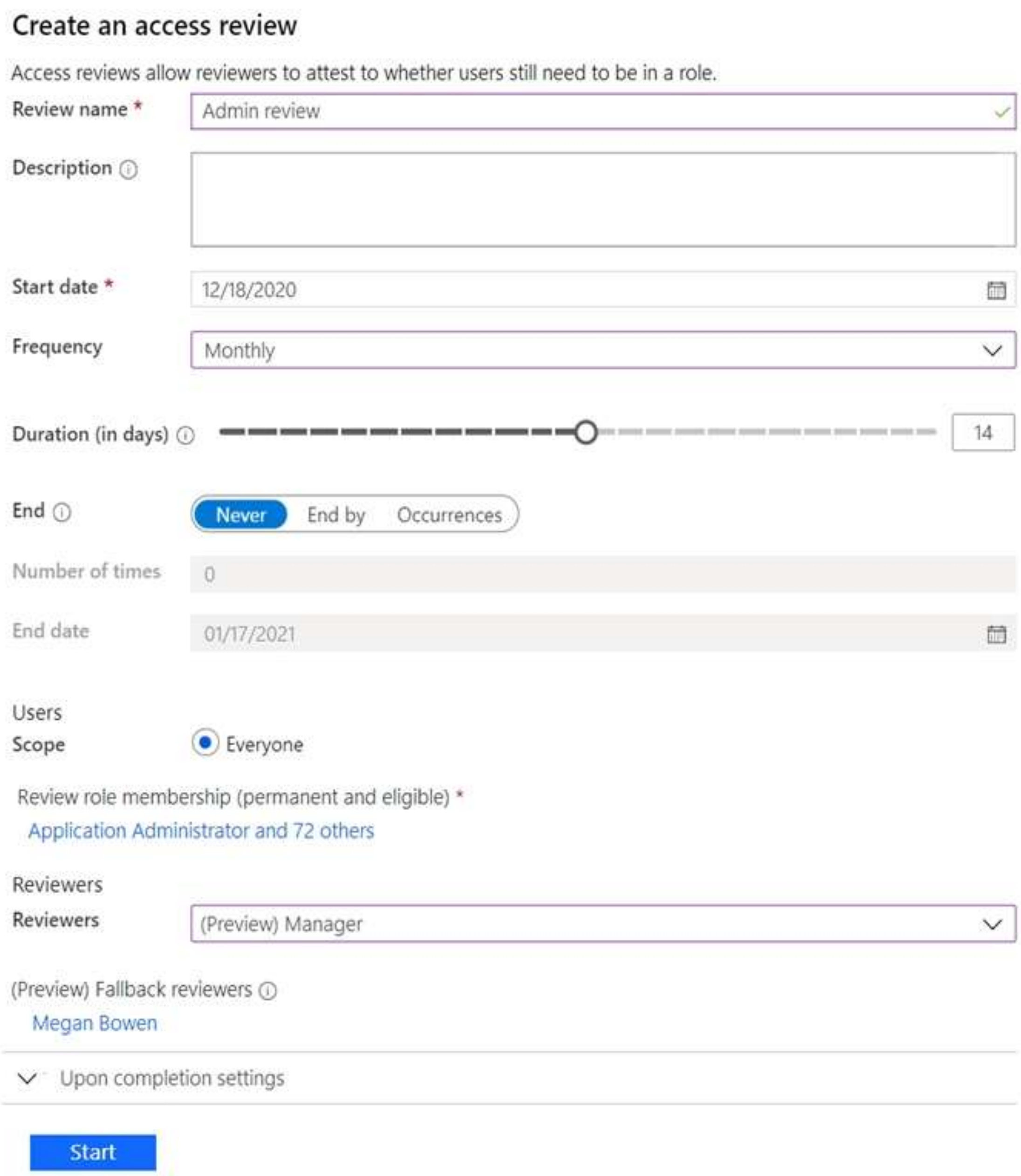
- **Vendor:** Microsoft
- **Exam Code:** SC-300
- **Exam Name:** Microsoft Identity and Access Administrator
- **New Updated Questions from Braindump2go**
- **(Updated in December/2021)**

QUESTION 37
You have a Microsoft 365 tenant.
The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.
You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.
What should you create?

A. an access package that targets users outside your directory
B. an access package that targets users in your directory
C. a group-based access review that targets guest users
D. an application-based access review that targets guest users

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

QUESTION 38
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.
You have 100 IT administrators who are organized into 10 departments.
You create the access review shown in the exhibit. (Click the Exhibit tab.)



Create an access review

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

Review name * Admin review

Description

Start date * 12/18/2020

Frequency Monthly

Duration (in days) 14

End ● Never ○ End by ○ Occurrences

Number of times 0

End date 01/17/2021

Users

Scope ● Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers (Preview) Manager

(Preview) Fallback reviewers

Megan Bowen

You discover that all access review requests are received by Megan Bowen.
You need to ensure that the manager of each department receives the access reviews of their respective department.
Solution: You create a separate access review for each role.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

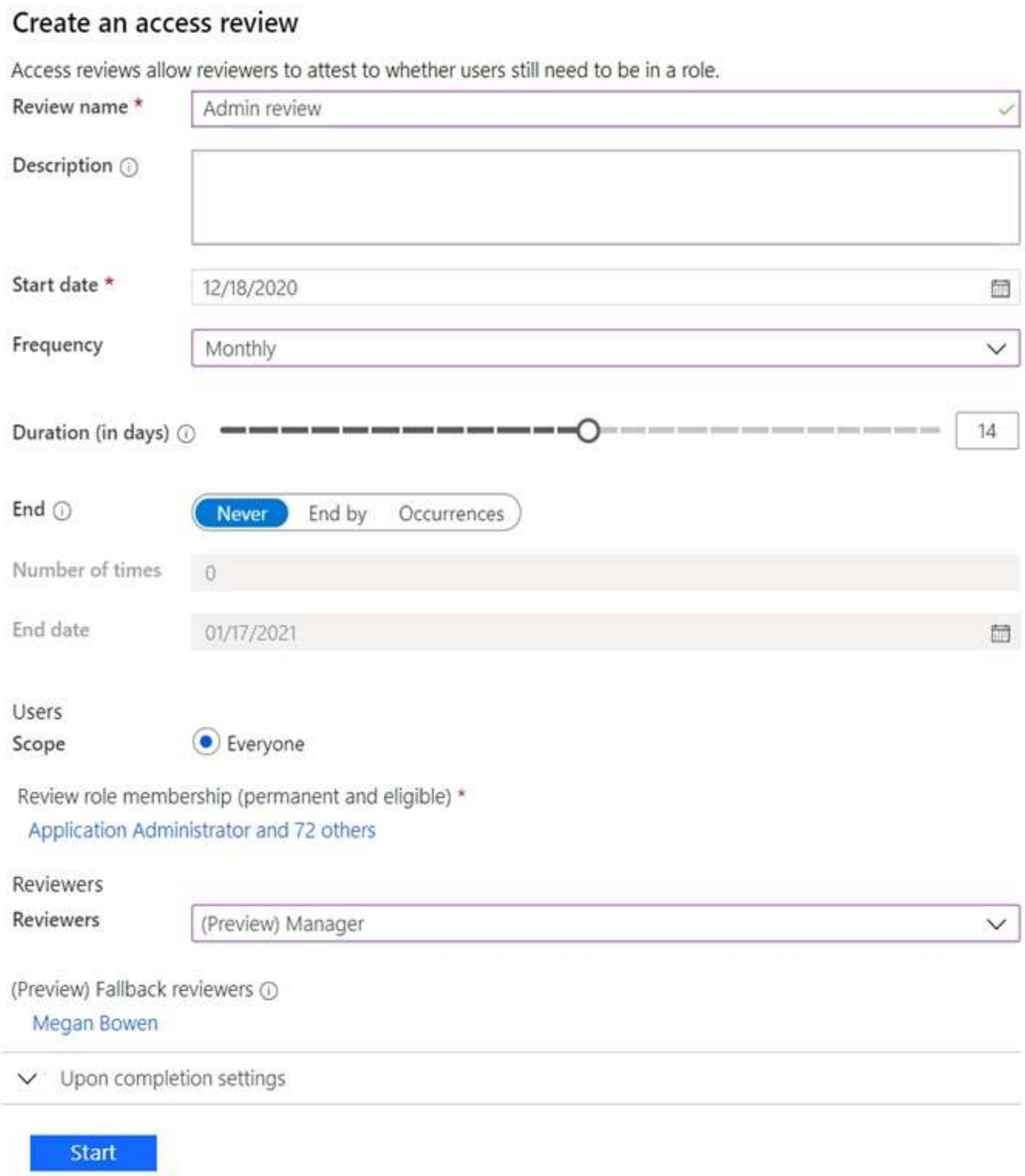
QUESTION 39
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)



Create an access review

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

Review name *: Admin review

Description:

Start date *: 12/18/2020

Frequency: Monthly

Duration (in days): 14

End: Never | End by | Occurrences

Number of times: 0

End date: 01/17/2021

Users

Scope: ● Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers: (Preview) Manager

(Preview) Fallback reviewers

Megan Bowen

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You modify the properties of the IT administrator user accounts.

Does this meet the goal?

A. Yes
B. No

Answer: A

Explanation:

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

QUESTION 40

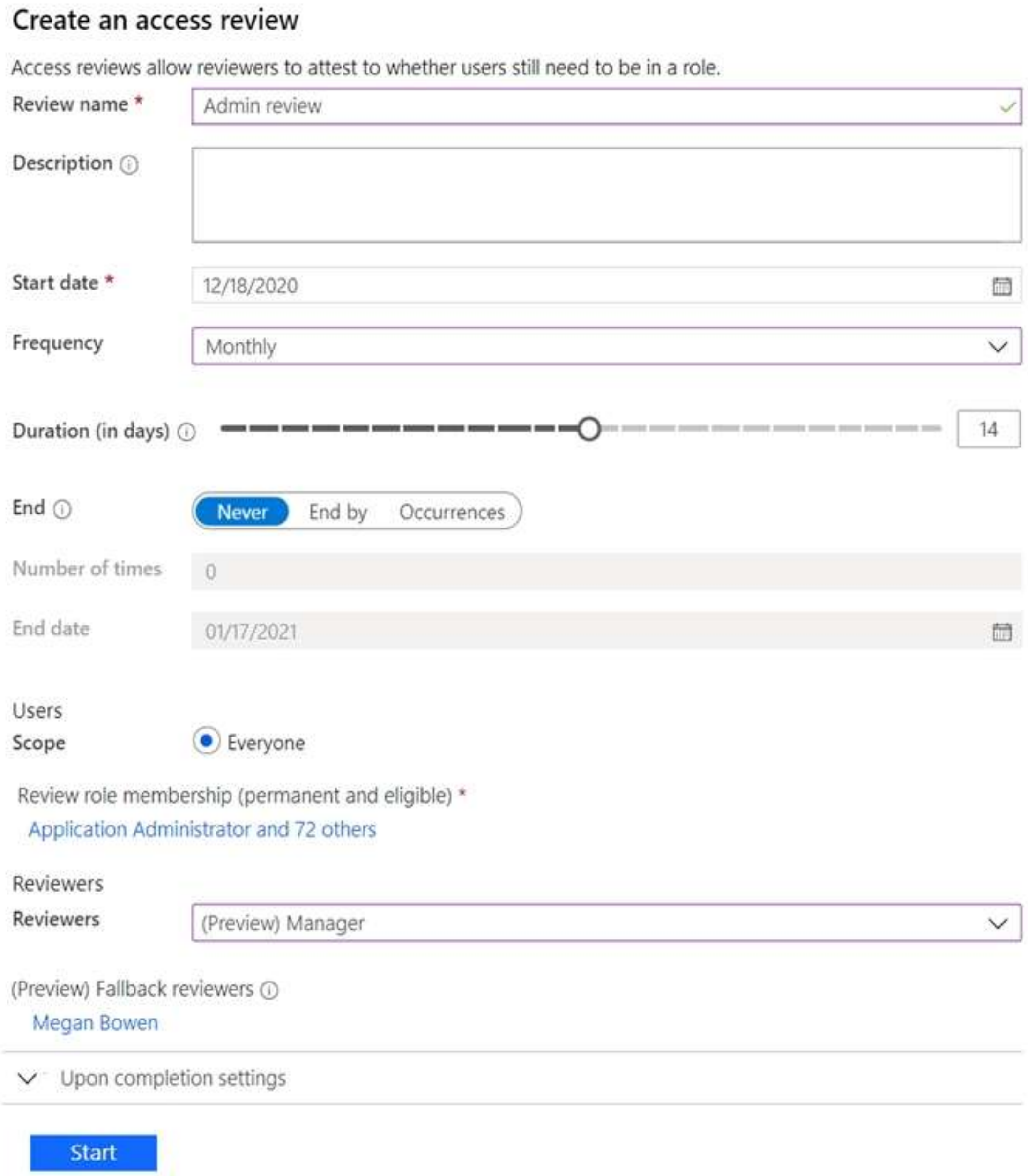
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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.

You have 100 IT administrators who are organized into 10 departments.

You create the access review shown in the exhibit. (Click the Exhibit tab.)



Create an access review

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

Review name *: Admin review

Description ⓘ:

Start date *: 12/18/2020

Frequency: Monthly

Duration (in days) ⓘ: 14

End ⓘ: ● Never | End by | Occurrences

Number of times: 0

End date: 01/17/2021

Users

Scope: ● Everyone

Review role membership (permanent and eligible) *

Application Administrator and 72 others

Reviewers

Reviewers: (Preview) Manager

(Preview) Fallback reviewers ⓘ

Megan Bowen

You discover that all access review requests are received by Megan Bowen.

You need to ensure that the manager of each department receives the access reviews of their respective department.

Solution: You set Reviewers to Member (self).

Does this meet the goal?

A. Yes

B. No

Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

QUESTION 41
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 Azure Active Directory (Azure AD) tenant that syncs to an Active Directory forest.
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 password writeback.
Does this meet the goal?

A. Yes
B. No

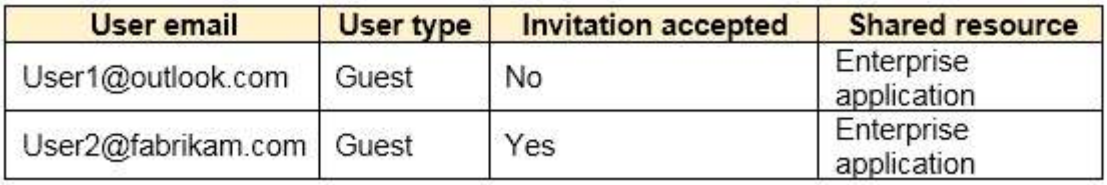
Answer: B
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION 42
Note: This question is part of 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 Azure Active Directory (Azure AD) tenant that contains a group named Group1.
You need to enable multi-factor authentication (MFA) for the users in Group1 only.
Solution: From Multi-Factor Authentication, you select Bulk update, and you provide a CSV file that contains the members of Group1.
Does this meet the goal?

A. Yes
B. No

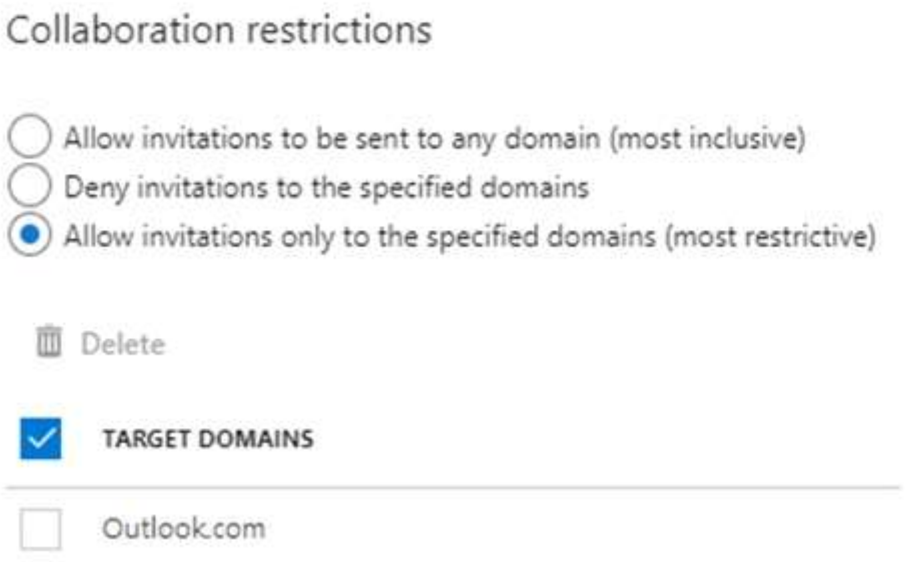
Answer: B

QUESTION 43
Hotspot Question
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.



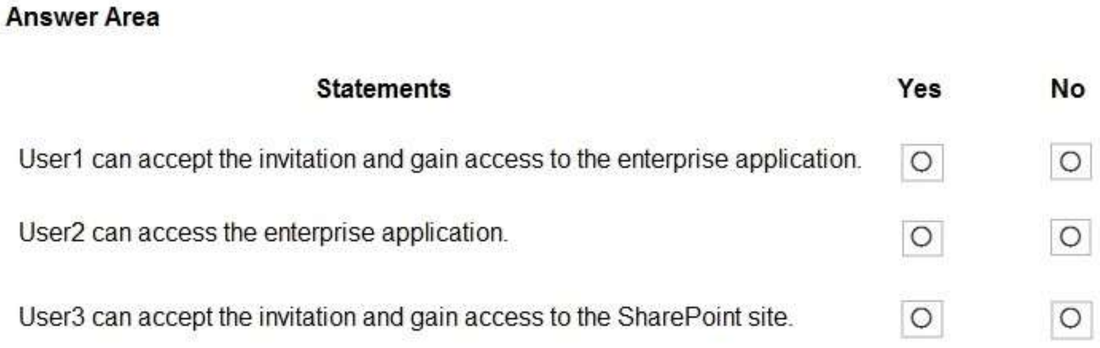
Collaboration restrictions

○ Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
● Allow invitations only to the specified domains (most restrictive)

☑ TARGET DOMAINS

□ Outlook.com

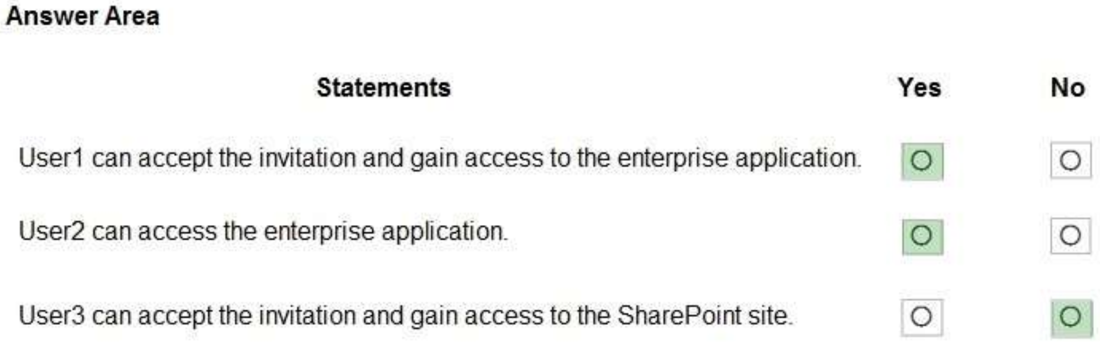
From a Microsoft SharePoint Online site, a user invites user3@adatum.com to the site.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

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

Answer:



Answer Area

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

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

QUESTION 44

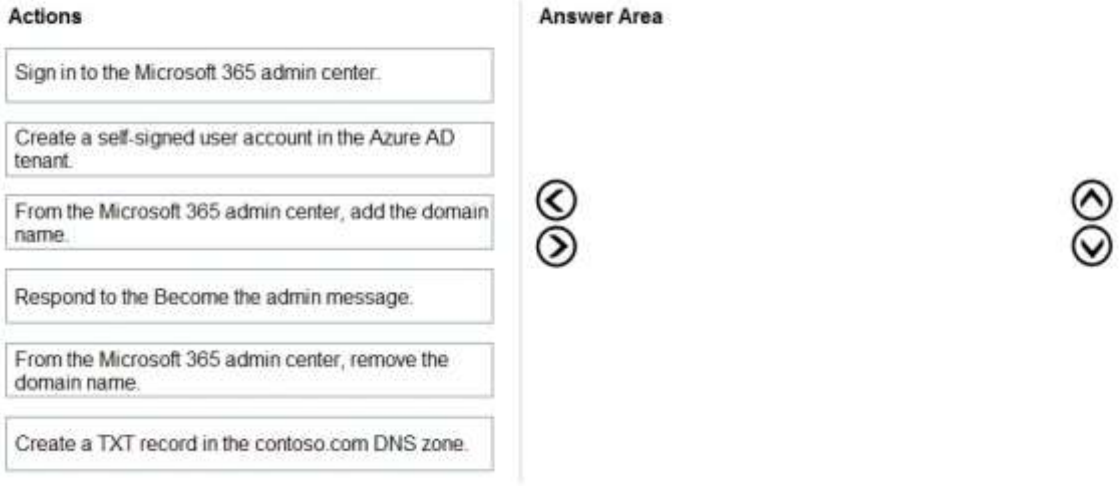
Drag and Drop Question

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.

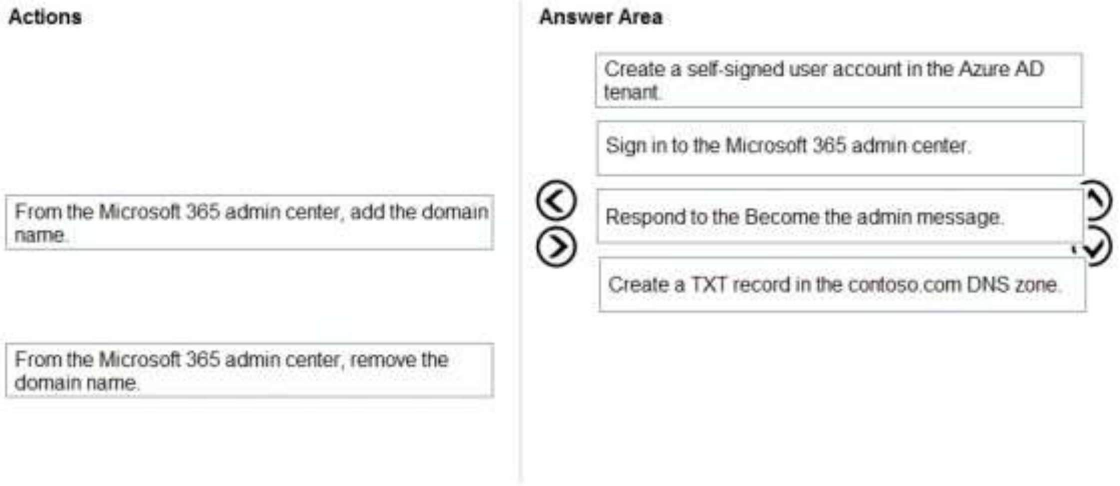


Actions

- Sign in to the Microsoft 365 admin center.
- Create a self-signed user account in the Azure AD tenant.
- From the Microsoft 365 admin center, add the domain name.
- Respond to the Become the admin message.
- From the Microsoft 365 admin center, remove the domain name.
- Create a TXT record in the contoso.com DNS zone.

Answer Area

Answer:



Actions

- From the Microsoft 365 admin center, add the domain name.
- From the Microsoft 365 admin center, remove the domain name.

Answer Area

- Create a self-signed user account in the Azure AD tenant.
- Sign in to the Microsoft 365 admin center.
- Respond to the Become the admin message.
- Create a TXT record in the contoso.com DNS zone.

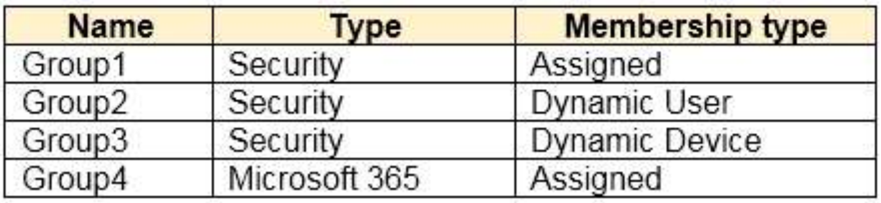
Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

QUESTION 45

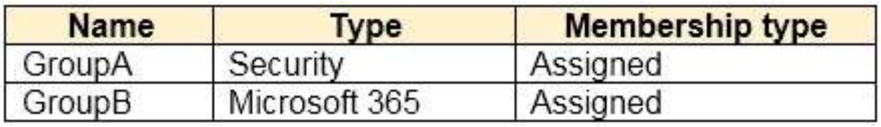
Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1 and the groups shown in the following table.



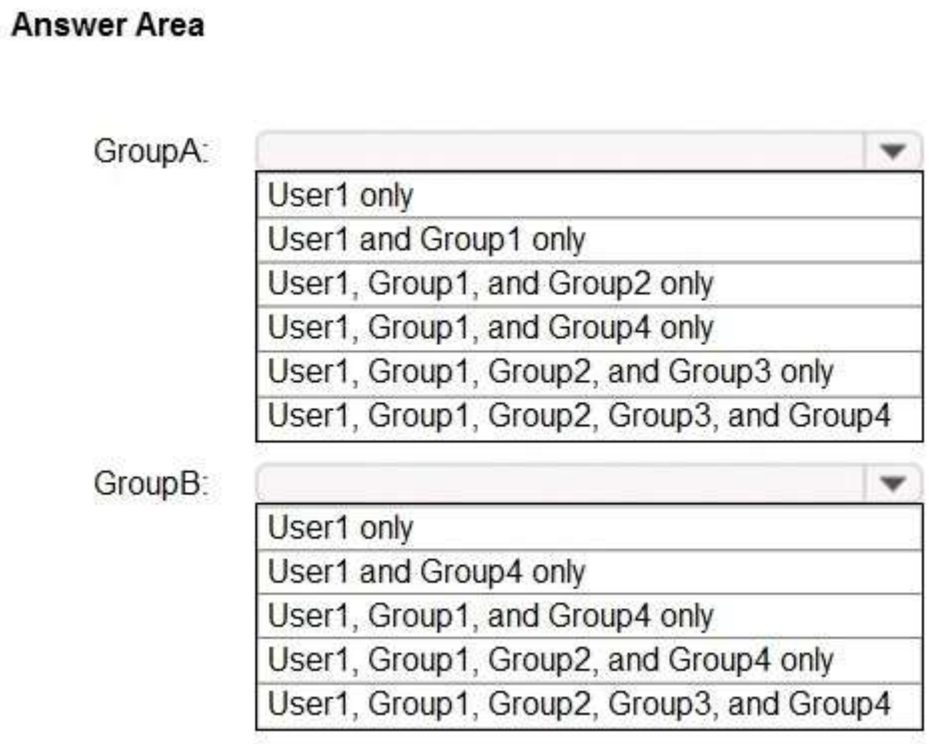
Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

In the tenant, you create the groups shown in the following table.



Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

Which members can you add to GroupA and GroupB? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

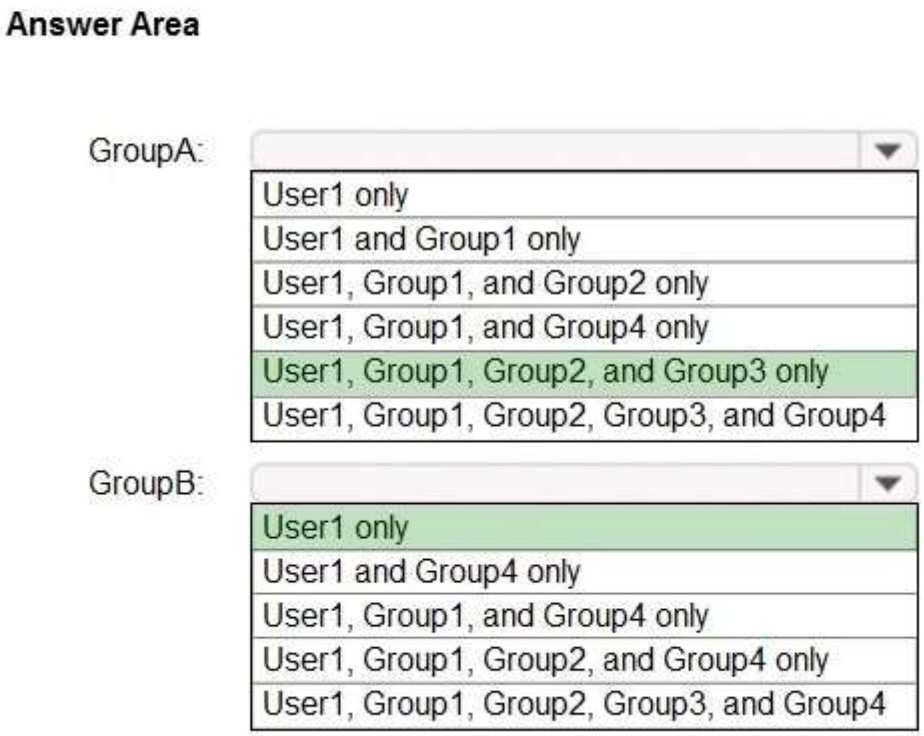


Answer Area

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:



Answer Area

GroupA:

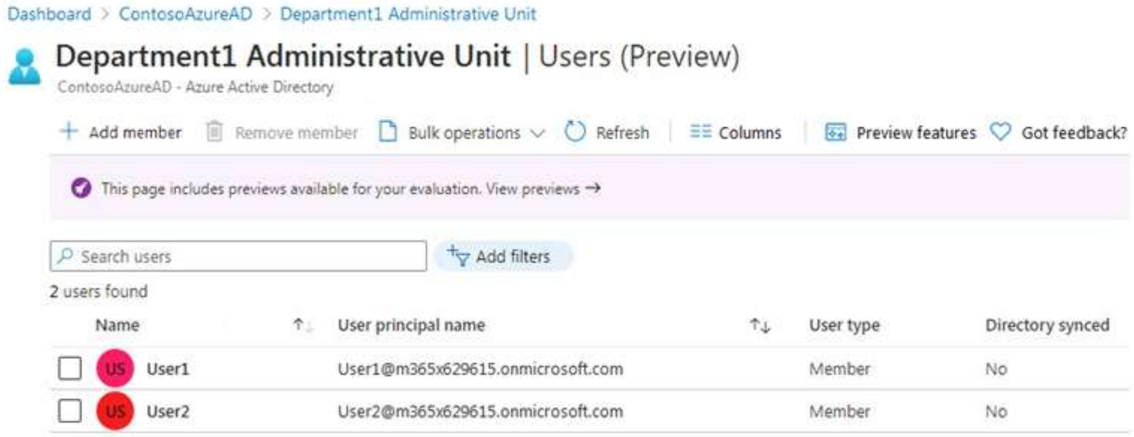
- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- [✓ User1, Group1, Group2, and Group3 only]
- User1, Group1, Group2, Group3, and Group4

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:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

QUESTION 46
Hotspot Question
You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1. Department1 has the users shown in the Users exhibit. (Click the Users tab.)



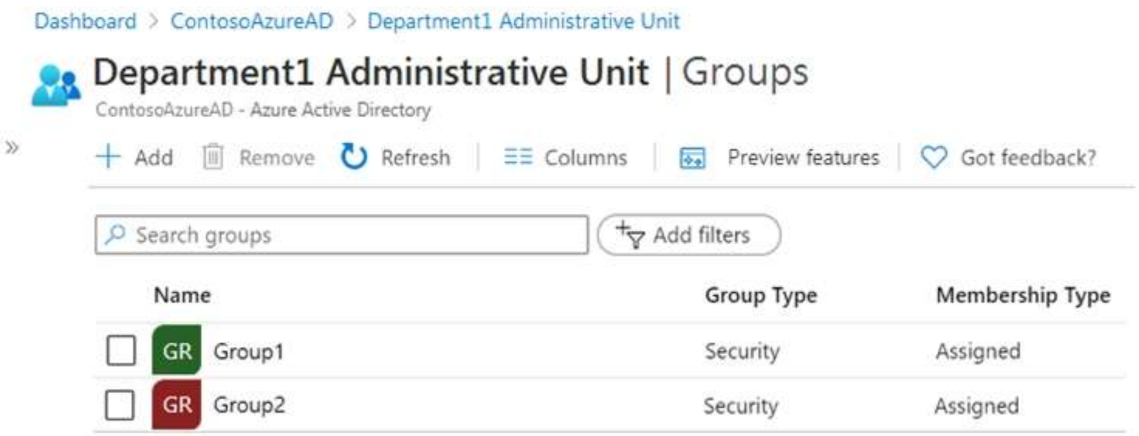
Department1 Administrative Unit | Users (Preview)
ContosoAzureAD - Azure Active Directory

This page includes previews available for your evaluation. View previews →

2 users found

	Name	User principal name	User type	Directory synced
□	User1	User1@m365x629615.onmicrosoft.com	Member	No
□	User2	User2@m365x629615.onmicrosoft.com	Member	No

Department1 has the groups shown in the Groups exhibit. (Click the Groups tab.)



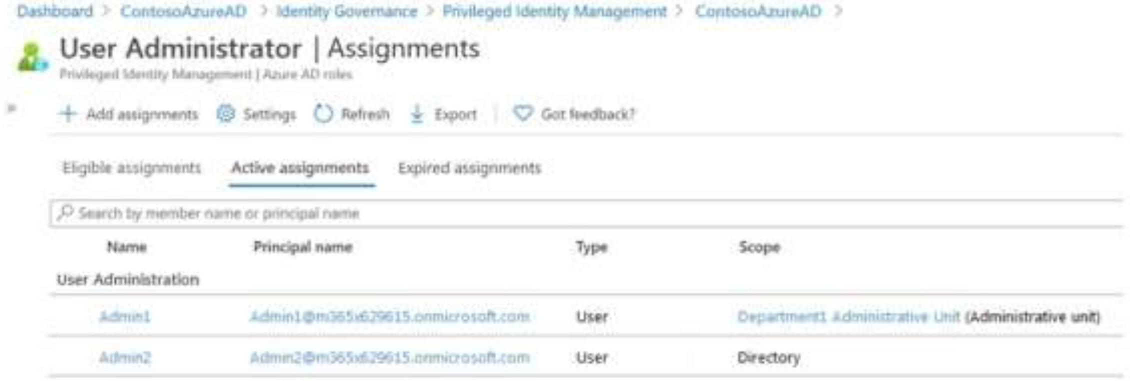
Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

	Name	Group Type	Membership Type
□	GR Group1	Security	Assigned
□	GR Group2	Security	Assigned

Department1 has the user administrator assignments shown in the Assignments exhibit. (Click the Assignments tab.)



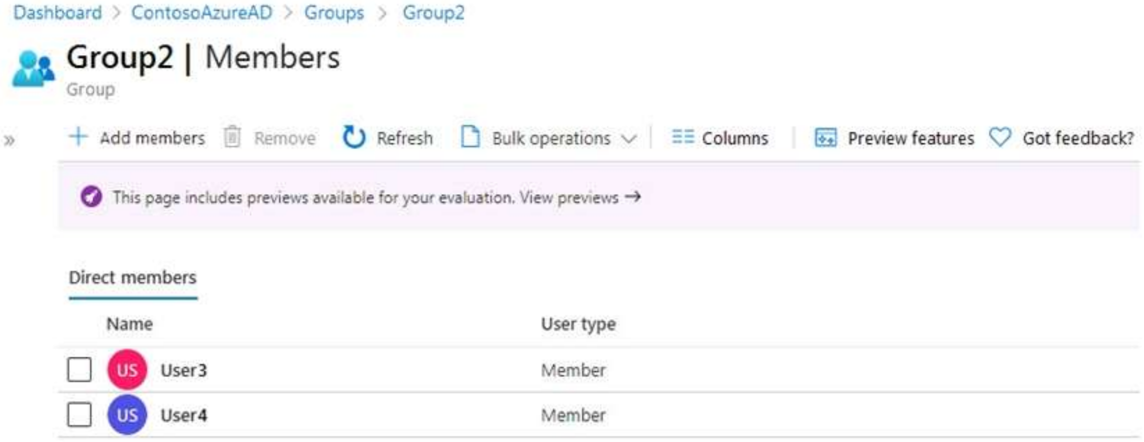
Dashboard > ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

Name	Principal name	Type	Scope
User Administration			
Admin1	Admin1@m365x629615.onmicrosoft.com	User	Department1 Administrative Unit (Administrative unit)
Admin2	Admin2@m365x629615.onmicrosoft.com	User	Directory

The members of Group2 are shown in the Group2 exhibit. (Click the Group2 tab.)



Dashboard > ContosoAzureAD > Groups > Group2

Group2 | Members

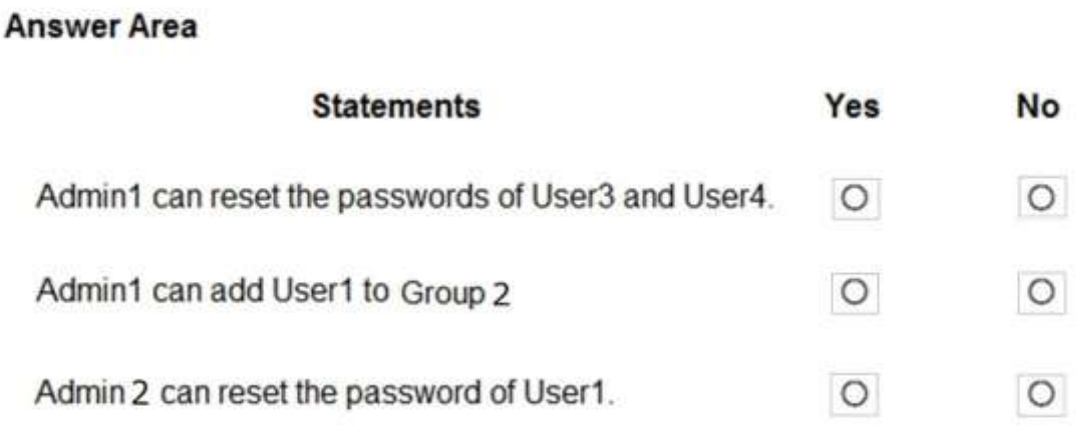
Group

This page includes previews available for your evaluation. View previews →

Direct members

	Name	User type
□	US User3	Member
□	US User4	Member

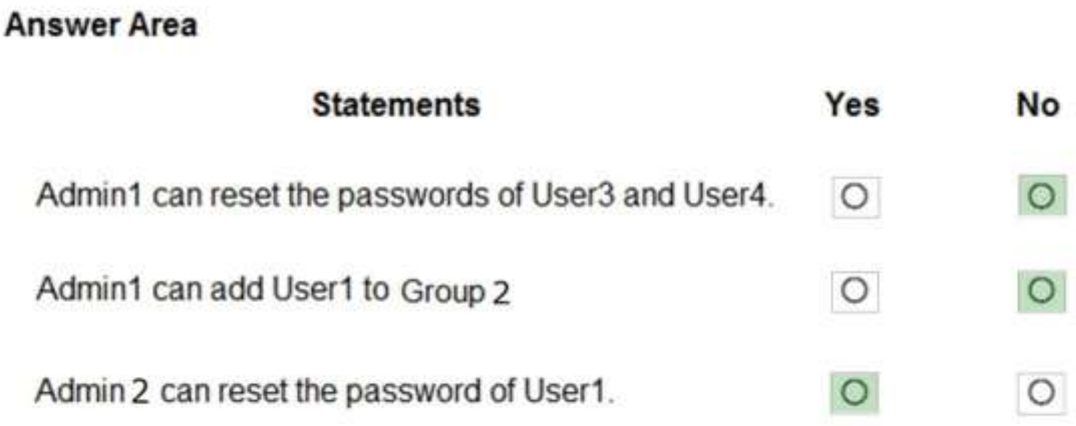
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

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

Answer:

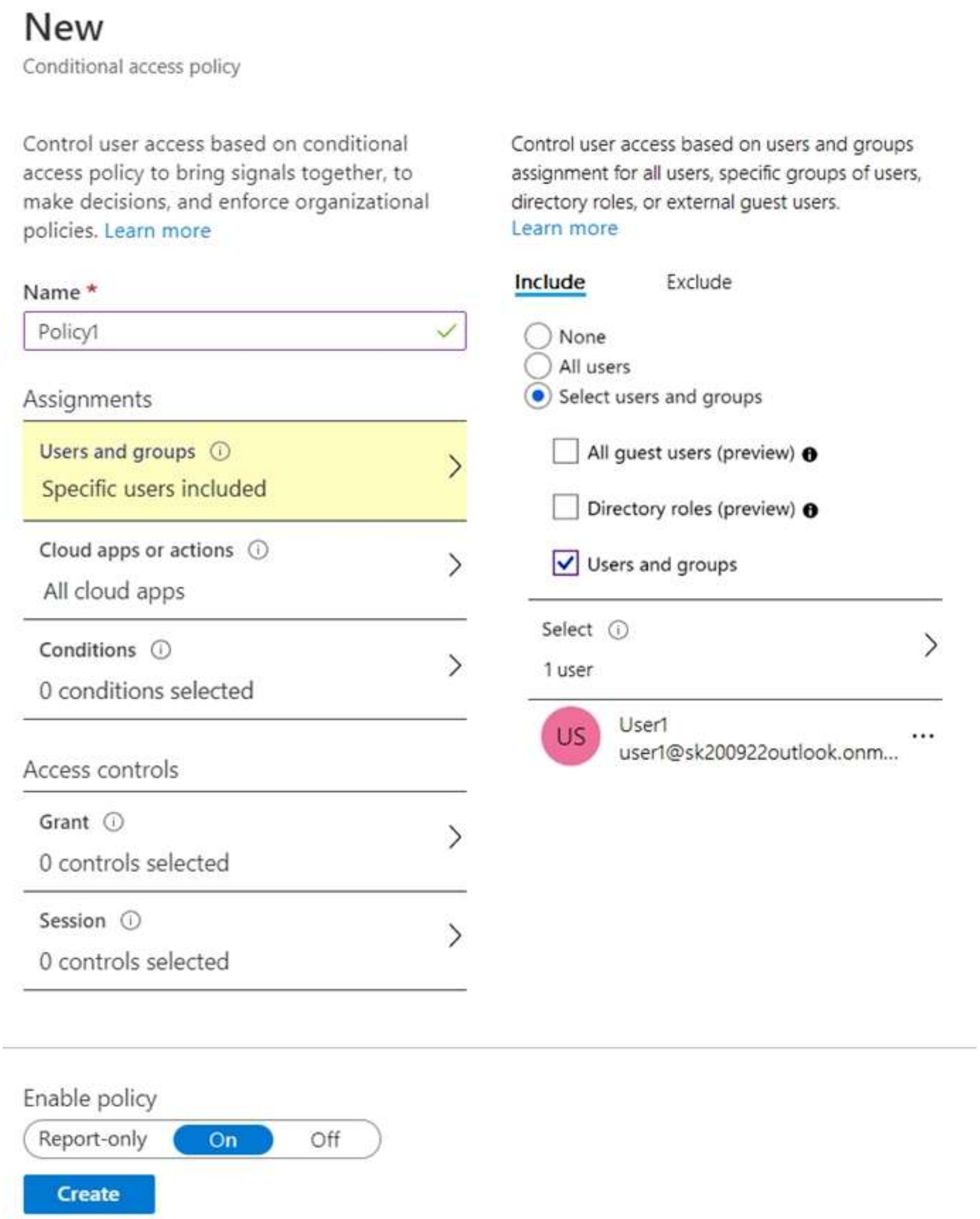


Answer Area

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

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

QUESTION 47
Hotspot Question
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.



New

Conditional access policy

Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more

Name *

Policy1

Assignments

Users and groups ⓘ
Specific users included

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
0 controls selected

Session ⓘ
0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users. Learn more

Include Exclude

○ None
○ All users
● Select users and groups

□ All guest users (preview)
□ Directory roles (preview)
☑ Users and groups

Select ⓘ
1 user

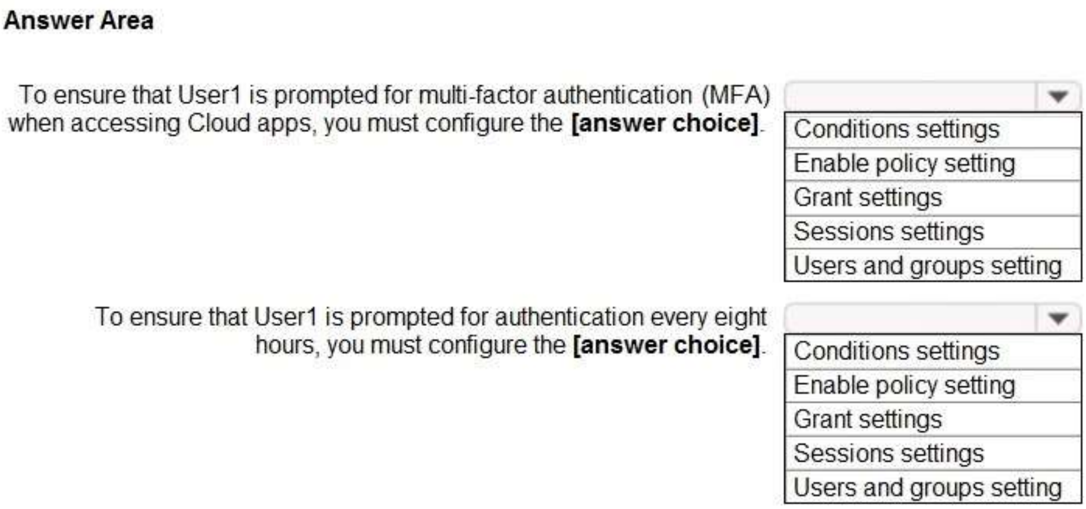
User1
user1@sk200922outlook.onm...

Enable policy

Report-only [✓ On] Off

Create

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 Area

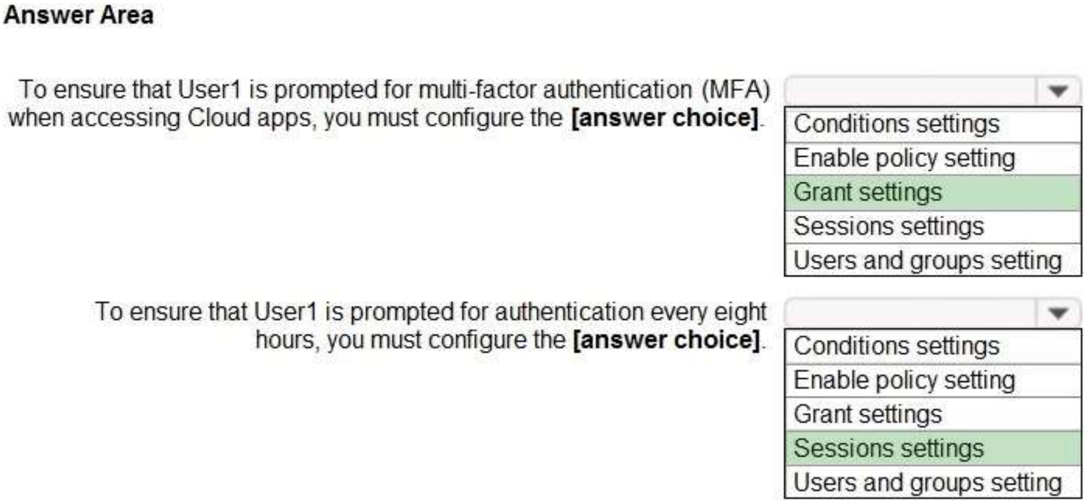
To ensure that User1 is prompted for multi-factor authentication (MFA) when accessing Cloud apps, you must configure the **[answer choice]**.

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

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

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

Answer:



Answer Area

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

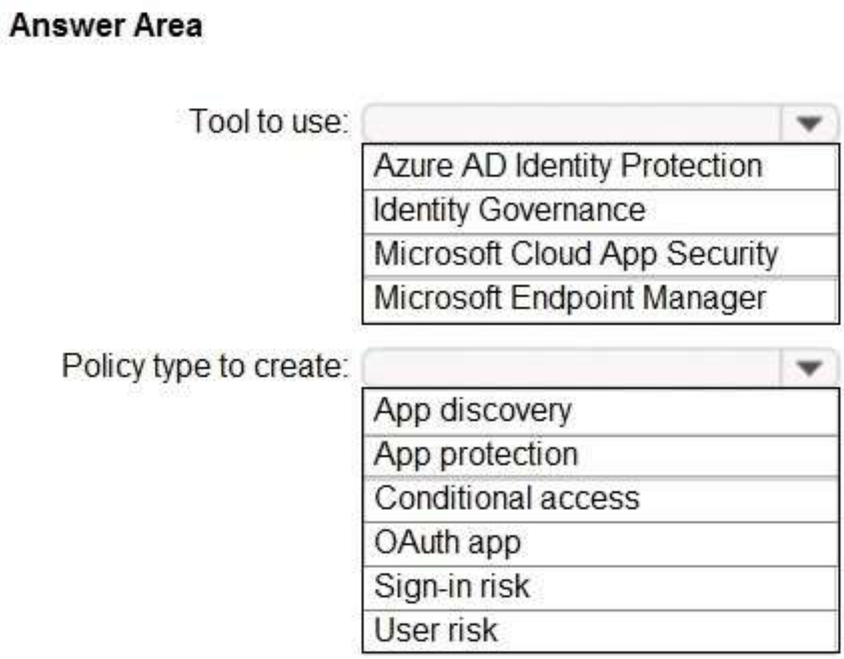
- Conditions settings
- Enable policy setting
- [✓ Grant settings]
- Sessions settings
- Users and groups setting

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

- Conditions settings
- Enable policy setting
- Grant settings
- [✓ Sessions settings]
- Users and groups setting

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

QUESTION 48
Hotspot Question
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 Area

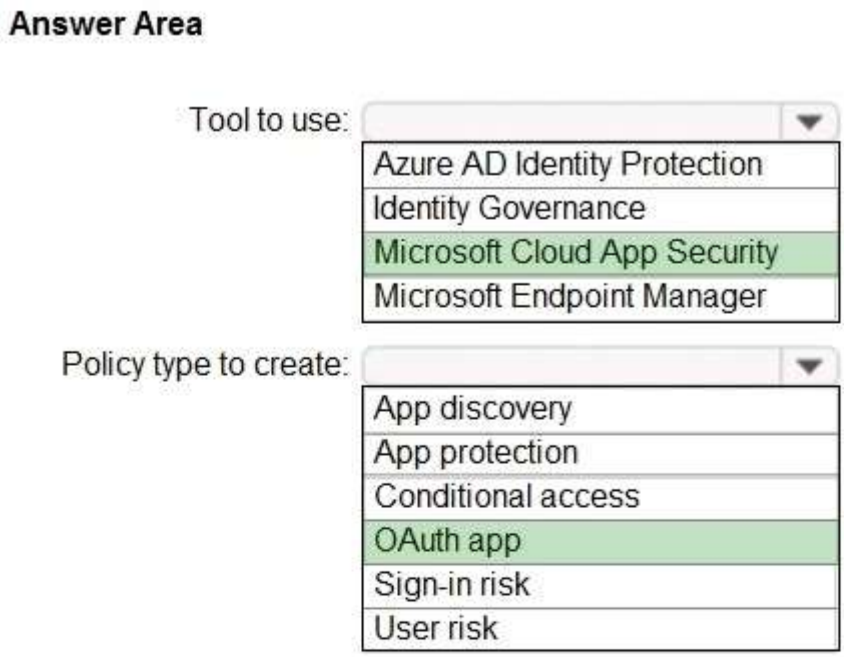
Tool to use:

- Azure AD Identity Protection
- Identity Governance
- Microsoft Cloud App Security
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- OAuth app
- Sign-in risk
- User risk

Answer:



Answer Area

Tool to use:

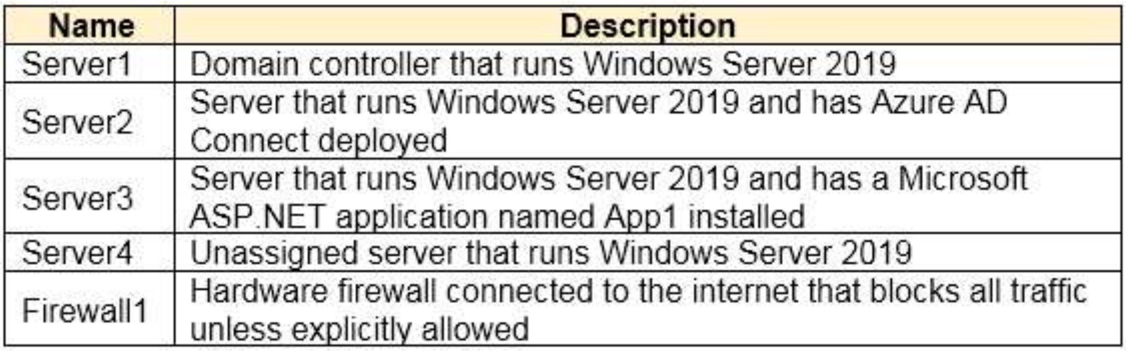
- Azure AD Identity Protection
- Identity Governance
- [✓ Microsoft Cloud App Security]
- Microsoft Endpoint Manager

Policy type to create:

- App discovery
- App protection
- Conditional access
- [✓ OAuth app]
- Sign-in risk
- User risk

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

QUESTION 49
Hotspot Question
You have an on-premises datacenter that contains the hosts shown in the following table.



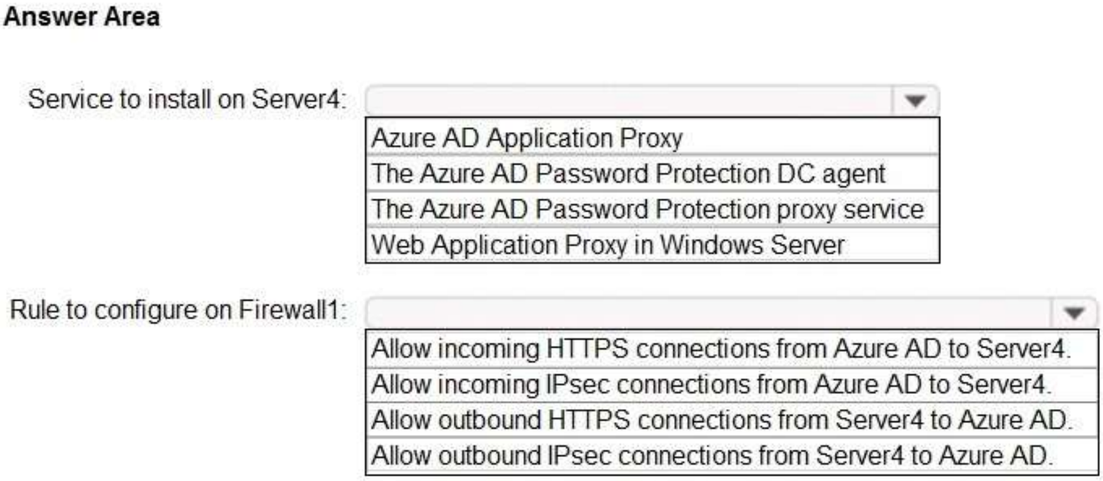
Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows 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 Area

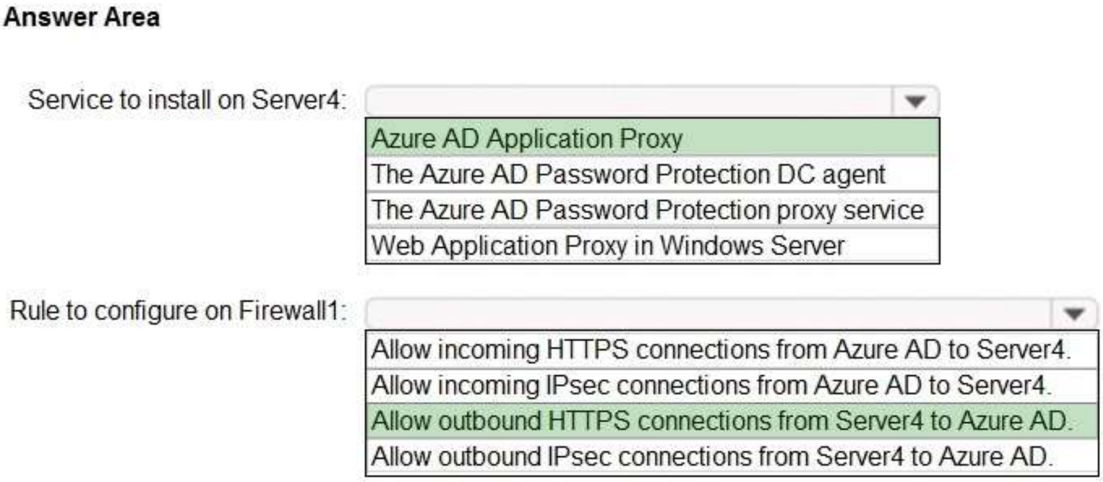
Service to install on Server4:

- Azure AD Application Proxy
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

Answer:



Answer Area

Service to install on Server4:

- [✓ Azure AD Application Proxy]
- The Azure AD Password Protection DC agent
- The Azure AD Password Protection proxy service
- Web Application Proxy in Windows Server

Rule to configure on Firewall1:

- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- [✓ Allow outbound HTTPS connections from Server4 to Azure AD.]
- Allow outbound IPsec connections from Server4 to Azure AD.

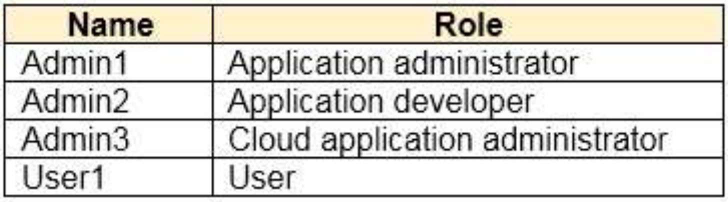
Explanation:

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

QUESTION 50

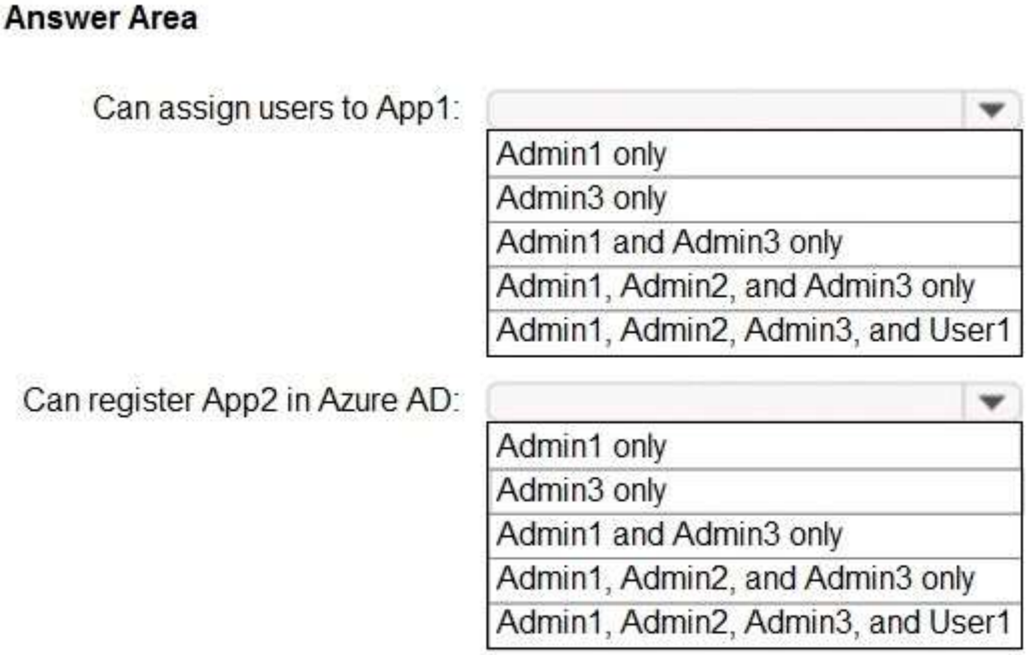
Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has the default App registrations settings. The tenant contains the users shown in the following table.



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

You purchase two cloud apps named App1 and App2. The global administrator registers App1 in Azure AD.
You need to identify who can assign users to App1, and who can register App2 in Azure AD.
What should you identify? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer Area

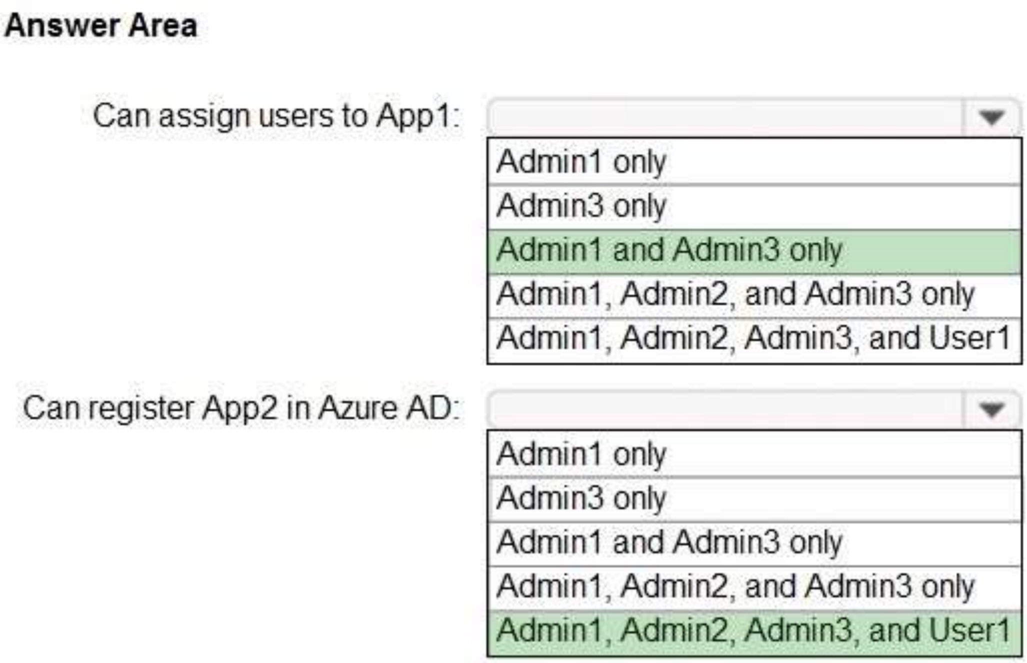
Can assign users to App1:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Answer:



Answer Area

Can assign users to App1:

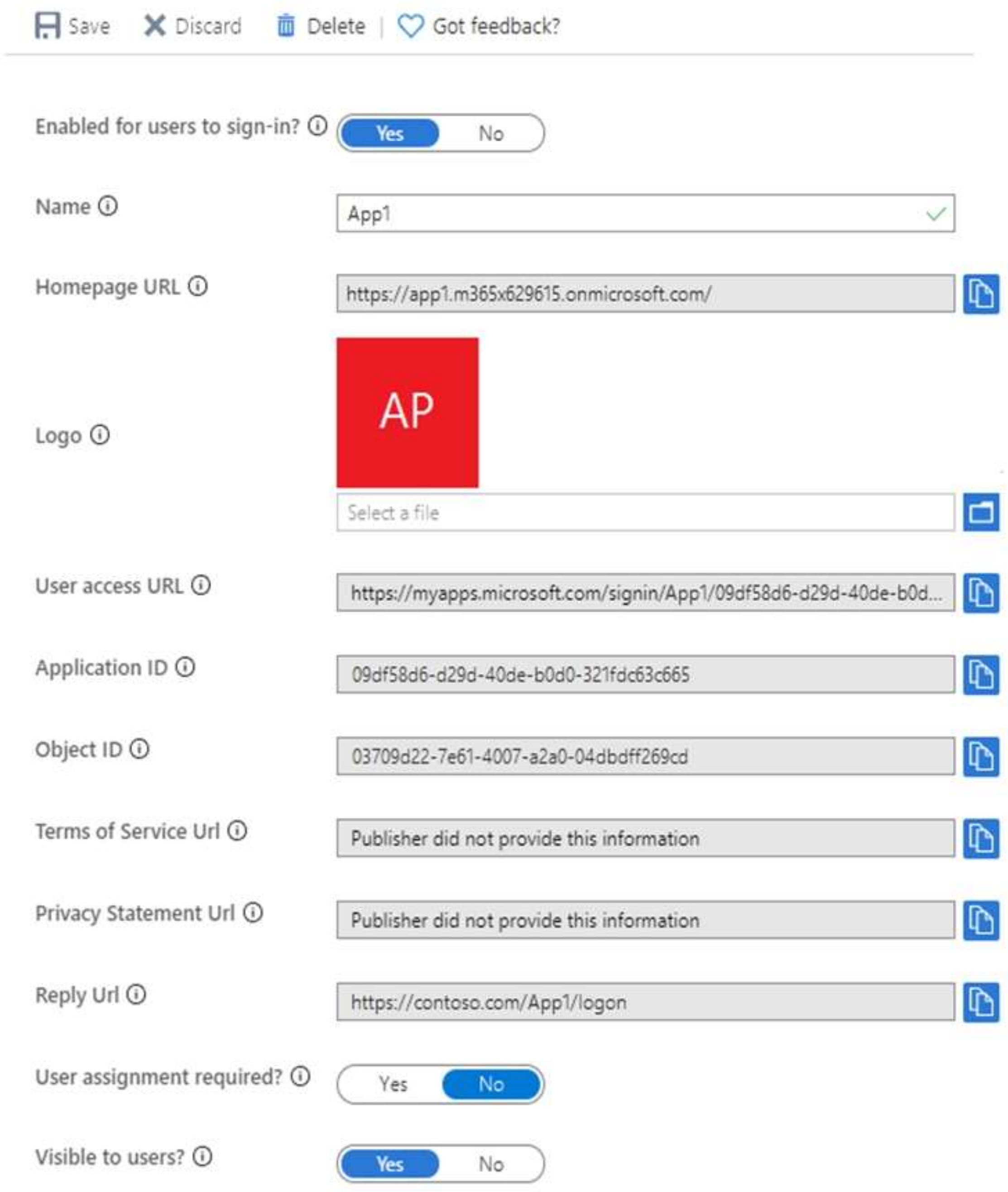
- Admin1 only
- Admin3 only
- [✓ Admin1 and Admin3 only]
- Admin1, Admin2, and Admin3 only
- Admin1, Admin2, Admin3, and User1

Can register App2 in Azure AD:

- Admin1 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, and Admin3 only
- [✓ Admin1, Admin2, Admin3, and User1]

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

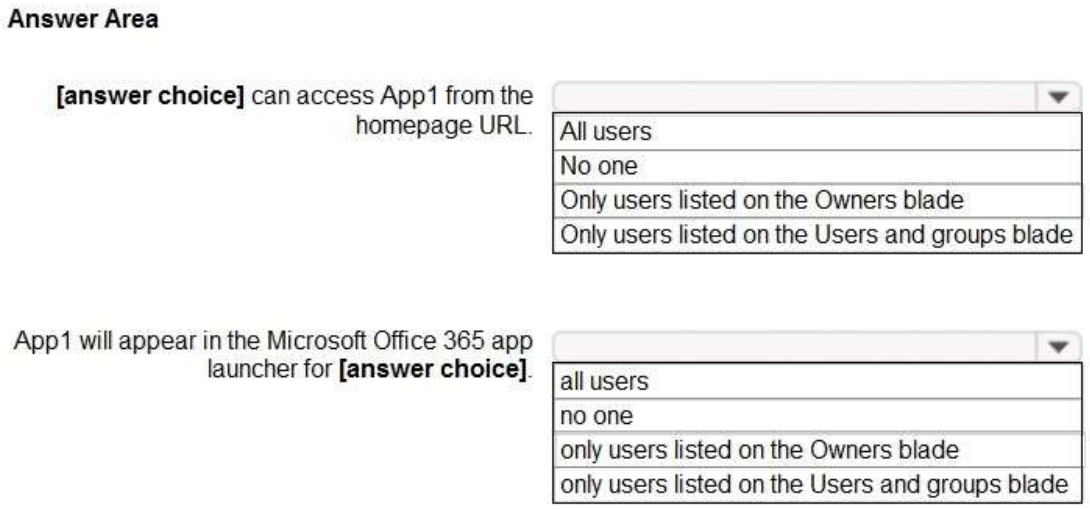
QUESTION 51
Hotspot Question
You have a custom cloud app named App1 that is registered in Azure Active Directory (Azure AD).
App1 is configured as shown in the following exhibit.



Save | Discard | Delete | Got feedback?

Enabled for users to sign-in?	[✓ Yes] No
Name	App1
Homepage URL	https://app1.m365x629615.onmicrosoft.com/
Logo	AP Select a file
User access URL	https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...
Application ID	09df58d6-d29d-40de-b0d0-321fdc63c665
Object ID	03709d22-7e61-4007-a2a0-04dbdff269cd
Terms of Service Url	Publisher did not provide this information
Privacy Statement Url	Publisher did not provide this information
Reply Url	https://contoso.com/App1/logon
User assignment required?	Yes [✓ No]
Visible to users?	[✓ Yes] No

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 Area

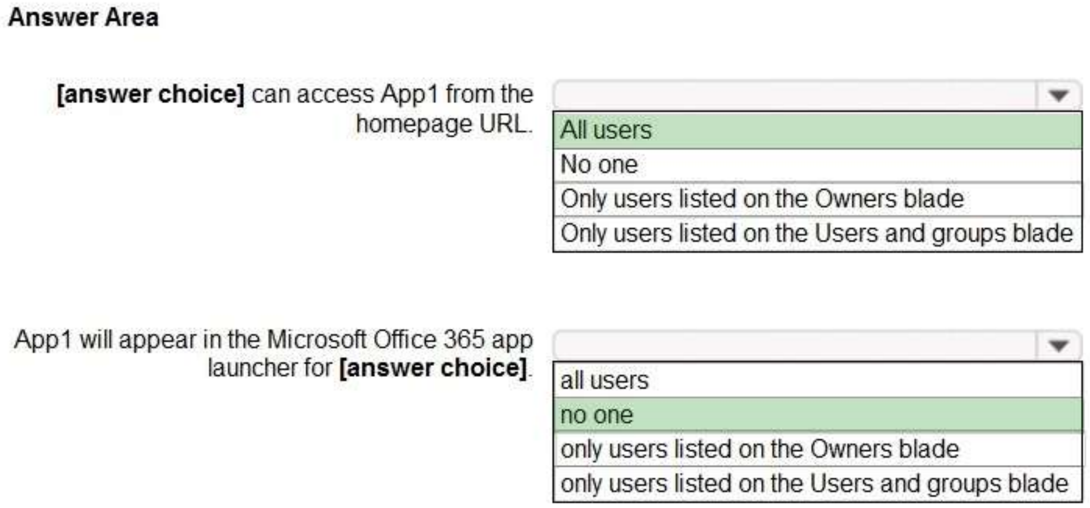
[answer choice] can access App1 from the homepage URL.

- All users
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- no one
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Answer:



Answer Area

[answer choice] can access App1 from the homepage URL.

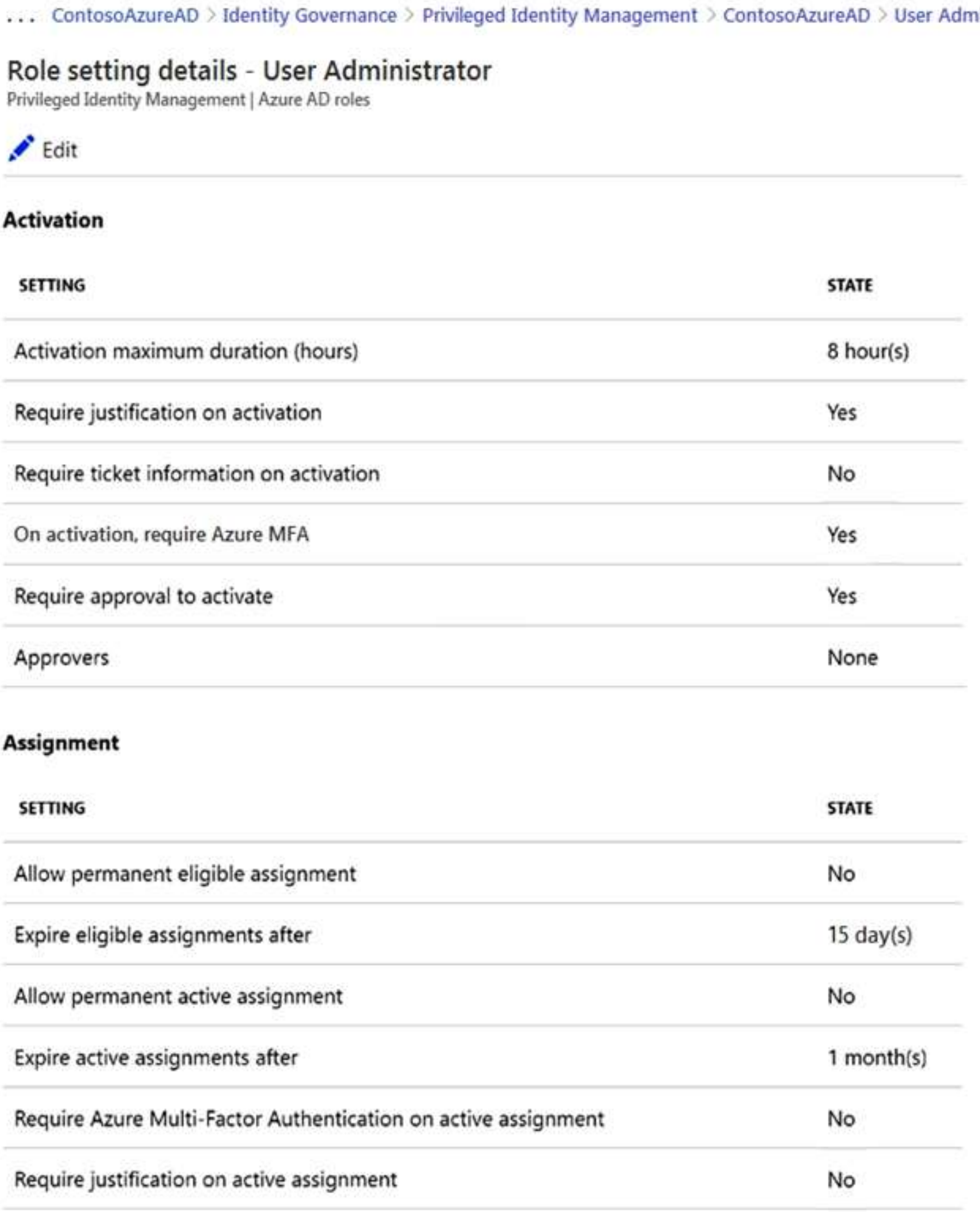
- [✓ All users]
- No one
- Only users listed on the Owners blade
- Only users listed on the Users and groups blade

App1 will appear in the Microsoft Office 365 app launcher for [answer choice].

- all users
- [✓ no one]
- only users listed on the Owners blade
- only users listed on the Users and groups blade

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal

QUESTION 52
Hotspot Question
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.



... ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD > User Administrator >

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Activation

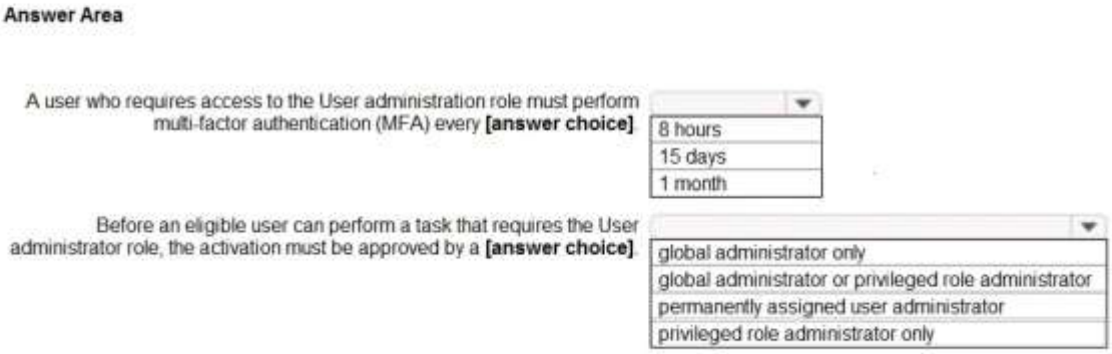
SETTING	STATE
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	Yes
Approvers	None

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

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 Area

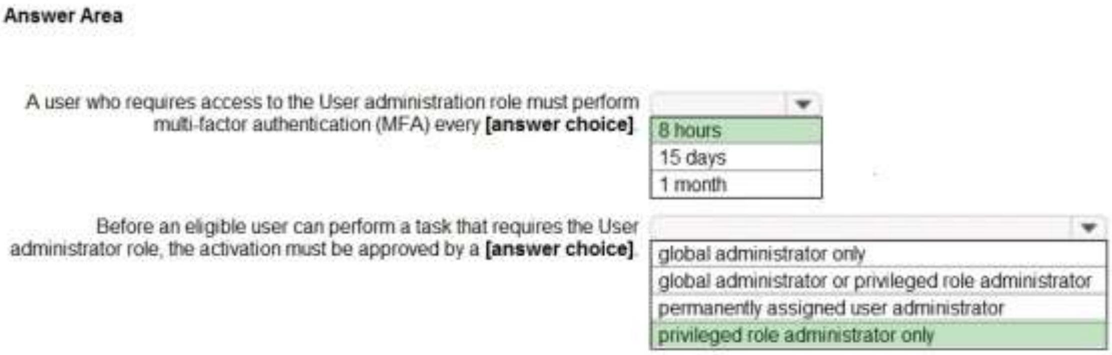
A user who requires access to the User administration role must perform multi-factor authentication (MFA) every **[answer choice]**

- 8 hours
- 15 days
- 1 month

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

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

Answer:



Answer Area

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

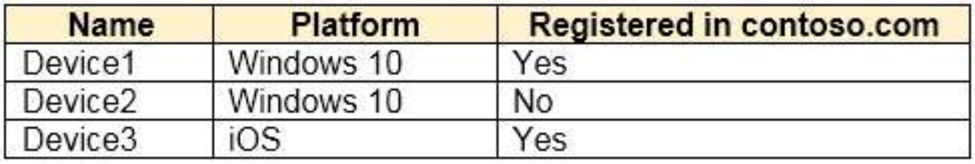
- [✓ 8 hours]
- 15 days
- 1 month

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

- global administrator only
- global administrator or privileged role administrator
- permanently assigned user administrator
- [✓ privileged role administrator only]

Explanation:
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

QUESTION 53
Hotspot Question
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1.
User1 has the devices shown in the following table.

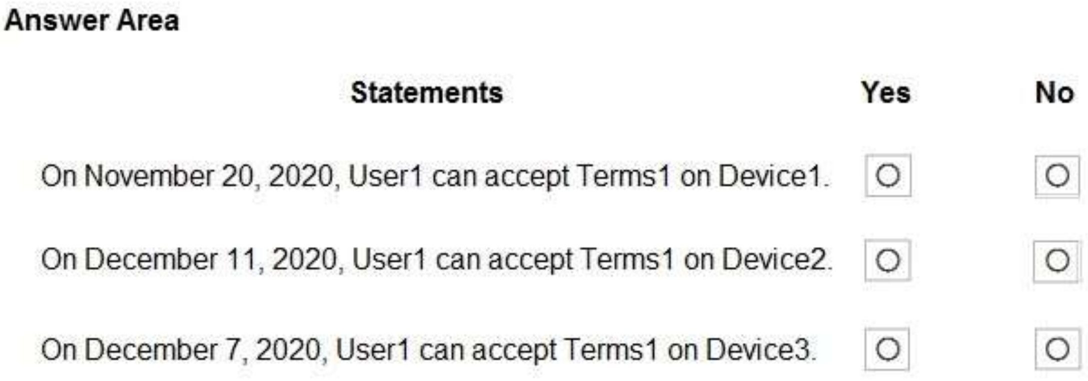


Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

On November 5, 2020, you create and enforce terms of use in contoso.com that has the following settings:

```
- Name: Terms1
- Display name: Contoso terms of use
- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2020
- Frequency: Monthly
```

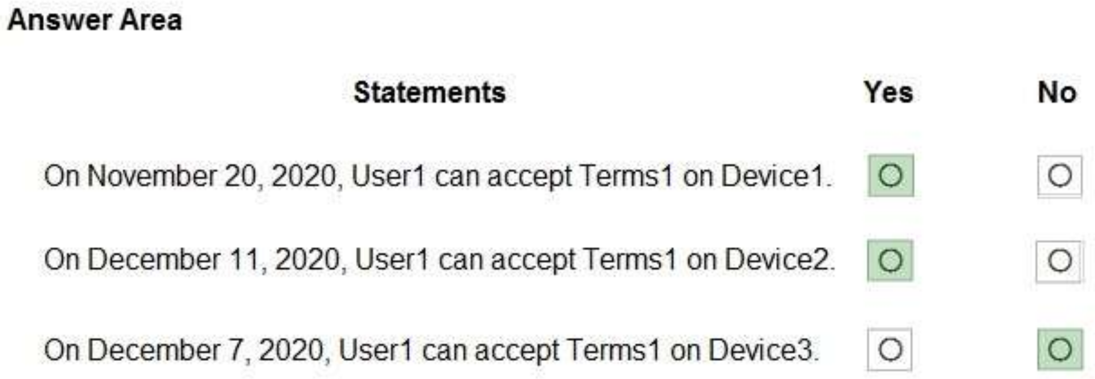
On November 15, 2020, User1 accepts Terms1 on Device3.
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.



Answer Area

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

Answer:



Answer Area

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

Explanation:

Box 1: Yes because User1 has not yet accepted the terms on Device1.

Box 2: Yes because User1 has not yet accepted the terms on Device2. User1 will be prompted to register the device before the terms can be accepted.

Box 3: No because User1 has already accepted the terms on Device3. The terms do not expire until December 10th and then monthly after that.

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

QUESTION 54

Case Study 1 - Contoso, Ltd

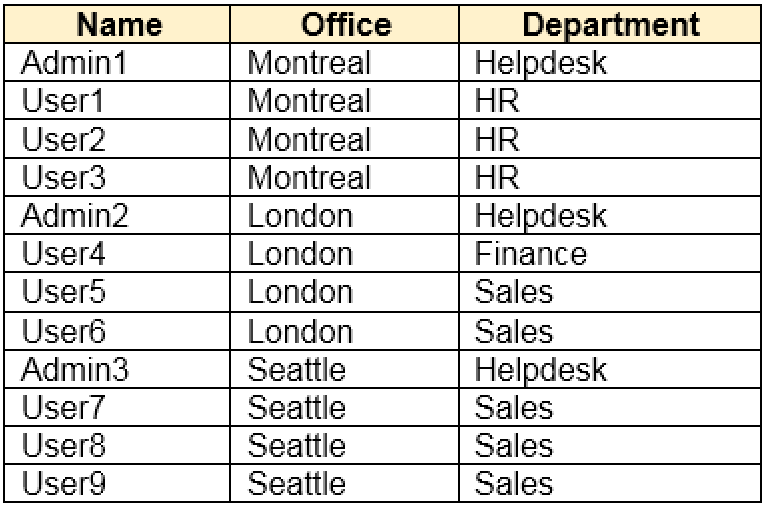
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources 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

Existing Environment. 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 E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (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 users have all 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 protect administrative roles.

Existing Environment. 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.

Requirements. 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 Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

- All 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.

You need to meet the planned changes for the User administrator role.

What should you do?

A. Create an access review.
B. Create an administrative unit.
C. Modify Active assignments.
D. Modify Role settings.

Answer: C

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user?tabs=new

QUESTION 55

Case Study 1 - Contoso, Ltd

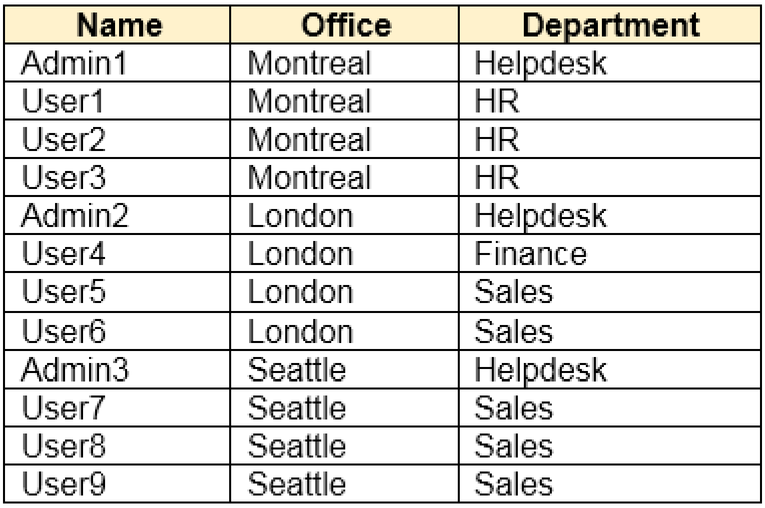
Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources 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

Existing Environment. 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 E3
- Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (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 users have all 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 protect administrative roles.

Existing Environment. 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.

Requirements. 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 Adatum Corporation. One hundred new ADatum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

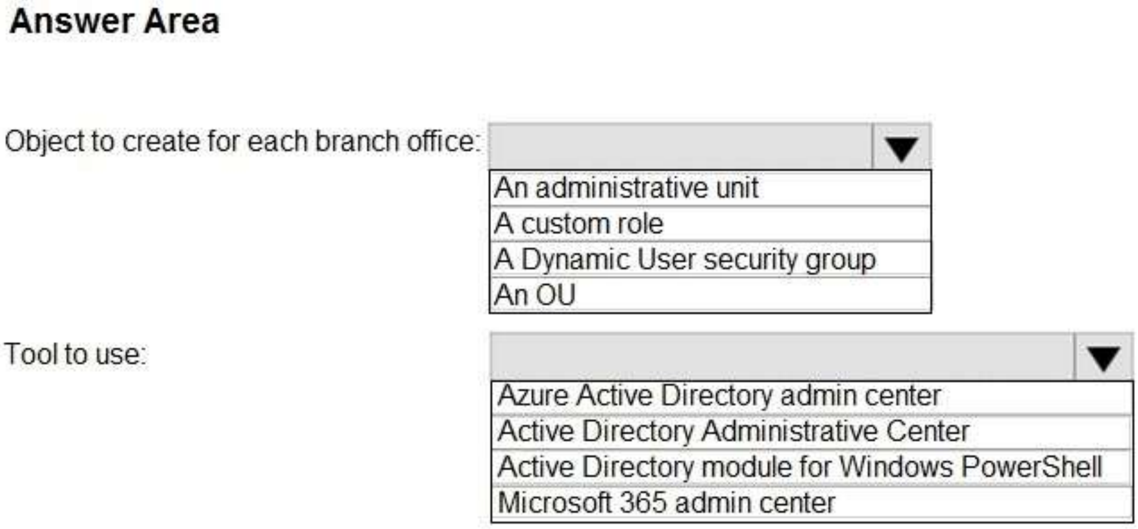
- All users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth- response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing 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.

Hotspot Question

You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

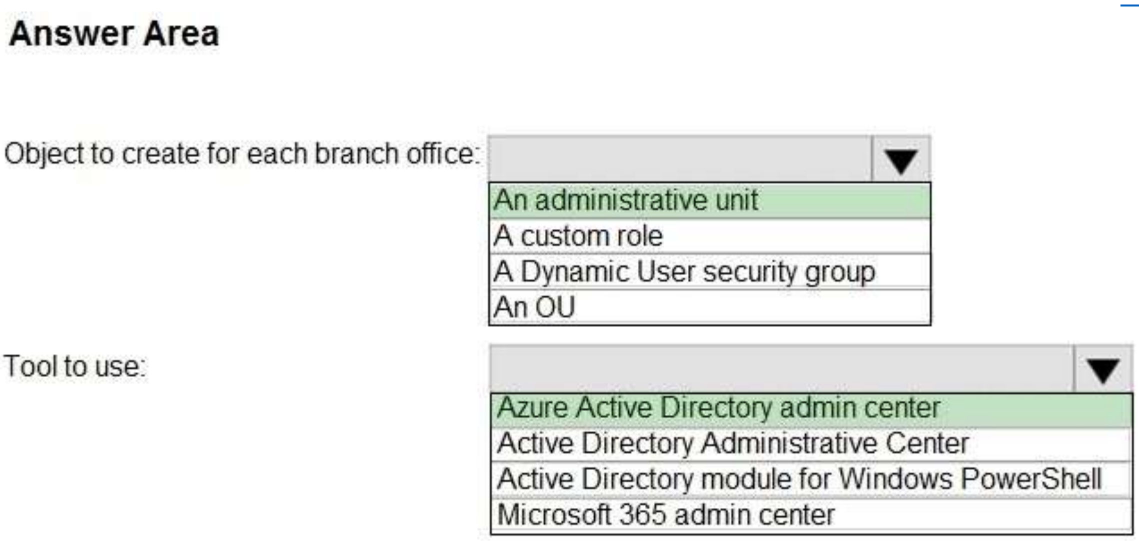


Answer Area

Object to create for each branch office:
- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:
- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Answer:



Answer Area

Object to create for each branch office:

- [✓ An administrative unit]
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- [✓ Azure Active Directory admin center]
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units
https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage

QUESTION 56
Case Study 2 - Litware, Inc
Overview

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 VPN connection.

Existing Environment. Identify 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 synchronization 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 litware.com by using guest accounts in the litware.com tenant.

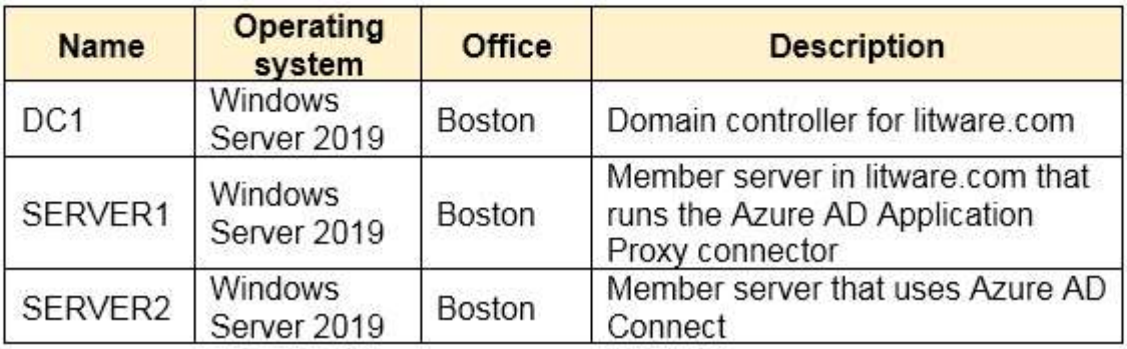
Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription 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 audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers 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.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged 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.

Requirements. 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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management 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.

Requirements. 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.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

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 include in the configuration?

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: B

Explanation:

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

QUESTION 57

Case Study 2 - Litware, Inc

Overview

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 VPN connection.

Existing Environment. Identify 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 synchronization 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 litware.com by using guest accounts in the litware.com tenant.

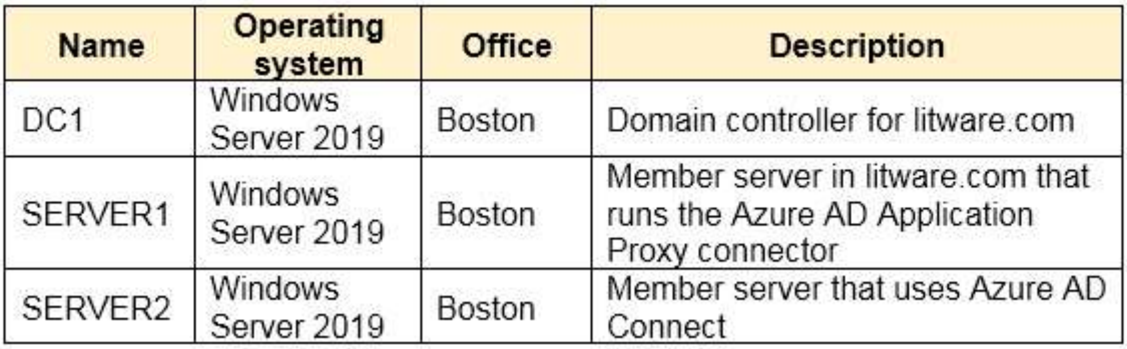
Existing Environment. Cloud Environment

All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection policies in Microsoft Cloud App Security are enabled.

Litware has an Azure subscription 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 audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers 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.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- Delegate the management of privileged roles by using Azure AD Privileged 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.

Requirements. 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 a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management 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.

Requirements. 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.

Requirements. Access Requirements

Litware identifies the following access requirements:

- Control all access to all Azure resources and Azure AD applications by using conditional access policies.
- Implement a conditional access policy that has session controls for Microsoft SharePoint Online.
- Control privileged access to applications by using access reviews in Azure AD.

Requirements. Monitoring Requirements

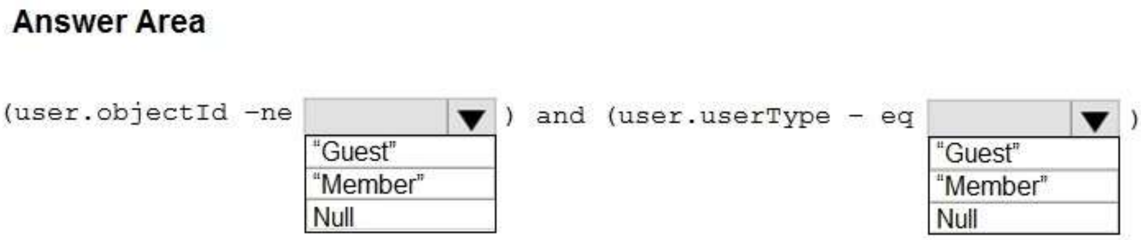
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged attacks that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

Hotspot Question

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



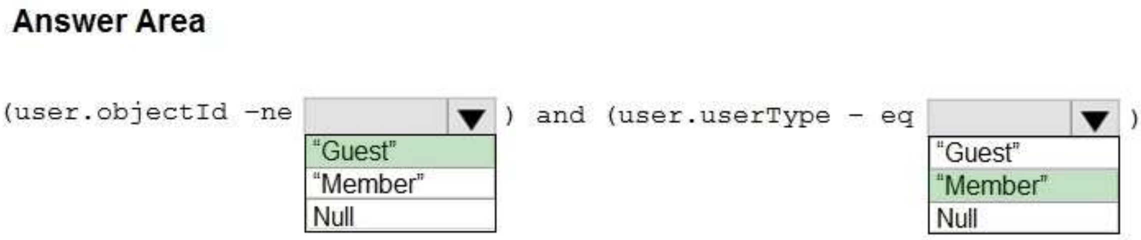
Answer Area

(user.objectId -ne [▼]) and (user.userType - eq [▼])

First dropdown:
- "Guest"
- "Member"
- Null

Second dropdown:
- "Guest"
- "Member"
- Null

Answer:



Answer Area

(user.objectId -ne [▼]) and (user.userType - eq [▼])

First dropdown:
- [✓ "Guest"]
- "Member"
- Null

Second dropdown:
- "Guest"
- [✓ "Member"]
- Null