

Microsoft.SC-300.v2026-09-01.q197

|                                                                                                                                                               |                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Exam Code:                                                                                                                                                    | SC-300                                      |
| Exam Name:                                                                                                                                                    | Microsoft Identity and Access Administrator |
| Certification Provider:                                                                                                                                       | Microsoft                                   |
| Free Question Number:                                                                                                                                         | 197                                         |
| Version:                                                                                                                                                      | v2026-09-01                                 |
| # of views:                                                                                                                                                   | 105                                         |
| # of Questions views:                                                                                                                                         | 2116                                        |
| <a href="https://www.freecram.net/torrent/Microsoft.SC-300.v2026-09-01.q197.html">https://www.freecram.net/torrent/Microsoft.SC-300.v2026-09-01.q197.html</a> |                                             |

NEW QUESTION: 1

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains an administrative unit named Department1.

Department1 has the users shown in the Users exhibit. (Click the Users tab.)

Dashboard > ContosoAzureAD > Department1 Administrative Unit

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

Add member

Remove member

Bulk operations

Refresh

Columns

Preview features

Got feedback?

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

Add filters

2 users found

|                          | Name  | User principal name               | User type | Directory synced |
|--------------------------|-------|-----------------------------------|-----------|------------------|
| <input type="checkbox"/> | User1 | User1@m365x629615.onmicrosoft.com | Member    | No               |
| <input type="checkbox"/> | User2 | User2@m365x629615.onmicrosoft.com | Member    | No               |

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

Dashboard > ContosoAzureAD > Department1 Administrative Unit

## Department1 Administrative Unit | Groups

ContosoAzureAD - Azure Active Directory

» + Add Remove Refresh Columns Preview features Got feedback?

Search groups Add filters

| Name                                                                                     | Group Type | Membership Type |
|------------------------------------------------------------------------------------------|------------|-----------------|
|  Group1 | Security   | Assigned        |
|  Group2 | Security   | Assigned        |

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

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

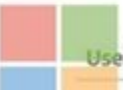
## User Administrator | Assignments

Privileged Identity Management | Azure AD roles

» + Add assignments Settings Refresh Export Got feedback?

Eligible assignments Active assignments Expired assignments

Search by member name or principal name

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

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

Dashboard > ContosoAzureAD > Groups > Group2

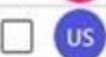
## Group2 | Members

Group

» + Add members Remove Refresh Bulk operations Columns Preview features Got feedback?

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

Direct members

| Name                                                                                      | User type |
|-------------------------------------------------------------------------------------------|-----------|
|  User3 | Member    |
|  User4 | Member    |

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

NOTE: Each correct selection is worth one point.

Answer Area

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

Microsoft

Answer:

Answer Area

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

Explanation:  
Admin1 and Admin2 are not members of Administrative group(Department1). However Admin1 has User administrator role scope for Department1 and Admin2 has User administrator role scope for the whole directory User 1  
And User 2 are users of Department1 Group1(No members) and Group2(User 3 and User4 are members) are groups of Department1.  
Box 1: No  
Admin1 cannot reset the password for User 3 and User4 because they are part of group2.(User admin role assigned to admin unit cannot reset password of users present inside the group.  
Admin1 can reset the password of User1 and User2 who are not part of any groups inside the admin unit) Box 2: Yes Admin1 can add/remove users to the GROUPS present inside the admin unit (Admin1 cannot add/remove users from USERS section) Box 3: Yes Admin2 is User admin at directory scope ,hence can reset password of any uses except the password of global admin/higher power roles

NEW QUESTION: 2

You have a Microsoft 365 tenant.  
All users have mobile phones and Windows 11 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.** email
- B.** Windows Hello for Business
- C.** voice
- D.** an app password

**Answer:** ([SHOW ANSWER](#))

Correct:

- \* a verification code from the Microsoft Authenticator app
- \* Windows Hello for Business

Incorrect:

- \* a notification through the Microsoft Authenticator app
- \* an app password
- \* email
- \* security questions
- \* SMS
- \* voice

Note:

Correct:

- \* Windows Hello for Business

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" 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.

- \* a verification code from the Microsoft Authenticator app

The Authenticator app can be used as a software token to generate an OATH verification code.

After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect:

- \* a notification through the Microsoft Authenticator app

A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the logon

- \* an app password

An app password can be used to open an application but it cannot be used to sign in to a computer.

- \* email

An email requires network connectivity.

Password reset authentication only. You'll need to choose a different method for two-'actor verification.

- \* security questions

Security questions are not used as an authentication method but can be used during the self- service password reset (SSPR) process.

- \* SMS

SMS requires a mobile phone

- \* voice

A voice call requires mobile connectivity.

Reference:

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

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

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

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

**NEW QUESTION: 3**

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1 and a Microsoft Teams team named Team1. The subscription contains five security groups named Group1, Group2, Group3, Group4, and Group5.

You need to implement access packages for Site1 and Team1. The solution must meet the following requirements:

- Members of Group3 must be able to request access to Site1 only.
- Members of Group1 must be able to request access to Site1 and Team1.
- Members of Group4 must be able to request access to Site1 and Team1.
- Only members of Group2 must be able to approve access package requests from Group1 members.
- Only members of Groups must be able to approve access package requests from Group3 and Group4 members.

What is the minimum number of access packages you should create?

- A.** 2
- B.** 3
- C.** 4
- D.** 5

**Answer:** ([SHOW ANSWER](#))

Three access packages needed.

- \* Members of Group3 must be able to request access to Site1 only. [One access package for Site1 named X1]
- \* Members of Group1 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X2]
- \* Members of Group4 must be able to request access to Site1 and Team1. [One access package for Site1 and Team1 named X3]
- \* Only members of Group2 must be able to approve access package requests from Group1 members. [Add Group2 as approver for X2]
- \* Only members of Group5 must be able to approve access package requests from Group3 and Group4 members. [Add Group5 as approver for X1 and for X3] Reference:  
<https://learn.microsoft.com/en-us/entra/id-governance/entitlement-management-access-package-first>

**NEW QUESTION: 4**

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the User Administrator role to User1.

Does this meet the goal?

- A.** Yes
- B.** No

Answer: (SHOW ANSWER)

<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/identity-secure-score#read- and-write-roles>

NEW QUESTION: 5

You have a Microsoft 365 tenant.

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

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

What should you create?

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

Answer: (SHOW ANSWER)

You can target a group with a conditional policy to detect and remediate the login at the end of each month.

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

NEW QUESTION: 6

Hotspot Question

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.

| Name  | Member of      | Role                 |
|-------|----------------|----------------------|
| User1 | Group1         | None                 |
| User2 | Group1, Group2 | None                 |
| User3 | Group2         | Global Administrator |

The subscription contains a Conditional Access policy that has the following settings:

- Name: Policy1
- Assignments
  - o Include
    - Users and Groups: Group1
    - Directory roles: Global Administrator
  - o Exclude
    - Users and Groups: Group2
- Target resources
  - o Target resources
    - Include
      - All cloud apps
    - Access controls
      - Grant
      - Require multifactor authentication

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

|                                                                                        | Yes                   | No                    |
|----------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input type="radio"/> | <input type="radio"/> |
| User2 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input type="radio"/> | <input type="radio"/> |
| User3 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

Statements

|                                                                                        | Yes                              | No                               |
|----------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 must use multifactor authentication (MFA) when signing in to Microsoft 365 apps. | <input type="radio"/>            | <input checked="" type="radio"/> |

NEW QUESTION: 7

As the Azure Administrator for your organization, you need to create several security groups and populate those groups based on specific profile attributes of your users. As users join your organization, they should be automatically added to the correct group. What should you configure for this?

- A. Power Groups
- B. Smart Groups
- C. Microsoft 365 Groups
- D. Dynamic Groups

Answer: (SHOW ANSWER)

Dynamic groups allow administrators to set rules to populate groups that are created in Azure AD based on user attributes such as userType, department, or country/region.

Reference:

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

NEW QUESTION: 8

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

| Name  | Group  |
|-------|--------|
| User1 | Group1 |
| User2 | Group1 |
| User3 | Group2 |
| User4 | Group2 |
| User5 | None   |

You have an administrative unit named Au1. Group1, User2, and User3 are members of Au1.

User5 is assigned the User administrator role for Au1.

For which users can User5 reset passwords?

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

Answer: (SHOW ANSWER)

Adding a group to an administrative unit brings the group itself into the management scope of the administrative unit, but not the members of the group. In other words, an administrator scoped to the administrative unit can manage properties of the group, such as group name or membership, but they cannot manage properties of the users or devices within that group (unless those users and devices are separately added as members of the administrative unit).

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

NEW QUESTION: 9

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

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

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

What should you configure for the Security administrator role assignment?

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

Answer: (SHOW ANSWER)

"Assignment type to Eligible" so the admins can request the role in future, for a limited time based on the Role Setting of "Activation maximum duration (hours): 8 (by default)".

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

NEW QUESTION: 10

You have an Azure subscription that contains an Azure Automation account named Automation1. You need to grant Automation1 access to Azure resources. The solution must meet the following requirements:

- Ensure that any permissions granted to Automation1 are removed when the account is deleted.
- Minimize administrative effort.

What should you use?

- A.** a system-assigned managed identity
- B.** a client secret
- C.** a certificate
- D.** user-assigned managed identity

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 11**

Hotspot Question

You have an Azure subscription that contains two resource groups named RG1 and RG2, a storage account named storage1.

You assign roles for the subscription as shown in the following table.

| User  | Role   |
|-------|--------|
| User1 | Reader |
| User2 | Reader |
| User3 | Reader |
| User4 | Owner  |

You assign roles for RG1 as shown in the following table.

| User  | Role                   |
|-------|------------------------|
| User1 | Reader and Data Access |
| User2 | Contributor            |

You assign roles for storage1 as shown in the following exhibit.

```
1 [
2   {
3     "RoleAssignmentId": "9dea588b-7569-4cfb-b92b-92748cdc550b",
4     "Scope": "/subscriptions/7fe6d66e-8694-4b54-beae-17fd819d4873/resourceGroups/RG2/providers/Microsoft.Storage/storageAccounts/storage1",
5     "DisplayName": "User3",
6     "SignInName": "User3@contoso.com",
7     "RoleDefinitionName": "User Access Administrator",
8     "RoleDefinitionId": "/subscriptions/7fe6d66e-8694-4b54-beae-17fd819d4873/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
9     "ObjectId": "919948b2-bc93-41a0-9562-9399576cc8f0",
10    "ObjectType": "User",
11    "RoleAssignmentDescription": "",
12    "ConditionVersion": "",
13    "Condition": ""
14  }
15 ]
```

Roles are NOT assigned for other Azure resources.

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements                                  | Yes                   | No                    |
|---------------------------------------------|-----------------------|-----------------------|
| User1 can read the data stored in storage1. | <input type="radio"/> | <input type="radio"/> |
| User2 can create a virtual network in RG2.  | <input type="radio"/> | <input type="radio"/> |
| User3 can assign roles for storage1.        | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                  | Yes                              | No                               |
|---------------------------------------------|----------------------------------|----------------------------------|
| User1 can read the data stored in storage1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can create a virtual network in RG2.  | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can assign roles for storage1.        | <input checked="" type="radio"/> | <input type="radio"/>            |

Explanation:

Box 1: Yes

User1 has the Reader role in the subscription.

The subscription includes the storage account.

User1 will have read access to the storage account.

(For RG1 User1 has the Reader and Data Access role.  
User1 has no role at the storage account scope level.)

Note:  
The Azure Reader role is a built-in role that grants users read-only access to view Azure resources. This means they can see information about resources, their properties, and configurations, but they cannot make any changes or modifications to those resources.

Box 2: No  
User2  
User2 has the Contributor role for RG1 only, but not for RG2.  
User2 has the Reader role in the subscription.  
User2 will not be able to create a virtual network in RG2.

Box 3: Yes  
User3 has the User Access Administrator role for the storage1storage account.  
The User Access Administrator role can assign roles. This role is specifically designed to manage access to Azure resources, including assigning roles to other users, groups, or service principals.

Reference:  
<https://learn.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

NEW QUESTION: 12

SIMULATION  
You are configuring the security for external users that are added to the tenant through access package assignments.  
If an external user was added to the tenant by using an access package assignment, you need to ensure that the user is removed from the tenant automatically 15 days after the access package is unassigned from the user.

**Answer:**  
To automatically delete external guest users 15 days after they lose their last access package assignment, you need to configure the global entitlement management settings in the admin portal.  
Follow these steps using the Microsoft Entra admin center:  
Step 1: Sign in and Navigate: Log in to the Microsoft Entra admin center as at least an Identity Governance Administrator.  
Step 2: Access Governance Settings: In the left navigation menu, expand Identity Governance, then expand Entitlement management, and select Settings (or Control configurations depending on your portal theme updates).  
Step 3: Locate Lifecycle Settings: Look for the Lifecycle of external users card and click Edit (or View settings).  
Step 4: Configure Account Removal: Locate the Remove external user setting and set it to Yes.  
Step 5: Set the Retention Period: In the field labeled Number of days before removing external user from this directory, enter 15.  
Step 6: Save Changes: Click Save at the bottom of the page to apply the policy.

Reference:  
[https://microsoftlearning.github.io/SC-300-Identity-and-Access-Administrator/Instructions/Labs/Lab\\_24\\_ManageTheLifecycleOfExternalUsersInAADIdentityGove rnanceSettings%20.html](https://microsoftlearning.github.io/SC-300-Identity-and-Access-Administrator/Instructions/Labs/Lab_24_ManageTheLifecycleOfExternalUsersInAADIdentityGovernanceSettings%20.html)

NEW QUESTION: 13

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

| Name   |  Microsoft 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 Area**

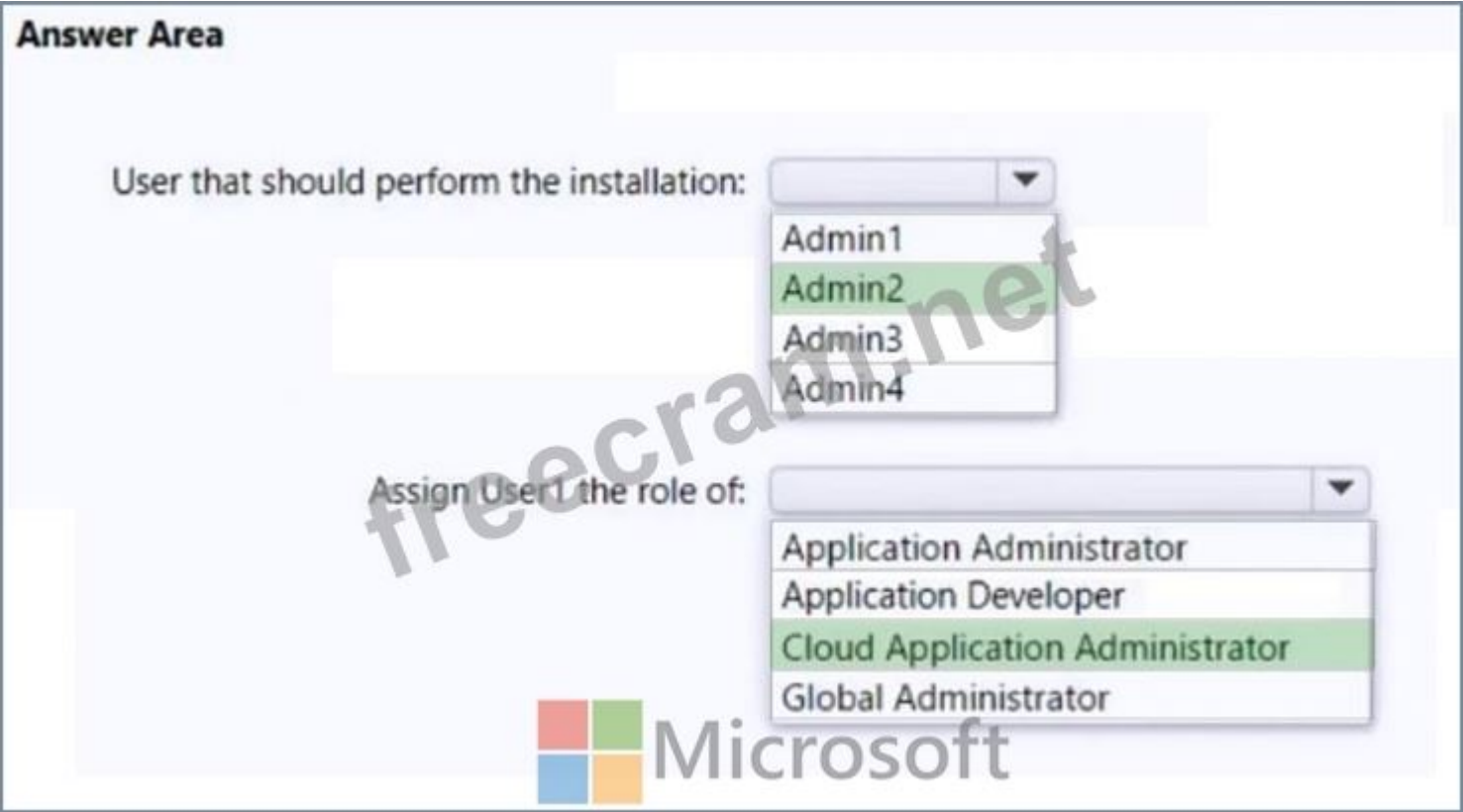
User that should perform the installation:

- Admin1
- Admin2
- Admin3
- Admin4

Assign User1 the role of:

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

**Answer:**



**NEW QUESTION: 14**

Your network contains an on-premises Active Directory Domain Services (AD DS) domain that syncs user accounts with a Microsoft 365 E5 subscription. You need to ensure that on-premises account lockout policies are applied to Microsoft Entra sign- ins. What should you configure?

- A. Microsoft Entra Cloud Sync
- B. Azure Active Directory Seamless Single Sign-on (Azure AD Seamless SSO)
- C. pass-through authentication
- D. password hash synchronization

Answer: (SHOW ANSWER)

**NEW QUESTION: 15**

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

Answer: (SHOW ANSWER)

<https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#clone-a- role>

NEW QUESTION: 16

Drag and Drop Question

You have an Azure subscription that is linked to an Azure AD tenant named contoso.com. The subscription contains a group named Group1 and a virtual machine named VM1.

You need to meet the following requirements:

- Enable a system-assigned managed identity for VM1.
- Add VM1 to Group1.

How should you complete the PowerShell script? To answer, drag the appropriate cmdlets to the correct targets. Each cmdlet 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.

Cmdlets

Get-AzADGroup

Get-AzADServicePrincipal

Get-AzVM

Update-AzADServicePrincipal

Update-AzVM

Answer Area

\$vm =

Cmdlet

-ResourceGroupName myResourceGroup -Name vm1

Update-AzVM -ResourceGroupName myResourceGroup -VM \$vm -IdentityType SystemAssigned

\$displayname =

Cmdlet

-displayname "vm1"

\$group = Get-AzADGroup -searchstring "group1"

Add-AzureADGroupMember -ObjectId \$group.id -RefObjectId \$displayname.id

Answer:

Cmdlets

Get-AzADGroup

Update-AzADServicePrincipal

Update-AzVM

Answer Area

\$vm =

Get-AzVM

-ResourceGroupName myResourceGroup -Name vm1

Update-AzVM -ResourceGroupName myResourceGroup -VM \$vm -IdentityType SystemAssigned

\$displayname =

Get-AzADServicePrincipal

-displayname "vm1"

\$group = Get-AzADGroup -searchstring "group1"

Add-AzureADGroupMember -ObjectId \$group.id -RefObjectId \$displayname.id

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

**NEW QUESTION: 17**

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.** From the Microsoft 365 Defender portal, unsanction Facebook.
- B.** Create a Defender for Cloud Apps access policy.
- C.** Create a Conditional Access policy.
- D.** Create an app configuration policy in Microsoft Intune.

**Answer:** ([SHOW ANSWER](#))

**NEW QUESTION: 18**

Hotspot Question

A user named User1 attempts to sign in to the tenant by entering the following incorrect passwords:

- \* Pa55w0rd12
- \* Pa55w0rd12
- \* Pa55w0rd12
- \* Pa55w.rd12
- \* Pa55w.rd123
- \* Pa55w.rd123
- \* Pa55w.rd123
- \* Pa55word12
- \* Pa55word12
- \* Pa55word12
- \* Pa55w.rd12

You need to identify how many sign-in attempts were tracked for User1, and how User1 can unlock her account before the 300-second lockout duration expires.

What should identify? To answer, select the appropriate

NOTE: Each correct selection is worth one point.

Answer Area

Tracked sign-in attempts:

|    |
|----|
| ▼  |
| 4  |
| 5  |
| 10 |
| 11 |

Unlock by:

|                                                 |
|-------------------------------------------------|
| ▼                                               |
| Clearing the browser cache                      |
| Signing in by using inPrivate browsing mode     |
| Performing a self-service password reset (SSPR) |

Answer:

Answer Area

Tracked sign-in attempts:

|    |
|----|
| ▼  |
| 4  |
| 5  |
| 10 |
| 11 |

Unlock by:

|                                                 |
|-------------------------------------------------|
| ▼                                               |
| Clearing the browser cache                      |
| Signing in by using inPrivate browsing mode     |
| Performing a self-service password reset (SSPR) |

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

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

Answer: (SHOW ANSWER)

NEW QUESTION: 20

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.

You need to ensure that use Modern authentication.

What should you implement?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 21

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

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

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

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

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

Solution: You configure conditional access policies.

Does this meet the goal?

- A. Yes
- B. No

Answer: (SHOW ANSWER)

Azure Active Directory (Azure AD) Pass-through Authentication allows your users to sign into both on-premises and cloud-based applications using the same passwords. It uses a lightweight on-premises agent that listens for and responds to password validation requests. If disabled user can not login.

Reference:

<https://docs.microsoft.com/en-us/answers/questions/3221/disable-account-sync.html>

NEW QUESTION: 22

You have a Microsoft Entra tenant that uses Microsoft Entra ID Protection and contains the users shown in the following table.

| Name  | Role                             |
|-------|----------------------------------|
| User1 | Conditional Access Administrator |
| User2 | Security Administrator           |
| User3 | Authentication Administrator     |

You need to implement a Conditional Access policy that enforces a remediation requirement for risky users.

Which users can create the policy?

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

Answer: (SHOW ANSWER)

Both User1 (Conditional Access Administrator) and User2 (Security Administrator) can create this Conditional Access policy.

User1 (Conditional Access Administrator): This role is explicitly designed with the least-privileged permissions needed to create, manage, and edit Microsoft Entra Conditional Access policies.

User2 (Security Administrator): This role has broad security management permissions in the tenant, which include full capabilities to create and manage Conditional Access policies, as well as handling Microsoft Entra ID Protection risk signals.

Incorrect:

User3 (Authentication Administrator): This role can view, set, and reset authentication method information for non-administrative users. It does not possess the permissions required to create or modify Conditional Access policies.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

NEW QUESTION: 23

Case Study 3 - A Datum Corp

Overview

A Datum Corporation is a consulting company in Montreal. A Datum recently acquired a Vancouver-based company named Litware, Inc.

Existing Environment

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.

| Name  | Role                              |
|-------|-----------------------------------|
| User1 | None                              |
| User2 | None                              |
| User3 | User administrator                |
| User4 | Privileged role administrator     |
| User5 | Identity Governance Administrator |

The tenant contains the groups shown in the following table.

|  Name | Type     | Membership type | Owner | Members                        |
|----------------------------------------------------------------------------------------|----------|-----------------|-------|--------------------------------|
| IT_Group1                                                                              | Security | Assigned        | None  | All users in the IT department |
| AdatumUsers                                                                            | Security | Assigned        | None  | User1, User2                   |

Existing Environment

Litware Environment

Litware has an AD DS forest named litware.com

Existing Environment

Problem Statements

A Datum identifies the following issues:

- Multiple users in the sales department have up to five devices. The sales department users report that sometimes they must contact the support department to join their devices to the Azure AD tenant because they have reached their device limit.
- A recent security incident reveals that several users leaked their credentials, a suspicious browser was used for a sign-in, and resources were accessed from an anonymous IP address.
- When you attempt to assign the Device Administrators role To IT\_Group1, the group does NOT appear in the selection list.
- Anyone in the organization can invite guest users, including other guests and non- administrators.
- The helpdesk spends too much time resetting user passwords.
- Users currently use only passwords for authentication.

Requirements

Planned Changes

A Datum plans to implement the following changes;

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

Requirements

Technical Requirements

A Datum identifies the following technical requirements:

- Users assigned the User administrator role must be able to request permission to use the role when needed for up to one year.
- Users must be prompted to register for MFA and provided with an option to bypass the registration for a grace period.
- Users must provide one authentication method to reset their password by using SSPR.

Available methods must include:

- Email
- Phone
- Security questions

- The Microsoft Authenticator app
- Trust relationships must NOT be established between the adatum.com and litware.com AD DS domains.
- The principle of least privilege must be used.

Drag and Drop Question

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.

Policy Types

An authentication method policy

A Conditional Access policy

A sign-in risk policy

A user risk policy

Answer Area

Microsoft

Leaked credentials:

A sign-in from a suspicious browser:

Resources accessed from an anonymous IP address:

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

Explanation:

Box 1: A user risk policy

User-linked detections include:

Leaked credentials: This risk detection type indicates that the user's valid credentials have been leaked. When cybercriminals compromise valid passwords of legitimate users, they often share those credentials.

User risk policy

Identity Protection can calculate what it believes is normal for a user's behavior and use that to base decisions for their risk. User risk is a calculation of probability that an identity has been compromised. Administrators can make a decision based on this risk score signal to enforce organizational requirements. Administrators can choose to block access, allow access, or allow access but require a password change using Azure AD self-service password reset.

Box 2: A sign-in risk policy

Suspicious browser: Suspicious browser detection indicates anomalous behavior based on suspicious sign-in activity across multiple tenants from different countries in the same browser.

Box 3: A sign-in risk policy

A sign-in risks include activity from anonymous IP address: This detection is discovered by Microsoft Defender for Cloud Apps. This detection identifies that users were active from an IP address that has been identified as an anonymous proxy IP address.

Note: The following three policies are available in Azure AD Identity Protection to protect users and respond to suspicious activity. You can choose to turn the policy enforcement on or off, select users or groups for the policy to apply to, and decide if you want to block access at sign-in or prompt for additional action.

\* User risk policy

Identifies and responds to user accounts that may have compromised credentials. Can prompt the user to create a new password.

\* Sign in risk policy

Identifies and responds to suspicious sign-in attempts. Can prompt the user to provide additional forms of verification using Azure AD Multi-Factor Authentication.

\* MFA registration policy

Makes sure users are registered for Azure AD Multi-Factor Authentication. If a sign-in risk policy prompts for MFA, the user must already be registered for Azure AD Multi-Factor Authentication.

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

**NEW QUESTION: 24**

Hotspot Question

You have a Microsoft 365 subscription.

You configure a Global Secure Access security profile named SecurityProfile1.

You need to create a Conditional Access policy named CAPolicy1 that will use SecurityProfile1.

Which two settings should you configure to ensure that CAPolicy1 uses SecurityProfile1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

[Home](#) > [Conditional Access | Overview](#) >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

CAPolicy1

Microsoft

Assignments

Users

All users

Target resources

No target resources selected

Network

NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

Answer:

Microsoft

Answer Area

Home > Conditional Access | Overview >

New

...

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

CAPolicy1

Assignments

Users

All users

Target resources

No target resources selected

Network

NEW

Not configured

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Session

0 controls selected

**NEW QUESTION: 25**  
You have an Azure Active Directory (Azure AD) tenant that uses Azure AD Identity Protection and contains the resources shown in the following table.

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

Azure Multi-factor Authentication (MFA) is enabled for all users.

User1 triggers a medium severity alert that requires additional investigation.

You need to force User1 to reset his password the next time he signs in. The solution must minimize administrative effort.

What should you do?

**A.** Reconfigure the user risk, policy to trigger on medium or low severity.

**B.** Mark User1 as compromised.

**C.** Reset the Azure MIFA registration for User1.

**D.** Configure a sign-in risk policy.

**Answer:** (SHOW ANSWER)

Scenario: User compromised (True positive)

'Risky users' report shows an at-risk user [Risk state = At risk] with low risk [Risk level = Low] and that user was indeed compromised.

Feedback: Select the user and click on 'Confirm user compromised'.

What happens under the hood? Azure AD will move the user risk to High [Risk state = Confirmed compromised; Risk level = High] and will add a new detection 'Admin confirmed user compromised'.

Notes: Currently, the 'Confirm user compromised' option is only available in 'Risky users' report.

The detection 'Admin confirmed user compromised' is shown in the tab 'Risk detections not linked to a sign-in' in the 'Risky users' report.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-risk-feedback>

**NEW QUESTION: 26**

You have a Microsoft 365 E5 subscription that contains a user named User1.

You need to ensure that User1 can create access reviews for Microsoft Entra roles. The solution must use the principle of least privilege.

Which role should you assign to User1?

**A.** User Access Administrator

**B.** Identity Governance Administrator

**C.** User Administrator

**D.** Privileged Role Administrator

**Answer:** (SHOW ANSWER)

**NEW QUESTION: 27**

Hotspot Question

You have an Azure subscription that contains a resource group named RG1. RG1 contains two virtual machines named VM1 and VM2 that have Microsoft Entra ID login enabled.

The subscription contains the users shown in the following table.

| Name  | Role                                | Role scope   |
|-------|-------------------------------------|--------------|
| User1 | Virtual Machine User Login          | Subscription |
| User2 | Virtual Machine Contributor         | RG1          |
| User3 | Virtual Machine Administrator Login | VM1          |

Which users can sign in to VM1, and which users can sign in to VM2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VM1:

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

VM2:

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

Answer:

Answer Area

VM1:

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

VM2:

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

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

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

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

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

Which type of credentials should you use?

- A.** a system-assigned managed identity
- B.** a user-assigned managed identity
- C.** an Azure Active Directory (Azure AD) user account
- D.** a SQL Server account

**Answer: A** ([LEAVE A REPLY](#))

**NEW QUESTION: 29**

SIMULATION

You need to add Microsoft SharePoint Online as a Conditional Access App Control app in Microsoft Defender for Cloud Apps.

**Answer:**

To add Microsoft SharePoint Online as a Conditional Access App Control app, you must create a Conditional Access policy in the Microsoft Entra admin center that routes traffic to Microsoft Defender for Cloud Apps. Because SharePoint Online is a native Microsoft application, it onboards automatically to Defender for Cloud Apps as soon as a user session triggers the policy for the first time.

Follow these steps to complete the deployment:

Create the Conditional Access Policy in Microsoft Entra

Step 1: Sign in to the Microsoft Entra admin center as a Conditional Access Administrator.

Step 2: Navigate to Identity > Protection > Conditional Access.

Step 3: Select + New policy.

Step 4: Under Assignments, select Users to include your targeted users or groups.

Step 5: Under Target resources, choose Select apps, search for, and select Office 365 SharePoint Online (or Office 365 to include all core suites).

Step 6: Under Conditions > Client apps, set the toggle to Yes, check the Browser box, and click Done. (Session control only applies to interactive browser sessions).

Step 7: Under Access controls > Session, select Use Conditional Access App Control.

Step 8: Choose a policy type from the dropdown, such as Use custom policy (recommended for advanced granular rules) or Monitor only.

Step 9: Set Enable policy to On, and click Create.

Reference:

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

**NEW QUESTION: 30**

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

| Name     | Type              |
|----------|-------------------|
| VM1      | Virtual machine   |
| App1     | Azure App Service |
| Vault1   | Azure Key Vault   |
| storage1 | Storage account   |

You need to grant permissions to the resources by using attribute-based access control (ABAC).

To which resource can you grant permissions?

- A. Vault1
- B. VM1
- C. Storage1
- D. App1

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 31

You have a Microsoft 365 tenant.

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

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

What should you implement?

- A. a conditional access policy in Azure AD
- B. a compliance policy in Microsoft Intune
- C. an OAuth policy in Microsoft Defender for Cloud Apps
- D. an application control profile in Microsoft Intune

**Answer:** ([SHOW ANSWER](#))

<https://learn.microsoft.com/en-gb/entra/identity/conditional-access/howto-conditional-access-policy-block-legacy>

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### NEW QUESTION: 32

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 smartcard
- C. an FIDO2 security token
- D. a Microsoft Teams chat

**Answer:** ([SHOW ANSWER](#))

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone

- Office phone (available only for tenants with paid subscriptions)
  - Security questions
- <https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

**NEW QUESTION: 33**

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

| Name   | Description         |
|--------|---------------------|
| User1  | User account        |
| Group1 | Security group      |
| Group2 | Microsoft 365 group |
| SP1    | Service principal   |

You register an app named App1 in the tenant.

To which identities can you assign the Owner role for App1?

- A. User1 only
- B. User1 and Group1 only
- C. User1 and SP1 only
- D. User1, Group1, and Group2 only
- E. User1, Group1, and SP1 only
- F. User1, Group1, Group2, and SP1

**Answer:** (SHOW ANSWER)

In Microsoft Entra ID, the Owner role for a registered application can be assigned to users [User1] and service principals [SP1]. Groups cannot be assigned as owners of enterprise applications. A user is automatically added as an owner when they register an application, unless they have administrator roles. Service principals, which represent applications, hosted services, or automated tools, can also be owners.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

**NEW QUESTION: 34**

Hotspot Question

You have a Microsoft 365 tenant.

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

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

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

NOTE: Each correct selection is worth one point.

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:

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

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

**NEW QUESTION: 35**

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

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

You have 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

**Answer: B** ([LEAVE A REPLY](#))

Members (self) - Use this option to have the users review their own role assignments. Groups assigned to the role will not be a part of the review when this option is selected. This option is only available if the review is scoped to Users and Groups.

Also Megan Brow still there as Fallback Reviewer so will still receiving reviews.

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

#### NEW QUESTION: 36

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 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 Licenses blade in the Azure Active Directory admin center

**B.** the Set-WindowsProductKey cmdlet

**C.** the Update-MgGroup cmdlet

**D.** the Administrative units blade in the Azure Active Directory admin center

**Answer: (**[SHOW ANSWER](#)**)**

#### NEW QUESTION: 37

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

**Answer: (**[SHOW ANSWER](#)**)**

On the My Apps portal, applications appear in default collections and your custom app collections. The Apps collection in My Apps is a default collection that contains all the applications that have been assigned to you, sorted alphabetically.

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

#### NEW QUESTION: 38

Due to a recent company acquisition, you have inherited a new Azure tenant with 1 subscription associated that you have the manage. The security has been neglected and you are looking for a quick and easy way to enable various security settings like requiring users to Register for Multi- factor authentication, blocking legacy authentication protocols, and protecting privileged activities like access to the Azure portal. What is the best way to enforce these settings with the least amount of administrative effort.

**A.** Enable Security Defaults

**B.** Configure Conditional Access Policies

- C. Configuring an Azure Policy
- D. Utilize Active Directory Sign-In Logs

Answer: (SHOW ANSWER)

As enabling security defaults would fulfill all of your requirements and enabling security defaults requires very little administrative effort.

Reference:

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

NEW QUESTION: 39

You have a Microsoft Entra tenant that contains an access package named Package1 and a user named User1. Package1 is configured as shown in the following exhibit.

\* BasicsResource roles\* RequestsRequestor information\*LifecycleCustom extensionsReview + create

Expiration

Access package assignments expire ⓘ

On dateNumber of daysNumber of hoursNever

Assignments expire after (number of days) \*

365

Users can request specific timeline \* ⓘ

YesNo

Show advanced expiration settings

Access Reviews

Require access reviews \*

YesNo

Starting on ⓘ

25/01/2024

Review frequency ⓘ

AnnuallyBi-annuallyQuarterlyMonthlyWeekly

Duration (in days) \* ⓘ

90

Maximum 175

Reviewers ⓘ

☒ Self-review

☐ Specific reviewer(s)

☐ Manager

Show advanced access review settings

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. Privileged Role Administrator
- B. External Identity Provider Administrator
- C. Identity Governance Administrator
- D. Security Administrator

Answer: (SHOW ANSWER)

Correct:

\* Identity Governance Administrator

\* User administrator

Check catalog for resources

If you need to add resources to an access package, you should check whether the resources you need are available in the access package's catalog. If you're an access package manager, you can't add resources to a catalog, even if you own them. You're restricted to using the resources available in the catalog.

Prerequisite role: Global administrator, Identity Governance administrator, User administrator, Catalog owner, or Access package manager.

In the Azure portal, select Azure Active Directory and then select Identity Governance.

In the left menu, select Catalog and then open the catalog.

In the left menu, select Resources to see the list of resources in this catalog.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-resources>

#### NEW QUESTION: 40

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

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

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

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

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

Solution: You configure Azure AD Password Protection.

Does this meet the goal?

**A.** Yes

**B.** No

**Answer:** (SHOW ANSWER)

Azure AD Password Protection

With this feature, you can use the same checks for passwords in AzureAD on your on-premises Active Directory implementation.

You can enforce both the Microsoft Global Banned Passwords and Custom banned-passwords list stored in Azure AD tenant.

The DC agent software must be installed on all DCs in a domain.

#### NEW QUESTION: 41

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 Group1.
- Add User1 and User2 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: Security

Membership type: Dynamic User

**B.** Group type: Microsoft 365  
Membership type: Dynamic User

**C.** Group type: Security  
Membership type: Assigned

**D.** Group type: Microsoft 365  
Membership type: Assigned

**E.** Group type: Security  
Membership type: Dynamic Device

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 42

Your network contains an on-premises Active Directory Domains Services (AD DS) domain named contoso.com and a web app named WebApp1. WebApp1 uses Integrated Windows authentication.

Remote users access WebApp1 by establishing a VPN connection to the on-premises network and using a URL of https://webapp1.contoso.com.

You have a Microsoft Entra tenant that syncs with contoso.com.

You perform the following actions:

- Deploy Microsoft Entra Private Access.

- Configure a connector group that contains a connector named Connector1.

You need to ensure that the remote users can access WebApp1 by using Microsoft Entra Private Access.

What should you do?

**A.** Enroll the remote users' devices in Microsoft Defender for Endpoint.

**B.** Deploy Microsoft Entra Internet Access.

**C.** Create a Conditional Access policy.

**D.** Create an application segment.

**Answer:** ([SHOW ANSWER](#))

To allow remote users to access the web app seamlessly using Microsoft Entra Private Access, you must explicitly publish the application as an Enterprise Application segment and ensure that Kerberos-based Integrated Windows Authentication (IWA) operates correctly through Single Sign-On (SSO).

Define the Application Segment

1. You must publish the web application within the Microsoft Entra admin center:Go to Global Secure Access (Preview) > Applications > Enterprise applications.

2. Add a new application and choose Microsoft Entra Private Access.

3. Assign the existing connector group (which holds Connector1) to this new application segment.

4. Configure the Application Segment destination targeting the specific internal URL:

mywebapp.contoso.com and its required web ports (typically port 80 or 443).

Reference:

<https://charbelnemnom.com/evaluate-microsoft-entra-private-access/>

#### NEW QUESTION: 43

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.** Configure password protection for the Azure AD tenant.

- B. Disable Security defaults.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Disable the User consent settings.

Answer: (SHOW ANSWER)

NEW QUESTION: 44

Hotspot Question

You have a Microsoft 365 E5 subscription that contains two attribute sets named Set1 and Set2. The subscription contains the users shown in the following table.

| Name  | Role                               |
|-------|------------------------------------|
| User1 | Global Administrator               |
| User2 | Global Administrator               |
| User3 | Attribute Assignment Administrator |

You have the custom security attributes shown in the following table.

| Name    | Attribute set |
|---------|---------------|
| Secure1 | Set1          |
| Secure2 | Set1          |
| Secure3 | Set2          |

You assign User2 the Attribute Definition Administrator role for Set1. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1 can modify the configuration of Secure1.

☐

☐

User2 can view the value of Secure2 for all users.

☐

☐

User3 can view the value of Secure3 for all users.

☐

☐

Answer:

Statements

User1 can modify the configuration of Secure1.

Yes

☐

No

☒

User2 can view the value of Secure2 for all users.

☐☒

User3 can view the value of Secure3 for all users.

☒☐

Explanation:

Box 1: No

User1 is Global Administrator.

By default, Global Administrator and other administrator roles do not have permissions to read, define, or assign custom security attributes.

Note: The roles that apply to configuration sets are:

Attribute Definition Administrator

Attribute Assignment Administrator

Attribute Definition Reader

Attribute Assignment Reader

Box 2: No

User2 is Attribute Definition Administrator.

Attribute Definition Administrator

Users with this role can define a valid set of custom security attributes that can be assigned to supported Microsoft Entra objects. This role can also activate and deactivate custom security attributes.

Box 3: Yes

User3 is Attribute assignment Administrator.

Attribute Assignment Administrator

Users with this role can assign and remove custom security attribute keys and values for supported Microsoft Entra objects such as users, service principals, and devices.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference>

NEW QUESTION: 45

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.

**Answer:** ([SHOW ANSWER](#))

Monitor sign-in and audit logs

Organizations should monitor sign-in and audit log activity from the emergency accounts and trigger notifications to other administrators.

When you monitor the activity on break glass accounts, you can verify these accounts are only used for testing or actual emergencies.

You can use Azure Log Analytics to monitor the sign-in logs and trigger email and SMS alerts to your admins whenever break glass accounts sign in.

## **NEW QUESTION: 46**

### **SIMULATION**

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

You need to lock out accounts for five minutes when they have 10 failed sign-in attempts.

To complete this task, sign in to the appropriate admin center.

**Answer:**

Protect user accounts from attacks with Microsoft Entra smart lockout

Manage Microsoft Entra smart lockout values

Based on your organizational requirements, you can customize the Microsoft Entra smart lockout values.

To check or modify the smart lockout values for your organization, complete the following steps:

Step 1: Sign in to the Microsoft Entra admin center as at least an Authentication Administrator.

Step 2: Browse to Protection > Authentication methods > Password protection.

Step 3: Set the Lockout threshold, based on how many failed sign-ins are allowed on an account before its first lockout.

Step 4: The default is 10 for Azure Public tenants and 3 for Azure US Government tenants. [Specify: 10]

Step 5: Set the Lockout duration in seconds, to the length in seconds of each lockout. [Specify 300 seconds]

The default is 60 seconds (one minute).

Microsoft Entra admin center

Search resources, services, and docs (G+)

Home > Authentication methods

### Authentication methods | Password protection

Contoso - Microsoft Entra ID Security

Search Save Discard Got feedback?

**Manage**

- Policies
- Password protection**
- Registration campaign
- Authentication strengths
- Settings

**Monitoring**

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

**Custom smart lockout**

Lockout threshold 10

Lockout duration in seconds 60

**Custom banned passwords**

Enforce custom list Yes No

Custom banned password list

- contoso
- fabrikam
- tailwind
- michigan
- wolverine
- harbaugh
- howard

**Password protection for Windows Server Active Directory**

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit



**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### NEW QUESTION: 47

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.

**Answer:** ([SHOW ANSWER](#))

Creating a Sentinel instance and configuring the Azure AD Connector = configuring the Azure AD connector within Sentinel settings, as detailed here: <https://learn.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

#### NEW QUESTION: 48

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

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

What should you do in Azure AD Connect?

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

**Answer:** ([SHOW ANSWER](#))

You create an inbound rule because information is taken from Active Directory to Metaverse object.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-configure-filtering#negative-filtering-do-not-sync-these>

#### NEW QUESTION: 49

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.  
**Answer: (SHOW ANSWER)**  
**C.** Add a WS-Fed identity provider.  
<https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>  
**D.** Create a guest user account in contoso.com.

**NEW QUESTION: 50**

**SIMULATION**

You need to ensure that only users from the fabrikam.com domain can be invited to your Microsoft Entra tenant.

**Answer:**

To restrict external invitations to a specific domain, you must configure the Collaboration restrictions allowlist within the Microsoft Entra admin center.  
Step 1: Sign in to the Microsoft Entra admin center using an account with at least Global Administrator privileges.  
Step 2: Navigate through the left-hand sidebar menu: Identity > External Identities > External collaboration settings.  
Step 3: Scroll down to locate the Collaboration restrictions section near the bottom of the page.  
Step 4: Select the radio button labeled "Allow invitations only to the specified domains (most restrictive)".  
Step 5: Target the domain: Under the Target domains input field, type the exact domain name you want to allow. [Enter fabrikam.com] Note: If you need to include multiple domains, type each one on a new line.  
Step 6: Apply changes by clicking the Save button at either the top or bottom of the page.  
Reference:  
<https://learn.microsoft.com/en-us/entra/external-id/allow-deny-list>

**NEW QUESTION: 51**

You have a Microsoft Entra tenant that uses Microsoft Entra ID Premium licenses.  
You plan to configure a terms of use (ToU) for the tenant.  
You need to upload the ToU document.  
Which format should you use for the document?

- A.** HTML
- B.** RTF
- C.** PDF Most Voted
- D.** DOCX

**Answer: (SHOW ANSWER)**  
<https://learn.microsoft.com/en-us/entra/identity/conditional-access/terms-of-use>

**NEW QUESTION: 52**

Hotspot Question  
You have two Microsoft Entra tenants named contoso.com and fabrikam.com. Contoso.com contains the users shown in the following table.

| Name  | Department | Job title  | City      | Member of |
|-------|------------|------------|-----------|-----------|
| User1 | IT         | Support    | Vancouver | Group1    |
| User2 | IT         | Technician | Madrid    | None      |
| User3 | HR         | Consultant | Montreal  | Group1    |

You configure cross-tenant synchronization from contoso.com to fabrikam.com by using the following settings:

- Users and groups: Group1
- Provisioning Mode: Automatic
- Attribute Mappings
- Source Object Scope: Filter1, Filter2

Filter1 is configured as shown in the following table.

| Source attribute | Operator | Clause value          |
|------------------|----------|-----------------------|
| department       | EQUALS   | IT                    |
| jobTitle         | PRESENT  | <i>Not applicable</i> |

Filter2 is configured as shown in the following table.

| Source attribute | Operator | Clause value |
|------------------|----------|--------------|
| city             | INCLUDES | M            |

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yes

No

User1 syncs to fabrikam.com.

☐

☐

User2 syncs to fabrikam.com.

☐

☐

User3 syncs to fabrikam.com.

☐

☐

Answer:

Answer Area

Statements

Yes

No

User1 syncs to fabrikam.com.

☐

☒

User2 syncs to fabrikam.com.

☒

☐

User3 syncs to fabrikam.com.

☐

☒

Explanation:

Box 1: No

User1 is in IT department and has the job title support. Filter1 matches.

User1 is in city Vancouner, which does not have a letter M. Filter2 does not match.

User1 is not synced.

Note:

Both filter must match.

Filter1 matches if department is IT, and there is jobTitle value.

Filter2 matches any city that has the letter M in it.

In Microsoft Entra Connect Sync, the "PRESENT" operator in scoping filters specifies that the attribute must exist with any value, even if it's empty or null. This is different from EQUALS, which requires a specific value, or NOT EQUALS, which excludes a specific value. The PRESENT operator is used to ensure that an attribute exists in the object being synchronized, regardless of its actual value.

Box 2: Yes

User2 is in IT department and has the job title technician. Filter1 matches.

User2 is in city Madrid, which does not have a letter M. Filter2 matches.

User2 syncs.

Box 3: No

User3 is in HR department, so Filter1 will not match.

User3 will not sync.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering>

NEW QUESTION: 53

Hotspot Question

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

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

The users have the devices shown in the following table.

| Name    | Platform   | Azure AD join type  |
|---------|------------|---------------------|
| Device1 | Windows 11 | None                |
| Device2 | Windows 10 | Azure AD joined     |
| Device3 | Android    | Azure AD registered |

You create the following two Conditional Access policies:

- Name: CAPolicy1
  - Assignments
    - o Users or workload identities: Group1
    - o Cloud apps or actions: Office 365 SharePoint Online
    - o Conditions
- Filter for devices: Exclude filtered devices from the policy
- Rule syntax: device.displayName -startsWith device?
- o Access controls
- Grant: Block access
- Session: 0 controls selected
- o Enable policy: On
- Name: CAPolicy2
- Assignments
  - o Users or workload identities: Group2
  - o Cloud apps or actions: Office 365 SharePoint Online

o Conditions: 0 conditions selected

- Access controls

o Grant: Grant access  
Require multifactor authentication

o Session: 0 controls selected

- Enable policy: On

All users confirm that they can successfully authenticate using MFA.

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

NOTE: Each correct selection is worth one point.

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

Answer:

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

NEW QUESTION: 54

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3 and a Microsoft SharePoint Online site named Site1. The subscription contains the devices shown in the following table.

| Name    | Azure AD   | Compliance     |
|---------|------------|----------------|
| Device1 | Joined     | Noncompliant   |
| Device2 | Registered | Compliant      |
| Device3 | None       | Not applicable |

The users sign in to the devices as shown in the following table.

| User  | Device  |
|-------|---------|
| User1 | Device1 |
| User2 | Device2 |
| User3 | Device3 |

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

- Name: CA1
- Assignments
  - o Users and groups: User1, User2, User3
  - o Cloud apps or actions: SharePoint - Site1
- Access controls
  - o Session: Use app enforced restrictions

From the SharePoint admin center, you configure Access control for unmanaged devices to allow limited, web-only access.

Which users will have full access to Site1?

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

**Answer: A** ([LEAVE A REPLY](#))

<https://learn.microsoft.com/en-us/microsoft-365/business-premium/m365bp-managed-unmanaged-devices?view=o365-worldwide&tabs=Managed>

**NEW QUESTION: 55**

You work for a company named Contoso, Ltd. that has a Microsoft Entra tenant named contoso.com.

Contoso is working on a project with the following two partner companies:

- A company named A. Datum Corporation that has a Microsoft Entra tenant named adatum.com.
- A company named Fabrikam, Inc. that has a Microsoft Entra tenant named fabrikam.com.

When you attempt to invite a new guest user from adatum.com to contoso.com, you receive an error message.

You can successfully invite a new guest user from fabnkam.com to contoso.com.

You need to be able to invite new guest users from adatum.com to contoso.com.

What should you configure?

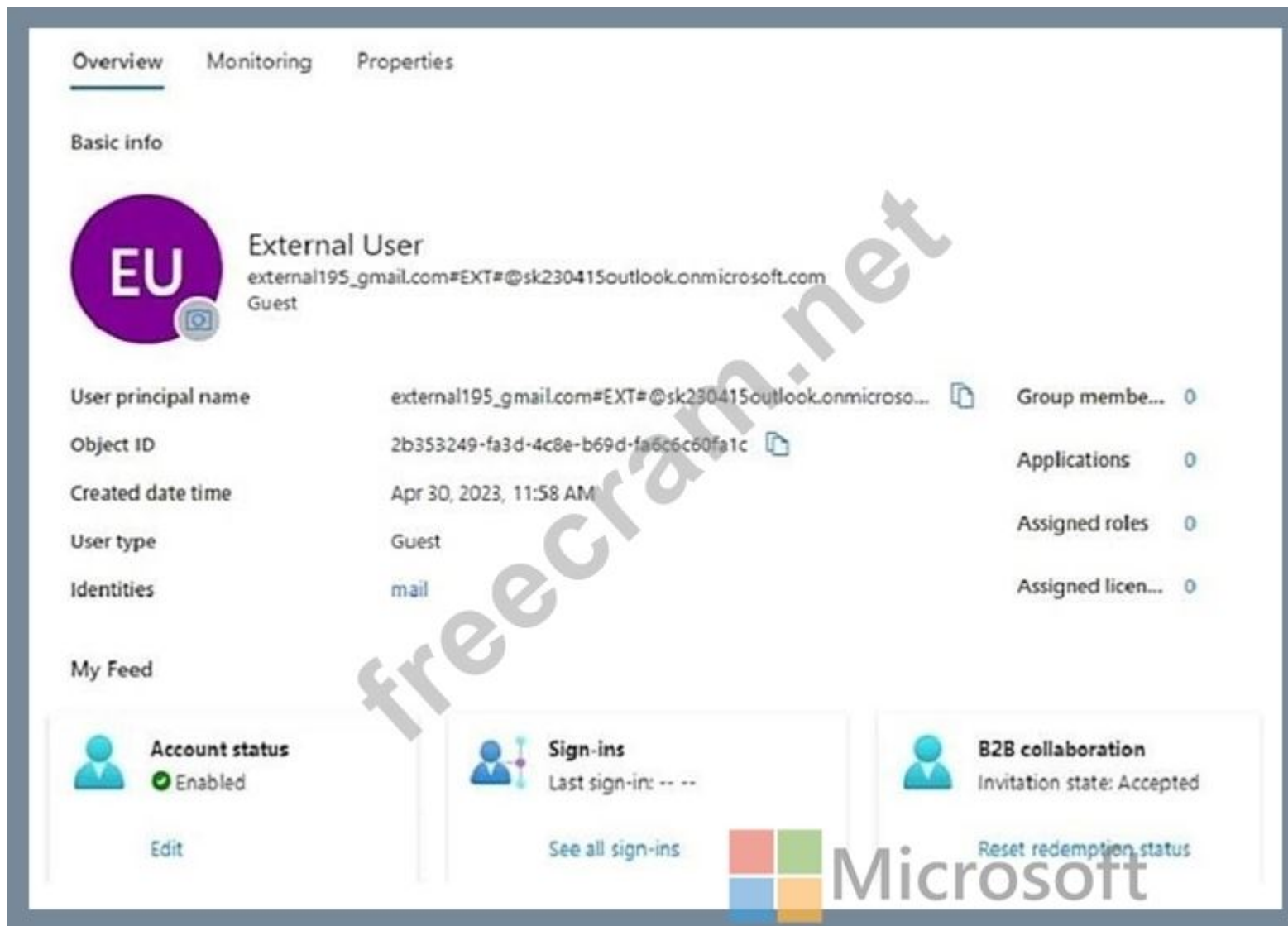
- A.** Guest invite settings
- B.** Verifiable credentials
- C.** Named locations
- D.** Collaboration restrictions

**Answer: (SHOW ANSWER)**

You need to add adatum.com to the list of domains on External Identities >> External Collab Settings >> Collaboration Restrictions >> Allow invitations only to the specified domains.

**NEW QUESTION: 56**

You have an Azure AD tenant that contains the external user shown in the following exhibit.



You update the email address of the user.

You need to ensure that the user can authenticate by using the updated email address.

What should you do for the user?

**A.** Modify the Authentication methods settings.

**B.** Reset the password.

**C.** Revoke the active sessions.

**D.** Reset the redemption status.

**Answer: D (LEAVE A REPLY)**

<https://learn.microsoft.com/en-us/entra/external-id/reset-redemption-status> Update the guest user's sign-in information after they've redeemed your invitation for B2B collaboration. There might be times when you'll need to update their sign-in information, for example when:

- The user wants to sign in using a different email and identity provider
- etc

To manage these scenarios previously, you had to manually delete the guest user's account from your directory and reinvite the user. Now you can use the Microsoft Entra admin center, PowerShell or the Microsoft Graph invitation API to reset the user's redemption status and reinvite the user while keeping the user's object ID, group memberships, and app assignments.

#### NEW QUESTION: 57

##### SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 999999999

You need to ensure the owner of each Microsoft 365 group is notified to renew their group every

180 days. Groups that are NOT renewed must be deleted. For groups without an owner, the notifications must be sent to Allan Deyoung.

To complete this task, sign in to the appropriate admin center.

**Answer:**

Microsoft 365 group expiration policy

With the increase in usage of Microsoft 365 groups and Microsoft Teams, administrators and users need a way to clean up unused groups and teams. A Microsoft 365 groups expiration policy can help remove inactive groups from the system and make things cleaner.

How to set the expiration policy

As noted above, expiry is turned off by default. An administrator will have to enable the expiration policy and set the properties for it to take effect.

Step 1: To enable it, go to Microsoft Entra ID > Groups > Expiration. Here you can set the default group lifetime.

Step 2: Set Group lifetime (in days) to 180

Save Discard

Renewal notifications are emailed to group owners 30 days, 15 days, and one day prior to group expiration. Group owners must have Exchange licenses to receive notification emails. If a group is not renewed, it is deleted along with its associated content from sources such as Outlook, SharePoint, Teams, and PowerBI.

\* Group lifetime (in days) 180

\* Email contact for groups with no owners admin@contoso.com

Enable expiration for these Office 365 groups All Selected None

Select Office 365 groups >

BD Business Development ...

Step 3: Set Email contact for groups with no owners: Allan Deyoung

Step 4: Set Enable expiration for these Office 365 groups: All

Step 5: Click Save

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-groups-expiration-policy>

**NEW QUESTION: 58**

You have a Microsoft 365 E5 subscription.

You plan to deploy a third-party software as a service (SaaS) app named App1.

You need to onboard App1 to Microsoft Defender for Cloud Apps. The solution must ensure that you can implement session control policies.

What should you do first?

- A. From the Microsoft Entra admin center, configure a traffic forwarding profile.
- B. From the Microsoft Defender portal, configure Cloud discovery.
- C. From the Microsoft Defender portal, create an OAuth app policy.
- D. From the Microsoft Entra admin center, configure single sign-on (SSO) for App1.

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 59

##### SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

You need to ensure that when users in the sg-Operations group go to the My Apps portal, a tab named Operations appears that contains only the following applications:

- LinkedIn

- Box

To complete this task, sign in to the appropriate admin center.

**Answer:**

Deploy conditional access app control for catalog apps with Microsoft Entra ID

Access and session controls in Microsoft Defender for Cloud Apps work with applications from the Cloud app catalog and with custom applications.

Configure the Microsoft Entra ID integration

Use the following steps to create a Microsoft Entra Conditional Access policy that routes app sessions to Defender for Cloud Apps.

Step 1: In Microsoft Entra ID, browse to Security > Conditional Access.

Step 2: On the Conditional Access pane, in the toolbar at the top, select New policy -> Create new policy.

Step 3: On the New pane, in the Name textbox, enter the policy name.

Step 4: Under Assignments, select Users or workload identities and assign the users and groups that will be onboarding (initial sign-on and verification) the app. [Select the sg-Operations group]

Step 5: Under Assignments, select Cloud apps or actions and assign the apps and actions you want to control with conditional access app control. [Select the My Apps portal app]

Step 6: Under Access controls, select Session, select Use Conditional Access App Control, and choose a built-in policy (Monitor only (Preview) or Block downloads (Preview)) or Use custom policy to set an advanced policy in Defender for Cloud

Apps, and then select Select. [Select Use custom policy]

Home > Security > Conditional Access >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

Test: Route JIRA to Microsoft Defender

Assignments

Users or workload identities

Specific users included

Cloud apps or actions

1 app included

Conditions

0 conditions selected

Access controls

Grant

0 controls selected

Enable policy

Report-only On Off

Create

Session

Control access based on session controls to enable limited experiences within specific cloud applications.  
[Learn more](#)

☐ Use app enforced restrictions

☒ Use Conditional Access App Control

Monitor only (Preview)

Monitor only (Preview)

Block downloads (Preview)

Use custom policy...

☐ Sign-in frequency

☐ Persistent browser session

☐ Customize continuous access evaluation

☐ Disable resilience defaults

Select

Step 7: Add conditions and grant controls as required.

Step 7a: Configure the Custom policy so that it satisfies the question (Details omitted)

Question: A tab named Operations appears that contains only the following applications: LinkedIn, Box

Step 8: Set Enable policy to On and then select Create.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policies>

NEW QUESTION: 60

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

| Name  | Usage location | Department | Job title |
|-------|----------------|------------|-----------|
| User1 | United States  | Sales      | Associate |
| User2 | Finland        | Sales      | SalesRep  |
| User3 | Australia      | Sales      | Manager   |

You create a dynamic user group and configure the following rule syntax.

user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle - eq "Manager") -or (user. jobTitle -eq "SalesRep") Which users will be added to the group?

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

Answer: A (LEAVE A REPLY)

user.usageLocation -in ["US","AU"] == User 1 & User 3  
-and (user.department -eq "Sales") == User 1 & User 3  
-and -not (user.jobTitle -eq "Manager") == User 1  
-or (user. jobTitle -eq "SalesRep")

NEW QUESTION: 61

You have an on-premises app named App1.

You have a Microsoft Entra tenant.

You plan to publish App1 by using Microsoft Entra Private Access.

You need to enable the Private access profile.

Which blade should you use in the Microsoft Entra admin center?

- A. Remote networks
- B. Traffic forwarding
- C. Security profiles
- D. Connectors

Answer: (SHOW ANSWER)

Enable the Private Access traffic forwarding profile

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 62

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

| Name   | Role                                |
|--------|-------------------------------------|
| Admin1 | Global Administrator                |
| Admin2 | Conditional Access Administrator    |
| Admin3 | Authentication Policy Administrator |
| Admin4 | Global Administrator                |

Admin4 creates a Conditional Access policy named Policy1 by using the Require multifactor authentication for Azure management template.

Which users will be required to use multi-factor authentication (MFA) the next time they sign in?

- A. Admin1 and Admin4 only
- B. Admin2 and Admin3 only
- C. Admin1, Admin2, and Admin3 only
- D. Admin1, Admin2, Admin3, and Admin4

Answer: (SHOW ANSWER)

NEW QUESTION: 63

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint Online site named Site1.

You need to be notified if a user downloads more than 50 files in one minute from Site1.

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

- A. session policy
- B. activity policy
- C. file policy
- D. anomaly detection policy

Answer: B (LEAVE A REPLY)

<https://learn.microsoft.com/en-us/defender-cloud-apps/user-activity-policies>

NEW QUESTION: 64

You have a Microsoft Entra tenant named contoso.com that contains an 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-MgUser cmdlet.
- B. Run the New-MgInvitation cmdlet.
- C. Configure the External collaboration settings.
- D. Implement Microsoft Entra Connect sync.

Answer: (SHOW ANSWER)

The New-MgInvitation cmdlet is used to invite external users (guests) to your Microsoft Entra tenant. This process enables external users to access your organization's resources using their existing credentials, such as an Outlook.com account.

Reference:

<https://learn.microsoft.com/en-us/entra/external-id/tutorial-bulk-invite>

NEW QUESTION: 65

Drag and Drop Question

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

You register the name contoso.com with a domain registrar.  
You need to use contoso.com as the default domain name for new Microsoft 365 users.  
Which four actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Delete the contoso.ommicrosoft.com domain.

Add a custom domain name of contoso.com.

Set the domain to primary.

Create a new TXT record in DNS.

Successfully verify the domain name.

Answer:

Actions

Delete the contoso.ommicrosoft.com domain.

Answer Area

Add a custom domain name of contoso.com.

Create a new TXT record in DNS.

Successfully verify the domain name.

Set the domain to primary.

Explanation:  
<https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide>

**NEW QUESTION: 66**

You have a Microsoft 365 tenant.  
In Azure Active Directory (Azure AD), you configure the terms of use.  
You need to ensure that only users who accept the terms of use can access the resources in the tenant.  
Other users must be denied access.

What should you configure?

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

**Answer:** (SHOW ANSWER)

To configure Condition Access Terms of Use, at: Azure AD Conditional Access - Policies - Policy Name - Grant - myToUname - Terms Of Use Policy (Create the ToU settings first)  
<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use>

NEW QUESTION: 67

Hotspot Question

You have a Microsoft 365 E5 subscription that contains three groups named Group1, Group2, and Group3, and the users shown in the following table.

| Name  | Role                 | Member of      |
|-------|----------------------|----------------|
| User1 | Global Administrator | Group1         |
| User2 | None                 | Group2         |
| User3 | Global Reader        | Group2, Group3 |

You create a Conditional Access policy named CA1 that has the following settings:

- Users
  - Users and groups: Group1
- Exclude
  - Users and groups: Group2
  - Directory roles: Global Administrator
- Target resources
  - Include: All cloud apps
- Access controls
  - Grant: Require multifactor authentication

You create a Conditional Access policy named CA2 that has the following settings:

- Users
  - Users and groups: Group2
- Exclude
  - Users and groups: Group3
- Target resources
  - Include: All cloud apps
- Access controls
  - Grant: Block access

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements                                                                                                         | Yes                   | No                    |
|--------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online. | <input type="radio"/> | <input type="radio"/> |
| User2 will be prevented from signing in to Microsoft SharePoint Online.                                            | <input type="radio"/> | <input type="radio"/> |
| User3 will be prevented from signing in to Microsoft SharePoint Online.                                            | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                                                                         | Yes                              | No                               |
|--------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be prompted for multifactor authentication (MFA) when the user signs in to Microsoft SharePoint Online. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 will be prevented from signing in to Microsoft SharePoint Online.                                            | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 will be prevented from signing in to Microsoft SharePoint Online.                                            | <input type="radio"/>            | <input checked="" type="radio"/> |

Explanation:

Box 1: No

User1 is Global Administrator.

User1 is member of Group1.

CA1 includes Group1.

CA1 excludes Global Administrators.

The exclusion takes precedence.

CA1 will not be applied to User1.

CA2 does not apply to User1 or Group1, only to Group2 and Group3.

User1 will NOT be prompted for multifactor authentication (MFA).

Note: In Azure Conditional Access policies, exclusion takes precedence over inclusion. This means that if a user is a member of both an included group and an excluded group, the exclusion policy will apply, denying them access or requiring different conditions.

Note 2: When no Azure Conditional Access policies are matched for a user, the user is granted access to the resource without any additional access controls or authentication requirements.

Essentially, it's treated as a normal sign-in. Conditional Access policies don't have a default deny policy, meaning if no policy applies, the user's access is not restricted.

Box 2: Yes

User2 has no role.

User2 is member of Group2.

CA1 excludes Group2.

CA1 will not be applied to User2.

CA2 includes Group2.

CA2 block access to all cloud apps.

CA2 will block access for user to Microsoft SharePoint Online.

Box 3: No

(User3 is Global Reader.)

User3 is member of Group2 and Group3.

CA1 excludes Group2.

CA1 will not be applied to User3.

CA2 includes Group2, and excluded Group3.

The exclusion takes precedence.

CA2 will not be applied to User3.

No Conditional Access policy will be applied to User3.

User3 will not be prevented from signing in to Microsoft SharePoint Online.

Reference:  
https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access- users-groups  
https://learn.microsoft.com/en-us/answers/questions/1004659/how-multiple-conditional-access- policies-are-appli

NEW QUESTION: 68

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 Microsoft Entra admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all 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 Set-WindowsProductKey cmdlet
- B. the Update-MgGroup cmdlet
- C. the Set-MgUserLicense cmdlet
- D. the Update-MgUser cmdlet

Answer: C (LEAVE A REPLY)

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the Set-MgUserLicense cmdlet. This cmdlet allows you to modify the licenses assigned to a user. By using this cmdlet, you can remove the Office 365 Enterprise E3 licenses from all users who are part of the group where you assigned the Office 365 Enterprise E5 licenses.

NEW QUESTION: 69

Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. Contoso.com contains the identities shown in the following table.

| Name   | Type  | Member of | In organizational unit (OU) |
|--------|-------|-----------|-----------------------------|
| User1  | User  | Group1    | OU1                         |
| User2  | User  | Group2    | OU2                         |
| Group1 | Group | None      | OU1                         |
| Group2 | Group | Group1    | OU1                         |

You have a Microsoft Entra tenant that contains a user named User1. You deploy Microsoft Entra Cloud Sync and configure a scoping filter by using the following string: CN=Group1,OU=OU1,DC=contoso,DC=com.

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements                                           | Yes                   | No                    |
|------------------------------------------------------|-----------------------|-----------------------|
| Contoso\User1 syncs from contoso.com to the tenant   | <input type="radio"/> | <input type="radio"/> |
| Contoso\User2 syncs from contoso.com to the tenant.  | <input type="radio"/> | <input type="radio"/> |
| Contoso\Group1 syncs from contoso.com to the tenant. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Answer Area                                                                       |                                  |                                  |
|-----------------------------------------------------------------------------------|----------------------------------|----------------------------------|
|  |                                  |                                  |
| Statements                                                                        | Yes                              | No                               |
| Contoso\User1 syncs from contoso.com to the tenant                                | <input checked="" type="radio"/> | <input type="radio"/>            |
| Contoso\User2 syncs from contoso.com to the tenant.                               | <input type="radio"/>            | <input checked="" type="radio"/> |
| Contoso\Group1 syncs from contoso.com to the tenant.                              | <input checked="" type="radio"/> | <input type="radio"/>            |

Explanation:

Box 1: Yes

User1 is in Group1.

User1 is in OU1.

Note:

The filter is for Group1 and OU1.

Box 2: No

User2 is in OU2.

User2 is in Group2.

Group2 is in OU1.

Group2 is a member of Group1.

Box 3: Yes

Group1 is in OU1.

Note: You can use multiple filtering options at the same time. For example, you can use OU- based filtering to only include objects in one OU. At the same time, you can use attribute-based filtering to filter the objects further. When you use multiple filtering methods, the filters use a logical "AND" between the filters.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-sync-configure-filtering>

NEW QUESTION: 70

You have an Azure AD tenant that contains a user named User1 and a Microsoft 365 group named Group1. User1 is the owner of Group1.

You need to ensure that User1 is notified every three months to validate the guest membership of Group1.

What should you do?

- A. Configure the External collaboration settings.
- B. Create an access review.
- C. Configure an access package.
- D. Create a group expiration policy.

Answer: (SHOW ANSWER)

An access review is a process that allows you to review and manage the access of users and groups to resources. You can use access reviews to validate the guest membership of Group1 every three months.

NEW QUESTION: 71

Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain. The domain contains 500 Windows 11 devices.

You have a Microsoft 365 subscription that syncs with the domain.  
You create a Conditional Access policy named Policy1.  
You need to meet the following requirements:

- Apply Policy1 to all the Windows devices.
- Assess the compliance of the Windows devices with Policy1.

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

Answer Area

Apply Policy1 to all the Windows devices:

Microsoft

Microsoft Entra hybrid join the devices to the subscription.

Microsoft Entra join the devices to the subscription.

Microsoft Entra register the devices to the subscription.

Assess the compliance of the Windows devices with Policy1:

Enroll the devices in Microsoft Intune.

Onboard the devices to Microsoft Defender for Endpoint.

Onboard the devices to Microsoft Purview.

Answer:

Answer Area

Apply Policy1 to all the Windows devices:

Microsoft

Microsoft Entra hybrid join the devices to the subscription.

Microsoft Entra join the devices to the subscription.

Microsoft Entra register the devices to the subscription.

Assess the compliance of the Windows devices with Policy1:

Enroll the devices in Microsoft Intune.

Onboard the devices to Microsoft Defender for Endpoint.

Onboard the devices to Microsoft Purview.

NEW QUESTION: 72

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

| Name  | Role                 |
|-------|----------------------|
| User1 | Global Administrator |
| User2 | User Administrator   |
| User3 | Groups Administrator |
| User4 | None                 |

From the tenant, you configure a naming policy for groups.

Which users are affected by the naming policy?

- A. User2 only
- B. User3only
- C. User2 and User3 only
- D. User3 and User4 only
- E. User1, User2, and User3 only
- F. User1, User2, User3, and User4

Answer: (SHOW ANSWER)

Naming policy doesn't apply to certain directory roles, such as Global Administrator or User Administrator.

<https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy#roles-and-permissions>.

NEW QUESTION: 73

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

| Name  | Member of |
|-------|-----------|
| User1 | Group1    |
| User2 | None      |
| User3 | None      |

You add an enterprise application named App1 and configure the following Self-service settings:

- Allow users to request access to this application: Yes
- To which group should assigned users be added: Group1
- Require approval before granting access to this application: Yes
- Who is allowed to approve access to this application: User2

Which users can request access to App1?

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

Answer: (SHOW ANSWER)

NEW QUESTION: 74

Hotspot Question

You have an Azure subscription named Sub1.

You plan to deploy Microsoft Entra Permissions Management.

You need to ensure that Permission Management can onboard Sub1. The solution must follow the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Answer Area

New-AzRoleAssignment

New-AzRoleDefinition

New-AzTag

-ApplicationId

b46c3ac5-9da6-418f-a849-0a07a10b3c6c

-RoleDefinitionName

Contributor

Owner

Reader

-Scope

"/subscriptions/<subscriptionID>"



Answer:

Answer Area

New-AzRoleAssignment

New-AzRoleDefinition

New-AzTag

-ApplicationId

b46c3ac5-9da6-418f-a849-0a07a10b3c6c

-RoleDefinitionName

Contributor

Owner

Reader

-Scope

"/subscriptions/<subscriptionID>"



NEW QUESTION: 75

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: (SHOW ANSWER)

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>

NEW QUESTION: 76

You have a Microsoft Entra tenant.

You need to create a Conditional Access policy to manage administrative access to the tenant.

The solution must ensure that administrators are authenticated by using a phishing-resistant multi-factor authentication (MFA) method.

Which three authentication methods should you include in the solution? Each correct answer presents a complete solution.

- A. an FIDO2 security key
- B. Windows Hello for Business
- C. Microsoft Authenticator

- D. email OTP
- E. SMS
- F. voice call
- G. certificate-based authentication (single-factor)
- H. certificate-based authentication (multi-factor)

**Answer:** ([SHOW ANSWER](#))

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### NEW QUESTION: 77

You have an Azure AD tenant.

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

Which roles can you manage by using PIM?

- A. Global Administrator only
- B. Global Administrator and Security Administrator only
- C. Global Administrator, Security Administrator, and Security Contributor only
- D. Account Administrator, Global Administrator, Security Administrator, and Security Contributor only

**Answer:** ([SHOW ANSWER](#))

You can manage just-in-time assignments to all Microsoft Entra roles and all Azure roles using Privileged Identity Management (PIM) in Microsoft Entra ID.

<https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

#### NEW QUESTION: 78

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Microsoft Entra.

You gain global administrator privileges to the Microsoft Entra tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Microsoft Entra tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Update-MgPolicyAuthorizationPolicy
- B. Update-MgDomain
- C. Update-MgPolicyPermissionGrantPolicyExclude
- D. Update-MgDomainFederationConfiguration

**Answer:** ([SHOW ANSWER](#))

Use the "Update-MgPolicyAuthorizationPolicy" cmdlet with the

"AllowedToSignUpEmailBasedSubscriptions" parameter set to False.

<https://learn.microsoft.com/en-us/entra/identity/users/directory-self-service-signup>

#### NEW QUESTION: 79

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

Answer: (SHOW ANSWER)

You need to use "Use app enforced restrictions" from the "Session" control of the CA.

<https://docs.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices>

NEW QUESTION: 80

Case Study 1 - Contoso, Ltd

Overview

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

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

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com.

The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

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

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

Existing Environment. Microsoft 365/Azure Environment

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

- \* Microsoft Office 365 Enterprise E5
- \* Enterprise Mobility + Security
- \* Windows 10 Enterprise E3
- \* Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

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

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- \* The users in the London office have the Microsoft 365 Phone System license unassigned.
- \* The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

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

Requirements. Planned Changes

Contoso plans to implement the following changes:

- \* Implement self-service password reset (SSPR).
- \* Analyze Azure audit activity logs by using Azure Monitor.
- \* Simplify license allocation for new users added to the tenant.
- \* Collaborate with the users at Fabrikam on a joint marketing campaign.
- \* Configure the User administrator role to require justification and approval to activate.
- \* Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- \* For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

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

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

Question

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

**Answer:** ([SHOW ANSWER](#))

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

Require justification.

You can require that users enter a business justification when they activate. To require justification, check the Require justification on active assignment box or the Require justification on activation box.

To require justification need assignment to be Eligible instead of Active.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>

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

#### NEW QUESTION: 81

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 Microsoft Entra admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all 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 Set-WindowsProductKey Cmdlet

**B.** the Set-MgUserLicense Cmdlet

**C.** the Identity Governance blade in the Microsoft Entra admin center

**D.** the Administrative units blade in the Microsoft Entra admin center

**Answer: B** ([LEAVE A REPLY](#))

#### NEW QUESTION: 82

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

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

You have a Microsoft 365 tenant.

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

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

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

Solution: From the Azure portal, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

**A.** Yes

**B.** No

**Answer: (SHOW ANSWER)**

You need to configure the fraud alert settings.

Fraud alert setting literally has an option to configure it to automatically block.

To enable and configure fraud alerts, complete the following steps:

1. Go to Azure Active Directory > Security > MFA > Fraud alert.
2. Set Allow users to submit fraud alerts to On.
3. Configure the Automatically block users who report fraud or Code to report fraud during initial greeting setting as needed.
4. Select Save.

Reference:

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

#### NEW QUESTION: 83

Hotspot Question

You have a Microsoft Entra tenant named contoso.com that has cross-tenant access configured as shown in the following table.

| Access   | Type               | Applies to                | Status      |
|----------|--------------------|---------------------------|-------------|
| Inbound  | B2B collaboration  | External users and groups | All blocked |
| Inbound  | B2B collaboration  | Applications              | All blocked |
| Inbound  | B2B direct connect | External users and groups | All blocked |
| Inbound  | B2B direct connect | Applications              | All blocked |
| Inbound  | Trust settings     | <i>Not applicable</i>     | Disabled    |
| Outbound | B2B collaboration  | Users and groups          | All blocked |
| Outbound | B2B collaboration  | External applications     | All blocked |
| Outbound | B2B direct connect | Users and groups          | All blocked |
| Outbound | B2B direct connect | External applications     | All blocked |

You have two partner organizations named Fabrikam, Inc. and A Datum Corporation. Fabrikam has a Microsoft 365 domain named fabrikam.com. A Datum has a Microsoft 365 domain named adatum.com.

You configure cross-tenant access for fabrikam.com as shown in the following table.

| Access   | Type               | Applies to                | Status      |
|----------|--------------------|---------------------------|-------------|
| Inbound  | B2B collaboration  | External users and groups | All allowed |
| Inbound  | B2B collaboration  | Applications              | All allowed |
| Inbound  | B2B direct connect | External users and groups | All allowed |
| Inbound  | B2B direct connect | Applications              | All allowed |
| Inbound  | Trust settings     | <i>Not applicable</i>     | Disabled    |
| Outbound | B2B collaboration  | Users and groups          | All blocked |
| Outbound | B2B collaboration  | External applications     | All blocked |
| Outbound | B2B direct connect | Users and groups          | All blocked |
| Outbound | B2B direct connect | External applications     | All blocked |

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                    |
|------------------------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| A user in contoso.com can send a guest invitation to a user that has an email address of user1@fabrikam.com.     | <input type="radio"/> | <input type="radio"/> |
| A user in contoso.com can send a guest invitation to a user that has an email address of user1@adatum.com.       | <input type="radio"/> | <input type="radio"/> |
| A user in contoso.com can accept a guest invitation from a user that has an email address of user1@fabrikam.com. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                                                                                                       | Yes                              | No                               |
|------------------------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| A user in contoso.com can send a guest invitation to a user that has an email address of user1@fabrikam.com.     | <input type="radio"/>            | <input checked="" type="radio"/> |
| A user in contoso.com can send a guest invitation to a user that has an email address of user1@adatum.com.       | <input type="radio"/>            | <input checked="" type="radio"/> |
| A user in contoso.com can accept a guest invitation from a user that has an email address of user1@fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |

Explanation:

Box 1: No

All outbound B2B collaboration settings are blocked.

Note: To send a guest invitation in Microsoft 365, you need to configure both inbound and outbound cross-tenant access settings for B2B collaboration. This involves specifying which external organizations are allowed to invite users to your tenant (inbound) and which organizations your users can invite (outbound) Inbound Access (Allowing Others to Invite Your Users as Guests):

Outbound Access (Allowing Your Users to Invite Guests):

Box 2: No

All outbound B2B collaboration settings are blocked.

Box 3: Yes

All inbound B2B collaboration settings are allowed.

Reference:

<https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure>

#### NEW QUESTION: 84

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

**Answer:** ([SHOW ANSWER](#))

The Authenticator app can be used as a software token to generate an OATH verification code.

After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

A: A notification through the Microsoft Authenticator app requires connectivity to send the verification code to the device requesting the login.

B: An email requires network connectivity.

C: Security questions are not used as an authentication method but can be used during the self- service password reset (SSPR) process.

Reference:

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

#### NEW QUESTION: 85

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 create an assignment for the Insights at administrator role.

Does this meet the goal?

**A.** Yes

**B.** No

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 86

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

SigninLogs

| where ResultType == 0

▼

login\_count = count() by Identity

extend

print

project

render

summarize

▼

columnchart

extend

print

project

render

summarize

Answer:

Answer Area

SigninLogs

| where ResultType == 0

▼

login\_count = count() by Identity

extend

print

project

render

summarize

▼

columnchart

extend

print

project

render

summarize

NEW QUESTION: 87

You have a Microsoft 365 E5 subscription that uses Microsoft Defender for Cloud Apps.

You discover that users connect to unsanctioned third-party apps.

You need to automatically identify and block the use of unsanctioned apps that have a risk score of 5 or higher and generate more than 200 GB of daily traffic. The solution must minimize administrative effort.

What should you do?

- A. From the Microsoft Defender portal, create an app governance policy.
- B. Create an app discovery policy by using the New popular app template.
- C. From the Microsoft Entra admin center, create a Conditional Access policy.
- D. Create an app discovery policy by using the New risky app template.

Answer: (SHOW ANSWER)

The best action to take is to create an app discovery policy by using the New risky app template.

Perfect Alignment: The New risky app template in Microsoft Defender for Cloud Apps is specifically designed to trigger alerts and take automatic actions based on risk scores and traffic volume.

Automation: By configuring this Cloud Discovery anomaly detection policy, you can automatically tag matching discoveries as Unsanctioned.

Low Administration: Once integrated with your security appliances or Microsoft Defender for Endpoint, unsanctioned apps are blocked automatically without requiring manual administrator intervention for each app.

Reference:

<https://learn.microsoft.com/en-ca/answers/questions/5876601/using-defender-for-cloud-apps-to-control-access-to>

NEW QUESTION: 88

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

Microsoft

Statements

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.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area

Microsoft

Statements

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.

Yes

No

☒

☐

☐

☒

☒

☐

NEW QUESTION: 89

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

Answer: (SHOW ANSWER)

Pass-through authentication is configured, Sync user will try to authenticate on local AD and unable to authenticate due to internet outage only cloud users (User 1 and User 3) can be authenticated.

Reference:

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

NEW QUESTION: 90

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

Answer: D (LEAVE A REPLY)

Leaked credentials indicates that the user's valid credentials have been leaked.

Note:

There are several versions of this question in the exam. The question can have other incorrect answer options, including the following:

- password spray
- malicious IP address
- unfamiliar sign-in properties

Reference:

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

**NEW QUESTION: 91**

You have an Azure subscription named Sub1.

You purchase a Microsoft Entra Permissions Management license.

You need to onboard Permissions Management.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A.** From the Microsoft Entra admin center, configure the Diagnostic settings.
- B.** From the Microsoft Entra admin center, create an app registration.
- C.** Create a role assignment for Sub1.
- D.** From Microsoft Entra Permissions Management, configure data collection.
- E.** From the Azure portal, create a data collection rule (DCR).
- F.** Implement a Microsoft Entra application proxy.

**Answer:** ([SHOW ANSWER](#))

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

**NEW QUESTION: 92**

Case Study 1 - Contoso, Ltd

Overview

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

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

Existing Environment. Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contoso.com.

The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers.

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

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

Existing Environment. Microsoft 365/Azure Environment

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

- \* Microsoft Office 365 Enterprise E5
- \* Enterprise Mobility + Security
- \* Windows 10 Enterprise E3
- \* Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

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

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- \* The users in the London office have the Microsoft 365 Phone System license unassigned.
- \* The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

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

Requirements. Planned Changes

Contoso plans to implement the following changes:

- \* Implement self-service password reset (SSPR).
- \* Analyze Azure audit activity logs by using Azure Monitor.
- \* Simplify license allocation for new users added to the tenant.
- \* Collaborate with the users at Fabrikam on a joint marketing campaign.
- \* Configure the User administrator role to require justification and approval to activate.
- \* Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- \* For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

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

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

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

What should you implement?

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

Answer: (SHOW ANSWER)

You can assign a redirect URI as part of the registration process.

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

NEW QUESTION: 93

Drag and Drop Question

You have a Microsoft 365 E5 subscription that contains three users named User1, User2, and User3.

You need to configure the users as shown in the following table.

| User  | Configuration                                                                                                                                                   |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User1 | <ul style="list-style-type: none"><li>• User administrator role</li><li>• Device Administrators role</li><li>• Identity Governance Administrator role</li></ul> |
| User2 | <ul style="list-style-type: none"><li>• Records Management role</li><li>• Quarantine Administrator role group</li></ul>                                         |
| User3 | <ul style="list-style-type: none"><li>• Endpoint Security Manager role</li><li>• Intune Role Administrator role</li></ul>                                       |

Which portal should you use to configure each user? To answer, drag the appropriate portals to the correct users. Each portal 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.

Portals

Azure Active Directory admin center

Exchange admin center

Microsoft 365 compliance center

Microsoft Endpoint Manager admin center

SharePoint admin center

Answer Area

User1:

User2:

User3:

Answer:

Portals

Exchange admin center

SharePoint admin center

Answer Area

User1: Azure Active Directory admin center

User2: Microsoft 365 compliance center

User3: Microsoft Endpoint Manager admin center

Explanation:

User 1: Azure Active Directory Admin Center

User 2: Microsoft Purview admin center (legacy Microsoft Compliance Admin center) These roles came from Exchange, Microsoft is not enforcing the roles permission from Exchange, Microsoft is recommending using Microsoft Purview Admin center. I believe this answer is too old.

it could be true years ago, however, Microsoft today is with MS purview to assign these roles.

Record management and Quarantine role are known as SCC (security and compliance center) SCC roles have evolved from Exchange role groups design to MS Purview.

User 3: Microsoft Endpoint Manager Admin Center

You will see these two roles in the endpoint admin center.

NEW QUESTION: 94

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 999999999

You need to configure the Group Administrator role to meet the following requirements:

- Ensure that Allan Deyoung can approve and reject requests to activate the role.
- Ensure that Christie Cline can request activation of the role.
- Use the principle of least privilege.

To complete this task, sign in to the appropriate admin center.

**A.** In Privileged Identity Management (PIM):

Assign Christie Cline an eligible assignment for the Group Administrator role.

Open the role settings for Group Administrator, enable approval workflow, add Allan Deyoung as the designated approver.

**B.** In Entra ID Roles:

Assign Christie Cline permanent Group Administrator rights.

Add Allan Deyoung to the Global Administrator role to approve activation requests.

**C.** In Microsoft 365 Admin Center > Groups:

Add Christie Cline as group owner.

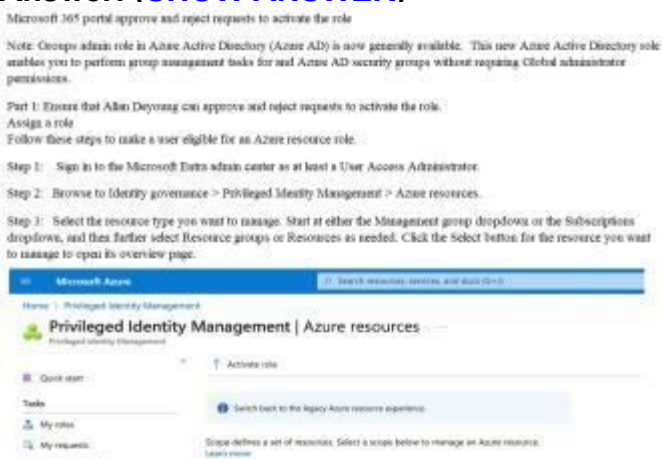
Assign Allan Deyoung the User Administrator role to manage role requests.

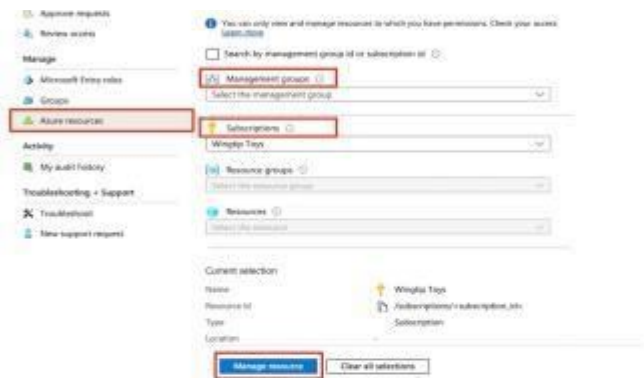
**D.** In Exchange Admin Center:

Create a role assignment policy granting Christie group management permissions.

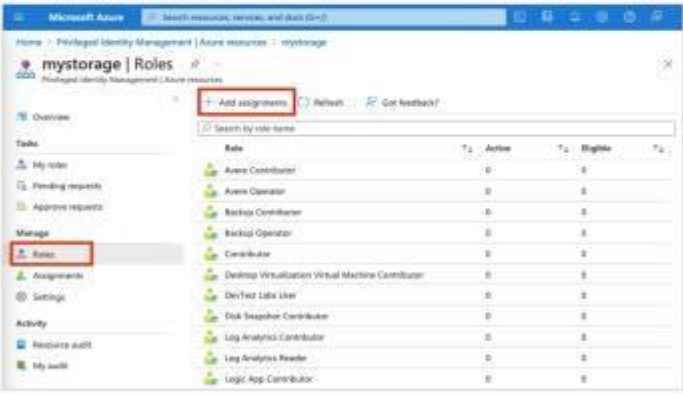
Assign Allan the Compliance Management role to approve access requests.

Answer: (SHOW ANSWER)



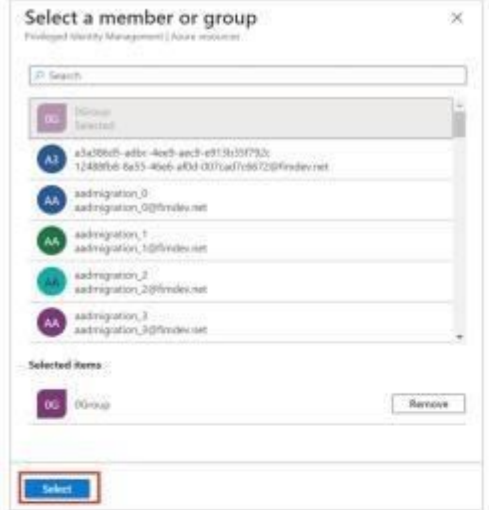
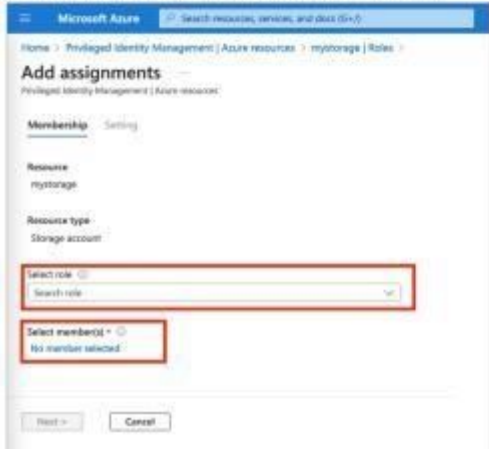


Step 5: Select Add assignments to open the Add assignments page.



Step 6: Select a Role you want to assign. [Here: Select the Group Administrator role]

Step 7: Select No member selected link to open the Select a member or group page.



Add assignments

Proteged Identity Management | Admin resources

Membership

Setting

Assignment type

☒ Eligible

☐ Active

Maximum allowed eligible duration is 1 year(s)

Assignment starts \*

07/06/202210:50:22 AM

Assignment ends \*

07/06/202510:50:22 AM

Assign

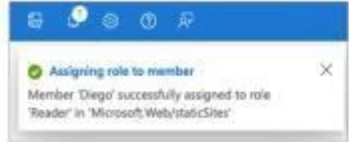
+ Prev

Cancel

Active assignments don't require the member to activate the role before usage. Members assigned as active have the privileges assigned ready to use. This type of assignment is also available to customers that don't use Microsoft Entra PIM.

Step 10: When finished, select Assign.

Step 11: After the new role assignment is created, a status notification is displayed.



Part 2: Ensure that Christie Cline can request activation of the role.

Repeat steps 1-7 above.

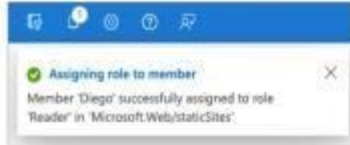
Step 8: Select a member or group you want to assign to the role and then choose Select. [Here: select Christie Cline]

Step 9: On the Settings tab, in the Assignment type list, select Eligible or Active. [Here: Select Eligible]

Eligible assignments require the member to activate the role before using it. Administrator may require role member to perform certain actions before role activation, which might include performing a multi-factor authentication (MFA) check, providing a business justification, or requesting approval from designated approvers.

Step 10: When finished, select Assign.

Step 11: After the new role assignment is created, a status notification is displayed.



Reference:

<https://techcommunity.microsoft.com/t5/microsoft-365-groups/introducing-the-groups-admin-role-in-p973997>

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/iam-resource-roles-assign-roles>

NEW QUESTION: 95

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 999999999

You need to prevent all users from using passwords that are variations of the word Falcon.

To complete this task, sign in to the appropriate admin center.

Eliminate bad passwords using Microsoft Entra Password Protection

Step 1: Select Authentication methods

Step 2: Select Password Protection

Step 3: In Custom banned passwords, Set Enforce Custom list: Yes

**Authentication methods | Password protection**  

Contoso - Microsoft Entra ID Security

Search  Save  Discard  Got feedback?

**Manage**

- Policies
- Password protection**
- Registration campaign
- Authentication strengths
- Settings

**Monitoring**

- Activity
- User registration details
- Registration and reset events
- Bulk operation results

Custom smart lockout

Lockout threshold  10 

Lockout duration in seconds  60 

Custom banned passwords

Enforce custom list  ☒ Yes ☐ No

Custom banned password list 

- contoso
- fabrikam
- tailwind
- michigan
- wolverine
- harbaugh
- howard

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory  ☐ Yes ☒ No

Mode  ☒ Enforced ☐ Audit

Step 4: In Custom banned password list, add the word Falcon

Reference:

<https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad>

**NEW QUESTION: 96**

Hotspot Question

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

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

 Edit

Activation

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

Assignment

| SETTING                                                        | STATE      |
|----------------------------------------------------------------|------------|
| Allow permanent eligible assignment                            | No         |
| Expire eligible assignments after                              | 15 day(s)  |
| Allow permanent active assignment                              | No         |
| Expire active assignments after                                | 1 month(s) |
| Require Azure Multi-Factor Authentication on active assignment | No         |
| Require justification on active assignment                     | No         |



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

Answer Area



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

|         |
|---------|
| 8 hours |
| 15 days |
| 1 month |

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

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

Answer:

Answer Area

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

|         |
|---------|
| 8 hours |
| 15 days |
| 1 month |

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

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

Explanation:  
Select at least one approver. If no specific approvers are selected, Privileged Role Administrators and Global Administrators become the default approvers.

Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-change-default-settings>  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>  
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan>

**NEW QUESTION: 97**

Hotspot Question

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

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

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

Answer Area

Service to install on Server4:

Azure AD Application Proxy

The Azure AD Password Protection DC agent

The Azure AD Password Protection proxy service

Web Application Proxy in Windows Server

Rule to configure on Firewall1:

Allow incoming HTTPS connections from Azure AD to Server4.

Allow incoming IPsec connections from Azure AD to Server4.

Allow outbound HTTPS connections from Server4 to Azure AD.

Allow outbound IPsec connections from Server4 to Azure AD.

Answer:

**Answer Area**

Service to install on Server4:

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

Rule to configure on Firewall1:

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

Explanation:

Application Proxy is an Azure AD service you configure in the Azure portal. It enables you to publish an external public HTTP/HTTPS URL endpoint in the Azure Cloud, which connects to an internal application server URL in your organization.

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

**NEW QUESTION: 98**

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

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

You have a Microsoft 365 tenant.

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

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

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

Solution: From the Azure Active Directory admin center, you configure the Block/unblock users settings for multi-factor authentication (MFA).

Does this meet the goal?

A. Yes

B. No

Answer: (SHOW ANSWER)

Report suspicious activity and the legacy Fraud Alert implementation can operate in parallel. You can keep your tenant-wide Fraud Alert functionality in place while you start to use Report suspicious activity with a targeted test group.

If Fraud Alert is enabled with Automatic Blocking, and Report suspicious activity is enabled, the user will be added to the blocklist and set as high-risk and in-scope for any other policies configured. These users will need to be removed from the blocklist and have their risk remediated to enable them to sign in with MFA.

<https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#report-suspicious-activity-and-fraud-alert>

**NEW QUESTION: 99**

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.  
Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com  
Microsoft 365 Password: =1122334455667788  
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.  
The following information is for technical support purposes only:  
Lab Instance: 999999999  
You need to ensure that users in the sg-Legal group must reauthenticate every 12 hours when they access any cloud apps managed by the tenant.  
To complete this task, sign in to the appropriate admin center.

Answer:

Microsoft Entra, Microsoft Entra ID, Conditional Access, Configure adaptive session lifetime policies

Sign-in frequency control

- Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.
- Step 2: Browse to Protection > Conditional Access.
- Step 3: Select Create new policy.
- Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.
- Step 5: Choose all required conditions for customer’s environment, including the target cloud apps.
- Step 6: Under Access controls > Session.
- Step 6a: Select Sign-in frequency.
- Step 6b: Choose Periodic reauthentication and enter a value of hours or days [Specify 12 hours: 12 + Hours as Unit] or select Every time.

Home > Contoso | Security > Security | Conditional Access > Conditional Access | Policies >

New

Conditional Access policy

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.  
[Learn more](#)

Name \*

Sign-in frequency

Session

Control access based on session controls to enable limited experiences within specific cloud applications.  
[Learn more](#)

☐ Use app enforced restrictions ⓘ

☐ Use Conditional Access App Control ⓘ

## Assignments

Users or workload identities ⓘ

Specific users included

Cloud apps or actions ⓘ

1 app included

Conditions ⓘ

0 conditions selected

## Access controls

Grant ⓘ

0 controls selected

Session ⓘ

0 controls selected

## Enable policy

Report-only

On

Off

Create

☒ Sign-in frequency ⓘ

☒ Periodic reauthentication

0

Select units

☐ Every time

⚠ Some of the applications currently selected are not compatible with the "Sign-in frequency" option of "Every time"

☐ Persistent browser session ⓘ

☐ Customize continuous access evaluation ⓘ

☐ Disable resilience defaults ⓘ

Select

Step 6c: For Assignments, User or workload identities, specify the sg-Legal group

Step 6d: For Cloud apps or actions, specify any/all cloud apps.

Step 7: Click Create, and save your policy.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-session-lifetime>

**NEW QUESTION: 100**

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

- A device named Devie1
- 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        | User4                        |
| Group5 | Microsoft 365 | Assigned        | User5                        |

How many licenses are used if you assign the Microsoft 365 Enterprise E5 license to Group1?

- A. 0
- B. 2
- C. 3
- D. 4

Answer: (SHOW ANSWER)

Group-based licensing currently does not support groups that contain other groups (nested groups). If you apply a license to a nested group, only the immediate first-level user members of the group have the licenses applied.

Reference:

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

**NEW QUESTION: 101**

You have a Microsoft Exchange organization that uses an SMTP address space of contoso.com.

Several users use their contoso.com email address for self-service sign-up to Azure Active Directory (Azure AD).

You gain global administrator privileges to the Azure AD tenant that contains the self-signed users.

You need to prevent the users from creating user accounts in the contoso.com Azure AD tenant for self-service sign-up to Microsoft 365 services.

Which PowerShell cmdlet should you run?

- A. Set-MsolCompanySettings
- B. Set-MsolDomainFederationSettings
- C. Update-MsolfederatedDomain
- D. Set-MsolDomain

Answer: (SHOW ANSWER)

Self-service sign-up: Method by which a user signs up for a cloud service and has an identity automatically created for them in Azure AD based on their email domain.

Azure AD cmdlet Set-MsolCompanySettings could help you to prevent creating user accounts with parameters:

AllowEmailVerifiedUsers (users can join the tenant by email validation)-->when is TRUE.

AllowAdHocSubscriptions (controls the ability for users to perform self-service sign-up) e.g. Set-MsolCompanySettings -AllowEmailVerifiedUsers \$false -AllowAdHocSubscriptions \$false Reference: <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup>

You have a Microsoft Entra tenant named contoso.com that contains an 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. Implement Microsoft Entra Connect sync.
- B. Create a guest user account in contoso.com.
- C. Configure the External collaboration settings.
- D. Run the New-MgUsercmdlet.

Answer: B (LEAVE A REPLY)

- \* Create a guest user account in contoso.com.
- \* Run the New-AzureADMSInvitation cmdlet. [For Microsoft Active Directory]
- \* Run the New-MgInvitationcmdlet. [For Microsoft Entra]

Note:

\* New-AzureADMSInvitation

This cmdlet is used to invite a new external user to your directory.

\* New-MgInvitation

Microsoft.Graph.Identity.SignIns

Use this API to create a new invitation or reset the redemption status for a guest user who already redeemed their invitation. Invitation adds an external user to the organization Reference:

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

<https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/new-mginvitation>

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

NEW QUESTION: 103

Hotspot Question

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

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

The subscription contains the users shown in the following table.

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

On June 1, Admin4 performs the following actions:

- Deletes a certificate named Certificate1 from KeyVault1
- Deletes a secret named Secret1 from KeyVault2

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements                                | Yes                   | No                    |
|-------------------------------------------|-----------------------|-----------------------|
| Admin1 can recover Secret1 on June 7.     | <input type="radio"/> | <input type="radio"/> |
| Admin2 can purge Certificate1 on June 12. | <input type="radio"/> | <input type="radio"/> |
| Admin3 can purge Certificate1 on June 14. | <input type="radio"/> | <input type="radio"/> |

Answer:

Statements

Yes

No

Admin1 can recover Secret1 on June 7.

☒☐

Admin2 can purge Certificate1 on June 12.

☐☒

Admin3 can purge Certificate1 on June 14.

☐☒

Explanation:

Box 1: Yes

Key Vault Administrator can perform all data plane operations on a key vault.

And purge protection is disabled for KeyVault2.

NB: Purge protection is an optional Key Vault behavior and is not enabled by default.

Do not mismatch with soft-delete

Box 2: No

We are still in the Purge protection remaining period.

NB: Also the Key Vault contributor role doesn't allow to get access to certificate Box 3: No We are still in the Purge protection remaining period.

Even if the Certificate Officer role allow to get access to certificate

NEW QUESTION: 104

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that has an Azure Active Directory Premium Plan 2 license. The tenant contains the users shown in the following table.

| Name   | Role                       |
|--------|----------------------------|
| Admin1 | Cloud device administrator |
| Admin2 | Device administrator       |
| User1  | None                       |

You have the Device Settings shown in the following exhibit.

All devices

Device settings

Enterprise State Roaming

BitLocker keys (Preview)

Diagnose and solve problems

Activity

Audit logs

Bulk operation results (Preview)

Troubleshooting + Support

New support request

<< Save Discard Got feedback?

Users may join devices to Azure AD ⓘ  

All Selected None

Selected  
No member selected

Users may register their devices with Azure AD ⓘ  

All None

Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication ⓘ  

Yes No

⚠ We recommend that you require Multi-Factor Authentication to register or join devices using Conditional Access. Set this device setting to No if you require Multi-Factor Authentication using Conditional Access.

Maximum number of devices per user ⓘ  

5

 **Microsoft**

Additional local administrators on all Azure AD joined devices  
[Manage Additional local administrators on All Azure AD joined devices](#)

User1 has the devices shown in the following table.

| Name    | Operating system | Device identity     |
|---------|------------------|---------------------|
| Device1 | Windows 10       | Azure AD joined     |
| Device2 | iOS              | Azure AD registered |
| Device3 | Windows 10       | Azure AD registered |
| Device4 | Android          | Azure AD registered |

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

Answer Area

Statements

Yes

No

User1 can join four additional Windows 10 devices to Azure AD.

☐☐

Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.

☐☐

Admin2 is a local administrator on Device3.

☐☐

Answer:

Answer Area



Statements

Yes

No

User1 can join four additional Windows 10 devices to Azure AD.

☐☒

Admin1 can set Devices to be Azure AD joined or Azure AD registered require Multi-Factor Authentication to **Yes**.

☒☐

Admin2 is a local administrator on Device3.

☐☒

Explanation:

Box 1: No

Maximum number of devices: This setting enables you to select the maximum number of Azure AD joined or Azure AD registered devices that a user can have in Azure AD.

Box 2: Yes

You must be assigned one of the following roles to view or manage device settings in the Azure portal:

- \* Global Administrator
- \* Cloud Device Administrator
- \* Global Reader
- \* Directory Reader

Box 3: No

Additional local administrators on Azure AD joined devices (Device is Registered not Joined) Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal>

NEW QUESTION: 105

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: (SHOW ANSWER)

NEW QUESTION: 106

Hotspot Question

You have a Microsoft Entra tenant that contains two groups named Group1 and Group2 and the users shown in the following table.

| Name  | Type   | Member of | Description                        |
|-------|--------|-----------|------------------------------------|
| User1 | Member | Group1    | None                               |
| User2 | Guest  | Group1    | None                               |
| User3 | Member | None      | Assigned the Owner role for Group1 |
| User4 | Member | Group2    | Assigned the Owner role for Group2 |
| User5 | Guest  | Group2    | None                               |

Group2 is a member of Group1.

You configure an access review that has the following settings:

- Name: Review1
- Select what to review: Teams + Groups
- Review scope: Select Teams + groups
- Group: Group1
- Scope: Guest users only
- Select reviewers: Group owners(s)

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

User3 can perform an access review of User1.

User3 can perform an access review of User4.

User3 can perform an access review of User5.

Yes

No

☐

☐

☐

☐

☐

☐

Answer:

Answer Area

Statements

User3 can perform an access review of User1.

User3 can perform an access review of User4.

User3 can perform an access review of User5.

Yes

No

☐

☒

☐

☒

☒

☐

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

**NEW QUESTION: 107**

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

**Answer:** (SHOW ANSWER)

You cannot manage the following classic subscription administrator roles in Privileged Identity Management:

- Account Administrator
- Service Administrator
- Co-Administrator

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/pim-roles>

**NEW QUESTION: 108**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains two administrative units named AU1 and AU2.

You create five users as shown in the following table.

| Name  | Administrative unit | Role                                    | Role scope |
|-------|---------------------|-----------------------------------------|------------|
| User1 | AU2                 | Global Administrator                    | None       |
| User2 | AU2                 | Helpdesk Administrator                  | AU1        |
| User3 | AU1                 | Privileged Authentication Administrator | AU2        |
| User4 | AU1                 | Helpdesk Administrator                  | AU1        |
| User5 | AU1                 | None                                    | None       |

For which users can User2 and User3 reset passwords? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

User2 can reset password for:

|                                |
|--------------------------------|
| User1 and User4 only           |
| User1, User3, User4, and User5 |
| User3 only                     |
| User4 only                     |
| User5 only                     |

User3 can reset password for:

|                         |
|-------------------------|
| User1 only              |
| User1 and User2 only    |
| User1, User2, and User4 |
| User2 and User4 only    |
| User 5 only             |

Answer:  
Answer Area

User2 can reset password for:

|                                |
|--------------------------------|
| User1 and User4 only           |
| User1, User3, User4, and User5 |
| User3 only                     |
| User4 only                     |
| User5 only                     |

User3 can reset password for:

|                         |
|-------------------------|
| User1 only              |
| User1 and User2 only    |
| User1, User2, and User4 |
| User2 and User4 only    |
| User 5 only             |

NEW QUESTION: 109

You are the lead cloud administrator for Pass4test Inc. and you just hired a new employee that will be in charge of Azure AD Support issues. This new employee needs the ability to reset the passwords for all types of users when requested, including users with the user admin, global admin, or password admin roles. You need to ensure that you follow the principle of least privilege when granting access. What role should you grant the new employee?

- A. Password Admin
- B. Global Admin

C. Security Admin

D. User Admin

**Answer:** ([SHOW ANSWER](#))

The Global Admin role would allow the new employee to reset passwords for all users.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#user-administrator>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

#### NEW QUESTION: 110

You have an Azure AD tenant.

You need to ensure that only users from specific external domains can be invited as guests to the tenant.

Which settings should you configure?

A. Linked subscriptions

B. All identity providers

C. External collaboration settings

D. Cross-tenant access settings

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 111

You have multiple on-premises devices that run either Windows or Linux.

You have a Microsoft 365 E5 subscription.

You configure Microsoft Entra Internet Access.

You need to ensure that all the on-premises devices access the internet by using Global Secure Access.

What should you do in the Microsoft Entra admin center?

A. Create a remote network.

B. Create a named location.

C. Create an access package.

D. Deploy the Global Secure Access client.

**Answer:** ([SHOW ANSWER](#))

A remote network can be used with Global Secure Access, specifically with Microsoft Entra Internet Access. Users can access Microsoft traffic through remote network connectivity, such as in a branch office, without needing the Global Secure Access client. This allows users to connect and access Microsoft services from remote locations while still benefiting from the security and control provided by Global Secure Access.

Global Secure Access supports two connectivity options: installing a client on end-user device and configuring a remote network, for example a branch location with a physical router. Remote network connectivity streamlines how your end-users and guests connect from a remote network without needing to install the Global Secure Access Client.

Note: To define a remote network in the Microsoft Entra admin center, navigate to Global Secure Access > Connect > Remote networks. Select "Create remote network" and provide the necessary details, including name, region, and connectivity information Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/concept-remote-network-connectivity>

#### NEW QUESTION: 112

Drag and Drop Question

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

Attire AD Connect is installed on a server named Server1.

You deploy a new server named Server1 that runs Windows Server 2019.

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

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

Actions

On Server1, run export for all connectors.

On Server2, run export for all connectors.

On Server2, run full import for all connectors.

On Server2, run delta synchronization for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

Answer:

Actions

On Server2, run full import for all connectors.

On Server2, install Azure AD Connect.

On Server1, configure the staging mode.

Answer Area

On Server2, run export for all connectors.

On Server2, run delta synchronization for all connectors.

On Server1, run export for all connectors.

NEW QUESTION: 113

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains a registered app named App1.

You have a partner organization that has a Microsoft Entra tenant. The tenant contains a registered app named App2.

You need to ensure that App1 can access App2.

Which two types of credentials can App1 use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. managed identity
- B. secret
- C. certificate
- D. one-time password
- E. user account

Answer: (SHOW ANSWER)

NEW QUESTION: 114

You have an Azure subscription that contains a storage account named storage1 and a web app named WebApp1. WebApp1 uses a system-assigned managed identity.

You need to ensure that WebApp1 can read and write files to storage1 by using the system- assigned managed identity.

What should you configure for storage1 in the Azure portal?

- A. data protection

- B. a shared access signature (SAS)
- C. the Access control (IAM) settings
- D. the File share settings
- E. access keys

Answer: (SHOW ANSWER)

In the Azure portal, go into your storage account to grant your web app access. Select Access control (IAM) in the left pane, and then select Role assignments. You'll see a list of who has access to the storage account. Now you want to add a role assignment to a robot, the app service that needs access to the storage account. Select Add > Add role assignment to open the Add role assignment page.

<https://learn.microsoft.com/en-us/entra/identity-platform/multi-service-web-app-access-storage?tabs=azure-portal%2Cprogramming-language-csharp#grant-access-to-the-storage-account>

NEW QUESTION: 115

Hotspot Question

You have an Azure subscription named Sub1.

You plan to onboard Microsoft Entra Permissions Management.

You need to ensure that Permissions Management users can manage role assignments for Sub1.

The solution must follow the principle of least privilege.

Which role should you assign and to which identity should you assign the role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role:

Contributor

Reader

Security Admin

User Access Administrator

Identity:

Azure Credential Configuration Endpoint Service

Cloud Infrastructure Entitlements Management

Microsoft Azure Management

Answer:

Answer Area

Role:

Contributor

Reader

Security Admin

User Access Administrator

Identity:

Azure Credential Configuration Endpoint Service

Cloud Infrastructure Entitlements Management

Microsoft Azure Management

Explanation:

<https://learn.microsoft.com/en-us/entra/permissions-management/onboard-enable-controller- after-onboarding#enable-or-disable-the-controller-in-azure>

**NEW QUESTION: 116**

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and a certification authority (CA) named CA1.

You have an Azure AD tenant.

You need to implement certificate-based authentication in Azure AD. The solution must ensure that users can sign in by using certificates issued by CA1. What should you do first?

- A. Deploy an Azure key vault.
- B. Add CA1 as a Certificate Authority to the Microsoft Entra ID tenant.
- C. Enable auto-enrollment for CA1.
- D. Deploy Windows Hello for Business.

**Answer:** [\(SHOW ANSWER\)](#)

<https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-certificate-based- authentication>

**NEW QUESTION: 117**

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

**Answer:** [\(SHOW ANSWER\)](#)

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

**NEW QUESTION: 118**

Hotspot Question

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

| Name        | Type                     | In resource group |
|-------------|--------------------------|-------------------|
| Vault1      | Azure Key Vault          | RG1               |
| Automation1 | Azure Automation account | RG1               |
| Automation2 | Azure Automation account | RG2               |
| VM1         | Virtual machine          | RG2               |

Sub1 contains the managed identities shown in the following table.

| Name      | Type            | Assigned to |
|-----------|-----------------|-------------|
| Identity1 | User-assigned   | Automation1 |
| Identity2 | System-assigned | Automation2 |
| Identity3 | System-assigned | VM1         |

Sub1 has the role-based access control (RBAC) role assignments shown in the following table.

| Identity  | Role                   | Scope |
|-----------|------------------------|-------|
| Identity1 | Key Vault Secrets User | RG2   |
| Identity2 | Key Vault Secrets User | Sub1  |
| Identity3 | Key Vault Secrets User | RG1   |

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

Automation1 can access the contents of the secrets stored in Vault1.

Identity2 can be assigned to Automation2 to gain access to the contents of the secrets stored in Vault1.

VM1 can access the contents of the secrets stored in Vault1.

Yes

No

Answer Area

Statements

Automation1 can access the contents of the secrets stored in Vault1.

Identity2 can be assigned to Automation2 to gain access to the contents of the secrets stored in Vault1.

VM1 can access the contents of the secrets stored in Vault1.

Yes

No

NEW QUESTION: 119

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 Microsoft Entra admin center, you assign Microsoft Office 365 Enterprise E5 licenses to a group that includes all 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 Licenses blade in the Microsoft Entra admin center
- B. the Administrative units blade in the Microsoft Entra admin center
- C. the Identity Governance blade in the Microsoft Entra admin center
- D. the Update-MgUser cmdlet

Answer: (SHOW ANSWER)

To remove the Office 365 Enterprise E3 licenses from the users who are now part of a group with Office 365 Enterprise E5 licenses assigned, you should use the "Licenses" blade in the Microsoft Entra admin center. This allows you to manage license assignments at a group level, making it easier to apply and remove licenses for multiple users simultaneously.

NEW QUESTION: 120

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has Azure AD Identity Protection enabled.  
You need to implement a sign-in risk remediation policy without blocking user access.  
What should you do first?

- A. Configure access reviews in Azure AD.
- B. Enforce Azure AD Password Protection.
- C. Configure self-service password reset (SSPR) for all users.
- D. Implement multi-factor authentication (MFA) for all users.

Answer: (SHOW ANSWER)

To implement a sign-in risk remediation policy.

When a sign in risk policy triggers:

Azure AD MFA can be triggered, allowing to user to prove it's them by using one of their registered authentication methods, resetting the sign in risk.

Reference:

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

NEW QUESTION: 121

Drag and Drop Question

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

Admin1 uses the Require password change for high-risk users 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

Options

Admin1

All guest and external users

All users

Directory roles

None

Include:

Exclude:

Answer:

## Options

 All guest and external users

Directory roles

None

## Answer Area

Include: All users

Exclude: Admin1

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk-user>

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

### NEW QUESTION: 122

You have a Microsoft Entra tenant.

You need to ensure that users are prevented from consenting to high-privilege permission requests for enterprise applications. The solution must ensure that the users can consent to low- risk permission requests.

What should you modify first?

- A. Admin consent settings
- B. Permission classifications
- C. User consent settings
- D. App registrations

**Answer: (SHOW ANSWER)**

To let users consent to low-risk permissions but block others in Microsoft Entra, use User Consent Settings in the Microsoft Entra admin center to select "Allow user consent for apps from verified publishers for selected permissions," then define those low-risk permissions under Permission classifications, requiring admin approval for anything beyond that, especially high-risk or unverified app requests. This balances security by restricting risky requests (often flagged by risk-based step-up consent) while allowing productivity for trusted apps.

Reference:

<https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent>

### NEW QUESTION: 123

Hotspot Question

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.

Answer Area

VM1: 

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

App1: 

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:

Answer Area

VM1: 

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

App1: 

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

NEW QUESTION: 124

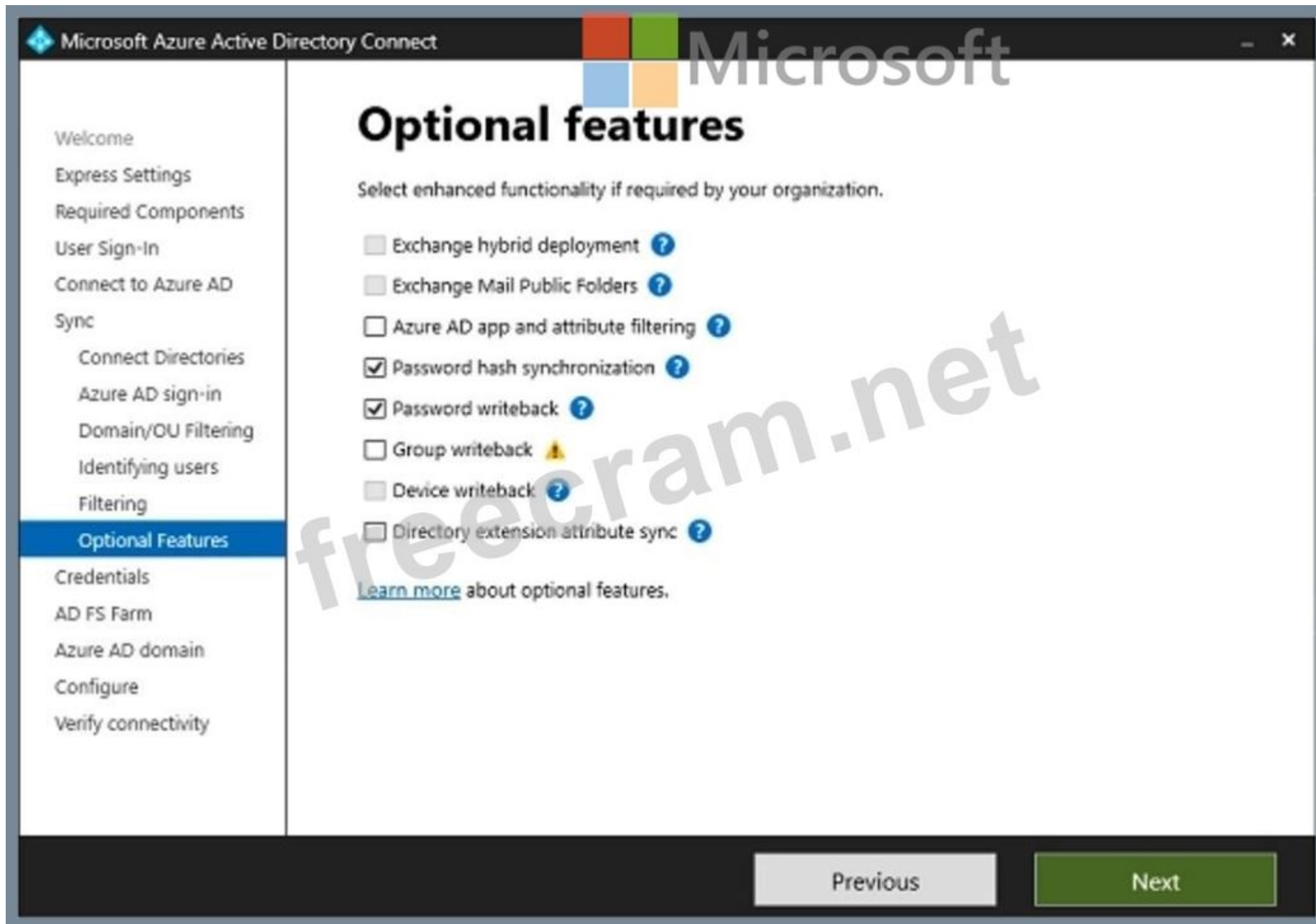
Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named fabrikam.com. The domain contains an Active Directory Federation Services (AD FS) instance and a member server named Server1 that runs Windows Server. The domain contains the users shown in the following table.

| Name  | Description                                                       |
|-------|-------------------------------------------------------------------|
| User1 | The user account has a six-character password and is enabled.     |
| User2 | The user account has a 12-character password and is enabled.      |
| User3 | The user account has an eight-character password and is disabled. |

You have a Microsoft Entra tenant named contoso.com that is linked to a Microsoft 365 subscription.

You establish federation between fabrikam.com and contoso.com by using a Microsoft Entra Connect instance that is configured as shown in the following exhibit.



You perform the following tasks in contoso.com:

- Create a group named Group1.
- Disable User2.
- Enable 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.

| Statements                          | Yes                   | No                    |
|-------------------------------------|-----------------------|-----------------------|
| You can add User1 to Group1.        | <input type="radio"/> | <input type="radio"/> |
| User2 can sign in to Server1.       | <input type="radio"/> | <input type="radio"/> |
| User3 can sign in to Microsoft 365. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                          | Yes                              | No                               |
|-------------------------------------|----------------------------------|----------------------------------|
| You can add User1 to Group1.        | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can sign in to Server1.       | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 can sign in to Microsoft 365. | <input type="radio"/>            | <input checked="" type="radio"/> |

Explanation:

Box 1: Yes

Group1 is created in the entra ID tenant, and the user is synced, so this is possible. It doesn't state that the group should be visible on-prem.

Box 2: Yes

The user is a directory-synced user, so authority lies on-prem. Disabling it from the Entra ID portal will have no effect. The server is also an on-prem server. Disabling should be done in on- prem adds.

Box 3: No

You enable the account in the entra id tenant, but the account is directory synced, so authority lies with the on-prem AD, enabling from the portal is not possible.

**NEW QUESTION: 125**

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 verification code from the Microsoft Authenticator app

**B.** security questions

**C.** voice

**D.** SMS

**Answer: (SHOW ANSWER)**

The Authenticator app can be used as a software token to generate an OATH verification code.

After entering your username and password, you enter the code provided by the Authenticator app into the sign-in interface.

Incorrect Answers:

B: Security questions are not used as an authentication method but can be used during the self- service password reset (SSPR) process.

C, D: An automated voice call and an SMS requires mobile connectivity.

Reference:

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

**NEW QUESTION: 126**

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.** a Microsoft Teams chat
- B.** a mobile app notification
- C.** a mobile app code
- D.** an FID02 security token

**Answer:** (SHOW ANSWER)

The following authentication methods are available for SSPR (self-service password reset)

- app notification
- Mobile app code
- Email
- Mobile phone
- Office phone (available only for tenants with paid subscriptions)
- Security questions

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

**NEW QUESTION: 127**

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

- A device named Device1
- Users named User1, User2, User3, User4, and User5
- Groups named Group1, Group2, Group3, Group4, and Group5

The groups are configured as shown in the following table.

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

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

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

**Answer:** (SHOW ANSWER)

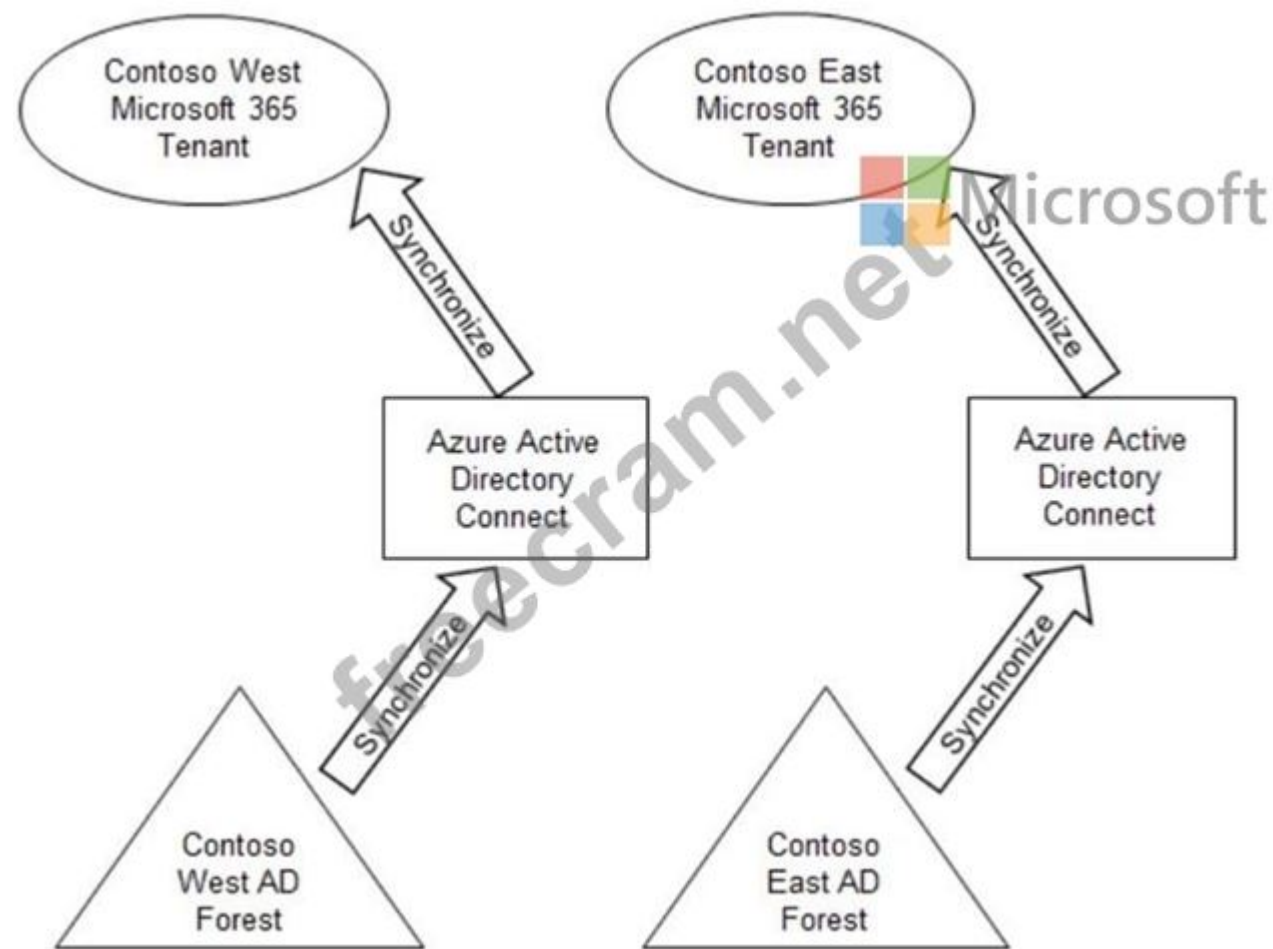
You cannot assign licenses to group 3 because it is a device group. You cannot assign licenses to device groups.

You cannot assign licenses to group 4 and group 5. You cannot assign licenses to Microsoft 365 groups.

[https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group- advanced](https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced)

**NEW QUESTION: 128**

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.

**Answer:** ([SHOW ANSWER](#))

Before any of your users can grant SharePoint Online team site access to external guests, you will have to enable guest sharing from within Azure Active Directory.

Reference:

<https://redmondmag.com/articles/2020/03/11/guest-access-sharepoint-online-team-sites.aspx>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/multi-tenant-common-considerations>

**NEW QUESTION: 129**

Your organization is planning to implement Microsoft Sentinel as its dedicated Security Information Event Management System. Which of the below is a prerequisite before you can begin working with Microsoft Sentinel?

- A. Azure AD Premium P1 License
- B. Log Analytics Workspace
- C. Azure AD Premium P2 License
- D. Azure Key Vault

**Answer:** ([SHOW ANSWER](#))

As having a configured Log Analytics Workspace is a prerequisite before begging to ingest data into Microsoft Sentinel.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/quickstart-onboard#:~:text=%20Enable%20Azure%20Sentinel%20%201%20Sign%20in,support%20the%20moving%20of%20that%20workspace...%20See%20More>

#### NEW QUESTION: 130

You have a Microsoft Entra tenant.

You discover that a large number of new apps were added to the tenant.

You need to implement an approval process for new enterprise applications.

What should you do?

- A.** From the Microsoft Defender portal, configure an app connector.
- B.** From the Microsoft Entra admin center, configure an access review.
- C.** From the Microsoft Defender portal, create an app detection policy.
- D.** From the Microsoft Entra admin center, configure the Admin consent settings.

**Answer: (SHOW ANSWER)**

Correct:

\* From the Microsoft Entra admin center, configure the Admin consent settings.

Incorrect:

- \* From the Microsoft 365 Defender portal, configure an app connector.
- \* From the Microsoft 365 Defender portal, create a Cloud Discovery anomaly detection policy.
- \* From the Microsoft Defender portal, create an app detection policy.
- \* From the Microsoft Entra admin center, configure an access review.

Note:

Configure the admin consent workflow

The admin consent workflow gives admins a secure way to grant access to applications that require admin approval. When a user tries to access an application but is unable to provide consent, they can send a request for admin approval. The request is sent via email to admins who have been designated as reviewers. A reviewer takes action on the request, and the user is notified of the action.

Enable the admin consent workflow

To enable the admin consent workflow and choose reviewers:

Sign in to the Microsoft Entra admin center as as a Global Administrator.

Browse to Identity > Applications > Enterprise applications > Consent and permissions > Admin consent settings.

Under Admin consent requests, select Yes for Users can request admin consent to apps they are unable to consent to .

Etc.

Note: Access and consent

You can manage user consent settings to choose whether users can allow an application or service to access user profiles and organizational data. When applications are granted access, users can sign in to applications integrated with Azure AD, and the application can access your organization's data to d'liver rich data-driven experiences.

In situations where users are unable to consent to the permissions an application is requesting, consider configuring the admin consent workflow. The workflow allows users to provide a justification and request an administrator's review an approval of an application.

Reference:

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

#### NEW QUESTION: 131

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.

The screenshot displays the configuration interface for Microsoft Entra Permissions Management. It is divided into two main sections: 'Expiration' and 'Access Reviews'.

**Expiration Section:**

- Access package assignments expire:** A dropdown menu is set to 'Number of days'.
- Assignments expire after (number of days):** A text input field contains the value '365'.
- Show advanced expiration settings:** A link to expand the configuration options.

**Access Reviews Section:**

- Require access reviews:** A toggle switch is set to 'Yes'.
- Starting on:** A date picker shows '03/01/2022'.
- Review frequency:** A dropdown menu is set to 'Bi-annually'.
- Duration (in days):** A text input field contains '90', with a note indicating 'Maximum 175'.
- Reviewers:** Radio buttons are present for 'Self-review' (selected), 'Specific reviewer(s)', and 'Manager'.

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:** (SHOW ANSWER)

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

#### NEW QUESTION: 132

You have a Microsoft 365 subscription that is onboarded to Microsoft Entra Permissions Management.

You need to identify managed identities that are assigned permissions and remove any permissions that have been unused for 90 days. The solution must minimize administrative effort.

What should you do in the Entra Permissions Management portal?

- A. Configure an Autopilot rule.
- B. Schedule a Permissions analytics report.
- C. From Microsoft Entra Insights, review Service principals with privileged role assignments.
- D. Run an audit query.

**Answer:** (SHOW ANSWER)

Microsoft Entra Permissions Management includes an Autopilot feature that allows you to create prebuilt or custom rules to automatically remediate permissions based on usage patterns, including removing unused permissions after a specified period such as 90 days.

The Remediation tab in the Permissions Management portal supports Autopilot rules to automate right-sizing of permissions, reducing manual effort.

**NEW QUESTION: 133**

You have a Microsoft 365 tenant.

All users have mobile phones and Windows 10 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 laptops 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. Windows Hello for Business
- B. a notification through the Microsoft Authenticator app
- C. security questions
- D. voice

Answer: (SHOW ANSWER)

**NEW QUESTION: 134**

You configure Azure Active Directory (Azure AD) Password Protection as shown in the exhibit.

(Click the Exhibit tab.)

Custom smart lockout

Lockout threshold ⓘ 5 ✓

Lockout duration in seconds ⓘ 3600 ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

Custom banned password list ⓘ

- Contoso ✓
- Litware
- Tailwind
- project
- Zettabyte
- MainStreet

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ Yes No

Mode ⓘ Microsoft Enforced Audit

You are evaluating the following passwords:

- Pr0jectlitw@re
- T@ilw1nd
- C0nt0s0

Which passwords will be blocked?

- A. Pr0jectlitw@re and T@ilw1nd only
- B. C0nt0s0 only
- C. C0nt0s0, Pr0jectlitw@re, and T@ilw1nd

- D. C0nt0s0 and T@ilw1nd only
- E. C0nt0s0 and Pr0jectlitw@re only

Answer: (SHOW ANSWER)

After normalization we have :

- Pr0jectlitw@re - > projectlitware = 2 points
- T@ilw1nd -> tailwind =1 point
- C0nt0s0 -> contoso = 1 point

You need 5 points therefore everything is blocked.

NEW QUESTION: 135

You have a Microsoft 365 subscription.

You have an Azure subscription that contains an Azure App Service web app named App1.

You have multiple devices that run Windows and are enrolled in Microsoft Intune.

You deploy the Global Secure Access client to the devices by using Intune.

You need to configure private access to App1.

What should you do next?

- A. Configure a traffic forwarding profile.
- B. Deploy a private network connector.
- C. Create a remote network.
- D. Create an application security group.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 136

Hotspot Question

You have a Microsoft Entra ID P2 tenant that contains four users named User1, User2, User3, and User4. The tenant contains the groups shown in the following table.

| Name   | Owner | Members             |
|--------|-------|---------------------|
| Group1 | User2 | User1, User3, User4 |
| Group2 | User2 | User2               |

Group2 is onboarded to Privileged Identity Management (PIM).

You assign Group2 the roles shown in the following table.

| Member | Role   | Assignment type |
|--------|--------|-----------------|
| User1  | Member | Eligible        |
| Group1 | Member | Eligible        |
| User4  | Owner  | Active          |

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                    |
| User2 can request to become a member of Group1 by using PIM. | <input type="radio"/> | <input type="radio"/> |
| User3 can request to become a member of Group2 by using PIM. | <input type="radio"/> | <input type="radio"/> |
| User4 can request to become a member of Group2 by using PIM. | <input type="radio"/> | <input type="radio"/> |

Answer:

| Answer Area                                                  |                                  |                                  |
|--------------------------------------------------------------|----------------------------------|----------------------------------|
| Statements                                                   | Yes                              | No                               |
| User2 can request to become a member of Group1 by using PIM. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can request to become a member of Group2 by using PIM. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User4 can request to become a member of Group2 by using PIM. | <input type="radio"/>            | <input checked="" type="radio"/> |

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 137

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. 90 days
- C. 180 days
- D. 60 days

Answer: (SHOW ANSWER)

NEW QUESTION: 138

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 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 Set-MsolUserLicense cmdlet
- B. the Set-AzureADGroup cmdlet
- C. the Set-WindowsProductKey cmdlet

**D.** the Administrative units blade in the Azure Active Directory admin center

**Answer:** ([SHOW ANSWER](#))

The Set-MsolUserLicense cmdlet updates the license assignment for a user. This can include adding a new license, removing a license, updating the license options, or any combination of these actions.

Note:

There are several versions of this QUESTION 11 in the exam. The QUESTION 11 has two possible correct answers:

the Licenses blade in the Azure Active Directory admin center

the Set-MsolUserLicense cmdlet

Other incorrect answer options you may see on the exam include the following:

the Identity Governance blade in the Azure Active Directory admin center

the Set-WindowsProductKey cmdlet

the Set-AzureAdGroup cmdlet

Reference:

<https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0>

### NEW QUESTION: 139

You have a Microsoft 365 subscription.

You need to create a Conditional Access policy that will use a Global Secure Access security profile. The solution must ensure that users are prevented from accessing websites that include the word gambling in the URL.

What should you do first?

**A.** Create a web content filtering policy.

**B.** Create a named location.

**C.** Configure the Adaptive Access settings.

**D.** Create a network security group (NSG).

**Answer:** ([SHOW ANSWER](#))

Configure Global Secure Access web content filtering

Web content filtering empowers you to implement granular Internet access controls for your organization based on website categorization.

Microsoft Entra Internet Access's first Secure Web Gateway (SWG) features include web content filtering based on domain names. Microsoft integrates granular filtering policies with Microsoft Entra ID and Microsoft Entra Conditional Access, which results in filtering policies that are user- aware, context-aware, and easy to manage.

Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-configure-web-content-filtering>

### NEW QUESTION: 140

#### SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@XXYyz112233.onmicrosoft.com

Microsoft 365 Password: =1122334455667788

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

Lab Instance: 99999999

You need to assign a Windows 10/11 Enterprise E3 license to the sg-Retail group.

To complete this task, sign in to the appropriate admin center.

Answer:

To assign a license to a group

Step 1: Sign in to the Microsoft Entra admin center as at least a License Administrator.

Step 2: Browse to Identity > Billing > Licenses.

Step 3: Select the name of the license plan [Select Windows 10/11 Enterprise E3 license] you want to assign to the group.

[Home](#) > [Licenses](#)

 Licenses | All products

Contoso - Microsoft Entra ID for workforce

«

[+ Try / Buy](#) [+ Assign](#) [Bills](#) | [Columns](#) | [Got feedback?](#)

Overview

Diagnose and solve problems

Manage

Licensed features

All products

| <input type="checkbox"/>            | Name                          | Total   | Assigned | Available | Expiring soon |
|-------------------------------------|-------------------------------|---------|----------|-----------|---------------|
| <input type="checkbox"/>            | Microsoft Fabric (Free)       | 1000000 | 9        | 999991    | 0             |
| <input checked="" type="checkbox"/> | Microsoft Power Automate Free | 10000   | 2        | 9998      | 0             |

Step 4: On the Product page, select Assign.

[Home](#) > [Licenses](#)

 Licenses | All products

Contoso - Microsoft Entra ID for workforce

«

[+ Try / Buy](#) [+ Assign](#) [Bills](#) | [Columns](#) | [Got feedback?](#)

Overview

Diagnose and solve problems

Manage

Licensed features

All products

Self-service sign up products

Activity

Audit logs

Troubleshooting + Support

New support request

| <input type="checkbox"/>            | Name                          | Total   | Assigned | Available | Expiring soon |
|-------------------------------------|-------------------------------|---------|----------|-----------|---------------|
| <input checked="" type="checkbox"/> | Microsoft Fabric (Free)       | 1000000 | 9        | 999991    | 0             |
| <input type="checkbox"/>            | Microsoft Power Automate Free | 10000   | 2        | 9998      | 0             |

Step 5: On the Assign page, select Users and groups, and then search for and select the group you're assigning the license.  
[Select the sg-Retail group]

Add users and groups

Try changing or adding filters if you don't see what you're looking for.

Search

mdm

1 result found

All

Users

Groups

|                                     | Name                                                                                                | Type  | Email |
|-------------------------------------|-----------------------------------------------------------------------------------------------------|-------|-------|
| <input checked="" type="checkbox"/> |  MDM policy – West | Group |       |

Selected (1)

Reset

 MDM policy – West

Select

Step 6: Select Assignment options, make sure you have the appropriate license options turned on, and then select OK.

Dashboard > Company Name cDeQx > Licenses - Overview > Products > Microsoft Dynamics

Assign license

Company Name cDeQx

Users and groups

1 group selected

Assignment options

Assignment options

Microsoft Dynamics CRM Online

Flow for Dynamics 365

Microsoft Dynamics CRM Online Professional

Microsoft Dynamics Marketing Sales Collaboration – Eligibility criteria apply

Microsoft Social Engagement Professional – Eligibility Criteria apply

Off

On

Off

On

Off

On

Off

On



The Assign license page updates to show that a user is selected and that the assignments are configured.

Step 7: Select Assign.

The group is added to the list of licensed groups and all of the members have access to the included Microsoft Entra services.

Reference:

<https://learn.microsoft.com/en-us/entra/fundamentals/license-users-groups>

#### NEW QUESTION: 141

You have a Microsoft 365 tenant.

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

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

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

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

What should you use to gather the information?

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

**Answer: C (LEAVE A REPLY)**

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

#### NEW QUESTION: 142

You have an Azure subscription that contains a user named User1.

The App registration settings for the Azure AD tenant are configured as shown in the following exhibit.



User1 builds an ASP.NET web app named App1.

You need to ensure that User1 can register App1. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Application Developer
- B. Cloud App Security Administrator
- C. Cloud Application Administrator
- D. Application Administrator

**Answer:** ([SHOW ANSWER](#))

Assign the Application Developer role to grant the ability to create application registrations when the Users can register applications setting is set to No. This role also grants permission to consent on one's own behalf when the Users can consent to apps accessing company data on their behalf setting is set to No.

#### NEW QUESTION: 143

<https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#grant-individual-permissions-to-create-and-consent-to-applications-when-the-default-ability-is-disabled>

You have a Microsoft Entra tenant that contains 1,000 users. The users are assigned Microsoft Entra Suite licenses.

You are deploying Global Secure Access.

You need to ensure that connections to www.microsoft.com are bypassed by Global Secure Access.

Which profiles should you update?

- A. Internet access profile only
- B. Microsoft traffic profile only
- C. Microsoft traffic profile and Internet access profile only
- D. Microsoft traffic profile, Private access profile, and Internet access profile

**Answer:** ([SHOW ANSWER](#))

Global Secure Access, How to manage the Internet Access traffic forwarding profile The Internet Access traffic forwarding profile routes internet traffic through the Global Secure Access client. Enabling this traffic forwarding profile allows remote workers to connect to the internet in a controlled and secure way. With the features of Microsoft Entra Internet Access, you can control which internet sites can be accessed. You can also configure which traffic to exclude from Global Secure Access based on IP addresses, IP address ranges, IP subnets, and Fully Qualified Domain Names (FQDNs).

Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-manage-internet-access-profile>

#### NEW QUESTION: 144

Your company has an Azure Active Directory (Azure AD) tenant named contosri.com. The company has the business partners shown in the following table.

| Name           | Description                                                                                  |
|----------------|----------------------------------------------------------------------------------------------|
| Fabrikam, Inc. | An Azure AD tenant that has two verified domains named fabrikam.com and adatum.com           |
| Litware, Inc.  | A third-party identity provider that uses the domain names of litwareinc.com and contoso.com |

Users can request access by using package 1.

Users at Fabrikam and Litware use ail then respective domain names for email addresses.

You plan to create an access package named packagel that will be accessible only to the Fabrikam and Litware users.

You need to configure connected organizations for Fabrikam and litware so that any of their users can request access by using package1.

What is the minimum of connected organization that you should create?

- A. 1
- B. 3
- C. 2
- D. 4

Answer: (SHOW ANSWER)

NEW QUESTION: 145

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 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. Update-MgOrganization
- B. Update-MgPolicyPermissionGrantPolicyExclude
- C. Update-MgDomain
- D. Update-MgDomainFederationConfiguration

Answer: (SHOW ANSWER)

The Update-MgPolicyPermissionGrantPolicyExclude cmdlet is used to exclude a policy from being applied to a specific set of users. In this case, you can use the cmdlet to exclude the self- service sign-up policy from being applied to users with the contoso.com SMTP address space.

NEW QUESTION: 146

Hotspot Question

You have a Microsoft 365 tenant named contoso.com.

Guest user access is enabled.

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

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

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

Collaboration restrictions

- ☐ Allow invitations to be sent to any domain (most inclusive)
- ☐ Deny invitations to the specified domains
- ☒ Allow invitations only to the specified domains (most restrictive)

 Delete

☒ TARGET DOMAINS

☐ Outlook.com



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

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

Answer:  
Answer Area

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

Explanation:

Box 1: Yes

Invitations can only be sent to outlook.com. Therefore, User1 can accept the invitation and access the application.

Box 2: Yes

Invitations can only be sent to outlook.com. However, User2 has already received and accepted an invitation so User2 can access the application.

Box 3. No  
Invitations can only be sent to outlook.com. Therefore, User3 will not receive an invitation.

**NEW QUESTION: 147**

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

**Answer:** (SHOW ANSWER)

From October 13, 2020 onward, only these versions of Office are supported for connecting to Microsoft 365 (and Office 365) services: Microsoft 365 Apps for enterprise (previously named Office 365 ProPlus) Microsoft 365 Apps for business (previously named Office 365 Business) Office LTSC 2021, such as Office LTSC Professional Plus 2021 Office 2019, such as Office Professional Plus 2019 Office 2016, such as Office Standard 2016 Note: Office 2019 and Office 2016 will be supported for connecting to Microsoft 365 (and Office 365) services until October 2023. Note: Client software: To support tenant restrictions, client software must request tokens directly from Azure AD, so that the proxy infrastructure can intercept traffic. Browser-based Microsoft 365 applications currently support tenant restrictions, as do Office clients that use modern authentication (like OAuth 2.0).

Reference:  
<https://docs.microsoft.com/en-us/deployoffice/endofsupport/microsoft-365-services-connectivity>  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/tenant-restrictions>

**NEW QUESTION: 148**

You have a Microsoft 365 tenant. The Azure Active Directory (Azure AD) tenant syncs to an on-premises Active Directory domain. The domain contains the servers shown in the following table.

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

The domain controllers are prevented from communicating to the internet. You implement Azure AD Password Protection on Server1 and Server2. You deploy a new server named Server4 that runs Windows Server 2019. You need to ensure that Azure AD Password Protection will continue to work if a single server fails. What should you implement on Server4?

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

**Answer:** (SHOW ANSWER)

The AzureAD Password Protection proxy service initiates an outbound connection (Port 443) to Azure to pull the banned password list. The downloaded banned password list is pulled by the agent installed on DCs.

NEW QUESTION: 149

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc. Litware has offices in Boston and Seattle, but has employees located across the United States. Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

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

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- \* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- \* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- \* Use custom catalogs and custom programs for Identity Governance.
- \* Ensure that User1 can create enterprise applications in Azure AD.
- \* Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicensesto the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicensesattribute. Users who have the appropriate value for LWLicensesmust be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

#### Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- \* Implement multi-factor authentication (MFA) for all Litware users.
- \* Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- \* Implement a banned password list for the litware.com forest.
- \* Enforce MFA when accessing on-premises applications.
- \* Automatically detect and remediate externally leaked credentials.

#### Requirements. Access Requirements

Litware identifies the following access requirements:

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

#### Requirements. Monitoring Requirements

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

You need to meet the authentication requirements for leaked credentials.

What should you do?

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

**Answer:** ([SHOW ANSWER](#))

Password hash synchronization

Risk detections like leaked credentials require the presence of password hashes for detection to occur. For more information about password hash synchronization, see the article, Implement password hash synchronization with Azure AD Connect sync.

Reference:

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

#### NEW QUESTION: 150

You have a Microsoft 365 subscription that uses Microsoft Defender for Cloud Apps.

You have multiple third-party apps that access the resources in the subscription.

You need to monitor the access of the third-party apps.

What should you create?

- A.** an endpoint protection policy
- B.** an access policy
- C.** an app permission policy
- D.** an OAuth app policy

**Answer:** ([SHOW ANSWER](#))

#### NEW QUESTION: 151

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 Site1. 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.

**Answer:** (SHOW ANSWER)

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

**NEW QUESTION: 152**

You have a Microsoft Entra tenant that contains a terms of use (ToU) named Terms1.

You create a Conditional Access policy named Policy1 to deploy Terms1.

You need to configure Policy1 to require users to accept Terms1.

Which settings should you configure for Policy1?

- A.** Conditions
- B.** Session
- C.** Grant
- D.** Target resources

**Answer:** B (LEAVE A REPLY)

To enforce Terms of Use (ToU) acceptance in a Conditional Access policy, you must configure it under the Grant section :

<https://learn.microsoft.com/en-us/entra/identity/conditional-access/policy-all-users-require-terms- of-use>

**NEW QUESTION: 153**

Drag and Drop Question

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

| Name    | Type            | Description                     |
|---------|-----------------|---------------------------------|
| User1   | User            | Not applicable                  |
| User2   | User            | Not applicable                  |
| 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.

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:

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

User1:

The Key Vault Secrets Officer RBAC role

User2:

The Key Vault Secrets User RBAC role

**NEW QUESTION: 154**

You have an Azure subscription named Sub1 that contains a virtual machine named VM1.

You need to enable Microsoft Entra login for VM1 and configure VM1 to access the resources in Sub1.

Which type of identity should you assign to VM1?

- A.** Microsoft Entra user account
- B.** user-assigned managed identity
- C.** Azure Automation account
- D.** system-assigned managed identity

**Answer:** ([SHOW ANSWER](#))

System-assigned managed identity: This type of managed identity is enabled directly on an Azure resource. In this case, enabling a system-assigned managed identity on VM1 would allow VM1 to authenticate with other Azure resources within Sub1, using the identity associated with VM1.

**NEW QUESTION: 155**

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

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

You have a Microsoft 365 E5 subscription.

You create a user named User1.

You need to ensure that User1 can update the status of Identity Secure Score improvement actions.

Solution: You assign the Security Operator role to User1.

Does this meet the goal?

- A.** Yes
- B.** No

**Answer:** ([SHOW ANSWER](#))

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>

**NEW QUESTION: 156**

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. Entitlement management settings
- C. Terms of use
- D. Access reviews

Answer: (SHOW ANSWER)

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users#manage-the-lifecycle-of-external-users>

NEW QUESTION: 157

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

| Name   | Role                                                                                             |
|--------|--------------------------------------------------------------------------------------------------|
| Admin1 | Cloud application administrator                                                                  |
| Admin2 | Application administrator                                                                        |
| Admin3 | Security administrator                                                                           |
| User1  | None  Microsoft |

You add an enterprise application named App1 to Azure AD and set User1 as the owner of App1.

App1 requires admin consent to access Azure AD before the app can be used.

You configure the Admin consent requests settings as shown in the following exhibit.

Admin consent requests

Users can request admin consent to apps they are unable to consent to ? Yes No

Who can review admin consent requests ?

| Reviewer type    | Reviewers        |
|------------------|------------------|
| Users            | 4 users selected |
| Groups (Preview) | + Add groups     |
| Roles (Preview)  | + Add roles      |

Selected users will receive email notifications for requests ? Yes No

Selected users will receive request expiration reminders ? Yes No

Consent request expires after (days) ?  30

Admin1, Admin2, Admin3, and User1 are added as reviewers.

Which users can review and approve the admin consent requests?

- A. Admin1 only
- B. Admin1, Admin2 and Admin3 only
- C. Admin1, Admin2, and User1 only
- D. Admin1 and Admin2 only
- E. Admin1, Admin2, Admin3, and User1

Answer: [SHOW ANSWER](#)

To approve requests, a reviewer must be a global administrator, cloud application administrator, or application administrator. The reviewer must already have one of these admin roles assigned; simply designating them as a reviewer doesn't elevate their privileges.

<https://learn.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow>

NEW QUESTION: 158

Hotspot Question

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

| Name  | Microsoft Role                          |
|-------|-----------------------------------------|
| User1 | None                                    |
| User2 | Privileged authentication administrator |
| User3 | Global administrator                    |

In Azure AD Privileged Identity Management (PIM), you configure the Global administrator role as shown in the following exhibit.

|  Edit |           |
|----------------------------------------------------------------------------------------|-----------|
| Setting                                                                                | State     |
| Activation maximum duration (hours)                                                    | 1 hour(s) |
| Require justification on activation                                                    | Yes       |
| Require ticket information on activation                                               | No        |
| On activation, require Azure MFA                                                       | Yes       |
| Require approval to activate                                                           | No        |
| Approvers                                                                              | None      |
| Assignment                                                                             |           |
| Setting                                                                                | State     |
| Allow permanent eligible assignment                                                    | Yes       |
| Expire eligible assignments after                                                      | -         |
| Allow permanent active assignment                                                      | Yes       |
| Expire active assignments after                                                        | -         |

|                                                                |     |
|----------------------------------------------------------------|-----|
| Require Azure Multi-Factor Authentication on active assignment | No  |
| Require justification on active assignment                     | Yes |

User1 is eligible for the Global administrator role.  
For each of the following statements, select Yes if the statement is true. Otherwise, select No.  
NOTE: Each correct selection is worth one point.

Answer Area

| Statements                                                                                        | Yes                   | No                    |
|---------------------------------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role. | <input type="radio"/> | <input type="radio"/> |
| User2 must approve all activation requests for the Global administrator role.                     | <input type="radio"/> | <input type="radio"/> |
| User2 and User3 can edit the Global administrator role assignment.                                | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                                                                        | Yes                              | No                               |
|---------------------------------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global administrator role. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 must approve all activation requests for the Global administrator role.                     | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 and User3 can edit the Global administrator role assignment.                                | <input type="radio"/>            | <input checked="" type="radio"/> |

Explanation:

Box 1: Yes

MFA is required on activation

Box 2: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

Box 3: No

The Privileged Authentication Administrator can set or reset any authentication method for any user, including Global Administrators.

The Privileged Role Administrator can manage role assignments, including the Global Administrator role, in Azure Active Directory, as well as within Azure AD Privileged Identity Management. In addition, this role allows management of all aspects of Privileged Identity Management and administrative units.

#### NEW QUESTION: 159

Your organization has implemented Azure AD Connect to help support its Hybrid cloud initiatives and has synced all on-prem AD users to Azure AD. To meet organization compliance requirements, you need to ensure you can enforce password policies and limit sign-in hours for your users. Your solution should require the least administrative overhead. Which cloud authentication method should you use?

- A. Hybrid Authentication
- B. Federated Authentication
- C. Azure AD Password Hash synchronization
- D. Azure AD Pass-through authentication

Answer: (SHOW ANSWER)

Azure AD pass-through authentication ensures that all authentications occur on-premise as opposed to in the cloud. By authenticating users by the on-premise Active Directory, you are able to enforce password policies and limit the sign in hours for your users. This option meets your requirements.

Reference:

<https://docs.microsoft.com/en-us/learn/modules/implement-manage-hybrid-identity/2-plan-design-implement-azure-active-directory-connect>

**NEW QUESTION: 160**

Hotspot Question

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

Enabled for users to sign-in? ⓘ ☒ Yes ☐ No

Name ⓘ  

Homepage URL ⓘ  

Logo ⓘ   

User access URL ⓘ  

Application ID ⓘ  

Object ID ⓘ  

Terms of Service Url ⓘ  

Privacy Statement Url ⓘ  

Reply Url ⓘ  

User assignment required? ⓘ ☐ Yes ☒ No

Visible to users? ⓘ ☒ Yes ☐ No

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.  
NOTE: Each correct selection is worth one point.

Answer Area

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

All users

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

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

all users

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

Answer:

Answer Area

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

All users

No one

Only users listed on the Owners blade

Only users listed on the Users and groups blade

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

all users

no one

only users listed on the Owners blade

only users listed on the Users and groups blade

Explanation:

Box 1: All users

"Enable for users to sign-in" is selected and "User assignment required" is set to No. Any user can login using the app url.

Box 2: Only users listed on the users and groups blade

User assignment required - This option does not affect whether or not an application appears on My Apps. To show the application there, assign an appropriate user or group to the application.

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

**NEW QUESTION: 161**

Hotspot Question

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

| Name   | Member of      |
|--------|----------------|
| Admin1 | Group1         |
| Admin2 | Group2         |
| Admin3 | Group1, Group2 |

You add the following assignment for the User Administrator role:

- Scope type: Directory
- Selected members: Group1
- Assignment type: Active
- Assignments starts: August 15, 2022
- Assignment ends: December 15, 2022

You add the following assignment for the Exchange Administrator role:

- Scope type: Directory
- Selected members: Group2
- Assignment type: Eligible
- Assignments starts: October 15, 2022
- Assignment ends: January 15, 2023

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**

On November 15, 2022, Admin1 can reset the password of Admin2.

**Yes**

**No**

☐☐

On October 15, 2022, Admin2 signs in and can administer Exchange Online.

☐☐

On September 1, 2022, Admin3 can reset the password of Admin1.

☐☐

**Answer:**

Answer Area

Microsoft

Statements

Yes

No

On November 15, 2022, Admin1 can reset the password of Admin2.

☒

☐

On October 15, 2022, Admin2 signs in and can administer Exchange Online.

☐

☒

On September 1, 2022, Admin3 can reset the password of Admin1.

☒

☐

NEW QUESTION: 162

Hotspot Question

You have a Microsoft Entra tenant named contoso.com that contains a user named User1.

User1 has the devices shown in the following table:

| Name    | Platform   | Registered in contoso.com |
|---------|------------|---------------------------|
| Device1 | Windows 11 | Yes                       |
| Device2 | Windows 11 | No                        |
| Device3 | iOS        | Yes                       |

On November 5, 2025, you create and enforce terms of use in contoso.com that has the following settings:

- Name: Terms1
- Display name: Contoso terms of use
- Require users to expand the terms of use: On
- Require users to consent on every device: On
- Expire consents: On
- Expire starting on: December 10, 2025
- Frequency: Monthly

On November 15, 2025, User1 accepts Terms1 on Device3.

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

NOTE: Each correct selection is worth one point.

Answer Area

Microsoft

Statements

Yes

No

On November 20, 2025, User1 can accept Terms1 on Device1.

☐

☐

On December 11, 2025, User1 can accept Terms1 on Device2.

☐

☐

On December 7, 2025, User1 can accept Terms1 on Device3.

☐

☐

Answer:

Answer Area

| Statements                                                | Yes                                 | No                                  |
|-----------------------------------------------------------|-------------------------------------|-------------------------------------|
| On November 20, 2025, User1 can accept Terms1 on Device1. | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| On December 11, 2025, User1 can accept Terms1 on Device2. | <input checked="" type="checkbox"/> | <input type="checkbox"/>            |
| On December 7, 2025, User1 can accept Terms1 on Device3.  | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

NEW QUESTION: 163

Hotspot Question

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the identities shown in the following table.

| Name   | Type           | Role                             |
|--------|----------------|----------------------------------|
| User1  | User           | Helpdesk Administrator           |
| User2  | User           | Conditional Access Administrator |
| Group1 | Group          | Global Administrator             |
| Group2 | Group          | Exchange Administrator           |
| App1   | Registered app | Authentication Administrator     |

The tenant is onboarded to Permissions Management.

You create the Azure resources shown in the following table.

| Name         | Type              | Role                            |
|--------------|-------------------|---------------------------------|
| Managed1     | Managed identity  | Owner                           |
| Managed2     | Managed identity  | Cloud Application Administrator |
| SPPrincipal1 | Service principal | Security Operator               |

From Microsoft Entra Insights, which identity will be included in Accounts assigned to highly privileged roles, and which identity will be included in Service principals with privileged role assignments?

Answer Area



Accounts assigned to highly privileged roles:

User1  
User2  
Group1  
Group2

Service principals with privileged role assignments:

App1  
Managed1  
Managed2  
SPrincipal1

Answer:

Answer Area

Accounts assigned to highly privileged roles:

User1  
User2  
Group1  
Group2

Service principals with privileged role assignments:

App1  
Managed1  
Managed2  
SPrincipal1

NEW QUESTION: 164

You have a Microsoft Entra tenant.  
You have the end-user desktop environments shown in the following table.

| Name              | Description                                                                                  |
|-------------------|----------------------------------------------------------------------------------------------|
| Office staff      | Contains Windows 11 devices that are Microsoft Entra joined                                  |
| Contractors       | Contains Windows 11 devices that are Microsoft Entra registered                              |
| Frontline workers | Contains Windows 11 Enterprise multi-session remote desktops that are Microsoft Entra joined |
| Senior managers   | Contains Windows 11 single session hosts that are Microsoft Entra joined                     |
| Developers        | Contains Windows 365 devices that are Microsoft Entra joined                                 |

You need to deploy Global Secure Access.

In which environments can you install the Global Secure Access client?

- A.** Contractors, Developers, Frontline workers, Office staff, and Senior managers
- B.** Frontline workers and Senior managers only
- C.** Contractors and Office staff only
- D.** Developers, Office staff, and Senior managers only

**Answer:** ([SHOW ANSWER](#))

\* Office staff - yes

The client requires a 64-bit version of Windows 10 or 11 and local administrator credentials for installation or upgrade.

\* Contractors - No [Not A, not C]

To successfully deploy the Global Secure Access client, devices must be either Entra joined or Entra hybrid joined. Microsoft Entra registered devices are not supported.

\* Frontline workers - No [Not A, not B]

Azure Virtual Desktop single-session is supported, but multi-session is not.

\* Senior Managers - Yes

Azure Virtual Desktop single-session is supported.

\* Developers - Yes

Windows 365 is also supported.

Reference:

<https://learn.microsoft.com/en-us/entra/global-secure-access/how-to-install-windows-client>

#### NEW QUESTION: 165

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.

**Answer:** ([SHOW ANSWER](#))

One of the prerequisites to using a session policy is "The relevant apps should be deployed with Conditional Access App Control", which is done via the Azure AD Admin Center.

<https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy-aad#prerequisites-to-using-session-policies>

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

#### NEW QUESTION: 166

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.** a smartcard
- B.** a mobile app code

- C. a mobile app notification
- D. an email to an address outside your organization

Answer: (SHOW ANSWER)

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>

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 167

Hotspot Question

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.

| 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:

| 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 checked="" type="radio"/> |
| User3 can sign in from an anonymous IP address.               | <input checked="" type="radio"/> | <input type="radio"/>            |

Explanation:

Box 1: No

Blocked access prevents self-remediation through password resets & Azure AD MFA.

Box 3: No

Blocked access prevents self-remediation through password resets & Azure AD MFA Box 3: Yes Anonymous IP address sign-in risk is Medium.

NEW QUESTION: 168

Hotspot Question

You have an Azure subscription named Sub1 that contains two storage accounts named storage1 and storage2 and the blob containers shown in the following table.

| Name  | In storage account | Contains blob named |
|-------|--------------------|---------------------|
| cont1 | storage1           | blob1               |
| cont2 | storage1           | blob2               |
| cont1 | storage2           | blob3               |

Sub1 contains the users shown in the following table.

| Name  | Role                     | Scope    | Role assignment condition |
|-------|--------------------------|----------|---------------------------|
| User1 | Reader                   | Sub1     | Not applicable            |
|       | Storage Blob Data Reader | Sub1     | Condition1                |
| User2 | Reader                   | Sub1     | Not applicable            |
|       | Storage Blob Data Owner  | storage1 | Condition2                |

Condition1 has the following definition:



# Microsoft

```
(
  (
    !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1'
  )
)
```

Condition2 has the following definition:

```
(
  (
    !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'})
  )
  OR
  (
    @Resource[Microsoft.Storage/storageAccounts/blobServices/containers/blobs:path] StringLike '*2*'
  )
)
```

NOTE: Each correct selection is worth one point.

## Answer Area



### Statements

Yes

No

User1 can read the contents of blob2.

☐☐

User1 can read the contents of blob3.

☐☐

User2 can read the contents of blob1.

☐☐

Answer:

Answer Area

Statements

|                                       | Yes                              | No                               |
|---------------------------------------|----------------------------------|----------------------------------|
| User1 can read the contents of blob2. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User1 can read the contents of blob3. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can read the contents of blob1. | <input checked="" type="radio"/> | <input type="radio"/>            |

Explanation:

Box 1: No

User1 has the Reader role. Does not apply to the blob container.

User1 also has the Storage Blob Data Reader with Condition1.

Blob2 is in Cont2.

Condition1 will be false:

The action is ..blob/reads

Resource name is cont2 not cont1

Note: Storage Blob Data Reader

Read and list Azure Storage containers and blobs.

Box 2: Yes

Blob3 is in cont1. Condition1 will be true.

Box 3: Yes

User2 has the Reader role. Does not apply to the blob container.

User2 also has the Storage Blob Data Owner Role with Condition2.

blob1 is in cont1

Condition2 will be true, as the action is read, not a write.

NEW QUESTION: 169

Hotspot Question

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.

**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:

**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

Explanation:

After you delete an app registration, the app remains in a suspended state for 30 days. During that 30-day window, the app registration can be restored, along with all its properties.

Box 1: App1, App2, App3, and App4

Box 2: App roles, Users and groups, client secrets, and Self-service

<https://learn.microsoft.com/en-us/entra/identity-platform/howto-restore-app>

NEW QUESTION: 170

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: Admin1
- 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?

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

**Answer: A (LEAVE A REPLY)**

User assignment and Visible to Users goes hand in hand for this.  
If Visible to Users is set to Yes then this is the explanation from the 'i' next to it:  
If this option is set to yes, then assigned users will see the application on My Apps and O365 app launcher. If this option is set to no, then no users will see this application on their My Apps and O365 launcher. Assigned User is the key here.

Unless the users are assigned to the app, then No one will see the application on their MyApps or O365 Launcher.  
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>  
<https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces>

**NEW QUESTION: 171**

Hotspot Question

You have a Microsoft 365 E5 subscription that contains two groups named Group1 and Group2 and the users shown in the following table.

| Name  | Department | Member of |
|-------|------------|-----------|
| User1 | Marketing  | Group1    |
| User2 | marketing  | Group2    |
| User3 | HR         | Group1    |

Group2 is a member of Group1.  
You configure cross-tenant synchronization with a partner organization named fabrikam.com by using the following configurations:

- Provisioning status: On
- Users and groups: Group1
- Prevent accidental deletion: 500
- Scope: Sync only assigned users and groups
- Scoping filter: Department EQUALS Marketing

From the Cross-tenant synchronization settings, you set Provisioning Mode to Automatic.  
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

Microsoft

| Statements                                                               | Yes                   | No                    |
|--------------------------------------------------------------------------|-----------------------|-----------------------|
| User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

Microsoft

| Statements                                                               | Yes                              | No                               |
|--------------------------------------------------------------------------|----------------------------------|----------------------------------|
| User1 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 will be provisioned in the Microsoft Entra tenant of fabrikam.com. | <input type="radio"/>            | <input checked="" type="radio"/> |

Explanation:

Box 1: Yes  
User1 belongs to the Marketing Department, and is a member of Group1.  
Cross-tenant synchronization settings:  
\* Sync Group1  
\* Filter Department EQUALS Marketing  
Box 2: No  
User2 belongs to the marketing Department, and is a member of Group2.  
Group2 will not be synchronized.  
Box 3: No  
User3 belongs to the HR Department, and is a member of Group1.  
HR department will not be synchronized.

Your on-premises network contains an Active Directory Domain Services (AD DS) domain. The domain contains computers that run Windows 11.

You have a Microsoft 365 E5 subscription.

You plan to enable hybrid join and enroll the computers in Microsoft Intune.

You need to recommend the software that should be deployed to the domain, and the actions that should be performed in Intune.

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

NOTE: Each correct selection is worth one point.

Answer Area

Domain:

Intune:

Answer:

Answer Area

Domain:

Intune:

Explanation:

Box 1: The Intune Connector for Active Directory

Deploy Microsoft Entra hybrid joined devices by using Intune and Windows Autopilot Intune connector server requirements

- \* The Intune Connector for Active Directory must be installed on a computer that's running Windows Server 2016 or later with .NET Framework version 4.7.2 or later.
- \* The server hosting the Intune Connector must have access to the Internet and Active Directory.

Box 2: Modify the mobile device management (MDM) User scope

Set up Windows automatic MDM enrollment

1. Sign in to the Azure portal and select Microsoft Entra ID.
2. In the left hand pane, select Manage | Mobility (MDM and WIP) > Microsoft Intune.
3. Make sure users who deploy Microsoft Entra joined devices by using Intune and Windows are members of a group included in MDM User scope.
4. Use the default values in the MDM Terms of use URL, MDM Discovery URL, and MDM Compliance URL boxes, and then select Save.

Reference:

<https://learn.microsoft.com/en-us/autopilot/windows-autopilot-hybrid>

**NEW QUESTION: 173**

You have an Azure Active Directory (Azure AD) tenant named Contoso that contains a terms of use (Toll) 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.** sign-in logs
- B.** the Usage and Insights report
- C.** provisioning logs
- D.** audit logs

**Answer:** ([SHOW ANSWER](#))

View Azure AD audit logs

If you want to view more activity, Azure AD terms of use policies include audit logs. Each user consent triggers an event in the audit logs that is stored for 30 days.

You can view these logs in the portal or download as a .csv file.

To get started with Azure AD audit logs, use the following procedure:

1. Sign in to the Azure portal as a global administrator, security administrator, or Conditional Access administrator.
2. Browse to Azure Active Directory > Security > Conditional Access > Terms of use.
3. Select a terms of use policy.
4. Select View audit logs.
5. On the Azure AD audit logs screen, you can filter the information using the provided lists to target specific audit log information.

Reference:

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

**NEW QUESTION: 174**

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.

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

Answer: (SHOW ANSWER)

Modify the properties of the IT administrator user accounts is not like to modify admin review to assign a manager, so, Because admin review is not modified, Megan Brow as Fallback Reviewer will still receiving reviews, no manager has been assigned to admin review.

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

NEW QUESTION: 175

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the groups shown in the following table.

| Name   | Type          | Membership type | Security enabled | Role assignment allowed |
|--------|---------------|-----------------|------------------|-------------------------|
| Group1 | Security      | Assigned        | Yes              | No                      |
| Group2 | Security      | Assigned        | Yes              | Yes                     |
| Group3 | Microsoft 365 | Assigned        | Yes              | Yes                     |
| Group4 | Microsoft 365 | Assigned        | No               | No                      |

Which groups can you manage by using Privileged Identity Management (PIM)?

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

Answer: (SHOW ANSWER)

\* Group1 - Yes

Group1 is security enabled, role assignment is not allowed.

Group1 can be managed.

All security enabled groups can be manged by PIM.

Note: Groups in Microsoft Entra ID can be classified as either role-assignable or non-role- assignable. Additionally, any group can be enabled or not enabled for use with Microsoft Entra Privileged Identity Management (PIM) for Groups. These are independent properties of the group.

Any Microsoft Entra security group and any Microsoft 365 group (except dynamic membership groups and groups synchronized from on-premises environment) can be enabled in PIM for Groups. The group doesn't have to be role-assignable group to be enabled in PIM for Groups.

\* Group2 - Yes

Group2 is security enabled, role assignment is allowed.

Group2 can be managed.

All security enabled groups can be manged by PIM.

\* Group 3 - Yes

Group3 is security enabled, role assignment is allowed.

Group3 can be managed.

All security enabled groups can be manged by PIM.

\* Group4 - No

Group4 is not security enabled.

Reference:

<https://learn.microsoft.com/en-us/entra/id-governance/privileged-identity-management/concept- pim-for-groups>

NEW QUESTION: 176

You have a Microsoft 365 E5 subscription.

You create an access review named Review1. Review1 requires that every six months, Microsoft

365 group owners review guest user access to their groups.

You need to ensure that if the group owners fail to review the membership of Review1, guest users are removed automatically.

Which settings should you configure for Review1?

- A. Scheduling
- B. Reviewers
- C. When completed
- D. General

Answer: (SHOW ANSWER)

NEW QUESTION: 177

You have a Microsoft 365 E5 subscription and an Azure subscription.  
You plan to analyze Microsoft Entra sign-in logs by using Azure Monitor.  
You need to configure diagnostic settings for Microsoft Entra.  
Which destination should you configure for the sign-in logs?

- A. an Azure event hub
- B. an Azure SQL database
- C. a Log Analytics workspace
- D. an Azure Storage account

Answer: (SHOW ANSWER)

Integrate Microsoft Entra logs with Azure Monitor logs

A Log Analytics workspace allows you to collect data based on a variety or requirements, such as geographic location of the data, subscription boundaries, or access to resources.

Note: Use the integration of Microsoft Entra activity logs and Azure Monitor to perform the following tasks:

- \*-> Compare your Microsoft Entra sign-in logs against security logs published by Microsoft Defender for Cloud.
- \* Troubleshoot performance bottlenecks on your application's sign-in page by correlating application performance data from Azure Application Insights.
- \* Analyze the Identity Protection risky users and risk detections logs to detect threats in your environment.
- \* Identify sign-ins from applications still using the Active Directory Authentication Library (ADAL) for authentication.

Reference:

https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-integrate-activity-logs- with-azure-monitor-logs

NEW QUESTION: 178

Hotspot Question

You have a Microsoft 365 E5 subscription that contains a Microsoft Teams team named Team1 and two Microsoft 365 groups named Group1 and Group2. The subscription contains the users shown in the following table.

| Name  | Member of | Role                 |
|-------|-----------|----------------------|
| User1 | Group1    | None                 |
| User2 | Group2    | None                 |
| User3 | Group1    | Global Administrator |

You create an access package that has the following settings:

Name: Package1

Resource roles:

- o Team1: Owner

Users who can request access: For users in your directory

- o Specific Users and Groups: Group1

Require approval: Yes

- o Require requestor justification: No

- o How many stages: 1
  - o First Approver: Team1, User3
  - o Require approver justification: Yes
- Enable new requests: Yes
- Expiration:
- o Access package assignments expire: 7 days
  - o Users can request specific timeline: Yes
- For each of the following statements, select Yes if the statement is true. Otherwise, select No.
- NOTE: Each correct selection is worth one point.

| Statements                                             | Yes                   | No                    |
|--------------------------------------------------------|-----------------------|-----------------------|
| User1 can gain access to Team1 by requesting Package1. | <input type="radio"/> | <input type="radio"/> |
| User2 can gain access to Team1 by requesting Package1. | <input type="radio"/> | <input type="radio"/> |
| User3 can approve their own request for Package1.      | <input type="radio"/> | <input type="radio"/> |

Answer:

| Statements                                             | Yes                              | No                               |
|--------------------------------------------------------|----------------------------------|----------------------------------|
| User1 can gain access to Team1 by requesting Package1. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User2 can gain access to Team1 by requesting Package1. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User3 can approve their own request for Package1.      | <input type="radio"/>            | <input checked="" type="radio"/> |

NEW QUESTION: 179

You have accounts for the following cloud platforms:

- Azure
- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

You configure an Azure subscription to use Microsoft Entra Permissions Management to manage the permissions in Azure only.

Which additional cloud platforms can be managed by using Permissions Management?

- A. AWS only
- B. Alibaba Cloud and AWS only
- C. Alibaba Cloud and GCP only
- D. AWS and GCP only

E. Alibaba Cloud, AWS, and GCP

**Answer:** ([SHOW ANSWER](#))

Microsoft Entra Permissions Management is a cloud infrastructure entitlement management (CIEM) solution that provides comprehensive visibility into permissions assigned to all identities.

For example, over-privileged workload and user identities, actions, and resources across multicloud infrastructures in Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

#### NEW QUESTION: 180

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:** ([SHOW ANSWER](#))

<https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#helpdesk-administrator>

#### NEW QUESTION: 181

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

**Answer:** ([SHOW ANSWER](#))

Adding the GitHub app connector to Microsoft Defender for Cloud Apps will allow you to monitor OAuth authentication requests from GitHub to Microsoft 365. However, it will not allow you to monitor OAuth authentication requests to your AWS account, Google Workspace subscription, or Azure subscription.

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

#### NEW QUESTION: 182

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

You enable combined registration in interrupt mode.

You create a new user named User1.

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

NOTE: Each correct selection is worth one point.

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

**Answer:** ([SHOW ANSWER](#))

<https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>

- Hardware token is not an option to register.
- a one-time passcode email is not even listed.
- Windows Hello for Bussines is not even listed.

#### **NEW QUESTION: 183**

You have an Azure subscription that contains a virtual machine named VM1 and an Azure key vault named Vault1. VM1 has a system-assigned managed identity.

You need to ensure that VM1 can retrieve the values of secrets stored in Vault1. The solution must minimize administrative effort.

What should you do first?

- A.** Add a user-assigned managed identity to VM1.
- B.** Configure the Resource access settings for Vault1.
- C.** Assign an Azure role to VM1.
- D.** Configure the permissions model for Vault1.

**Answer:** ([SHOW ANSWER](#))

#### **NEW QUESTION: 184**

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:** ([SHOW ANSWER](#))

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

#### **NEW QUESTION: 185**

Case Study 2 - Litware, Inc

Overview

Litware, Inc. is a pharmaceutical company that has a subsidiary named Fabrikam, Inc.

Litware has offices in Boston and Seattle, but has employees located across the United States.

Employees connect remotely to either office by using a VPN connection.

Existing Environment. Identify Environment

The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.

Litware.com contains a user named User1 who oversees all application development.

Litware implements Azure AD Application Proxy.

Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.

Existing Environment. Cloud Environment

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

Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.

Existing Environment. On-premises Environment

The on-premises network contains the servers shown in the following table.

| Name    | Operating system    | Office | Description                                                                     |
|---------|---------------------|--------|---------------------------------------------------------------------------------|
| DC1     | Windows Server 2019 | Boston | Domain controller for litware.com                                               |
| SERVER1 | Windows Server 2019 | Boston | Member server in litware.com that runs the Azure AD Application Proxy connector |
| SERVER2 | Windows Server 2019 | Boston | Member server that uses Azure AD Connect                                        |

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.

Requirements. Delegation Requirements

Litware identifies the following delegation requirements:

- \* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
- \* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant.
- \* Use custom catalogs and custom programs for Identity Governance.
- \* Ensure that User1 can create enterprise applications in Azure AD.
- \* Use the principle of least privilege.

Requirements. Licensing Requirements

Litware recently added a custom user attribute named LWLicensesto the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicensesattribute.

Users who have the appropriate value for LWLicensesmust be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

Requirements. Management Requirements

Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.

Requirements. Authentication Requirements

Litware identifies the following authentication requirements:

- \* Implement multi-factor authentication (MFA) for all Litware users.
- \* Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
- \* Implement a banned password list for the litware.com forest.
- \* Enforce MFA when accessing on-premises applications.
- \* Automatically detect and remediate externally leaked credentials.

Requirements. Access Requirements

Litware identifies the following access requirements:

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

Requirements. Monitoring Requirements

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

Hotspot Question

You need to configure app registration in Azure AD to meet the delegation requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Azure AD tenant-level setting to modify:

▼

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

▼

Application administrator

Application developer

Cloud application administrator

Answer:

Answer Area

Azure AD tenant-level setting to modify:

▼

Allow users to register application

Users can consent to apps accessing company data on their behalf

Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

▼

Application administrator

Application developer

Cloud application administrator

Explanation:

1: Requirements for delegation clearly says " Prevent users to register applications"

2: User1 would need App Developer to register an app in tenant using "principle of least privilege"

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

**NEW QUESTION: 186**

You create a new Microsoft 365 E5 tenant.

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

What should you configure?

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

**Answer:** (SHOW ANSWER)

Examples for Sign-In Risk:

- Anonymous IP address
- Atypical travel
- Malware linked IP address
- Unfamiliar sign-in properties
- Leaked credentials
- Password spray

**NEW QUESTION: 187**

Hotspot Question

You have two Microsoft Entra tenants named contoso.com and fabrikam.com.

Contoso.com contains the users shown in the following table.

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

Contoso.com contains the groups shown in the following table.

| Name   | Membership type | Members       |
|--------|-----------------|---------------|
| Group1 | Assigned        | User1         |
| Group2 | Assigned        | Group1, User2 |

You configure cross-tenant synchronization from contoso.com to fabrikam.com and enable cross- tenant synchronization for User3 and Group2.

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements                       | Yes                   | No                    |
|----------------------------------|-----------------------|-----------------------|
| User1 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User2 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |
| User3 will sync to fabrikam.com. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements                       | Yes                              | No                               |
|----------------------------------|----------------------------------|----------------------------------|
| User1 will sync to fabrikam.com. | <input type="radio"/>            | <input checked="" type="radio"/> |
| User2 will sync to fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |
| User3 will sync to fabrikam.com. | <input checked="" type="radio"/> | <input type="radio"/>            |

NEW QUESTION: 188

Hotspot Question

You have a Microsoft Entra tenant that contains a user named User1.

You have an Azure subscription named Sub1. User1 is assigned the Owner role for Sub1.

You need to ensure that User1 can onboard Sub1 to Permissions Management. The solution must follow the principle of least privilege.

Which role should you assign for Sub1, and which role should you assign to User1 for the tenant?

To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Sub1:

Owner

Reader

Security Reader

User Access Administrator

Tenant:

Global Administrator

Global Secure Access Administrator

Permissions Management Administrator

Security Administrator

Answer:

Answer Area

Sub1:

Owner

Reader

Security Reader

User Access Administrator

Tenant:

Global Administrator

Global Secure Access Administrator

Permissions Management Administrator

Security Administrator

NEW QUESTION: 189

SIMULATION

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.  
To enter your password, place your cursor in the Enter password box and click on the password below.  
Microsoft 365 Username:admin@XXYyz112233.onmicrosoft.com  
Microsoft 365 Password: =1122334455667788  
If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.  
The following information is for technical support purposes only:  
Lab Instance: 99999999  
Your company is developing a new custom web app named App1.  
You need to register App1 with Microsoft Entra ID. Authenticated users must be redirected to the URI https://app1.contoso.com.  
To complete this task, sign in to the appropriate admin center.

**Answer:**

Register an application with the Microsoft identity platform.  
Registering your application establishes a trust relationship between your app and the Microsoft identity platform. The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around. Once created, the application object can't be moved between different tenants.

Specify who can use the application in the Supported account types section.

- Step 1: Sign in to the Microsoft Entra admin center.
- Step 2: If you have access to multiple tenants, use the Settings icon in the top menu to switch to the tenant in which you want to register the application from the Directories + subscriptions menu.
- Step 3: Browse to Identity > Applications > App registrations and select New registration.
- Step 4: Enter a display Name for your application. [Here: App1]
- Step 5: Specify who can use the application in the Supported account types section.
- Step 6: Redirect URI (optional). [Here: https://app1.contoso.com]
- Step 7: Select Register to complete the initial app registration.

[Home](#) > [Contoso AD \(dev\)](#) >

## Register an application

×

\* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Contoso AD (dev) only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼

e.g. https://myapp.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

Reference:

<https://learn.microsoft.com/en-us/graph/auth-register-app-v2>

#### NEW QUESTION: 190

Your organization is looking to tighten its security posture when it comes to Azure AD users passwords. There has been reports on local news recently of various organizations having user identities compromised due to using weak passwords or passwords that resemble the organization name or local sports team names. You want to provide protection for your organization as well as supplying a list of common words that are not acceptable passwords.

What should you configure.

- A. Azure AD Password Protection
- B. Azure AD Privileged Identity Management
- C. Azure Defender for Passwords
- D. Azure AD Multi-factor Authentication

Answer: [\(SHOW ANSWER\)](#)

Azure AD Password Protection is a feature that detects and blocks known weak passwords and their variants, and can also block additional weak terms that are specific to your organization or other local entities such as sports teams.

Reference:

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

#### NEW QUESTION: 191

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 Windows 10 computers to support Azure AD Seamless SSO.

What should you do?

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

Answer: (SHOW ANSWER)

You can gradually roll out Seamless SSO to your users using the instructions provided below.

You start by adding the following Azure AD URL to all or selected users' Intranet zone settings by using Group Policy in Active Directory:

<https://autologon.microsoftazuread-ss.com>

In addition, you need to enable an Intranet zone policy setting called Allow updates to status bar via script through Group Policy.

more information in:

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

NEW QUESTION: 192

Hotspot Question

You have an Azure subscription named Sub1 that contains a resource group named RG1. RG1 contains two Azure key vaults named KV1 and KV2 that use Azure role-based access control (Azure RBAC).

| Name  | Role                    | Scope |
|-------|-------------------------|-------|
| User1 | Key Vault Administrator | Sub1  |
| User2 | Key Vault Reader        | RG1   |
| User3 | Key Vault Secrets User  | KV1   |

ing table.

KV1 contains a secret named Secret1. KV2 contains a secret named Secret2.

Which users can read the values of each secret? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Secret1:  ▼

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

Secret2: ▼

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

Answer:

Answer Area

Secret1:

User1 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

Secret2:

User1 only

User2 only

User3 only

User1 and User3 only

User2 and User3 only

User1, User2, and User3

NEW QUESTION: 193

You have an Azure subscription that contains a user named User1 and two resource groups named RG1 and RG2.

You need to ensure that User1 can perform the following tasks:

- View all resources.
- Restart virtual machines.
- Create virtual machines in RG1 only.
- Create storage accounts in RG1 only.

What is the minimum number of role-based access control (RBAC) role assignments required?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: (SHOW ANSWER)

Assign User1 the "Reader" role at the subscription level to view all resources.

Assign User1 the "Virtual Machine Contributor" role at the RG1 level to restart virtual machines and create virtual machines in RG1 only.

Assign User1 the "Storage Account Contributor" role at the RG1 level to create storage accounts in RG1 only.

NEW QUESTION: 194

Hotspot Question

You have an Azure AD tenant.  
You need to configure the following External Identities features:  
- B2B collaboration  
- Monthly active users (MAU)-based pricing  
Which two settings should you configure? To answer, select the settings in the answer area.  
NOTE: Each correct selection is worth one point.

Answer Area



## External Identities

Contoso Ltd - Azure Active Directory

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

### Self-service sign up

Custom user attributes

All API connectors

User flows

### Subscriptions

Linked subscriptions

### Lifecycle management

Terms of use

Access reviews

Answer:

Answer Area



## External Identities

Contoso Ltd - Azure Active Directory

<<

Overview

Cross-tenant access settings

All identity providers

External collaboration settings

Diagnose and solve problems

### Self-service sign up

Custom user attributes

All API connectors

User flows

### Subscriptions

Linked subscriptions

Lifecycle management

 Microsoft

Terms of use

Access reviews

### Drag and Drop Question

### Drag and Drop Question

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

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

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

Actions

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

Answer Area



Answer:

Actions

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

Answer Area



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



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

NEW QUESTION: 196

Hotspot Question

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com. The company has a business partner named Fabrikam, Inc.

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

Answer Area

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

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

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

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



Answer:

Answer Area

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



An access package assignment in Identity Governance

An access package policy in Identity Governance

A conditional access policy in Azure AD

The External collaboration settings in Azure AD

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

An access package assignment in Identity Governance

An access package policy in Identity Governance

A conditional access policy in Azure AD

The External collaboration settings in Azure AD

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

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (480 Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)

NEW QUESTION: 197

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and branch offices in London and Seattle. Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Azure Active Directory (Azure AD) tenant named fabrikam.com. Existing Environment. Existing Environment The on-premises network of Contoso contains an Active Directory domain named contoso.com. The domain contains an organizational unit (OU) named Contoso\_Resources. The Contoso\_Resources OU contains all users and computers. The contoso.com Active Directory domain contains the users shown in the following table.

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

Existing Environment. Microsoft 365/Azure Environment

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

- \* Microsoft Office 365 Enterprise E5
- \* Enterprise Mobility + Security
- \* Windows 10 Enterprise E3
- \* Project Plan 3

Azure AD Connect is configured between Azure AD and Active Directory Domain Services (AD DS). Only the Contoso\_Resources OU is synced.

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

User administrators currently use the Microsoft 365 admin center to manually assign licenses. All users have all licenses assigned besides the following exceptions:

- \* The users in the London office have the Microsoft 365 Phone System license unassigned.
- \* The users in the Seattle office have the Yammer Enterprise license unassigned.

Security defaults are disabled for contoso.com.

Contoso uses Azure AD Privileged Identity Management (PIM) to protect administrative roles.

Existing Environment. Problem Statements

Contoso identifies the following issues:

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

Requirements. Planned Changes

Contoso plans to implement the following changes:

- \* Implement self-service password reset (SSPR).
- \* Analyze Azure audit activity logs by using Azure Monitor.
- \* Simplify license allocation for new users added to the tenant.
- \* Collaborate with the users at Fabrikam on a joint marketing campaign.
- \* Configure the User administrator role to require justification and approval to activate.
- \* Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.
- \* For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

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

Requirement. Technical Requirements

Contoso identifies the following technical requirements:

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

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

What should you do?

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

**Answer: D (**[\*\*LEAVE A REPLY\*\*](#)**)**

Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles Default Setting State Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No Approvers None

**Valid SC-300 Dumps** shared by EduDump.com for Helping Passing SC-300 Exam! EduDump.com now offer the **newest SC-300 exam dumps**, the EduDump.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com SC-300 dumps with Test Engine here: <https://www.edudump.com/exams/Microsoft/SC-300/premium/> (**480** Q&As Dumps, **35%OFF** Special Discount Code: **freecram**)