

Microsoft.SC-300.vFeb-2024.by.Isata.111q

Number: SC-300
Passing Score: 800
Time Limit: 120
File Version: 19.4

Exam Code: SC-300
Exam Name: Microsoft Identity and Access Administrator



Exam A

QUESTION 1

You have a Microsoft 365 subscription that contains the following:

- An Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium P2 license
- A Microsoft SharePoint Online site named Site1
- A Microsoft Teams team named Team1

You need to create an entitlement management workflow to manage Site1 and Team1. What should you do first?

- A. Create an access package.
- B. Create a catalog.
- C. Create an administrative unit.
- D. Configure an app registration.

Correct Answer: A

Section:

QUESTION 2

You have an Azure subscription that contains the custom roles shown in the following table.

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

You need to create a custom Azure subscription role named Role3 by using the Azure portal. Role3 will use the baseline permissions of an existing role. Which roles can you clone to create Role3?

- A. Role2 only
- B. built-in Azure subscription roles only
- C. built-in Azure subscription roles and Role2 only
- D. built-in Azure subscription roles and built-in Azure AD roles only
- E. Role1, Role2 built-in Azure subscription roles, and built-in Azure AD roles

Correct Answer: C

Section:

QUESTION 3

You have a Microsoft 365 tenant.

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

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. Cloud App Discovery in Microsoft Defender for Cloud Apps
- B. enterprise applications in Azure AD
- C. access reviews in Azure AD

D. Application Insights in Azure Monitor

Correct Answer: A

Section:

QUESTION 4

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 Service support administrator role.
- B. From the identity Governance blade, modify the Entitlement management settings.
- C. From the Identity Governance blade, modify the roles and administrators for the General catalog
- D. From the Roles and administrators blade, modify the Groups administrator role.

Correct Answer: B

Section:

QUESTION 5

DRAG DROP

You have a Microsoft 365 E5 tenant. You purchase a cloud app named App1. You need to enable real-time session-level monitoring of App1 by using Microsoft Cloud App Security. In which order should you perform the actions? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

| Actions | Answer Area |
|---|-------------|
| From Microsoft Cloud App Security, create a session policy. | |
| Publish App1 in Azure Active Directory (Azure AD). | ⬅️ |
| Create a conditional access policy that has session controls configured. | ➡️ |
| From Microsoft Cloud App Security, modify the Connected apps settings for App1. | ⬆️ ⬇️ |

Correct Answer:

| Actions | Answer Area |
|---------|---|
| | Publish App1 in Azure Active Directory (Azure AD). |
| | From Microsoft Cloud App Security, modify the Connected apps settings for App1. |
| | From Microsoft Cloud App Security, create a session policy. |
| | Create a conditional access policy that has session controls configured. |

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app>

<https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad>

QUESTION 6

HOTSPOT

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](#)

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

Enable policy

Report-only On Off

Create

Include

Exclude

- None
- All users
- Select users and groups

- All guest users (preview) ⓘ
- Directory roles (preview) ⓘ
- Users and groups

Select ⓘ >

1 user

US User1
user1@sk200922outlook.onm...

Vdumps

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.

Hot Area:

Answer Area

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

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 |

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

Answer Area:

Answer Area

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

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 |

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

Section:

Explanation:

Reference:

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

QUESTION 7

HOTSPOT

You have a Microsoft 365 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.

Hot Area:

Answer Area

Configure HighRiskCountries by using:

| | |
|--------------------------|-----------------------|
| <input type="checkbox"/> | A cloud app or action |
| <input type="checkbox"/> | A condition |
| <input type="checkbox"/> | A grant control |
| <input type="checkbox"/> | A session control |

Configure Sign-in frequency by using:

| | |
|--------------------------|-----------------------|
| <input type="checkbox"/> | A cloud app or action |
| <input type="checkbox"/> | A condition |
| <input type="checkbox"/> | A grant control |
| <input type="checkbox"/> | A session control |

Answer Area:

Answer Area

Configure HighRiskCountries by using:

▼

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

Configure Sign-in frequency by using:

▼

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

Section:

Explanation:

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

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

QUESTION 8

HOTSPOT

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.

Hot Area:

| Statements | Yes | No |
|--|--------------------------|--------------------------|
| User1 can accept the invitation and gain access to the enterprise application. | <input type="checkbox"/> | <input type="checkbox"/> |
| User2 can access the enterprise application. | <input type="checkbox"/> | <input type="checkbox"/> |
| User3 can accept the invitation and gain access to the SharePoint site. | <input type="checkbox"/> | <input type="checkbox"/> |

Answer Area:

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 can accept the invitation and gain access to the enterprise application. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 can access the enterprise application. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can accept the invitation and gain access to the SharePoint site. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

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 9

DRAG DROP

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.

Select and Place:



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



Correct 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.



Section:

Explanation:

Reference:

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

QUESTION 10

HOTSPOT

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.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

Department1 Administrative Unit | Users (Preview)

ContosoAzureAD - Azure Active Directory

+ Add member | Remove member | Bulk operations | Refresh | Columns | Preview features | Got feedback?

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

Search users | Add filters

2 users found

| Name | User principal name | User type | Directory synced |
|-----------------------------------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> US User1 | User1@m365x629615.onmicrosoft.com | Member | No |
| <input type="checkbox"/> US 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

+ Add | Remove | Refresh | Columns | Preview features | Got feedback?

Search groups | Add filters

2 groups found

| Name | Group Type | Membership Type |
|------------------------------------|------------|-----------------|
| <input type="checkbox"/> GR Group1 | Security | Assigned |
| <input type="checkbox"/> 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

» + Add assignments ⚙ Settings ↻ Refresh ↓ Export | ❤ Got feedback?

Eligible assignments Active assignments Expired assignments

🔍 Search by member name or principal name

| Name | Principal name | Type | Scope |
|---------------------|------------------------------------|------|---|
| User 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

» + Add members 🗑 Remove ↻ Refresh 📄 Bulk operations | 📄 Columns | 🖨 Preview features | ❤ Got feedback?

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

Direct members

| Name | User type |
|--|-----------|
| <input type="checkbox"/>  User3 | Member |
| <input type="checkbox"/>  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.


Hot Area:

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/> | <input type="radio"/> |
| Admin1 can add User1 to Group 2 | <input type="radio"/> | <input type="radio"/> |
| Admin 2 can reset the password of User1. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area



| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| Admin1 can reset the passwords of User3 and User4. | <input type="radio"/> | <input checked="" type="radio"/> |
| Admin1 can add User1 to Group 2 | <input type="radio"/> | <input checked="" type="radio"/> |
| Admin 2 can reset the password of User1. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

Reference:

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

QUESTION 11

HOTSPOT

You have a Microsoft 365 tenant.

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

- Identify sign-ins 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 in the answer area.

Hot Area:

Answer Area

The screenshot shows the 'High-risk sign-ins' remediation configuration page in the Microsoft 365 security center. It contains three dropdown menus:

- To classify leaked credentials as high-risk, use:** This dropdown is open, showing options: Azure Active Directory (Azure AD) Identity Protection, Azure Active Directory (Azure AD) Privileged Identity Management (PIM), Identity Governance, and Self-service password reset (SSPR).
- To trigger remediation, use:** This dropdown is open, showing options: Client apps not using Modern authentication, Device state, Sign-in risk (highlighted), User location, and User risk.
- To mitigate the risk, select:** This dropdown is open, showing options: Apply app enforced restrictions, Block access, Grant access but require app protection policy, and Grant access but require password change.

A watermark 'Vdumps' is visible over the center of the image.

Answer Area:



Section:

Explanation:



QUESTION 12

You have an Azure AD tenant that contains two users named User1 and User2. You plan to perform the following actions:

- Create a group named Group 1.
- Add User1 and User 2 to Group1.
- Assign Azure AD roles to Group1.

You need to create Group1.

Which two settings can you use? Each correct answer presents a complete solution

NOTE: Each correct selection is worth one point

- A. Group type: Microsoft 365 Membership type: Dynamic User
- B. Group type: Security Membership type: Dynamic Device
- C. Group type Security Membership type: Dynamic User
- D. Group type Security Membership type: Assigned
- E. Group type: Microsoft 365 Membership type: Assigned

Correct Answer: D, E

Section:

QUESTION 13

DRAG DROP

You have a Microsoft 365 E5 subscription and an Azure subscription. You need to meet the following requirements:

- Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials.

- Delegate the ability to create new virtual machines.

What should you use for each requirement? To answer, drag the appropriate features to the correct requirements. Each feature may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Select and Place:

Correct Answer:

Section:

Explanation:



QUESTION 14

HOTSPOT

Your network contains an on-premises Active Directory Domain services (AD DS) domain that syncs with an Azure AD tenant. The AD DS domain contains the organizational units (OUs) shown in the following table.

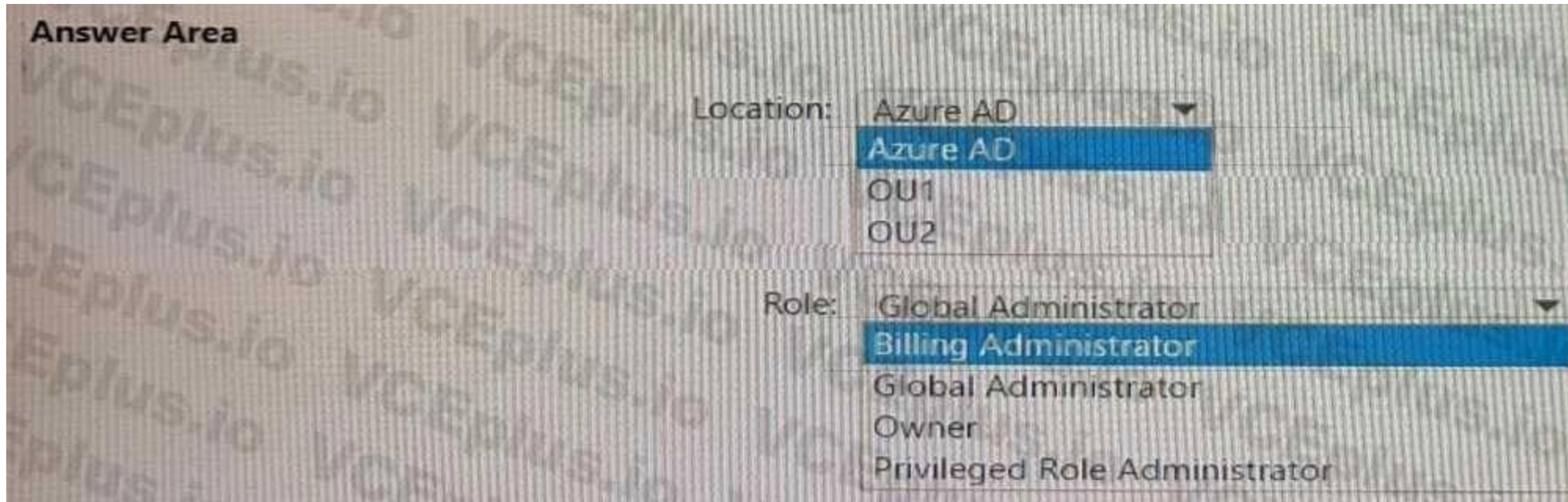
| Name | Description |
|------|------------------------------------|
| OU1 | Syncs with Azure AD |
| OU2 | Does NOT sync with Azure AD |

You need to create a break-glass account named BreakGlass.

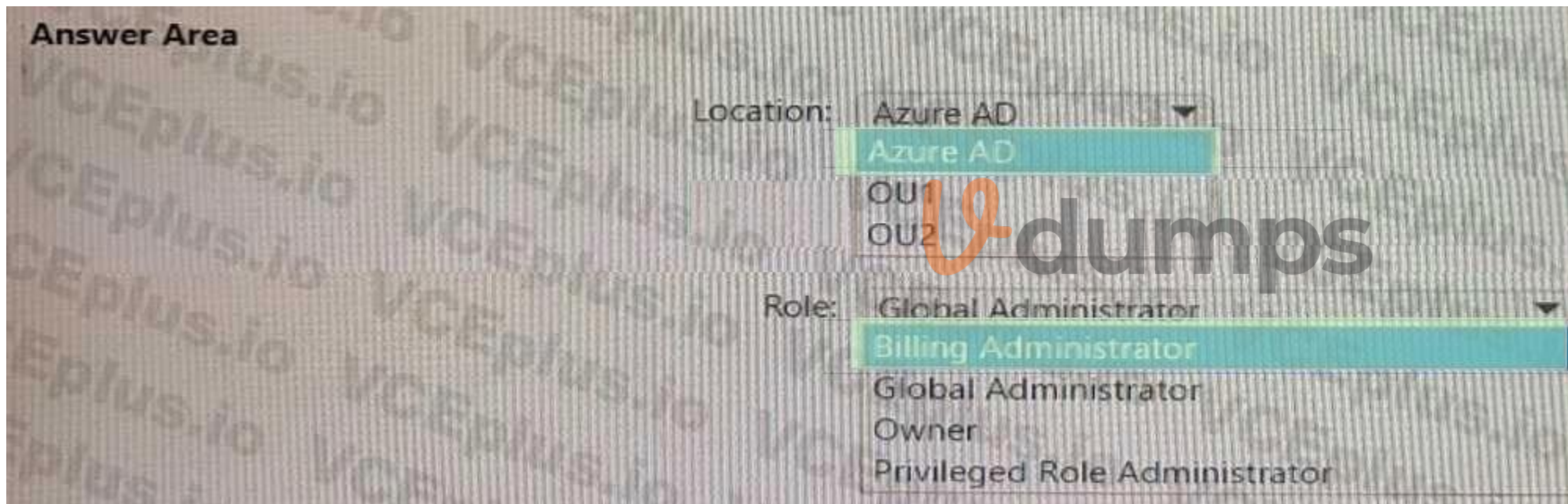
Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 15

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 compliance policy
- B. an access review for application access
- C. a guest access review
- D. a Conditional Access policy

Correct Answer: C

Section:

QUESTION 16

HOTSPOT

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.

Hot Area:

Answer Area

Feature:

- An authentication method policy
- A Conditional Access policy
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- 14 days
- 28 days

Answer Area:

Answer Area

Feature:

- An authentication method policy
- A Conditional Access policy
- An MFA registration policy
- The Multi-Factor Authentication Server settings

Grace period:

- 7 days
- 14 days
- 28 days

Section:

Explanation:

QUESTION 17

You need to resolve the issue of the guest user invitations. What should you do for the Azure AD tenant?

- A. Configure the Continuous access evaluation settings
- B. Modify the External collaboration settings.
- C. Configure the Access reviews settings
- D. Configure a Conditional Access policy.

Correct Answer: B

Section:

QUESTION 18

DRAG DROP

You have a Microsoft 365 E5 subscription. You need to perform the following tasks:

- Identify the locations and IP addresses used by Azure AD users to sign in
- Review the Azure AD security settings and identify improvement recommendations.
- Identify changes to Azure AD users or service principle.

What should you use for each task? To answer, drag the appropriate resources to the correct requirements. Each resource may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Select and Place:

Resources

- Audit logs
- Identity secure score
- Provisioning logs
- Sign-in logs

Answer Area

Identify the locations and IP addresses used by Azure AD users to sign in:

Identify changes to Azure AD users or service principals:

Review the Azure AD security settings and identify improvement recommendations:

Correct Answer:

Resources

-
-
- Provisioning logs
-

Answer Area

Identify the locations and IP addresses used by Azure AD users to sign in:

Identify changes to Azure AD users or service principals:

Review the Azure AD security settings and identify improvement recommendations:

Section:

Explanation:

QUESTION 19

You have an Azure Active Directory (Azure AD) tenant that uses conditional access policies.

You plan to use third-party security information and event management (SIEM) to analyze conditional access usage.

You need to download the Azure AD log that contains conditional access policy data.

What should you export from Azure AD?

- A. sign-ins in JSON format
- B. sign-ins in CSV format
- C. audit logs in JSON format
- D. audit logs in CSV format

Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs>

QUESTION 20

You have an Azure Active Directory (Azure AD) tenant.

You need to review the Azure AD sign-ins log to investigate sign ins that occurred in the past.

For how long does Azure AD store events in the sign-in log?

- A. 14 days
- B. 30 days
- C. 90 days
- D. 365 days

Correct Answer: B

Section:

QUESTION 21

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

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pimdeployment-plan>

QUESTION 22

You have a Microsoft 365 tenant.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor. What should you do first?

- A. Run the Get-AzureADAuditDirectoryLogs cmdlet.
- B. Create an Azure AD workbook.
- C. Run the Set-AzureADTenantDetail cmdlet.
- D. Modify the Diagnostics settings for Azure AD.

Correct Answer: A

Section:

QUESTION 23

You have an Azure Active Directory (Azure AD) tenant.

For the tenant, Users can register applications is set to No.

A user named Admin1 must deploy a new cloud app named App1.

You need to ensure that Admin1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which role should you assign to Admin1?

- A. Application developer in Azure AD
- B. App Configuration Data Owner for Subscription1
- C. Managed Application Contributor for Subscription1
- D. Cloud application administrator in Azure AD

Correct Answer: A

Section:

Explanation:

Reference:

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



QUESTION 24

Your company requires that users request access before they can access corporate applications.

You register a new enterprise application named MyApp1 in Azure Active Directory (Azure AD) and configure single sign-on (SSO) for MyApp1.

Which settings should you configure next for MyApp1?

- A. Self-service
- B. Provisioning
- C. Roles and administrators
- D. Application proxy

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

QUESTION 25

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 see 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?

- From Users and groups, add HRUsers.
- From Properties, change User assignment required to No.
- From Permissions, review the User consent permissions.
- From Single sign on, configure a sign-on method.

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-accessportal>

<https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portalworkspaces>

QUESTION 26

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?

- Group1 and Group
- Group2 only
- Group3 only
- Group1 only
- Group1 and Group4

Correct Answer: A

Section:

QUESTION 27

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 resource-, by using conditional access policy.

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.

Correct Answer: B

Section:

QUESTION 28

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.

Correct Answer: C

Section:

Explanation:

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>



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

Correct Answer: C

Section:

QUESTION 30

You have an Azure Active Directory (Azure AD) tenant.

You configure self-service password reset (SSPR) by using the following settings:

- Require users to register when signing in: Yes
- Number of methods required to reset: 1

What is a valid authentication method available to users?

- A. home phones
- B. mobile app notification
- C. a mobile app code
- D. an email to an address in your organization

Correct Answer: C

Section:

QUESTION 31

You have a Microsoft 365 tenant.

You currently allow email clients that use Basic authentication to connect to Microsoft Exchange Online.

You need to ensure that users can connect to Exchange only run email clients that use Modern authentication protocols.

What should you implement?

You need to ensure that use Modern authentication

- A. a compliance policy in Microsoft Endpoint Manager
- B. a conditional access policy in Azure Active Directory (Azure AD)
- C. an application control profile in Microsoft Endpoint Manager
- D. an OAuth policy in Microsoft Cloud App Security



Correct Answer: C

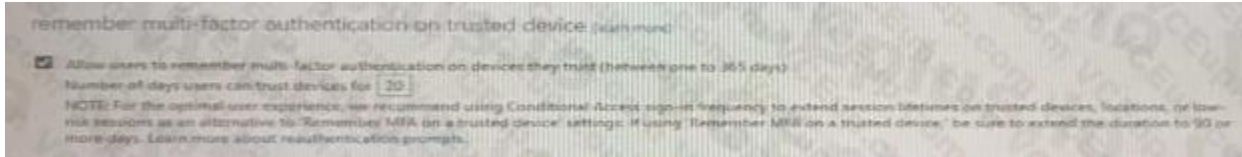
Section:

QUESTION 32

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 | Disabled |
| User2 | Enabled |
| User3 | Enforced |

B.

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

C.

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

D.

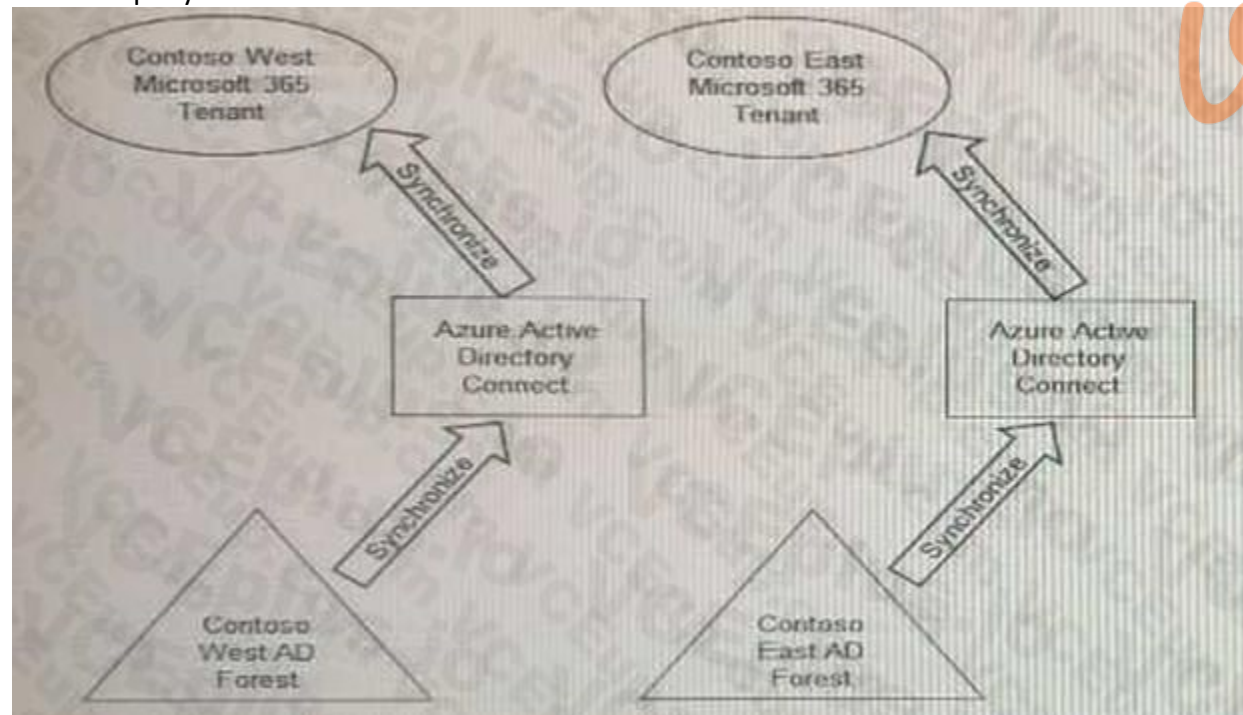
| Name | Multi-factor auth status |
|-------|--------------------------|
| User1 | Disabled |
| User2 | Enforced |
| User3 | Enforced |

Correct Answer: B

Section:

QUESTION 33

Your company has two divisions named Contoso East and Contoso West. The Microsoft 365 identity architecture for 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 365 licenses. What should you do?

- A. Configure The exiting Azure AD Connect server in Contoso Cast to sync the Contoso East Active Directory forest to the Contoso West tenant.
- B. Configure Azure AD Application Proxy in the Contoso West tenant.
- C. 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.
- D. Invite the Contoso East users as guests in the Contoso West tenant.

Correct Answer: D

Section:

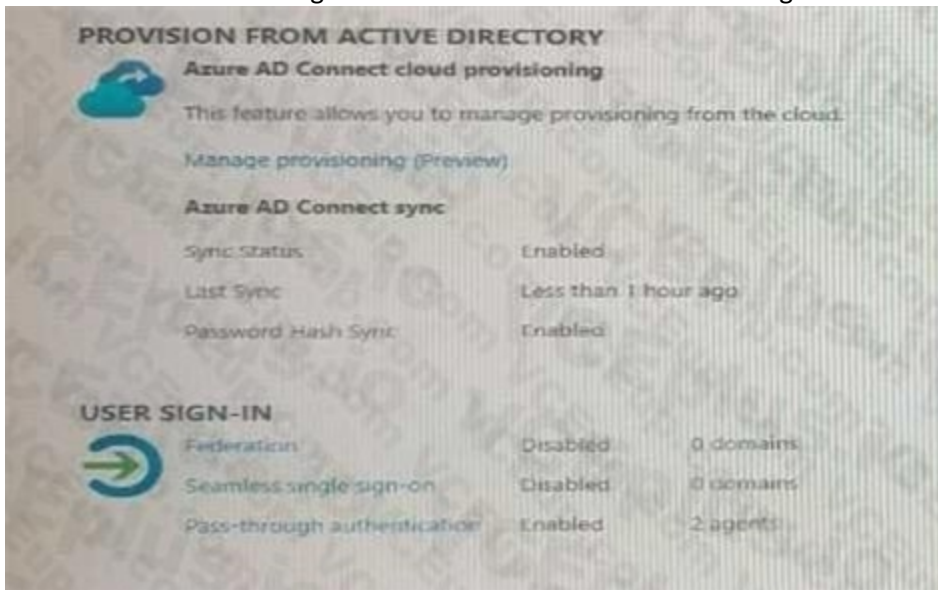
QUESTION 34

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 only
- B. User1 and User 3 only
- C. User1, and User2 only
- D. User1, User2, and User3

Correct Answer: A

Section:

QUESTION 35

You have an Azure Active Directory (Azure AD) tenant named contoso.com.

You need to ensure that Azure AD External Identities pricing is based on monthly active users (MAU).

What should you configure?

- A. an access review
- B. the terms of use
- C. a linked subscription
- D. a user flow



Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identitiespricing>

QUESTION 36

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, Group4, 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

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 37

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

Correct Answer: A

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-servicesignup>



QUESTION 38

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.

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 39

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs. You receive more than 100 email alerts each day for tailed 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 create an assignment for the Insights at administrator role. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 40

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs. You receive more than 100 email alerts each day for tailed Azure AD user sign-in attempts. You need to ensure that a new security administrator receives the alerts instead of you. Solution: From Azure monitor, you modify the action group. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 41

You use Azure Monitor to analyze Azure Active Directory (Azure AD) activity logs. You receive more than 100 email alerts each day for tailed Azure AD 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

Correct Answer: B
Section:

QUESTION 42

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 Block/unblock users settings for multi-factor authentication (MFA). Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section:

Explanation:

You need to configure the fraud alert settings.

Reference:

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

QUESTION 43

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 Account lockout settings for multi-factor authentication (MFA). Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B
Section:

Explanation:

You need to configure the fraud alert settings.

Reference:

[https://docs.microsoft.com/en-us/active-directory/authentication/howto-mfa-mfasettings](https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings)

QUESTION 44

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 Fraud alert settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

Explanation:

The fraud alert feature lets users report fraudulent attempts to access their resources. When an unknown and suspicious MFA prompt is received, users can report the fraud attempt using the Microsoft Authenticator app or through their phone.

The following fraud alert configuration options are available:

Automatically block users who report fraud.

Code to report fraud during initial greeting.

Reference:

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

QUESTION 45

You have an Azure Active Directory (Azure AD) tenant that contains the following objects:

A device named Device1

Users named User1, User2, User3, User4, and User5

Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

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

To which groups can you assign a Microsoft Office 365 Enterprise E5 license directly?

- A. Group1 and Group4 only
- B. Group1, Group2, Group3, Group4, and Group5
- C. Group1 and Group2 only
- D. Group1 only
- E. Group1, Group2, Group4, and Group5 only

Correct Answer: C

Section:

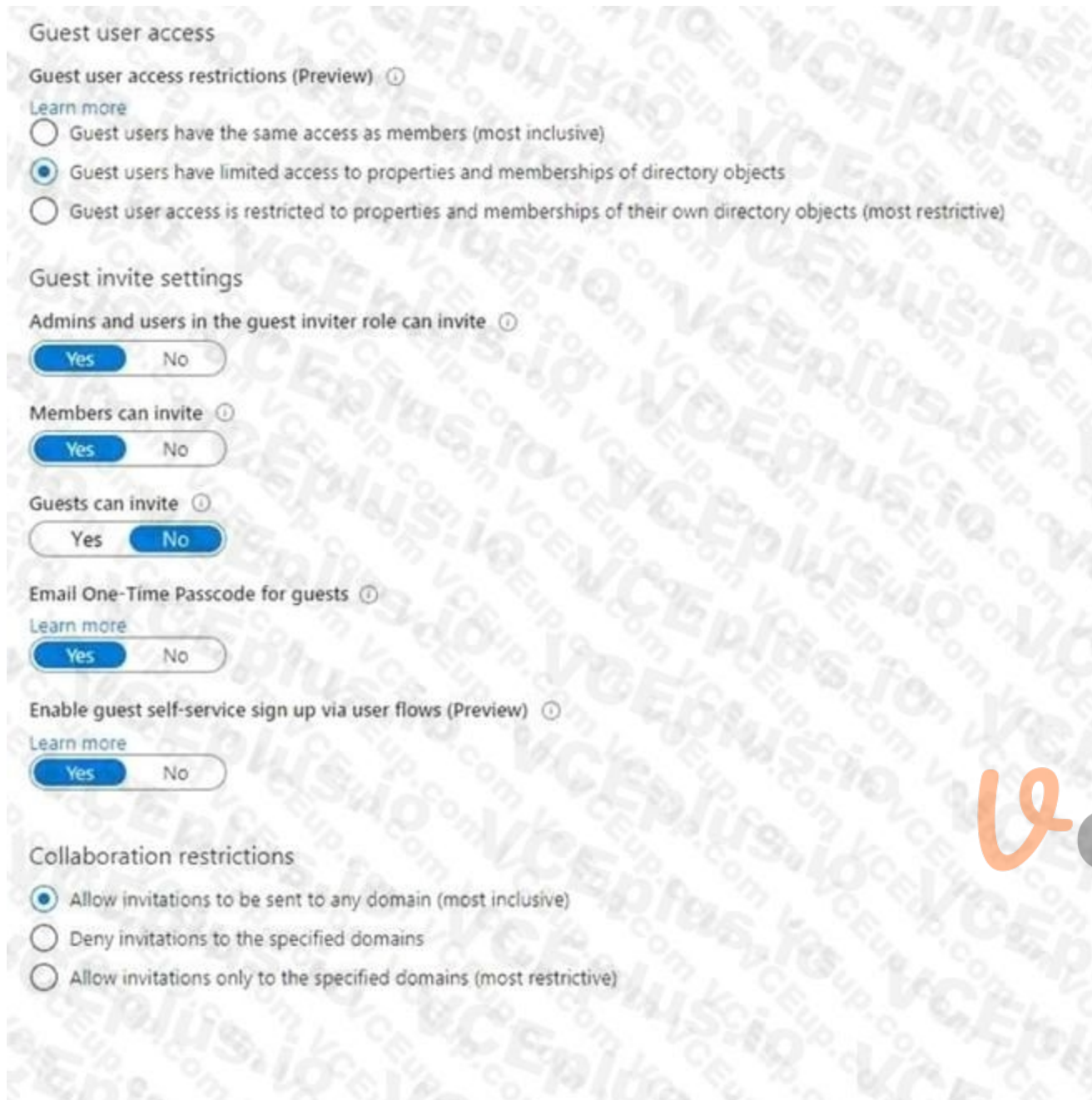
Explanation:

Reference:

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

QUESTION 46

You have a Microsoft 365 tenant that uses the domain named fabrikam.com. The Guest invite settings for Azure Active Directory (Azure AD) are configured as shown in the exhibit. (Click the Exhibit tab.)



A user named bsmith@fabrikam.com shares a Microsoft SharePoint Online document library to the users shown in the following table.

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

Which users will be emailed a passcode?

- A. User2 only
- B. User1 only
- C. User1 and User2 only
- D. User1, User2, and User3

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode>

QUESTION 47

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.

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-addguest-users-portal>

<https://docs.microsoft.com/en-us/powershell/module/azuread/newazureadmsinvitation?view=azureadps-2.0>

QUESTION 48

You have 2,500 users who are assigned Microsoft Office 365 Enterprise E3 licenses. The licenses are assigned to individual users.

From the Groups blade in the Azure Active Directory admin center, you assign Microsoft 365 Enterprise E5 licenses to the users.

You need to remove the Office 365 Enterprise E3 licenses from the users by using the least amount of administrative effort.

What should you use?

- A. the Administrative units blade in the Azure Active Directory admin center
- B. the Set-AzureAdUser cmdlet
- C. the Groups blade in the Azure Active Directory admin center
- D. the Sec-MsolUserLicense cmdlet

Correct Answer: C

Section:

Explanation:

QUESTION 49

You have an Azure Active Directory (Azure AD) tenant that contains cloud-based enterprise apps.

You need to group related apps into categories in the My Apps portal.

What should you create?

- A. tags
- B. collections
- C. naming policies
- D. dynamic groups

Correct Answer: B

Section:

Explanation:

Reference:

<https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-appsportal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d>

QUESTION 50

You have an Azure Active Directory Premium P2 tenant.

You create a Log Analytics workspace.

You need to ensure that you can view Azure Active Directory (Azure AD) audit log information by using Azure Monitor.

What should you do first?

- A. Run the Set-AzureADTenantDetail cmdlet.
- B. Create an Azure AD workbook.
- C. Modify the Diagnostics settings for Azure AD.
- D. Run the Get-AzureADAuditDirectoryLogs cmdlet.

Correct Answer: D

Section:

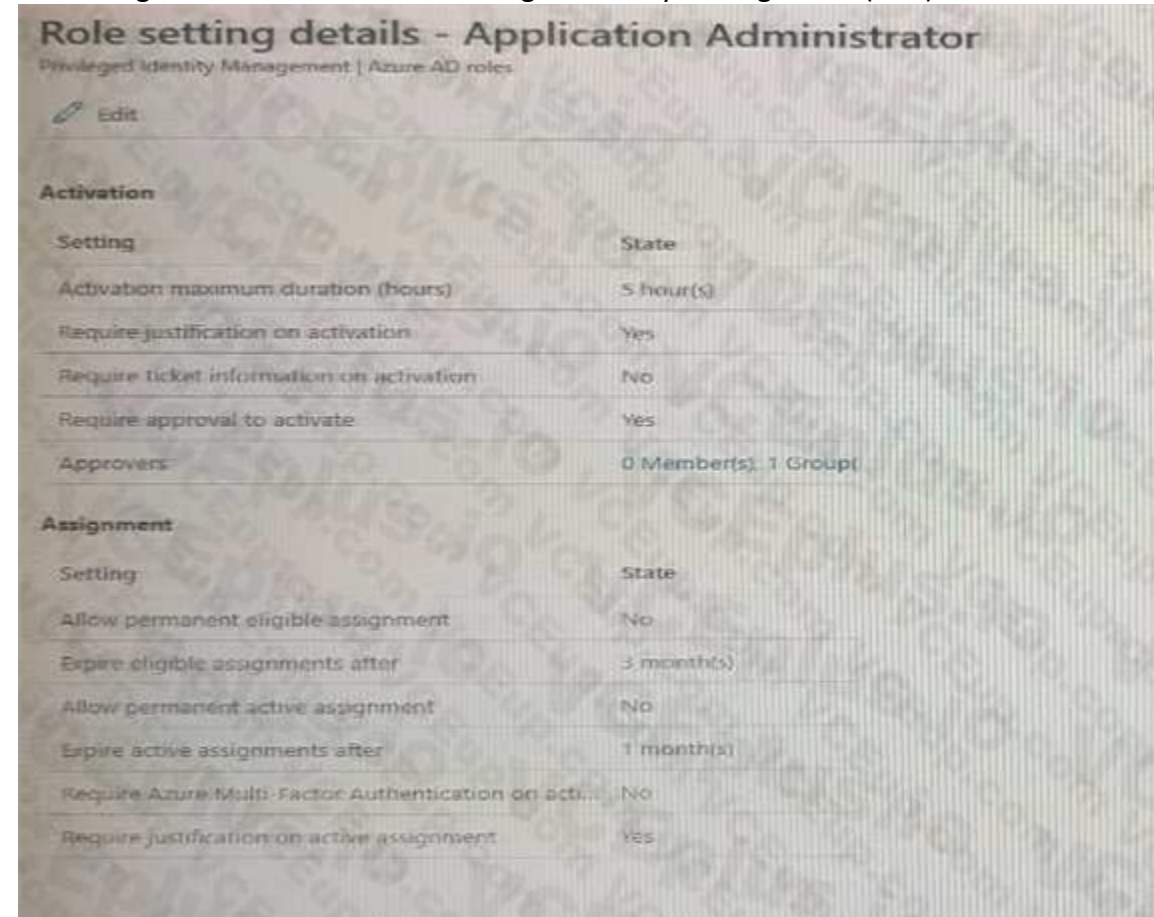
Explanation:

QUESTION 51

HOTSPOT

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 User2 to 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.

Hot Area:



Answer Area:



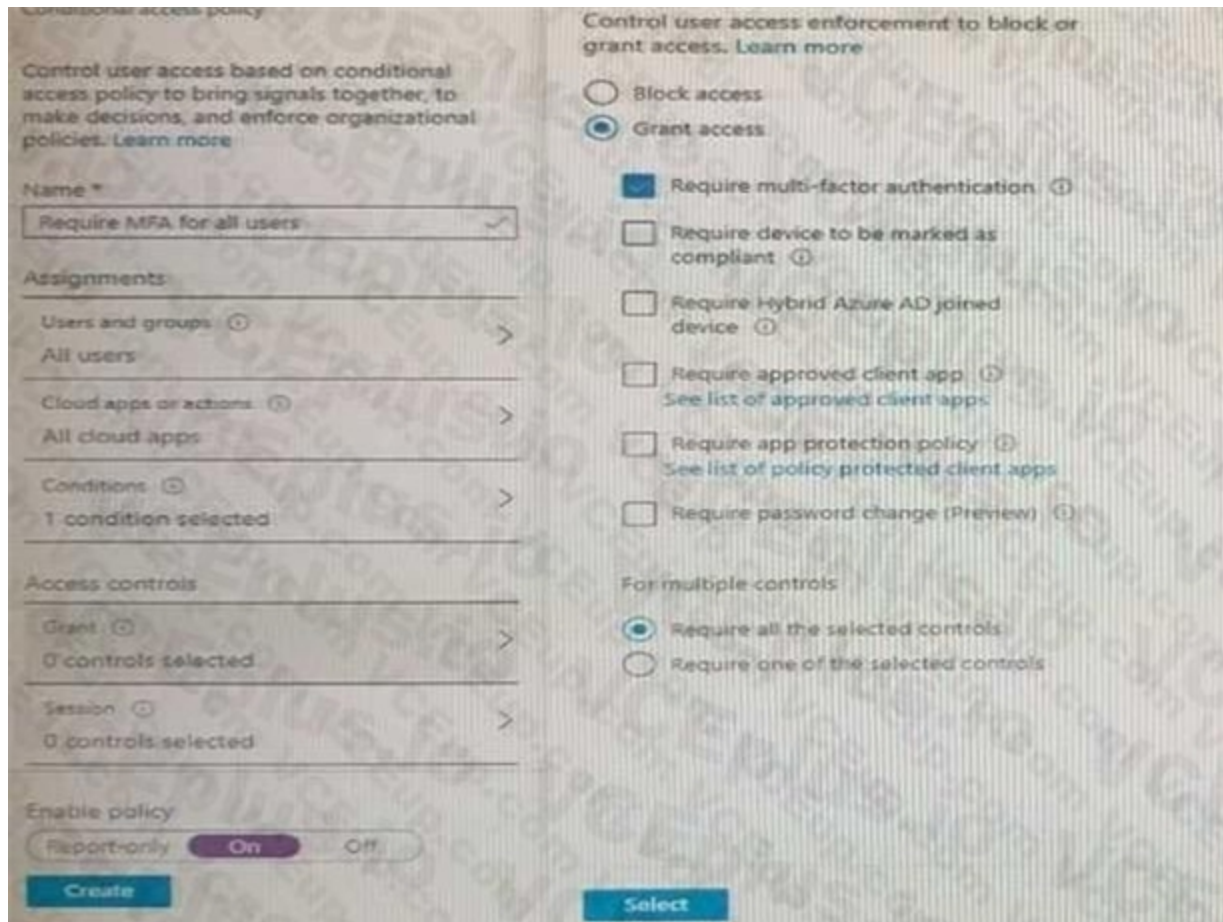
Section:

Explanation:

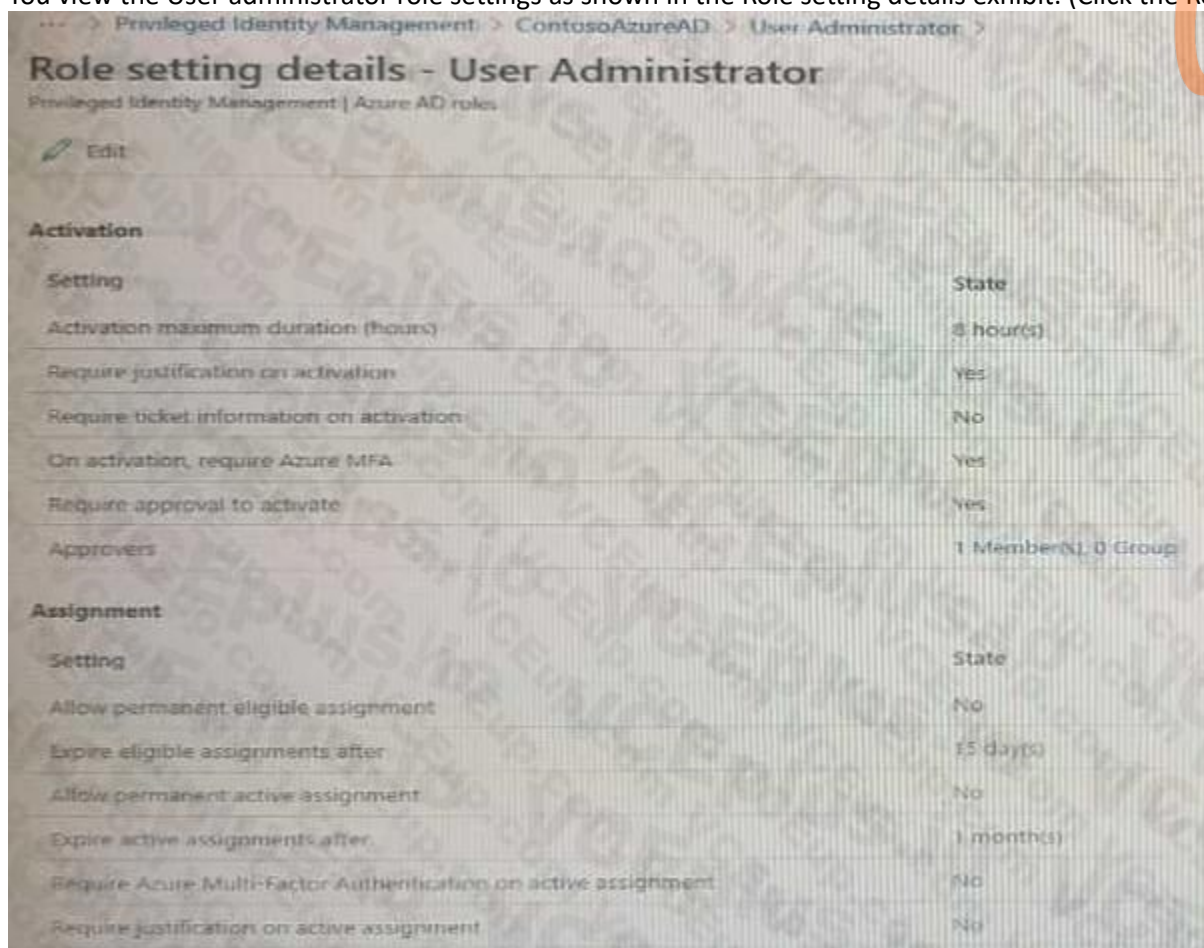
QUESTION 52

HOTSPOT

You have a Microsoft 365 tenant.
 You configure a conditional access policy as shown in the Conditional Access policy exhibit. (Click the Conditional Access policy tab.)



You view the User administrator role settings as shown in the Role setting details exhibit. (Click the Role setting details tab.)



You view the User administrator role assignments as shown in the Role assignments exhibit. (Click the Role assignments tab.)

ContosoAzureAD > Identity Governance > Privileged Identity Management > ContosoAzureAD >

User Administrator | Assignments

Privileged Identity Management | Azure AD roles

+ Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

| Name | Principal name | Type | Scope | Membership |
|--------------------|------------------------------------|------|-----------|------------|
| User Administrator | | | | |
| Admin1 | Admin1@m365x629615.onmicrosoft.com | User | Directory | Direct |
| Admin2 | Admin2@m365x629615.onmicrosoft.com | User | Directory | Direct |
| Admin3 | Admin3@m365x629615.onmicrosoft.com | User | Directory | Direct |

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request. | <input type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User administrator role for a period of two hours. | <input type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|-----------------------|
| Before Admin1 can perform a task that requires the User administrator role, an approver must approve the activation request. | <input checked="" type="radio"/> | <input type="radio"/> |
| Admin2 can request activation of the User administrator role for a period of two hours. | <input checked="" type="radio"/> | <input type="radio"/> |
| If Admin3 connects to the Azure Active Directory admin center, and then activates the User administrator role, Admin3 will be prompted to authenticate by using multi-factor authentication (MFA) twice. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

QUESTION 53

HOTSPOT

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.

Hot Area:

Answer Area

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

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

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

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

Answer Area:



Answer Area

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

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



Section:

Explanation:

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>

QUESTION 54

HOTSPOT

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

```
PS C:\> Get-AzureADGroup -searchstring "group1" | Get-AzureADGroupowner

ObjectId                DisplayName      UserPrincipalName      UserType
-----
a7f7d405-636f-4493-b971-5c2b7a131b1c Admin           admin@M365x629615.onmicrosoft.com Member

PS C:\> Get-AzureADGroup -searchstring "group1" | GetAzureADGroupMember | ft displayname

DisplayName
-----
User1
User4
Group3
```

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

App1 | Properties

Enterprise Application


- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators (Prev.)
 - Users and groups
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-ins

Save Discard Delete Got feedback?

Enabled for users to sign-in? Yes No

Name

Homepage URL

Logo 

User access URL

Application ID

Object ID

Terms of Service Url

Privacy Statement Url

Reply URL

User assignment required? Yes No

Visible to users? Yes No

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

Dashboard > ContosoAzureAD > Enterprise applications > App1

App1 | Self-service

Enterprise application

« Save Discard

Search

Allow users to request access to this application? Yes No

To which group should assigned users be added?

Require approval before granting access to this application? Yes No

Who is allowed to approve access to this application?

To which role should users be assigned in this application? *

Select approvers

- User1
User1@m365x629615.onmicrosoft.com
Selected
- User2
User2@m365x629615.onmicrosoft.com
- User3
User3@m365x629615.onmicrosoft.com
- User4
User4@m365x629615.onmicrosoft.com

Selected approvers

- User1
User1@m365x629615.onmicrosoft.com



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

Hot Area:

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| The members of Group3 can access App1 without first being approved by User1. | <input type="radio"/> | <input type="radio"/> |
| After you configure self-service for App1, the owner of Group1 is User1. | <input type="radio"/> | <input type="radio"/> |
| App1 appears in the Microsoft Office 365 app launcher of User4. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|--|-----------------------|----------------------------------|
| The members of Group3 can access App1 without first being approved by User1. | <input type="radio"/> | <input checked="" type="radio"/> |
| After you configure self-service for App1, the owner of Group1 is User1. | <input type="radio"/> | <input checked="" type="radio"/> |
| App1 appears in the Microsoft Office 365 app launcher of User4. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

Reference:

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

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

QUESTION 55

HOTSPOT

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

Homepage URL

Logo 

User access URL

Application ID

Object ID

Terms of Service Url

Privacy Statement Url

Reply Url

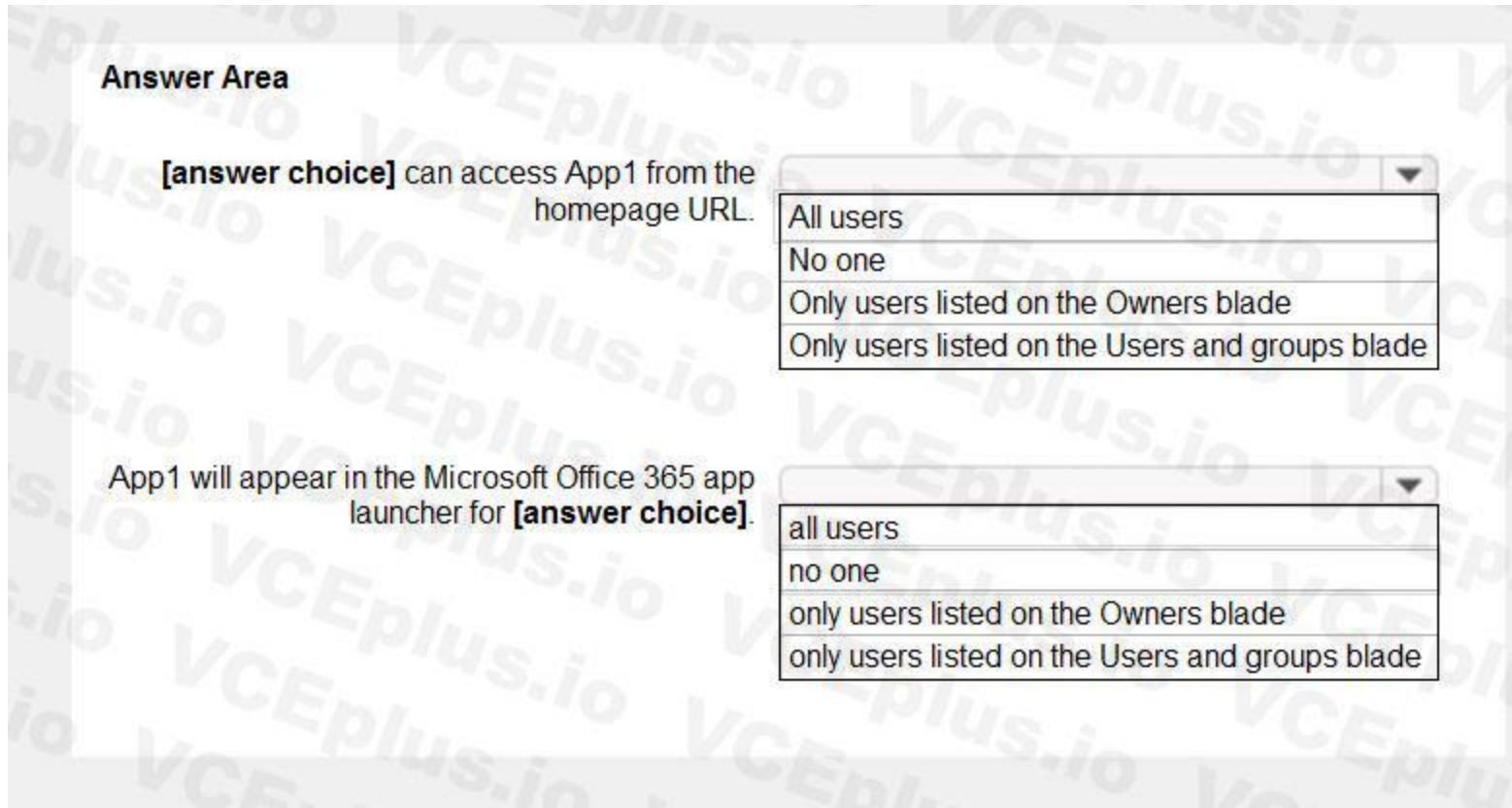
User assignment required? Yes No

Visible to users? Yes No

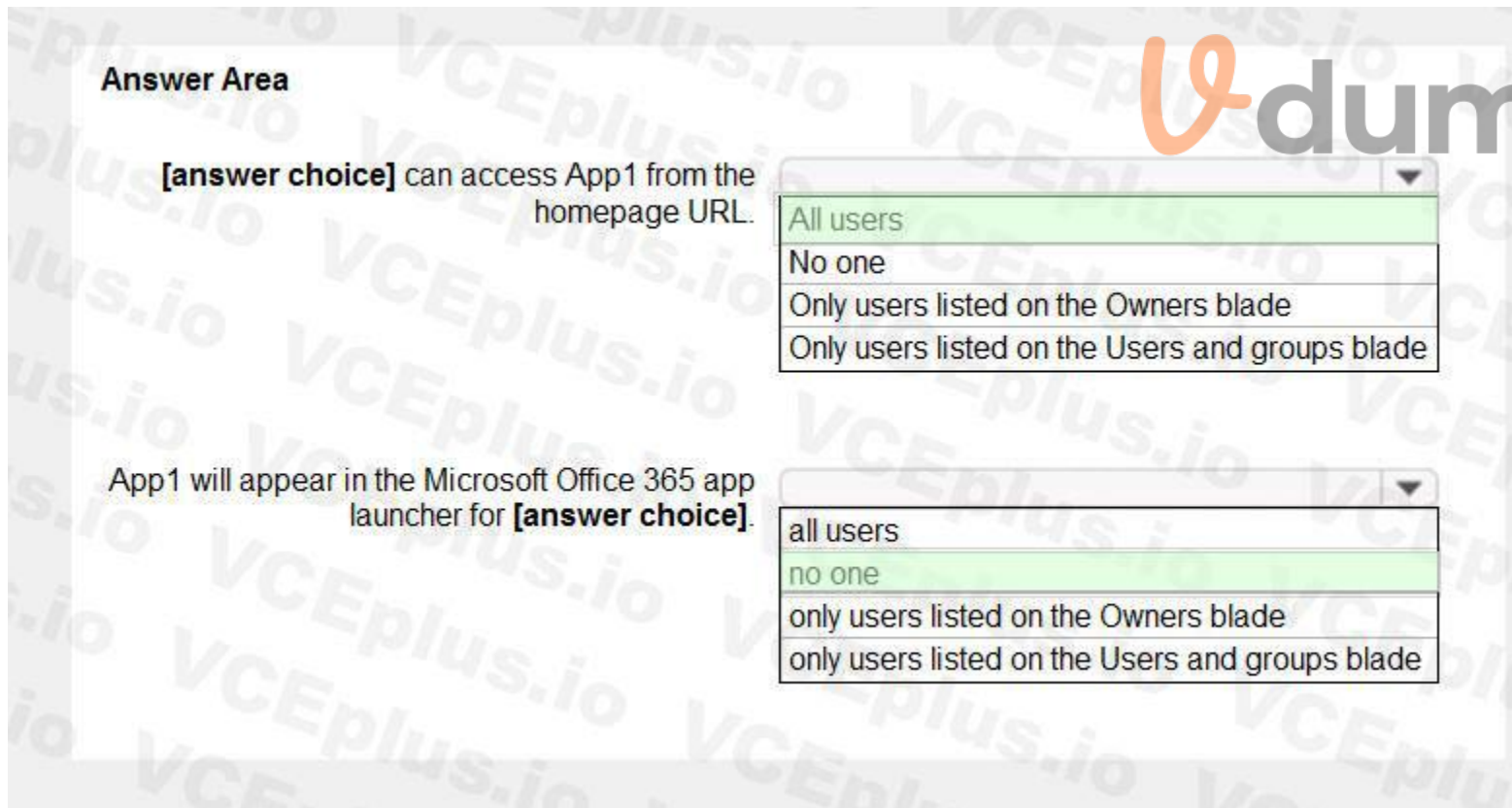
Vdumps

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.

Hot Area:



Answer Area:



Section:

Explanation:

Reference:

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

QUESTION 56

DRAG DROP

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 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.

Select and Place:

Actions

Add a group claim.

Create an app registration.

Grant admin consent.

Add delegated permissions.

Add app permissions.

Answer Area



Correct Answer:

Actions

Add a group claim.

Add delegated permissions.

Answer Area

Create an app registration.

Grant admin consent.

Add app permissions.

Section:

Explanation:

1. Create an app registration:

Your app must be registered with the Microsoft identity platform and be authorized by either a user or an administrator for access to the Microsoft Graph resources it needs.

2. Grant admin consent:

Higher-privileged permissions require administrator consent.

3. Add app permissions:

After the consents to permissions for your app, your app can acquire access tokens that represent the app's permission to access a resource in some capacity. Encoded inside the access token is every permission that your app has been granted for that resource.

Reference:

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

QUESTION 57

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. provisioning logs
- B. the Usage and Insights report
- C. sign-in logs
- D. audit logs

Correct Answer: D

Section:

QUESTION 58

You have an Azure AD tenant that contains a user named User1 and a registered app named App1.

User1 deletes the app registration of App1.

You need to restore the app registration.

What is the maximum number of days you have to restore the app registration from when it was deleted?

- A. 14
- B. 30
- C. 60
- D. 180

Correct Answer: B

Section:

QUESTION 59

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 Conditional Access policy.
- B. Create an access package.
- C. Configure Role settings in Azure AD Privileged Identity Management.



D. Create a Microsoft Defender for Cloud Apps access policy.

Correct Answer: B

Section:

QUESTION 60

HOTSPOT

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.

Hot Area:

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| You can assign Managed2 to VM1. | <input type="radio"/> | <input type="radio"/> |
| You can assign Managed3 to VM1. | <input type="radio"/> | <input type="radio"/> |
| You can assign VM1 the Owner role for RG1. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--|-------------------------------------|-------------------------------------|
| You can assign Managed2 to VM1. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| You can assign Managed3 to VM1. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| You can assign VM1 the Owner role for RG1. | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Section:

Explanation:

QUESTION 61

HOTSPOT

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 Certificate1 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.

Hot Area:

Answer Area

Statements

Admin1 can recover Secret1 on June 7.

Admin2 can purge Certificate1 on June 12.

Admin3 can purge Certificate1 on June 14.

Yes **No**

Answer Area:

Answer Area

Statements

Admin1 can recover Secret1 on June 7.

Admin2 can purge Certificate1 on June 12.

Admin3 can purge Certificate1 on June 14.

Yes **No**

Section:

Explanation:

QUESTION 62

HOTSPOT

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 has the following configurations:

* Name: location1

* Mark as trusted location: Enabled

* IPv4 range: 10.10.0.0/16

MFA has a trusted IP address 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.

Hot Area:

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA. | <input type="radio"/> | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA. | <input type="radio"/> | <input checked="" type="radio"/> |
| If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA. | <input checked="" type="radio"/> | <input type="radio"/> |



Section:

Explanation:

QUESTION 63

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 only
- B. User1 and Group1 only
- C. User1 and VW1 only
- D. User1, VM1, and App1 only
- E. User1, Group1, Vm1, and App1

Correct Answer: E

Section:

QUESTION 64

You have an Azure subscription that contains an Azure SQL database named db1.

You deploy an Azure App Service web app named App1 that provide product information to users that connect to App1 anonymously.

You need to provide App1 with Access to db1. The solution must meet the following requirements:

- * Credentials must only be available to App1.
- * Administrative effort must be minimized.

Which type of credentials should you use?

- A. a user-assigned managed identity
- B. an Azure AD user account
- C. A SQL Server account
- D. a system-assigned managed identity

Correct Answer: D

Section:

QUESTION 65

HOTSPOT

You have a hybrid Microsoft 365 subscription that contains the users show in the following table.

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

You plan to deploy an on-premises app1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.

You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.

Which user should perform the installation, and which role should you assign to Users1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

- Application Administrator
- Application Developer
- Cloud Application Administrator
- Global Administrator

Answer Area:

Answer Area

User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

- Application Administrator
- Application Developer
- Cloud Application Administrator
- Global Administrator

Section:

Explanation:

QUESTION 66

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. Yes

B. No

Correct Answer: B

Section:

QUESTION 67

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 Exchange Administrator role to User1.

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 68

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 User Administrator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 69

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 Security Operator role to User1.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 70

DRAG DROP

You have an Azure AD tenant that contains a user named Admin1.

Admin1 uses the Require password change for high-risk user's policy template to create a new Conditional Access policy.



Who is included and excluded by default in the policy assignment? To answer, drag the appropriate options to the correct target. Each option may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Options

- Admin1
- All guest and external users
- All users
- Directory roles
- None

Answer Area

Include:

Exclude:

Correct Answer:

Options

- Admin1
-
-
- Directory roles
- None

Answer Area



Include: All users

Exclude: All guest and external users

Section:

Explanation:

QUESTION 71

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Amazon Web Services app connector.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 72

You have an Azure AD tenant.

You deploy a new enterprise application named App1.

When users attempt to provide App1 with access to the tenant, the attempt fails.

You need to ensure that the users can request admin consent for App1. The solution must follow the principle of least privilege.

What should you do first?

- A. Enable admin consent requests for the tenant.
- B. Designate a reviewer of admin consent requests for the tenant.
- C. From the Permissions settings of App1, grant App1 admin consent for the tenant
- D. Create a Conditional Access policy for App1.

Correct Answer: A

Section:

QUESTION 73

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

| Name | Role |
|--------|--------------------------|
| Admin1 | Account Administrator |
| Admin2 | Service Administrator |
| Admin3 | SharePoint Administrator |



You need to implement Azure AD Privileged Identity Management (PIM).

Which users can use PIM to activate their role permissions?

- A. Admin1 only
- B. Admin2 only
- C. Admin3 only
- D. Admin1 and Admin2 only
- E. Admin2 and Admin3 only
- F. Admin1, Admin2, and Admin3

Correct Answer: D

Section:

QUESTION 74

HOTSPOT

You have an Azure AD tenant.

You perform the tasks shown in the following table.

| Date | Task |
|----------|--|
| March 1 | Register four enterprise applications named App1, App2, App3, and App4. |
| March 15 | From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service. |
| March 20 | From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service. |
| March 25 | From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service. |
| March 30 | From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service. |

On April 5, an administrator deletes App1, App2, App3, and App4.

You need to restore the apps and the settings.

Which apps can you restore on April 16, and which settings can you restore for App4 on April 16? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Apps:

- No apps
- App4 only
- App3 and App4 only**
- App2, App3, and App4 only
- App1, App2, App3, and App4

App4 settings:

- No settings
- Self-service only
- App roles and Client secret only
- Users and groups and Self-service only
- App roles, Users and groups, Client secret, and Self-service**

Answer Area:

Answer Area

Apps:

- No apps
- App4 only
- App3 and App4 only**
- App2, App3, and App4 only
- App1, App2, App3, and App4

App4 settings:

- No settings
- Self-service only
- App roles and Client secret only
- Users and groups and Self-service only
- App roles, Users and groups, Client secret, and Self-service**

Section:

Explanation:

QUESTION 75

HOTSPOT

You have an Azure AD tenant named contoso.com that contains a group named All Company and has the following Identity Governance settings:

* Block external users from signing in to this directory: Yes

* Remove external user Yes

* Number of days before removing external user from this directory: 30

On March 1, 2022, you create an access package named Package1 that has the following settings:

* Resource roles

o Name: All Company

o Type: Group and Team

o Role: Member

* Lifecycle

o Access package assignment expire: On date

o Assignment expiration date: April 1, 2022

On March 1, 2022, you assign Package1 to the guest users shown in the following table.

| Name | Email address |
|--------|--------------------|
| Guest1 | guest1@outlook.com |
| Guest2 | guest2@outlook.com |

On March 2, 2022, you assign the Reports reader role to Guest1.

On April 1(2022, you invite a guest user named Guest3 to contoso.com.

On April 4, 2022, you add Guest3 to the All Company group.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| On May 5, 2022, the Guest1 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |
| On May 5, 2022, the Guest2 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |
| On May 5, 2022, the Guest3 account is in contoso.com. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| On May 5, 2022, the Guest1 account is in contoso.com. | <input type="radio"/> | <input checked="" type="radio"/> |
| On May 5, 2022, the Guest2 account is in contoso.com. | <input type="radio"/> | <input checked="" type="radio"/> |
| On May 5, 2022, the Guest3 account is in contoso.com. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

QUESTION 76

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 Amazon Web Services (AWS) account a Google Workspace subscription, and a GitHub account

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the GitHub app connector

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Section:

QUESTION 77

You have a Microsoft 365 subscription that contains a Microsoft SharePoint Online site named Site1 and a Microsoft 365 group named Group1. You need to ensure that the members of Group1 can access Site1 for 90 days. The solution must minimize administrative effort. What should you use?

- A. an access review
- B. a lifecycle workflow
- C. an access package
- D. a Conditional Access policy

Correct Answer: C

Section:

QUESTION 78

HOTSPOT

You have an Azure AD tenant that contains multiple storage accounts.

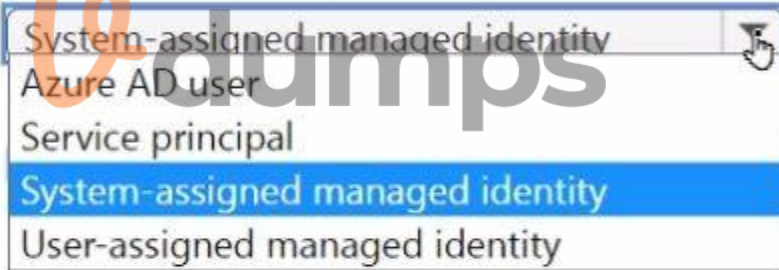
You plan to deploy multiple Azure App Service apps that will require access to the storage accounts.


You need to recommend an identity solution to provide the apps with access to the storage accounts. The solution must minimize administrative effort.

Which type of identity should you recommend, and what should you recommend using to control access to the storage accounts? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Identity type: 

To control access, use: 

Answer Area:

Answer Area

Identity type:

- System-assigned managed identity
- Azure AD user
- Service principal
- System-assigned managed identity**
- User-assigned managed identity

To control access, use:

- Shared access signature (SAS) tokens
- Azure Active Directory Domain Services (Azure AD DS)
- Role-based access control (RBAC)
- Shared access signature (SAS) tokens**
- X.509 certificates

Section:

Explanation:

QUESTION 79

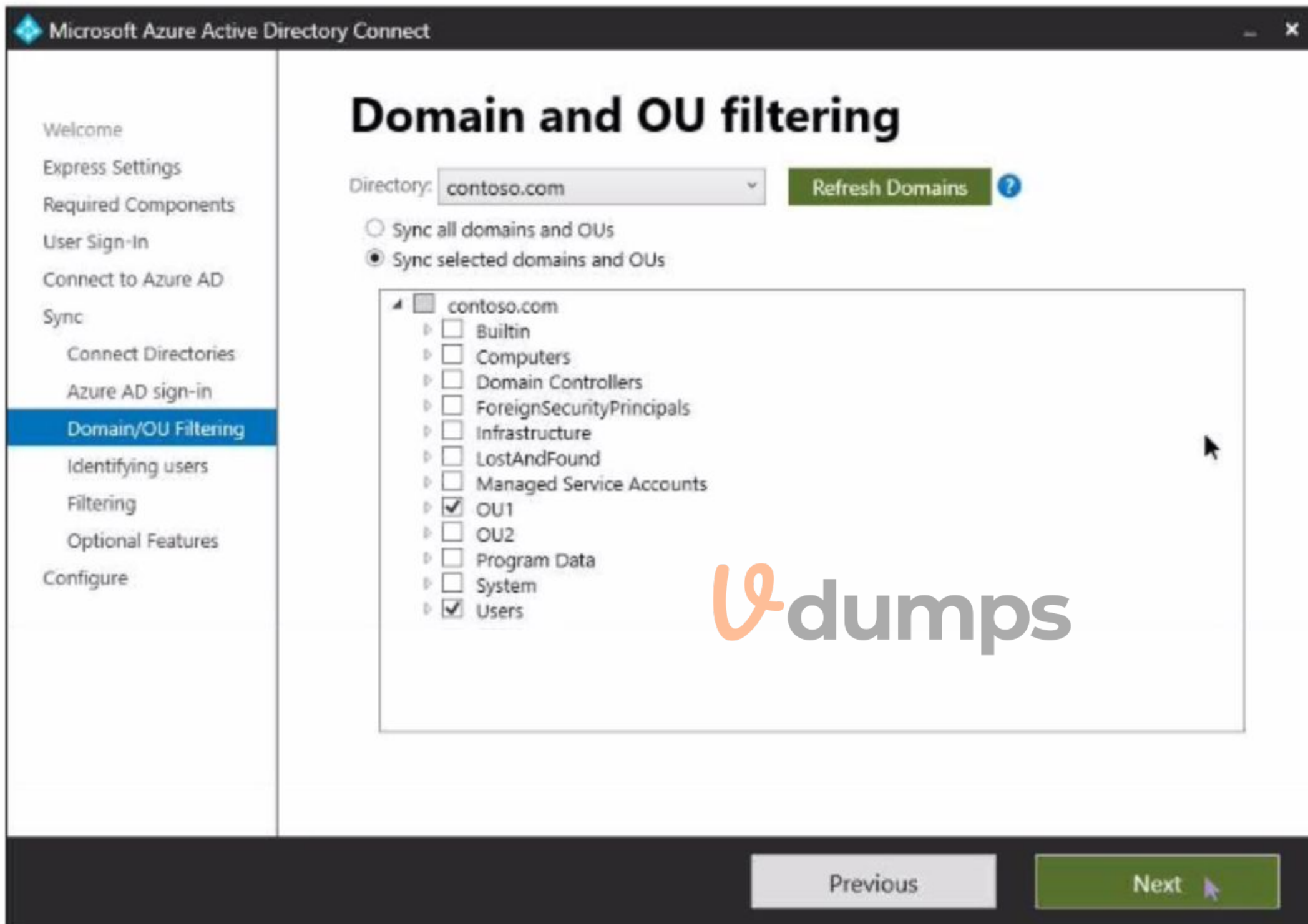
HOTSPOT

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with Azure AD and contains the users shown in the following table.

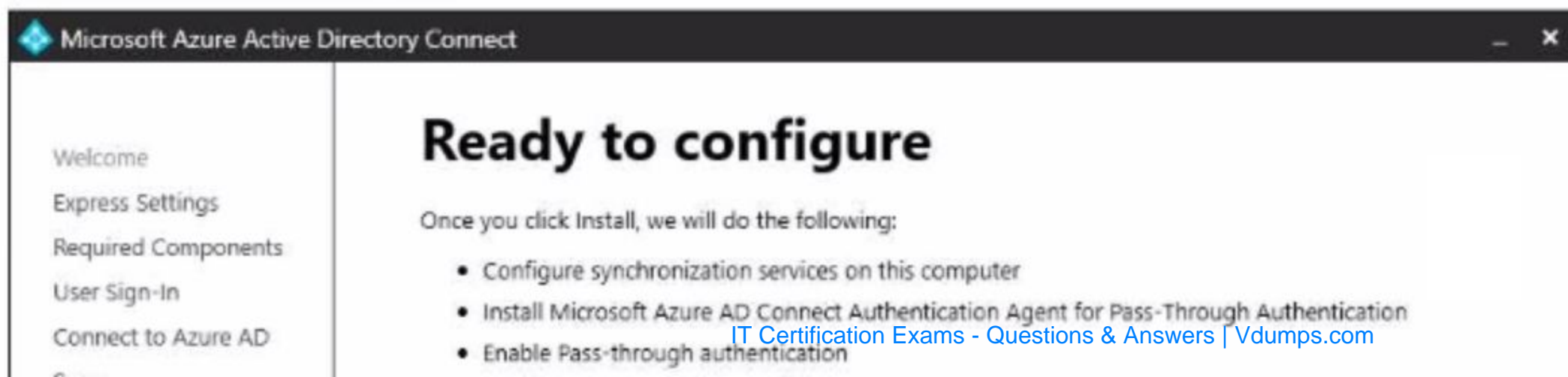
| Name | Organizational unit (OU) |
|-------|--------------------------|
| User1 | OU1 |
| User2 | OU2 |

In Azure AD Connect, Domain/OU Filtering is configured as shown in the following exhibit.





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



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

Hot Area:

Answer Area

Statements

User1 can use self-service password reset (SSPR) to reset his password.

Yes

No

If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.

User2 can be added to a Microsoft SharePoint Online site as a member.

Answer Area:

Answer Area

Statements

User1 can use self-service password reset (SSPR) to reset his password.

Yes

No

If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.

User2 can be added to a Microsoft SharePoint Online site as a member.

Section:

Explanation:

QUESTION 80

HOTSPOT

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

You need to configure access to Vault1. The solution must meet the following requirements:

- * Ensure that User1 can manage and create keys in Vault1.
- * Ensure that User2 can access a certificate stored in Vault1.
- * Use the principle of least privilege.

Which role should you assign to each user? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1: ▼
Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

User2: ▼
Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

Answer Area:

Answer Area

User1: ▼
Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

User2: ▼
Key Vault Certificates Officer
Key Vault Crypto Officer
Key Vault Secrets Officer

Section:

Explanation:

QUESTION 81

You have a Microsoft 365 E5 subscription.
You purchase the app governance add-on license.
You need to enable app governance integration.
Which portal should you use?

- A. the Microsoft Defender for Cloud Apps portal
- B. the Microsoft 365 admin center
- C. Microsoft 365 Defender
- D. the Azure Active Directory admin center
- E. the Microsoft Purview compliance portal

Correct Answer: A

Section:

QUESTION 82

You have an Azure AD tenant that contains a user named User1
User1 needs to manage license assignments and reset user passwords.
Which role should you assign to User1?

- A. License administrator
- B. Helpdesk administrator
- C. Billing administrator
- D. User administrator

Correct Answer: D

Section:

QUESTION 83

You have an Azure AD tenant that has multi-factor authentication (MFA) enforced and self-service password reset (SSPR) enabled.

You enable combined registration in interrupt mode.

You create a new user named User1.

Which two authentication methods can User1 use to complete the combined registration process? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. a FIDO2 security key
- B. a hardware token
- C. a one-time passcode email
- D. Windows Hello for Business
- E. the Microsoft Authenticator app

Correct Answer: A, E

Section:

QUESTION 84

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Conditional Access policies. You need to block access to cloud apps when a user is assessed as high risk.

Which type of policy should you create in the Microsoft Defender for Cloud Apps?

- A. OAuth app policy
- B. anomaly detection polio
- C. access policy
- D. activity policy

Correct Answer: C

Section:

QUESTION 85

You plan to deploy a new Azure AD tenant.

Which multifactor authentication (MFA) method will be enabled by default for the tenant?

- A. Microsoft Authenticator
- B. SMS
- C. voice call



D. email OTP

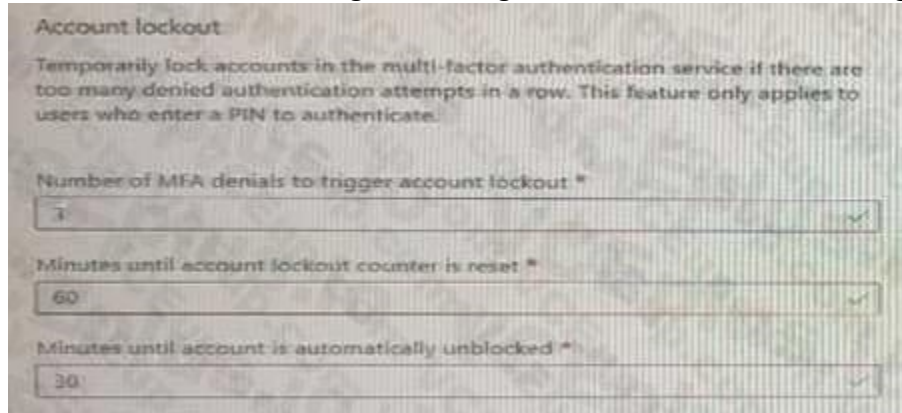
Correct Answer: B

Section:

QUESTION 86

HOTSPOT

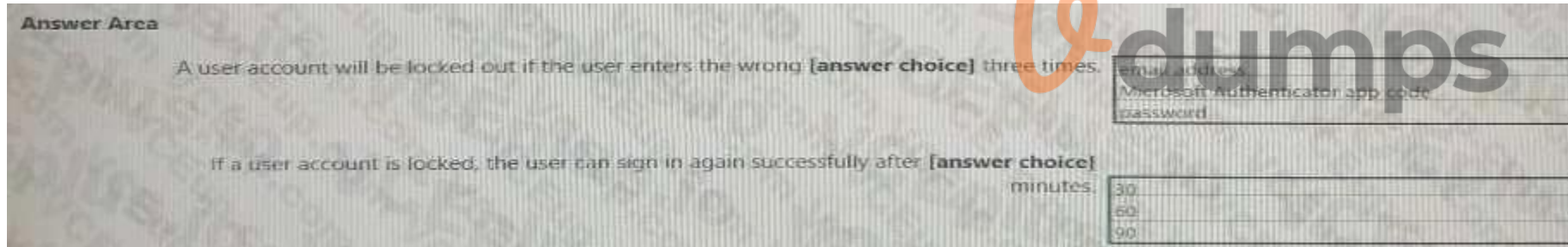
You have an Azure Active Directory (Azure AD) tenant that has multi-factor authentication (MFA) enabled. The account lockout settings are configured as shown in the following exhibit.



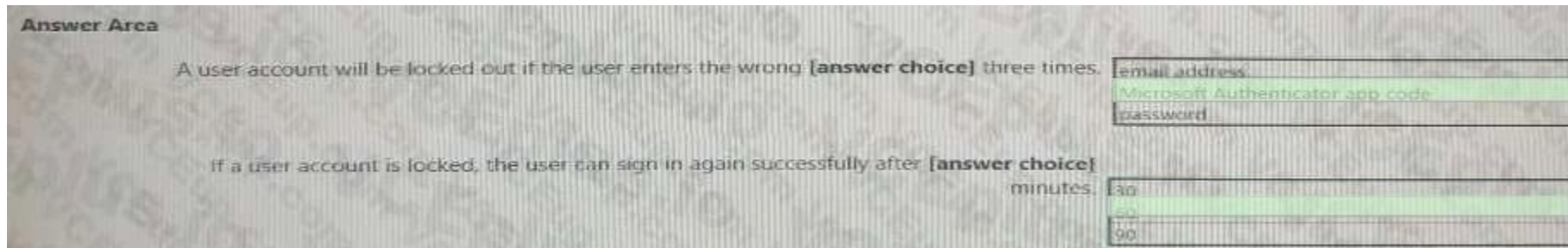
Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 87

HOTSPOT

You have a Microsoft 365 tenant.

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

Identify sign-ins 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 in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To classify leaked credentials as high-risk, use:

| |
|--|
| Azure Active Directory (Azure AD) Identity Protection |
| Azure Active Directory (Azure AD) Privileged Identity Management (PIM) |
| Identity Governance |
| Self-service password reset (SSPR) |

To trigger remediation, use:

| |
|---|
| Client apps not using Modern authentication |
| Device state |
| Sign-in risk |
| User location |
| User risk |

To mitigate the risk, select:

| |
|--|
| Apply app enforced restrictions |
| Block access |
| Grant access but require app protection policy |
| Grant access but require password change |

Vdumps

Answer Area:

Answer Area

To classify leaked credentials as high-risk, use:

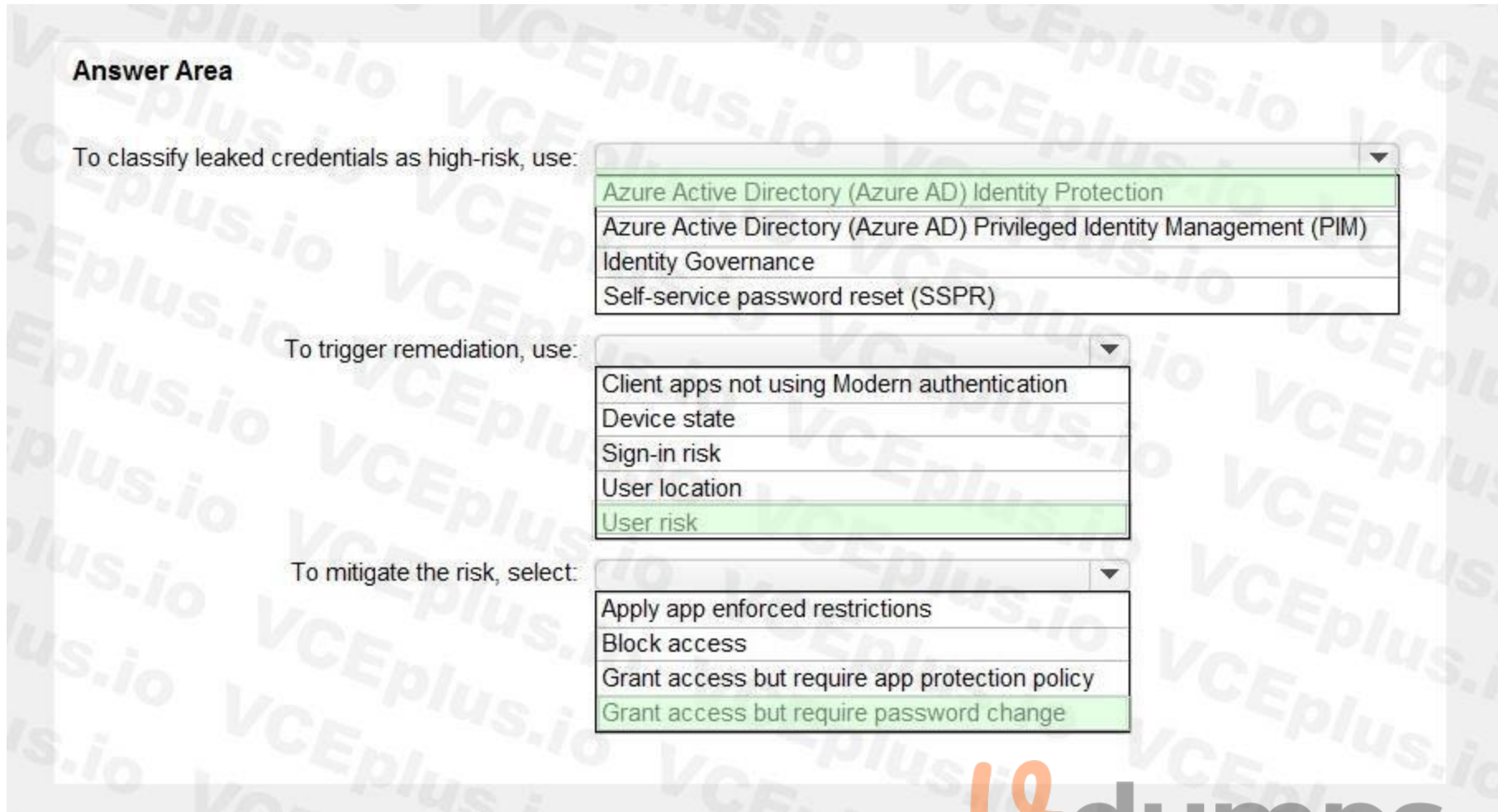
- Azure Active Directory (Azure AD) Identity Protection
- Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- Identity Governance
- Self-service password reset (SSPR)

To trigger remediation, use:

- Client apps not using Modern authentication
- Device state
- Sign-in risk
- User location
- User risk

To mitigate the risk, select:

- Apply app enforced restrictions
- Block access
- Grant access but require app protection policy
- Grant access but require password change




Section:

Explanation:

Reference:

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

QUESTION 88

DRAG DROP

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. Attire AD Connect is installed on a server named Server 1.

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

You need to implement a failover server for Azure AD Connect. The solution must minimize how long it takes to fail over if Server1 fails.

Which three 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.

Select and Place:

Actions:

- On Server1, run export for all connectors.
- On Server2, run export for all connectors.
- On Server2, run full import for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

Answer Area:

Correct Answer:

Actions:

- On Server2, run export for all connectors.
- On Server2, install Azure AD Connect.
- On Server1, configure the staging mode.

Answer Area:

- On Server2, run full import for all connectors.
- On Server2, run delta synchronization for all connectors.
- On Server1, run export for all connectors.



Section:

Explanation:

QUESTION 89

HOTSPOT

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.

Hot Area:

Answer Area

Job title property:

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

Usage location property:

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

Answer Area:

Answer Area

Job title property:

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

Usage location property:

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

Section:

Explanation:

QUESTION 90

HOTSPOT

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.



Hot Area:

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 Area:

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 |

Section:

Explanation:

Reference:

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



QUESTION 91

DRAG DROP

You have a new Microsoft 365 tenant that uses a domain name of contoso.onmicrosoft.com.

You register the name contoso.com with a domain registrar.

You need to use contoso.com as the default domain name for new Microsoft 365 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.

Select and Place:

Actions

- Delete the contoso.onmicrosoft.com domain.
- Register a custom domain name of contoso.com.
- Set the domain to primary.
- Create a new TXT record in DNS.
- Verify the domain name.

Answer Area



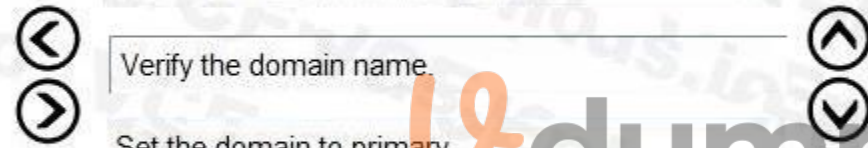
Correct Answer:

Actions

- Delete the contoso.onmicrosoft.com domain.
-
-
-
-

Answer Area

- Register a custom domain name of contoso.com.
- Create a new TXT record in DNS.
- Verify the domain name.
- Set the domain to primary.



Section:

Explanation:

Reference:

<https://practical365.com/configure-a-custom-domain-in-office-365/>

QUESTION 92

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

| Name | Role |
|--------|---------------------------|
| Admin1 | User Administrator |
| Admin2 | Password Administrator |
| Admin3 | Application Administrator |

You need to compare the role permissions of each user. The solution must minimize administrative effort.

What should you use?

- A. the Microsoft 365 Defender portal
- B. the Microsoft 365 admin center

- C. the Microsoft Entra admin center
- D. the Microsoft Purview compliance portal

Correct Answer: C

Section:

QUESTION 93

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender.

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Google Workspace app connector.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 94

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 Amazon Web Services (AWS) account, a Google Workspace subscription, and a GitHub account.

You deploy an Azure subscription and enable Microsoft 365 Defender

You need to ensure that you can monitor OAuth authentication requests by using Microsoft Defender for Cloud Apps.

Solution: From the Microsoft 365 Defender portal, you add the Microsoft Azure app connector.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 95

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and the users shown in the following table.

The users have the devices shown in the following table.

You create the following two Conditional Access policies:

* Name: CAPolicy1

* Assignments

o Users or workload identities: Group 1

o Cloud apps or actions: Office 365 SharePoint Online

o Conditions

Filter for devices: Exclude filtered devices from the policy

Rule syntax: device.displayName -starts With 'Device*'

o Access controls

Grant: Block access

Session: 0 controls selected

o Enable policy: On

* Name: CAPolicy2

* Assignments

o Users or workload identities: Group2

o Cloud apps or actions: Office 365 SharePoint Online

o Conditions: 0 conditions selected

* Access controls

o Grant: Grant access

Require multifactor authentication

o Session:

0 controls selected

* Enable policy: On

All users confirm that they can successfully authenticate using MFA.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

| Statements | Yes | No |
|--------------------------------------|-----------------------|-----------------------|
| User1 can access Site1 from Device1. | <input type="radio"/> | <input type="radio"/> |
| User2 can access Site1 from Device2. | <input type="radio"/> | <input type="radio"/> |
| User3 can access Site1 from Device3. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--------------------------------------|-----------------------|-------------------------------------|
| User1 can access Site1 from Device1. | <input type="radio"/> | <input checked="" type="checkbox"/> |
| User2 can access Site1 from Device2. | <input type="radio"/> | <input checked="" type="checkbox"/> |
| User3 can access Site1 from Device3. | <input type="radio"/> | <input checked="" type="checkbox"/> |

Section:

Explanation:

QUESTION 96

You have an Azure subscription that contains an Azure Automation account named Automation1 and an Azure key vault named Vault1. Vault1 contains a secret named Secret 1.

You enable a system-assigned managed identity for Automation1.

You need to ensure that Automation1 can read the contents of Secret1. The solution must meet the following requirements:

* Prevent Automation1 from accessing other secrets stored in Vault1.

* Follow the principle of least privilege.

What should you do?

- A. From Vault1, configure the Access control (IAM) settings.
- B. From Automation1, configure the Identity settings.
- C. From Secret1, configure the Access control (IAM) settings
- D. From Automation1, configure the Run as accounts settings.

Correct Answer: A

Section:

QUESTION 97

You have a Microsoft 365 E5 subscription.

Users authorize third-party cloud apps to access their data.

You need to configure an alert that will be triggered when an app requires high permissions and is authorized by more than 20 users.

Which type of policy should you create in the Microsoft Defender for Cloud Apps portal?

- A. anomaly detection policy
- B. OAuth app policy
- C. access policy
- D. activity policy



Correct Answer: C

Section:

QUESTION 98

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. User3
- D. User4

Correct Answer: C

Section:

QUESTION 99

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

| Name | Role |
|--------|------------------------------|
| User1 | None |
| User2 | None |
| Admin1 | Application administrator |
| Admin2 | Authentication administrator |

The User settings for enterprise applications have the following configuration.

- Users can consent to apps accessing company data on their behalf:
- Users can consent to apps accessing company data for the groups they
- Users can request admin consent to apps they are unable to consent to: Yes
- Who can review admin consent requests: Admin2, User2

User1 attempts to add an app that requires consent to access company data.

Which user can provide consent?

- A. User1
- B. User2
- C. Admin1
- D. Admin2

Correct Answer: C

Section:

QUESTION 100

HOTSPOT

You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.

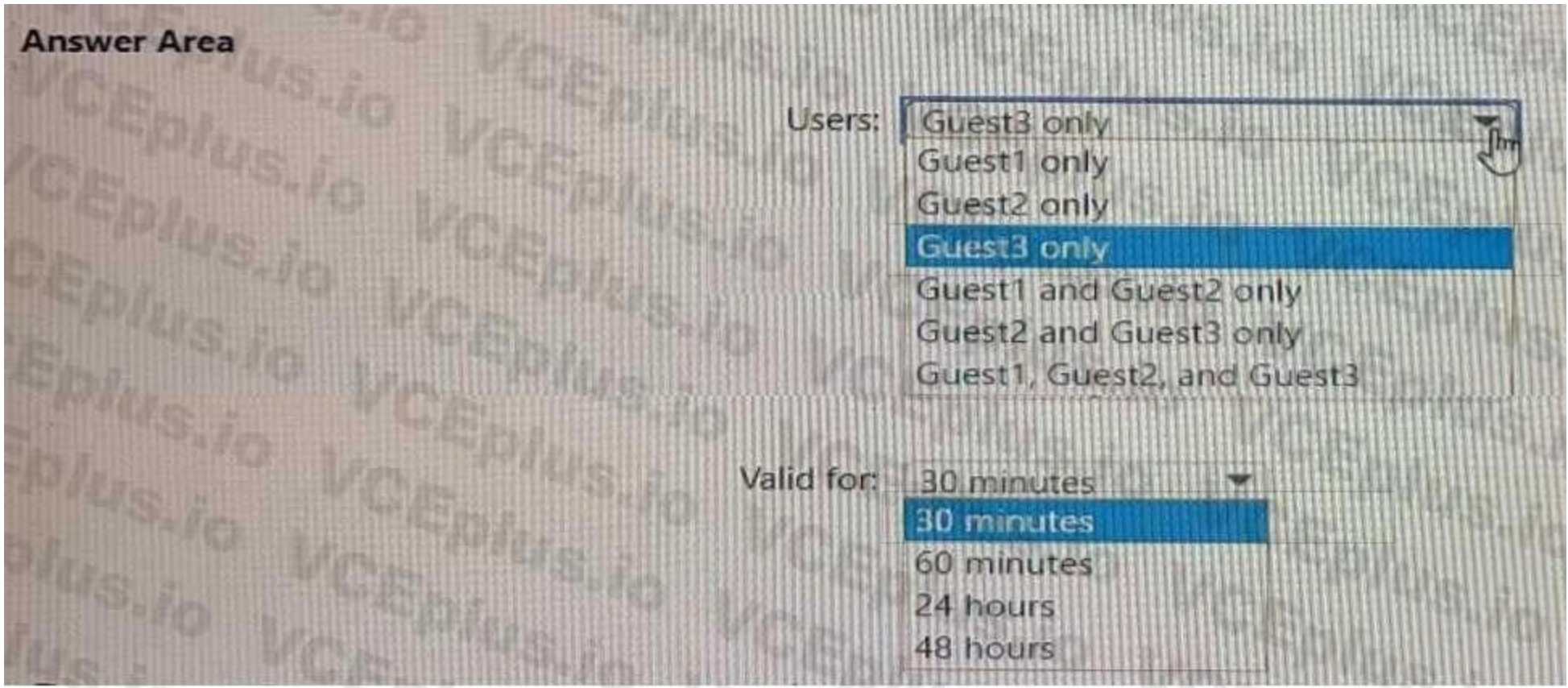
You invite the guest users shown in the following table.

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.

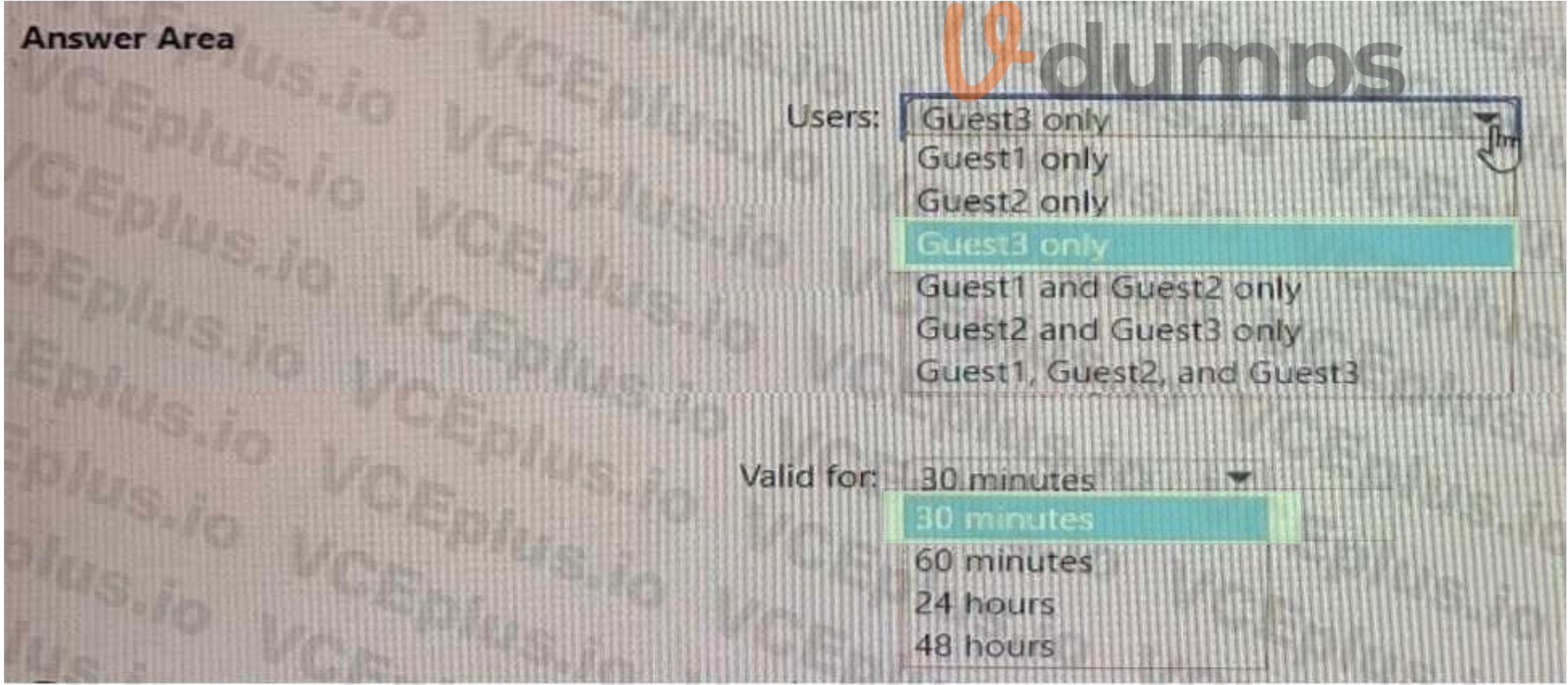
NOTE: Each correct selection is worth one point.

Hot Area:





Answer Area:



Section:

Explanation:

QUESTION 101

HOTSPOT

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

| Name | Role |
|-------|---|
| User1 | Security administrator |
| User2 | Privileged authentication administrator |
| User3 | Service support administrator |

User2 reports that he can only configure multi-factor authenticating (MFA) to use the Microsoft Authenticator app.

You need to ensure that User2 can configure alternate MFA methods.

Which configuration is required, and which user should perform the configuration? To answer, select the appropriate options in the answer area.

Hot Area:

Answer Area

Configuration: Modify security defaults.
 Enable access reviews.
 Enable Azure AD Privileged Identity Management (PIM).
 Modify security defaults.

User: User1 only
 User1 only
 User2 only
 User3 only
 User1 and User2 only
 User1 and User3 only
 User2 and User3 only

Answer Area:

Answer Area

Configuration:

- Modify security defaults.
- Enable access reviews.
- Enable Azure AD Privileged Identity Management (PIM).

User:

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

Section:

Explanation:

QUESTION 102

Your network contains an on-premises Active Directory domain that syncs to an 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 Windows 10 computers to support Azure AD Seamless SSO. What should you do?

- A. Modify the Local intranet zone settings
- B. Configure Sign-in options from the Settings app.
- C. Enable Enterprise State Roaming.
- D. Install the Azure AD Connect Authentication Agent.

Correct Answer: B

Section:

QUESTION 103

HOTSPOT

You have an Azure AD tenant and an Azure web app named App1.

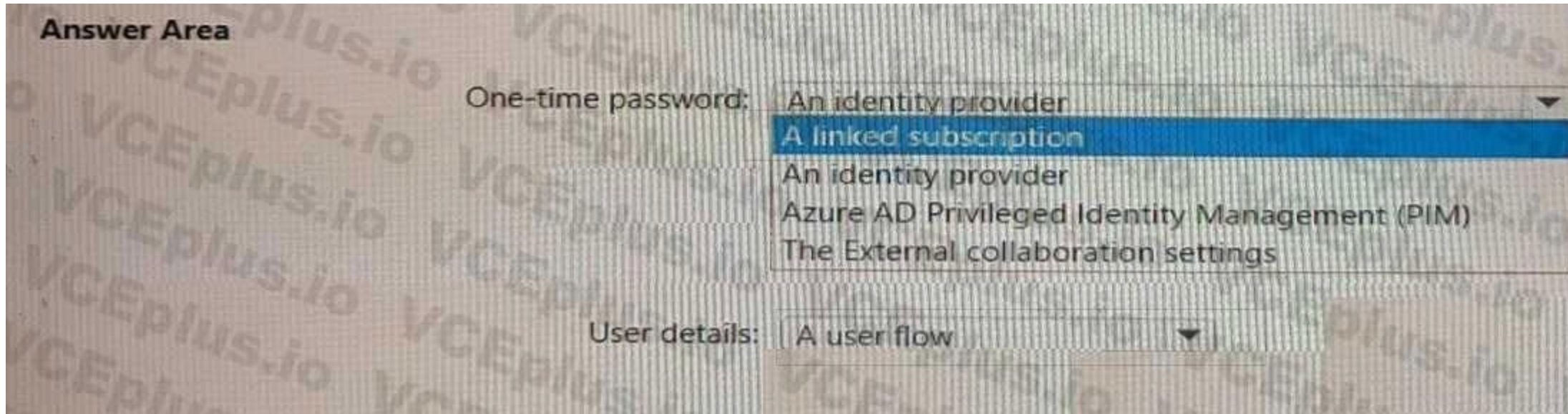
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:

- 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.

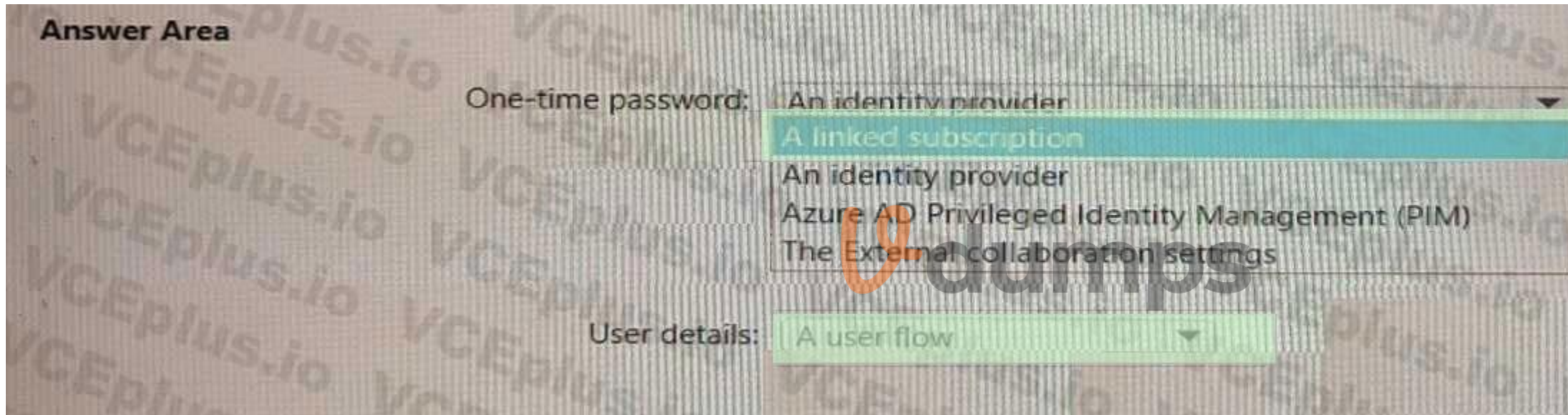
What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 104

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 | <i>Not applicable</i> |

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. Configure a sign-in risk policy.
- B. Mark User1 as compromised.

- C. Reconfigure the user risk policy to trigger on medium or low severity.
- D. Reset the Azure MFA registration for User1.

Correct Answer: B

Section:

QUESTION 105

HOTSPOT

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

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

In Azure AD Identity Protection, you configure a user risk policy that has the following settings:

- Assignments:
 - o Users: Group1
 - o User risk: Low and above
- Controls:
 - o Access: Block access

In Azure AD Identity Protection, you configure a sign-in risk policy that has the following settings:

- Assignments:
 - o Users: Group2
 - o Sign-in risk: Low and above
- Controls:
 - o Access: Require multi-factor authentication

the following settings:

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

NOTE: Each correct selection is worth one point.



Hot Area:

| Answer Area | Statements | Yes | No |
|-------------|---|-----------------------|-----------------------|
| | User1 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| | User2 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |
| | User3 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|---|-------------------------------------|-------------------------------------|
| User1 can sign in from an anonymous IP address. | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| User2 can sign in from an anonymous IP address. | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| User3 can sign in from an anonymous IP address. | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Section:

Explanation:

QUESTION 106

You have an Azure AD tenant that contains a user named User1 and the conditional access policies shown in the following table.

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

You need to evaluate which policies will be applied User1 when User1 attempts to sign-in from various IP addresses.

Which feature should you use?

- A. Access reviews
- B. Identity Secure Score
- C. The What If tool
- D. the Microsoft 365 network connectivity test tool

Correct Answer: C

Section:

QUESTION 107

You have three Azure subscriptions that are linked to a single Microsoft Entra tenant.

You need to evaluate and remediate the risks associated with highly privileged accounts. The solution must minimize administrative effort.

What should you use?

- A. Microsoft Entra Verified ID
- B. Privileged Identity Management (PIM)
- C. Global Secure Access
- D. Microsoft Entra Permissions Management

Correct Answer: B

Section:

QUESTION 108

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

| Name | Member of |
|-------|----------------|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group1, Group2 |

You have a user risk policy that has the following settings:

* Assignments:

o Include: Group1

o Exclude: Group2

* Sign-in risk Medium and above

* Access controls:

o Grant access: Require password change

When the users attempt to sign in, user risk levels are detected as shown in the following table.

| User | Risk level |
|-------|------------|
| User1 | High |
| User2 | Medium |
| User3 | High |

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



Hot Area:

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| User1 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |
| User2 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |
| User3 must change their password during sign in. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 must change their password during sign in. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 must change their password during sign in. | <input type="radio"/> | <input checked="" type="radio"/> |
| User3 must change their password during sign in. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

QUESTION 109

You have a Microsoft Entra tenant that contains the groups shown in the following table. You need to implement Privileged Identity Management (PIM) for the groups. Which groups can be managed by using PIM?

- A. Group1 only
- B. Group1 and Group2 only
- C. Group1 and Group3 only
- D. Group3 and Group4 only
- E. Group1, Group2, Group3, and Group4

Correct Answer: C**Section:****QUESTION 110**

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains an Azure Cosmos DB database named DB1 and an Azure Kubernetes Service (AKS) cluster named AKS1. AKS1 uses a managed identity.

You need to ensure that AKS1 can access DB1. The solution must meet the following requirements:

- * Ensure that AKS1 uses the managed identity to access DB1.
- * Follow the principle of least privilege.

Which role should you assign to the managed identity of AKS1.

- A. For RG1, assign the Azure Cosmos DB Data Reader Role role.
- B. For Sub1, assign the Owner role.
- C. For RG1, assign the Reader role.
- D. For DB1, assign the Azure Cosmos DB Account Reader Role role.

**Correct Answer: A****Section:****QUESTION 111**

HOTSPOT

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

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

The subscription contains the virtual machines shown in the following table.

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

Which identities can be assigned the Owner role for RG1, and to which virtual machines can you assign Managed2? To answer, select the appropriate options in the answer area NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

Answer Area:

Answer Area



Identities with Owner role:

- Managed1 only
- Managed1, VM1, and VM3 only
- Managed1, Managed2, and VM1 only
- Managed1, Managed2, VM1, and VM2 only
- Managed1, Managed2, VM1, VM2, and VM3 only

Virtual machines assigned to Managed2:

- VM4 only
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM1, VM2, VM3, and VM4

Section:

Explanation: