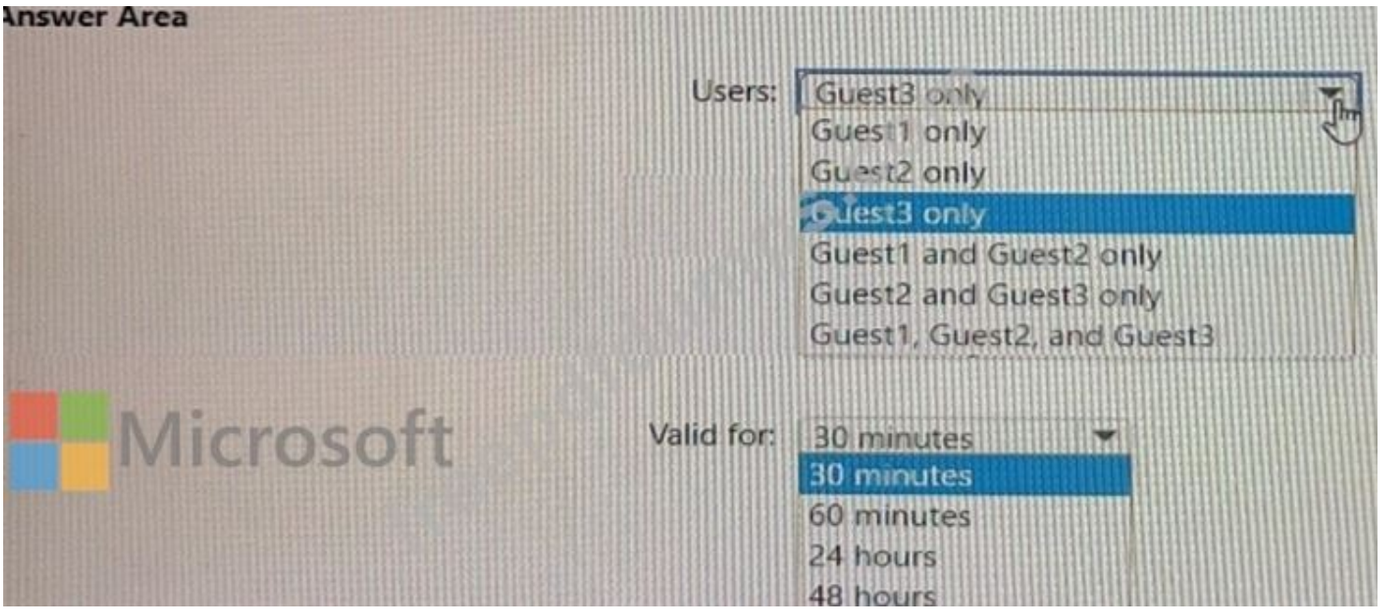
* Name: CAPolicy1
* Assignments
o Users or workload identities: Group 1
o Cloud apps or actions: All cloud apps
* Conditions
* Locations All trusted locations
* Access controls
o Gant
* Grant access: Require multi-factor authentication
Session: 0 controls selected
* Enable policy: On
For each of the following statements select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer:

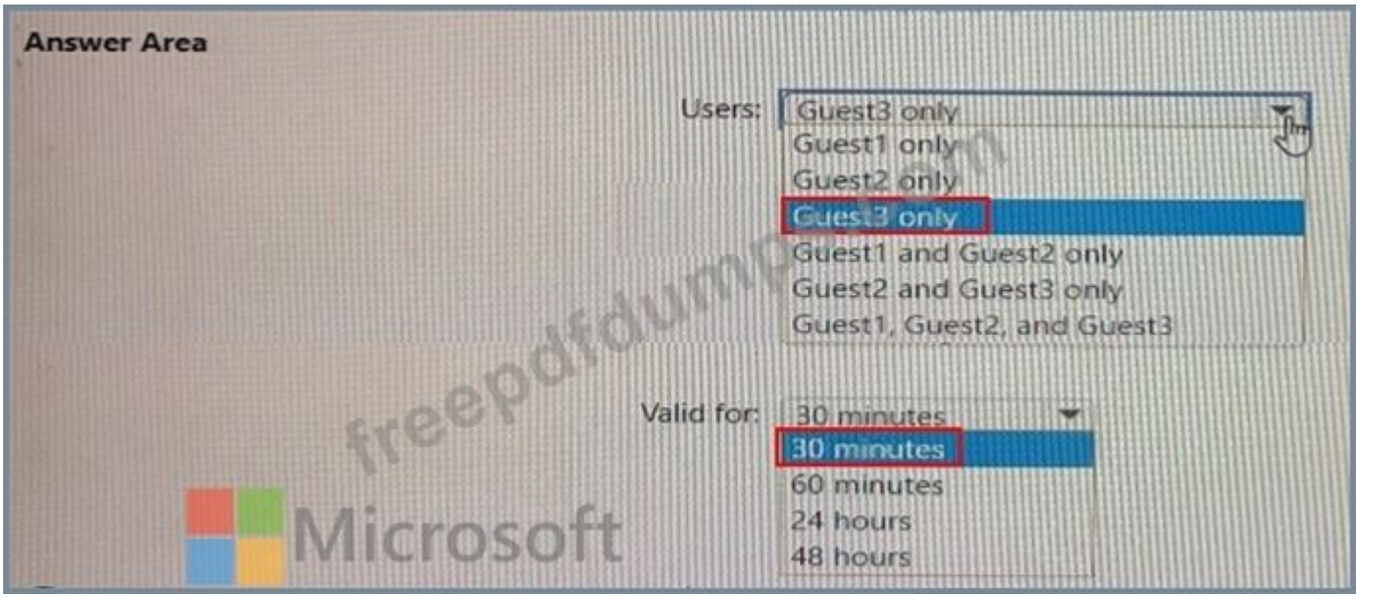
NEW QUESTION: 24
You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.
You invite the guest users shown in the following table.

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

Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

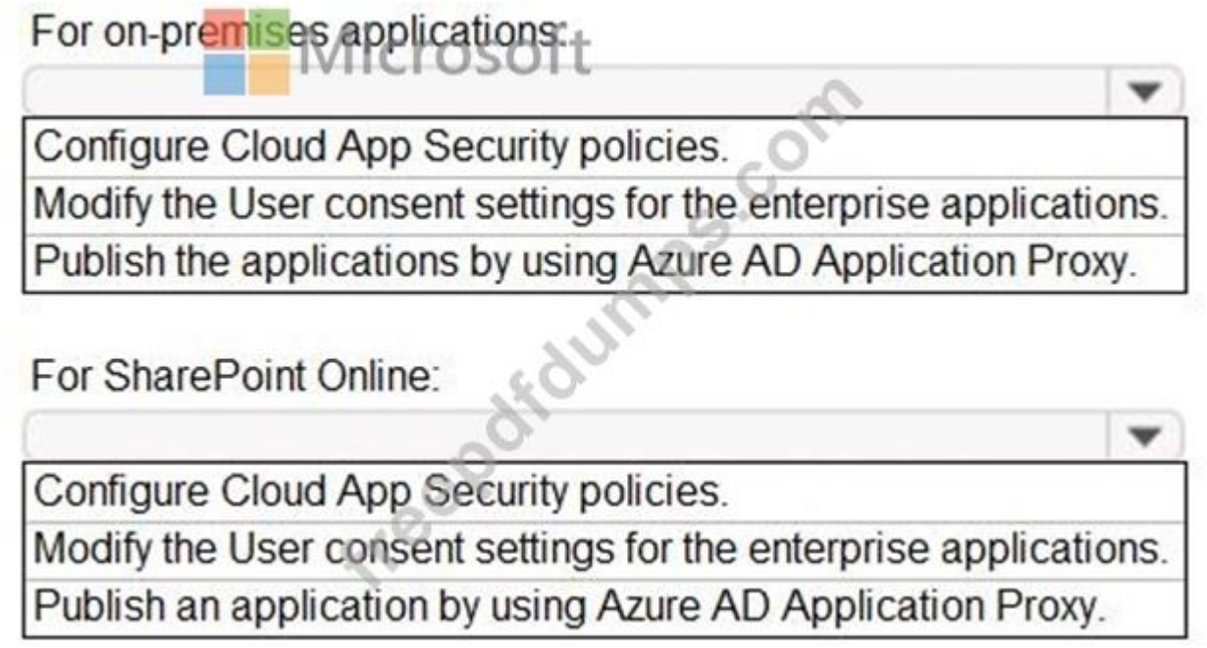


NEW QUESTION: 25

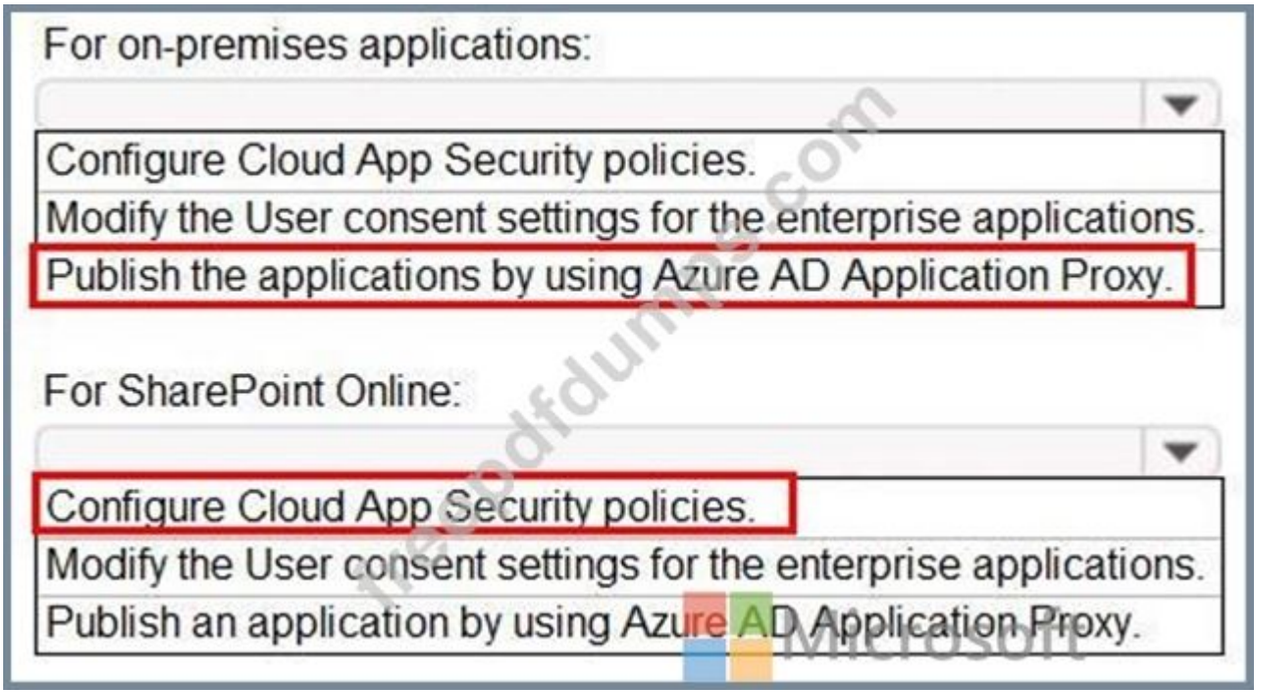
You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

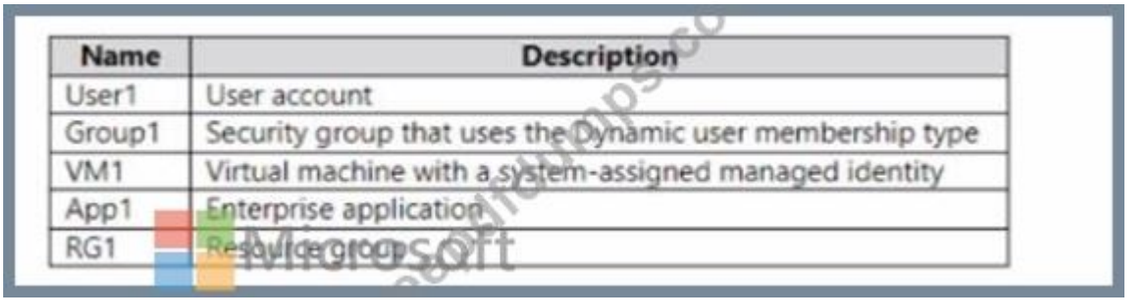


Answer:



NEW QUESTION: 26

You have the Azure resources show in the following table.



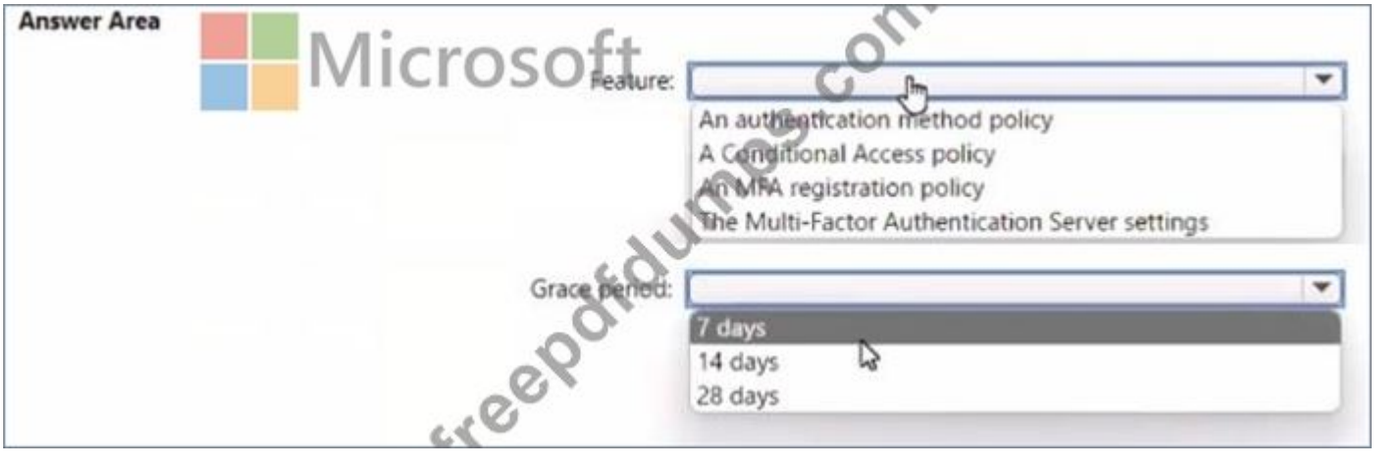
Name	Description
User1	User account
Group1	Security group that uses the Dynamic user membership type
VM1	Virtual machine with a system-assigned managed identity
App1	Enterprise application
RG1	Resource group

To Which identities can you assign the Contributor role for RG1?

A. User1, VM1, and App1 only

B. User1 and Group1 only
C. User1 only
D. User1, Group1, Vm1, and App1
E. User1 and VW1 only
Answer: D (LEAVE A REPLY)

NEW QUESTION: 27
You need to support the planned changes and meet the technical requirements for MFA.
Which feature should you use, and how long before the users must complete the registration? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

NEW QUESTION: 28
You need implement the planned changes for application access to organizational dat a. What should you configure?
A. access packages
B. authentication methods
C. an application proxy
D. the User consent settings
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.

The tenant-uses through authentication.

A corporate security policy states the following:

Domain controllers must never communicate directly to the internet.

Only required software must be- installed on servers.

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

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

You need to ensure that users can authenticate to Azure AD if a server fails.

On which server should you install an additional pass-through authentication agent?

A. Server2

B. Server4

C. Server1

D. Server3

Answer: B (LEAVE A REPLY)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start

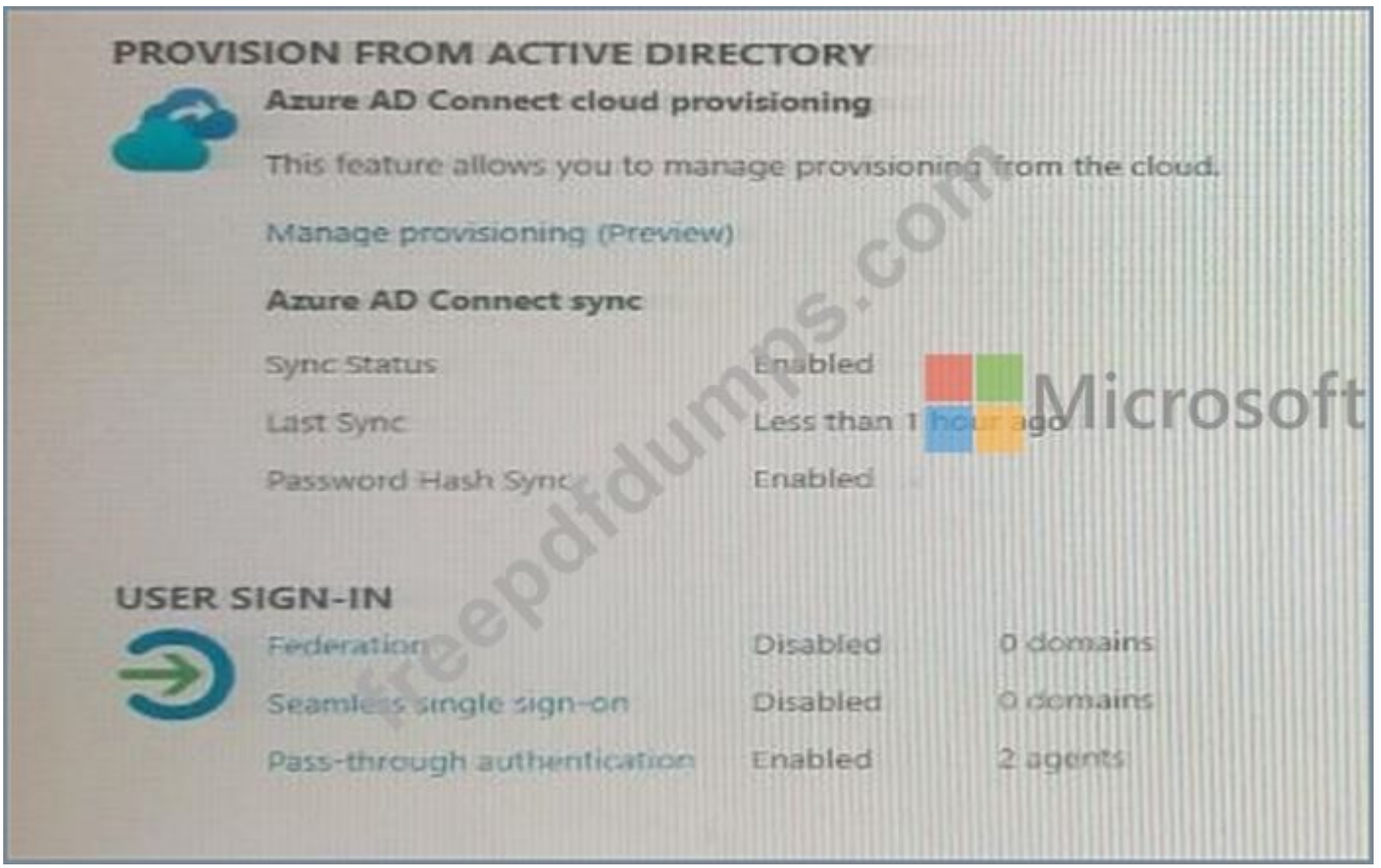
NEW QUESTION: 30

Your network contains an on-premises Active Directory domain that sync to an Azure Active Directory (Azure AD) tenant. The tenant contains the shown in the following table.

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

All the users work remotely.

Azure AD Connect is configured in Azure as shown in the following exhibit.



Connectivity from the on-premises domain to the internet is lost.

Which user can sign in to Azure AD?

A. User1, and User2 only

B. User1, User2, and User3

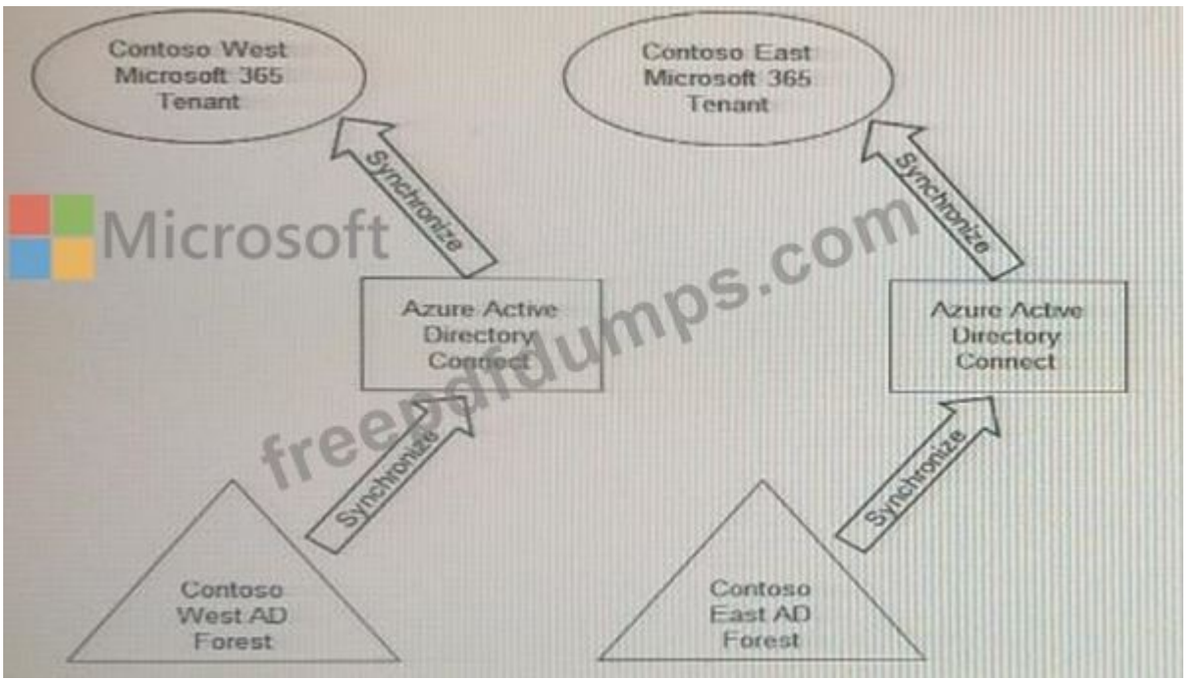
C. User1 only

D. User1 and User 3 only

Answer: D (LEAVE A REPLY)

NEW QUESTION: 31

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture tor both divisions is shown in the following exhibit.



You need to assign users from the Contoso East division access to Microsoft SharePoint Online sites in the Contoso West tenant. The solution must not require additional Microsoft 3G5 licenses.
What should you do?

A. Configure Azure AD Application Proxy in the Contoso West tenant.

B. Configure The exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.

C. Create guest accounts for all the Contoso East users in the West tenant.

D. Deploy a second Azure AD Connect server to Contoso East and configure the server to sync the Contoso East Active Directory forest to the Contoso West tenant.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 32

You have an Azure Active Directory (Azure AD) tenant that syncs to an Active Directory domain. The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).
You need to recommend a solution to provide Azure MFA for VPN connections.
What should you include in the recommendation?

A. a pass-through authentication proxy

B. Network Policy Server (NPS)
C. Azure AD Application Proxy
D. an Azure AD Password Protection proxy
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
You need to implement the planned changes for Package1. Which users can create and manage the access review?
A. User3 and User4
B. User3 only
C. User4and User5
D. User4 only
E. User3 and User5
F. User5 only
Answer: (SHOW ANSWER)

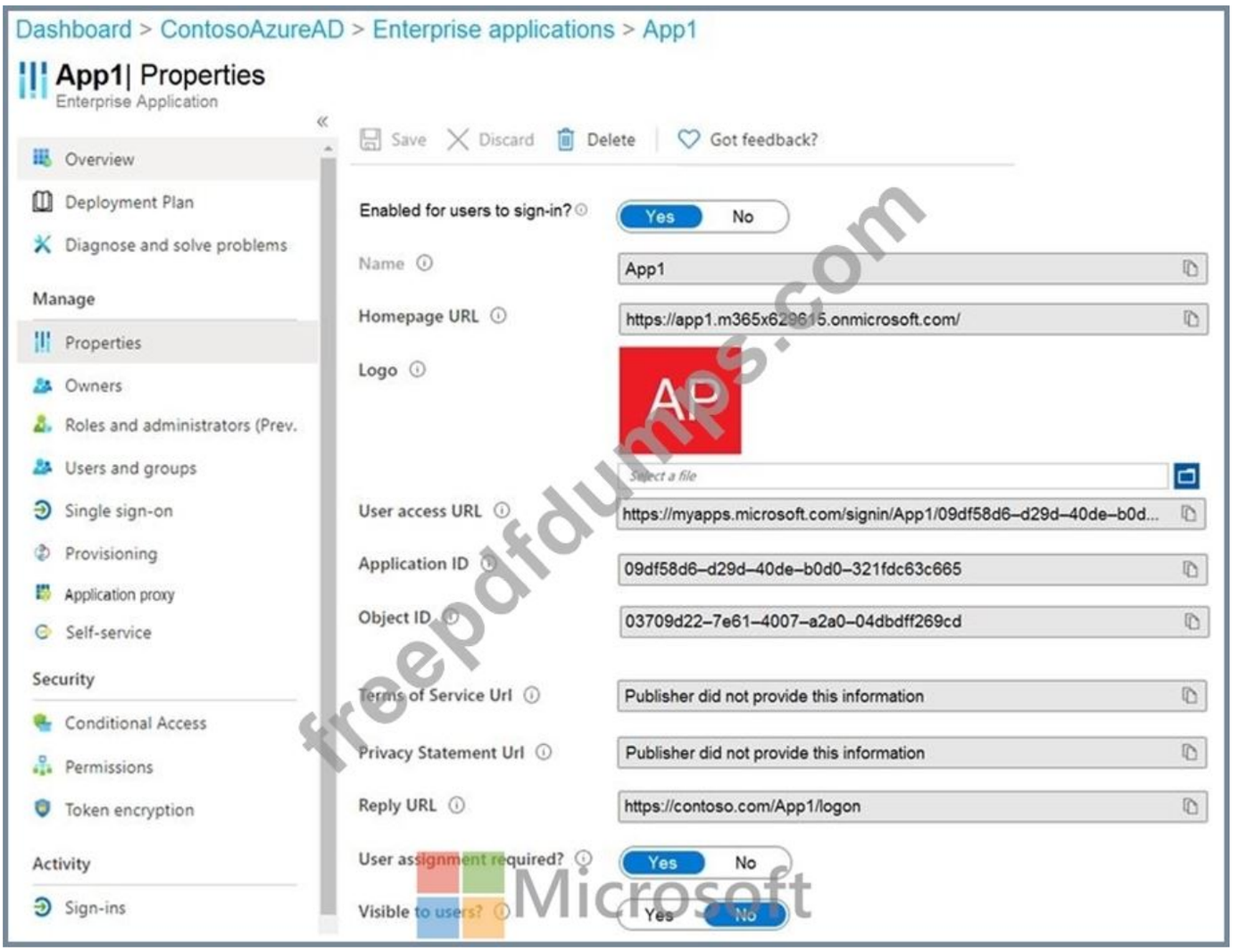
NEW QUESTION: 34
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 tenant.
All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.
Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.
You need to block the users automatically when they report an MFA request that they did not initiate.
Solution: From the Azure portal, you configure the Notifications settings for multi-factor authentication (MFA).
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

NEW QUESTION: 35

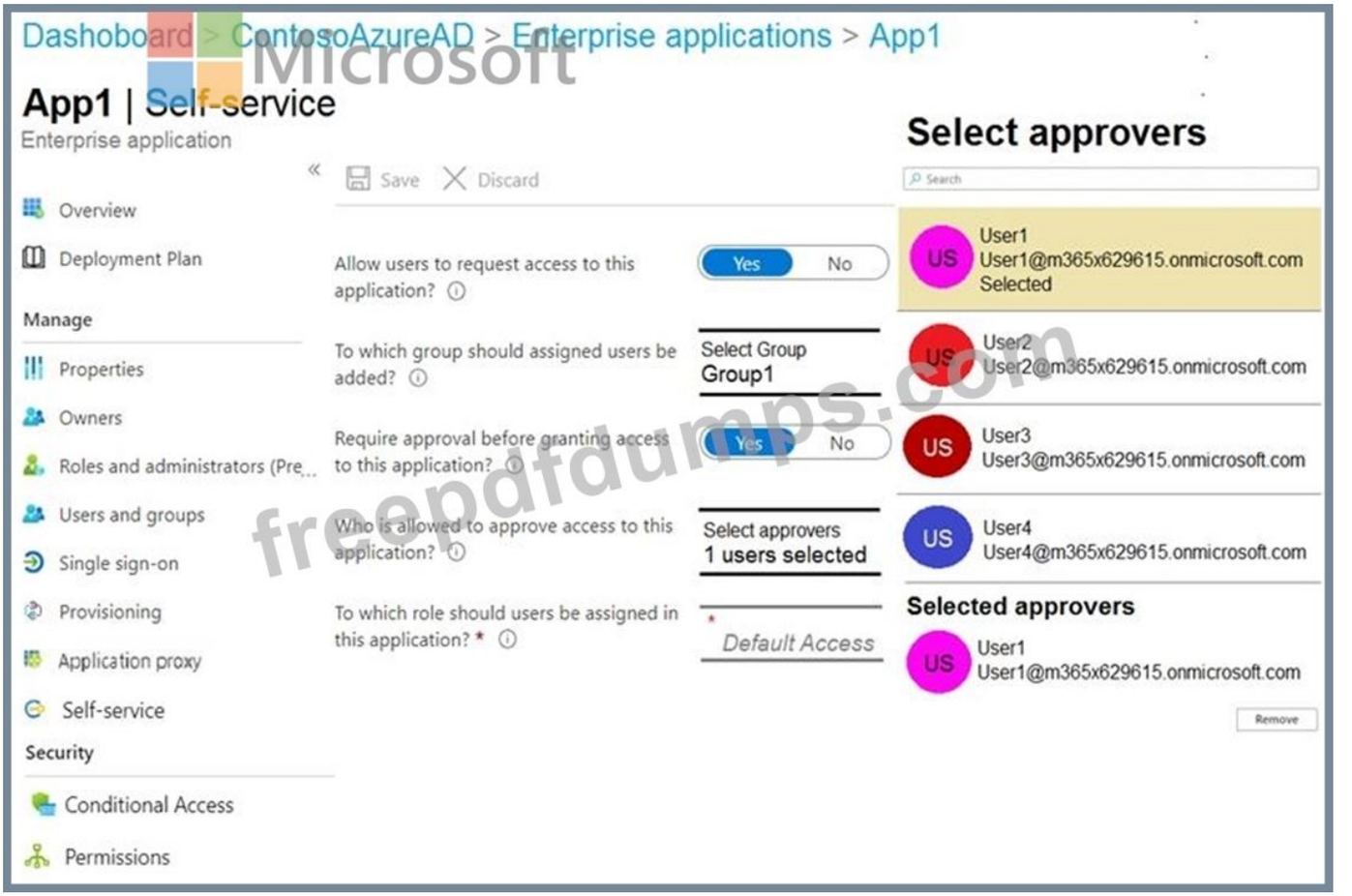
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have an Active Directory forest that syncs to an Azure Active Directory (Azure AD) tenant.
You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.
You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.
Solution: You configure Azure AD Password Protection.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)

NEW QUESTION: 36
You have a Microsoft 365 tenant that contains a group named Group1 as shown in the Group1 exhibit. (Click the Group1 tab.)

You create an enterprise application named App1 as shown in the App1 Properties exhibit. (Click the App1 Properties tab.)



You configure self-service for App1 as shown in the App1 Self-service exhibit. (Click the App1 Self-service tab.)



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

NOTE: Each correct selection is worth one point.

Answer:

Answer Area

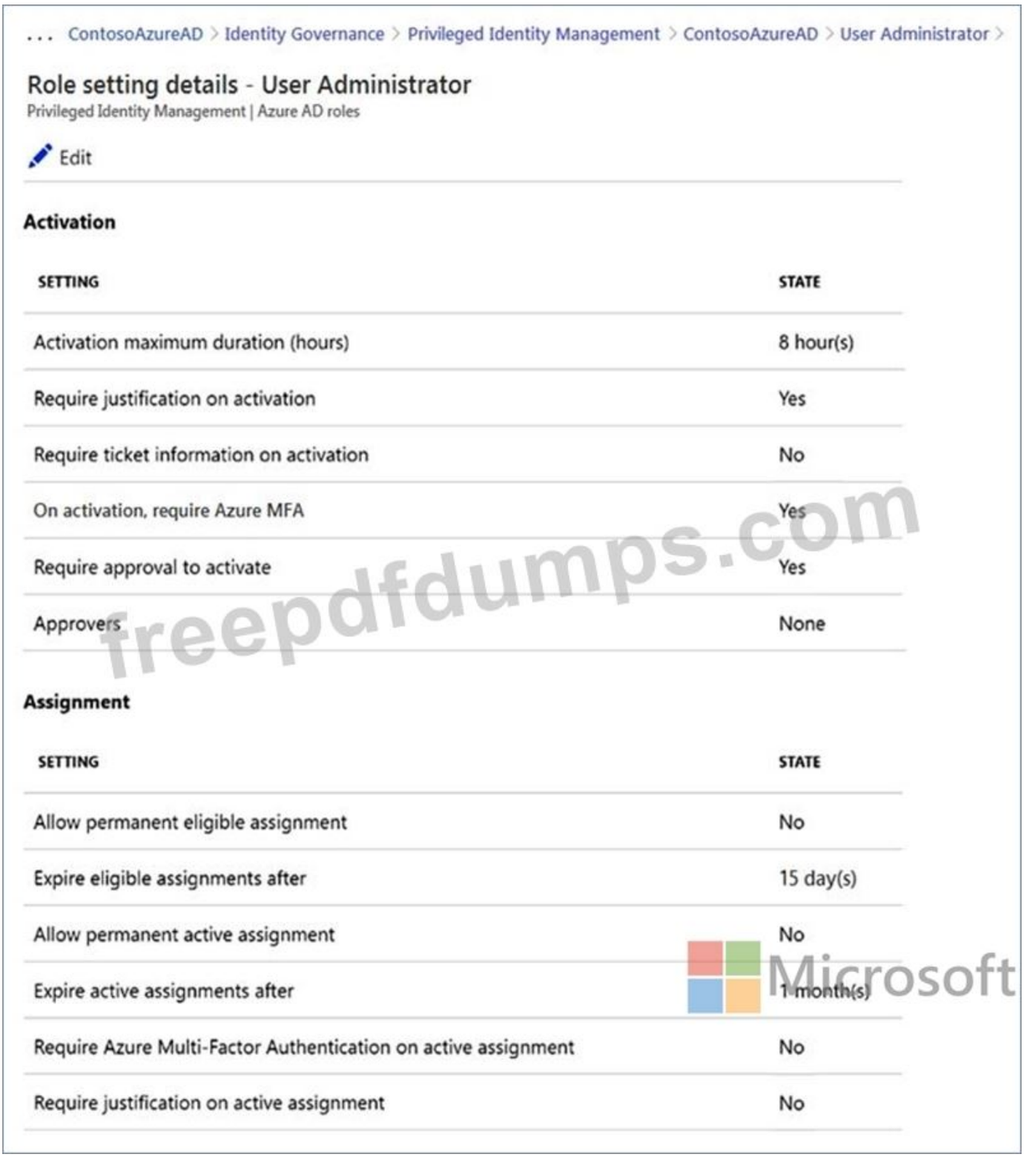
Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Reference

a) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal b) maybe https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage-groups c) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users

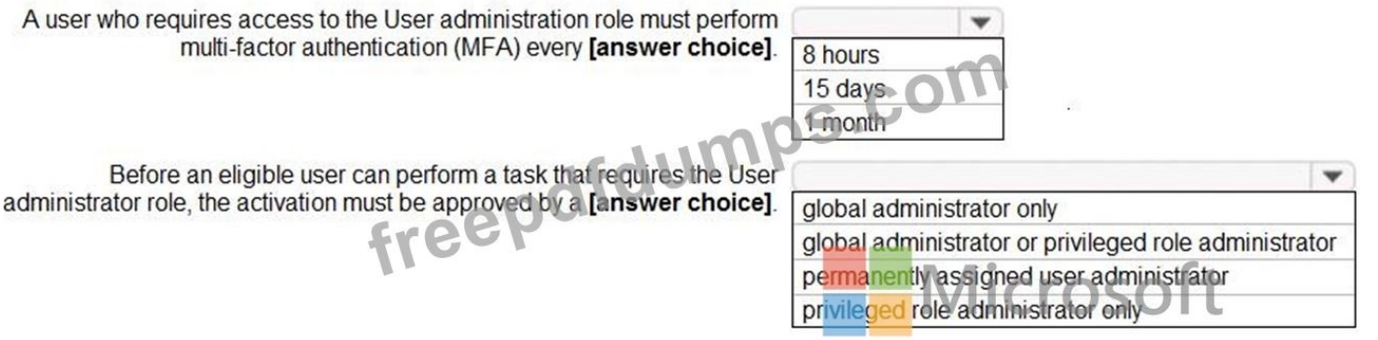
NEW QUESTION: 37

You have an Azure Active Directory (Azure AD) tenant that contains Azure AD Privileged Identity Management (PIM) role settings for the User administrator role as shown in the following exhibit.

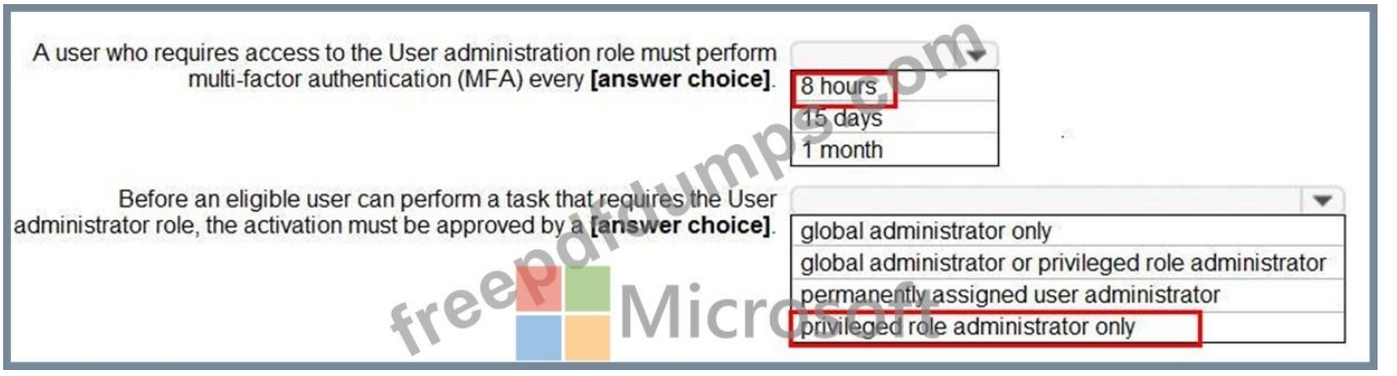


Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.



Answer:

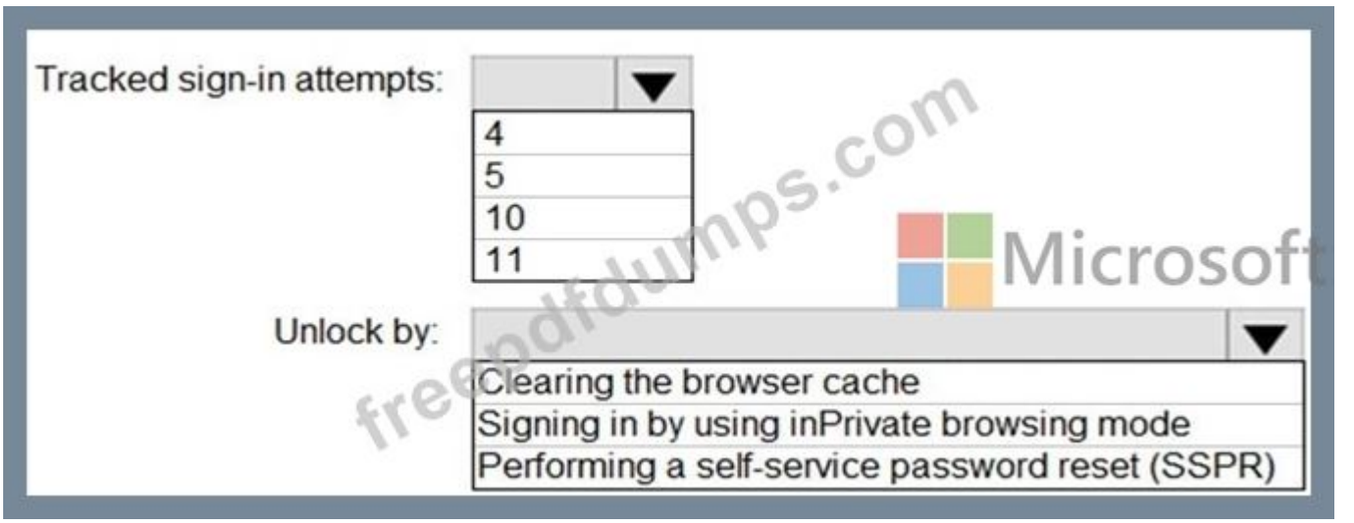


Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

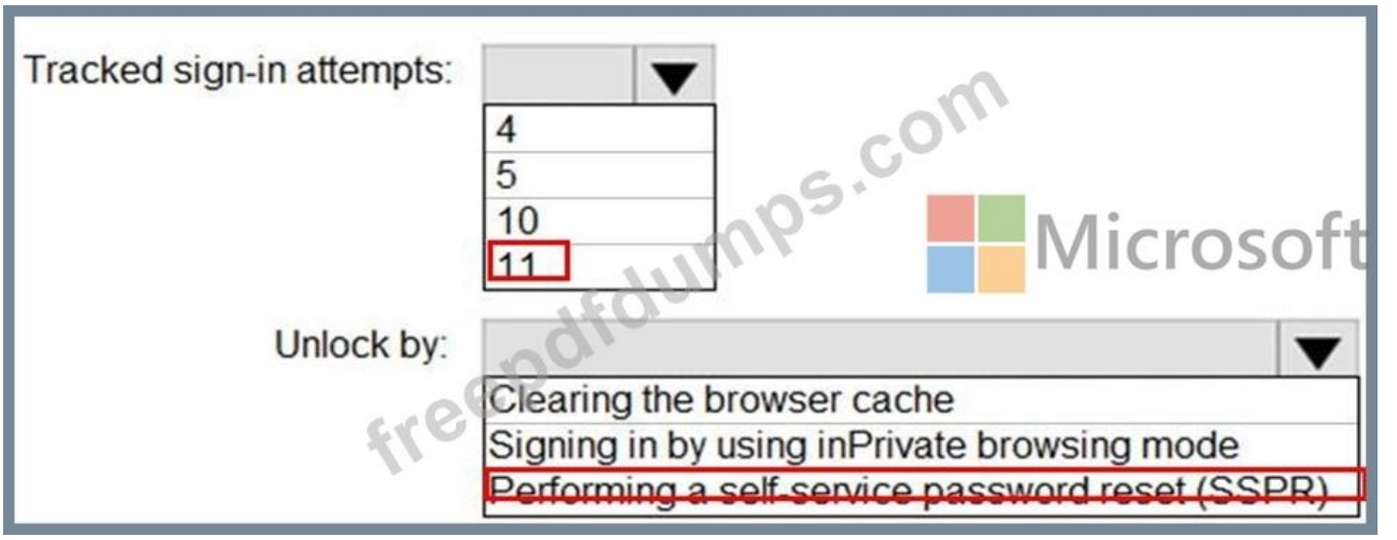
NEW QUESTION: 38

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:
Pa55w0rd12
Pa55w0rd12
Pa55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55word12
Pa55word12
Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.
What should identify? To answer, select the appropriate
NOTE: Each correct selection is worth one point.



Answer:



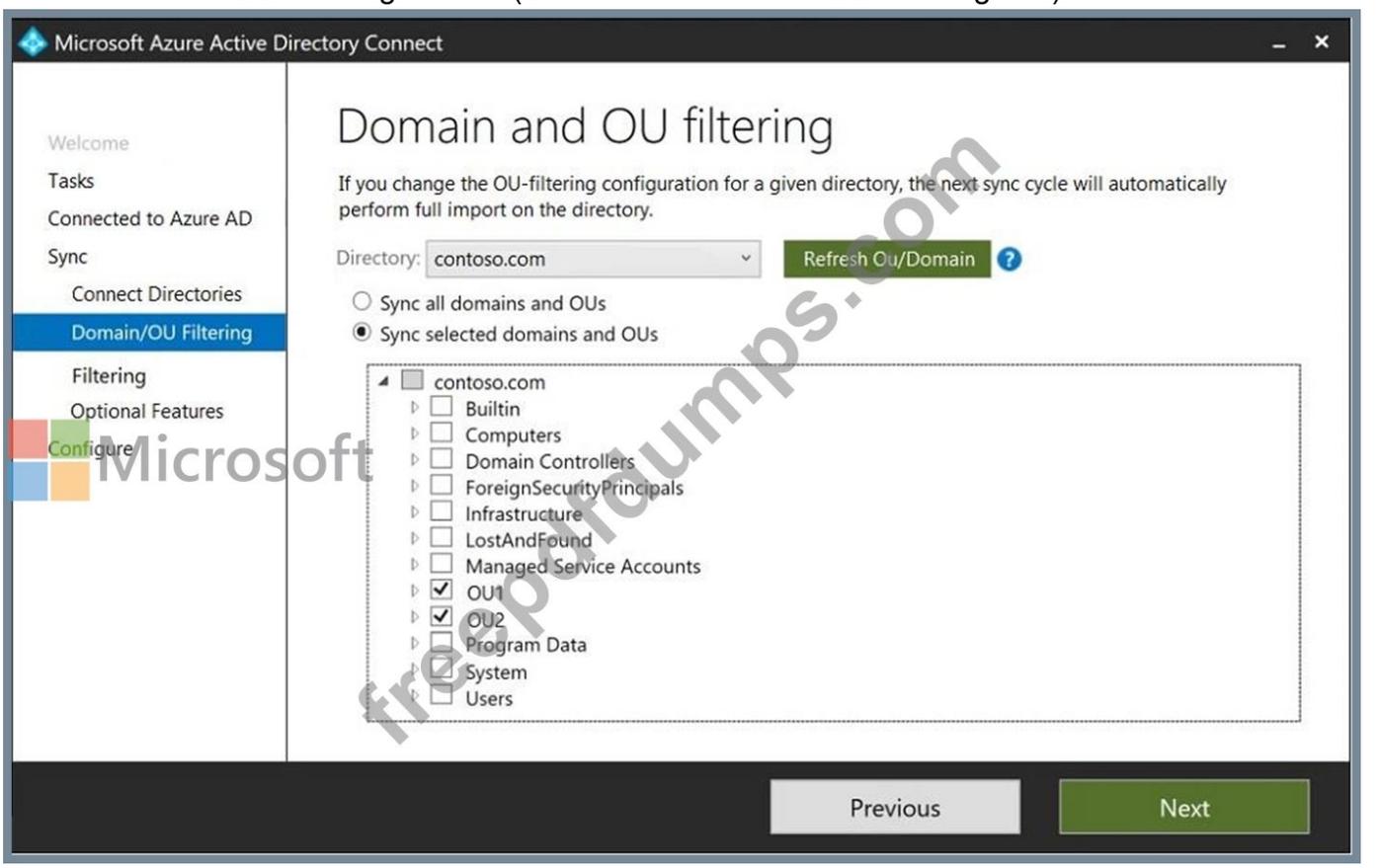
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

NEW QUESTION: 39

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the objects shown in the following table.

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.

You install Azure AD Connect. You configure the Domain and OU filtering settings as shown in the Domain and OU Filtering exhibit. (Click the Domain and OU Filtering tab.)

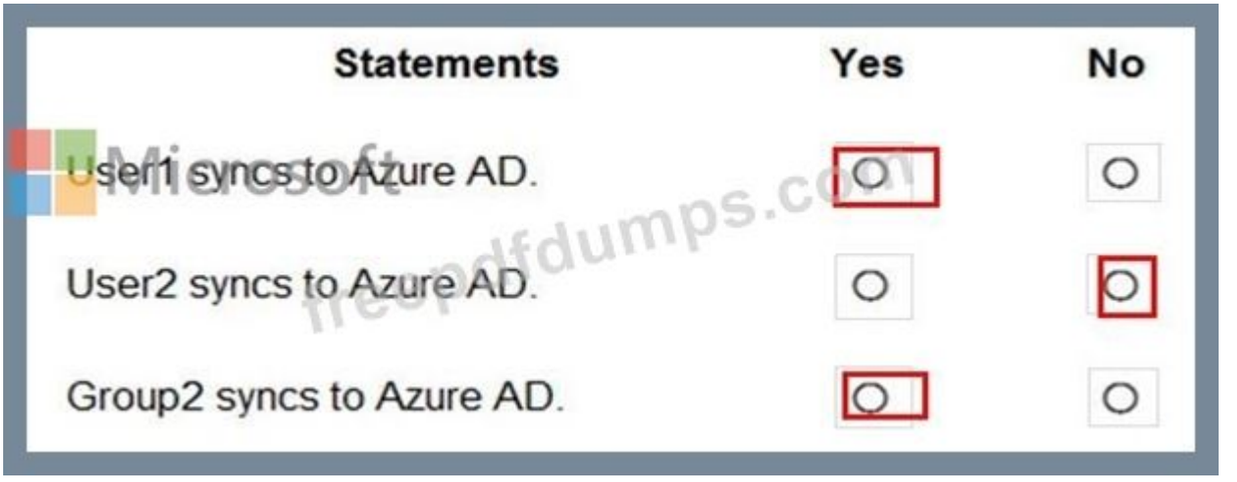


You configure the Filter users and devices settings as shown in the Filter Users and Devices exhibit. (Click the Filter Users and Devices tab.)

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

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:



Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

NEW QUESTION: 40
You have a Microsoft 365 ES subscription that contains a user named User1. User1 is eligible for the Application administrator role.
User1 needs to configure a new connector group for an application proxy.
What should you to activate the role for User1?
A. the Microsoft Defender for Cloud Apps portal
B. the Microsoft 365 Defender portal
C. the Microsoft 365 admin center
D. the Azure Active Directory admin center
Answer: D (LEAVE A REPLY)

NEW QUESTION: 41
Your company purchases 2 new Microsoft 365 ES subscription and an app named App.
You need to create a Microsoft Defender for Cloud Apps access policy for App1.
What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)
A. Configure a Token configuration for App1.
B. Add an API permission for App.

C. Configure a Conditional Access policy to use app-enforced restrictions.
D. Configure a Conditional Access policy to use Conditional Access App Control.
Answer: (SHOW ANSWER)
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

NEW QUESTION: 42
You have an Azure AD tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

Name	Type	Configuration
Risk1	User risk policy	Users that have a high severity risk must reset their password upon next sign-in.
User1	User	*Not applicable*

Azure Multi-Factor Authentication (MFA) is enabled for all users.
User1 triggers a medium severity alert that requires additional investigation.
You need to force User1 to reset his password the next time he signs in. the solution must minimize administrative effort.
What should you do?
A. Mark User1 as compromised.
B. Reset the Azure MFA registration for User1.
C. Reconfigure the user risk policy to trigger on medium or low severity.
D. Configure a sign-in risk policy.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
You create the Azure Active Directory (Azure AD) users shown in the following table.

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

On February 1, 2021, you configure the multi-factor authentication (MFA) settings as shown in the following exhibit.

The users authentication to Azure AD on their devices as shown in the following table.

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

On February 26, 2021, what will the multi-factor auth status be for each user?

A.

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

B.

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

C.

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

D.

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

Answer: (SHOW ANSWER)

NEW QUESTION: 44

You need to modify the settings of the User administrator role to meet the technical requirements.

Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

A. Set all assignments to Eligible

B. Modify the Expire eligible assignments after setting.

C. Select Require ticket information on activation.

D. Select Require justification on activation

E. Set all assignments to Active

Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 45

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.

A contractor uses the credentials of user1@outlook.com.

You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.

What should you do?

A. Run the New-AzADUser cmdlet.

B. Configure the External collaboration settings.

C. Add a WS-Fed identity provider.

D. Create a guest user account in contoso.com.

Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal

NEW QUESTION: 46
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You need to ensure that User1 can create new catalogs and add resources to the catalogs they own.
What should you do?
A. From the Roles and administrators blade, modify the Groups administrator role.
B. From the Identity Governance blade, modify the roles and administrators for the General catalog
C. From the identity Governance blade, modify the Entitlement management settings.
D. From the Roles and administrators blade, modify the Service support administrator role.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 47
You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements. What should you configure?
A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP

address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

NEW QUESTION: 48
You have an Azure Active Directory (Azure AD) tenant.
You create an enterprise application collection named HR Apps that has the following settings:
* Applications: Appl. App?, App3
* Owners: Admin 1
* Users and groups: HRUsers
AH three apps have the following Properties settings:
* Enabled for users to sign in: Yes
* User assignment required: Yes
* Visible to users: Yes
Users report that when they go to the My Apps portal, they only sue App1 and App2-You need to ensure that the users can also see App3. What should you do from App3?
What should you do from App3?
A. From Users and groups, add HRUsers.
B. Prom Properties, change User assignment required to No.
C. From Permissions, review the User consent permissions.
D. From Single sign on, configure a sign-on method.
Answer: A (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces

NEW QUESTION: 49
You have a Microsoft 365 tenant.
Sometimes, users use external, third-party applications that require limited access to the Microsoft 365 data of the respective user. The users register the applications in Azure Active Directory (Azure AD).
You need to receive an alert if a registered application gains read and write access to the users' email.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

Reference:
https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy

NEW QUESTION: 50
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

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

All the users work remotely.

Azure AD Connect is configured in Azure AD as shown in the following exhibit.

Connectivity from the on-premises domain to the internet is lost.

Which users can sign in to Azure AD?

A. User1 and User3 only

B. User1 only

C. User1, User2, and User3

D. User1 and User2 only

Answer: (SHOW ANSWER)

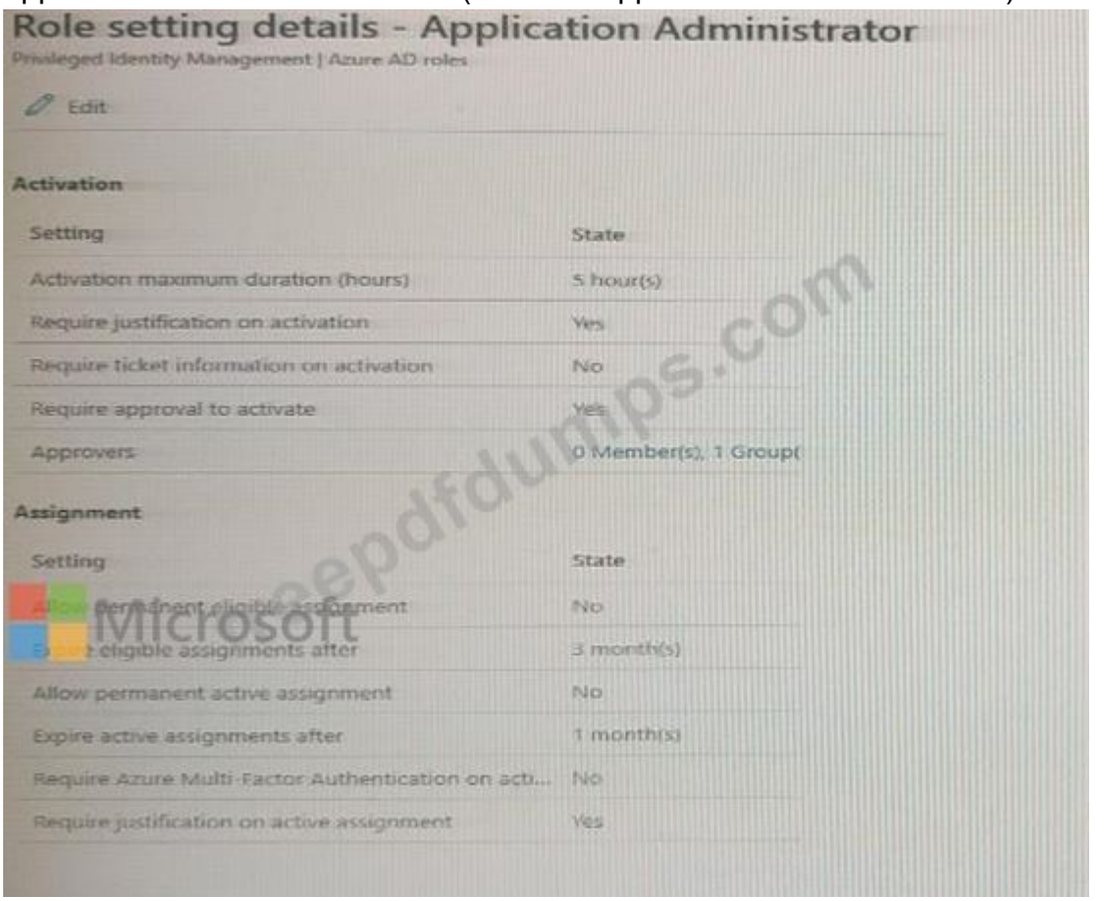
Reference:

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-current-limitations

NEW QUESTION: 51

You have an Azure Active Directory (Azure AD) tenant that contains three users named User1, User1, and User3, You create a group named Group1. You add User2 and User3 to Group1.

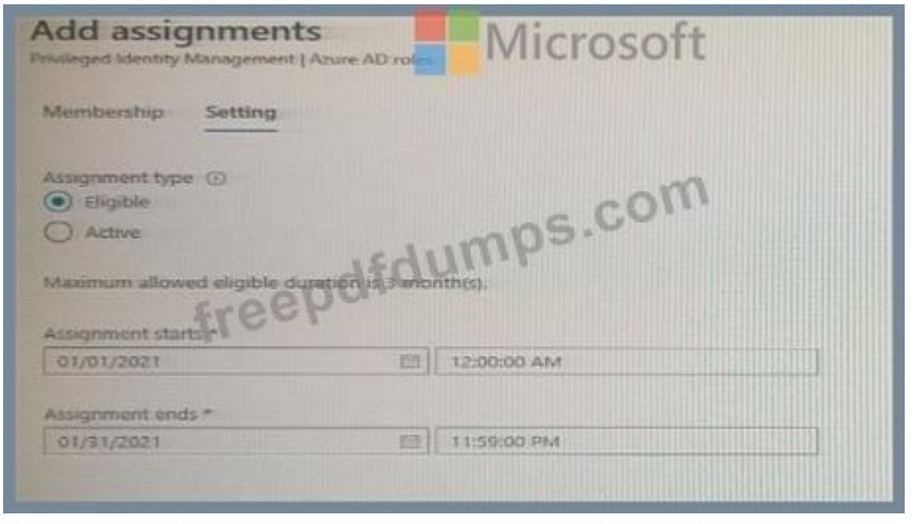
You configure a role in Azure AD Privileged identity Management (PIM) as shown in the application administrator exhibit. (Click the application Administrator tab.)



Group1 is configured as the approver for the application administrator role.

You configure User2to be eligible for the application administrator role.

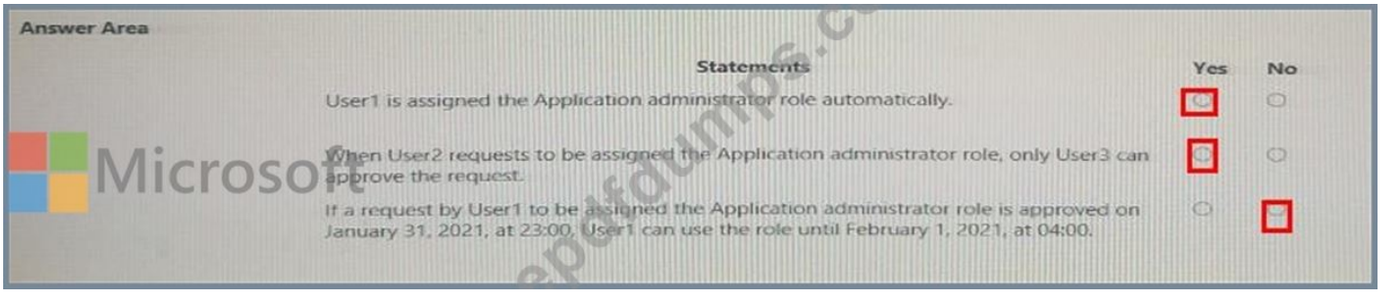
For User1, you add an assignment to the Application administrator role as shown in the Assignment exhibit. (Click Assignment tab)



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

NOTE: Each correct selection is worth one point.

Answer:



NEW QUESTION: 52

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.

You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.

You need to ensure that a new security administrator receives the alerts instead of you.

Solution: From Azure AD, you modify the Diagnostics settings.

Does this meet the goal?

A. No

B. Yes

Answer: (SHOW ANSWER)

NEW QUESTION: 53

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain.

The domain contains the servers shown in the following table.

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

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

You deploy a new server named Server4 that runs Windows Server 2019.

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.
What should you implement on Server4?
A. Azure AD Connect
B. Azure AD Application Proxy
C. Password Change Notification Service (PCNS)
D. the Azure AD Password Protection proxy service
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesdeploy

NEW QUESTION: 54
You have a Microsoft 365 E5 subscription that contains a web app named App1.
Guest users are regularly granted access to App1.
You need to ensure that the guest users that have NOT accessed App1 during the past 30 days have their access removed the solution must minimize administrative effort.
What should you configure?
A. a guest access review
B. a Conditional Access policy
C. a compliance policy
D. an access review for application access
Answer: (SHOW ANSWER)

NEW QUESTION: 55
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it as a result these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of identity Secure Score improvement actions.
Solution: You assign the SharePoint Administrator role to User1
Does this meet the goal?
A. No
B. Yes
Answer: (SHOW ANSWER)

NEW QUESTION: 56

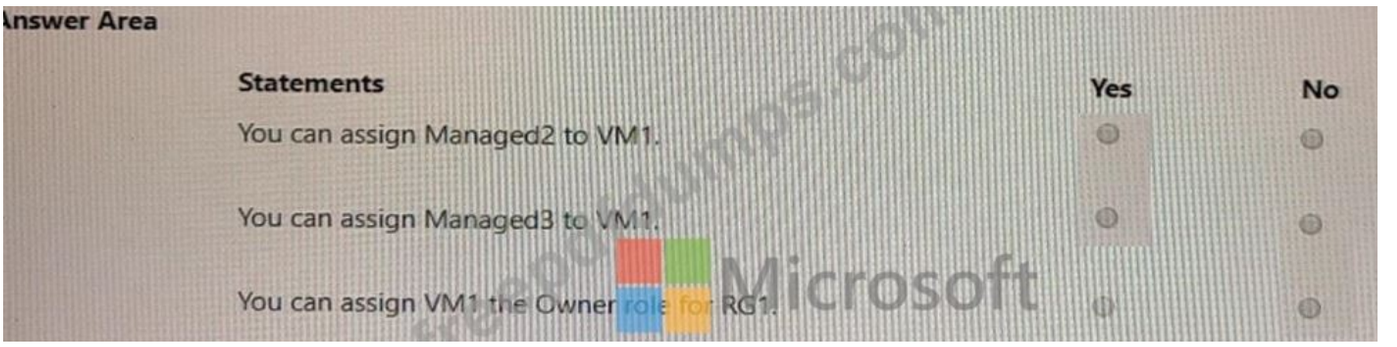
You have an Azure AD tenant named Contoso that contains a terms of use (ToU) named Terms1 and an access package. Contoso users collaborate with an external organization named Fabrikam. Fabrikam users must accept Terms1 before being allowed to use the access package.
You need to identify which users accepted or declined Terms1.
What should you use?
A. the Usage and Insights report
B. provisioning logs
C. audit logs
D. sign-in logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you create an assignment for the Insights at administrator role.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

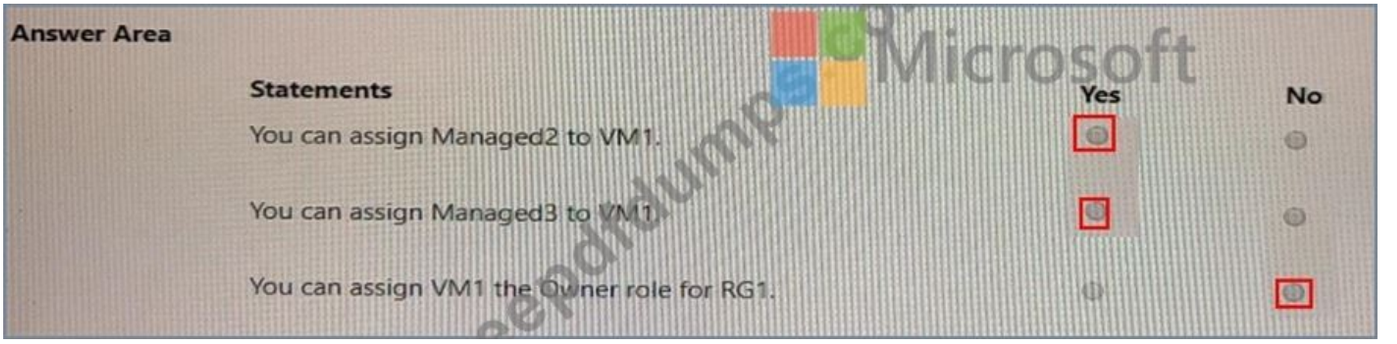
NEW QUESTION: 58
You have an Azure subscription that contains the following virtual machine Name: VM1 Azure region: East US System-assigned managed identity: Disabled You create the managed identities shown in the following table.

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

You perform the following actions:
* Assign Managed1 to VM1.
* Create a resource group named RG1 in the West US region.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer:



NEW QUESTION: 59

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

You create an access review for Group1 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

You create an access review for Group2 as shown in the following table.

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

What is the minimum number of Azure AD Premium P2 licenses required for each group? To answer, select the appropriate options in the answer are a. NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area

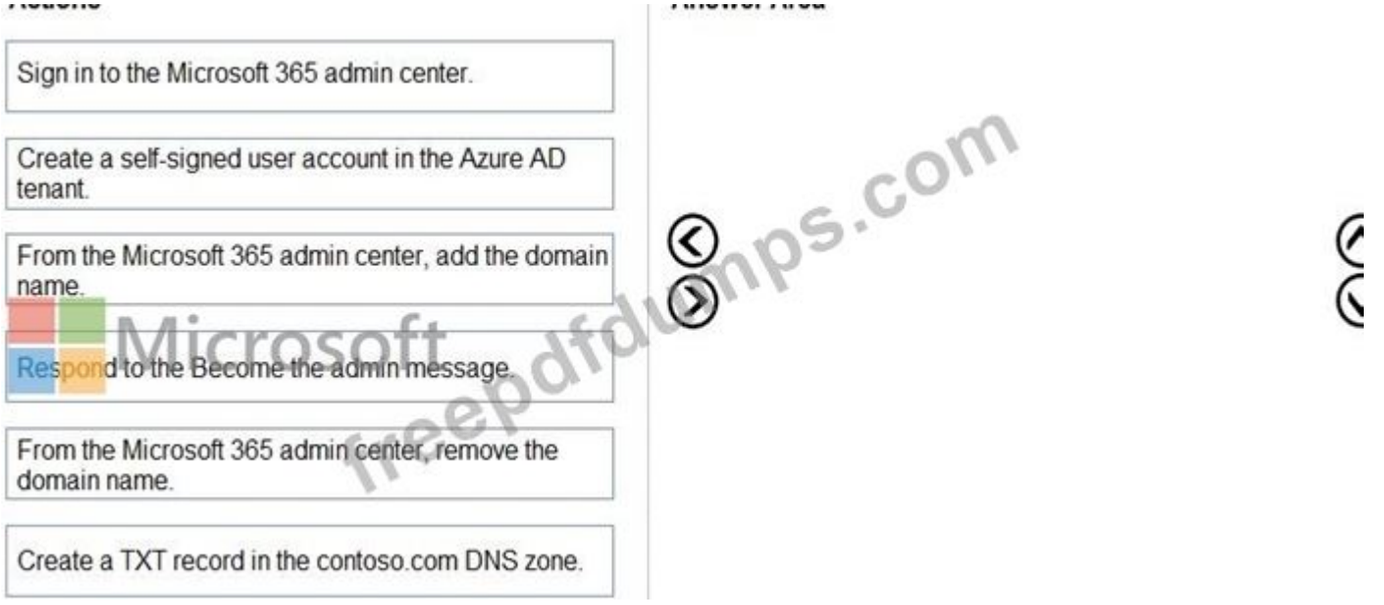
NEW QUESTION: 60

You have an on-premises Microsoft Exchange organization that uses an SMTP address space of contoso.com.

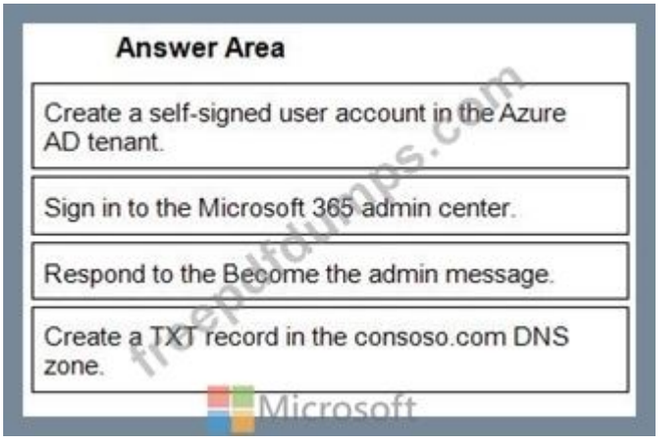
You discover that users use their email address for self-service sign-up to Microsoft 365 services.

You need to gain global administrator privileges to the Azure Active Directory (Azure AD) tenant that contains the self-signed users.

Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



1 - Create a self-signed user account in the Azure AD tenant.
2 - Sign in to the Microsoft 365 admin center.
3 - Respond to the Become the admin message.
4 - Create a TXT record in the consoso.com DNS zone.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

NEW QUESTION: 61
Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).
While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.
You need to ensure that the IT department users only have access to the Security administrator role when required.
What should you configure for the Security administrator role assignment?
A. Expire eligible assignments after from the Role settings details
B. Expire active assignments after from the Role settings details
C. Assignment type to Active

D. Assignment type to Eligible
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

NEW QUESTION: 62
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains an Azure AD enterprise application named App1.
A contractor uses the credentials of user1@outlook.com.
You need to ensure that you can provide the contractor with access to App1. The contractor must be able to authenticate as user1@outlook.com.
What should you do?
A. Run the New-AzureADMSInvitation cmdlet.
B. Configure the External collaboration settings.
C. Add a WS-Fed identity provider.
D. Implement Azure AD Connect.
Answer: (SHOW ANSWER)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

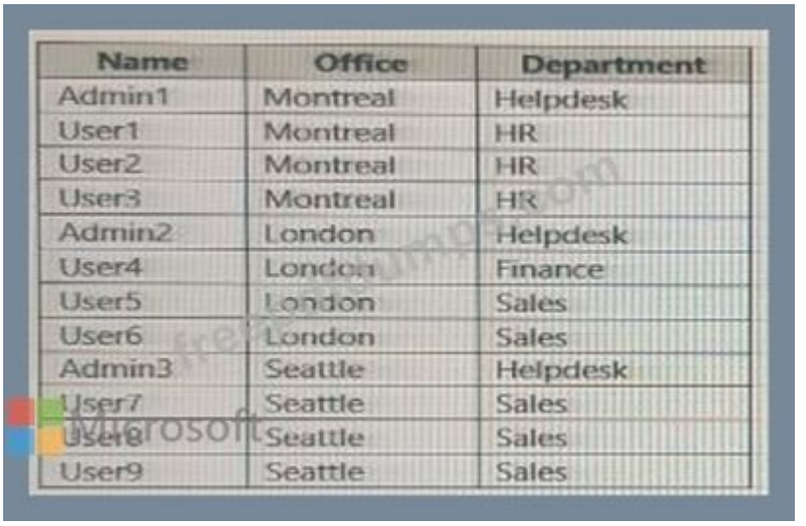
NEW QUESTION: 63
Your company has a Microsoft 365 tenant.
The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.
The users are prohibited from having a mobile phone in the call center.
You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?
A. a named network location
B. the Microsoft Authenticator app
C. Windows Hello for Business authentication
D. FIDO2 tokens
Answer: D (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

NEW QUESTION: 64
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
You receive more than 100 email alerts each day for failed Azure AD user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure AD, you modify the Diagnostics settings.
Does this meet the goal?
A. Yes
B. No
Answer: (SHOW ANSWER)
Topic 3, Overview
A Datum Environment
The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
The tenant contains the users shown in the following table.
Problem Statements
* Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
* 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 the maximum number of devices that can be joined or registered to Azure AD to 10.
Technical Requirements
* Users assigned the User administrator role must be able to request permission to use the role 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 methods 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: 65
You need to meet the planned changes for the User administrator role.
What should you do?
A. Create an access review.
B. Modify Role settings
C. Create an administrator unit.
D. Modify Active Assignments.
Answer: D (LEAVE A REPLY)
Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles Default Setting State Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No Approvers None
Topic 1, Contoso, Ltd
Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces OU contains all users and computers.
The Contoso.com Active Directory domain contains the users shown in the following table.



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

Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named Contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS). Only the Contoso Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses, All user have all licenses assigned besides following exception:

The users in the London office have the Microsoft 365 admin center to manually assign licenses.

All user have licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System License unassigned.

The users in the Seattle office have the Yammer Enterprise License unassigned.

Security defaults are disabled for Contoso.com.

Contoso uses Azure AD Privileged identity Management (PIM) to project administrator roles.

Problem Statements

Contoso identifies the following issues:

* Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.

* The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.

* The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.

* Currently, the helpdesk administrators can perform tasks by using the: User administrator role without justification or approval.

* When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Planned Changes

Contoso plans to implement the following changes.
Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor-Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign. Configure the User administrator role to require justification and approval to activate.
Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.
Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.
Technical Requirements
Contoso identifies the following technical requirements:
* AH users must be synced from AD DS to the contoso.com Azure AD tenant.
* App1 must have a redirect URI pointed to https://contoso.com/auth-response.
* License allocation for new users must be assigned automatically based on the location of the user.
* Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
* Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
* The helpdesk administrators must be able to manage licenses for only the users in their respective office.
* Users must be forced to change their password if there is a probability that the users' identity was compromised.

NEW QUESTION: 66
You have an Azure AD tenant
You open the risk detections report.
Which risk detection type is classified as a user risk?
A. unfamiliar sign-in properties
B. password spray
C. Azure AD threat intelligence
D. anonymous IP address
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
You have an Azure subscription that contains the resources shown in the following table.

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

For which resources can you create an access review?

A. Group1, App1, Contributor, and Role1

B. Hotel and Contributor only

C. Group1, Role1, and Contributor only

D. Group1 only

Answer: A (LEAVE A REPLY)

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

NEW QUESTION: 68

You have a Microsoft 365 tenant.

You need to identify users who have leaked credentials. The solution must meet the following requirements.

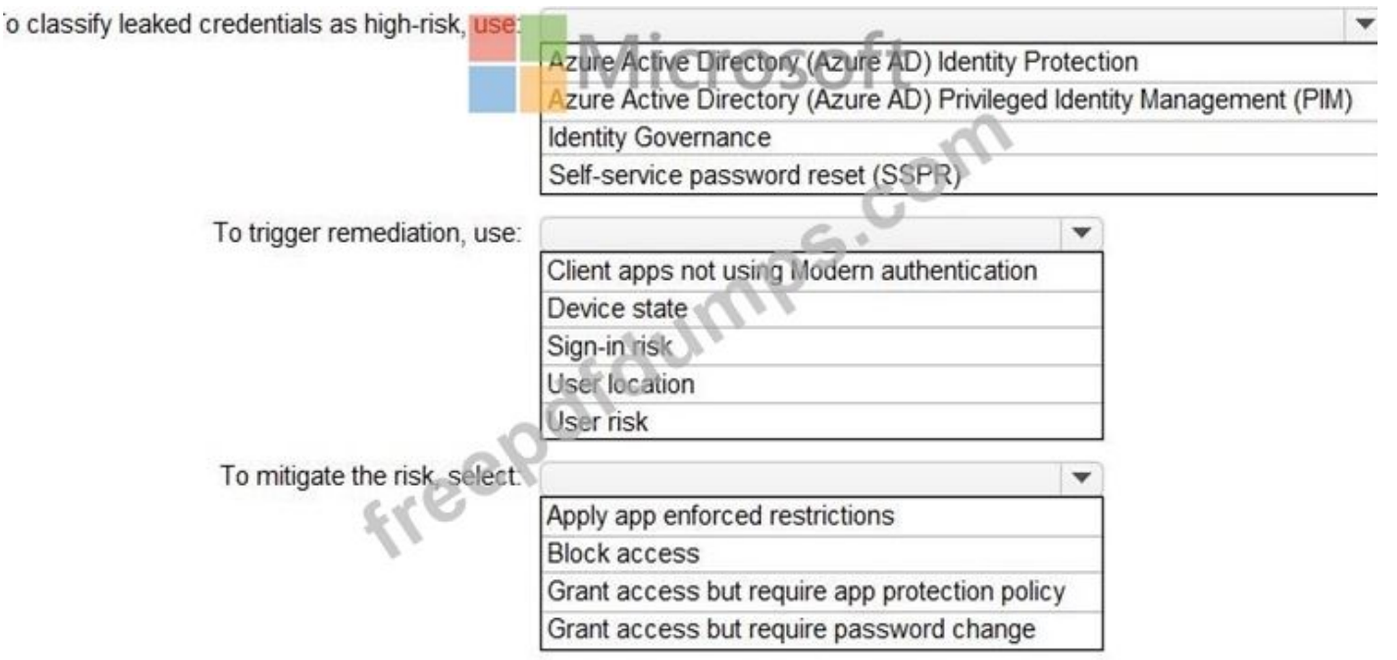
* Identity sign-Ins by users who ate suspected of having leaked credentials.

* Rag the sign-ins as a high risk event.

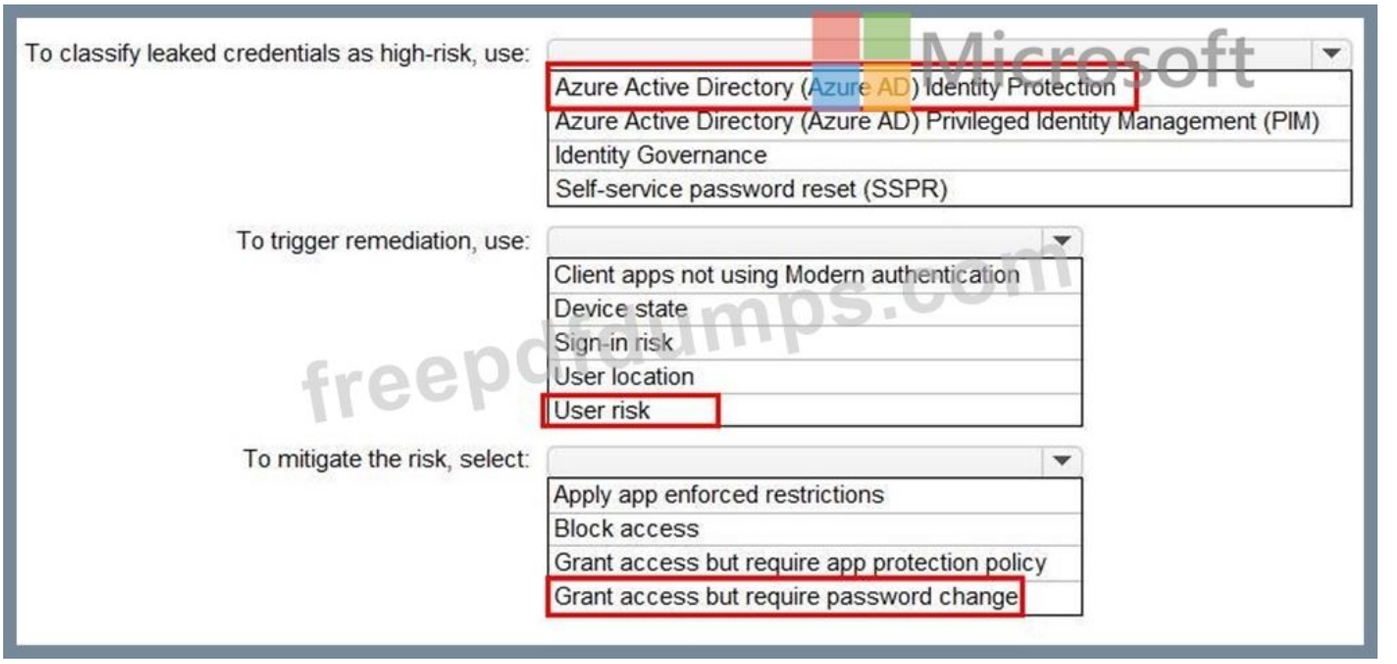
* Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

What should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



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

NEW QUESTION: 69

You need to create the LWGroup1 group to meet the management requirements.
How should you complete the dynamic membership rule? To answer, drag the appropriate values to the correct targets. Each value may be used once, more than once, or not at all. You many need to drag the split bar between panes or scroll to view content.
NOTE: Each correct selection is worth one point.

Answer:

NEW QUESTION: 70

You have an Azure AD tenant

You configure User consent settings to allow users to provide consent to apps from verified publishers.

You need to ensure that the users can only provide consent to apps that require low impact permissions.

What should you do?

A. Create an access package.

B. Configure permission classifications.

C. Create an enterprise application collection.

D. Create an access review.

Answer: (SHOW ANSWER)

NEW QUESTION: 71

You configure a new Microsoft 365 tenant to use a default domain name of contoso.com.

You need to ensure that you can control access to Microsoft 365 resources by using conditional access policies.

What should you do first?

A. Disable the User consent settings.

B. Disable Security defaults.

C. Configure a multi-factor authentication (MFA) registration policy.

D. Configure password protection for Windows Server Active Directory.

Answer: (SHOW ANSWER)

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults

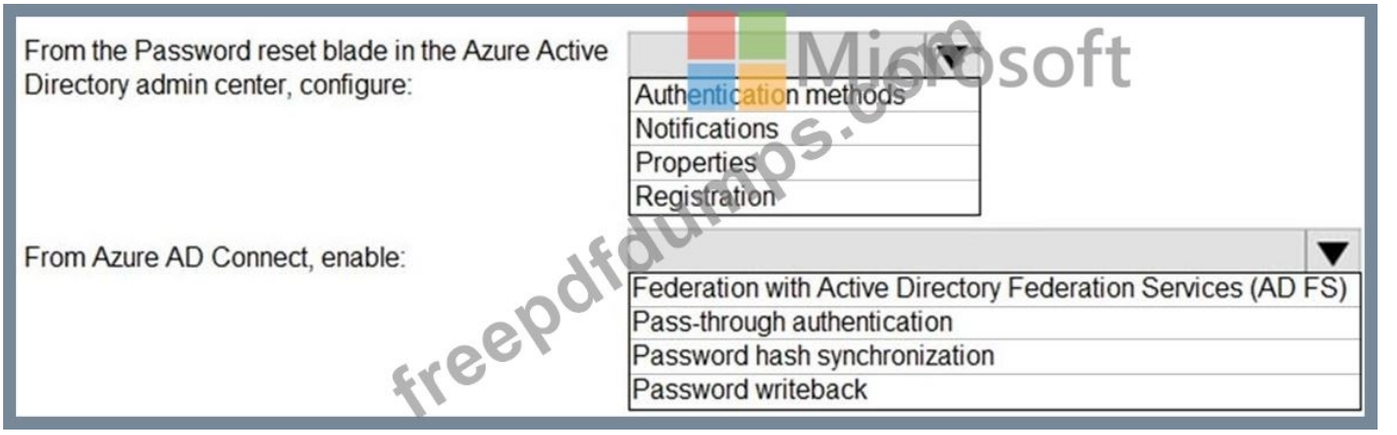
NEW QUESTION: 72

You have a Microsoft 365 tenant.

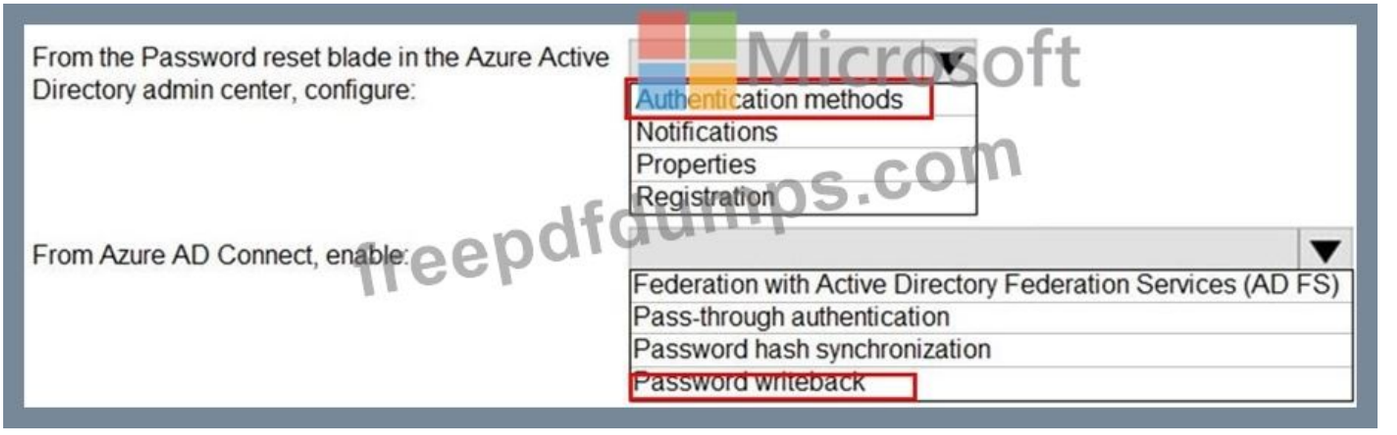
In Azure Active Directory (Azure AD), you configure the terms of use.

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.
What should you configure?
A. an access policy in Microsoft Cloud App Security.
B. Terms and conditions in Microsoft Endpoint Manager.
C. a conditional access policy in Azure AD
D. a compliance policy in Microsoft Endpoint Manager
Answer: C (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

NEW QUESTION: 73
You have a Microsoft 365 tenant and an Active Directory domain named adatum.com.
You deploy Azure AD Connect by using the Express Settings.
You need to configure self-service password reset (SSPR) to meet the following requirements:
When users reset their password, they must be prompted to respond to a mobile app notification or answer three predefined security questions.
Passwords must be synced between the tenant and the domain regardless of where the password was reset.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



Reference:

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-security-questions

NEW QUESTION: 74

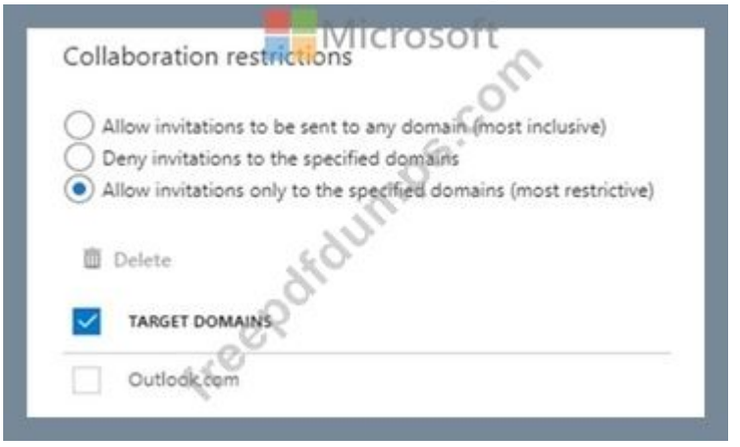
You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

Users are invited to collaborate with contoso.com as shown in the following table.

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

From the External collaboration settings in the Azure Active Directory admin center, you configure the Collaboration restrictions settings as shown in the following exhibit.



From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can 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.	○	○

NEW QUESTION: 75
You have an Azure Active Directory (Azure Azure) tenant that contains the objects shown in the following table.
* A device named Device1
* Users named User1, User2, User3, User4, and User5
* Five groups named Group1, Group2, Group3, Ciroup4, and Group5
The groups are configured as shown in the following table.

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

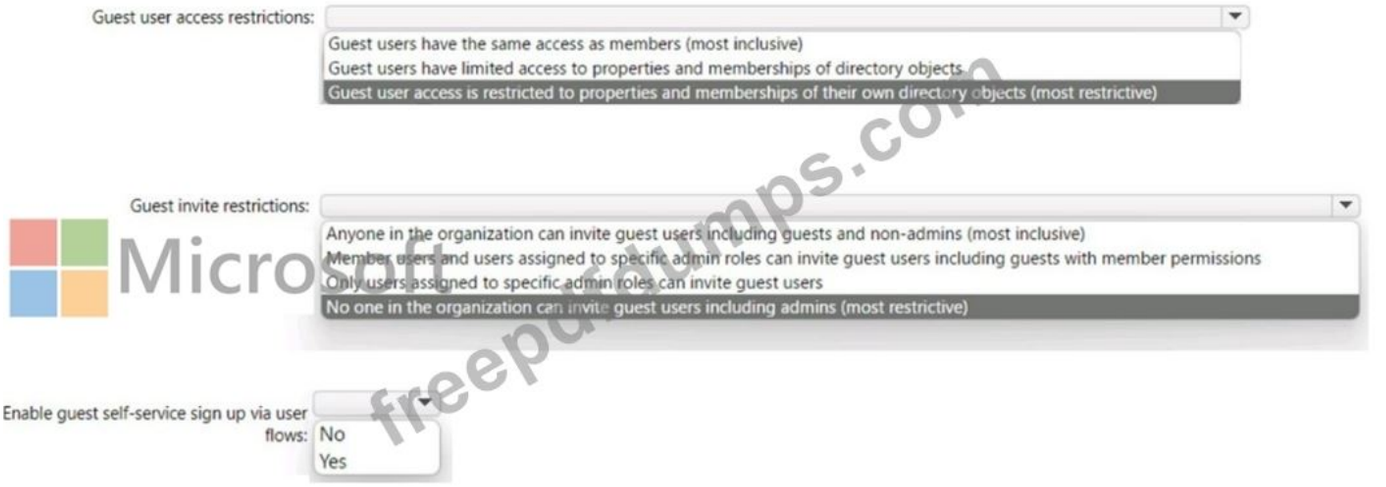
How many licenses are used if you assign the Microsoft Office 365 Enterprise E5 license to Group1?
A. 0
B. 2
C. 3
D. 4
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

NEW QUESTION: 76
You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs.
Yon receive more than 100 email alerts each day for tailed Azure Al) user sign-in attempts.
You need to ensure that a new security administrator receives the alerts instead of you.
Solution: From Azure monitor, you create a data collection rule.
Does this meet the goal?
A. Yes
B. No
Answer: B (LEAVE A REPLY)

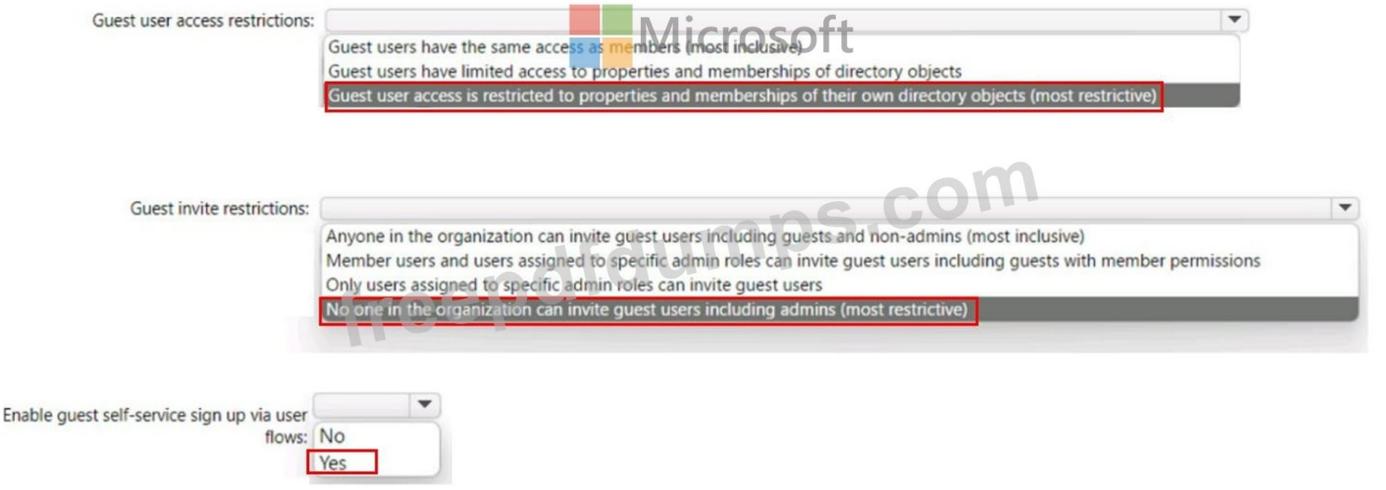
NEW QUESTION: 77
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?
A. Modify the User consent settings for the enterprise applications.
B. Create a catalog.
C. Create a program.
D. Modify the Admin consent requests settings for the enterprise applications.
Answer: B (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview Overview Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.

NEW QUESTION: 78
You have a Microsoft Exchange organization that uses an SMTP' address space of contoso.com. Several users use their contoso.com email address for self-service sign up to Azure Active Directory (Azure AD).
You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.
You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.
Which PowerShell cmdlet should you run?
A. Set-MsolCompanySettings
B. Set-MsolDomainFederationSettings
C. Update-MsolfederatedDomain
D. Set-MsolDomain
Answer: A (LEAVE A REPLY)
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

NEW QUESTION: 79
You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.
You need to configure External collaboration settings for the tenant to meet the following requirements: |
*Guest users must be prevented from querying staff email addresses.
*Guest users must be able to access the tenant only if they are invited by User1.
Which three settings should you configure? To answer, select the appropriate settings in the answer area.



Answer:



NEW QUESTION: 80
Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant- Users sign in to computers that run Windows 10 and are joined to the domain.
You plan to implement Azure AD Seamless Single Sign-On (Azure AD Seamless SSO).
You need to configure the computers for Azure AD Seamless SSO.
What should you do?

A. Enable Enterprise State Roaming.
B. Configure Sign-in options.
C. Install the Azure AD Connect Authentication Agent.
D. Modify the Intranet Zone settings.
Answer: D (LEAVE A REPLY)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

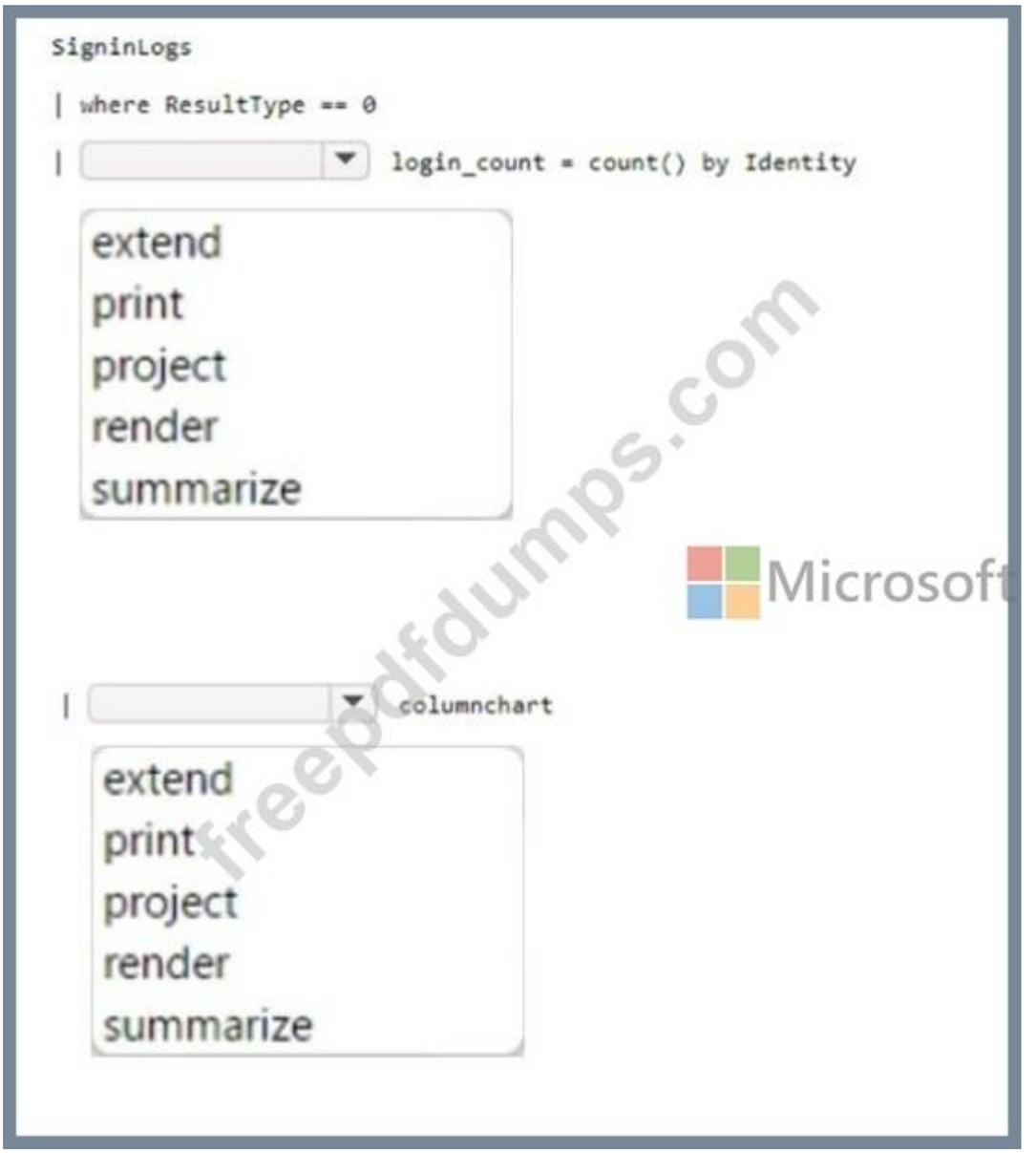
NEW QUESTION: 81
You need to meet the technical requirements for the probability that user identities were compromised.
What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer:

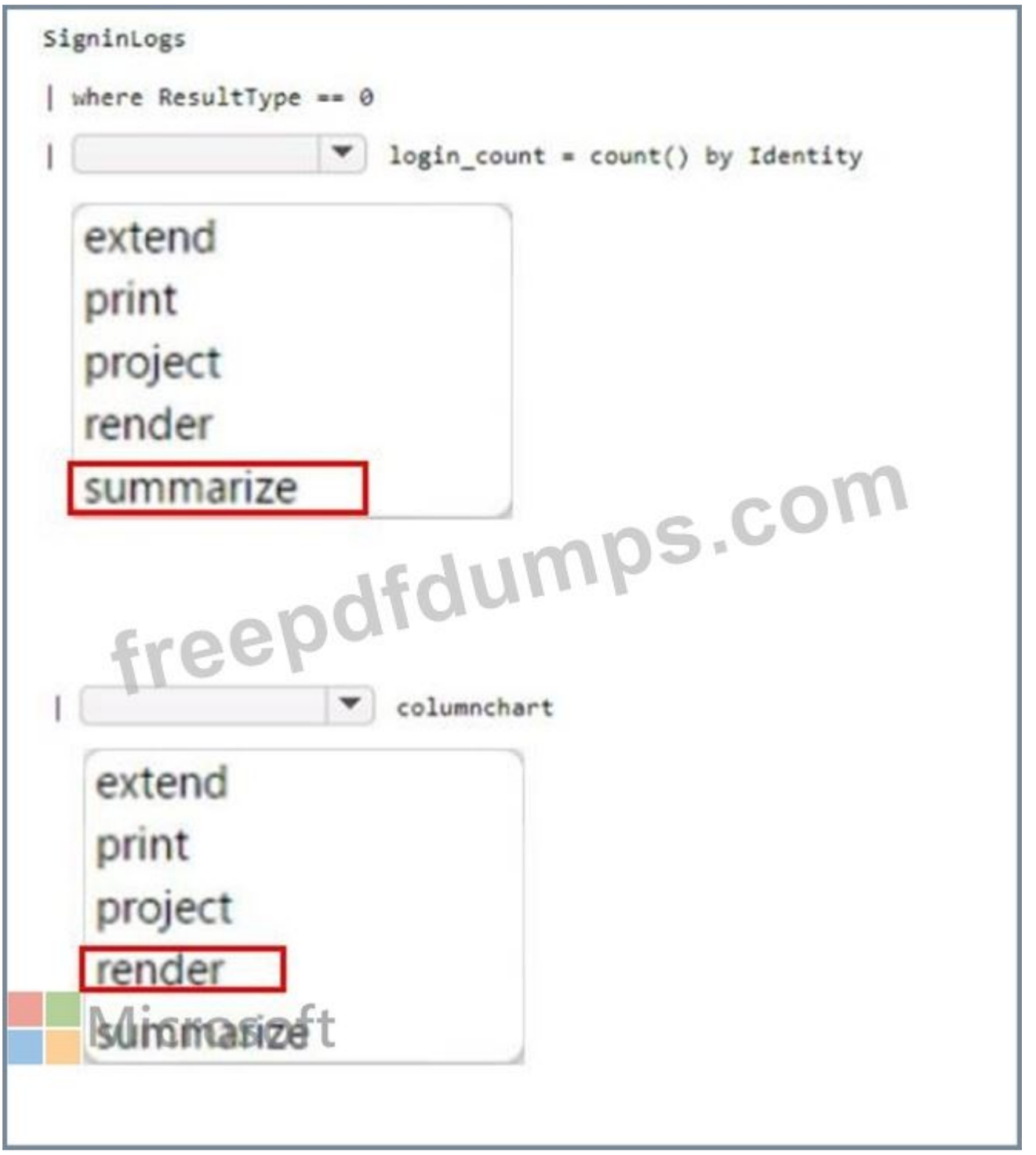
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

NEW QUESTION: 82
You have an Azure subscription.
Azure AD logs are sent to a Log Analytics workspace.
You need to query the logs and graphically display the number of sign-ins per user.

How should you complete the query? To answer, select the appropriate options in the answer area.



Answer:



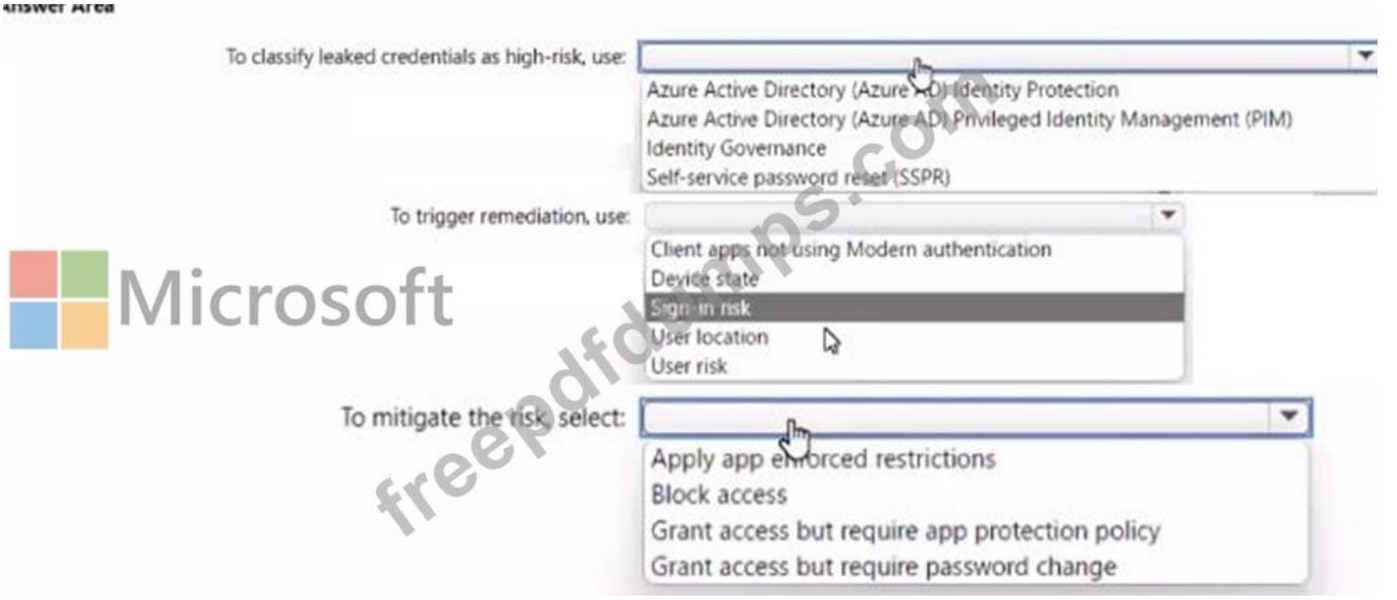
NEW QUESTION: 83

You have a Microsoft 365 tenant.

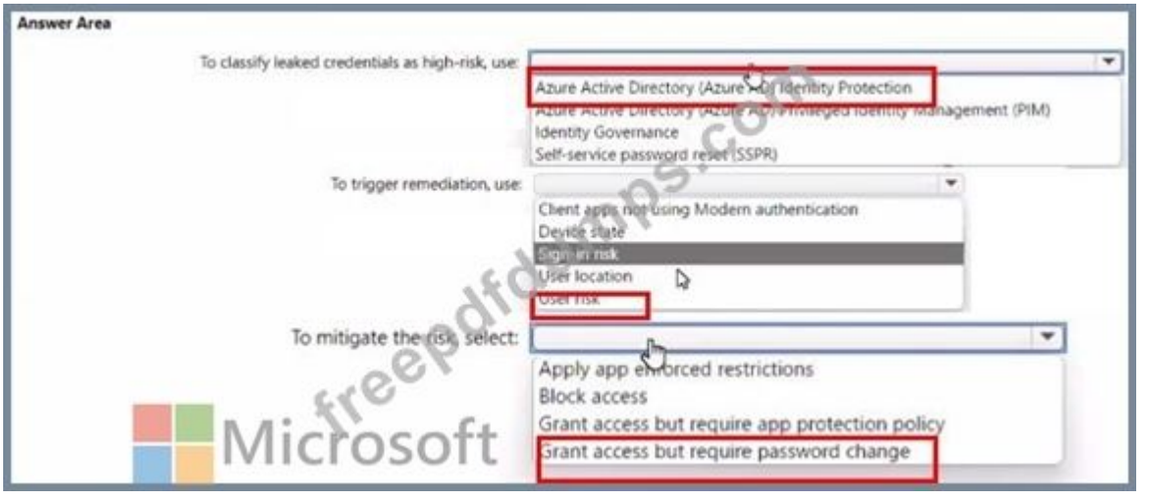
You need to Identity users who have leaked credentials. The solution must meet the following requirements:

* Identity sign-ms by users who are suspected of having leaked credentials.
* Flag the sign-ins as a high-risk event.
* Immediately enforce a control to mitigate the risk, while still allowing the user to access applications.

What should you use? To answer, select the appropriate options m the answer area.



Answer:



NEW QUESTION: 84

You have a Microsoft 36S tenant.

You create a named location named HighRiskCountries that contains a list of high-risk countries.

You need to limit the amount of time a user can stay authenticated when connecting from a high-risk country.

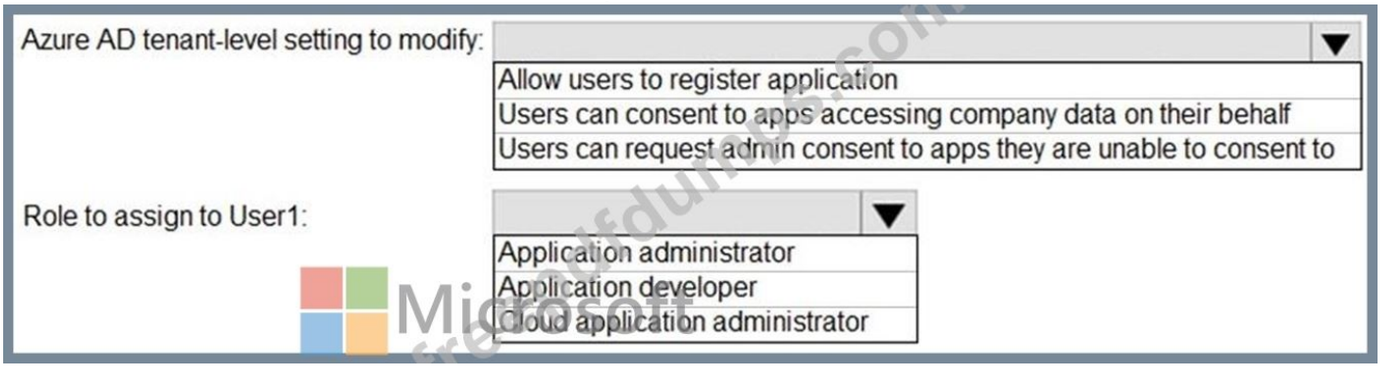
What should you configure in a conditional access policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

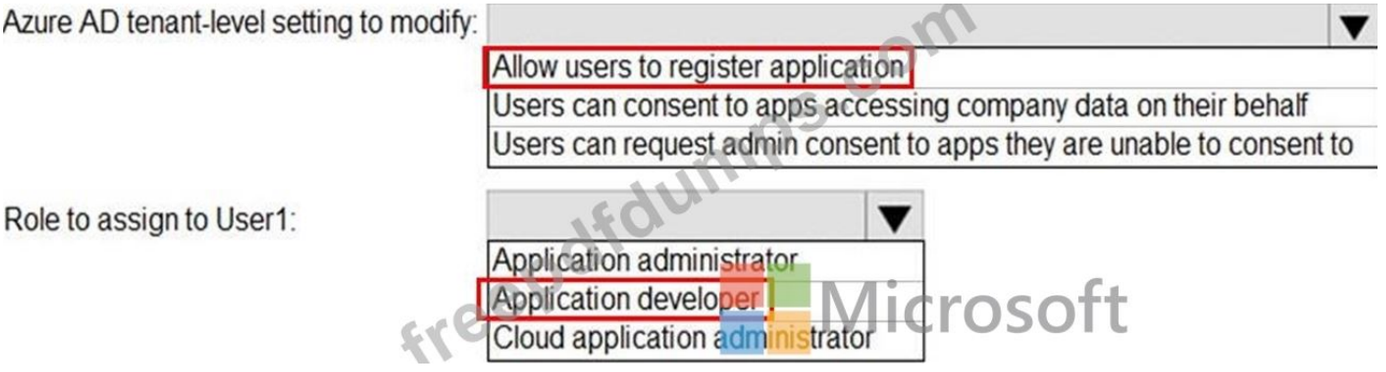
Answer:

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

NEW QUESTION: 85
You need to configure app registration in Azure AD to meet the delegation requirements.
What should you do? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:



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