- **Vendor: Microsoft**
- **Exam Code: SC-300**
- **Exam Name: Microsoft Identity and Access Administrator**
- **New Updated Questions from Braindump2go (Updated in August/2023)**

QUESTION 207
You have the Azure resources shown in the following table.

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

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

A. User1 only
B. User1 and Group1 only
C. User1 and VM1 only
D. User1, VM1, and App1 only
E. User1, Group1, VM1, and App1

QUESTION 208
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 Office 365 Enterprise E5 licenses to a group that includes all users.
You needed 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 Groups blade in the Azure Active Directory admin center
B. the Set-AzureAdUser cmdlet
C. the Identity Governance blade in the Azure Active Directory admin center
D. the Licenses blade in the Azure Active Directory admin center

Answer: D

QUESTION 209/
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, wu0gf others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of Identity Secure Score improvement actions.
Solution: You assign the Security Operator role to User1.
Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
With read and write access, you can make changes and directly interact with identity secure score.
Global administrator
Security administrator
Exchange administrator
SharePoint administrator
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score

QUESTION 210
Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.
You have a Microsoft 365 E5 subscription.
You create a user named User1.
You need to ensure that User1 can update the status of Identity Secure Score improvement actions.
Solution: You assign the SharePoint Administrator role to User1.
Does this meet the goal?

A. Yes
B. No

Answer: A
Explanation:
With read and write access, you can make changes and directly interact with identity secure score.
Global administrator
Security administrator
Exchange administrator
SharePoint administrator
https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#who-can-use-the-identity-secure-score

QUESTION 211
You have an Azure AD tenant that contains a user named Admin1.
You need to ensure that Admin1 can perform only the following tasks:
- From the Microsoft 365 admin center, create and manage service requests.
- From the Microsoft 365 admin center, read and configure service health.
- From the Azure portal, create and manage support tickets.
The solution must minimize administrative effort.
What should you do?

A. Create an administrative unit and add Admin1.
B. Enable Azure AD Privileged Identity Management (PIM) for Admin1.
C. Assign Admin1 the Helpdesk Administrator role.
D. Create a custom role and assign the role to Admin1.

Answer: C
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator

QUESTION 212
Hotspot Question
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.
NOTE: Each correct selection is worth one point.

Answer 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
- Only users assigned to specific admin roles can invite guest users
- No one in the organization can invite quest users including admins (most restrictive)

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

Answer:

Answer 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:

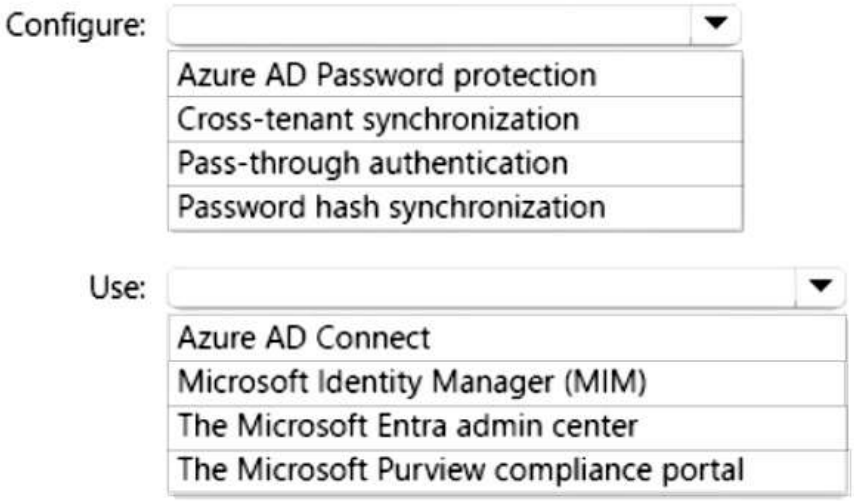
- Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
- Member users and users assigned to specific admin roles can invite guest users including guests with member
- **Only users assigned to specific admin roles can invite guest users**
- No one in the organization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

Enable guest self-service sign up via user flows:

- **No**
- Yes

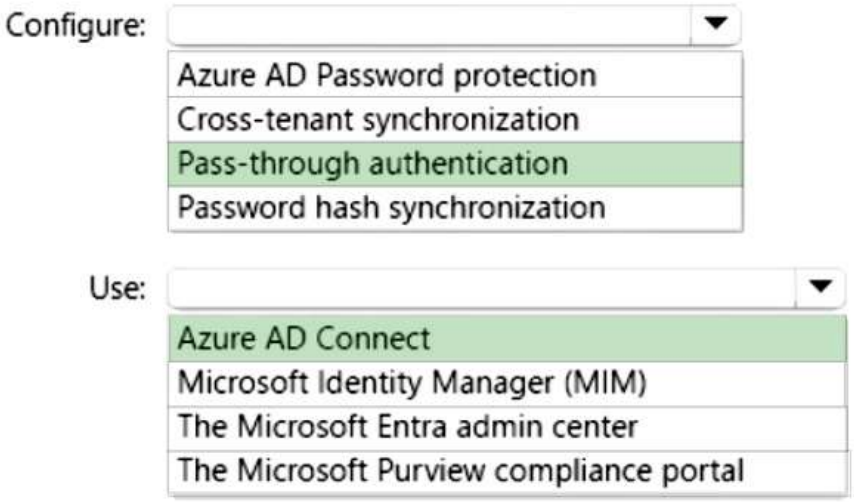
QUESTION 213
Hotspot Question
Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs with an Azure AD tenant.
You need to ensure that user authentication always occurs by validating passwords against the AD DS domain.
What should you configure, and what should you use? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



QUESTION 214
A user named User1 receives an error message when attempting to access the Microsoft Defender for Cloud Apps portal.
You need to identify the cause of the error. The solution must minimize administrative effort.
What should you use?

A. Log Analytics
B. sign-in logs
C. audit logs
D. provisioning logs

Answer: B

QUESTION 215
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps and Yammer.
You need prevent users from signing in to Yammer from high-risk locations.
What should you do in the Microsoft Defender for Cloud Apps portal?

A. Create an access policy.
B. Create an activity policy.
C. Unsanction Yammer.
D. Create an anomaly detection policy.

Answer: A
Explanation:
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad

QUESTION 216
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. an email to an address outside your organization
B. a mobile app notification
C. an FIDO2 security token
D. an email to an address in your organization

Answer: A
Explanation:
When using a mobile app as a method for password reset, like the Microsoft Authenticator app, the following considerations apply:
- When administrators require one method be used to reset a password, verification code is the only option available.
- When administrators require two methods be used to reset a password, users are able to use notification OR verification code in addition to any other enabled methods.
https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks#mobile-app-and-sspr

QUESTION 217
You have an Azure AD tenant.
You configure User consent settings to allow users to provide consent to apps from verified publishers.
You need to ensure that the users can only provide consent to apps that require low impact permissions.
What should you do?

A. Create an enterprise application collection.
B. Create an access review.
C. Create an access package.
D. Configure permission classifications.

Answer: D
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-permission-classifications?pivots=portal

QUESTION 218
Hotspot Question

You have a Microsoft 365 E5 subscription that contains a user named User1.
You configure app governance integration.
User1 needs to view the App governance dashboard. The solution must use the principle of the least privilege.
Which role should you assign to User1, and which portal should User1 use to view the dashboard? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Role:
- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:
- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Answer:

Answer Area

Role:
- Application Administrator
- Application Developer
- Cloud Application Administrator

Portal:
- The Microsoft 365 admin center
- The Microsoft 365 Defender portal
- The Microsoft Defender for Cloud Apps portal
- The Microsoft Purview compliance portal

Explanation:
https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles

QUESTION 219
You have an Azure subscription.
You are evaluating enterprise software as a service (SaaS) apps.
You need to ensure that the apps support automatic provisioning of Azure AD users.
Which specification should the apps support?

A. OAuth 2.0
B. WS-Fed
C. SCIM 2.0
D. LDAP 3

Answer: C
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/app-provisioning/user-provisioning

QUESTION 220
You have a Microsoft 365 E5 subscription that contains a user named User1.
You need to ensure that User1 can create access reviews for Azure AD roles. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Privileged role administrator
B. Identity Governance Administrator
C. User administrator
D. User Access Administrator

Answer: C
Explanation:
To create access reviews for Azure resources, you must be assigned to the Owner or the User Access Administrator role for the Azure resources. To create access reviews for Azure AD roles, you must be assigned to the Global Administrator or the Privileged Role Administrator role.
https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-create-roles-and-resource-roles-review#prerequisites

QUESTION 221
Hotspot Question
You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.
You have two Azure AD roles that have the Activation settings shown in the following table.

Name	Required justification on activation	Require approval to activate	Approvers
Role1	No	Yes	User1
Role2	Yes	No	None

The Azure AD roles have the Assignment settings shown in the following table.

Role	Allow permanent eligible assignment	Allow Permanent activate assignment	Require justification on active assignment
Role1	Yes	Yes	Yes
Role2	No	Yes	Yes

The Azure AD roles have the eligible users shown in the following table.

Role	Eligible assignment
Role1	User1, User2
Role2	User3

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

Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

Answer:

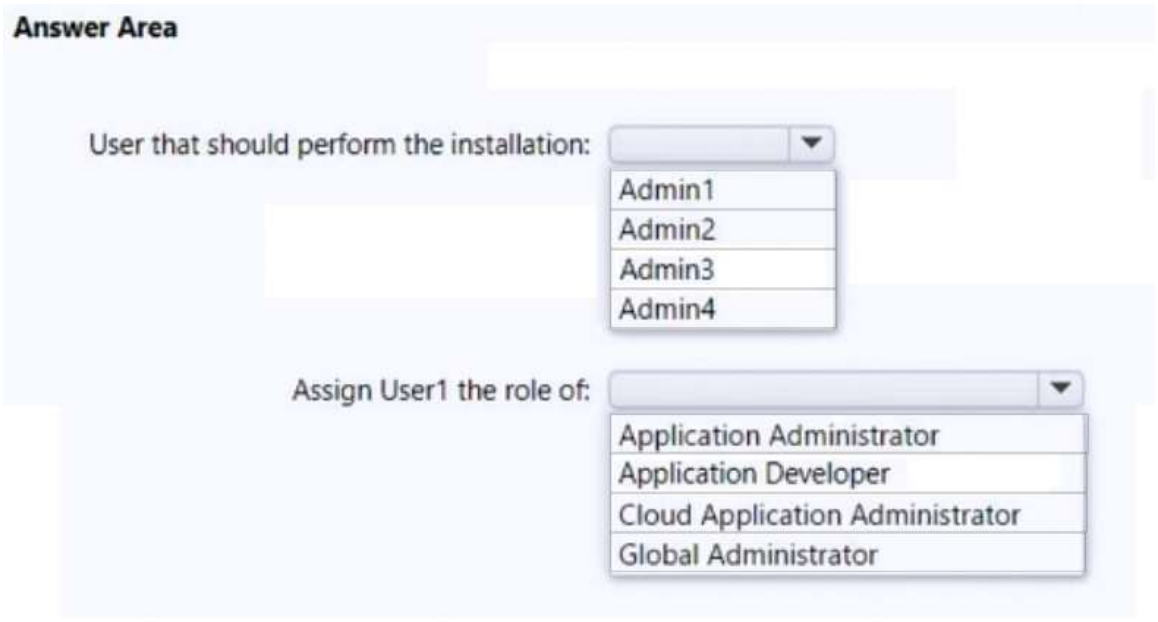
Answer Area

Statements	Yes	No
If User1 requests Role1, the request will be approved automatically.	○	○
User1 can approve the request of User3 for Role2.	○	○
User1 must provide justification to approve the request of User2 for Role1.	○	○

QUESTION 222
Hotspot Question
You have a hybrid Microsoft 365 subscription that contains the users shown in the following table.

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

You plan to deploy an on-premises app named App1. App1 will be registered in Azure AD and will use Azure AD Application Proxy.
You need to delegate the installation of the Application Proxy connector and ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which user should perform the installation, and which role should you assign to User1? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.



Answer:

QUESTION 223
Hotspot Question
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.

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

The users are assigned the roles shown in the following table.

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

For which users can User1 and User4 reset passwords? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

User 1:

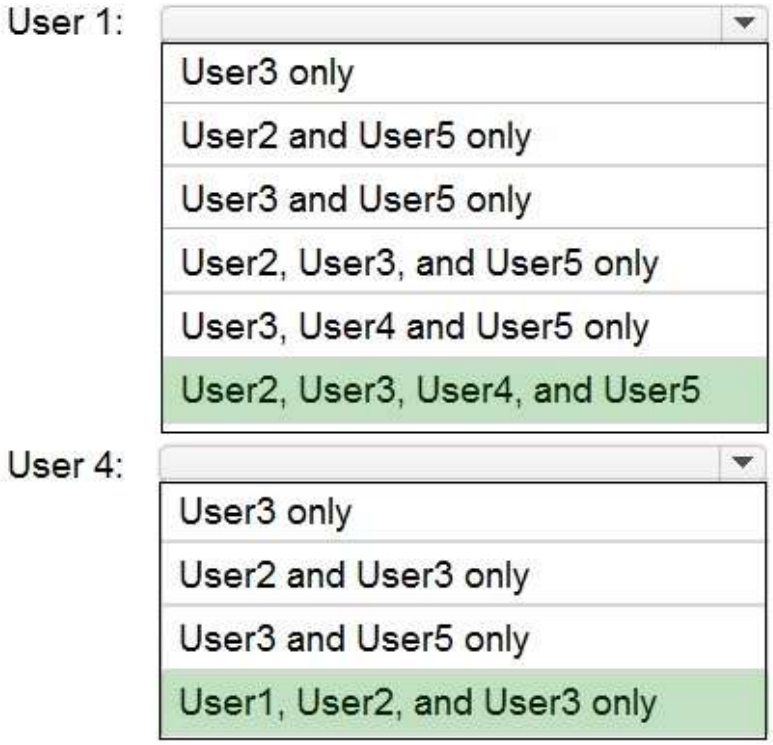
- User3 only
- User2 and User5 only
- User3 and User5 only
- User2, User3, and User5 only
- User3, User4 and User5 only
- User2, User3, User4, and User5

User 4:

- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

Answer:

Answer Area



Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#who-can-reset-passwords

QUESTION 224
You have a Microsoft 365 E5 subscription that contains a user named User1. User is eligible for the Application administrator role.
User1 needs to configure a new connector group for an application proxy.
What should you use to activate the role for User1?

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

Answer: C

QUESTION 225
You have an Azure subscription that contains a registered app named App1.
You need to review the sign-in activity for App1. The solution must meet the following requirements:
- Identify the number of failed sign-ins.
- Identify the success rate of sign-ins.
- Minimize administrative effort.

What should you use?

A. Sign-in logs

B. Access reviews
C. Audit logs
D. Usage & insights

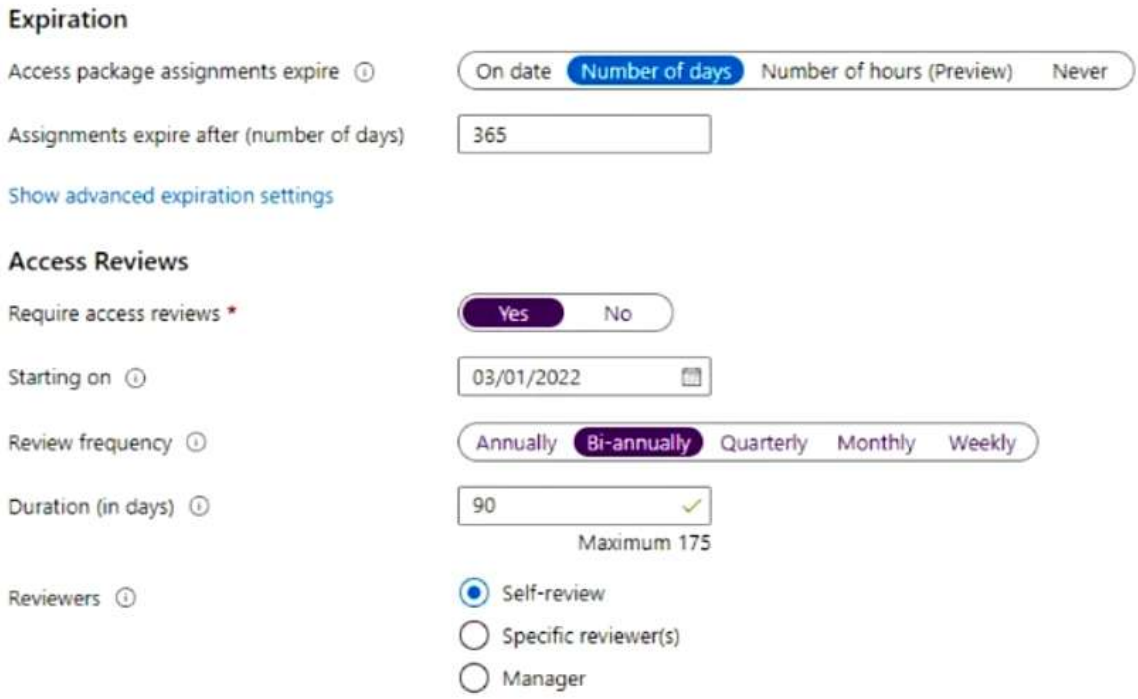
Answer: D

QUESTION 226
Your company has an Azure AD tenant that contains a user named User1.
The company has two departments named marketing and finance.
You need to grant permissions to User1 to manage only the users in the marketing department. The solution must ensure that User1 does NOT have permissions to manage the users in the finance department.
What should you create first?

A. a management group
B. an administrative unit
C. a resource group
D. a Microsoft 365 group

Answer: B

QUESTION 227
You have an Azure AD tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.



You need to ensure that User1 can modify the review frequency of Package1. The solution must use the principle of least privilege.
Which role should you assign to User1?

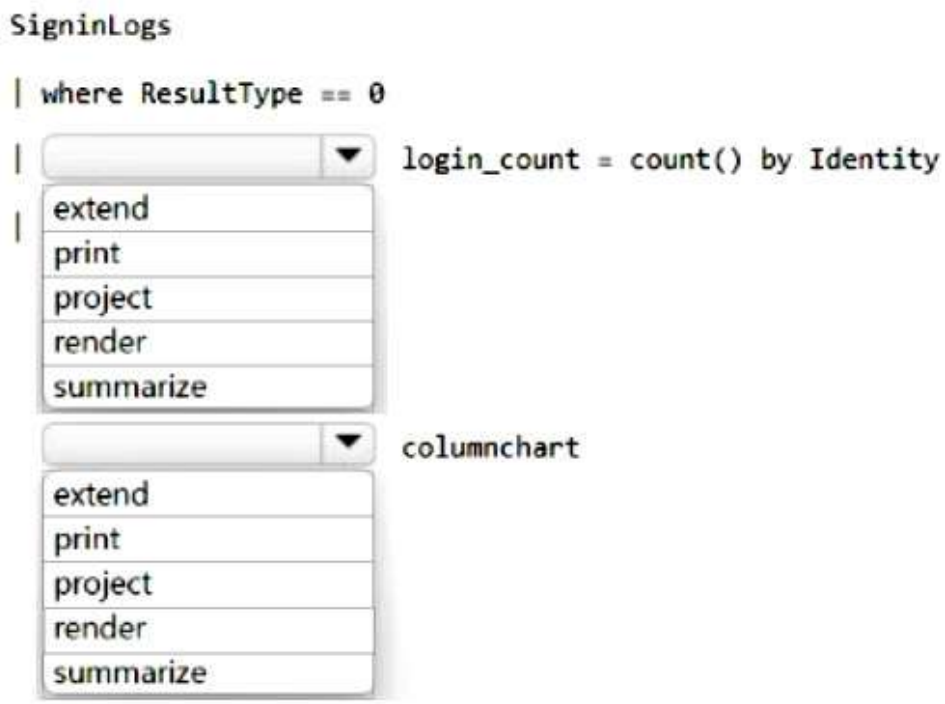
A. Security administrator
B. Privileged role administrator
C. External Identity Provider administrator
D. User administrator

Answer: D

Explanation:
To enable reviews of access packages, you must meet the prerequisites for creating an access package:
- Microsoft Azure AD Premium P2 or Microsoft Entra ID Governance
- Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager

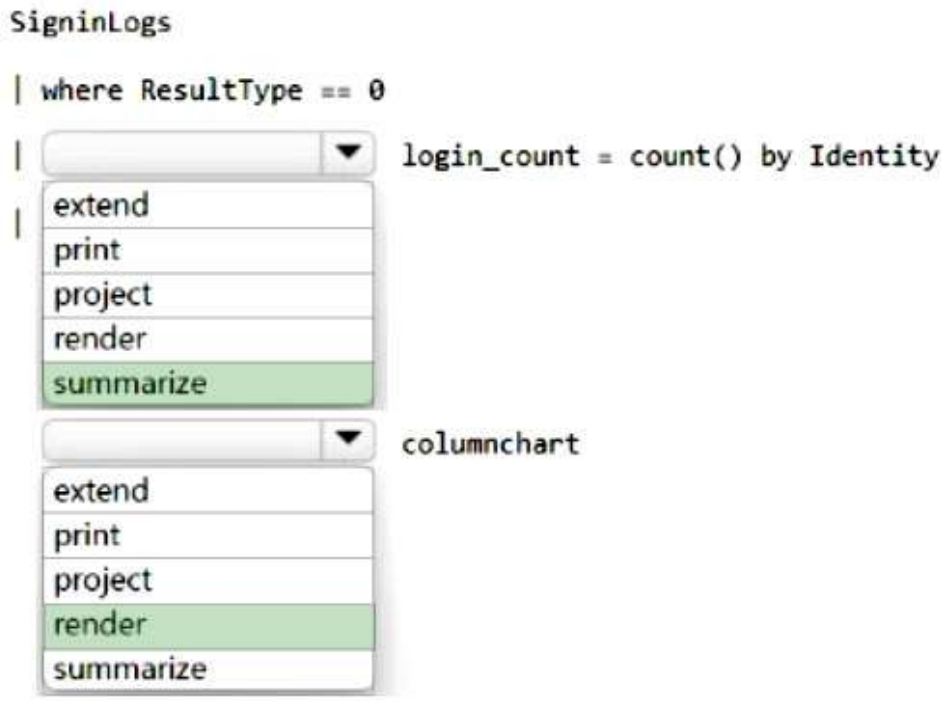
QUESTION 228
Hotspot Question
You have an Azure subscription.
Azure AD logs are sent to a Log Analytics workspace.
You need to query the logs and graphically display the number of sign-ins per user.
How should you complete the query? To answer, select the appropriate options in the answer area,
NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



QUESTION 229
You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.
You need to identify which users access Facebook from their devices and browsers. The solution must minimize administrative effort.
What should you do first?

A. Create a Conditional Access policy.
B. Create a Defender for Cloud Apps access policy.
C. Create an app configuration policy in Microsoft Endpoint Manager.
D. From the Microsoft Defender for Cloud Apps portal, unsanction Facebook.

Answer: D
Explanation:
Unsanctioning an app doesn't block use, but enables you to more easily monitor its use with the Cloud Discovery filters. You can then notify users of the unsanctioned app and suggest an alternative safe app for their use, or generate a block script using the Defender for Cloud Apps APIs to block all unsanctioned apps.
https://learn.microsoft.com/en-us/defender-cloud-apps/governance-discovery#sanctioningunsanctioning-an-app

QUESTION 230
You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).
You need to identify users that are eligible for the Cloud Application Administrator role.
Which blade in the Privileged Identity Management settings should you use?

A. Azure resources
B. Privileged access groups
C. Review access
D. Azure AD roles

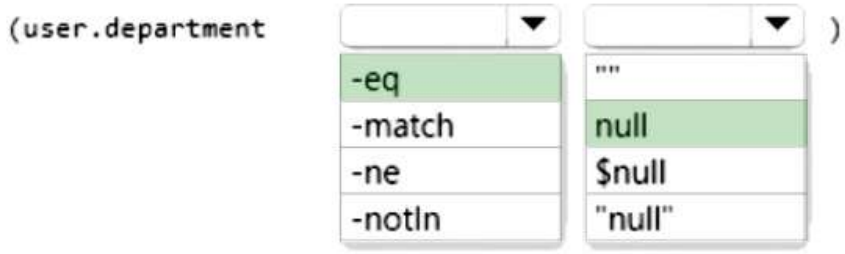
Answer: B

QUESTION 231
Hotspot Question
You have a Microsoft 365 E5 subscription.
You need to create a dynamic user group that will include all the users that do NOT have a department defined in their user profile.
How should you complete the membership rule? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Answer:

Answer Area



Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership#use-of-null-values