

Microsoft.SC-300.vOct-2024.by.Unamo.125q

Number: SC-300
Passing Score: 800
Time Limit: 120
File Version: 13.0

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

Case Study

Contoso, Ltd

Overview

Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc Fabricam has an Azure Active Directory (Azure AD) tenant named fabrikam.com.

Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resources OU contains all users and computers.

The Contoso.com Active Directory domain contains the users shown in the following table.

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

Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS).

Only the Contoso Resources OU is synced.

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

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

The users in the London office have the Microsoft 365 admin center to manually assign licenses. All user have licenses assigned besides the following exceptions:

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

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

Security defaults are disabled for Contoso.com.

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

Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the: User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Planned Changes

Contoso plans to implement the following changes.

Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor-Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign.

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

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Technical Requirements

Contoso identifies the following technical requirements:

- AH users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth-response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

QUESTION 1

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Object to create for each branch office:

| |
|-------------------------------|
| An administrative unit |
| A custom role |
| A Dynamic User security group |
| An OU |

Tool to use:

| |
|--|
| Azure Active Directory admin center |
| Active Directory Administrative Center |
| Active Directory module for Windows PowerShell |
| Microsoft 365 admin center |

Answer Area:

Answer Area

Object to create for each branch office:

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

Tool to use:

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

Section:

Explanation:

Reference:

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

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

QUESTION 2

HOTSPOT

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Answer Area:

Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Section:

Explanation:

Reference:

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

QUESTION 3

HOTSPOT

You need to implement the planned changes and technical requirements for the marketing department.

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

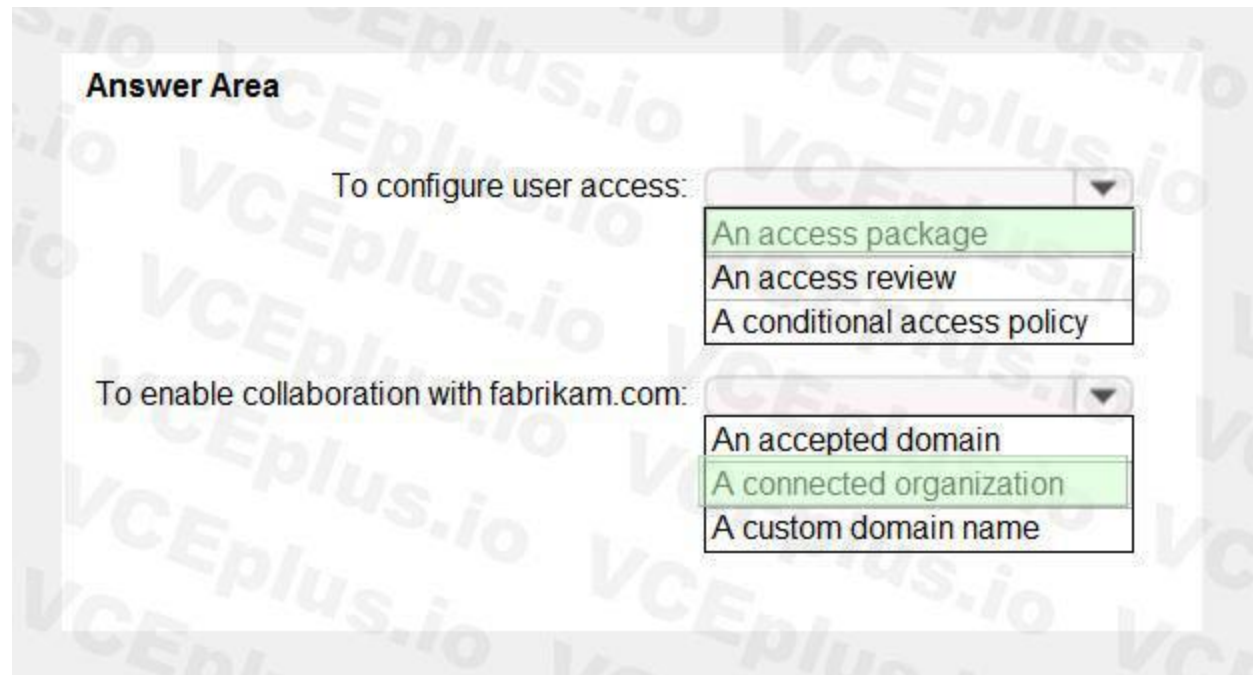
To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name

Answer Area:



Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization>

QUESTION 4

You need to allocate licenses to the new users from A. Datum. The solution must meet the technical requirements. Which type of object should you create?

- A. a distribution group
- B. a Dynamic User security group
- C. an administrative unit
- D. an OU

Correct Answer: C

Section:

QUESTION 5

You need to locate licenses to the ADatum users. The solution must need the technical requirements. Which type of object should you create?

- A. A Dynamo User security group
- B. An OU
- C. A distribution group
- D. An administrative unit

Correct Answer: D

Section:

QUESTION 6

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

What should you do?

- A. Create an access review.
- B. Modify Role settings
- C. Create an administrator unit.
- D. Modify Active Assignments.

Correct Answer: B

Section:

Explanation:

Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles Default Setting State Require justification on activation Yes Require ticket information on activation No

On activation, require Azure MFA Yes Require approval to activate No Approvers None

QUESTION 7

You need to sync the ADatum users. The solution must meet the technical requirements.

What should you do?

- A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
- B. From PowerShell, run Set-ADSyncScheduler.
- C. From PowerShell, run Start-ADSyncSyncCycle.
- D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: A

Section:

Explanation:

You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 8

You need to meet the planned changes and technical requirements for App1.

What should you implement?

- A. a policy set in Microsoft Endpoint Manager
- B. an app configuration policy in Microsoft Endpoint Manager
- C. an app registration in Azure AD
- D. Azure AD Application Proxy

Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>

QUESTION 9

You create a Log Analytics workspace.

You need to implement the technical requirements for auditing.

What should you configure in Azure AD?

- A. Company branding
- B. Diagnostics settings
- C. External Identities
- D. App registrations

Correct Answer: B

Section:

Explanation:

Reference:

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

Case Study

A Datum Corp

Overview

A Datum Corporation is a consulting company in Montreal.

A Datum recently acquired a Vancouver-based company named Litware, Inc.

A Datum Environment

The on-premises network of A. Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.

A Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect.

A Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.

The tenant contains the users shown in the following table.

Problem Statements

A Datum identifies the following issues:

- bullet Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- bullet A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address,
- bullet When you attempt to assign the Device Administrators role To IT_Group1, the group does NOT appear in the selection list.
- bullet Anyone in the organization can invite guest users, including other guests and non-administrators.
- bullet The helpdesk spends too much time resetting user passwords.
- bullet Users currently use only passwords for authentication.

Requirements

A. Datum plans to implement the following changes;

- bullet Configure self-service password reset {SSPR}.
- bullet Configure multi-factor authentication (MFA) for all users.
- bullet Configure an access review for an access package named Package1.
- bullet Require admin approval for application access to organizational data.
- bullet Sync the AD DS users and groupsoflitware.com with the Azure AD tenant.
- bullet Ensure that only users that are assigned specific admin roles can invite guest users.
- bullet Increase the maximum number of devices that can be joined or registered to Azure AD to 10.

Technical Requirements

A. Datum identifies the following technical requirements:

- bullet Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- bullet Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- bullet Users must provide one authentication method to reset their password by using SSPR. Available methods must include:
 - bullet Email
 - bullet Phone
 - bullet Security questions
- bullet The Microsoft Authenticator app
- bullet Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- bullet The principle of least privilege must be used.

QUESTION 1

You need to resolve the issue of the sales department users. What should you configure for the Azure AD tenant?

- A. the User settings

- B. the Device settings
- C. the Access reviews settings
- D. Security defaults

Correct Answer: B

Section:

QUESTION 2

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

- A. Recreate the IT-Group 1 group.
- B. Change Membership type of IT-Group1 to Dynamic Device
- C. Add an owner to IT_Group1.
- D. Change Membership type of IT-Group1 to Dynamic User

Correct Answer: A

Section:

QUESTION 3

You need to implement the planned changes for Package1. Which users can create and manage the access review?

- A. User3 only
- B. User4 only
- C. User5 only
- D. User3 and User4
- E. User3 and User5
- F. User4and User5

Correct Answer: E

Section:

QUESTION 4

You need to implement the planned changes for litware.com. What should you configure?

- A. Azure AD Connect cloud sync between the Azure AD tenant and litware.com
- B. Azure AD Connect to include the litware.com domain
- C. staging mode in Azure AD Connect for the litware.com domain

Correct Answer: C

Section:

QUESTION 5

You need implement the planned changes for application access to organizational data. What should you configure?

- A. authentication methods
- B. the User consent settings
- C. access packages

D. an application proxy

Correct Answer: B

Section:

QUESTION 6

You implement the planned changes for SSPR.

What occurs when User3 attempts to use SSPR? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

A.

Answer Area

Number of authentication methods required:

Authentication methods that can be used:

Correct Answer: A

Section:

QUESTION 7

DRAG DROP

You need to resolve the recent security incident issues.

What should you configure for each incident? To answer, drag the appropriate policy types to the correct issues. Each policy type 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:

| Policy Types | Answer Area |
|---------------------------------|---|
| An authentication method policy | Leaked credentials: <input type="text"/> |
| A Conditional Access policy | A sign-in from a suspicious browser: <input type="text"/> |
| A sign-in risk policy | Resources accessed from an anonymous IP address: <input type="text"/> |
| A user risk policy | |

Correct Answer:

Policy Types

- An authentication method policy
- A Conditional Access policy
- A sign-in risk policy
- A user risk policy

Answer Area

- Leaked credentials: A user risk policy
- A sign-in from a suspicious browser: A sign-in risk policy
- Resources accessed from an anonymous IP address: A sign-in risk policy

Section:

Explanation:

QUESTION 8

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 9

You need to modify the settings of the User administrator role to meet the technical requirements. Which two actions should you perform for the role? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Select Require justification on activation
- B. Set all assignments to Active
- C. Set all assignments to Eligible
- D. Modify the Expire eligible assignments after setting.
- E. Select Require ticket information on activation.

Correct Answer: A, B

Section:

Exam C

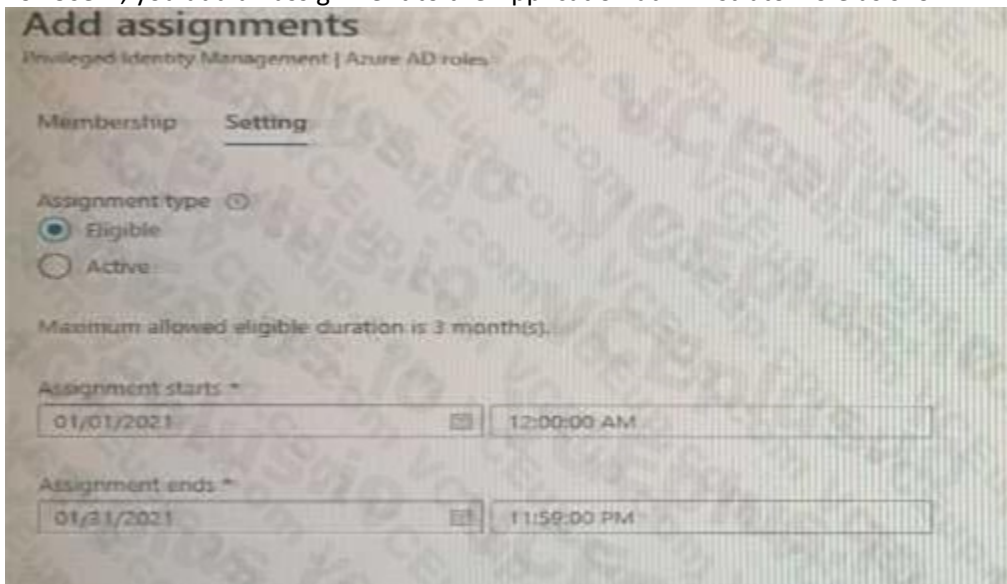
QUESTION 1

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

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| User1 is assigned the Application administrator role automatically. | <input type="radio"/> | <input type="radio"/> |
| When User2 requests to be assigned the Application administrator role, only User3 can approve the request. | <input type="radio"/> | <input type="radio"/> |
| If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| User1 is assigned the Application administrator role automatically. | <input checked="" type="radio"/> | <input type="radio"/> |
| When User2 requests to be assigned the Application administrator role, only User3 can approve the request. | <input checked="" type="radio"/> | <input type="radio"/> |
| If a request by User1 to be assigned the Application administrator role is approved on January 31, 2021, at 23:00, User1 can use the role until February 1, 2021, at 04:00. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

QUESTION 2

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1. An administrator deletes User1. You need to identify the following:

- How many days after the account of User1 is deleted can you restore the account?
- Which is the least privileged role that can be used to restore User1?

What should you identify? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Number of days:

Role:

Answer Area:

Answer Area

Number of days:

Role:

- User administrator
- Network administrator
- Helpdesk administrator
- Domain name administrator

Section:

Explanation:

QUESTION 3

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 | Answer Area |
|-----------------------|--|
| Audit logs | Identify the locations and IP addresses used by Azure AD users to sign in: <input type="text"/> |
| Identity secure score | Identify changes to Azure AD users or service principals: <input type="text"/> |
| Provisioning logs | Review the Azure AD security settings and identify improvement recommendations: <input type="text"/> |
| Sign-in logs | |

Correct Answer:

| Resources | Answer Area |
|----------------------|--|
| <input type="text"/> | Identify the locations and IP addresses used by Azure AD users to sign in: <input type="text" value="Sign-in logs"/> |
| <input type="text"/> | Identify changes to Azure AD users or service principals: <input type="text" value="Audit logs"/> |
| Provisioning logs | Review the Azure AD security settings and identify improvement recommendations: <input type="text" value="Identity secure score"/> |
| <input type="text"/> | |

Section:

Explanation:

QUESTION 4

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 5

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:

Features

- Azure AD built-in roles
- Azure AD managed identities
- Azure role-based access control (Azure RBAC)

Answer Area

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

Delegate the ability to create new virtual machines:

Correct Answer:

Features

- Azure AD managed identities

Answer Area

Ensure that users can sign in to Azure virtual machines by using their Microsoft 365 credentials: Azure AD built-in roles

Delegate the ability to create new virtual machines: Azure role-based access control (Azure RBAC)

Section:

Explanation:

QUESTION 6

You create a new Microsoft 365 E5 tenant.

You need to ensure that when users connect to the Microsoft 365 portal from an anonymous IP address, they are prompted to use multi-factor authentication (MFA).

What should you configure?

- A. a sign-in risk policy
- B. a user risk policy
- C. an MFA registration policy

Correct Answer: A

Section:

QUESTION 7

You have a Microsoft 365 E5 subscription.

You need to create a Microsoft Defender for Cloud Apps session policy.

What should you do first?

- A. From the Microsoft Defender for Cloud Apps portal, select User monitoring.
- B. From the Microsoft Defender for Cloud Apps portal, select App onboarding/maintenance
- C. From the Azure Active Directory admin center, create a Conditional Access policy.
- D. From the Microsoft Defender for Cloud Apps portal, create a continuous report.

Correct Answer: A

Section:

QUESTION 8

You need to meet the authentication requirements for leaked credentials.

What should you do?

- A. Enable federation with PingFederate in Azure AD Connect.
- B. Configure Azure AD Password Protection.
- C. Enable password hash synchronization in Azure AD Connect.
- D. Configure an authentication method policy in Azure AD.

Correct Answer: C

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity>

QUESTION 9

HOTSPOT

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant.

The tenant contains the groups shown in the following table.

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

The tenant contains the users shown in the following table.

Hot Area:

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| User1 will be removed automatically from Group1 if the user does not respond to the review request. | <input type="radio"/> | <input type="radio"/> |
| User2 will be removed automatically from Group3 if the user does not respond to the review request. | <input type="radio"/> | <input type="radio"/> |
| User3 will be removed automatically from Group2 if the user does not respond to the review request. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| User1 will be removed automatically from Group1 if the user does not respond to the review request. | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 will be removed automatically from Group3 if the user does not respond to the review request. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 will be removed automatically from Group2 if the user does not respond to the review request. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

QUESTION 10

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 11

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 12

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 13

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

You create an enterprise application collection named HR Apps that has the following settings:

- Applications: App1, App2, App3
- Owners: Admin 1
- Users and groups: HRUsers

All 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?

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

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 14

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant contains the groups shown in the following table.

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

In Azure AD, you add a new enterprise application named Appl. Which groups can you assign to App1?

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

Correct Answer: A

Section:

QUESTION 15

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 policy1.
- D. Configure password protection for Windows Server Active Directory.

Correct Answer: B

Section:

QUESTION 16

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-identityprotection-remediate-unblock>

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

QUESTION 17

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 18

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

Correct Answer: C

Section:

QUESTION 19

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

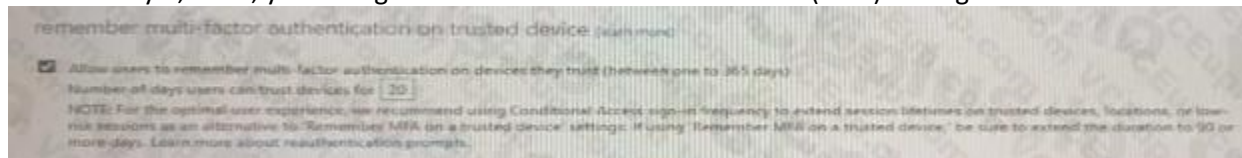
Section:

QUESTION 20

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.

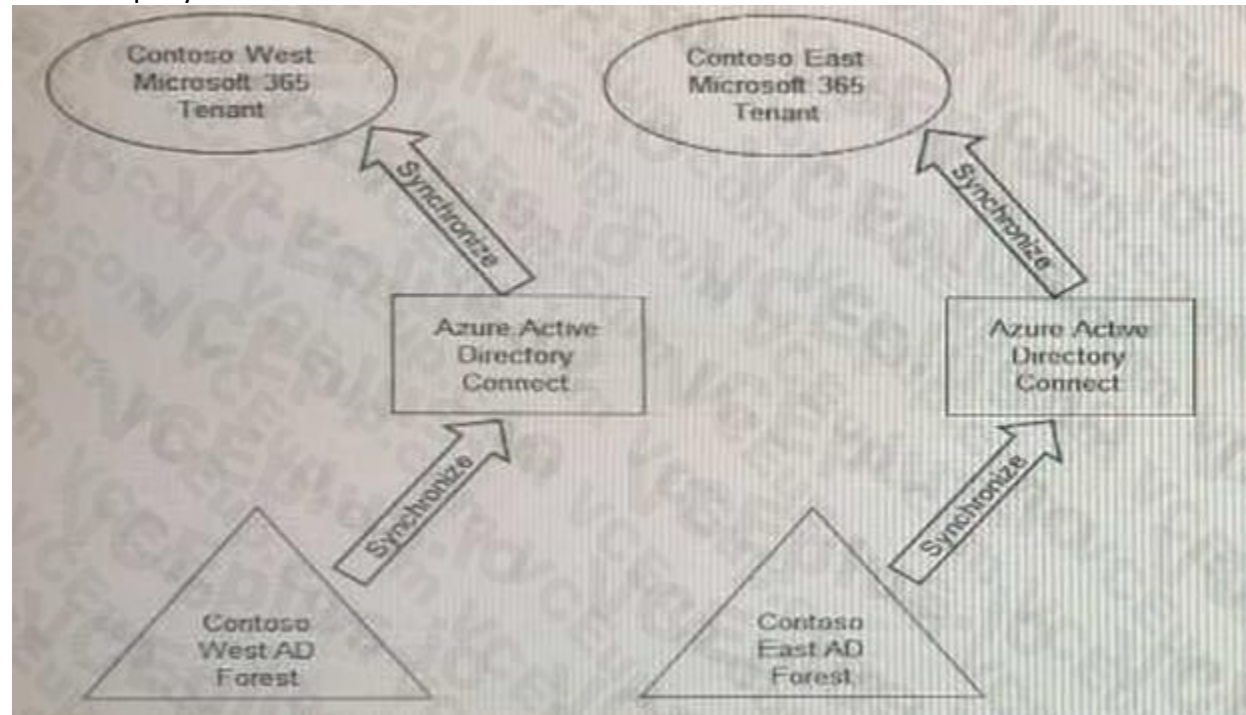
| Name | Multi-factor auth status |
|-------|--------------------------|
| User1 | Disabled |
| User2 | Enforced |
| User3 | Enforced |

Correct Answer: B

Section:

QUESTION 21

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 East 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 22

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 23

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 24

You have an Azure Active Directory (Azure AD) 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 25

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 26

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 27

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 28

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

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

What should you do first?

- A. Disable the User consent settings.
- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Configure password protection for Windows Server Active Directory.

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 29

Your company has a Microsoft 365 tenant.

The company has a call center that contains 300 users. In the call center, the users share desktop computers and might use a different computer every day. The call center computers are NOT configured for biometric identification.

The users are prohibited from having a mobile phone in the call center.

You need to require multi-factor authentication (MFA) for the call center users when they access Microsoft 365 services.

What should you include in the solution?

- A. a named network location
- B. the Microsoft Authenticator app
- C. Windows Hello for Business authentication
- D. FIDO2 tokens

Correct Answer: D

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authenticationpasswordless>

QUESTION 30

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

All users who run applications registered in Azure AD are subject to conditional access policies.

You need to prevent the users from using legacy authentication.

What should you include in the conditional access policies to filter out legacy authentication attempts?

- A. a cloud apps or actions condition
- B. a user risk condition
- C. a client apps condition
- D. a sign-in risk condition

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 31

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

You open the risk detections report.

Which risk detection type is classified as a user risk?

- A. impossible travel
- B. anonymous IP address
- C. atypical travel
- D. leaked credentials

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 32

You have a Microsoft 365 tenant.

All users have computers that run Windows 10. Most computers are company-owned and joined to Azure Active Directory (Azure AD). Some computers are user-owned and are only registered in Azure AD.

You need to prevent users who connect to Microsoft SharePoint Online on their user-owned computer from downloading or syncing files. Other users must NOT be restricted.

Which policy type should you create?

- A. a Microsoft Cloud App Security activity policy that has Microsoft Office 365 governance actions configured
- B. an Azure AD conditional access policy that has session controls configured
- C. an Azure AD conditional access policy that has client apps conditions configured
- D. a Microsoft Cloud App Security app discovery policy that has governance actions configured

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 33

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

The on-premises network contains a VPN server that authenticates to the on-premises Active Directory domain. The VPN server does NOT support Azure Multi-Factor Authentication (MFA).

You need to recommend a solution to provide Azure MFA for VPN connections.

What should you include in the recommendation?

- A. Azure AD Application Proxy
- B. an Azure AD Password Protection proxy
- C. Network Policy Server (NPS)
- D. a pass-through authentication proxy

Correct Answer: C

Section:

QUESTION 34

You have a Microsoft 365 tenant.

The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain. The domain contains the servers shown in the following table.

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

The domain controllers are prevented from communicating to the internet.

You implement Azure AD Password Protection on Server1 and Server2.

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

You need to ensure that Azure AD Password Protection will continue to work if a single server fails.

What should you implement on Server4?

- A. Azure AD Connect
- B. Azure AD Application Proxy
- C. Password Change Notification Service (PCNS)
- D. the Azure AD Password Protection proxy service

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-badon-premisesdeploy>

QUESTION 35

You have a Microsoft 365 tenant.

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

Users connect to the internet by using a hardware firewall at your company. The users authenticate to the firewall by using their Active Directory credentials.

You plan to manage access to external applications by using Azure AD.

You need to use the firewall logs to create a list of unmanaged external applications and the users who access them.

What should you use to gather the information?

- A. Application Insights in Azure Monitor
- B. access reviews in Azure AD
- C. Cloud App Discovery in Microsoft Cloud App Security
- D. enterprise applications in Azure AD

Correct Answer: C

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discoveryreports#using-traffic-logs-for-cloud-discovery>

QUESTION 36

You have a Microsoft 365 tenant.

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

You plan to create an emergency-access administrative account named Emergency1. Emergency1 will be assigned the Global administrator role in Azure AD. Emergency1 will be used in the event of Azure AD functionality failures and on-premises infrastructure failures.

You need to reduce the likelihood that Emergency1 will be prevented from signing in during an emergency.

What should you do?

- A. Configure Azure Monitor to generate an alert if Emergency1 is modified or signs in.
- B. Require Azure AD Privileged Identity Management (PIM) activation of the Global administrator role for Emergency1.
- C. Configure a conditional access policy to restrict sign-in locations for Emergency1 to only the corporate network.
- D. Configure a conditional access policy to require multi-factor authentication (MFA) for Emergency1.

Correct Answer: A

Section:

QUESTION 37

You have a Microsoft 365 tenant.

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

You need to ensure that only users who accept the terms of use can access the resources in the tenant. Other users must be denied access.

What should you configure?

- A. an access policy in Microsoft Cloud App Security.
- B. Terms and conditions in Microsoft Endpoint Manager.
- C. a conditional access policy in Azure AD
- D. a compliance policy in Microsoft Endpoint Manager

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 38

You have an Azure Active Directory (Azure AD) tenant that contains 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 |
| Group5 | Microsoft 365 | Dynamic User |

For which groups can you create an access review?

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

Correct Answer: D

Section:

Explanation:

You cannot create access reviews for device groups.

Reference:

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

QUESTION 39

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

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

User1 is the owner of Group1.

You create an access review that has the following settings:

Users to review: Members of a group

Scope: Everyone

Group: Group1

Reviewers: Members (self)

Which users can perform access reviews for User3?

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

Correct Answer: B

Section:

QUESTION 40

Your company recently implemented Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

While you review the roles in PIM, you discover that all 15 users in the IT department at the company have permanent security administrator rights.

You need to ensure that the IT department users only have access to the Security administrator role when required.

What should you configure for the Security administrator role assignment?

- A. Expire eligible assignments after from the Role settings details
- B. Expire active assignments after from the Role settings details
- C. Assignment type to Active
- D. Assignment type to Eligible

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 41

You have a Microsoft 365 tenant.

The Sign-ins activity report shows that an external contractor signed in to the Exchange admin center.

You need to review access to the Exchange admin center at the end of each month and block sign-ins if required.

What should you create?

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

Correct Answer: C

Section:

Explanation:

Reference:

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

QUESTION 42

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

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

You have a Microsoft 365 tenant.

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

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

Create an access review

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

Review name * Admin review

Description

Start date * 12/18/2020

Frequency Monthly

Duration (in days) 14

End Never End by Occurrences

Number of times 0

End date 01/17/2021

Users Scope Everyone

Review role membership (permanent and eligible) * Application Administrator and 72 others

Reviewers (Preview) Manager

(Preview) Fallback reviewers Megan Bowen

Upon completion settings

Start

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

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference:

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

QUESTION 43

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

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

You have a Microsoft 365 tenant.

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

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

Create an access review

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

Review name * Admin review

Description

Start date * 12/18/2020

Frequency Monthly

Duration (in days) 14

End Never End by Occurrences

Number of times 0

End date 01/17/2021

Users Scope Everyone

Review role membership (permanent and eligible) * Application Administrator and 72 others

Reviewers Reviewers (Preview) Manager

(Preview) Fallback reviewers Megan Bowen

Upon completion settings

Start

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

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

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: A

Section:

Explanation:

Reference:

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

QUESTION 44

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

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

You have a Microsoft 365 tenant.

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

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

Create an access review

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

Review name * Admin review ✓

Description ○

Start date * 12/18/2020 📅

Frequency Monthly ▼

Duration (in days) ○ 14

End ○ Never End by Occurrences

Number of times 0

End date 01/17/2021 📅

Users Scope Everyone

Review role membership (permanent and eligible) * Application Administrator and 72 others

Reviewers Reviewers (Preview) Manager ▼

(Preview) Fallback reviewers ○ Megan Bowen

✓ Upon completion settings

Start

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

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

Solution: You set Reviewers to Member (self).

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 45

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

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

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

What should you do?

- A. Run the New-AzADUser cmdlet.
- B. Configure the External collaboration settings.
- C. Add a WS-Fed identity provider.
- D. Create a guest user account in contoso.com.

Correct Answer: D

Section:

Explanation:

Reference:

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

QUESTION 46

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

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

What should you do in Azure AD Connect?

- A. Create an inbound synchronization rule for the Windows Azure Active Directory connector.
- B. Configure a Full Import run profile.
- C. Create an inbound synchronization rule for the Active Directory Domain Services connector.
- D. Configure an Export run profile.

Correct Answer: C

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-theconfiguration>

QUESTION 47

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

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

All the users work remotely.

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

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

| | |
|--------------------|----------------------|
| Sync Status | Enabled |
| Last Sync | Less than 1 hour ago |
| Password Hash Sync | Enabled |

USER SIGN IN



| | | |
|-----------------------------|----------|-----------|
| Federation | Disabled | 0 domains |
| Seamless single sign-on | Disabled | 0 domains |
| Pass-through authentication | Enabled | 2 agents |

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

Which users can sign in to Azure AD?

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

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-currentlimitations>

QUESTION 48

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

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

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

You discover that when a user account is disabled in Active Directory, the disabled user can still authenticate to Azure AD for up to 30 minutes.

You need to ensure that when a user account is disabled in Active Directory, the user account is immediately prevented from authenticating to Azure AD.

Solution: You configure Azure AD Password Protection.

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 49

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

You implement entitlement management to provide resource access to users at a company named Fabrikam, Inc. Fabrikam uses a domain named fabrikam.com.

Fabrikam users must be removed automatically from the tenant when access is no longer required.

You need to configure the following settings:

Block external user from signing in to this directory: No

Remove external user: Yes

Number of days before removing external user from this directory: 90

What should you configure on the Identity Governance blade?

- A. Access packages
- B. Settings
- C. Terms of use
- D. Access reviews

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-managementexternal-users>

QUESTION 50

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

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

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

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

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reportsdataretention#how-long-does-azure-ad-store-the-data>

QUESTION 51

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

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

You have a Microsoft 365 tenant.

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

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

Create an access review

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

Review name * Admin review

Description

Start date * 12/18/2020

Frequency Monthly

Duration (in days) 14

End Never End by Occurrences

Number of times 0

End date 01/17/2021

Users Scope Everyone

Review role membership (permanent and eligible) * Application Administrator and 72 others

Reviewers (Preview) Manager

(Preview) Fallback reviewers Megan Bowen

Upon completion settings

Start

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

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

Reference:

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

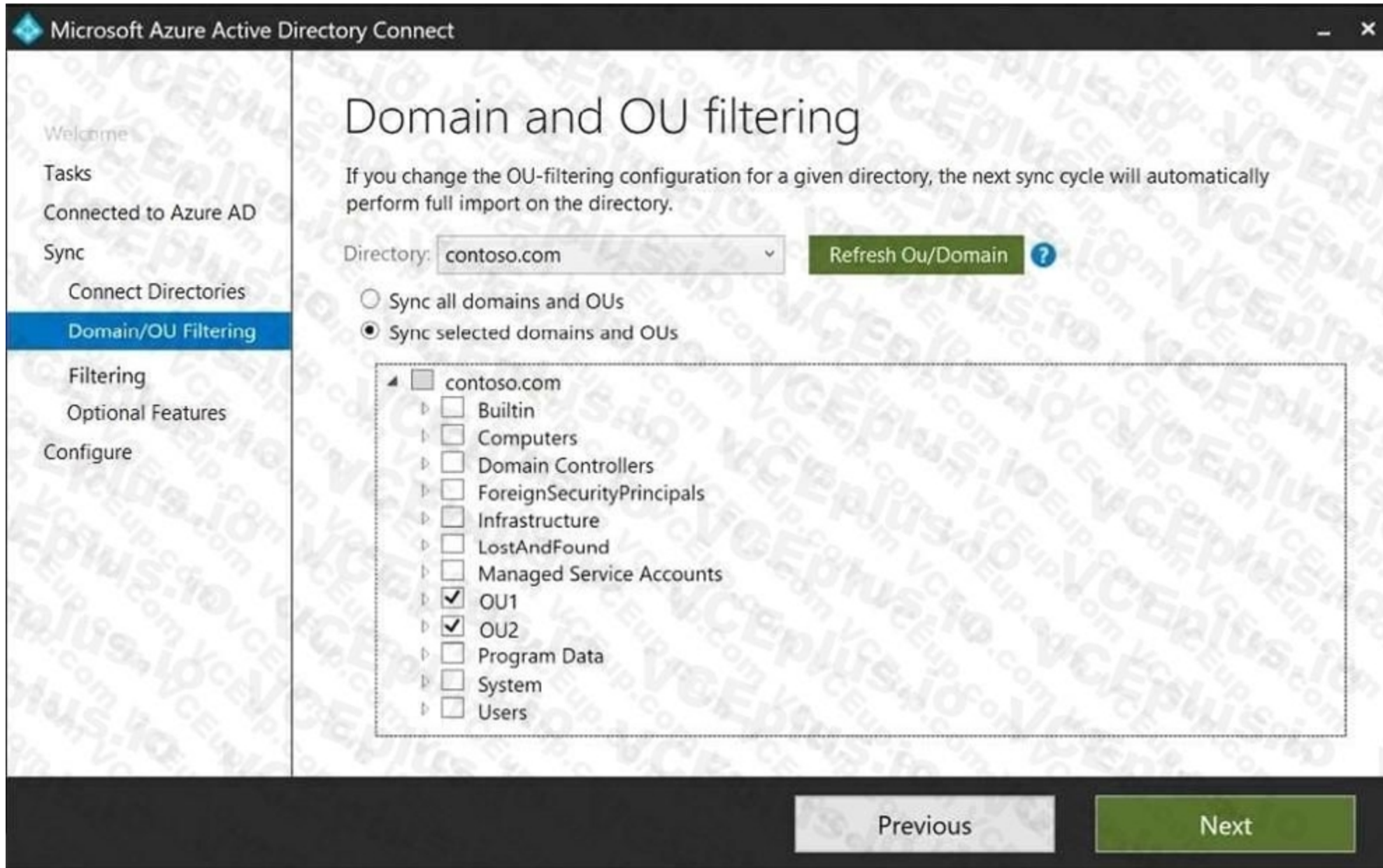
QUESTION 52

HOTSPOT

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

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

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



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

Microsoft Azure Active Directory Connect

Welcome

Tasks

Connected to Azure AD

Sync

Connect Directories

Domain/OU Filtering

Filtering


Optional Features

Configure

Filter users and devices


For a pilot deployment, specify a group containing your users and devices that will be synchronized. Nested groups are not supported and will be ignored.

Synchronize all users and devices

Synchronize selected 

FOREST: contoso.com

GROUP:

Resolve 

Previous

Next

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

- A.
- B.
- C.
- D.

Hot Area:

| Statements | Yes | No |
|---------------------------|-----------------------|-----------------------|
| User1 syncs to Azure AD. | <input type="radio"/> | <input type="radio"/> |
| User2 syncs to Azure AD. | <input type="radio"/> | <input type="radio"/> |
| Group2 syncs to Azure AD. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

| Statements | Yes | No |
|---------------------------|----------------------------------|----------------------------------|
| User1 syncs to Azure AD. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 syncs to Azure AD. | <input type="radio"/> | <input checked="" type="radio"/> |
| Group2 syncs to Azure AD. | <input checked="" type="radio"/> | <input type="radio"/> |

Section:

Explanation:

Only direct members of Group1 are synced. Group2 will sync as it is a direct member of Group1 but the members of Group2 will not sync.

Reference:

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

QUESTION 53

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. an app password
- C. Windows Hello for Business
- D. SMS

Correct Answer: C

Section:

Explanation:

In Windows 10, Windows Hello for Business replaces passwords with strong two-factor authentication on PCs and mobile devices. This authentication consists of a new type of user credential that is tied to a device and uses a biometric or

PIN.

After an initial two-step verification of the user during enrollment, Windows Hello is set up on the user's device and Windows asks the user to set a gesture, which can be a biometric, such as a fingerprint, or a PIN. The user provides the gesture to verify their identity. Windows then uses Windows Hello to authenticate users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authenticationmethods>

<https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hellooverview>

QUESTION 54

You have a Microsoft Entra tenant that has a Microsoft Entra ID P1 license. You need to review the Microsoft Entra ID sign-in logs to investigate sign-ins that occurred in the past. For how long does Microsoft Entra ID store events in the sign-in logs?

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

Correct Answer: B

Section:

Explanation:

×End Practice Test Are you sure you want to end the test? Yes No

QUESTION 55

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection policies enforced.

You create an Azure Sentinel instance and configure the Azure Active Directory connector.

You need to ensure that Azure Sentinel can generate incidents based on the risk alerts raised by Azure AD Identity Protection.

What should you do first?

- A. Add an Azure Sentinel data connector.
- B. Configure the Notify settings in Azure AD Identity Protection.
- C. Create an Azure Sentinel playbook.
- D. Modify the Diagnostics settings in Azure AD.

Correct Answer: A

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection>

QUESTION 56

You have a Microsoft 365 tenant.

All users have mobile phones and laptops.

The users frequently work from remote locations that do not have Wi-Fi access or mobile phone connectivity. While working from the remote locations, the users connect their laptop to a wired network that has internet access.

You plan to implement multi-factor authentication (MFA).

Which MFA authentication method can the users use from the remote location?

- A. a notification through the Microsoft Authenticator app
- B. email
- C. security questions
- D. a verification code from the Microsoft Authenticator app

Correct Answer: D

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authenticationauthenticator-app#verification-code-from-mobile-app>

QUESTION 57

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

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

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

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

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

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

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:

QUESTION 58

DRAG DROP

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

| Name | Type | Description |
|---------|-----------------|---------------------------------|
| User1 | User | None |
| User2 | User | None |
| Vault1 | Azure Key Vault | Contains a secret named Secret1 |
| Vault2 | Azure Key Vault | Contains a secret named Secret2 |
| Secret1 | Secret | Stored in Vault1 |
| Secret2 | Secret | Stored in Vault2 |

The subscription uses Privileged Identity Management (PIM).

You need to configure the following access controls by using PIM:

* Ensure that User1 can read and update Secret1.

* Ensure that User2 can read the contents of the secrets stored in Vault2.

The solution must follow the principle of least privilege.

Which authorization method should you use for each user? To answer, drag the appropriate authorization methods to the correct users. Each authorization method 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:

Authorization methods

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

Answer Area

User1:

User2:

Correct Answer:

Authorization methods

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

Answer Area

The Key Vault Secrets Officer RBAC role

The Key Vault Secrets User RBAC role

Section:

Explanation:

QUESTION 59

HOTSPOT

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

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

You create a Microsoft Entra user named User1.

Which identities can you add to VM1 and App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct answer is worth one point.

Answer Area

VM1: User1 only
 User1 only
 Managed2 only
 Managed1 and Managed2 only
 Managed2 and User1 only
 Managed1, Managed2, and User1

App1: A system-assigned managed identity only
 User1 only
 Managed2 only
 Managed2 and User1 only
 A system-assigned managed identity only
 A system-assigned managed identity and Managed2 only
 A system-assigned managed identity, Managed2, and User1

Answer:

Answer Area

VM1: User1 only
 User1 only
 Managed2 only
 Managed1 and Managed2 only
 Managed2 and User1 only
 Managed1, Managed2, and User1

App1: A system-assigned managed identity only
 User1 only
 Managed2 only
 Managed2 and User1 only
 A system-assigned managed identity only
 A system-assigned managed identity and Managed2 only
 A system-assigned managed identity, Managed2, and User1

Hot Area:

Answer Area

VM1: User1 only

- User1 only
- Managed2 only
- Managed1 and Managed2 only
- Managed2 and User1 only
- Managed1, Managed2, and User1

App1: A system-assigned managed identity only

- User1 only
- Managed2 only
- Managed2 and User1 only
- A system-assigned managed identity only
- A system-assigned managed identity and Managed2 only
- A system-assigned managed identity, Managed2, and User1

Answer Area:

Answer Area

VM1: User1 only

- User1 only
- Managed2 only
- Managed1 and Managed2 only
- Managed2 and User1 only
- Managed1, Managed2, and User1

App1: A system-assigned managed identity only

- User1 only
- Managed2 only
- Managed2 and User1 only
- A system-assigned managed identity only
- A system-assigned managed identity and Managed2 only
- A system-assigned managed identity, Managed2, and User1

Section:

Explanation:

QUESTION 60

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 61

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 62

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 63

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 64

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

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

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:

QUESTION 65

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 66

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 67

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 68

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 69

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 70

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 71

You have a Microsoft 365 subscription. The subscription contains users that use Microsoft Outlook 2016 and Outlook 2013 clients. You need to implement tenant restrictions. The solution must minimize administrative effort. What should you do first?

- A. Upgrade the Outlook 2013 clients to Outlook 2016.
- B. Configure the Outlook 2013 clients to use modem authentication.
- C. Upgrade all the Outlook clients to Outlook 2019.
- D. From the Exchange admin center, configure Organization Sharing.

Correct Answer: A

Section:

QUESTION 72

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

| Name | Member of |
|-------|-----------|
| User1 | Group1 |
| User2 | Group2 |
| User3 | Group3 |

The tenant has the authentication methods shown in the following table.

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

Which users will sign in to cloud apps by matching a number shown in the app with a number shown on their phone?

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

Correct Answer: A

Section:

QUESTION 73

HOTSPOT

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

| Name | User risk level |
|-------|-----------------|
| User1 | Low |
| User2 | Medium |
| User3 | High |

You have the Azure AD Identity Protection policies shown in the following table.

| Type | Users | User risk | Sign-in risk | Controls |
|---------------------|-----------|---------------|--------------|--------------|
| User risk policy | All users | Low and above | Unconfigured | Block access |
| Sign-in risk policy | All users | Unconfigured | High | Block access |

You review the Risky users report and the Risky sign-ins report and perform actions for each user as shown in the following table.

| User | Action |
|-------|--------------------------|
| User1 | Confirm user compromised |
| User2 | Confirm sign-in safe |
| User3 | Dismiss user risk |
| User2 | Confirm user compromised |

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 by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/> | <input type="radio"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|---|-----------------------|----------------------------------|
| User1 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 can sign in by using multi-factor authentication (MFA). | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in from an anonymous IP address. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

QUESTION 74

You have an Azure subscription that contains a user named User1. You need to meet the following requirements:

- Prevent User1 from being added as an owner of newly registered apps.
- Ensure that User1 can manage the application proxy settings.

- Ensure that User2 can register apps.
 - Use the principle of least privilege.
- Which role should you assign to User1?

- A. Application developer
- B. Cloud application administrator
- C. Service support administrator
- D. Application administrator

Correct Answer: D

Section:

QUESTION 75

Your company purchases 2 new Microsoft 365 ES subscription and an app named App. You need to create a Microsoft Defender for Cloud Apps access policy for App1. What should you do you first? (Choose Correct Answer based on Microsoft Identity and Access Administrator at microsoft.com)

- A. Configure a Token configuration for App1.
- B. Add an API permission for App.
- C. Configure a Conditional Access policy to use app-enforced restrictions.
- D. Configure a Conditional Access policy to use Conditional Access App Control.

Correct Answer: C

Section:

Explanation:

<https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad>

To create a Microsoft Defender for Cloud Apps access policy for App1, you should configure a Conditional Access policy to use app-enforced restrictions. This will allow you to control access to your cloud apps based on conditions such as user, device, location, and app state. You can also use app-enforced restrictions to control access to your cloud apps based on the state of the app, such as whether it's running on a managed or unmanaged device.

QUESTION 76

You have an Azure AD tenant named contoso.com that contains the resources shown in the following table. You create a user named Admin 1.

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

You need to ensure that Admin can enable Security defaults for contoso.com. What should you do first?

- A. Configure Identity Governance.
- B. Delete Package1.
- C. Delete CAPolicy1.
- D. Assign Admin1 the Authentication administrator role for Au1

Correct Answer: D

Section:

Explanation:

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

QUESTION 77

HOTSPOT

You have an Azure AD tenant that contains a user named User1. User1 is assigned the User Administrator role.

You need to configure External collaboration settings for the tenant to meet the following requirements:

*Guest users must be prevented from querying staff email addresses.

*Guest users must be able to access the tenant only if they are invited by User1.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

Hot Area:

Guest user access restrictions:

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

Guest invite restrictions:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite guest users including admins (most restrictive)

Enable guest self-service sign up via user flows: No Yes

Answer Area:



Section:

Explanation:

Box1 = User access is restricted to properties and memberships of their own directory objects (most restrictive). This setting ensures that guest users are prevented from querying staff email addresses and can access the tenant only if they are invited by User1.

Box2 = Only users assigned to specific admin roles can invite guest users. This setting ensures that guest users can access the tenant only if they are invited by User1.

Box3 = This setting enables guest users to sign up for the tenant only if they are invited by User1.

QUESTION 78

HOTSPOT

You have an Azure subscription.

Azure AD logs are sent to a Log Analytics workspace.

You need to query the logs and graphically display the number of sign-ins per user.

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

Hot Area:

SignInLogs

| where ResultType == 0

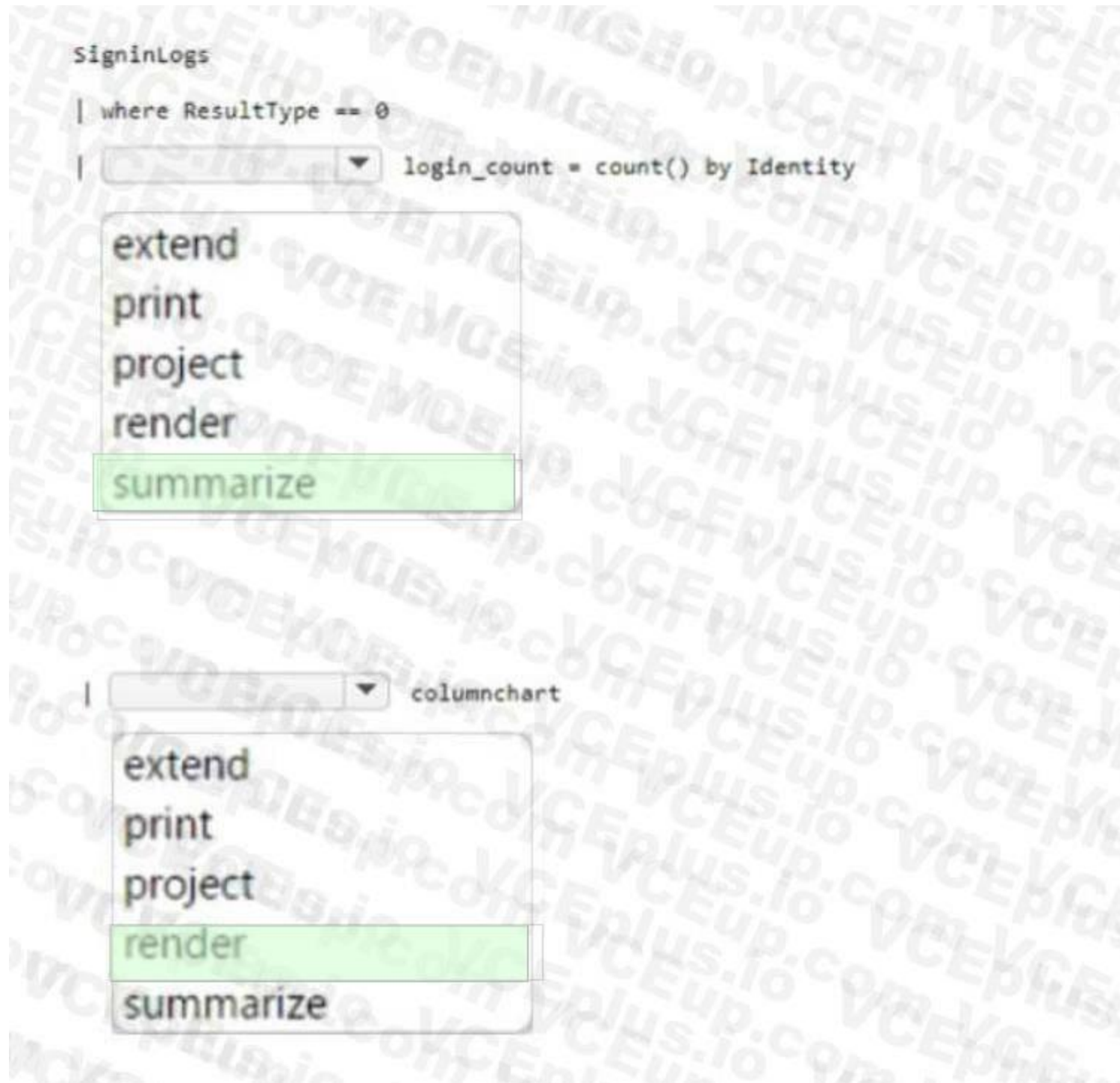
| login_count = count() by Identity

extend
print
project
render
summarize

| columnchart

extend
print
project
render
summarize

Answer Area:



Section:

Explanation:

Box 1 =

SigninLogs

| where ResultType == 0

| summarize login_count = count() by identity

| render piechart

This query retrieves the sign-in logs, filters the successful sign-ins, summarizes the count of sign-ins per user, and renders the result as a pie chart.

Box 2 = Render

QUESTION 79

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 80

HOTSPOT

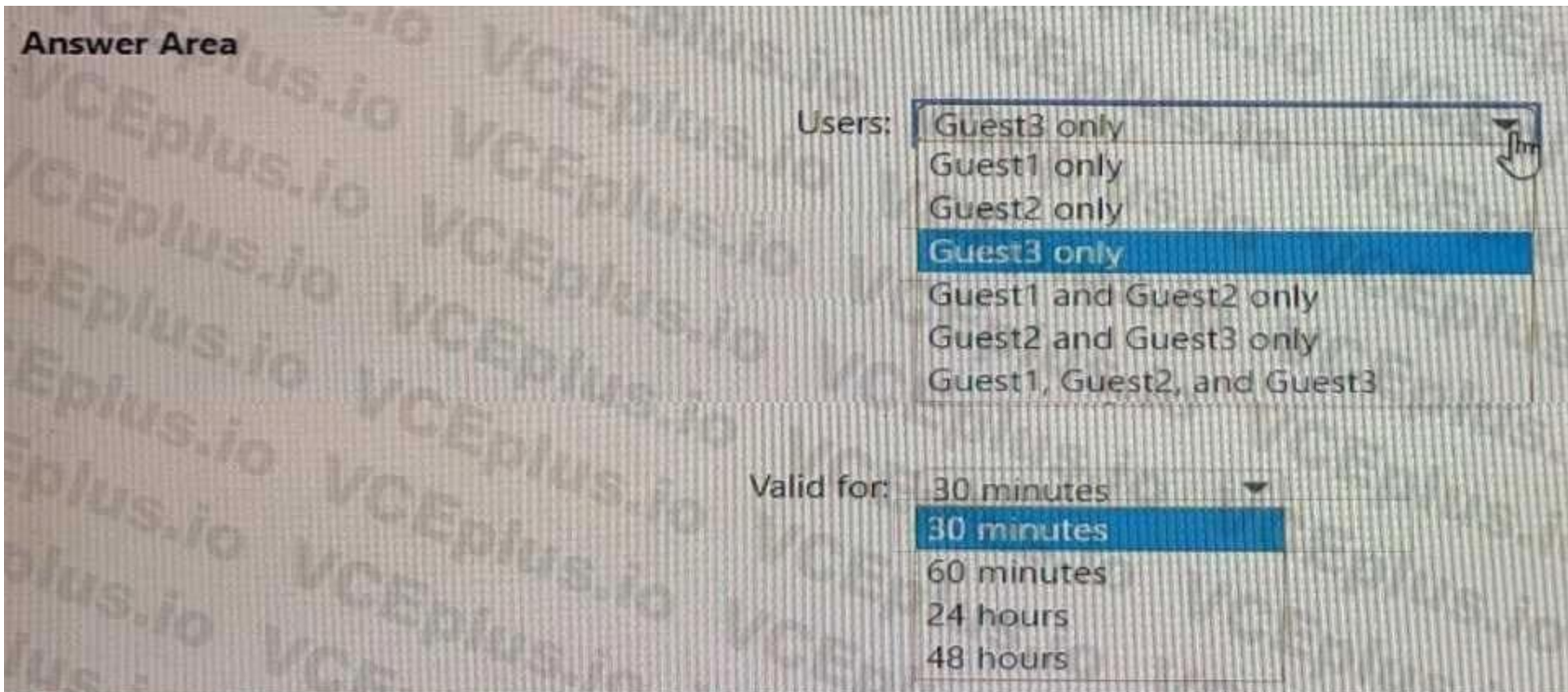
You have an Azure AD tenant named contoso.com that has Email one-time passcode for guests set to Yes.

You invite the guest users shown in the following table.

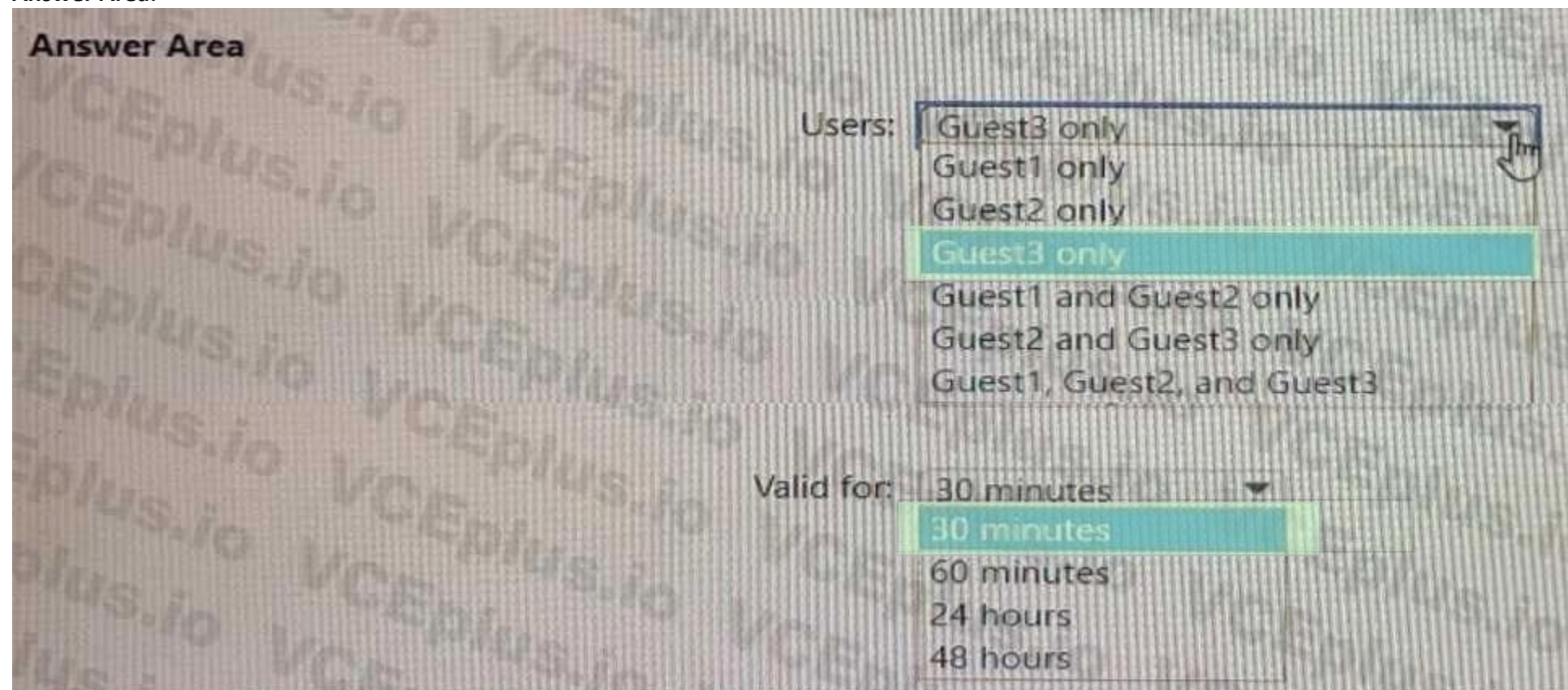
Which users will receive a one-time passcode, and how long will the passcode be valid? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 81

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.

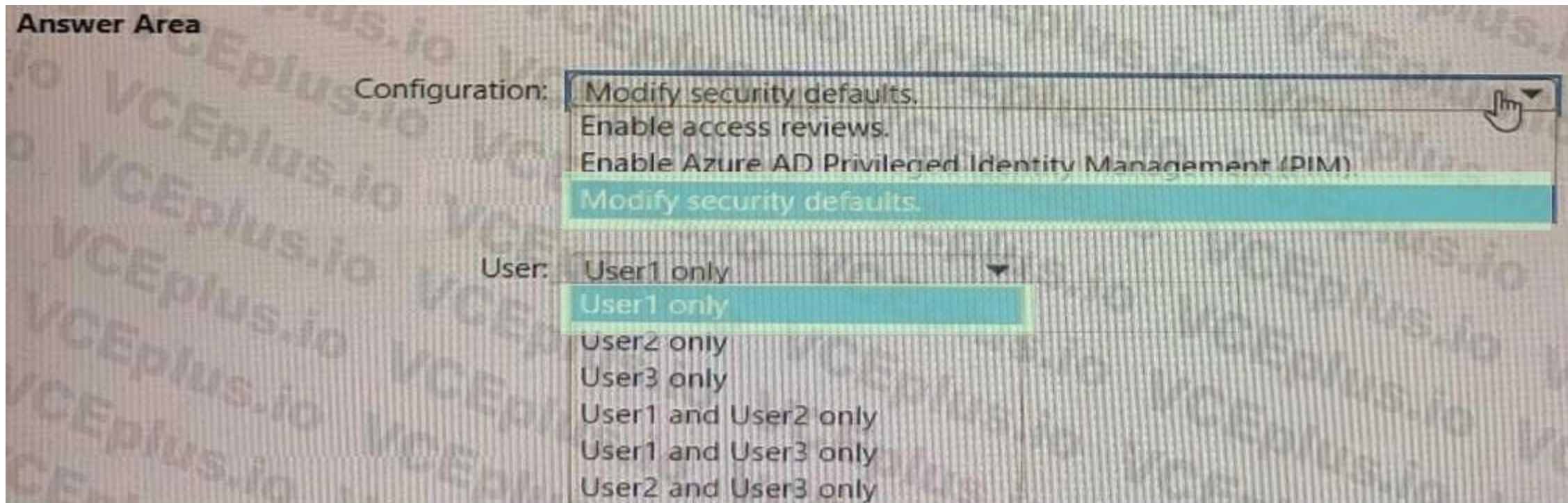
Hot Area:

Answer Area

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

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

Answer Area:



Section:

Explanation:

QUESTION 82

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 83

HOTSPOT

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

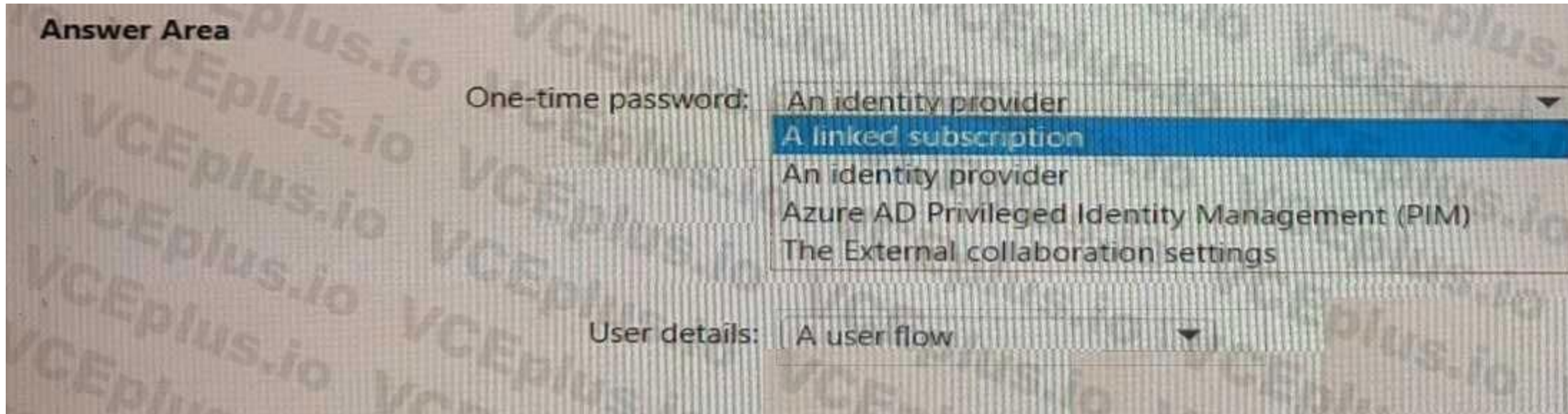
You need to provide guest users with self-service sign-up for App1. The solution must meet the following requirements:

- 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.

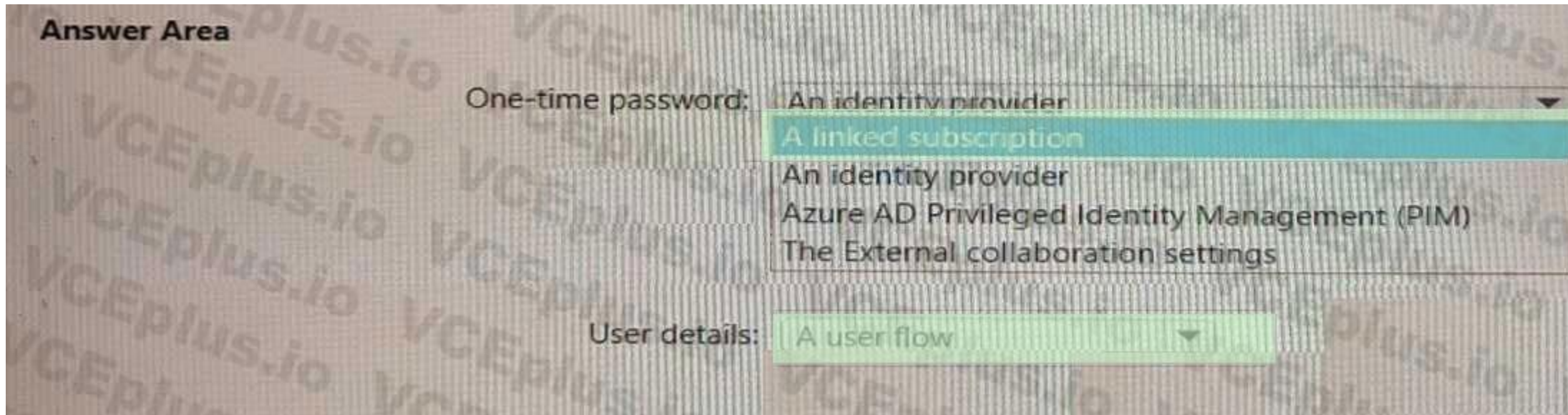
What should you configure in the Azure Active Directory admin center for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 84

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 85

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

- Enforce policy: On

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

- Enforce policy. On

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:

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 86

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 87

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.

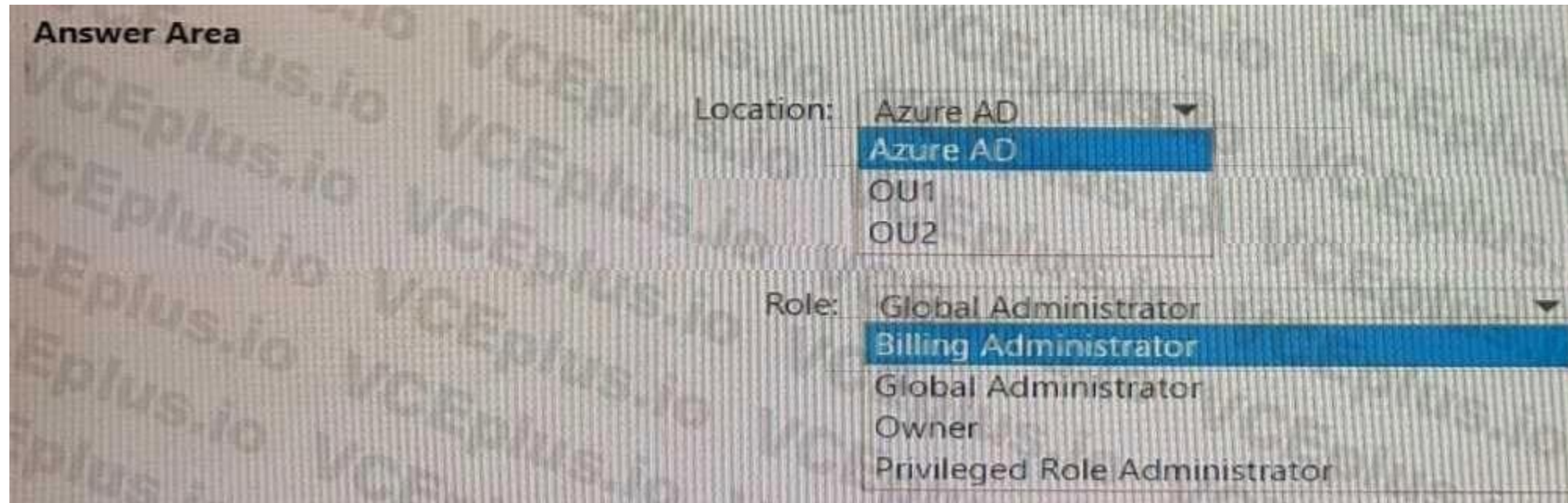
| Name | Description |
|------|------------------------------------|
| OU1 | Syncs with Azure AD |
| OU2 | Does NOT sync with Azure AD |

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

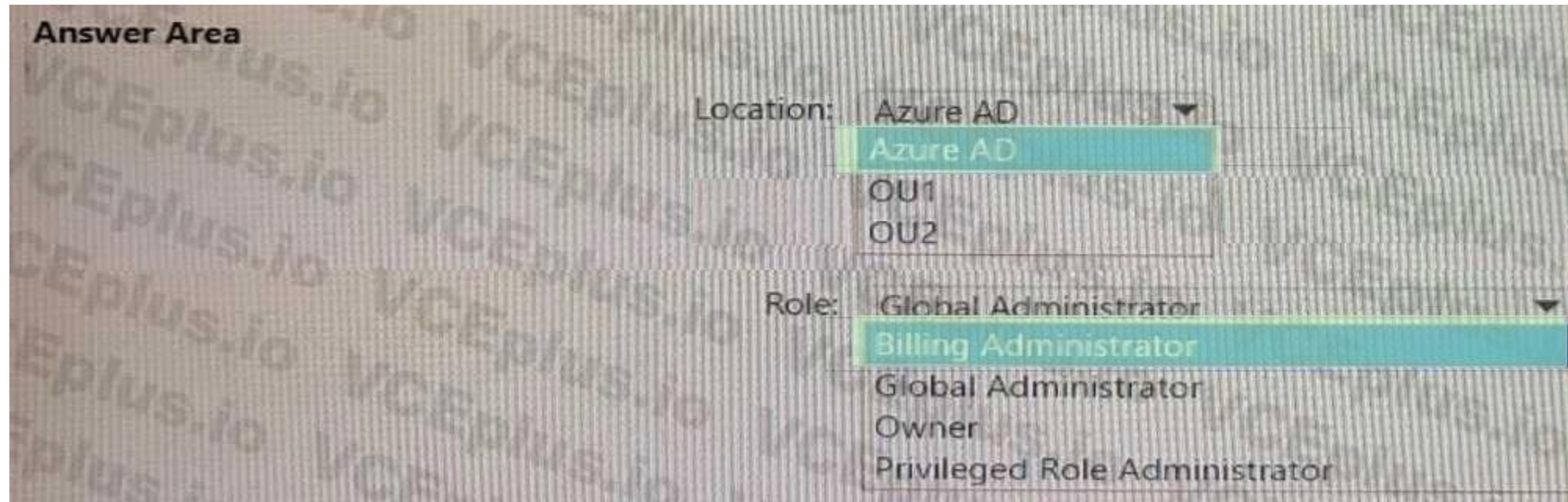
Where should you create BreakGlass, and which role should you assign to BreakGlass? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area:



Section:

Explanation:

QUESTION 88

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 89

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 90

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 91

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 92

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="radio"/> | <input type="radio"/> |
| You can assign Managed3 to VM1. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can assign VM1 the Owner role for RG1. | <input type="radio"/> | <input checked="" type="radio"/> |

Section:

Explanation:

QUESTION 93

HOTSPOT

You have an Azure subscription.

From Entitlement management, you plan to create a catalog named Catalog1 that will contain a custom extension.

What should you create first and what should you use to distribute Catalog1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

First create:

| | |
|-----------------------------|---|
| An Azure Automation account | ▼ |
| A managed account | |
| An Azure Automation account | |
| An Azure logic app | |

Distribute Catalog1 by using:

| | |
|-------------------|---|
| A playbook | ▼ |
| A playbook | |
| A workflow | |
| An access package | |

Answer Area:

Answer Area

First create:

| | |
|-----------------------------|---|
| An Azure Automation account | ▼ |
| A managed account | |
| An Azure Automation account | |
| An Azure logic app | |

Distribute Catalog1 by using:

| | |
|-------------------|---|
| A playbook | ▼ |
| A playbook | |
| A workflow | |
| An access package | |

Section:

Explanation:

QUESTION 94

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

| Name | Role |
|-------|------------------------|
| User1 | User Administrator |
| User2 | Password Administrator |
| User3 | Security Reader |
| User4 | User |

You enable self-service password reset (SSPR) for all the users and configure SSPR to require security questions as the only authentication method. Which users must use security questions when resetting their password?

- A. User4 only
- B. User3 and User4 only
- C. User1 and User4 only
- D. User1, User3, and User4 only
- E. User1, User2, User3, and User4

Correct Answer: B

Section:

QUESTION 95

You have an Azure AD tenant and a .NET web app named App1. You need to register App1 for Azure AD authentication. What should you configure for App1?

- A. the executable name
- B. the bundle ID
- C. the package name
- D. the redirect URI

Correct Answer: D

Section:

QUESTION 96

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 | Answer Area |
|------------------------------|---|
| Admin1 | |
| All guest and external users | Include: <input data-bbox="1893 212 2362 264" type="text"/> |
| All users | Exclude: <input data-bbox="1893 327 2362 380" type="text"/> |
| Directory roles | |
| None | |

Correct Answer:

| Options | Answer Area |
|-----------------|--|
| Admin1 | Include: <input data-bbox="1893 816 2362 869" type="text" value="All users"/> |
| | Exclude: <input data-bbox="1893 932 2362 984" type="text" value="All guest and external users"/> |
| | |
| Directory roles | |
| None | |

Section:

Explanation:

QUESTION 97

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 98

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 Appl.

Correct Answer: A

Section:

QUESTION 99

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 100

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 101

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 102

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 103

You have an Azure subscription.

You need to use Microsoft Entra Permissions Management to automatically monitor permissions and create and implement right-size roles. The solution must follow the principle of least privilege.

Which role should you assign to the service principal of Permissions Management?

- A. Reader
- B. Contributor
- C. Owner
- D. User Access Administrator

Correct Answer: D

Section:

QUESTION 104

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

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

You have a Microsoft 365 tenant.

All users must use the Microsoft Authenticator app for multi-factor authentication (MFA) when accessing Microsoft 365 services.

Some users report that they received an MFA prompt on their Microsoft Authenticator app without initiating a sign-in request.

You need to block the users automatically when they report an MFA request that they did not initiate.

Solution: From the Microsoft Entra admin center, you configure the Notifications settings for multi-factor authentication (MFA).

Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

QUESTION 105

You have a Microsoft Entra tenant.

You need to query risky user activity for the tenant.

How long will the logs of risky user activity be retained?

- A. 30 days
- B. 60 days
- C. 90 days
- D. 180 days

Correct Answer: A

Section:

QUESTION 106

You have a Microsoft Entra tenant.

You need to configure continuous access evaluation for app sign-ins and assign the configuration to users that are assigned the Application Administrator role.

What should you configure?

- A. a Conditional Access policy
- B. the Admin consent settings
- C. a sign-in risk policy
- D. an access review

Correct Answer: D

Section:

QUESTION 107

You have a Microsoft 365 E5 subscription.

You need to ensure that users are prompted to accept a custom terms of use (Toll) agreement when they sign in to the subscription.

What should you configure?

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

Correct Answer: B

Section: