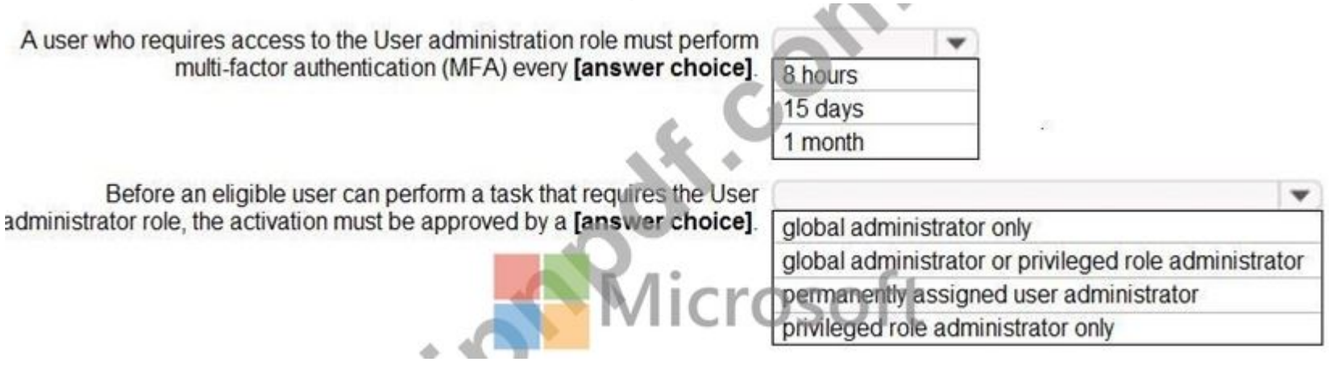
Microsoft.SC-300J.v2025-05-17.q150

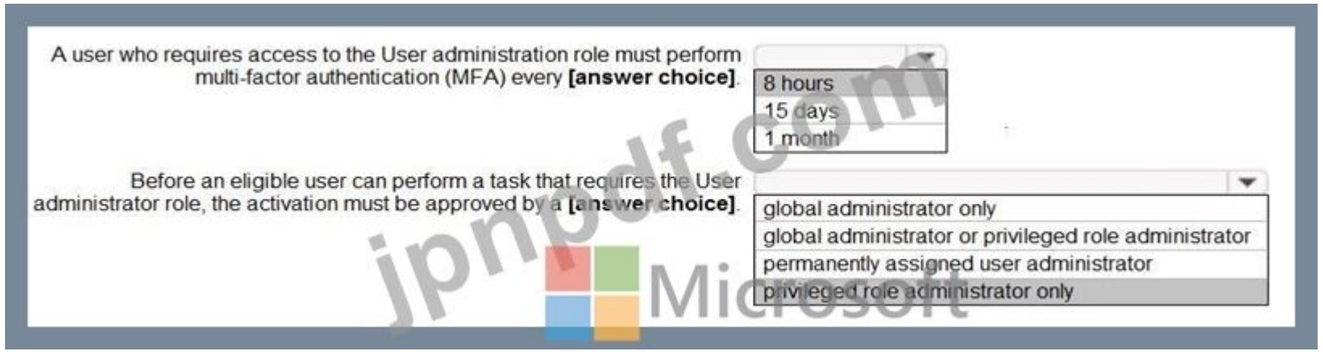
試験コード:	SC-300J
試験名称:	Microsoft Identity and Access Administrator (SC-300日本語版)
認定資格:	Microsoft
無料問題数:	150
バージョン:	v2025-05-17
アクセス数:	411
ページビュー数:	1500
https://www.jpnpdf.com/Microsoft.SC-300J.v2025-05-17.q150-mondaishu.html	

最新問題: **1**
次の図に示すように、ユーザー管理者ロールのAzure AD特権ID管理（PIM）ロール設定を含むAzure Active Directory（Azure AD）テナントがあります。

ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:



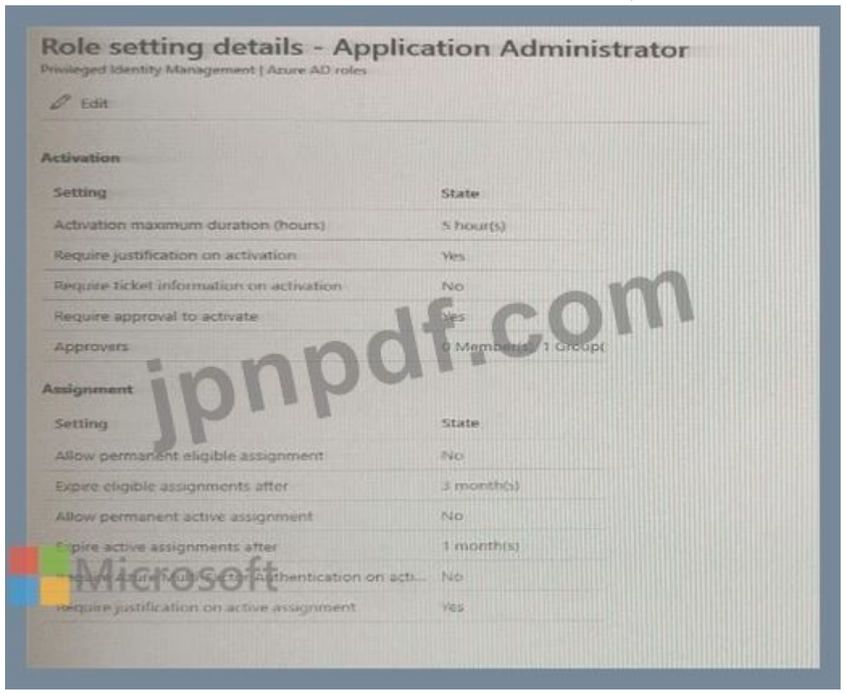
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

最新問題**: 2**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
A. New-AzureADMSInvitationコマンドレットを実行します。
B. 外部コラボレーション設定を構成します。
C. WS-FedIDプロバイダーを追加します。
D. Azure ADConnectを実装します。
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal
https://docs.microsoft.com/en-us/powershell/module/azuread/new-azureadmsinvitation?view=azureadps-2.0

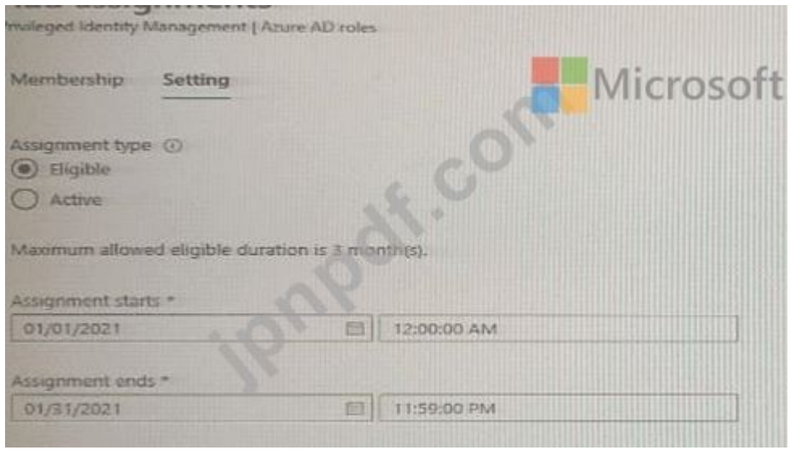
最新問題**: 3**
タスク 4
ユーザー プロファイルの読み取り権限を必要とするアプリにすべてのユーザーが同意できるようにする必要があります。ユーザーは、他の権限を必要とするアプリに同意できないようにする必要があります。
Answer:
See the Explanation for the complete step by step solution
Explanation:
To ensure that all users can consent to apps that require permission to read their user profile and prevent them from consenting to apps that require any other permissions, you can configure the user consent settings in the Microsoft Entra admin center. Here's how you can do it:
Sign in as a Global Administrator:
Access the Microsoft Entra admin center with Global Administrator privileges.
Navigate to user consent settings:

Go to Identity > Applications > Enterprise applications > Consent and permissions > User consent settings1.
Configure the consent settings:
Under User consent for applications, select the option that allows users to consent to apps that only require permission to read their user profile.
Ensure that all other permissions are set to require administrator consent, thus preventing users from consenting to apps that require additional permissions1.
Save the settings:
After configuring the consent settings, select Save to apply the changes.
By following these steps, you will have configured the system to allow user consent for apps that need to read the user profile while blocking consent for apps that require additional permissions. This setup helps maintain user autonomy where appropriate while safeguarding against unauthorized access to broader permissions.

最新問題: 4
User1、User1、およびUser3という名前の3人のユーザーを含むAzure Active Directory（Azure AD）テナントがあり、Group1という名前のグループを作成します。User2とUser3をGroup1に追加します。
アプリケーション管理者の展示に示されているように、Azure AD特権ID管理（PIM）でロールを構成します。 アプリケーションの[管理者]タブをクリックします。）



Group1は、アプリケーション管理者ロールの承認者として構成されます。
User2をアプリケーション管理者ロールの対象となるように構成します。
User1の場合、割り当ての展示に示されているように、アプリケーション管理者の役割に割り当てを追加します。 [割り当て]タブをクリックします）



次の各ステートメントについて、ステートメントがtrueの場合は[はい]を選択し、そうでない場合は[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:

最新問題: **5**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
すべてのユーザーは、Microsoft 365サービスにアクセスするときに、多要素認証（MFA）にMicrosoftAuthenticatorアプリを使用する必要があります。
一部のユーザーは、サインイン要求を開始せずにMicrosoftAuthenticatorアプリでMFAプロンプトを受信したと報告しています。
ユーザーが開始しなかったMFA要求を報告した場合、ユーザーを自動的にブロックする必要があります。
解決策 :Azureポータルから、多要素認証（MFA）の通知設定を構成します。

これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

最新問題**: 6**
注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。
Microsoft 365 ES サブスクリプションをお持ちです。
User1 という名前のユーザーを作成します。
User1 が ID セキュア スコア改善アクションのステータスを更新できることを確認する必要があります。
解決策: セキュリティ オペレータ ロール User1 を割り当てます。
これは目標を達成していますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**

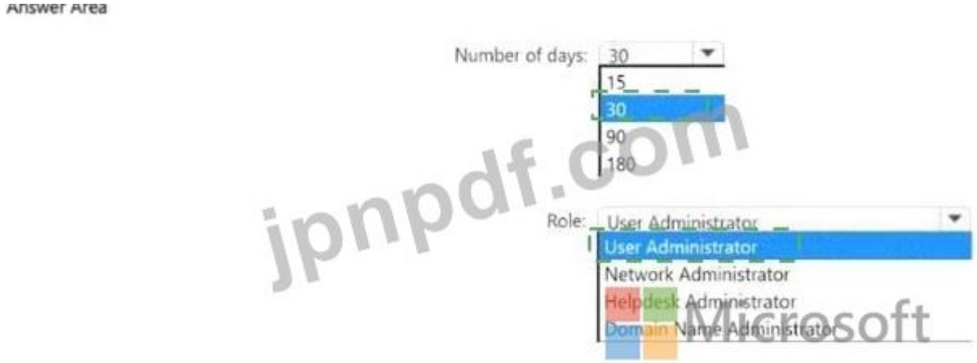
最新問題**: 7**
Azure Active Directory (Azure AD) テナントがあります。
リスク検出レポートを開きます。
どのリスク検出タイプがユーザーリスクとして分類されますか？
A. 不可能な旅行
B. 匿名IPアドレス
C. 非定型旅行
D. 漏洩したクレデンシャル
Answer: D (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

最新問題**: 8**
Azure Active Directory (Azure AD) テナントがあります。
次の設定を使用して、セルフサービスパスワードリセット (SSPR) を構成します。
*サインイン時にユーザーに登録を要求する :はい
*リセットに必要なメソッドの数 :1
ユーザーが利用できる有効な認証方法は何ですか？
A. モバイルアプリの通知

B. ホームプリオン
C. 組織内のアドレスへのメール
D. モバイルアプリコード
Answer: (解答を表示する**)**

最新問題**: 9**
User1 という名前のユーザーを含む Microsoft Entra テナントがあります。
管理者が User1 を削除します。次の点を特定する必要があります。
* User1 アカウントを復元できるオプションの最大日数はどれくらいですか?
* User1 を復元するために使用できる最も権限の少ないロールはどれですか?
回答するには、回答エリアで適切なオプションを選択します。注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:

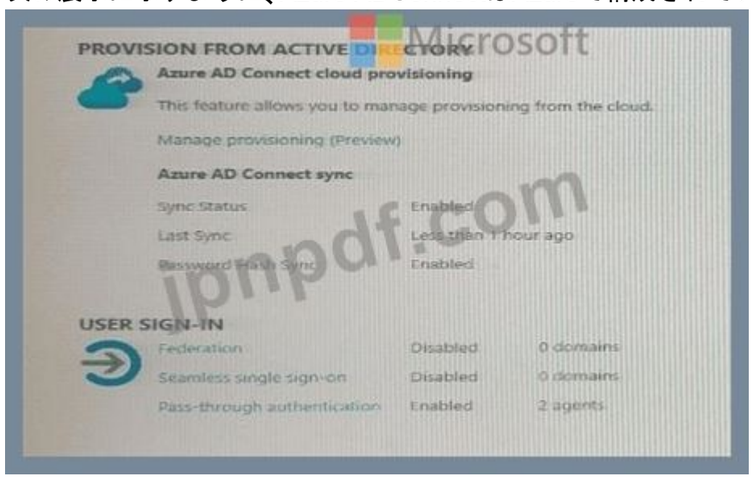


Explanation:

最新問題**: 10**
ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスのActiveDirectoryドメインが含まれています。テナントには、次の表に示すものが含まれています。

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

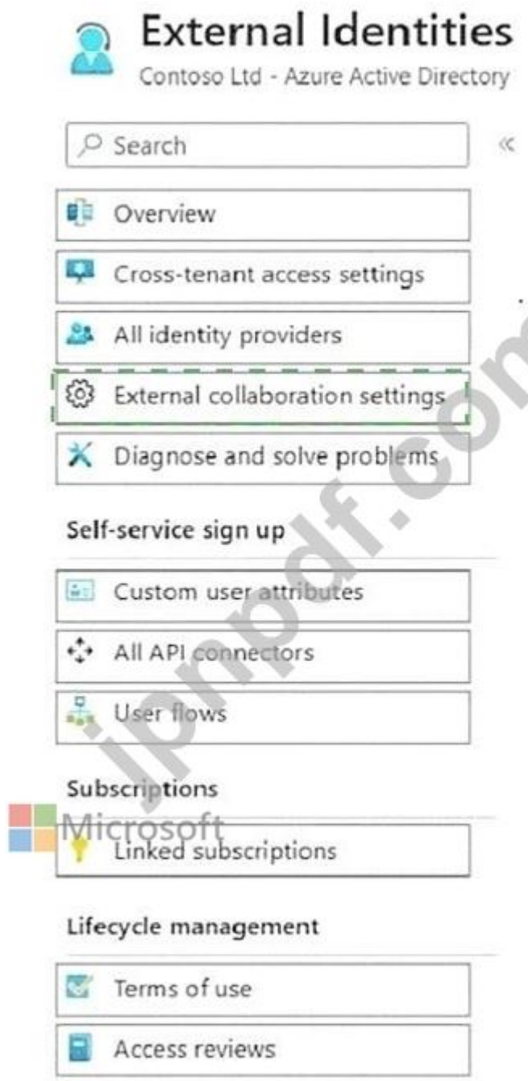
すべてのユーザーはリモートで作業します。
次の展示に示すように、Azure ADConnectはAzureで構成されています。



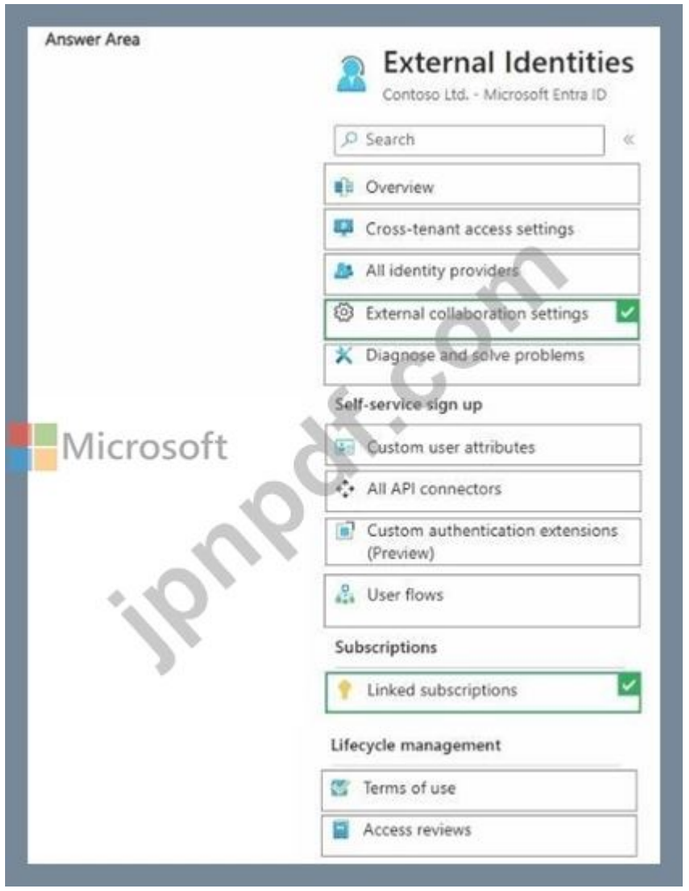
オンプレミスドメインからインターネットへの接続が失われます。
どのユーザーがAzureADにサインインできますか？
A. ユーザー1とユーザー3のみ
B. User1のみ
C. User1、User2、およびUser3
D. User1、およびUser2のみ
Answer: A (メーッセージを残す**)**

最新問題**: 11**
Microsoft Entra テナントをお持ちです。
次の外部 ID 機能を構成する必要があります。
* B2Bコラボレーション
* Monthly active users (MAU)-based pricing
どの 2 つの設定を構成する必要がありますか? 回答するには、回答領域で設定を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

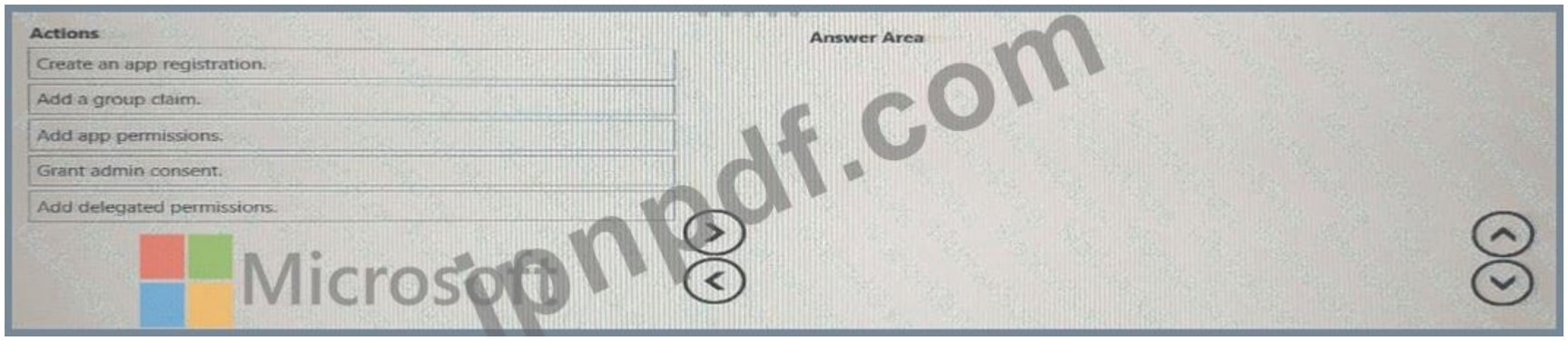


Explanation:

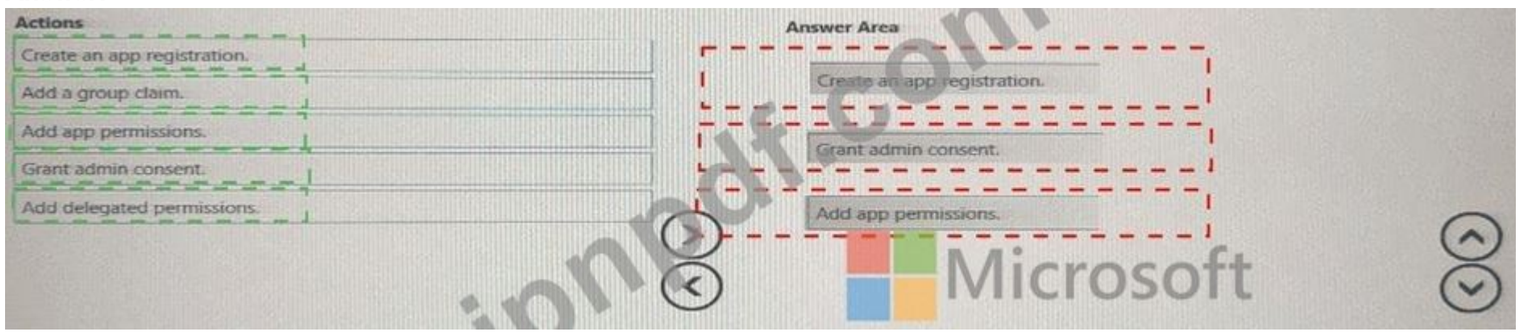


最新問題: **12**
「Terms1」という名前の使用条件 (ToU) を含む Microsoft Entra テナントがあります。Policy1 という名前の条件付きアクセス ポリシーを作成して、Terms1 を展開します。ユーザーにTerms1への同意を要求するようにPolicy1を構成する必要があります。Policy1 にはどの設定を構成する必要がありますか?
A. 許可
B. ターゲットリソース
C. セッション
D. 条件
Answer: D (メーッセージを残す**)**

最新問題: **13**
あなたの会社には、contoso.comという名前のAzure Active Directory（Azure AD）テナントがあります。
同社はApp1という名前のWebサービスを開発しています。
App1がMicrosoftGraphを使用してcontoso.comのディレクトリデータを読み取ることができることを確認する必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序で配置します。



Answer:



Explanation:

Create an app registration:

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

Grant admin consent:

Higher-privileged permissions require administrator consent.

Add app permissions:

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

Reference:

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

最新問題: 14

User1 という名前のユーザーと Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。

User1 が Vault1 に保存されている証明書、鍵、シークレットのメタデータを読み取れるようにする必要があります。このソリューションは、最小権限の原則に従う必要があります。
User1 に割り当てるべきロールはどれですか?
A. Key Vault 暗号化ユーザー
B. Key Vault 暗号化担当者
C. Key Vault リーダー
D. Key Vault シークレット ユーザー
Answer: C (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Azure Key Vault roles, permissions, and the principle of least privilege, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Azure Key Vault and the Requirement:
Azure Key Vault is a service that securely stores and manages cryptographic keys, secrets, and certificates. It uses role-based access control (RBAC) to manage permissions for users, groups, and applications.
The question requires that User1 canread the metadataof certificates, keys, and secrets in Vault1. In Azure Key Vault, "metadata" refers to the properties of these objects (e.g., name, creation date, expiration date), not the actual content (e.g., the secret value, key value, or certificate private key).
The solution must follow theprinciple of least privilege, meaning User1 should be granted the minimum permissions necessary to perform the task, without access to unnecessary actions (e.g., modifying or deleting objects).
Azure Key Vault RBAC Roles and Permissions:
Azure Key Vault supports built-in RBAC roles that define specific permissions for managing keys, secrets, and certificates. Let's examine each role in the options:
Key Vault Crypto User:
This role allows a user to perform cryptographic operations using keys (e.g., encrypt, decrypt, sign, verify) and to read key metadata.
Permissions include: Microsoft.KeyVault/vaults/keys/read (read key metadata) and cryptographic operations like encrypt, decrypt, etc.
However, this role does not grant permissions to read metadata for secrets or certificates, and it includes cryptographic operation permissions, which are not needed for the task.
Key Vault Crypto Officer:
This role is designed for managing keys and performing cryptographic operations. It includes permissions to create, delete, update, and read keys, as well as perform cryptographic operations.
Permissions include: Microsoft.KeyVault/vaults/keys/* (full control over keys).
This role does not grant access to secrets or certificates and provides more permissions than needed (e.g., create, delete), violating the principle of least privilege.
Key Vault Reader:
This role provides read-only access to the metadata of all objects in the Key Vault (keys, secrets, and certificates).
Permissions include: Microsoft.KeyVault/vaults/read (read vault properties) and Microsoft.KeyVault/vaults/*
/read (read metadata for keys, secrets, and certificates).
Importantly, this role does not allow access to the actual content of the objects (e.g., the secret value, key value, or certificate private key), only the metadata. It also does not allow write operations (e.g., create, update, delete).
This aligns perfectly with the requirement to "read the metadata" and follows the principle of least privilege.
Key Vault Secrets User:
This role allows a user to read the content of secrets (not just metadata) and perform operations like getting the secret value.
Permissions include: Microsoft.KeyVault/vaults/secrets/get (read secret values) and Microsoft.KeyVault
/vaults/secrets/read (read secret metadata).
This role does not grant access to keys or certificates, and it provides more access than needed (reading the secret value, not just metadata), violating the principle of least privilege.
Applying the Principle of Least Privilege:
The task requires User1 to read the metadata of certificates, keys, and secrets, but not to access their content or perform any write operations.
Key Vault Readeris the most appropriate role because:

It grants read-only access to the metadata of all objects (keys, secrets, certificates).
It does not allow access to the content of the objects (e.g., secret values), which is not required.
It does not allow write operations (e.g., create, delete), adhering to the principle of least privilege.
The other roles either provide too much access (e.g., Key Vault Crypto Officer, Key Vault Secrets User) or do not cover all required objects (e.g., Key Vault Crypto User, Key Vault Secrets User).
Analysis of the Options:
A: Key Vault Crypto User:
Incorrect. This role only allows reading key metadata and performing cryptographic operations, but it does not provide access to secrets or certificates metadata. It also grants unnecessary cryptographic permissions.
B: Key Vault Crypto Officer:
Incorrect. This role provides full control over keys, which is far more than needed, and does not grant access to secrets or certificates metadata.
C: Key Vault Reader:
Correct. This role provides read-only access to the metadata of keys, secrets, and certificates, exactly matching the requirement while following the principle of least privilege.
D: Key Vault Secrets User:
Incorrect. This role allows reading secret values (not just metadata) and does not provide access to keys or certificates metadata. It grants more access than needed.
Additional Considerations:
If the question had asked for User1 to read the content of secrets (not just metadata), the Key Vault Secrets User role might be considered, but it still wouldn't cover keys and certificates.
Custom RBAC roles could be created to fine-tune permissions, but the question asks for a built-in role, and Key Vault Reader is the best fit.
The question does not specify whether User1 needs to perform other actions (e.g., cryptographic operations, managing the vault). If additional permissions were needed, a combination of roles or a custom role might be required, but the principle of least privilege guides us to the minimal role.
Conclusion:To ensure User1 can read the metadata of certificates, keys, and secrets in Vault1 while following the principle of least privilege, theKey Vault Readerrole should be assigned. This role provides the exact permissions needed without granting unnecessary access. Therefore, the correct answer isC.
References:
Azure Key Vault documentation: "Azure Key Vault RBAC roles" (Microsoft Learn:https://learn.microsoft.
com/en-us/azure/key-vault/general/rbac-guide)
Azure Key Vault documentation: "Secure access to a key vault" (Microsoft Learn:https://learn.microsoft.com
/en-us/azure/key-vault/general/secure-your-key-vault)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Azure Key Vault access control and the principle of least privilege.

最新問題**: 15**
ADatum ユーザーを同期する必要があります。ソリューションは、技術要件を満たす必要があります。
あなたは何をするべきか？
A. Microsoft Azure Active Directory Connect ウィザードから、[同期オプションのカスタマイズ] を選択します。
B. PowerShell から Set-ADSyncScheduler を実行します。
C. PowerShell から、Start-ADSyncSyncCycle を実行します。
D. Microsoft Azure Active Directory Connect ウィザードから、[ユーザー サインインの変更] を選択します。
Answer: (解答を表示する**)**
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).
Topic 3, A Datum CorpOverviewA. Datum Corporation is a consulting company in Montreal.
A Datum recently acquired a Vancouver-based company named Litware, Inc.
A Datum Environment

The on-premises network of A Datum contains an Active Directory Domain Services (AD DS) forest named adatum.com.
A Datum has a Microsoft 365 E5 subscription. The subscription contains a verified domain that syncs with the adatum.com AD DS domain by using Azure AD Connect A Datum has an Azure Active Directory (Azure AD) tenant named adatum.com. The tenant has Security defaults disabled.
The tenant contains the users shown in the following table.
Problem Statements
A Datum identifies the following issues:
* 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
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.
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.

最新問題: 16
RG1 という名前のリソース グループを含む Sub1 という名前の Azure サブスクリプションがあります。RG1 には、DB1 という名前の Azure Cosmos DB データベースと、AKS1 という名前の Azure Kubernetes Service (AKS) クラスターが含まれています。AKS1 はマネージド ID を使用します。
AKS1 が DB1 にアクセスできることを確認する必要があります。ソリューションは次の要件を満たす必要があります。
* AKS1 がマネージド ID を使用して DB1 にアクセスすることを確認します。
* 最小特権の原則に従います。

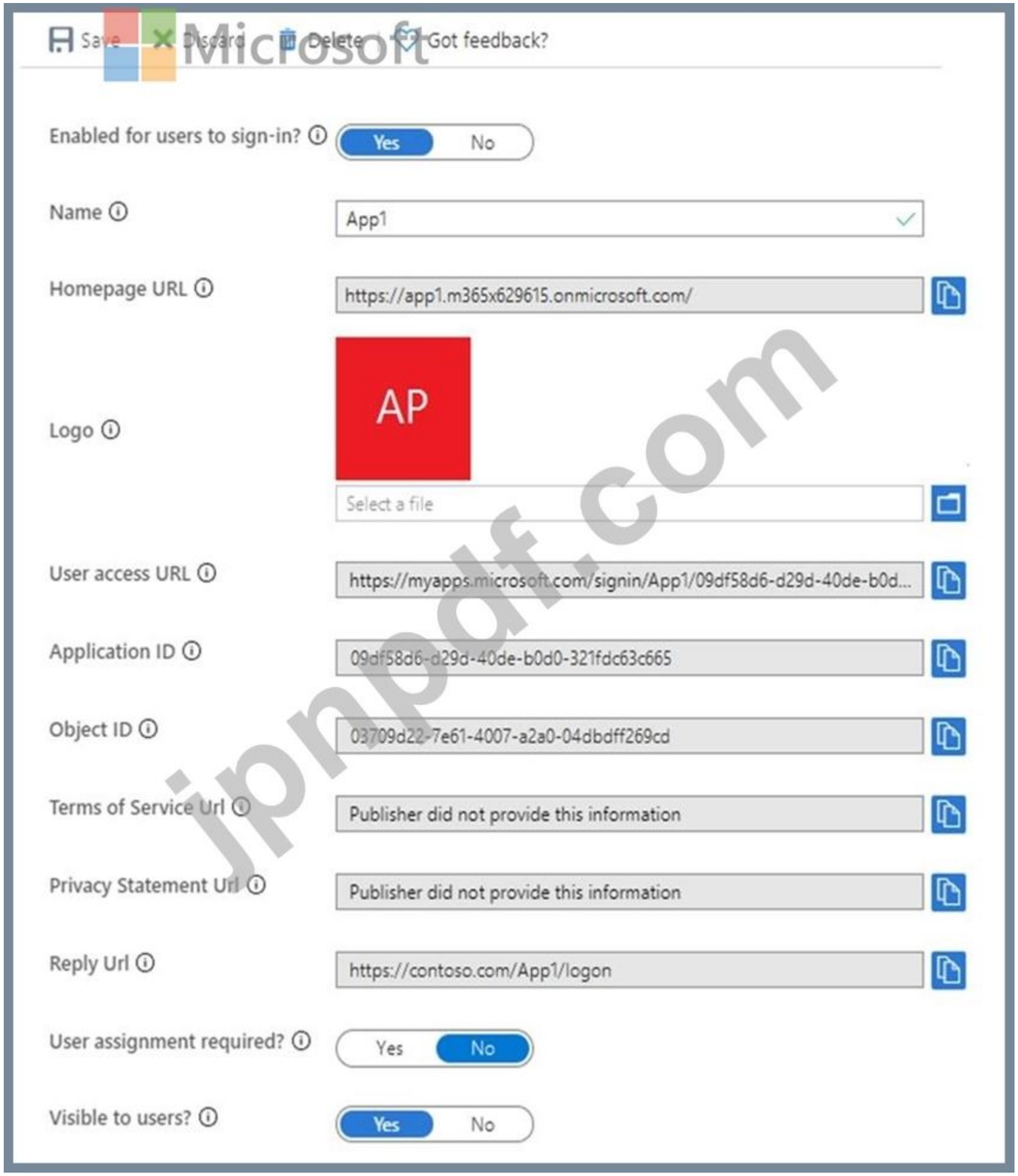
AKS1 のマネージド ID にどのロールを割り当てる必要がありますか。
A. DB1 の場合、Azure Cosmos DB アカウント閲覧者ロール ロールを割り当てます。
B. RG1 の場合、リーダーの役割を割り当てます。
C. R61 の場合、Azure Cosmos DB データ読み取りロール ロールを割り当てます。
D. Sub1 の場合。所有者の役割を割り当てます。
Answer: C (メーッセージを残す**)**

最新問題**: 17**
Microsoft 365 テナントがあります。
すべてのユーザーは携帯電話とラップトップを持っています。
ユーザーは、Wi-Fi アクセスや携帯電話接続のない遠隔地から作業することがよくあります。
遠隔地から作業しているとき、ユーザーはラップトップをインターネットにアクセスできる有線ネットワークに接続します。
多要素認証 (MFA) を実装する予定です。
ユーザーが遠隔地から使用できる MFA 認証方法はどれですか?
A. Microsoft Authenticator アプリを介した通知
B. 秘密の質問
C. 音声
D. アプリのパスワード
Answer: A (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

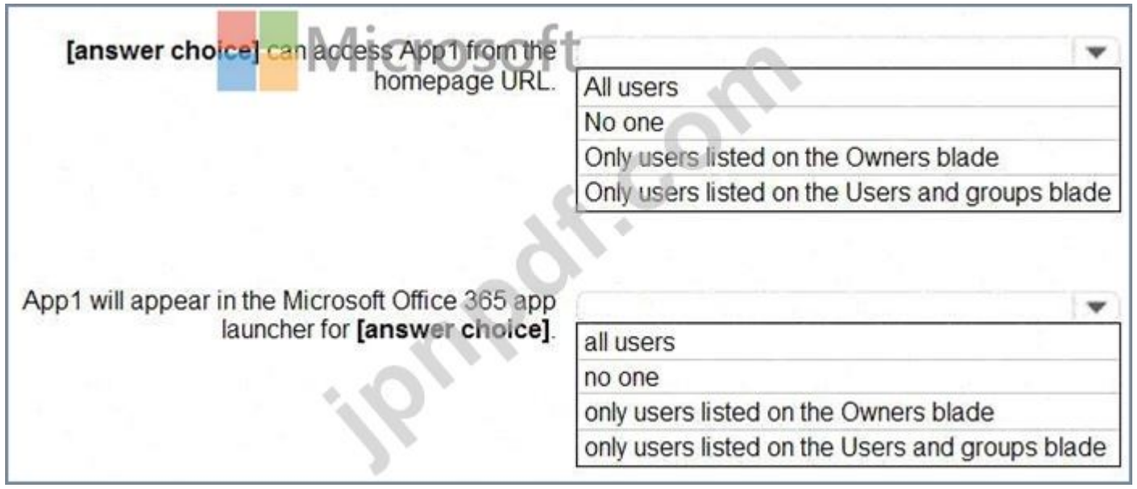
最新問題**: 18**
Microsoft Entra Permissions Management を使用する Sub1 という名前の Azure サブスクリプションがあります。Sub1 には User1 という名前のユーザーが含まれています。User1 には、Sub1 全体で複数の権限が付与されます。
User1 に付与されているすべての権限を読み取り専用権限に置き換える必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
アクセス許可管理の [修復] タブでは何をすべきですか?
A. [ロール/ポリシー テンプレート] サブタブから。テンプレートを作成します。
B. [ロール/ポリシー] サブタブから。役割を作成します。
C. [My Requests] サブタブから、新しいリクエストを作成します。
D. [権限] サブタブから、クイック アクションを使用します。
Answer: B (メーッセージを残す**)**

最新問題**: 19**

Azure Active Directory（Azure AD）に登録されているApp1という名前のカスタムクラウドアプリがあります。
App1は、次の展示に示すように構成されています。

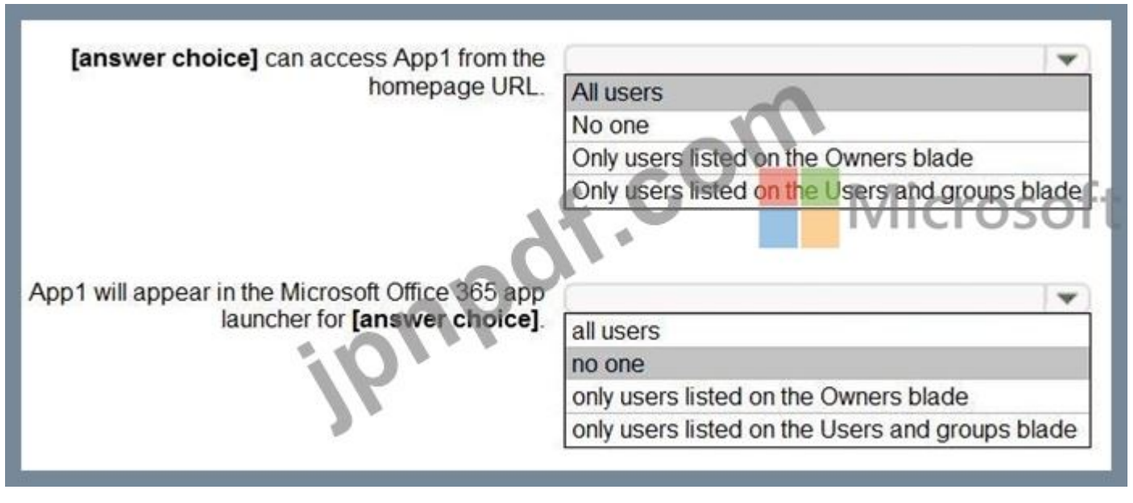

Save
Discard
Delete
Got feedback?
Enabled for users to sign-in?
Yes
No
Name
App1
Homepage URL
https://app1.m365x629615.onmicrosoft.com/
Logo
AP
Select a file
User access URL
https://myapps.microsoft.com/signin/App1/09df58d6-d29d-40de-b0d...
Application ID
09df58d6-d29d-40de-b0d0-321fdc63c665
Object ID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

ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

Explanation:



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

最新問題: **20**
Microsoft Office 365 EnterpriseE3ライセンスが割り当てられている2,500人のユーザーがいます。ライセンスは個々のユーザーに割り当てられます。
Azure Active Directory管理センターの[グループ]ブレードから、Microsoft 365 EnterpriseE5ライセンスをユーザーに割り当てます。
最小限の管理作業で、Office 365 EnterpriseE3ライセンスをユーザーから削除する必要があります。
何を使うべきですか？
A. Azure ActiveDirectory管理センターのIdentityGovernanceブレード
B. Set-AzureAdUserコマンドレット
C. Set-WindowsProductKeyコマンドレット
D. Azure ActiveDirectory管理センターのライセンスブレード
Answer: B (メーッセージを残す**)**

最新問題: **21**
Site1 という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。
ユーザーがサイトへのアクセスを要求できるようにする必要があります。ソリューションは次の要件を満たす必要があります。
* グループ メンバーシップに基づいて、ユーザーからの要求を自動的に承認します。
* 30 日後に自動的にアクセスを削除します
あなたは何をするべきか？
A. Microsoft Defender for Cloud Apps アクセス ポリシーを作成します。
B. Azure AD Privileged Identity Management でロール設定を構成します。
C. アクセス パッケージを作成します。
D. 条件付きアクセス ポリシーを作成します。
Answer: C (メーッセージを残す**)**

最新問題: **22**
User! という名前のユーザーを含む Azure サブスクリプションがあります。RG1 と RG2 という名前の 2 つのリソース グループ。
User1 が次のタスクを実行できることを確認する必要があります。
* すべてのリソースを表示します。
* 仮想マシンを再起動します。
※仮想マシンはRG1のみで作成します。
* ストレージ アカウントは RG1 でのみ作成します。
必要な役割ベースのアクセス制御 (RBAC) 役割割り当て* の最小数は何ですか?
A. 2
B. 4
C. 3
D. 1
Answer: (解答を表示する**)**

最新問題: **23**

ネットワークには、Azure Active Directory (Azure AD) テナントと同期するオンプレミスの Active Directory ドメインが含まれています。

テナントには、次の表に示すグループが含まれています。

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

テナントには、次の表に示すユーザーが含まれます。

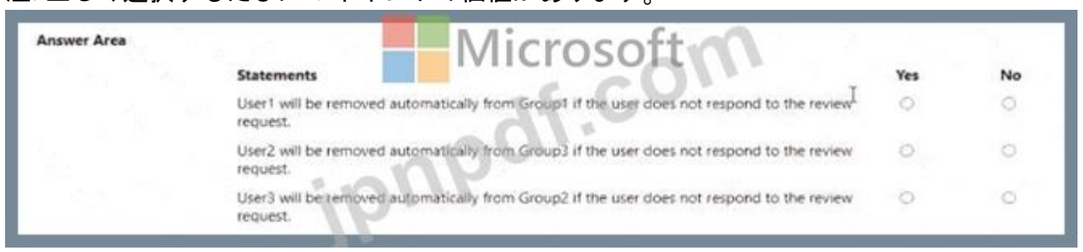
Name	Directory-synced	Member of
User1	No	Group1
User2	No	Group3
User3	Yes	Group2

次の表に示すように、アクセス レビューを作成します。

Setting	Value
Review type	Teams + Groups
Review scope	All users
Group	Group2, Group3
Reviewers	Users review own access
If reviewers don't respond	Remove access

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

Explanation:

最新問題: **24**
Microsoft365テナントがあります。
すべてのユーザーは、Microsoft 365サービスにアクセスするときに、多要素認証（MFA）にMicrosoftAuthenticatorアプリを使用する必要があります。
一部のユーザーは、サインイン要求を開始せずにMicrosoftAuthenticatorアプリでMFAプロンプトを受信したと報告しています。
ユーザーが開始しなかったMFA要求を報告した場合、ユーザーを自動的にブロックする必要があります。
解決策：Azureポータルから、多要素認証（MFA）のアカウントロックアウト設定を構成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: (解答を表示する**)**
You need to configure the fraud alert settings.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

最新問題: **25**
Microsoft Office 365 Enterprise E3 ライセンスが割り当てられているユーザーは 2,500 人います。ライセンスは個々のユーザーに割り当てられます。
Azure Active Directory 管理センターの [グループ] ブレードから、ユーザーに Microsoft 365 Enterprise E5 ライセンスを割り当てます。
最小限の管理労力で、ユーザーから Office 365 Enterprise E3 ライセンスを削除する必要があります。
何を使うべきでしょうか?
A. the Set -KindohsProductKcy cmdlct
B. the Update-MgGroup cmdlet
C. the Set-HgUserLicense cmdlet
D. the Update-MgUser cmdlet
Answer: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/powershell/module/msonline/set-msoluserlicense?view=azureadps-1.0

最新問題: **26**
タスク9
Sg-Operations グループのユーザーが My Apps ポータルにアクセスすると、次のアプリケーションのみを含む Operations という名前のタブが表示されることを確認する必要があります。
* アンクデリン
* 箱
Answer:
See the Explanation for the complete step by step solution

Explanation:
To ensure that users in the Sg-Operations group see a tab named "Operations" containing only LinkedIn and Box applications in the My Apps portal, you can create a collection with these specific applications. Here's how to do it:
Sign in to the Microsoft Entra admin center:
Make sure you have one of the following roles: Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the service principal.
Navigate to App launchers:
Go to Identity > Applications > Enterprise applications.
Under Manage, select App launchers.
Create a new collection:
Click on New collection.
Enter "Operations" as the Name for the collection.
Provide a Description if necessary.
Add applications to the collection:
Select the Applications tab within the new collection.
Click on + Add application.
Search for and select LinkedIn and Box applications.
Click Add to include them in the collection.
Assign the collection to the Sg-Operations group:
Select the Users and groups tab.
Click on + Add users and groups.
Search for and select the Sg-Operations group.
Click Select to assign the collection to the group.
Review and create the collection:
Select Review + Create to check the configuration.
If everything is correct, click Create to finalize the collection.
By following these steps, when users in the Sg-Operations group visit the My Apps portal, they will see a new tab named "Operations" that contains only the LinkedIn and Box applications1.
Please note that to create collections on the My Apps portal, you need a Microsoft Entra ID P1 or P2 license1.

最新問題**: 27**
営業部門のユーザーの問題を解決する必要があります。Azure AD テナントに対して何を構成する必要がありますか?
A. セキュリティのデフォルト
B. ユーザー設定
C. アクセス レビューの設定
D. デバイス設定
Answer: B (メーッセージを残す**)**

最新問題**: 28**
次の表に示すユーザーを含むAzureActive Directory（Azure AD）テナントがあります。

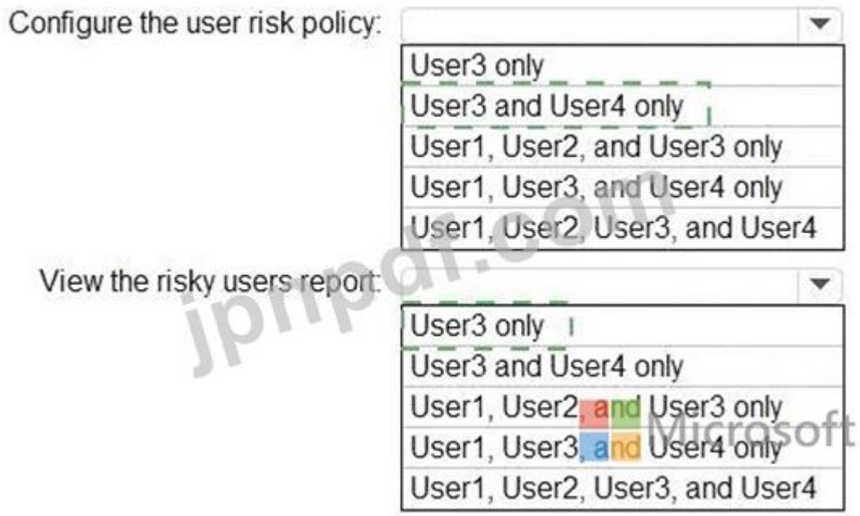
Name	Role
User1	Conditional Access administrator
User2	Authentication administrator
User3	Security administrator
User4	Security operator

Azure AD IdentityProtectionを実装する予定です。

どのユーザーがユーザーリスクポリシーを構成でき、どのユーザーがリスクのあるユーザーレポートを表示できますか？回答するには、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:



Explanation:

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection

最新問題**: 29**
RG1 という名前のリソース グループと、User1、User2、User3、および User4 という名前の 4 人のユーザーを含む Azure サブスクリプションがあります。ユーザーに RG1 の次のロールを割り当てることを計画しています。
* ユーザー 1: 読者
* User2: 投稿者
* User3: ストレージ BLOB データ リーダー
* User4: 仮想マシンの貢献者
属性ベースのアクセス制御 (ABAC) の使用を評価しています。ABAC の使用をサポートするユーザーの役割はどれですか?
A. ユーザー 3
B. ユーザー 4
C. ユーザー 1
D. ユーザー 2
Answer: A (メーッセージを残す**)**

最新問題**: 30**
Azure AD IdentityProtectionが有効になっているconto.so.comという名前のAzureActive Directory（Azure AD）テナントがあります。アクセスをブロックせずに、サインインリスク修復ポリシーを実装する必要があります。
あなたは最初に何をすべきですか？
A. AzureADでアクセスレビューを構成します。
B. AzureADパスワード保護を適用します。
C. すべてのユーザーに多要素認証（MFA）を実装します。
D. すべてのユーザーのセルフサービスパスワードリセット（SSPR）を構成します。
Answer: C (メーッセージを残す**)**
MFA and SSPR are both required. However, MFA is required first.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-remediate-unblock

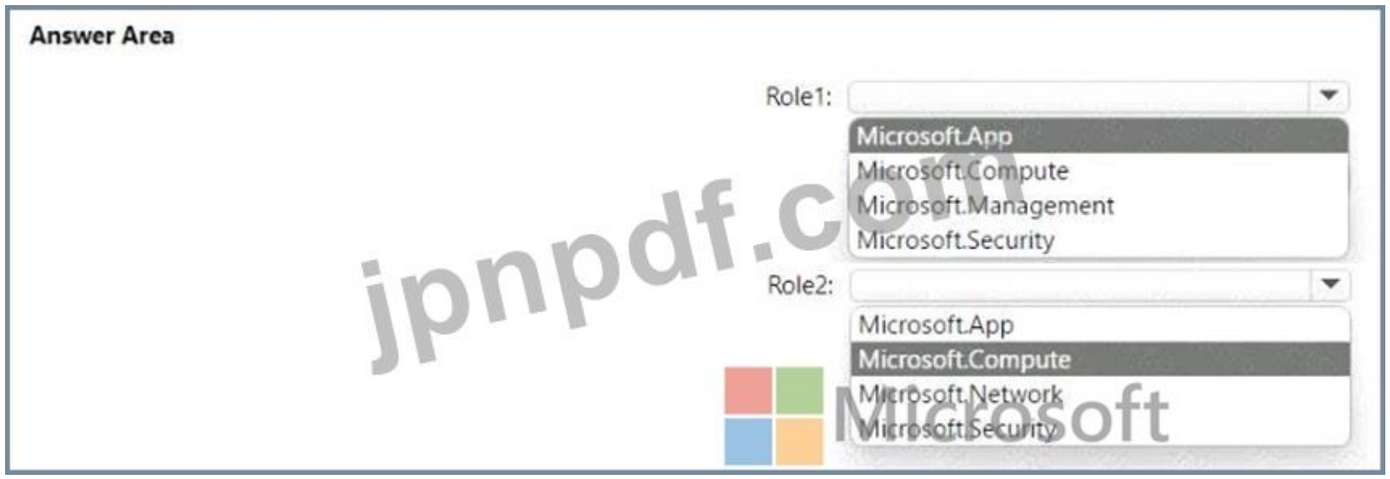
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

最新問題: **31**
次の表に示すユーザーを含む Azure AD テナントがあります。

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

エンタープライズ アプリケーションのユーザー設定には、次の構成があります。
* ユーザーは、自分に代わって会社のデータにアクセスするアプリに同意できます。
* ユーザーは、アプリがグループの会社データにアクセスすることに同意できます。
* ユーザーは、同意できないアプリに対して管理者の同意を要求できます: はい
* 管理者の同意要求を確認できるユーザー: Admin2、User2
User1 は、会社のデータへのアクセスに同意が必要なアプリを追加しようとします。
同意できるのはどのユーザーですか?
A. 管理者2
B. ユーザー1
C. ユーザー 2
D. 管理者1
Answer: (解答を表示する)

最新問題: **32**
Azure サブスクリプションがあります。
Role1 と Role2 という名前の 2 つのカスタム ロールを作成する必要があります。ソリューションは、次の要件を満たす必要があります。
* Role1 が割り当てられたユーザーは、Azure Container Apps のインスタンスを作成または削除できます。
* Role2 が割り当てられたユーザーは、適応型ネットワーク強化ルールを適用できます。
各ロールに必要なリソース プロバイダーのアクセス許可はどれですか? 回答するには、回答で適切なオプションを選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。



Answer:

Explanation:

最新問題: 33

次の表に示すユーザーを含む Azure サブスクリプションがあります。

Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

Azure AD Privileged Identity Management (PIM) を実装する必要があります。
PIM を使用して自分のロール権限をアクティブ化できるのはどのユーザーですか?
A. Admin2 のみ
B. 管理者1、管理者2、および管理者3
C. Admin1 と Admin2 のみ
D. Admin3 のみ
E. 管理者さん！のみ
F. Admin2 および Admin3 のみ
Answer: (解答を表示する**)**

最新問題**: 34**
User1 という名前のユーザーを含む Azure Active Directory (Azure AD) テナントがあります。
User1 が新しいカタログを作成し、所有するカタログにリソースを追加できるようにする必要があります。
あなたは何をするべきか？
A. ID ガバナンス ブレードから、資格管理設定を変更します。
B. Identity Governance ブレードから、一般カタログの役割と管理者を変更します。
C. [役割と管理者] ブレードから、サービス サポート管理者の役割を変更します。
D. [役割と管理者] ブレードから、グループ管理者の役割を変更します。
Answer: (解答を表示する**)**

最新問題**: 35**
SecAdmin1という名前のユーザーを含むAzureActive Directory（Azure AD）テナントがあります。SecAdmin1には、セキュリティ管理者の役割が割り当てられています。
SecAdmin1は、Azure AD IdentityProtectionポータルからパスワードをリセットできないと報告しています。
SecAdmin1が非管理ユーザーに代わってパスワードを管理し、セッションを無効にできることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。
SecAdmin1にどの役割を割り当てる必要がありますか？
A. 認証管理者
B. ヘルプデスク管理者
C. 特権認証管理者
D. セキュリティオペレーター
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

最新問題**: 36**
User1 という名前のユーザーを含む Azure サブスクリプションがあります。次の要件を満たす必要があります。
* User1 が新しく登録されたアプリの所有者として追加されないようにします。
* User1 がアプリケーション プロキシ設定を管理できることを確認します。
* User2 がアプリを登録できることを確認します。
* 最小権限の原則を使用します。
User1 にどの役割を割り当てる必要がありますか?

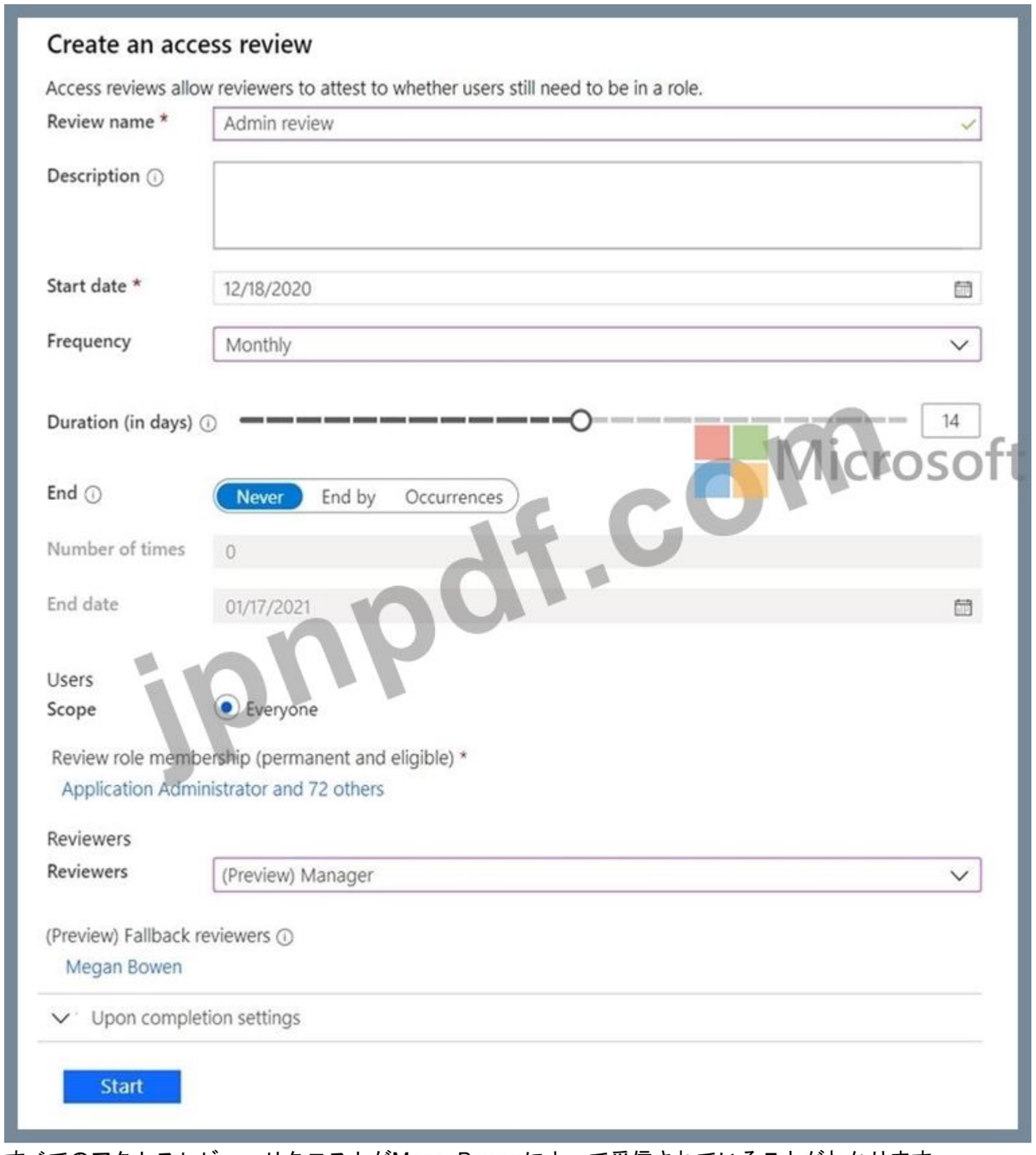
A. アプリケーション開発者
B. クラウド アプリケーション管理者
C. アプリケーション管理者
D. サービスサポート管理者
Answer: C (メーッセージを残す**)**

最新問題**: 37**
User1 と User2 という名前の 2 人のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
User1 がグループのアクセス レビューを作成できること、および User2 が完了したすべてのアクセス レビューの履歴レポートを確認できることを確認する必要があります。このソリューションでは、最小特権の原則を使用する必要があります。
各ユーザーにどの役割を割り当てる必要がありますか? 答えるには、適切な役割を適切なユーザーにドラッグします。各ロールは、1 回または複数回使用することも、まったく使用しないこともできます。
コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。注: 正しい選択はそれぞれ 1 ポイントの価値があります。

Answer:

Explanation:

最新問題: **38**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）

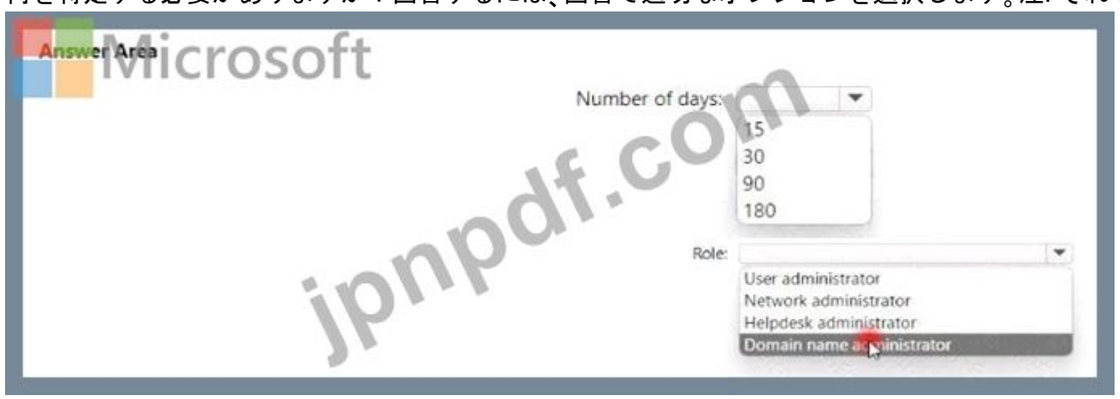


すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。
解決策：各マネージャーをフォールバックレビューアとして追加します。
これは目標を達成していますか？
A. はい

B. いいえ
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

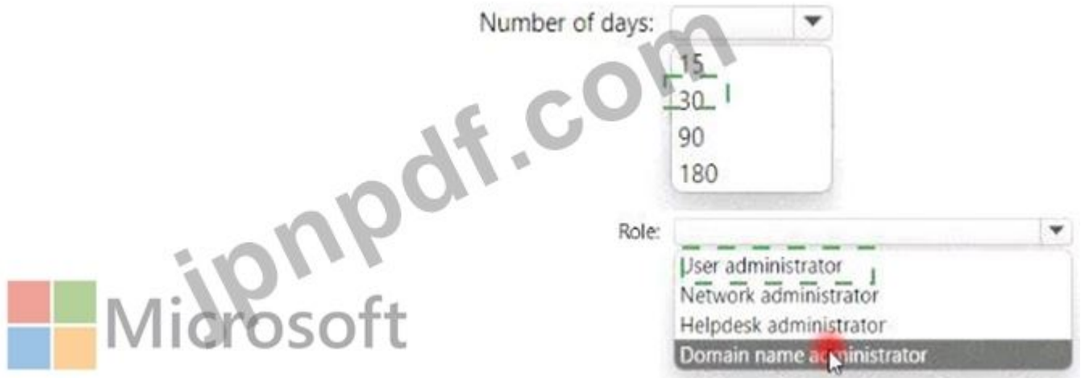
最新問題**: 39**
Azure Active Directory PremiumP2テナントがあります。
LogAnalyticsワークスペースを作成します。
Azure Monitorを使用して、Azure Active Directory（Azure AD）監査ログ情報を表示できることを確認する必要があります。
あなたは最初に何をすべきですか？
A. Set-AzureADTenantDetailコマンドレットを実行します。
B. AzureADワークブックを作成します。
C. AzureADの診断設定を変更します。
D. Get-AzureADAuditDirectoryLogsコマンドレットを実行します。
Answer: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-log-analytics

最新問題**: 40**
User1 という名前のユーザーを含む Azure Active Directory (Azure AD) テナントがあります。管理者が User1 を削除します。以下を識別する必要があります。
* User1 のアカウントを削除してから何日後にアカウントを復元できますか?
* User1 の復元に使用できる最も権限の低いロールはどれですか?
何を特定する必要がありますか？回答するには、回答で適切なオプションを選択します。注: それぞれの正しい選択は 1 ポイントの価値があります。



Answer:

Answer Area



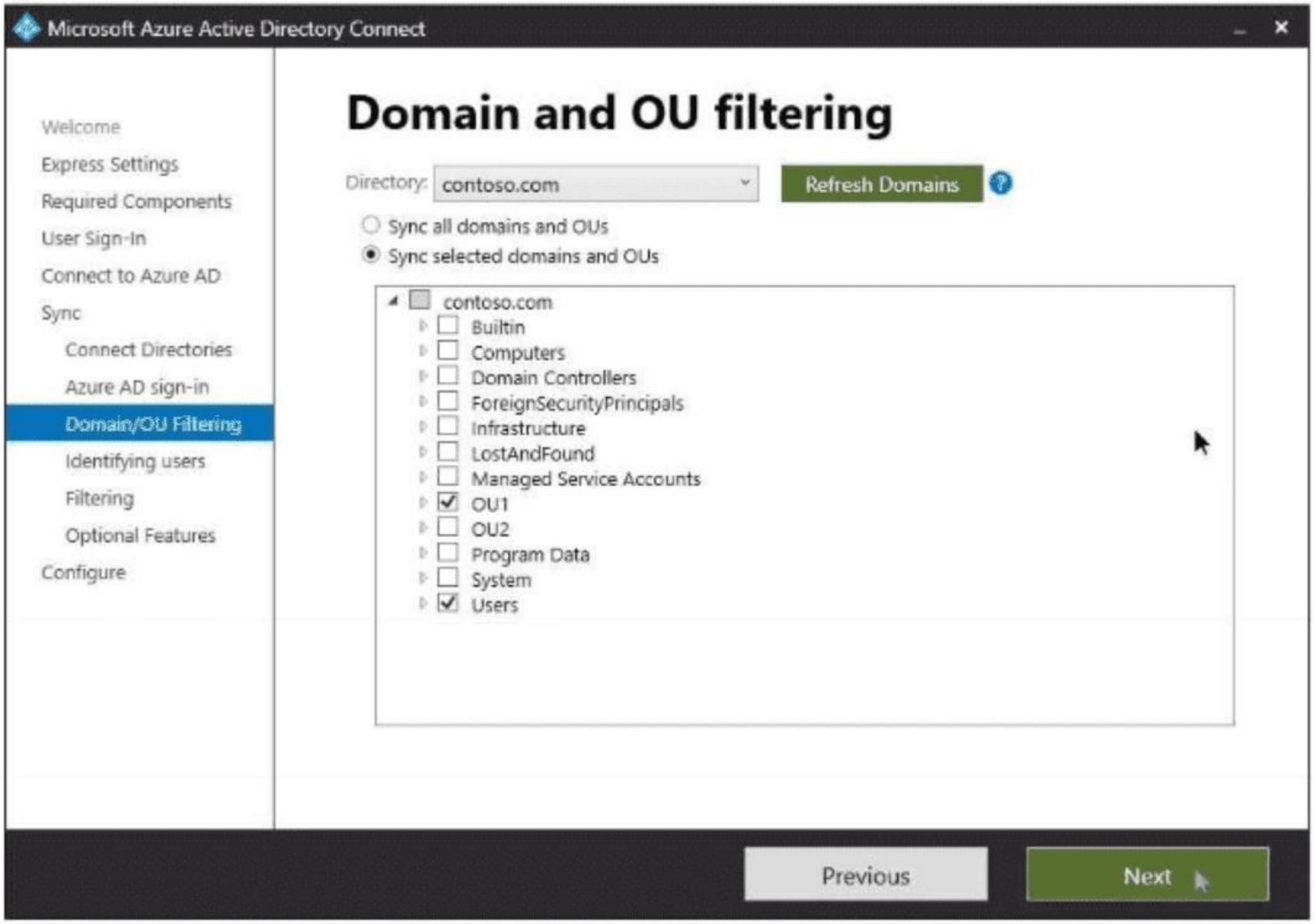
Explanation:

最新問題: **41**
漏洩したクレデンシャルの認証要件を満たす必要があります。
あなたは何をするべきか？
A. Azure ADConnectでPingFederateとのフェデレーションを有効にします。
B. AzureADパスワード保護を構成します。
C. Azure ADConnectでパスワードハッシュ同期を有効にします。
D. AzureADで認証方法ポリシーを構成します。
Answer: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

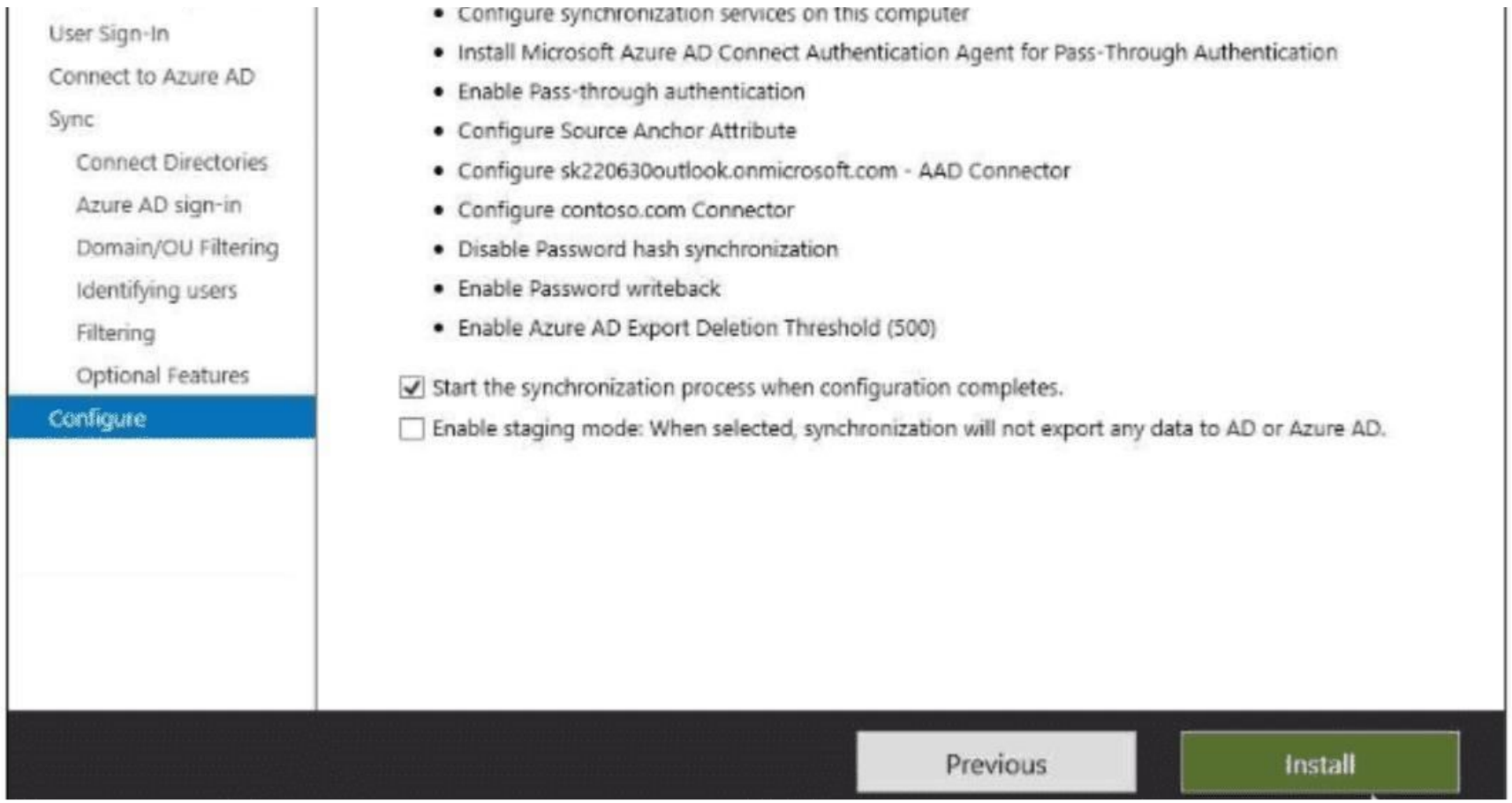
最新問題: **42**
ネットワークには、Azure AD と同期するオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれており、次の表に示すユーザーが含まれています。

Name	Organizational unit (OU)
User1	OU1
User2	OU2

Azure AD Connect 内。ドメイン/OU フィルタリングは次のように構成されます。



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



次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	○	○
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	○	○
User2 can be added to a Microsoft SharePoint Online site as a member.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can use self-service password reset (SSPR) to reset his password.	○	○
If User1 accesses Microsoft Exchange Online, he will be authenticated by an on-premises domain controller.	○	○
User2 can be added to a Microsoft SharePoint Online site as a member.	○	○

Explanation:

最新問題**: 43**

contoso.com という名前の Azure AD テナントがあり、All Company という名前のグループが含まれており、次の ID ガバナンス設定があります。

* 外部ユーザーがこのディレクトリにサインインできないようにブロックする: はい
* 外部ユーザーを削除する はい
* このディレクトリから外部ユーザーを削除するまでの日数: 30

2022 年 3 月 1 日に、次の設定を持つ Package1 という名前のアクセス パッケージを作成します。

* リソースの役割
o 名前: すべての会社
o タイプ: グループとチーム
o 役割: メンバー
* ライフサイクル
o アクセス パッケージ割り当ての有効期限: 日付
o 割り当ての有効期限: 2022 年 4 月 1 日

2022 年 3 月 1 日に、次の表に示すゲスト ユーザーに Package1 を割り当てます。

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

2022 年 3 月 2 日に、レポート閲覧者の役割を Guest1 に割り当てます。
2022 年 4 月 1 日に、Guest3 という名前のゲスト ユーザーを contoso.com に招待します。
2022 年 4 月 4 日に、Guest3 を All Company グループに追加します。
次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	○	○
On May 5, 2022, the Guest2 account is in contoso.com.	○	○
On May 5, 2022, the Guest3 account is in contoso.com.	○	○

Answer:

Answer Area

Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	○	○
On May 5, 2022, the Guest2 account is in contoso.com.	○	○
On May 5, 2022, the Guest3 account is in contoso.com.	○	○

Explanation:

最新問題: **44**

次の表に示すホストを含むオンプレミスのデータセンターがあります。

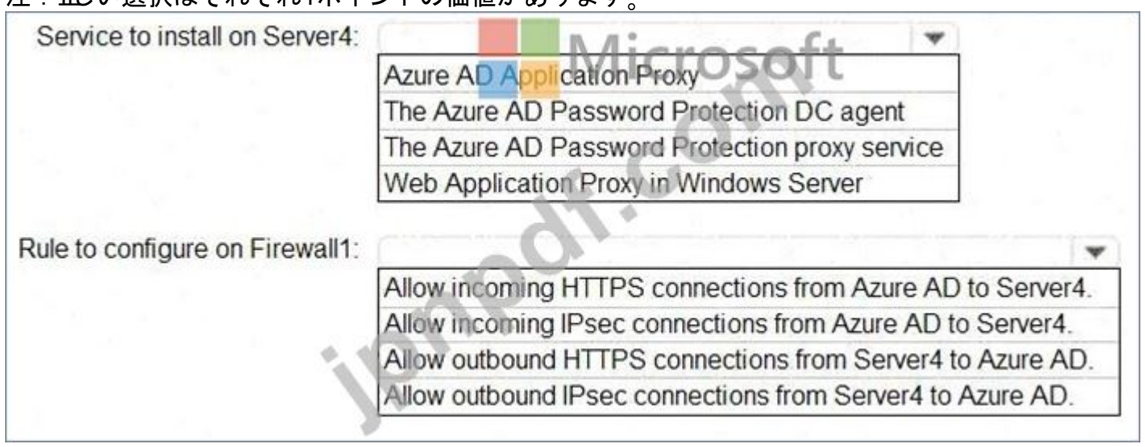
Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows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

ActiveDirectoryフォレストに同期するAzureActive Directory（Azure AD）テナントがあります。Azure ADには、多要素認証（MFA）が適用されます。

App1をAzureADユーザーに公開できることを確認する必要があります。

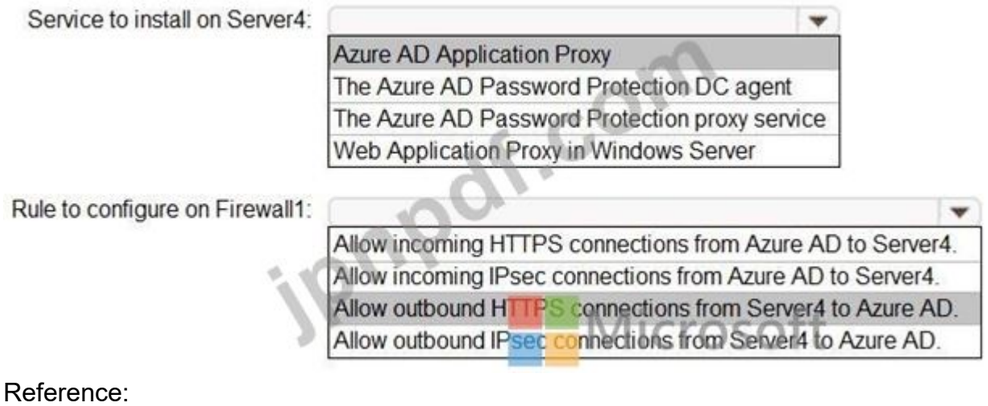
サーバーとFirewall1で何を構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

Explanation:



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

最新問題: **45**
Site! という名前の Microsoft SharePoint Online サイトを含む Microsoft 365 E5 サブスクリプションがあります。サイト！hosts PDF ファイル ユーザーが Sitel から直接ファイルを印刷できないようにする必要があります。
Microsoft Defender for Cloud Apps ポータルで作成する必要があるポリシーの種類はどれですか?
A. セッション ポリシー
B. アクセス ポリシー
C. ファイル ポリシー
D. 活動方針
Answer: A (メーッセージを残す**)**

最新問題: **46**
Package1 に対して計画された変更を実装する必要があります。アクセス レビューを作成および管理できるのはどのユーザーですか?
A. ユーザー 3 とユーザー 4
B. User3 のみ
C. User5 のみ
D. ユーザー 3 とユーザー 5

E. ユーザー 4 とユーザー 5
F. User4のみ
Answer: D (メーッセージを残す**)**

最新問題: **47**
Microsoft Entra テナントがあります。
サインイン失敗回数が 10 回をロックアウトしきい値とするスマート ロックアウトを実装する必要があります。Microsoft Entra 管理センターで何を構成すればよいですか?
A. サインインリスクポリシー
B. パスワード保護
C. ユーザーリスクポリシー
D. 認証の強度
Answer: B (メーッセージを残す**)**

最新問題: **48**
Microsoft 365 テナントがあります。
Azure Active Directory (Azure AD) テナントに同期する Active Directory ドメインがあります。
ユーザーは、会社のハードウェア ファイアウォールを使用してインターネットに接続します。ユーザーは、Active Directory 資格情報を使用してファイアウォールに対して認証を行います。
Azure AD を使用して外部アプリケーションへのアクセスを管理する予定です。
ファイアウォール ログを使用して、管理されていない外部アプリケーションとそれらにアクセスするユーザーのリストを作成する必要があります。
情報を収集するために何を使用する必要がありますか?
A. Azure AD のエンタープライズ アプリケーション
B. Microsoft Defender for Cloud Apps の Cloud App Discovery
C. Azure AD のアクセス レビュー
D. Azure Monitor のアプリケーション インサイト
Answer: B (メーッセージを残す**)**

最新問題: **49**
Microsoft365テナントがあります。
すべてのユーザーは携帯電話とラップトップを持っています。
ユーザーは、Wi-Fiアクセスや携帯電話接続がない遠隔地から頻繁に作業します。ユーザーは、離れた場所から作業しているときに、ラップトップをインターネットにアクセスできる有線ネットワークに接続します。
多要素認証（MFA）を実装することを計画しています。
ユーザーがリモートロケーションから使用できるMFA認証方法はどれですか？
A. MicrosoftAuthenticatorアプリを介した通知
B. メール

C. セキュリティの質問
D. MicrosoftAuthenticatorアプリからの確認コード
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#verification-code-from-mobile-app

最新問題**: 50**
Microsoft Entra テナントには、Group1 というグループと、User1 および User2 という 2 人のユーザーが含まれています。User1 は Group1 のメンバーです。
App1 という名前のエンタープライズ アプリケーションを登録します。
App1 のセルフサービス アプリケーション アクセスを有効にし、次の設定を構成します。
* ユーザーがこのアプリケーションへのアクセスをリクエストできるようにする: はい
* 割り当てられたユーザーをどのグループに追加するか: グループ1
* このアプリケーションへのアクセスを許可する前に承認が必要: はい
* このアプリケーションへのアクセスを承認できるユーザー: User2
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Answer:

Statements	Yes	No
User1 must request access to App1 before they can use the app.	○	○
If User2 requests access to App1, they will be added to Group1 automatically.	○	○
User2 can approve App1 requests by using the Microsoft Entra admin center.	○	○

Explanation:
User1 must request access to App1 before they can use the app: No
If User2 requests access to App1, they will be added to Group1 automatically: Yes User2 can approve App1 requests by using the Microsoft Entra admin center: Yes Let's break this down step by step based on Microsoft Entra ID self-service application access and the configured settings, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Self-Service Application Access in Microsoft Entra ID:
Self-service application access in Microsoft Entra ID allows users to request access to applications without needing an administrator to manually assign them. This is configured on a per-application basis.
The settings for App1 are:
Allow users to request access to this application: Yes- Users can request access to App1.
To which group should assigned users be added: Group1- Users who are granted access will be added to Group1, which provides the necessary permissions to use App1.
Require approval before granting access to this application: Yes- Access requests must be approved before the user is added to Group1.
Who is allowed to approve access to this application: User2- User2 is the designated approver for access requests to App1.
Statement 1: User1 must request access to App1 before they can use the app.
Analysis:
User1 is already a member of Group1, as stated in the question.
The self-service settings specify that users who are granted access to App1 will be added to Group1. This implies that membership in Group1 is what grants access to App1.
Since User1 is already a member of Group1, they already have access to App1. In Microsoft Entra ID, if a user is already assigned to an application (either directly or via group membership), they do not need to request access through the self-service process-they can simply use the app.
The self-service access request process is for users who are not yet assigned to the app (i.e., not in Group1).
Since User1 is already in Group1, they do not need to request access.
Conclusion:This statement isNo. User1 does not need to request access because they are already a member of Group1 and can use App1 immediately.
Statement 2: If User2 requests access to App1, they will be added to Group1 automatically.
Analysis:
User2 is not a member of Group1 (the question does not state that User2 is in Group1).
The self-service settings allow users to request access to App1, and the setting "To which group should assigned users be added: Group1" means that users who are granted access will be added to Group1.
However, the setting "Require approval before granting access to this application: Yes" means that User2's request must be approved before they are added to Group1. The approver for App1 requests is User2 themselves, which introduces a potential conflict.
In Microsoft Entra ID, if a user is both the requester and the approver, the system typically allows them to approve their own request (unless additional policies prevent this, which is not specified in the

question).
Therefore, User2 can request access and approve their own request.
Once the request is approved, User2 will be added to Group1 automatically as per the self-service settings.
The term "automatically" in the statement refers to the process after approval-once approved, the addition to Group1 happens without further manual intervention.
Conclusion:This statement isYes. If User2 requests access to App1 and approves their own request, they will be added to Group1 automatically.
Statement 3: User2 can approve App1 requests by using the Microsoft Entra admin center.
Analysis:
The self-service settings specify that User2 is the designated approver for access requests to App1.
In Microsoft Entra ID, approvers can manage access requests through the Microsoft Entra admin center (via the "My Access" portal or the "Access Requests" section, depending on their role and permissions).
User2, as the designated approver, will receive a notification (via email or the My Access portal) when a request is made. They can then log into the Microsoft Entra admin center, navigate to the access requests section, and approve or deny the request.
Even though User2 is not explicitly an admin, the fact that they are designated as the approver for App1 requests grants them the ability to approve requests through the Microsoft Entra admin center.
Conclusion:This statement isYes. User2 can approve App1 requests using the Microsoft Entra admin center.
Additional Considerations:
If User2 were not allowed to approve their own request (e.g., due to a separation of duties policy), Statement
2 might be affected. However, Microsoft Entra ID does not enforce such a restriction by default, and the question does not specify any additional policies.
The Microsoft Entra admin center is the primary interface for managing access requests, but users can also approve requests via email links or the My Access portal. The statement specifically mentions the admin center, which is a valid method.
Conclusion:
Statement 1:No- User1 does not need to request access since they are already in Group1.
Statement 2:Yes- User2 will be added to Group1 automatically after their request is approved (by themselves).
Statement 3:Yes- User2 can approve requests using the Microsoft Entra admin center.
References:
Microsoft Entra ID documentation: "Configure self-service application access" (Microsoft Learn:https://learn.
microsoft.com/en-us/entra/identity/enterprise-apps/configure-self-service) Microsoft Entra ID documentation: "Manage access requests" (Microsoft Learn:https://learn.microsoft.com
/en-us/entra/identity/governance/access-reviews-overview)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers self-service application access and approval workflows in Microsoft Entra ID.

最新問題**: 51**
1 つの Microsoft Entra テナントにリンクされた 3 つの Azure サブスクリプションがあります。
高度な特権を持つアカウントに関連するリスクを評価し、修正する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
何を使えばいいのでしょうか？
A. Microsoft Entra 権限管理
B. 特権 ID 管理 (PIM)
C. Microsoft Entra 認証済み ID
D. グローバルセキュアアクセス
Answer: B (メーッセージを残す**)**

最新問題**: 52**
次の表に示す Azure Active Directory (Azure AD) ユーザーを作成します。

Name	Multi-factor auth status	Device
User1	Disabled	Device1
User2	Enabled	Device2
User3	Enforced	Device3

2021 年 2 月 1 日に、次の図に示すように多要素認証 (MFA) 設定を構成します。

次の表に示すように、デバイス上の Azure AD に対するユーザー認証。

Date	User
February 2, 2021	User1
February 5, 2021	User2
February 21, 2021	User1

2021 年 2 月 26 日、各ユーザーの多要素認証ステータスはどうなりますか?

A.

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

B.

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

C.

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

D.

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

Answer: A (メーッセージを残す)

最新問題**: 53**

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。

アマゾン ウェブ サービス (AWS) アカウント、Google Workspace サブスクリプション、および GitHub アカウントをお持ちです。

Azure サブスクリプションをデプロイし、Microsoft 365 Defender を有効にします。

Microsoft Defender for Cloud Apps を使用して OAuth 認証要求を監視できることを確認する必要があります。

解決策: Microsoft 365 Defender ポータルから、アマゾン ウェブ サービス アプリ コネクタを追加します。

これは目標を達成していますか?

A. いいえ

B. はい

Answer: B (メーッセージを残す)

最新問題: **54**

AU1 という管理単位を含む Microsoft Entra テナントがあります。AU1 は割り当てられたメンバーシップ用に構成されています。

テナントには次の表に示すユーザーが含まれます。

Name	Department	Administrative unit
User1	HR	*None*
User2	IT	AU1

The tenant contains the groups shown in the following table.

Name	Members	Administrative unit
HR	User1	AU1
IT	User2	AU1

AU1 の場合、次の構成を更新します。

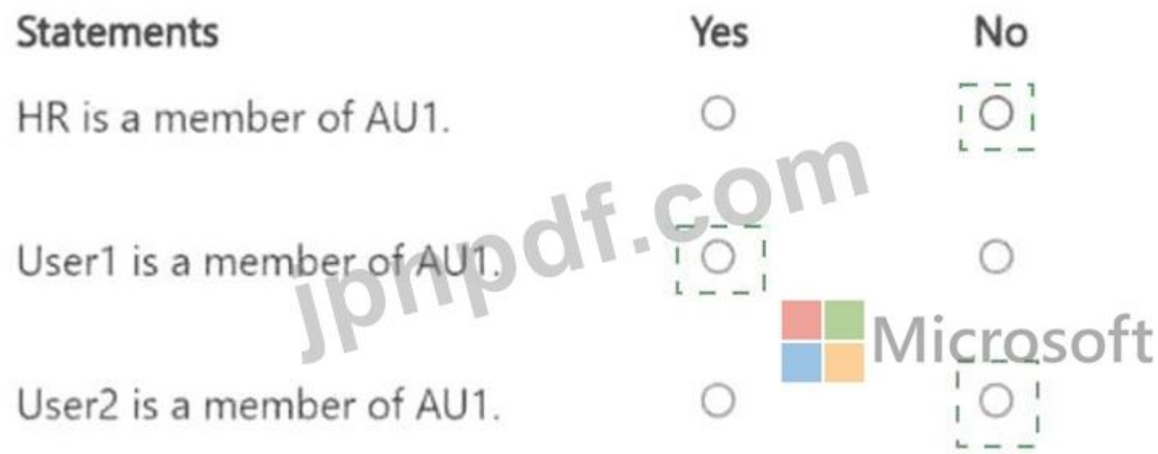
会員種別: ダイナミックユーザー

動的メンバーシップルール: (user.department -eq "hr")

以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

Statements	Yes	No
HR is a member of AU1.	○	○
User1 is a member of AU1.	○	○
User2 is a member of AU1.	○	○

Answer:



Explanation:
HR is a member of AU1: No
User1 is a member of AU1: Yes
User2 is a member of AU1: No
Let's break this down step by step based on Microsoft Entra ID dynamic membership rules, administrative units, and group membership, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding Administrative Units and Dynamic Membership in Microsoft Entra ID:
Administrative Units (AUs):Administrative Units in Microsoft Entra ID are used to delegate administrative tasks to a subset of users, groups, or devices. They allow you to scope administrative roles (e.g., User Administrator) to specific users or groups within the AU.
Membership Types for AUs:
Assigned Membership:Members (users, groups, or devices) are manually added to the AU by an administrator.
Dynamic Membership:Members are automatically added or removed based on a dynamic membership rule, similar to dynamic groups. Dynamic membership for AUs can be applied to users or devices (but not groups directly).
The question states that AU1 is initially configured for assigned membership but is then updated to useDynamic Usermembership with the rule (user.department -eq "HR").
Dynamic Membership Rule:The rule (user.department -eq "HR") means that AU1 will automatically include all users whose department attribute in Microsoft Entra ID is set to "HR". This rule applies to users, not groups or devices, because the membership type is "Dynamic User." Impact of Changing AU1 to Dynamic Membership:
When AU1's membership type is changed from assigned to dynamic, the existing assigned memberships (e.
g., User2, HR group, IT group) are no longer relevant. Thedynamic rule takes over, and AU1's membership is determined solely by the rule (user.department -eq "HR").
Dynamic User Membership:Only users whose attributes match the rule will be members of AU1. Groups (like HR and IT) are not evaluated by this rule because the membership type is "Dynamic User," not "Dynamic Group." Let's evaluate the users based on the rule:
User1:Department = "HR". The rule (user.department -eq "HR") matches, so User1 will be dynamically added to AU1.
User2:Department = "IT". The rule does not match, so User2 will not be a member of AU1, even though they were previously assigned to AU1 and are a member of the IT group.
Groups (HR and IT):The dynamic membership rule for AU1 applies to users, not groups. Therefore, groups like HR and IT are not directly evaluated by the rule. However, we need to consider whether group membership in AU1 affects the statements.
Statement 1: HR is a member of AU1:
Analysis:
The HR group is listed in the second table with AU1 as its administrative unit, indicating that it was initially assigned to AU1 when AU1 used assigned membership.
However, AU1's membership type has been updated to "Dynamic User" with the rule (user.department -eq
"HR"). Dynamic User membership applies to users, not groups.

In Microsoft Entra ID, administrative units with dynamic user membership do not include groups as members unless the AU's membership type is explicitly set to "Dynamic Group" (which is not the case here).
When AU1 was changed to dynamic membership, the HR group would no longer be considered a member of AU1 because the dynamic rule only evaluates users. Groups are not dynamically added to AUs based on user attributes.
Conclusion:The HR group is not a member of AU1 after the change to dynamic membership. Therefore, this statement isNo.
Statement 2: User1 is a member of AU1:
Analysis:
User1 has the department attribute set to "HR" (from the first table).
The dynamic membership rule for AU1 is (user.department -eq "HR"), which matches User1's department.
Therefore, User1 will be automatically added to AU1 as a member based on the dynamic rule.
Additionally, User1 is a member of the HR group, which was initially assigned to AU1. However, since AU1 now uses dynamic membership, the HR group's assignment to AU1 is irrelevant. User1's membership in AU1 is determined solely by the dynamic rule, not their group membership.
Conclusion:User1 is a member of AU1 because their department matches the dynamic rule. Therefore, this statement isYes.
Statement 3: User2 is a member of AU1:
Analysis:
User2 has the department attribute set to "IT" (from the first table).
The dynamic membership rule for AU1 is (user.department -eq "HR"), which does not match User2's department.
User2 was initially assigned to AU1 (as shown in the first table) and is a member of the IT group, which was also assigned to AU1. However, when AU1's membership type was changed to "Dynamic User," the assigned memberships (including User2 and the IT group) are no longer relevant.
The dynamic rule only includes users with the department "HR," so User2 is not added to AU1.
Conclusion:User2 is not a member of AU1 because their department does not match the dynamic rule.
Therefore, this statement isNo.
Additional Considerations:
If AU1's membership type were "Dynamic Group" instead of "Dynamic User," we would evaluate whether the HR and IT groups match a group-based rule. However, the question specifies "Dynamic User," so the rule applies to user attributes only.
The initial assigned memberships (e.g., User2, HR group, IT group) are overridden by the dynamic membership rule. Microsoft Entra ID does not retain assigned memberships when an AU or group is converted to dynamic membership.
The HR and IT groups being assigned to AU1 initially does not affect the dynamic membership of users, but it might be relevant for administrative scoping (e.g., if an admin role is scoped to AU1). However, the statements are about membership, not administrative roles.
Conclusion:Based on the dynamic membership rule (user.department -eq "HR") for AU1:
HR group:Not a member of AU1 because dynamic user membership does not apply to groups.
User1:A member of AU1 because their department is "HR," matching the rule.
User2:Not a member of AU1 because their department is "IT," which does not match the rule.Therefore, the answers are:
HR is a member of AU1:No
User1 is a member of AU1:Yes
User2 is a member of AU1:No
References:
Microsoft Entra ID documentation: "Dynamic membership rules for groups and administrative units" (Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/users/groups-dynamic-membership)
Microsoft Entra ID documentation: "Manage administrative units" (Microsoft Learn:https://learn.microsoft.
com/en-us/entra/identity/role-based-access-control/administrative-units) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers dynamic membership rules and administrative units in Microsoft Entra ID.

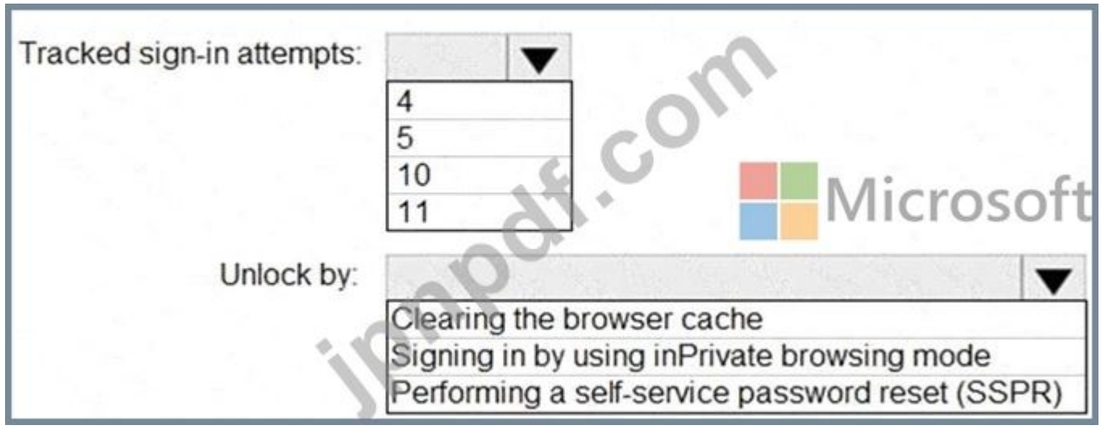
最新問題: **55**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。

Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

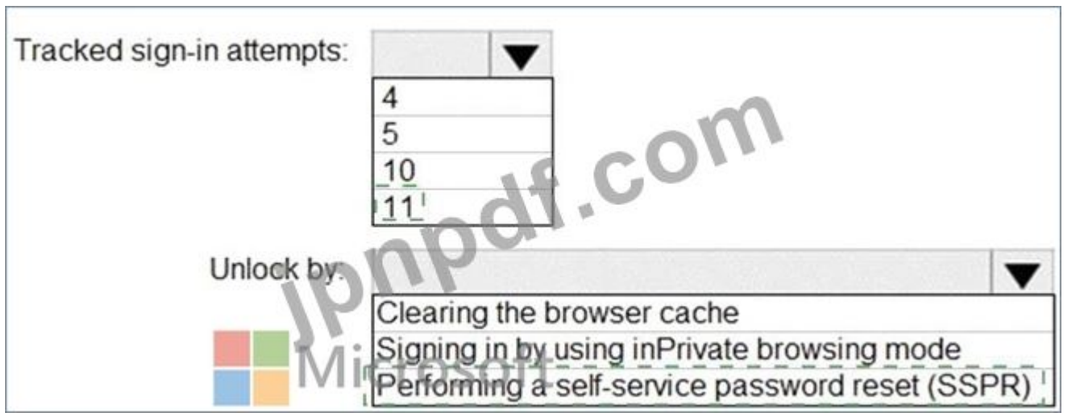
User1 は Group1 の所有者です。
次の設定を持つアクセス レビューを作成します。
* レビュー対象: チーム + グループ
* 対象: すべてのユーザー
* グループ: グループ1
* レビュー担当者: ユーザーは自分のアクセスをレビューします
User3 のアクセスレビューを実行できるのはどのユーザーですか?
A. ユーザー1のみ
B. ユーザー3のみ
C. ユーザー1とユーザー2のみ
D. ユーザー1、ユーザー2、ユーザー3
Answer: B (メーッセージを残す)
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on the Microsoft Entra access review settings and the principles outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Access Review Settings:
What to review: Teams + GroupsThis indicates that the access review is evaluating memberships in Teams and Groups within the Microsoft Entra tenant. Since the group specified is Group1, the review focuses on Group1 membership.
Scope: All usersThe scope defines who is being reviewed. "All users" in this

最新問題: **56**
User1という名前のユーザーが、次の誤ったパスワードを入力してテナントにサインインしようとしました。
Pa55w0rd12
Pa55w0rd12
Pa55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55w.rd123
Pa55word12

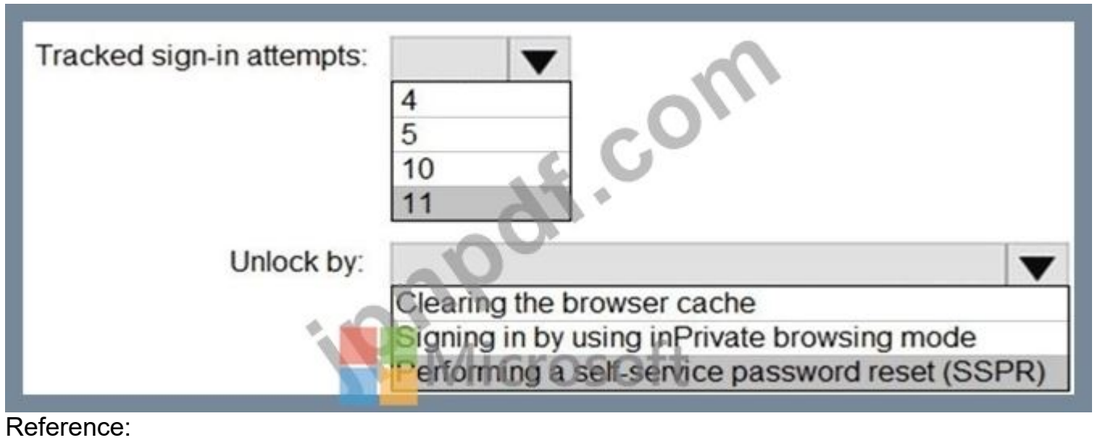
Pa55word12
Pa55w.rd12
User1で追跡されたサインインの試行回数と、300秒のロックアウト期間が終了する前にUser1がアカウントのロックを解除する方法を特定する必要があります。
何を特定する必要がありますか？答えるには、適切なものを選択してください
注：丌しい選択はそれぞれ1ポイントの価値があります。



Answer:



Explanation:



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

最新問題: **57**
Azure AD Privileged Identity Management (PIM) を使用する Azure サブスクリプションがあります。
クラウド アプリケーション管理者ロールに適格なユーザーを特定する必要があります。
Privileged Identity Management 設定のどのブレードを使用する必要がありますか?
A. Review access
B. Azure AD roles
C. Azure resources
D. Privileged access groups
Answer: D (メーッセージを残す**)**

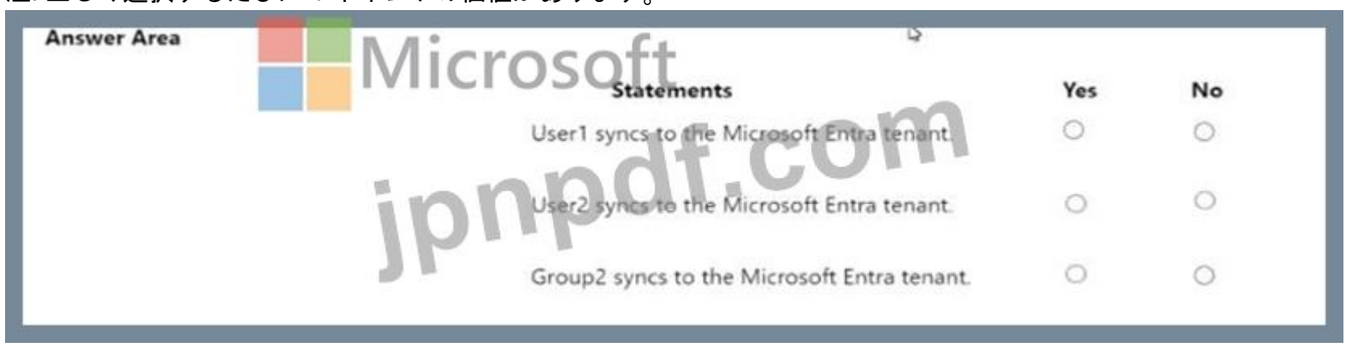
最新問題: **58**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。ドメインには、次の表に示すオブジェクトが含まれています。

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

Microsoft Entra Connect をインストールします。 「ドメインと OU のフィルタリング」の説明に従って、ドメインと OU のフィルタリング設定を構成します。([ドメインと OU フィルタリング] タブをクリックします。)

「ユーザーとデバイスのフィルター」の説明に従って、ユーザーとデバイスのフィルター設定を構成します。([ユーザーとデバイスのフィルター] タブをクリックします。) 次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

Explanation:

Answer Area

Statements	Yes	No
User1 syncs to the Microsoft Entra tenant.	●	○
User2 syncs to the Microsoft Entra tenant.	○	●
Group2 syncs to the Microsoft Entra tenant.	●	○

最新問題: **59**
次の表に示すカスタム ロールを含む Azure サブスクリプションがあります。

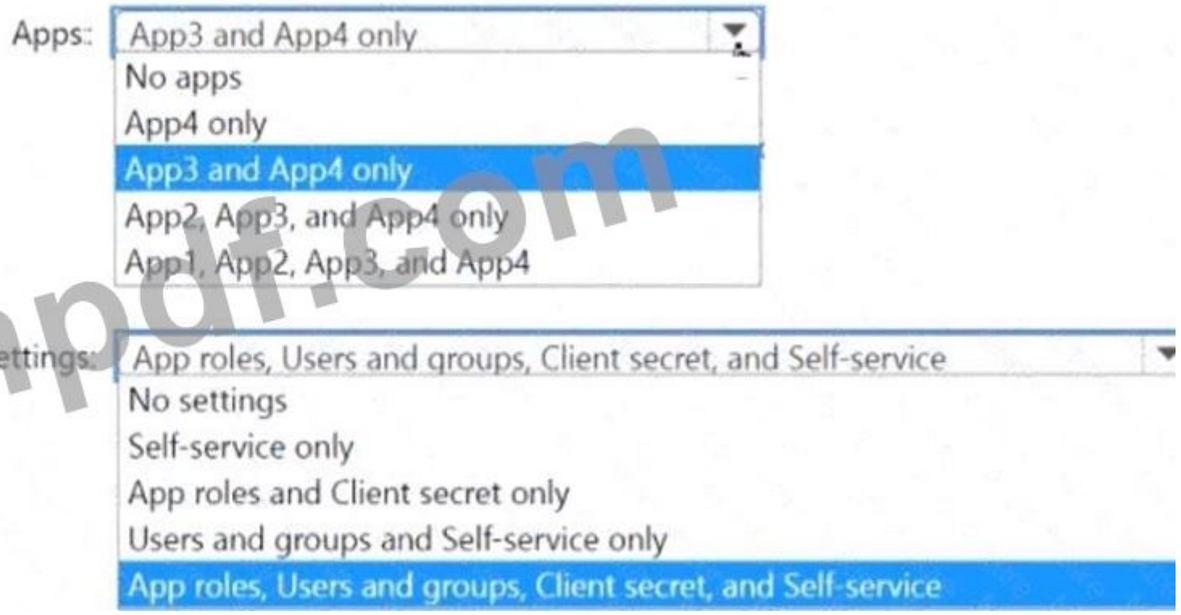
Name	Type
Role1	Azure Active Directory (Azure AD) role
Role2	Azure subscription role

Azure portal を使用して、Role3 という名前のカスタム Azure サブスクリプション ロールを作成する必要があります。Role3 は、既存の役割のベースライン権限を使用します。Role3 を作成するためにどのロールを複製できますか?
A. 組み込みの Azure サブスクリプション ロールと組み込みの Azure AD ロールのみ
B. Role2 のみ
C. 組み込みの Azure サブスクリプション ロールのみ
D. Role1、Role2 組み込み Azure サブスクリプション ロール、および組み込み Azure AD ロール
E. 組み込みの Azure サブスクリプション ロールと Role2 のみ
Answer: (解答を表示する)

最新問題: **60**
Azure AD テナントがあります。
次の表に示すタスクを実行します。

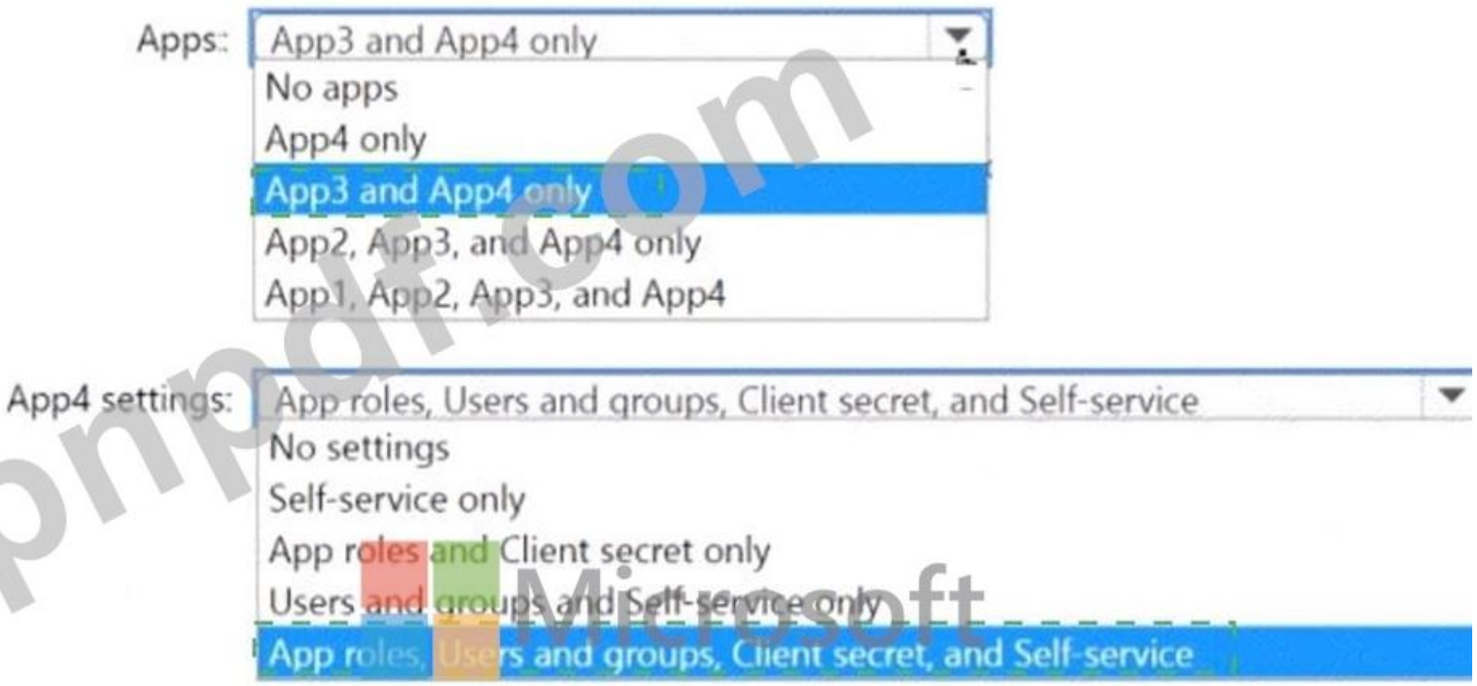
Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users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

4 月 5 日に、管理者は App1、App2、App3、および App4 を削除します。
アプリと設定を復元する必要があります。
4 月 16 日に復元できるアプリはどれですか? 4 月 16 日に App4 のどの設定を復元できますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

Answer Area



Explanation:

最新問題: **61**
Azure サブスクリプションをお持ちです。
権限を自動的に監視し、適切なサイズのロールを作成して実装するには、Microsoft Entra Permissions Management を使用する必要があります。ソリューションは、最小権限の原則に従う必要があります。
アクセス許可管理のサービス プリンシパルに割り当てるロールはどれですか?
A. 貢献者
B. ユーザー アクセス管理者
C. 所有者
D. 読者
Answer: (解答を表示する)

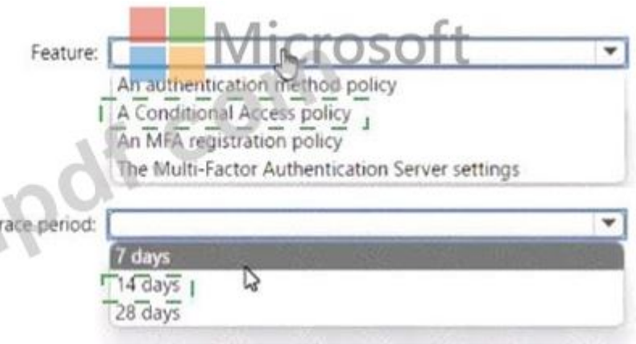
最新問題: **62**
Microsoft Entra テナントがあります。
多数の新しいアプリがテナントに追加されたことがわかります。
新しいエンタープライズ アプリケーションの承認プロセスを実装する必要があります。何をすべきでしょうか?
A. Microsoft Defender ポータルから、Cloud Discovery 異常検出ポリシーを作成します。
B. Microsoft Entra 管理センターから、管理者の同意設定を構成します。
C. Microsoft Entra 管理センターからアクセス レビューを構成します。
D. Microsoft Defender ポータルから、アプリ コネクタを構成します。
Answer: B (メーッセージを残す)

最新問題: **63**
Microsoft 365 E5 サブスクリプションをお持ちです。
ユーザーがサブスクリプションにサインインするときに、カスタム使用条件 (Toll) 契約に同意するように求めるプロンプトが表示されるようにする必要があります。
何を設定すればよいでしょうか?
A. ライフサイクルワークフロー
B. アクセス パッケージ

C. 認証方法
D. 条件付きアクセスポリシー
Answer: (解答を表示する**)**

最新問題**: 64**
計画された変更をサポートし、MFA の技術要件を満たす必要があります。
どの機能を使用する必要がありますか? また、ユーザーが登録を完了するまでにどのくらいかかりますか? 回答するには、回答エリアで適切なオプションを選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。
Answer Area

Answer:
Answer Area



Explanation:

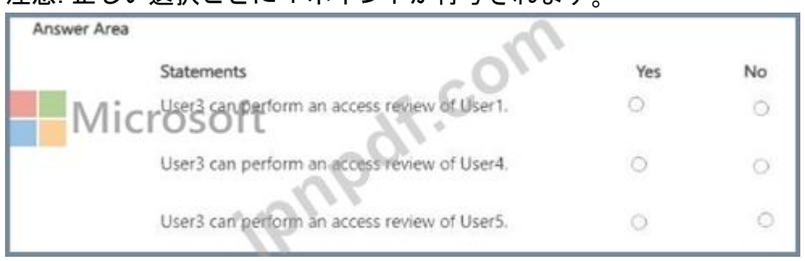
最新問題**: 65**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryフォレストに同期するAzureActive Directory（Azure AD）テナントがあります。
Active Directoryでユーザーアカウントが無効になっている場合でも、無効になっているユーザーは最大30分間AzureADに対して認証できることがわかります。
Active Directoryでユーザーアカウントが無効になっている場合、そのユーザーアカウントがAzureADへの認証をすぐに阻止されるようにする必要があります。

解決策 :パススルー認証を構成します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

最新問題**: 66**
Group! と Group2 という 2 つのグループと、次の表に示すユーザーを含む Microsoft Entra テナントがあります。

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

グループ2はグループ1のメンバーです。
次の設定を持つアクセス レビューを構成します。
* 名前: レビュー 1
* レビュー対象を選択: チーム + グループ
* レビュー範囲: チーム + グループを選択
* グループ: グループ1
* 対象: ゲストユーザーのみ
* レビュー担当者を選択: グループ所有者
次の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

Explanation:

最新問題: **67**
Microsoft 365 サブスクリプションをお持ちです。
ユーザーが企業アプリケーションに自分のプロファイルへのアクセスを許可できるようにする必要があります。ソリューションでは、ユーザーが委任されたユーザー権限（読み取り権限とプロファイル権限）にのみ同意できるようにする必要があります。
最初に何を設定する必要がありますか?
A. 権限の分類
B. 個人情報保護設定
C. セキュリティのデフォルト
D. 管理者の同意設定
Answer: D (メーッセージを残す**)**

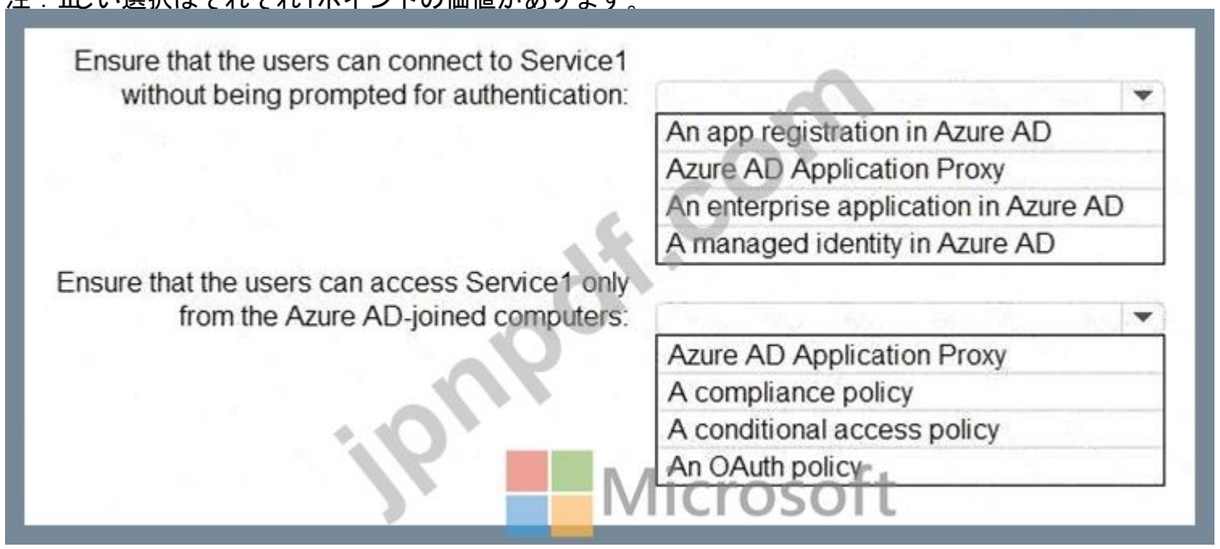
最新問題: **68**
contoso.com という名前の Microsoft Entra テナントがあり、その中に Appl という名前のエンタープライズ アプリケーションが含まれています。
請負業者は user1@outlook.com の資格情報を使用します。
請負業者に App1 へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @outlook.com として認証できる必要があります。
何をすべきでしょうか?
A. New-Mguserコマンドレットを実行する
B. Microsoft Entra Connect 同期を実装します。
C. 外部コラボレーション設定を構成する
D. New-MgInvitationコマンドレットを実行します
Answer: D (メーッセージを残す**)**

最新問題: **69**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
ActiveDirectoryフォレストに同期するAzureActive Directory（Azure AD）テナントがあります。
Active Directoryでユーザーアカウントが無効になっている場合でも、無効になっているユーザーは最大30分間AzureADに対して認証できることがわかります。
Active Directoryでユーザーアカウントが無効になっている場合、そのユーザーアカウントがAzureADへの認証をすぐに阻止されるようにする必要があります。
解決策：条件付きアクセスポリシーを構成します。
これは目標を達成していますか？
A. はい
B. いいえ

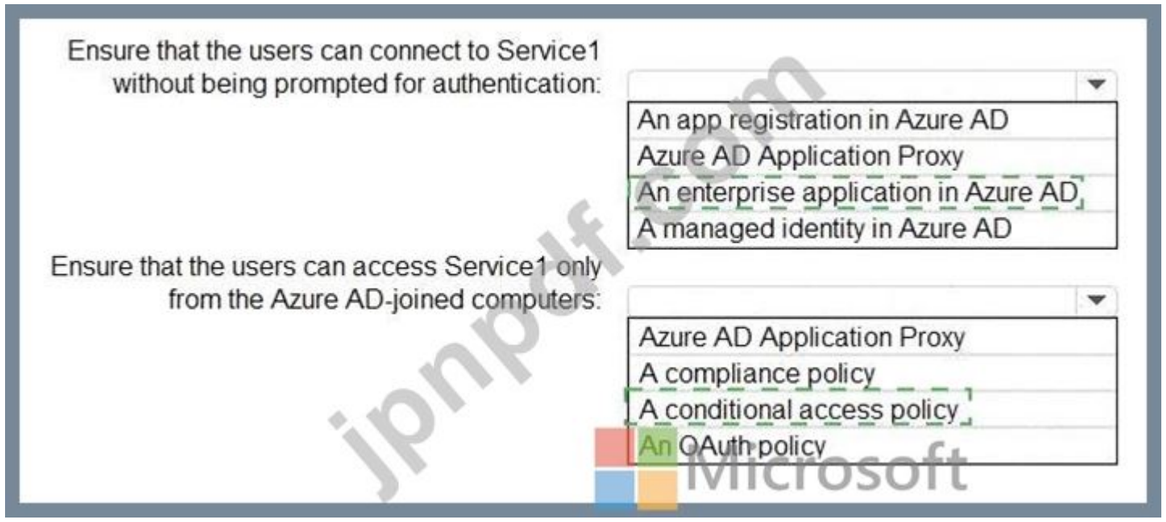
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

最新問題**: 70**
クラウドベースのエンタープライズアプリを含むAzureActive Directory（Azure AD）テナントがあります。
My Appsポータルで、関連するアプリをカテゴリにグループ化する必要があります。
何を作成する必要がありますか？
A. タグ
B. コレクション
C. 命名ポリシー
D. 動的グループ
Answer: B (メーッセージを残す**)**
Reference:
https://support.microsoft.com/en-us/account-billing/customize-app-collections-in-the-my-apps-portal-2dae6b8a-d8b0-4a16-9a5d-71ed4d6a6c1d

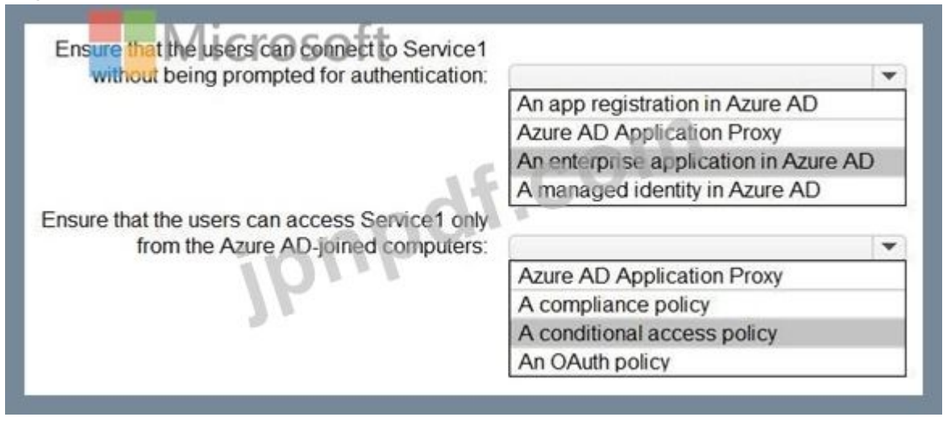
最新問題**: 71**
あなたの会社にはMicrosoft365テナントがあります。
すべてのユーザーは、Windows 10を実行し、Azure Active Directory（Azure AD）テナントに参加しているコンピューターを持っています。
同社は、Service1という名前のサードパーティのクラウドサービスに加入しています。Service1は、OAuthに基づくAzureAD認証と承認をサポートしています。Service1はAzureADギャラリーに公開されています。
ユーザーが認証を求められることなくService1に接続できるようにするためのソリューションを推奨する必要があります。このソリューションでは、ユーザーがAzureADに参加しているコンピューターからのみService1にアクセスできるようにする必要があります。ソリューションは、管理作業を最小限に抑える必要があります。
要件ごとに何をお勧めしますか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

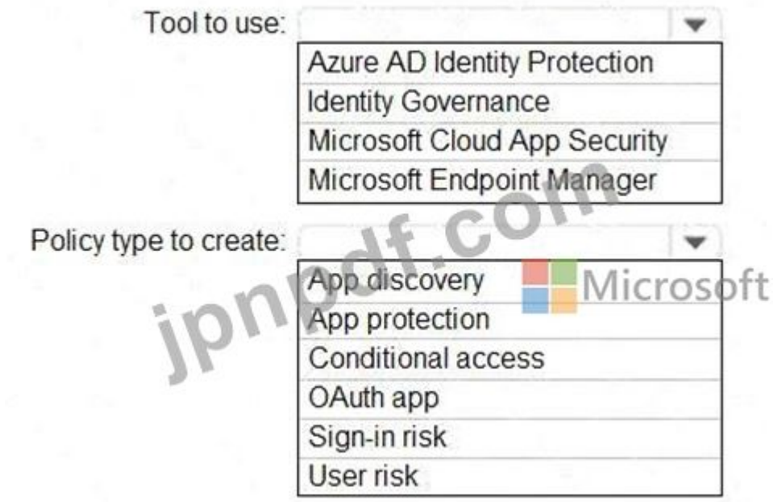


Explanation:

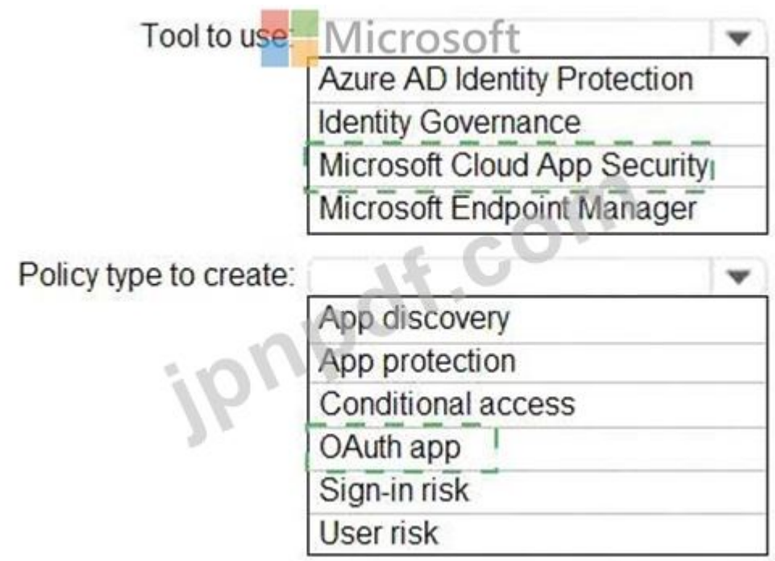


Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

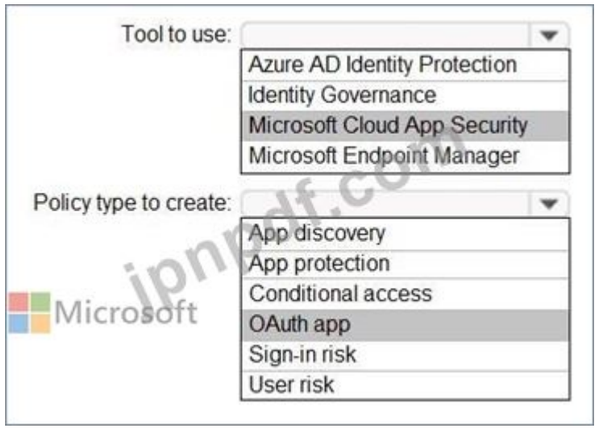
最新問題**: 72**
Microsoft365テナントがあります。
ユーザーは、それぞれのユーザーのMicrosoft365データへのアクセスを制限する必要がある外部のサードパーティアプリケーションを使用する場合があります。ユーザーは、アプリケーションをAzure Active Directory（Azure AD）に登録します。
登録されたアプリケーションがユーザーの電子メールへの読み取りおよび書き込みアクセスを取得した場合は、アラートを受信する必要があります。
あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:



Explanation:



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

最新問題**: 73**
Microsoft365テナントがあります。
現在、基本認証を使用する電子メールクライアントがMicrosoft ExchangeOnlineに接続することを許可しています。
ユーザーがExchangeに接続できることを確認する必要があります。これは、最新の認証プロトコルを使用する電子メールクライアントのみを実行します。
何を実装する必要がありますか？
最新の認証を使用していることを確認する必要があります
A. Microsoft Cloud AppSecurityのOAuthポリシー
B. Azure Active Directory（Azure AD）の条件付きアクセスポリシー
C. Microsoft EndpointManagerのアプリケーション制御プロファイル
D. Microsoft EndpointManagerのコンプライアンスポリシー
Answer: C (メーッセージを残す**)**

最新問題**: 74**
新しい Azure AD テナントをデプロイする予定です。
テナントに対してデフォルトでどの多要素認証 (MFA) 方法が有効になりますか?
A. 音声通話
B. 電子メール OTP
C. Microsoft Authenticator
D. SMS
Answer: D (メーッセージを残す**)**

最新問題**: 75**
多要素認証 (MFA) が強制され、セルフサービス パスワード リセット (SSPR) が有効になっている Azure AD テナントがあります。
割り込みモードで複合登録を有効にします。
User1 という名前の新しいユーザーを作成します。
User1 が結合された登録プロセスを完了するために使用できる 2 つの認証方法はどれですか? それぞれの正解は完全な解決策を示します。
注: 正しく選択するたびに 1 ポイントの価値があります。

A. FID02 セキュリティ キー
B. Windows Hello for Business
C. ハードウェアトークン
D. ワンタイムパスコードメール
E. Microsoft Authenticator アプリ
Answer: (解答を表示する**)**

最新問題**: 76**
オンプレミス ネットワークには、Active Directory ドメイン サービス (AD DS) ドメインと CAT という名前の証明機関 (CA) が含まれています。
Microsoft Entra テナントがあります。
Microsoft Entra 証明書ベースの認証を実装する必要があります。ソリューションでは、ユーザーが CAT によって発行された証明書を使用してサインインできるようにする必要があります。最初に何をする必要がありますか?
A. CAT の自動登録を有効にします。
B. Windows Hello for Business を展開します。
C. CA1 を認証局として Microsoft Entra テナントに追加します。
D. Azure Key Vault をデプロイします。
Answer: C (メーッセージを残す**)**

最新問題**: 77**
タスク6
Sg-Executive のメンバーが会社のアプリにアクセスできるようにするには、追加のセキュリティ チェックを実装する必要があります。会員は以下のいずれかの条件を満たしている必要があります。
* Microsoft Intune によって準拠としてマークされているデバイスを使用して接続します。
* アプリ保護ポリシーによって保護されているクライアント アプリを使用して接続します。
Answer:
See the Explanation for the complete step by step solution.
Explanation:
To implement additional security checks for the Sg-Executive group members before they can access any company apps, you can use Conditional Access policies in Microsoft Entra. Here's a step-by-step guide:
* Sign in to the Microsoft Entra admin center:
* Ensure you have the role of Global Administrator or Security Administrator.
* Navigate to Conditional Access:
* Go to Security > Conditional Access.
* Create a new policy:
* Select + New policy.
* Name the policy appropriately, such as "Sg-Executive Security Checks".

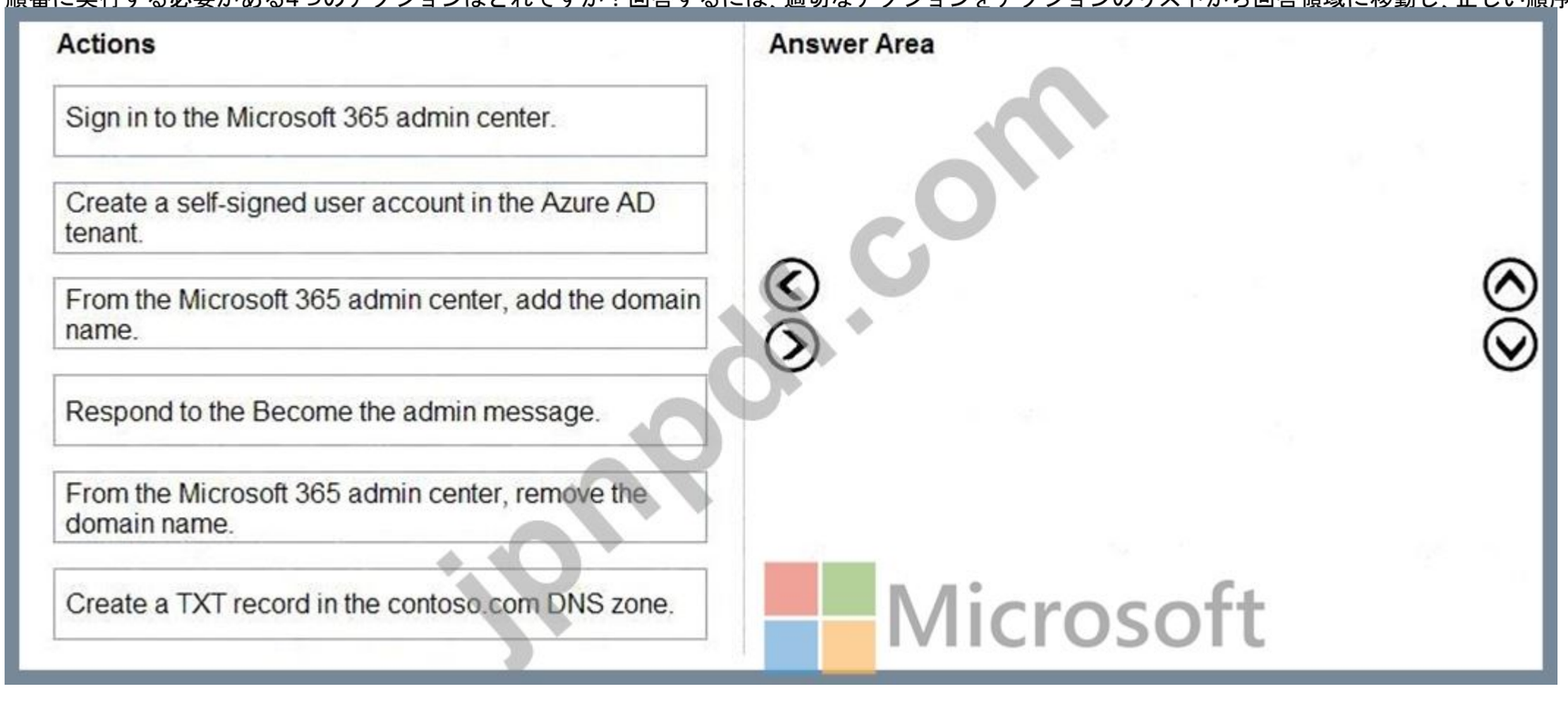
* Assign the policy to the Sg-Executive group:
* Under Assignments, select Users and groups.
* Choose Select users and groups and then Groups.
* Search for and select the Sg-Executive group.
* Define the application control conditions:
* Under Cloud apps or actions, select All cloud apps to apply the policy to any company app.
* Set the device compliance requirement:
* Under Conditions > Device state, configure the policy to include devices marked as compliant by Microsoft Intune.
* Set the app protection policy requirement:
* Under Conditions > Client apps, configure the policy to include client apps that are protected by app protection policies.
* Configure the access controls:
* Under Access controls > Grant, select Grant access.
* Choose Require device to be marked as compliant and Require approved client app.
* Ensure that the option Require one of the selected controls is enabled.
* Enable the policy:
* Set Enable policy to On.
* Review and save the policy:
* Review all settings to ensure they meet the requirements.
* Click Create to save and implement the policy.
By following these steps, you will ensure that the Sg-Executive group members can only access company apps if they meet one of the specified conditions, either by using a compliant device or a protected client app.
This enhances the security posture of your organization by enforcing stricter access controls for executive- level users.

最新問題**: 78**
Microsoft 365 E5 サブスクリプションをお持ちです。
Gateway1 という名前のサードパーティ Web ゲートウェイをデプロイします。
Gateway1 を Microsoft Defender for Cloud Apps と統合する必要があります。ソリューションは以下の要件を満たす必要があります。
* データが Defender for Cloud Apps に自動的に流れるようにします。
* 管理上の労力を最小限に抑えます。
まず何をすべきでしょうか?
A. データソースを追加する
B. アプリ登録を作成する
C. スナップショットレポートを作成する
D. ログコレクターを追加する
Answer: D (メーッセージを残す**)**
Comprehensive and Detailed In-Depth Explanation:
Let's break this down step by step based on Microsoft Defender for Cloud Apps (MDCA) integration with third-party web gateways, as outlined in Microsoft Identity and Access Administrator documentation.
Understanding the Scenario and Requirements:
Microsoft 365 E5 subscription:This subscription includes Microsoft Defender for Cloud Apps, which provides the necessary licensing for integrating with third-party web gateways.
Third-party web gateway named Gateway1:A web gateway (e.g., a Secure Web Gateway like Zscaler, Netskope, or Symantec) is deployed to manage and secure internet traffic. The question does not specify the vendor, but the process for integration with MDCA is generally the same for supported gateways.

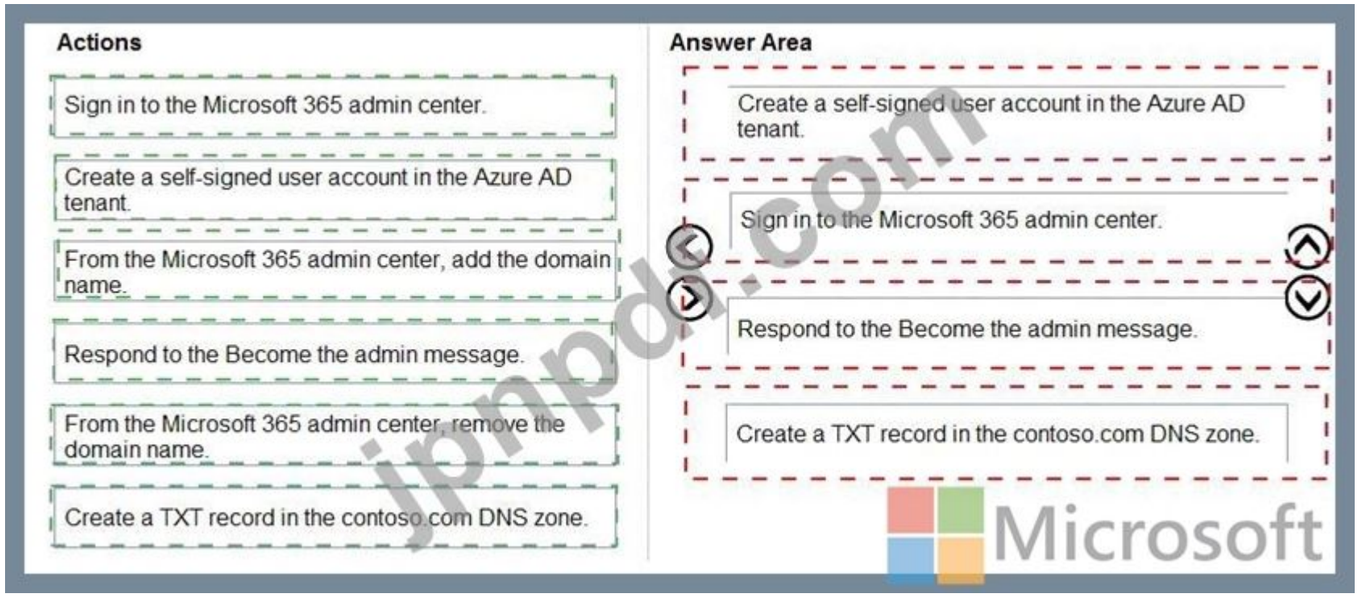
Requirement:Integrate Gateway1 with Microsoft Defender for Cloud Apps to ensure that data (e.g., traffic logs, events) flows automatically to MDCA for analysis, visibility, and policy enforcement. The solution must also minimize administrative effort.
Microsoft Defender for Cloud Apps supports integration with third-party web gateways to provide visibility into cloud app usage, detect shadow IT, and enforce security policies. This integration typically involves collecting logs from the gateway for analysis in MDCA.
How Microsoft Defender for Cloud Apps Integrates with Third-Party Web Gateways:
MDCA can integrate with third-party web gateways by collecting logs that contain traffic data (e.g., user activity, app usage, IP addresses). This allows MDCA to analyze the data and provide insights into cloud app usage, detect threats, and enforce policies.
The primary method for integrating a third-party web gateway with MDCA is toadd a log collector. This involves:
Configuring the web gateway to send logs to a log collector (e.g., via Syslog or FTP).
Setting up a log collector in MDCA to receive and process these logs.
Once configured, the log collector automatically pulls logs from the web gateway, ensuring that data flows to MDCA for analysis.
This method supports automatic data flow and minimizes administrative effort because, after the initial setup, the log collection process runs continuously without manual intervention.
Analyzing the Options:
A: Add a data source:
In Microsoft Defender for Cloud Apps, "data sources" typically refer to sources of user activity data, such as Microsoft Entra ID audit logs, Microsoft 365 audit logs, or other Microsoft services. Adding a data source in MDCA is used to import user activity data for correlation with cloud app usage, but it is not the mechanism for integrating a third-party web gateway.
Third-party web gateways are not considered "data sources" in MDCA; instead, they are integrated via log collectors.
Conclusion:This option is incorrect because adding a data source does not facilitate integration with a third- party web gateway like Gateway1.
B: Create an app registration:
Creating an app registration in Microsoft Entra ID is typically used to integrate cloud apps with MDCA for session control (e.g., via Conditional Access App Control) or to enable API-based log collection for supported apps (e.g., Salesforce, Box).
However, a third-party web gateway like Gateway1 is not a cloud app that requires an app registration. Web gateways are network appliances or services that manage traffic, and their integration with MDCA involves log collection, not app registration.
Conclusion:This option is incorrect because creating an app registration is not relevant to integrating a web gateway with MDCA.
C: Create a snapshot report:
A snapshot report in MDCA is a manual process where an administrator uploads a log file (e.g., a CSV or JSON file) from a third-party service to analyze cloud app usage. This is a one-time, manual process used for discovery (e.g., to identify shadow IT).
The requirement specifies that data must flow "automatically" to Defender for Cloud Apps, and a snapshot report does not meet this requirement because it requires manual uploads each time. It also does not minimize administrative effort due to the ongoing manual intervention.
Conclusion:This option is incorrect because creating a snapshot report does not enable automatic data flow and increases administrative effort.
D: Add a log collector:
Adding a log collector in Microsoft Defender for Cloud Apps is the standard method for integrating third- party web gateways. MDCA supports log collection from many web gateways (e.g., Zscaler, Netskope, Symantec) via Syslog or FTP.
Process:
In the Microsoft Defender for Cloud Apps portal, navigate toSettings > Log collectors.
Add a new log collector, specifying the protocol (e.g., Syslog over TCP/UDP or FTP) and the details of the web gateway (e.g., IP address, port).
Configure Gateway1 to send logs to the log collector (this step is done on the Gateway1 side, typically by the network team).
Once set up, the log collector automatically collects logs from Gateway1 and processes them in MDCA for analysis.
Automatic Data Flow:The log collector ensures that data flows automatically to MDCA, meeting the first requirement.
Minimize Administrative Effort:After the initial setup, the log collector runs continuously without manual intervention, minimizing administrative effort.
Conclusion:This option is correct because adding a log collector is the first step to integrate Gateway1 with MDCA, ensuring automatic data flow and minimizing administrative effort.

Why "Add a log collector" is the First Step:
The question asks for the first step to integrate Gateway1 with Microsoft Defender for Cloud Apps. Adding a log collector is the initial action in MDCA to enable log collection from a third-party web gateway. Subsequent steps (not asked in the question) would include configuring Gateway1 to send logs to the log collector, but this is done outside MDCA (e.g., in Gateway1's management console). The question focuses on the action in MDCA, making "Add a log collector" the correct first step.
Additional Considerations:
The question does not specify the vendor of Gateway1, but Microsoft Defender for Cloud Apps supports log collection from many third-party web gateways (e.g., Zscaler, Netskope, Symantec, Cisco Umbrella). The process is the same regardless of the vendor, as long as the gateway supports Syslog or FTP log export.
If Gateway1 were not a supported web gateway, additional steps (e.g., custom log parsing) might be required, but the question implies Gateway1 can be integrated using standard methods.
The Microsoft 365 E5 subscription includes Microsoft Defender for Cloud Apps, so no additional licensing is required.
Conclusion:To integrate Gateway1 with Microsoft Defender for Cloud Apps, ensuring that data flows automatically and minimizing administrative effort, the first step is toadd a log collectorin MDCA. This sets up the infrastructure to receive logs from Gateway1, enabling automatic data flow for analysis. Therefore, the correct answer isD.
References:
Microsoft Defender for Cloud Apps documentation: "Integrate with a third-party web gateway" (Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/connect-third-party-gateway) Microsoft Defender for Cloud Apps documentation: "Set up a log collector" (Microsoft Learn:https://learn.
microsoft.com/en-us/defender-cloud-apps/log-collector)
Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers integrating Microsoft Defender for Cloud Apps with third-party services for cloud app visibility and control.

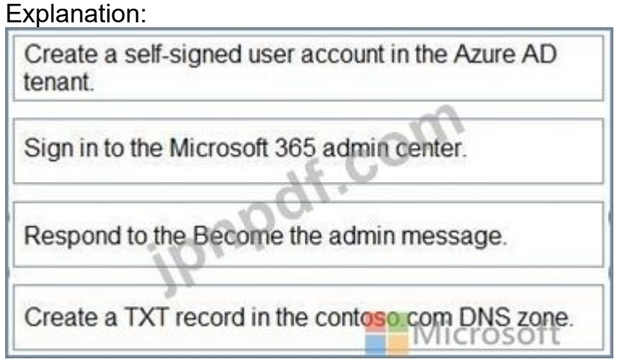
最新問題: 79
contoso.comのSMTPアドレス空間を使用するオンプレミスのMicrosoftExchange組織があります。
ユーザーが自分の電子メールアドレスを使用して、Microsoft365サービスへのセルフサービスサインアップを行っていることがわかりました。
自己署名ユーザーを含むAzureActive Directory（Azure AD）テナントに対するグローバル管理者特権を取得する必要があります。
順番に実行する必要がある4つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答領域に移動し、正しい順序に並べます。



Answer:



Explanation:



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

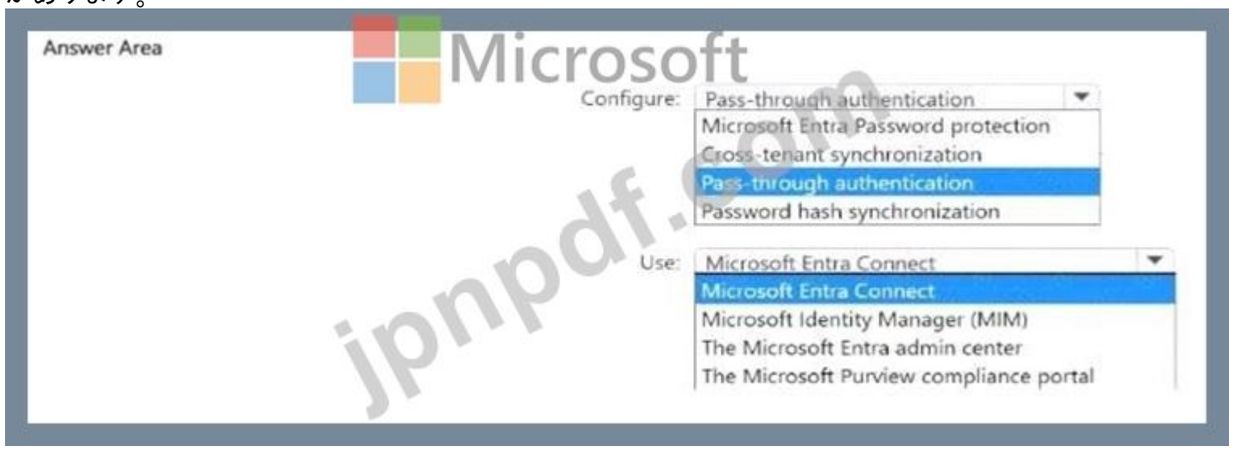
最新問題**: 80**
Microsoft365テナントがあります。
Azure Active Directory（Azure AD）テナントは、オンプレミスのActiveDirectoryドメインに同期します。ドメインには、次の表に示すサーバーが含まれています。

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

ドメインコントローラーはインターネットとの通信ができなくなります。
Server1とServer2にAzureADパスワード保護を実装します。
Windows Server2019を実行するServer4という名前の新しいサーバーを展開します。
単一のサーバーに障害が発生した場合でも、AzureADパスワード保護が引き続き機能することを確認する必要があります。

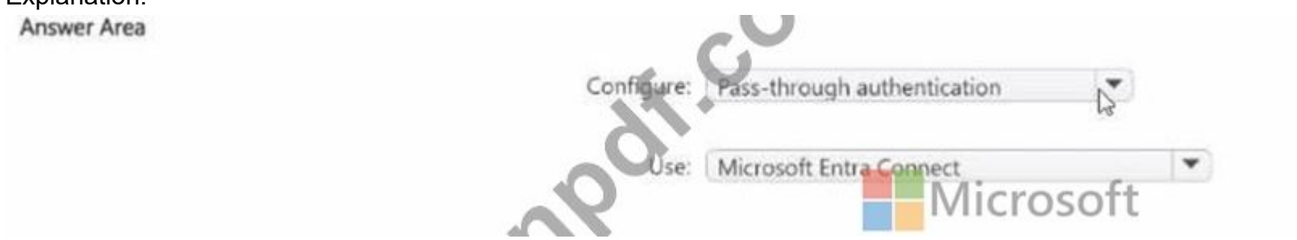
Server4に何を実装する必要がありますか？
A. Azure AD Connect
B. AzureADアプリケーションプロキシ
C. パスワード変更通知サービス（PCNS）
D. AzureADパスワード保護プロキシサービス
Answer: D (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on- premisesdeploy

最新問題: 81
ネットワークには、Microsoft Entra テナントと同期するオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。AD DS ドメインに対してパスワードを検証することで、ユーザー認証が常に行われるようにする必要があります。何を構成して、何を使用すればよいでしょうか。回答するには、回答領域で適切なオプションを選択してください。注: 各選択は 1 ポイントの価値があります。



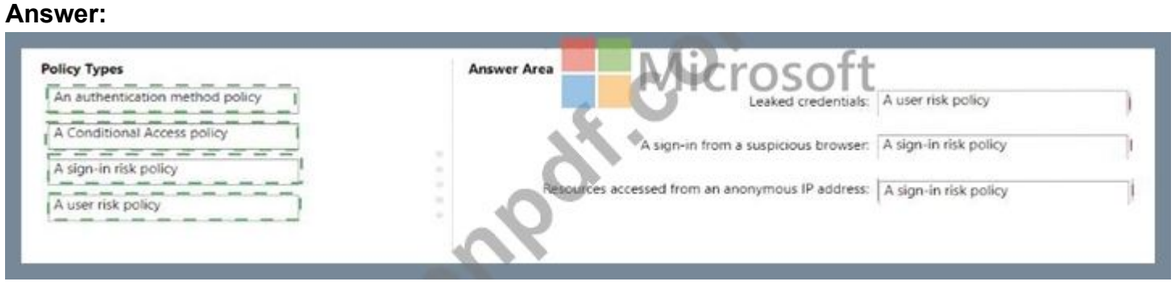
Answer:
Answer Area

Explanation:
Answer Area



最新問題: **82**
最近のセキュリティ インシデントの問題を解決する必要があります。
インシデントごとに何を構成する必要がありますか? 答えるには、適切なポリシー タイプを正しい課題にドラッグします。各ポリシー タイプは、1 回以上使用することも、まったく使用しないこともできます。ペイン間の分割バーをドラッグするか、コンテンツを表示するためにスクロールする必要がある場合があります。
注: それぞれの正しい選択は 1 ポイントの価値があります。

Answer:

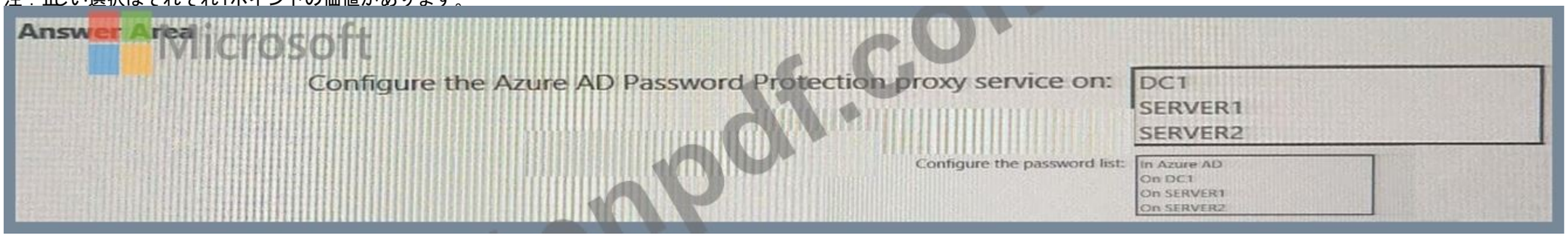


Explanation:

最新問題: **83**
Azure AD テナントがあります。
テンプレート ファイルをアップロードして、25 個の新しいユーザー アカウントを一括作成する必要があります。
テンプレート ファイルにはどのプロパティが必要ですか?

A. オプション A
B. オプション C
C. オプション B
D. オプション D
Answer: C (メーッセージを残す)

最新問題: **84**
認証要件を満たすには、パスワード制限を実装する必要があります。
DC1にAzureADパスワード保護DCエージェントをインストールします。
次に何をすべきですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

Explanation:
Server1
On DC1

最新問題: **85**

あなたは、contoso.com という Microsoft Entra テナントを持つ Contoso, Ltd. という会社で働いています。Contoso は、次の 2 つのパートナー企業とプロジェクトに取り組んでいます。
* adatum.com という Microsoft Entra テナントを持つ A Datum Corporation という会社
* Fabrikam, Inc. という会社で、fabtikam.com という Microsoft Entra テナントがある場合、adatum.com から contoso.com に新しいゲスト ユーザーを招待しようとすると、エラー メッセージが表示されます。
fabiikam.com から contoso.com に新しいゲスト ユーザーを正常に招待できます。adatum.com から contoso.com に新しいゲスト ユーザーを招待できるようにする必要があります。何を構成する必要がありますか?
A. ゲスト招待設定
B. 検証可能な資格情報
C. 名前の付いた場所
D. コラボレーションの制限
Answer: D (メーッセージを残す**)**

最新問題**: 86**
Automation1 という名前の Azure Automation アカウントと Vault1 という名前の Azure Key Vault を含む Azure サブスクリプションがあります。Vault1 には Secret 1 という名前のシークレットが含まれています。
Automation1 に対してシステム割り当てマネージド ID を有効にします。
自動化を確実にする必要があります。Secret1 の内容を読み取ることができます。ソリューションは次の要件を満たす必要があります。
* Automation1 が Vault1 に保存されている他のシークレットにアクセスできないようにします。
* 最小特権の原則に従います。
あなたは何をするべきか？
A. Automation1 から、「実行アカウント」設定を構成します。
B. Secret1 から、アクセス制御 (1AM) 設定を構成します
C. Automation1 から、ID 設定を構成します。
D. Vault1 から、アクセス制御 (1AM) 設定を構成します。
Answer: D (メーッセージを残す**)**

最新問題**: 87**
User1 という名前のユーザーを含む Azure サブスクリプションがあります。サブスクリプションは Microsoft Entra Permissions Management にオンボードされています。ユーザーを提供する必要があります。権限管理にアクセスできるようになります。ソリューションは次の要件を満たす必要があります。
* 最小特権の原則に従います。
* 管理労力を最小限に抑えます。
まず何をすべきでしょうか?
A. アクセス許可管理の [マイ リクエスト] サブタブから、新しいリクエストを作成します。
B. Microsoft Entra 管理センターから、User1 にロールを割り当てます。
C. Microsoft Entra 管理センターから、セキュリティ グループを作成します。
D. アクセス許可管理の [ロール/ポリシー テンプレート] サブタブから、テンプレートを作成します。
Answer: B (メーッセージを残す**)**

最新問題**: 88**
contoso.com と fabhkam.com という 2 つの Microsoft Entra テナントがあります。Contoso.com には、次の表に示すユーザーが含まれています。

Name	Type
User1	Member
User2	Member
User3	Guest

Contoso.com には、次の表に示すグループが含まれています。

Name	Membership type	Members
Group1	Assigned	User1
Group2	Assigned	Group1, User2

contoso.com から fabrikam.com へのテナント間同期を構成し、User3 と Group2 のテナント間同期を有効にします。
次の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

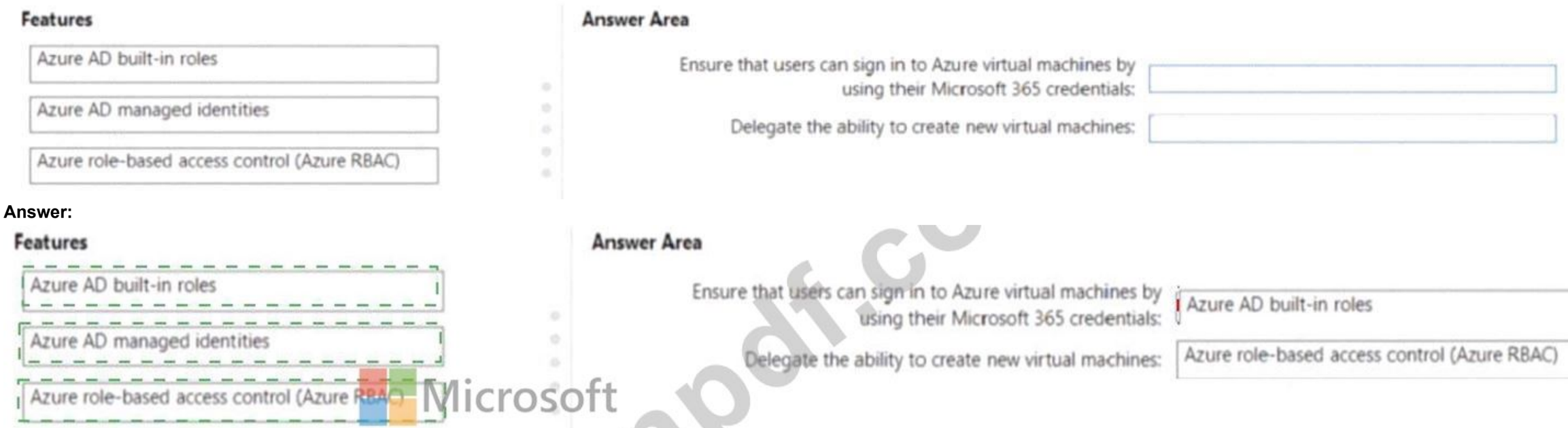
Answer:

Explanation:

最新問題**: 89**
ボストンオフィスから接続するユーザーのMFA設定を構成する必要があります。ソリューションは、認証要件とアクセス要件を満たしている必要があります。何を設定する必要がありますか？
A. プライベートIPアドレス範囲を持つ名前付きの場所
B. パブリックIPアドレス範囲を持つ名前付きの場所

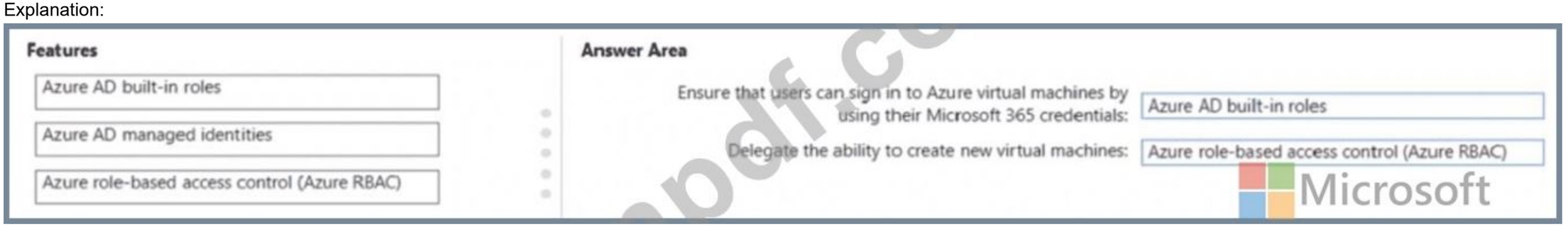
C. パブリックIPアドレス範囲を持つ信頼できるIP
D. プライベートIPアドレス範囲を持つ信頼できるIP
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
Location offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address:
This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

最新問題**: 90**
Microsoft 365 E5 サブスクリプションと Azure サブスクリプションがあります。次の要件を満たす必要があります。
* ユーザーが Microsoft 365 資格情報を使用して Azure 仮想マシンにサインインできることを確認します。
* 新しい仮想マシンを作成する機能を委任します。
各要件には何を使用する必要がありますか? 答えるには、適切な機能を正しい要件にドラッグします。各機能は、1 回以上使用することも、まったく使用しないこともできます。ペイン間の分割バーをドラッグするか、コンテンツを表示するためにスクロールする必要がある場合があります。



Answer:

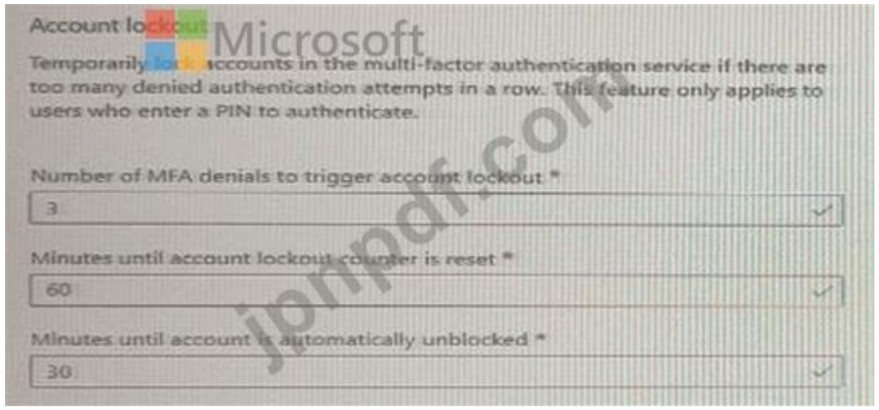
Explanation:



最新問題: **91**

多要素認証（MFA）が有効になっているAzure Active Directory（Azure AD）テナントがあります。

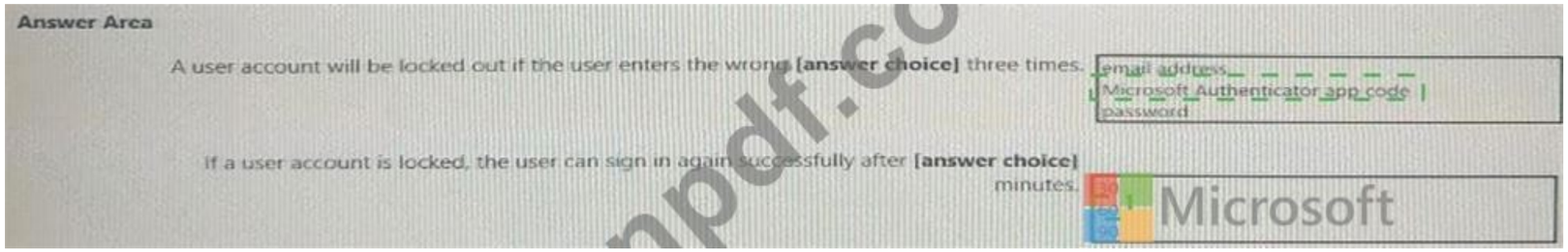
アカウントのロックアウト設定は、次の図に示すように構成されています。



ドロップダウンメニューを使用して、図に示されている情報に基づいて各ステートメントを完了する回答の選択肢を選択します。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:



Explanation:

App code

60

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#account- lockout

最新問題: **92**

App1 の計画された変更と技術要件を満たす必要があります。
何を実装する必要がありますか?
A. Microsoft Endpoint Manager で設定されたポリシー
B. Microsoft エンドポイント マネージャーのアプリ構成ポリシー
C. Azure AD でのアプリの登録
D. Azure AD アプリケーション プロキシ
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

最新問題**: 93**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。

Name	Microsoft Entra role
User1	Global Administrator
User2	Attribute Definition Administrator
User3	Security Administrator

テナントには、次の表に示す ID が含まれます。

Name	Type
Group1	Security group
Service1	Service principal
MI1	Managed identity

どのユーザーがカスタム セキュリティ属性を作成でき、どの ID に属性を割り当てることができますか? 回答するには、回答領域で適切なオプションを選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:

最新問題**: 94**

あなたの会社には、contosri.com という名前の Azure Active Directory (Azure AD) テナントがあります。同社には、次の表に示す取引先があります。

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

ユーザーは、パッケージ 1 を使用してアクセスを要求できます。

Fabrikam と Litware のユーザーは、電子メール アドレスにそれぞれのドメイン名を使用しています。

Fabrikam および Litware ユーザーのみがアクセスできる、packaqe1 という名前のアクセス パッケージを作成する予定です。

すべてのユーザーが package1 を使用してアクセスを要求できるように、Fabrikam と litware の接続された組織を構成する必要があります。

作成する必要がある接続された組織の最小数は何ですか。

A. 2

B. 1

C. 4

D. 3

Answer: D (メーッセージを残す**)**

最新問題**: 95**

Group1 と Group2 という 2 つのグループと、次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

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

サブスクリプションには、次の設定を持つ条件付きアクセス ポリシーが含まれています。

* 名前: ポリシー1
対象リソース
* 含む
* すべてのクラウドアプリ
* アクセス制御
* 付与
* 多要素認証が必要
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。
Answer Area

Answer:

Answer Area

Explanation:
Yes, No, Yes

最新問題**: 96**
App1という名前のAzureADエンタープライズアプリケーションを含むcontoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
請負業者はuser1@outlook.comのクレデンシャルを使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者は、user1 @ outlook.comとして認証できる必要があります。
あなたは何をするべきか？
A. New-AzADUserコマンドレットを実行します。
B. 外部コラボレーション設定を構成します。
C. WS-FedIDプロバイダーを追加します。
D. contoso.comでゲストユーザーアカウントを作成します。
Answer: D (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-usersportal

最新問題: **97**

Azure Active Directory Premium Plan 2 ライセンスを持つ Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	None

次の図に示すデバイス設定があります。

User1 には次の表に示すデバイスがあります。

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

次の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

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:

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: Yes
Users may join 5 devices to Azure AD.
Box 2: Yes
Box 3: No
An additional local device administrator has not been applied
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

最新問題**: 98**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
Azure AD外部IDの料金が月間アクティブユーザー（MAU）に基づいていることを確認する必要があります。
何を設定する必要がありますか？
A. アクセスレビュー
B. 用語または使用法
C. リンクされたサブスクリプション
D. ユーザーフロー

Answer: C (メーッセージを残す)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/external-identities-pricing

最新問題**: 99**
次の表に示すグループを含む Azure AD テナントがあります。

Name	Owner	Number of internal users	Number of guest users
Group1	User1	500	25
Group2	User2	295	100

次の表に示すように、Group1 のアクセス レビューを作成します。

Setting	Value
Review type	Teams + Groups
Review scope	All users
Reviewers	Users review own access

次の表に示すように、Group2 のアクセス レビューを作成します。

Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

各グループに必要な Azure AD Premium P2 ライセンスの最小数は? 回答するには、回答で適切なオプションを選択します。注: それぞれの正しい選択は 1 ポイントの価値があります。
Answer Area

Group1: 525
- 1
- 500
- 525

Group2: 1
- 1
- 100
- 295
- 395

Answer:

Explanation:

最新問題: 100

次の表に示すユーザーを含む Azure AD テナントがあります。

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

すべてのユーザーに対してセルフサービス パスワード リセット (SSPR) を有効にし、唯一の認証方法としてセキュリティの質問を要求するように SSPR を構成します。

パスワードをリセットするときに秘密の質問を使用する必要があるのはどのユーザーですか?

A. ユーザー 1 とユーザー 4 のみ

B. User1、User3、User4 のみ

C. ユーザー 3 とユーザー 4 のみ

D. ユーザー 1、ユーザー 2、ユーザー 3、とユーザー4

E. User4 のみ

Answer: (解答を表示する**)**

最新問題: 101

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

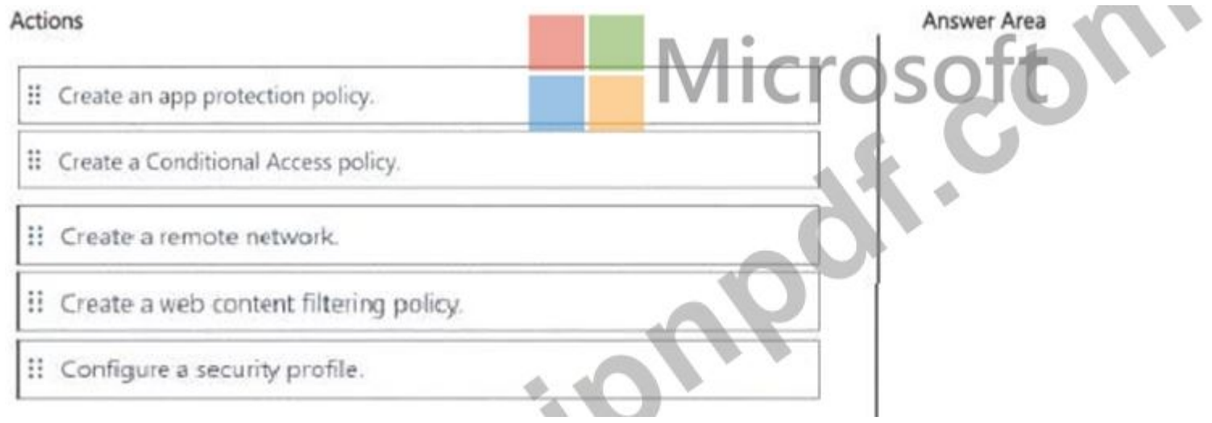
このセクションの質問に回答すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面には表示されません。

アマゾン ウェブ サービス (AWS) アカウント、Google Workspace サブスクリプション、および GitHub アカウントがある Azure サブスクリプションをデプロイし、Microsoft 365 Defender を有効にします。
Microsoft Defender for Cloud Apps を使用して OAuth 認証要求を監視できることを確認する必要があります。
解決策: Microsoft 365 Defender ポータルから、GitHub アプリ コネクタを追加します。これは目標を達成していますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**

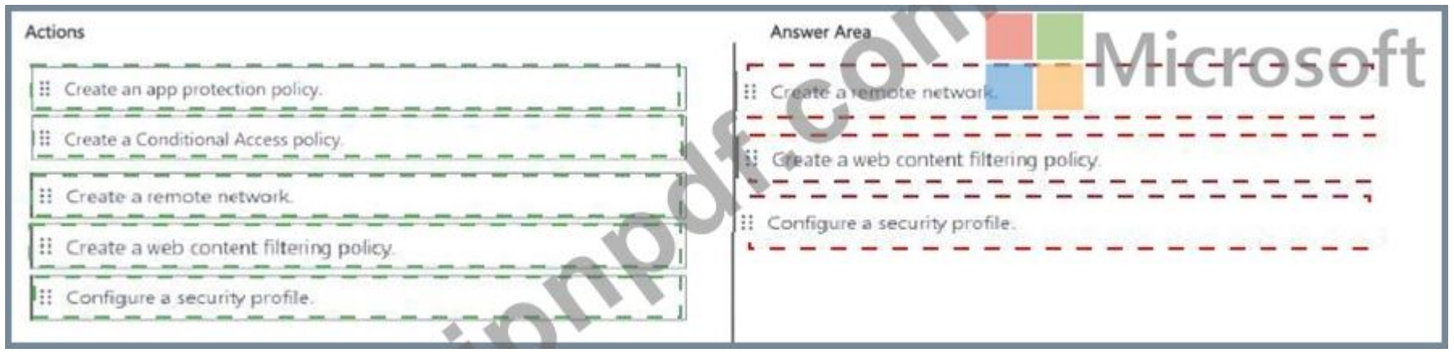
最新問題**: 102**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Azure Monitorを使用して、Azure Active Directory (Azure AD)アクティビティログを分析します。
Azure ADユーザーのサインインに失敗すると、毎日100を超える電子メールアラートが送信されます。
新しいセキュリティ管理者があなたの代わりにアラートを受信することを確認する必要があります。
解決策 :Azure ADから、診断設定を変更します。
これは目標を達成していますか？
A. いいえ
B. はい
Answer: B (メーッセージを残す**)**

最新問題**: 103**
storage1 という名前のストレージ アカウントを含む Azure サブスクリプションがあります。
複数の仮想マシンでホストされるApp1というアプリを展開する予定です。仮想マシンはシークレットを使用してサードパーティAPIに認証します。仮想マシン用の認証ソリューションを推奨する必要があります。ソリューションは以下の要件を満たす必要があります。
* 秘密を安全に保管します。
* 資格情報を App1 コードに保存する必要がないことを確認します。
* Microsoft Entra 認証を使用して、仮想マシンが Azure リソースにアクセスできることを確認します。
* 管理上の労力を最小限に抑えます。
推薦書には何を含めるべきでしょうか?
A. ユーザー アカウントと Azure Key Vault
B. システム割り当てマネージド ID とストレージ サービス暗号化
C. ユーザー割り当てマネージド ID と Azure Key Vault
D. ユーザーアカウントとストレージサービス暗号化
Answer: C (メーッセージを残す**)**

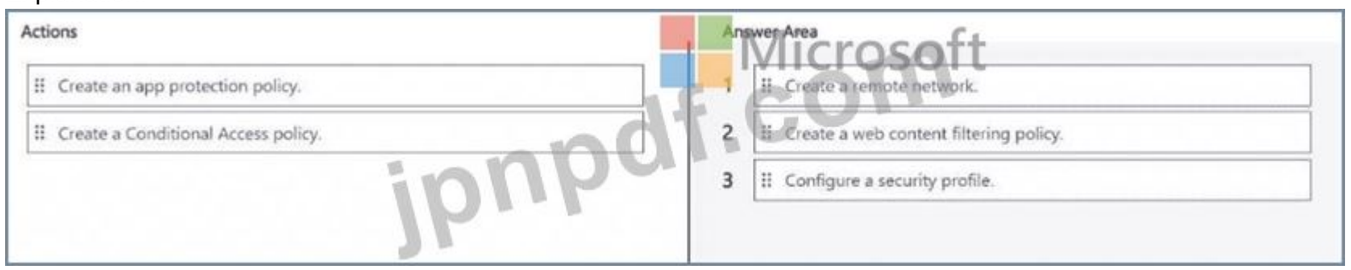
最新問題**: 104**
Microsoft 365 E5 サブスクリプションがあります。サブスクリプションには、Windows を実行するデバイスが 500 台含まれており、これらのデバイスに Global Secure Access クライアントを展開します。ユーザーがデバイスから httpsy/contoso.com にアクセスできないようにする必要があります。どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。



Answer:



Explanation:



最新問題**: 105**

注: この質問は、同じシナリオを示す一連の質問の一部です。このシリーズの各質問には、指定された目標を達成できる可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策が含まれる場合がありますが、他の質問セットには正しい解決策がない場合があります。

このセクションの質問に回答すると、その質問に戻ることはできなくなり、これらの質問はレビュー画面に表示されなくなります。

Microsoft 365 E5 サブスクリプションをお持ちです。

User1 という名前のユーザーを作成します。

User1 が ID セキュア スコア改善アクションのステータスを更新できることを確認する必要があります。

解決策: ユーザー管理者の役割を User1 に割り当てます。

これは目標を達成していますか?

A. はい

B. いいえ

Answer: B (メーッセージを残す)

最新問題: **106**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあります。
Azure ADに登録されているアプリケーションを実行するすべてのユーザーには、条件付きアクセスポリシーが適用されます。
ユーザーがレガシー認証を使用できないようにする必要があります。
従来の認証の試行を除外するために、条件付きアクセスポリシーに何を含める必要がありますか？
A. クラウドアプリまたはアクションの条件
B. ユーザーのリスク条件
C. クライアントアプリの状態
D. サインインのリスク条件
Answer: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

最新問題: **107**
Terms1 という名前の使用条件 (ToU) とアクセス パッケージを含む Contoso という名前の Azure AD テナントがあります。Contoso のユーザーは、Fabrikam という名前の外部組織と共同作業を行っています。Fabrikam ユーザーは、アクセス パッケージの使用を許可される前に、Terms1 に同意する必要があります。
どのユーザーが利用規約に同意または拒否したかを特定する必要があります1。
何を使うべきですか？
A. プロビジョニング ログ
B. 監査ログ
C. サインイン ログ
D. 使用状況と分析レポート
Answer: B (メーッセージを残す**)**

最新問題: **108**
Microsoft365テナントがあります。
すべてのユーザーは、Windows 10を実行するコンピューターを持っています。ほとんどのコンピューターは会社所有であり、Azure Active Directory（Azure AD）に参加しています。一部のコンピューターはユーザー所有であり、AzureADにのみ登録されます。
ユーザーが所有するコンピューターでMicrosoftSharePoint Onlineに接続するユーザーが、ファイルをダウンロードまたは同期できないようにする必要があります。他のユーザーを制限してはなりません。
どのポリシータイプを作成する必要がありますか？
A. Microsoft Office365ガバナンスアクションが構成されているMicrosoftCloud AppSecurityアクティビティポリシー
B. セッションコントロールが構成されているAzureAD条件付きアクセスポリシー
C. クライアントアプリの条件が構成されているAzureAD条件付きアクセスポリシー

D. ガバナンスアクションが構成されているMicrosoft Cloud AppSecurityアプリ検出ポリシー
Answer: B (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-intro-aad

最新問題**: 109**
次の表に示すユーザーを含む Azure AD テナントがあります。

Name	User risk level
User1	Low
User2	Medium
User3	High

次の表に示す Azure AD Identity Protection ポリシーがあります。

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

危険なユーザー レポートと危険なサインイン レポートを確認し、次の表に示すように各ユーザーに対してアクションを実行します。

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

次の各ステートメントについて、該当する場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。

Answer Area

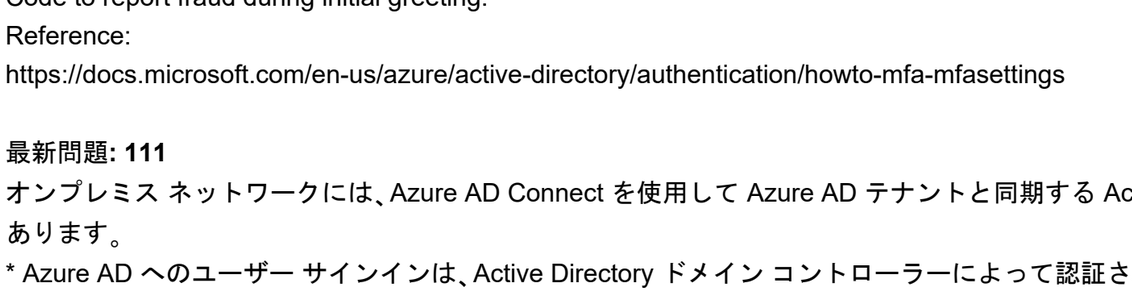
Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	○	○
User2 can sign in by using multi-factor authentication (MFA).	○	○
User3 can sign in from an anonymous IP address.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can sign in by using multi-factor authentication (MFA).	○	○
User2 can sign in by using multi-factor authentication (MFA).	○	○
User3 can sign in from an anonymous IP address.	○	○

Explanation:



最新問題: 110

Microsoft365テナントがあります。

すべてのユーザーは、Microsoft 365サービスにアクセスするときに、多要素認証（MFA）にMicrosoftAuthenticatorアプリを使用する必要があります。

一部のユーザーは、サインイン要求を開始せずにMicrosoftAuthenticatorアプリでMFAプロンプトを受信したと報告しています。

ユーザーが開始しなかったMFA要求を報告した場合、ユーザーを自動的にブロックする必要があります。

解決策：Azureポータルから、多要素認証（MFA）の不正警告設定を構成します。

これは目標を達成していますか？

A. はい

B. いいえ

Answer: (解答を表示する)

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

The following fraud alert configuration options are available:

Automatically block users who report fraud.

Code to report fraud during initial greeting.

Reference:

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

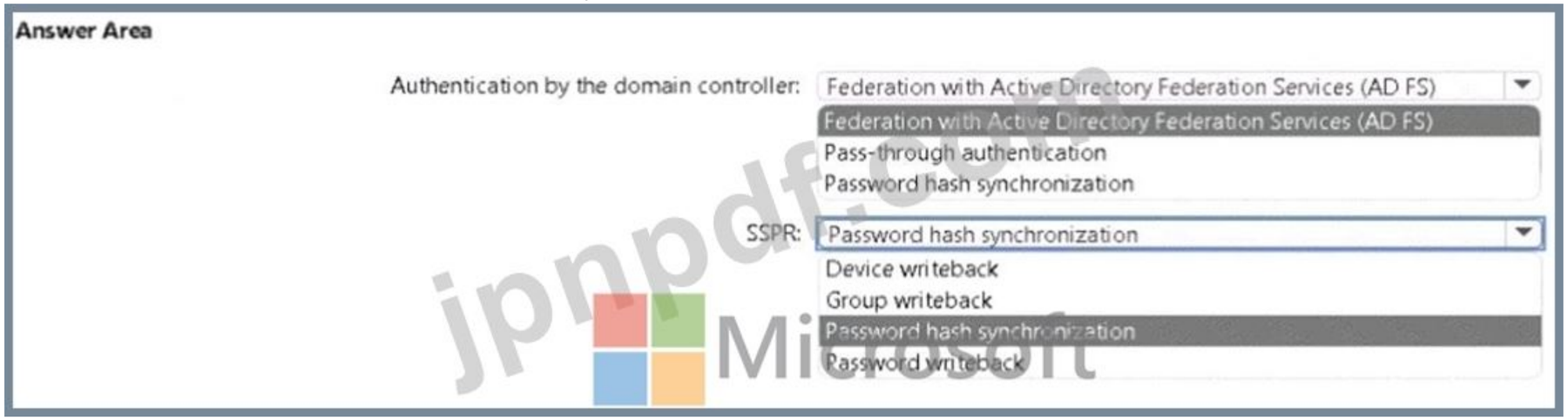
最新問題: 111

オンプレミス ネットワークには、Azure AD Connect を使用して Azure AD テナントと同期する Active Directory ドメインが含まれています。次の要件を満たすように Azure AD Connect を構成する必要があります。

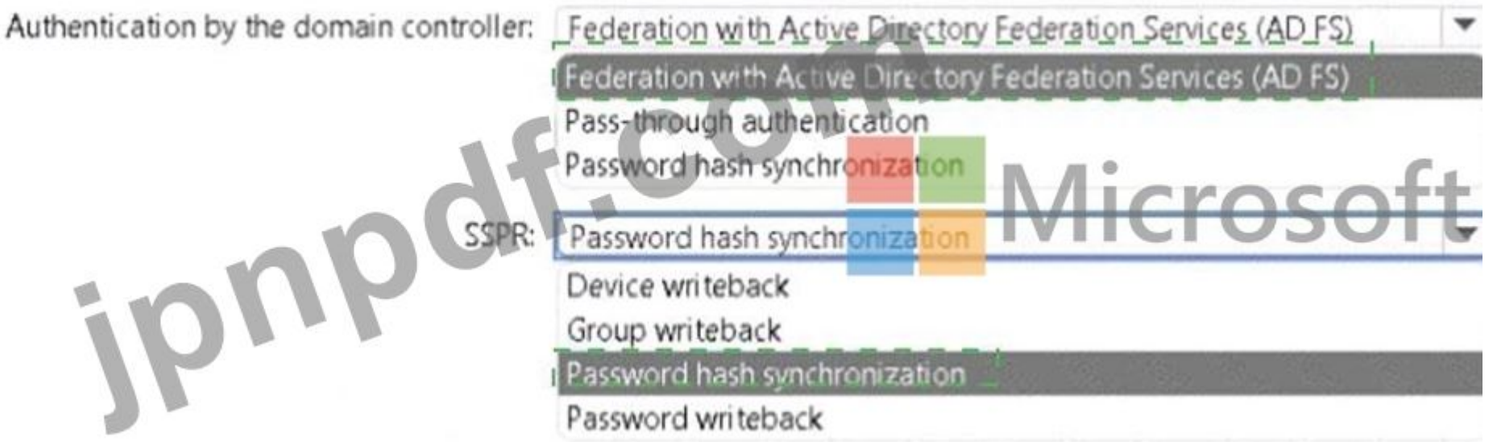
* Azure AD へのユーザー サインインは、Active Directory ドメイン コントローラーによって認証される必要があります。

* Active Directory ドメイン ユーザーは、Azure AD セルフサービス パスワード リセット (SSPR) を使用できる必要があります。

各要件には何を使用する必要がありますか? 回答するには、回答エリアで適切なオプションを選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。



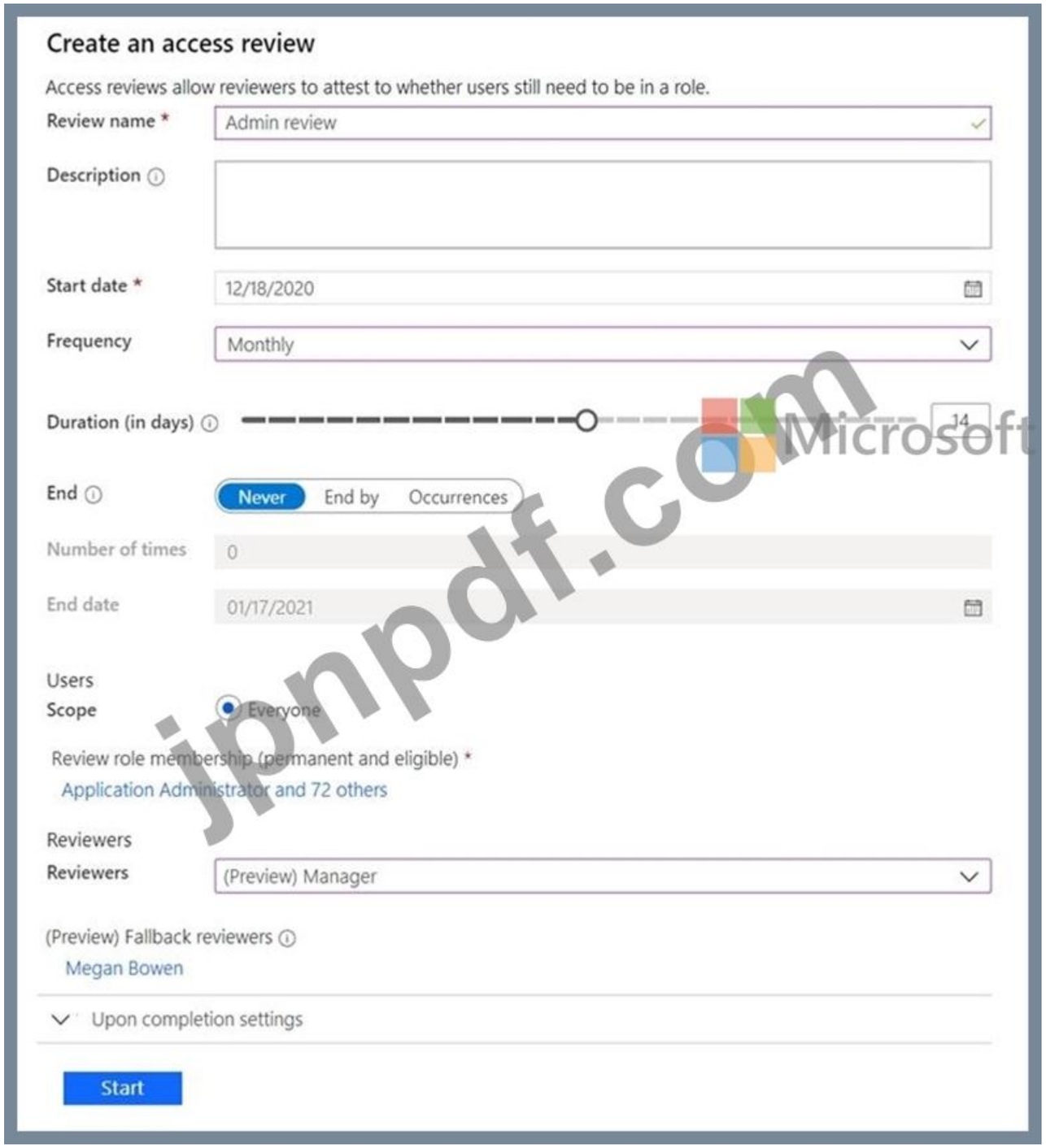
Answer:



Explanation:

最新問題: 112
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、述べられた目標を達成する可能性のある独自の解決策が含まれています。一部の質問セットには複数の正しい解決策がある場合がありますが、他の質問セットには正しい解決策がない場合があります。
このセクションの質問に回答した後は、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。

Microsoft365テナントがあります。
10の部門に編成された100人のIT管理者がいます。
展示に表示されるアクセスレビューを作成します。 [展示]タブをクリックします。）

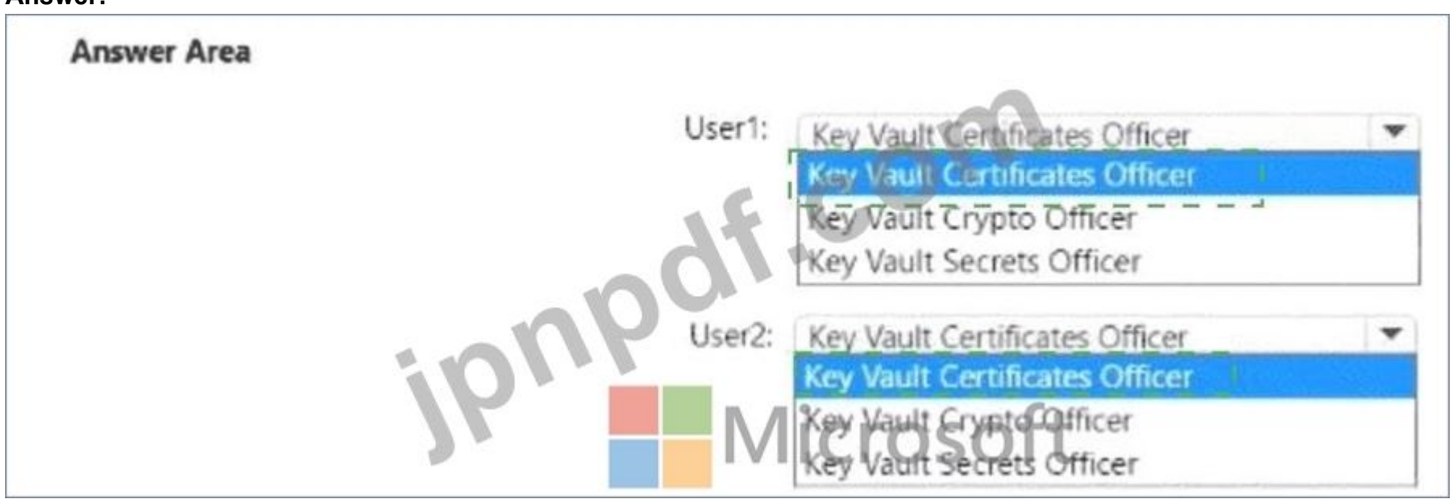


すべてのアクセスレビューリクエストがMeganBowenによって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取るようにする必要があります。

解決策 :レビュー担当者をメンバー（自己)に設定します。
これは目標を達成していますか？
A. はい
B. いいえ
Answer: B (メーッセージを残す)

最新問題**: 113**
次の表に示すリソースを含む Azure サブスクリプションがあります。
Vault1 へのアクセスを設定する必要があります。ソリューションは次の要件を満たす必要があります。
* User1 が Vault1 でキーを管理および作成できることを確認します。
* User2 が Vault1 に保存されている証明書にアクセスできることを確認します。
* 最小特権の原則を使用します。
各ユーザーにどの役割を割り当てる必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



Explanation:

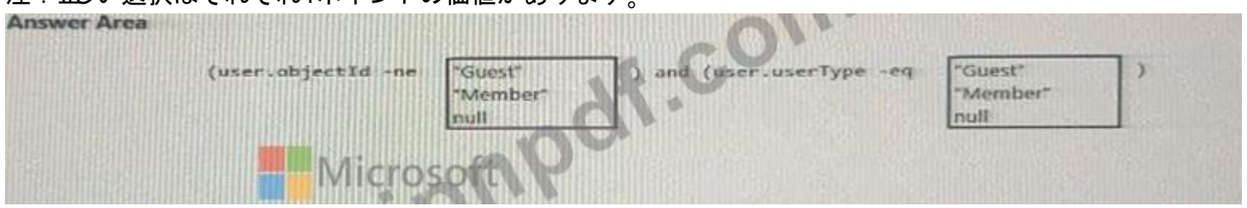
最新問題: **114**
Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションを持っています。
どのユーザーがデバイスやブラウザから Facebook にアクセスしているかを特定する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。
まず何をすべきでしょうか?
A. Microsoft エンドポイント マネージャーでアプリ構成ポリシーを作成します。
B. Microsoft Defender for Cloud Apps ポータル、未承認の Facebook から。
C. 条件付きアクセス ポリシーを作成します。
D. Defender for Cloud Apps アクセス ポリシーを作成します。
Answer: B (メーッセージを残す**)**

最新問題: **115**
Azure AD テナントがあります。
App1 という名前の新しいエンタープライズ アプリケーションをデプロイします。
ユーザーが App1 にテナントへのアクセスを提供しようとすると、失敗します。
ユーザーが App1 に対して管理者の同意を要求できることを確認する必要があります。ソリューションは最小特権の原則に従う必要があります。
まず何をすべきでしょうか?
A. App1 の権限設定から、App1 にテナントの管理者の同意を付与します。
B. テナントの管理者の同意リクエストを有効にします。
C. テナントの管理者の同意リクエストのレビュー担当者を指定します。
D. アプリケーションの条件付きアクセス ポリシーを作成します。
Answer: B (メーッセージを残す**)**

最新問題: **116**
contoso.com の SMTP アドレス スペースを使用する Microsoft Exchange 組織があります。
複数のユーザーが、1 Microsoft Entra へのセルフサービス サインアップに contoso.com の電子メール アドレスを使用しています。
自己署名ユーザーを含む Microsoft Entra テナントに対するグローバル管理者権限を取得します。
ユーザーが Microsoft 365 サービスにセルフサービスでサインアップできるように、contoso.com 2 Microsoft Entra テナントにユーザー アカウントを作成できないようにする必要があります。
どの PowerShell コマンドレットを実行する必要がありますか?
A. 更新-MgDomain
B. Update-MgPolicyAuthorizationPolicy
C. Update-MgPolicyPermissionGrantPolicyExclude
D. Update-MgDomainFederationConfiguration

Answer: C (メーッセージを残す)

最新問題: **117**
管理要件を満たすには、LWGroup1グループを作成する必要があります。
動的メンバーシップルールをどのように完了する必要がありますか？答えるには、適切な値を正しいターゲットにドラッグします。各値は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、多くの場合、ペイン間で分割バーをドラッグするか、スクロールする必要があります。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

Explanation:
Null
"Member"

最新問題: **118**
Azure AD テナントには、次の表に示すユーザーが含まれています。

Name	Role
User1	*None*
User2	Privileged Authentication Administrator
User3	Global Administrator

Azure AD Privileged Identity Management (PIM) では、次の図に示すように全体管理者ロールを構成します。

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

ユーザー 1 は全体管理者の役割を担う資格があります。

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Statements	Yes	No
User1 requires Azure Multi-Factor Authentication (MFA) to activate the Global Administrator role.	○	○
User2 can approve all activation requests for the Global Administrator role.	○	○
User1 and User3 can edit the Global Administrator role assignment.	○	○

Answer:

Explanation:

最新問題**: 119**

Microsoft Entra テナントにリンクされた Azure サブスクリプションがあります。テナントには、App1 という名前の登録済みアプリが含まれています。Microsoft Entra テナントを持つパートナー組織があります。テナントには、App2 という名前の登録済みアプリが含まれています。App1 が App2 にアクセスできることを確認する必要があります。

App1 が使用できる資格情報は 2 種類あります。それぞれの正解は完全なソリューションを示します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

A. ユーザーアカウント

B. ワンタイムパスワード

C. 秘密

D. マネージド ID

E. 証明書

Answer: C,E (メーッセージを残す**)**

最新問題**: 120**

次の表に示す ID を含む Microsoft Entra テナントがあります。

Name	Type	Member of
User1	User	Group1
Managed2	Managed identity	Group1
User3	User	Group2
User4	User	*None*

グループ1には次の構成があります。

* 所有者: ユーザー1、ユーザー4

* メンバー: User1、Managed2、Gioup2

次の設定を持つアクセス レビューを作成します。

* 名前: レビュー1

* レビュー範囲: チーム + グループを選択

* グループ: グループ1
* 対象: すべてのユーザー
* レビュー担当者を選択: グループ所有者

フォールバックレビュー担当者: 設定が構成されていません。

Answer:

Explanation:

最新問題**: 121**

contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

Fabrikam, Inc. という名前の会社のユーザーにリソース アクセスを提供する資格管理を実装します。Fabrikam は、fabrikam.com という名前のドメインを使用します。

アクセスが必要なくなった場合、Fabrikam ユーザーはテナントから自動的に削除される必要があります。

次の設定を行う必要があります。

外部ユーザーによるこのディレクトリへのサインインをブロックする: いいえ

外部ユーザーの削除: はい

このディレクトリから外部ユーザーを削除するまでの日数: 90

Identity Governance ブレードで何を構成する必要がありますか?

A. パッケージにアクセスする
B. 権利管理設定
C. 利用規約

D. レビュー設定にアクセスします
Answer: B (メーッセージを残す)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

最新問題: **122**
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

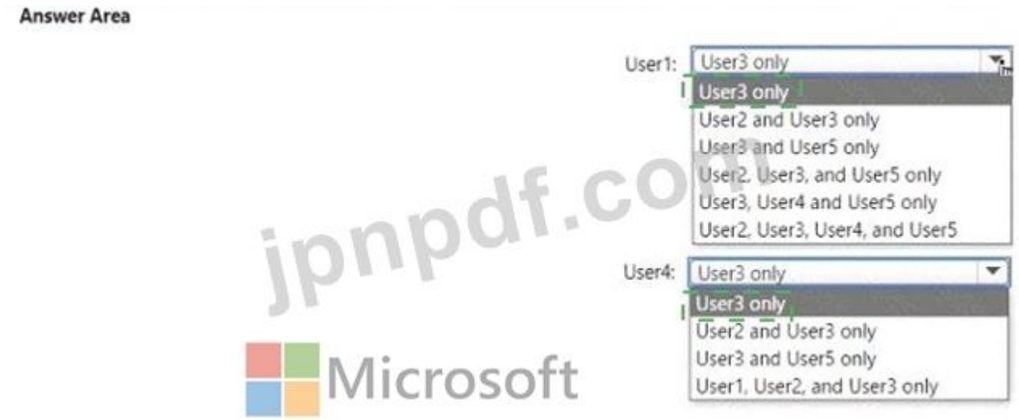
Name	Member of administrative unit
User1	AU1
User2	AU1
User3	AU1
User4	AU2
User5	Not a member of an administrative unit

ユーザーには、次の表に示す役割が割り当てられます。

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

User1 と User4 がパスワードをリセットできるのはどのユーザーですか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:



Explanation:

最新問題**: 123**

contoso.com と fabrikam.com という 2 つの Microsoft Entra テナントがあります。Contoso.com には、次の表に示す ID が含まれています。

Name	Type
User1	User
Group1	Security group
Group2	Microsoft 365 group

contoso.com から fabrikam.com へのテナント間同期を構成します。どの ID が fabrikam.com と同期されますか?

A. ユーザー1のみ

B. ユーザー1とグループ1のみ

C. ユーザー1、グループ1、グループ2

D. ユーザー1とGtoup2のみ

Answer: (解答を表示する**)**

最新問題**: 124**

User1、User2、User3 という 3 人のユーザーが含まれる Microsoft 365 E5 サブスクリプションがあります。

次の表に示すアクティブ化設定を持つ 2 つの Azure AD ロールがあります。

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

Azure AD ロールには、次の表に示す割り当て設定があります。

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

Azure AD ロールには、次の表に示す対象となるユーザーがいます。

Role	Eligible assignment
Role1	User1, User2
Role2	User3

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

Explanation:

最新問題**: 125**

Microsoft 365 E5 サブスクリプションをお持ちです。

ユーザー プロファイルに部門が定義されていないすべてのユーザーを含む動的ユーザー グループを作成する必要があります。

メンバーシップ ルールをどのように完了すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。

注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

Explanation:

最新問題: **126**

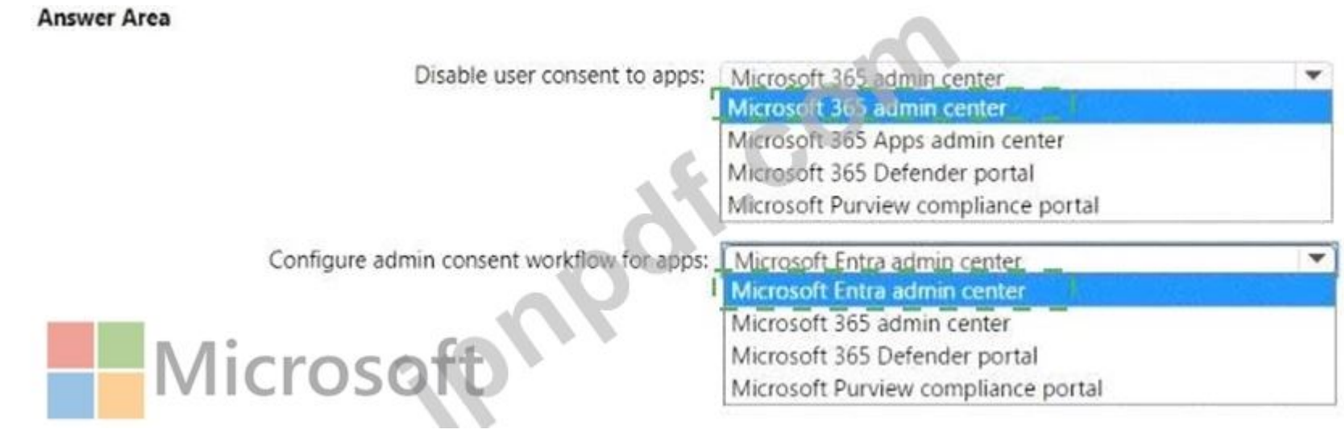
Microsoft 365 E5 サブスクリプションをお持ちです。

サブスクリプションに対するアプリの同意を構成する必要があります。ソリューションは次の要件を満たす必要があります。

* アプリに対するユーザーの同意を無効にします。
* アプリの管理者の同意ワークフローを構成します。

各要件に対してどのポータルを使用する必要がありますか? 回答するには、回答内の適切な選択肢を選択してください。注意 正しい選択はそれぞれ 1 ポイントの価値があります

Answer:



Explanation:

最新問題**: 127**

Azure Active Directory (Azure AD)テナントがあります。

テナント向け。ユーザーはアプリケーションを登録できます。いいえに設定されています。

Admin1という名前のユーザーは、App1という名前の新しいクラウドアプリをデプロイする必要があります。

Admin1がApp1をAzureADに登録できることを確認する必要があります。ソリューションは、最小特権の原則を使用する必要があります。

Admin1にどの役割を割り当てる必要がありますか？

A. AzureADのアプリケーション開発者

B. Subscription1のアプリ構成データ所有者

C. Subscription1のマネージドアプリケーションコントリビューター

D. AzureADのクラウドアプリケーション管理者

Answer: A (メーッセージを残す**)**

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

最新問題**: 128**

オンプレミス ネットワークには、Microsoft Entra Connect を使用して Microsoft Entra テナントと同期する Active Directory ドメインが含まれています。

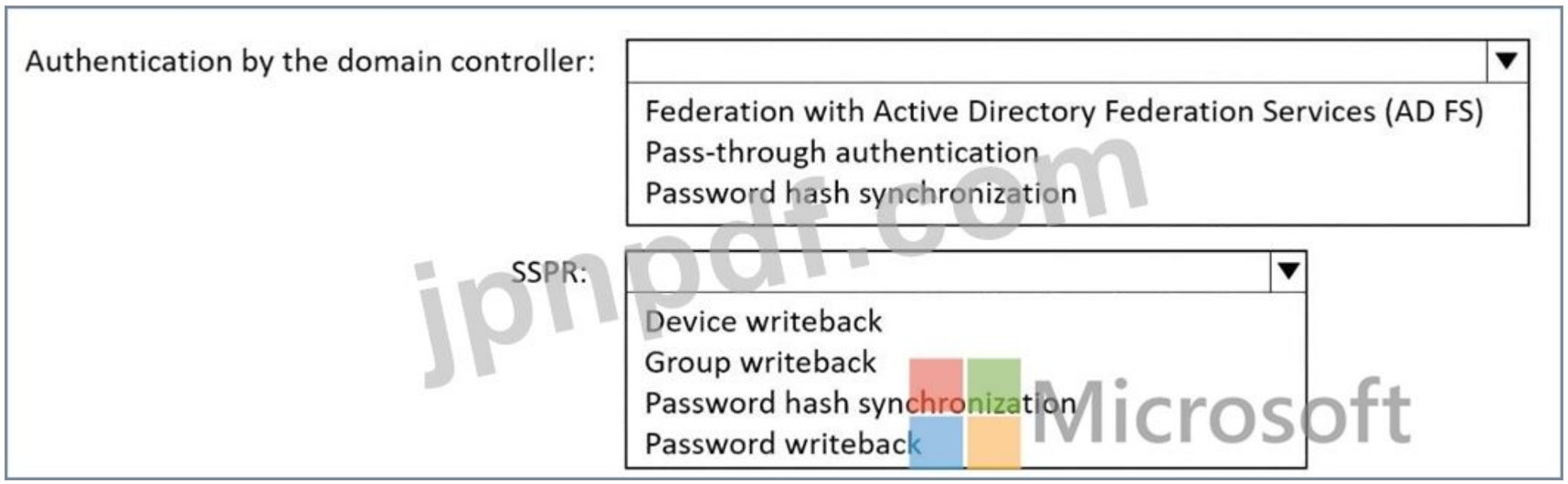
次の要件を満たすように Microsoft Entra Connect を構成する必要があります。

* Microsoft Entra サインインは、Active Directory ドメイン コントローラーによって認証される必要があります。

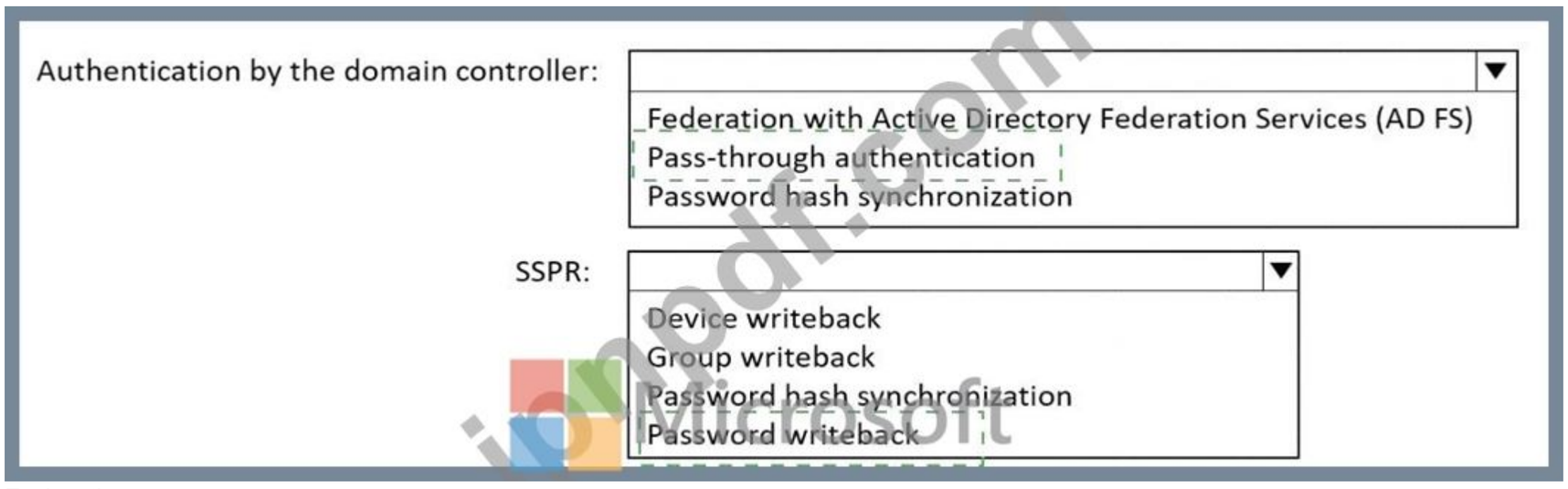
* Active Directory ドメイン ユーザーは、Microsoft Entra セルフサービス パスワード リセット (SSPR) を使用できる必要があります。

* 管理上の労力を最小限に抑えます。

各要件には何を使用すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。



Answer:



Explanation:

Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller: Pass-through authentication Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR):

Password writeback

Let's break this down step by step based on Microsoft Entra Connect, authentication methods, and SSPR requirements, as outlined in Microsoft Identity and Access Administrator documentation.

Requirement 1: Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller Understanding the Requirement:

The requirement states that Microsoft Entra sign-ins must be authenticated by an on-premises Active Directory domain controller. This means that the authentication process must occur on-premises rather than in the cloud.

Microsoft Entra Connect supports several authentication methods for hybrid identity:

Password Hash Synchronization (PHS):Password hashes are synchronized to Microsoft Entra ID, and authentication occurs in the cloud. This does not meet the requirement because the domain controller is not involved in the authentication process.

Pass-through Authentication (PTA):Users sign in to Microsoft Entra ID, but the authentication request is passed to an on-premises Active Directory domain controller for validation. This meets the requirement because the domain controller performs the authentication.

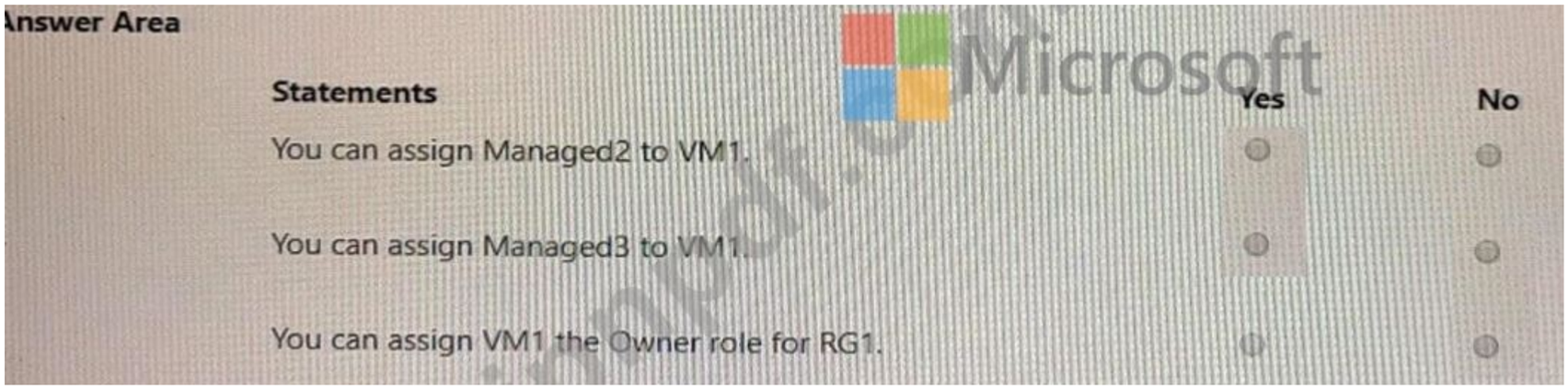
Federation with Active Directory Federation Services (AD FS):Users are redirected to an on-premises AD FS server, which authenticates them against the domain controller. This also meets the requirement because the domain controller is involved via AD FS.
Comparing the Options:
Federation with Active Directory Federation Services (AD FS):
AD FS provides federated authentication, where users are redirected to an on-premises AD FS server for authentication. The AD FS server communicates with the domain controller to validate credentials. This meets the requirement because the domain controller authenticates the user.
However, AD FS requires significant infrastructure (e.g., AD FS servers, Web Application Proxy servers) and ongoing maintenance, which increases administrative effort.
Pass-through Authentication (PTA):
PTA allows Microsoft Entra ID to pass the authentication request directly to an on-premises domain controller via a lightweight agent installed on a server in the on-premises environment.
This meets the requirement because the domain controller performs the authentication.
PTA is simpler to deploy and manage than AD FS. It requires only the Microsoft Entra Connect server and the PTA agent, with no additional infrastructure like AD FS servers. This aligns with the requirement to
"minimize administrative effort."
Minimizing Administrative Effort:
The question emphasizes minimizing administrative effort.
AD FS requires deploying and maintaining a federation infrastructure, including AD FS servers, Web Application Proxy servers, certificates, and load balancers. This involves significant administrative overhead.
PTA, on the other hand, is lightweight. It uses the existing Microsoft Entra Connect server and a small agent, with no additional infrastructure required. It also supports high availability by allowing multiple PTA agents.
Therefore, PTA is the better choice to minimize administrative effort while meeting the requirement.
Conclusion for Requirement 1:
Both options meet the requirement for domain controller authentication, but PTA is the better choice because it minimizes administrative effort.
The correct answer for this requirement isPass-through authentication.
Requirement 2: Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR) Understanding the Requirement:
The requirement states that Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR).
SSPR allows users to reset their passwords via a web portal (e.g., aka.ms/sspr) without contacting an administrator. In a hybrid environment (with Microsoft Entra Connect), SSPR must be configured to work with on-premises Active Directory accounts.
For SSPR to work in a hybrid environment, the password reset must be written back to the on-premises Active Directory so that the user's password is updated in both Microsoft Entra ID and Active Directory.
Understanding the Options:
Device writeback:
Device writeback synchronizes device objects (e.g., for Conditional Access or Windows Hello for Business) between Microsoft Entra ID and Active Directory.
This is unrelated to SSPR or password management.
Group writeback:
Group writeback synchronizes Microsoft 365 groups from Microsoft Entra ID to Active Directory, allowing on-premises applications to use these groups.
This is also unrelated to SSPR or password management.
Password hash synchronization:
Password hash synchronization (PHS) synchronizes the hash of a user's Active Directory password to Microsoft Entra ID, enabling cloud authentication.
While PHS is often used in hybrid environments, it only synchronizes passwords from Active Directory to Microsoft Entra ID (one-way). It does not support writing password changes (e.g., from SSPR) back to Active Directory, which is required for SSPR in a hybrid environment.
Password writeback:

Password writeback is a feature of Microsoft Entra Connect that allows password changes made in Microsoft Entra ID (e.g., via SSPR) to be written back to the on-premises Active Directory.
This is specifically designed for SSPR in hybrid environments. When a user resets their password using SSPR, the new password is written back to Active Directory, ensuring the user's credentials are consistent across both environments.
Password writeback requires Microsoft Entra ID P1 or P2 licenses and must be enabled in Microsoft Entra Connect.
SSPR in a Hybrid Environment:
For SSPR to work for Active Directory domain users, password writeback must be enabled. Without password writeback, a password reset in Microsoft Entra ID would not update the on-premises Active Directory, rendering the user unable to sign in to on-premises resources.
Password writeback ensures that when a user resets their password via SSPR, the new password is synchronized to Active Directory, meeting the requirement.
Conclusion for Requirement 2:
The only option that enables SSPR for Active Directory domain users in a hybrid environment isPassword writeback.
The other options (Device writeback, Group writeback, Password hash synchronization) do not support writing password changes back to Active Directory, which is necessary for SSPR.
Final Answer Summary:
Microsoft Entra sign-ins must be authenticated by an Active Directory domain controller:Pass-through authentication (meets the requirement and minimizes administrative effort compared to AD FS).
Active Directory domain users must be able to use Microsoft Entra self-service password reset (SSPR):
Password writeback (required for SSPR in a hybrid environment).
References:
Microsoft Entra Connect documentation: "Choose the right authentication method" (Microsoft Learn:
https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn) Microsoft Entra Connect documentation: "Password writeback for SSPR" (Microsoft Learn:https://learn.
microsoft.com/en-us/entra/identity/authentication/howto-sspr-writeback) Microsoft Identity and Access Administrator (SC-300) exam study guide, which covers Microsoft Entra Connect authentication methods and SSPR configuration in hybrid environments.

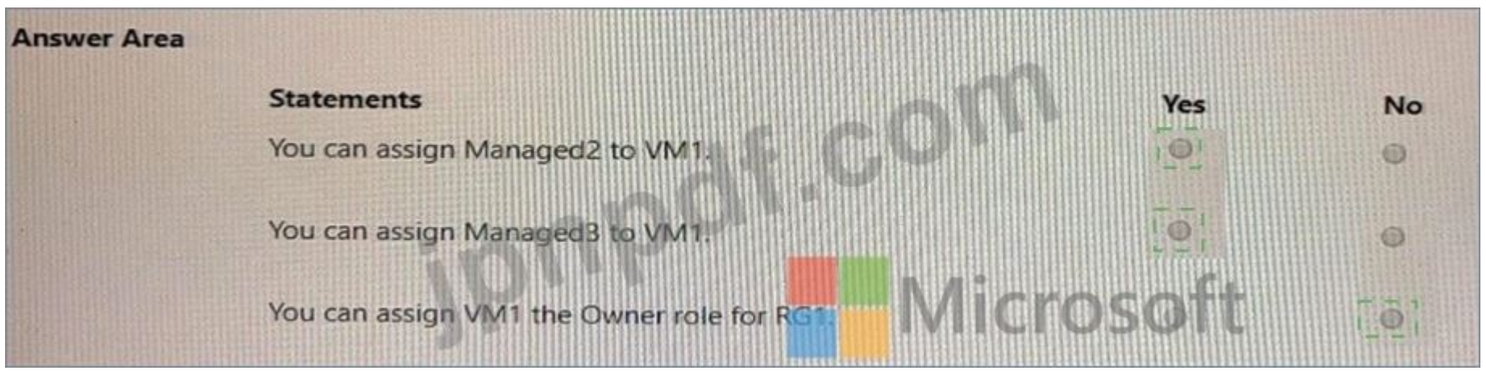
最新問題**: 129**
次の仮想マシン名を含む Azure サブスクリプションがあります: VM1 Azure リージョン: 米国東部 システム割り当てマネージド ID: 無効 次の表に示すマネージド ID を作成します。

Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

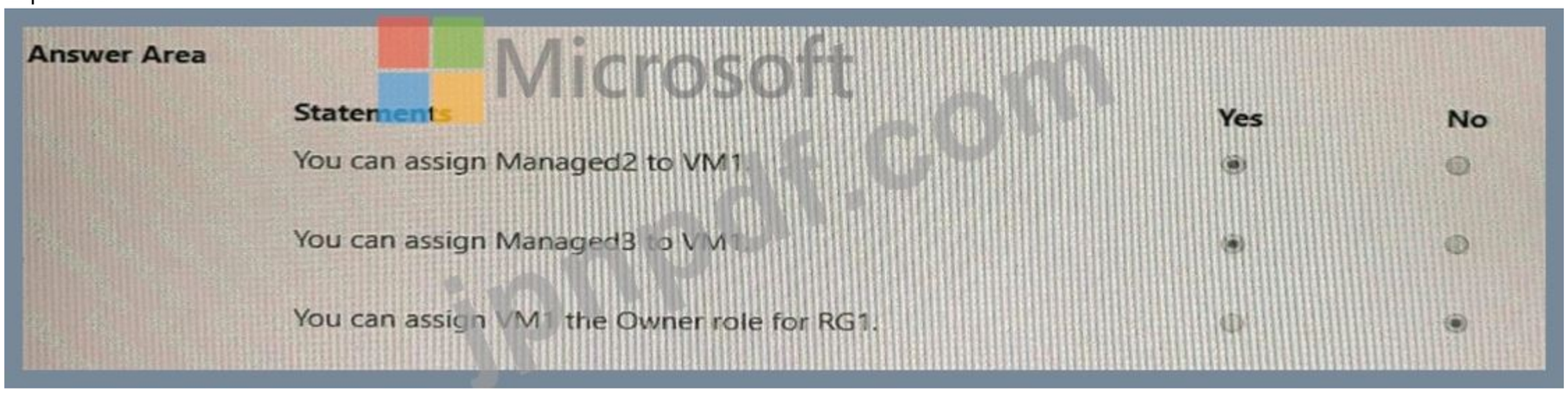
次のアクションを実行します。
* Managed1 を VM1 に割り当てます。
* 米国西部リージョンに RG1 という名前のリソース グループを作成します。
次の各ステートメントについて、該当する場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。



Answer:

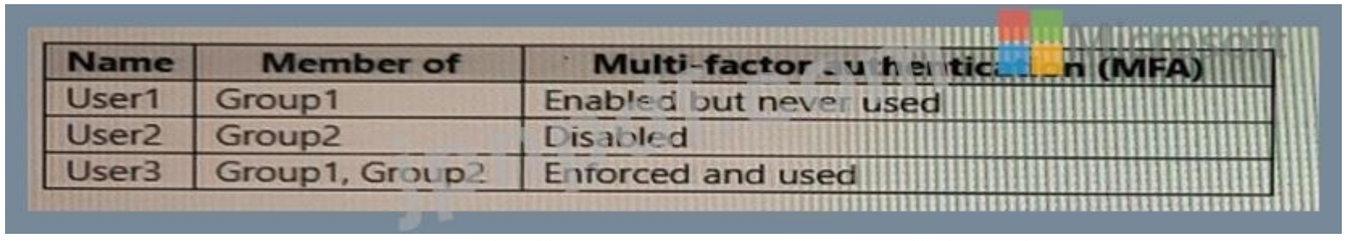


Explanation:



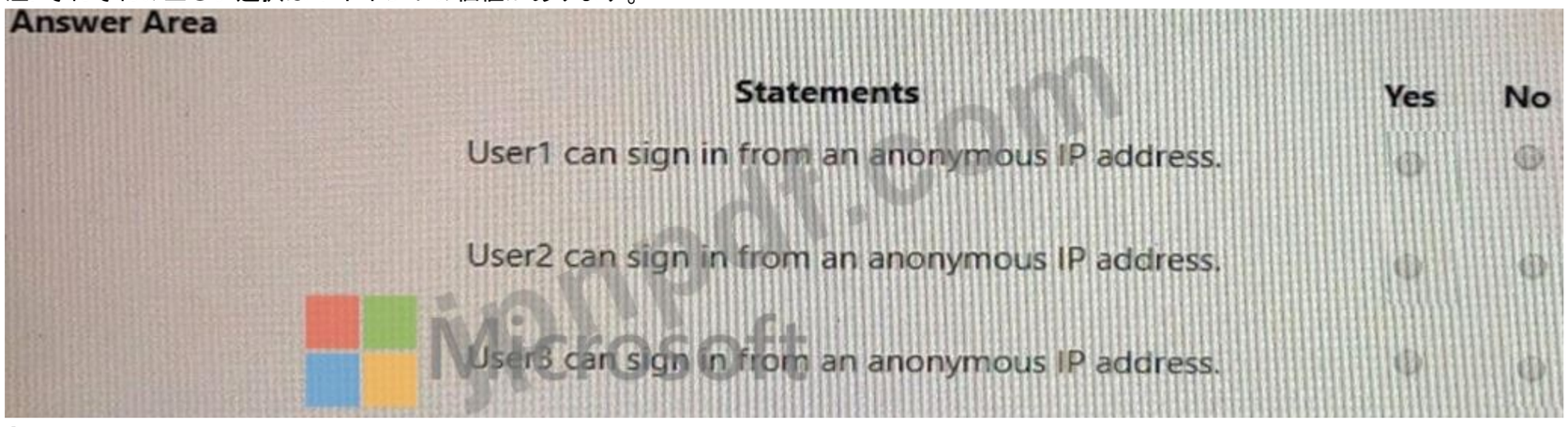
最新問題**: 130**

次の表に示すユーザーを含む Azure AD テナントがあります。

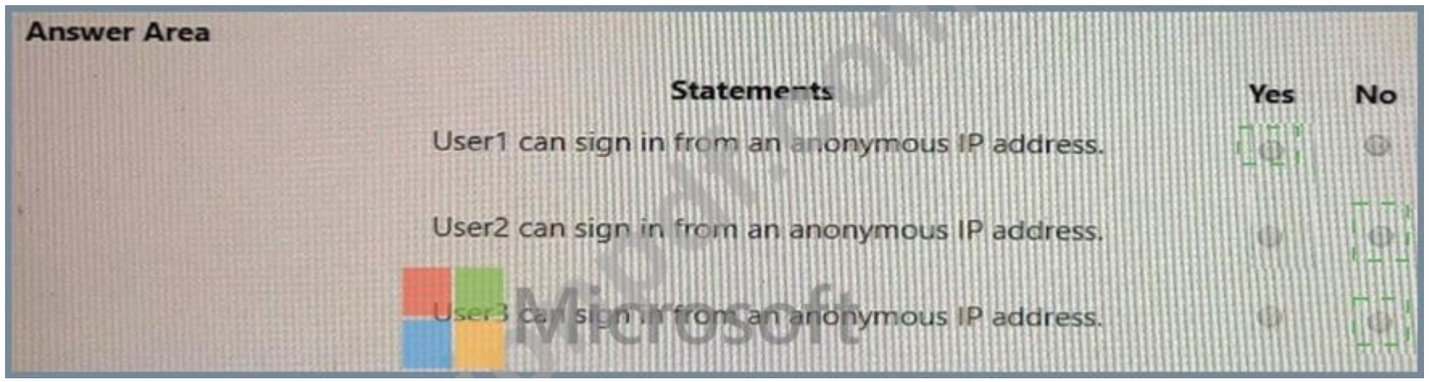


Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

Azure AD Identity Protection では、次の設定を持つユーザー リスク ポリシーを構成します。
* 割り当て:
o ユーザー: グループ 1
o ユーザーリスク: 低以上
* コントロール:
o アクセス: アクセスをブロック
* ポリシーの適用: オン
Azure AD Identity Protection では、次の設定を持つサインイン リスク ポリシーを構成します。
* 割り当て:
o ユーザー: グループ 2
o サインインのリスク: 低以上
* コントロール:
o アクセス: 多要素認証を要求する
* ポリシーを適用します。の上
次の設定:
設定の:
次の各ステートメントについて、該当する場合は [はい] を選択します。それ以外の場合は、[いいえ] を選択します。
注: それぞれの正しい選択は 1 ポイントの価値があります。



Answer:



Explanation:

最新問題: 131

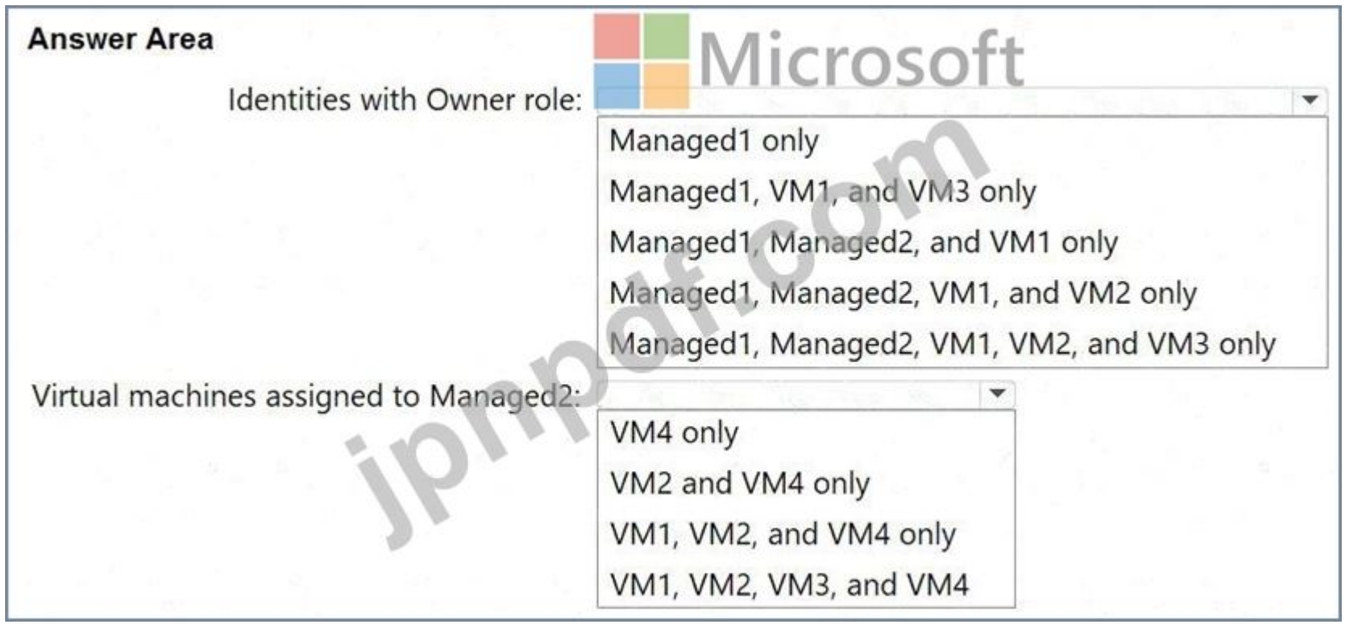
次の表に示すリソースを含む Azure サブスクリプションがあります。

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

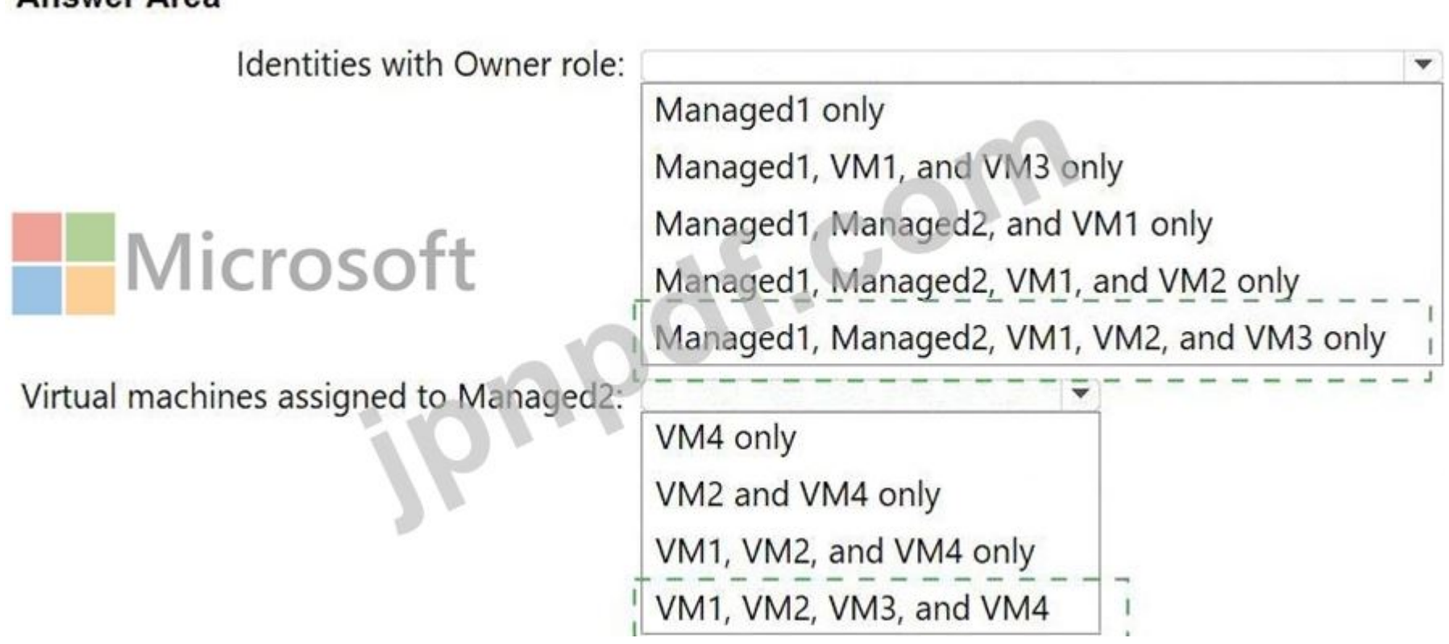
サブスクリプションには、次の表に示す仮想マシンが含まれています。

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

どの ID に RG1 の所有者ロールを割り当てることができますか?また、どの仮想マシンにマネージド 2 を割り当てることができますか? 回答するには、回答エリアで適切な選択肢を選択してください。注: 正しい選択肢はそれぞれ 1 ポイントの価値があります。



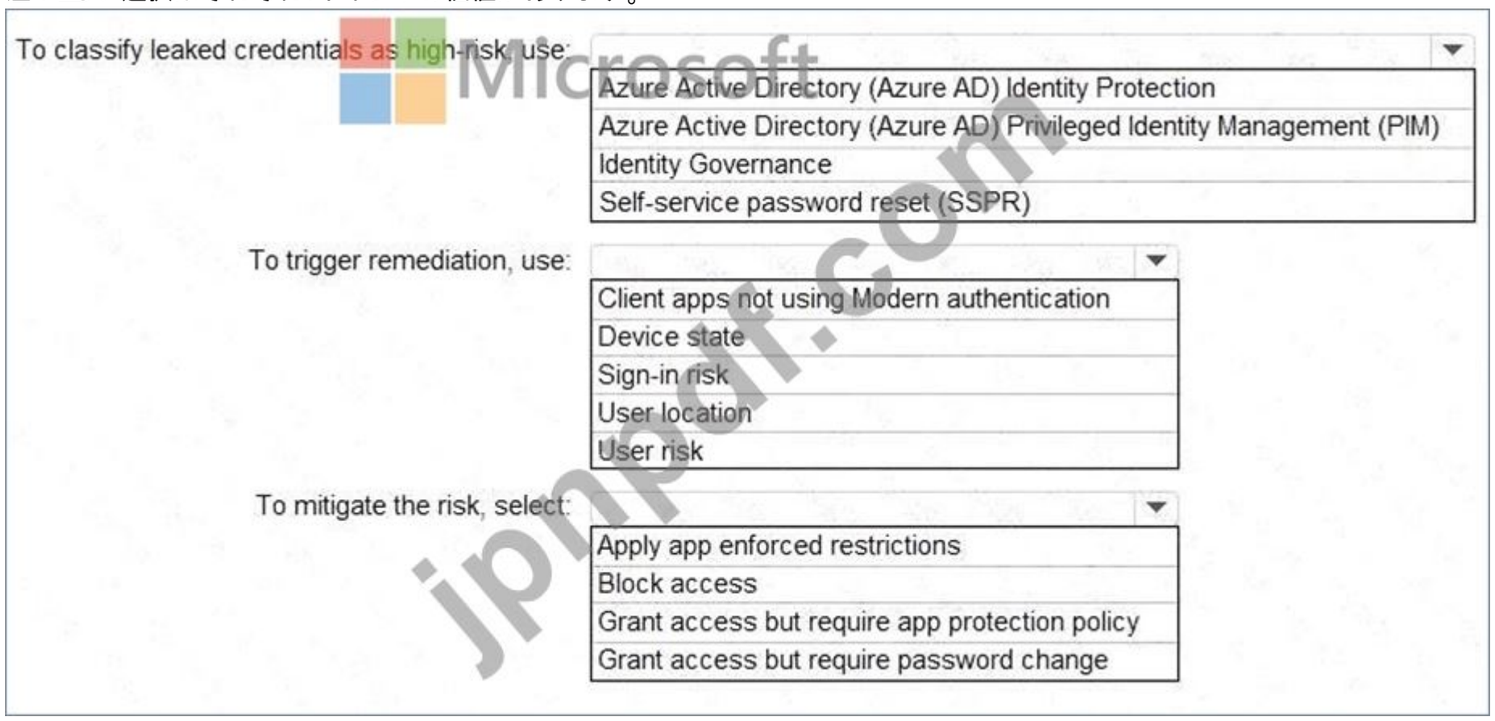
Answer:



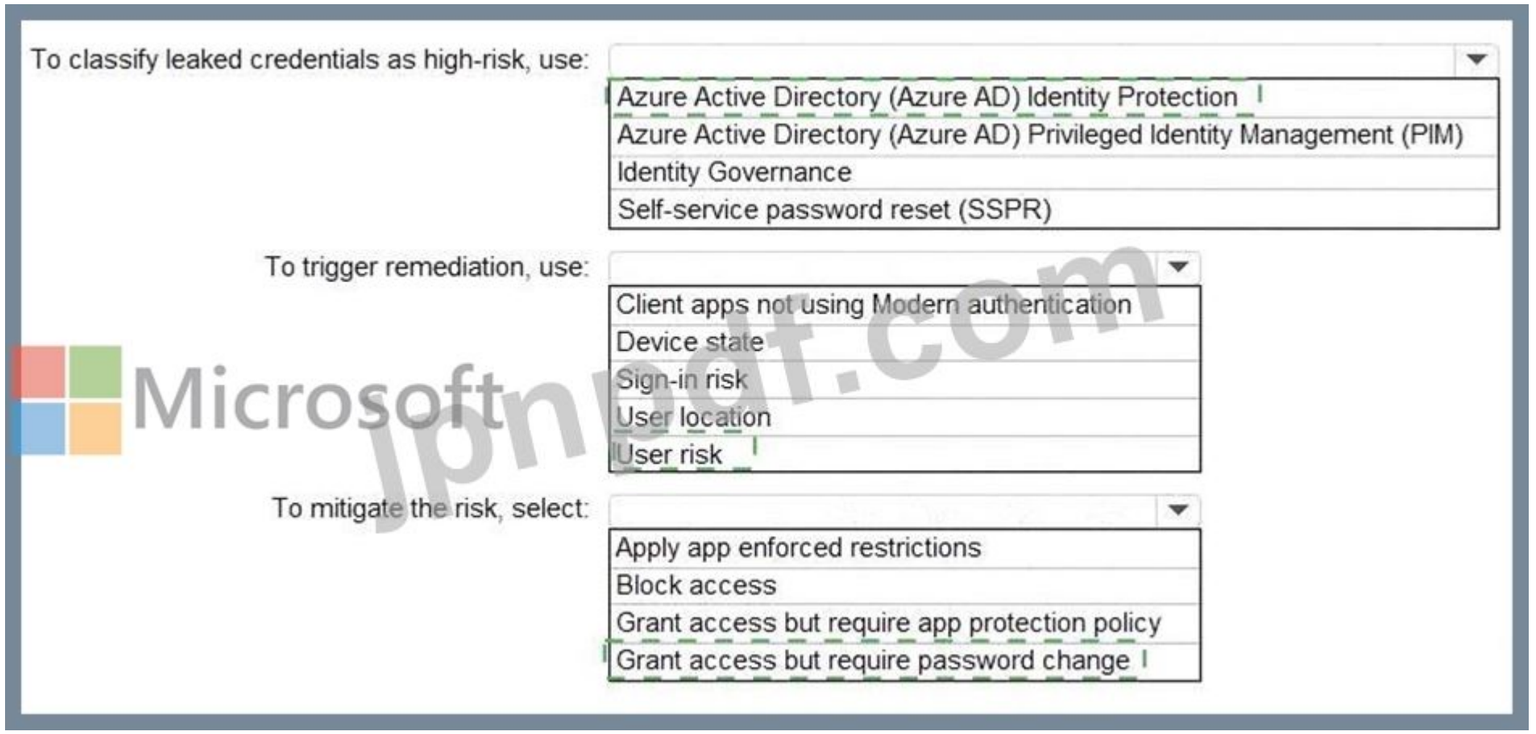
Explanation:
Box1:Managed1, Managed2, VM1, and VM2 VM3
Box2: VM1, VM2, VM3, VM4 This article confirms that managed identities can be used across geos:
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

最新問題: 132
Microsoft365テナントがあります。

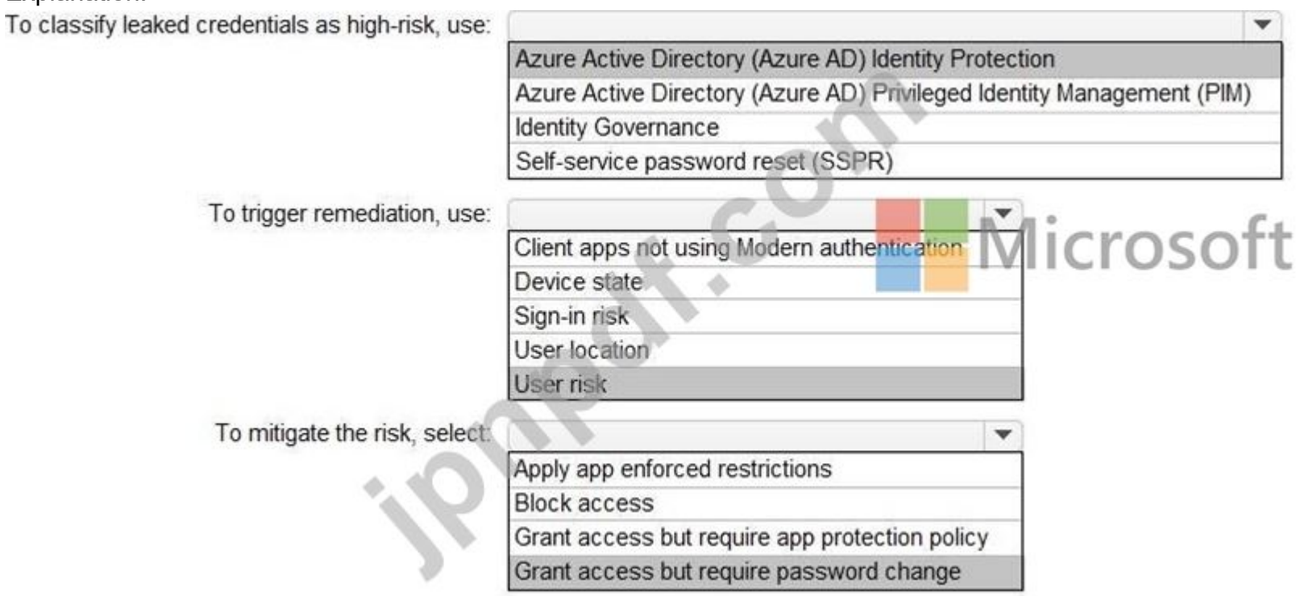
資格情報を漏えいしたユーザーを特定する必要があります。ソリューションは、次の要件を満たしている必要があります。
*クレデンシャルが漏洩した疑いで食事をしたユーザーによるIDサインイン。
*リスクの高いイベントとしてサインインをラグします。
*ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。
何を使うべきですか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:



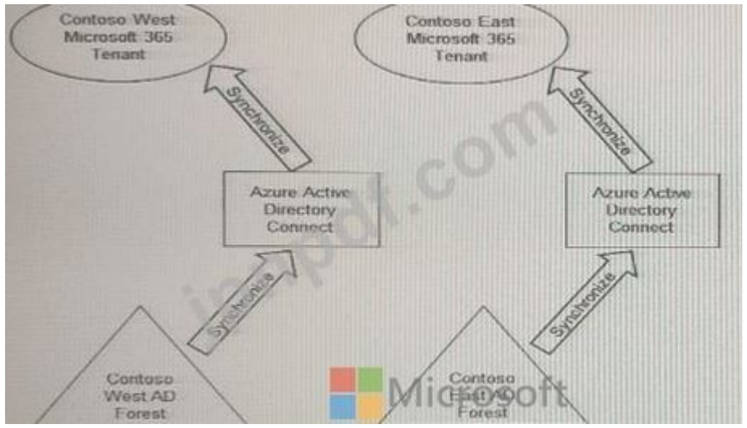
Explanation:



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

最新問題: 133

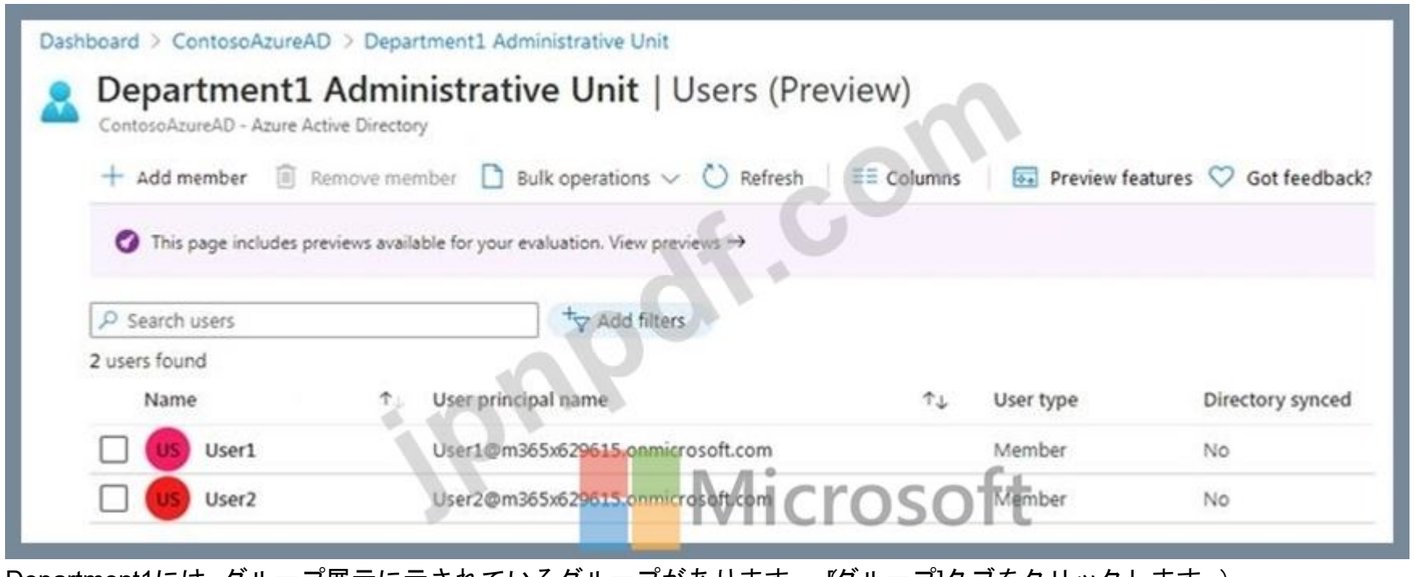
あなたの会社には、Contoso East と Contoso West という名前の 2 つの部門があります。両方の部門の Microsoft 365 ID アーキテクチャを次の図に示します。



Contoso East 部門のユーザーに、Contoso West テナントの Microsoft SharePoint Online サイトへのアクセスを割り当てる必要があります。このソリューションには追加の Microsoft 3G5 ライセンスが必要であってはなりません。
あなたは何をするべきか？

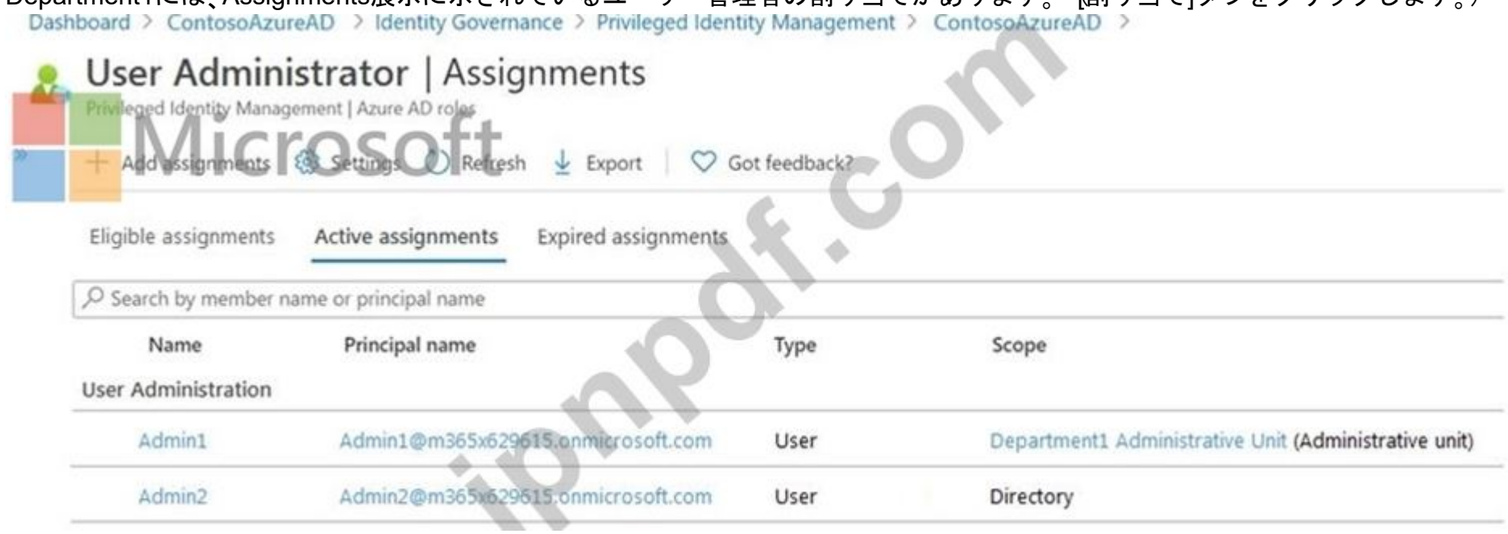
A. Contoso East Active Directory フォレストを Contoso West テナントに同期するように、Contoso Cast の既存の Azure AD Connect サーバーを構成します。
B. Contoso West テナントで Azure AD アプリケーション プロキシを構成します。
C. Contoso East ユーザーを Contoso West テナントのゲストとして招待します。
D. 2 番目の Azure AD Connect サーバーを Contoso East にデプロイし、Contoso East Active Directory フォレストを Contoso West テナントに同期するようにサーバーを構成します。
Answer: A (メーッセージを残す)

最新問題: **134**
Department1という名前の管理ユニットを含むAzureActive Directory (Azure AD)テナントがあります。
Department1には、ユーザー展示に表示されているユーザーがいます。 [ユーザー]タブをクリックします。)

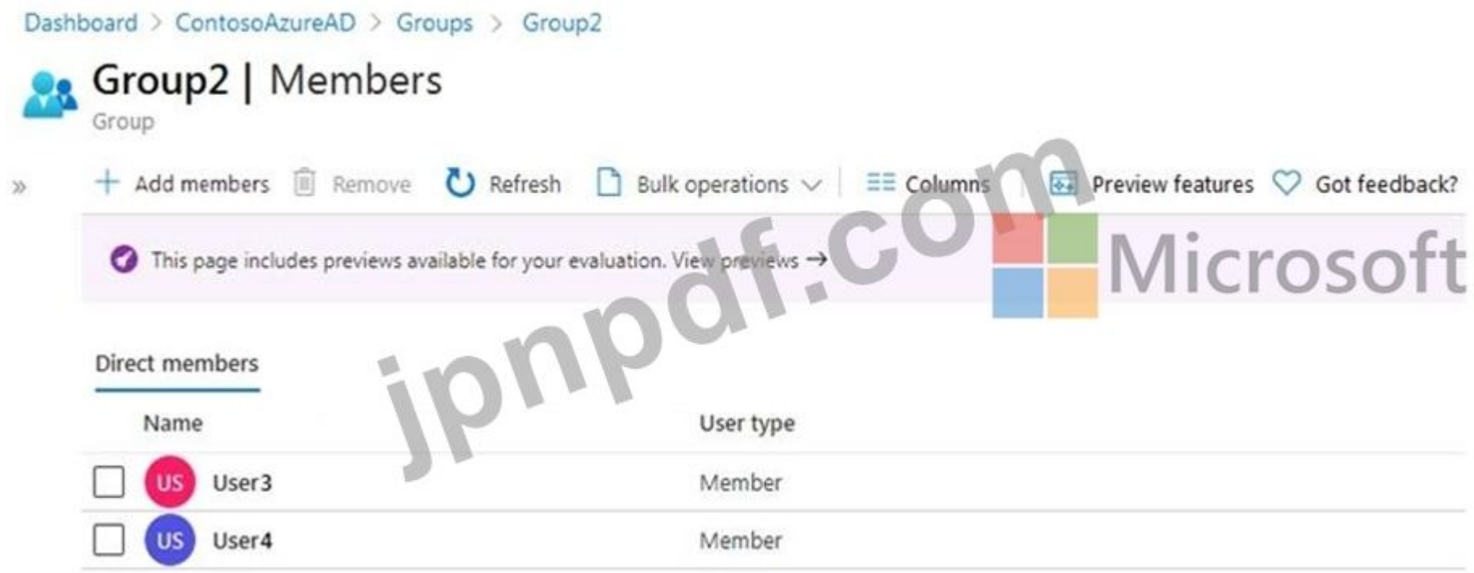


Department1には、グループ展示に示されているグループがあります。 [グループ]タブをクリックします。)

Department1には、Assignments展示に示されているユーザー管理者の割り当てがあります。 [割り当て]タブをクリックします。）



Group2のメンバーはGroup2の展示に展示されています。 [グループ2]タブをクリックします。）



次の各ステートメントについて、ステートメントがtrueの場合は、[はい]を選択します。それ以外の場合は、[いいえ]を選択します。
注：正しい選択はそれぞれ1ポイントの価値があります。

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

Answer:

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

Explanation:

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

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

最新問題**: 135**
次の表に示すユーザーを含む Azure Ad テナントがあります。

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

動的ユーザー グループを作成し、次のルール構文を構成します。

```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

どのユーザーがグループに追加されますか?
A. User1 と User3 のみ

B. User2のみ
C. User3 のみ
D. User1 のみ
E. ユーザー 1、ユーザー 2、およびユーザー 3
F. ユーザー 1 とユーザー 2 のみ
Answer: F (メーッセージを残す**)**

最新問題**: 136**
Site1 という名前の Microsoft SharePoint Online サイトと Group1 という名前の Microsoft 365 グループを含む Microsoft 365 サブスクリプションがあります。Group1 のメンバーが Site1 に 90 日間アクセスできることを確認する必要があります。ソリューションでは、管理労力を最小限に抑える必要があります。何を使えばいいのでしょうか？
A. アクセスレビュー
B. ライフサイクル ワークフロー
C. 条件付きアクセス ポリシー
D. アクセスパッケージ
Answer: D (メーッセージを残す**)**

最新問題**: 137**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。
このセクションで質問に答えた後は、そのセクションに戻ることはできません。そのため、これらの質問はレビュー画面に表示されません。
Microsoft Entra テナントに同期する Active Directory フォレストがあります。
Active Directory でユーザー アカウントが無効になっている場合でも、無効になっているユーザーは最大 30 分間 Microsoft Entra に対して認証できることがわかります。
Active Directory でユーザー アカウントが無効になっている場合は、そのユーザー アカウントが直ちに Microsoft Entra への認証を受けられないようにする必要があります。
Solution: You configure Microsoft Entra Password Protection.
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: B (メーッセージを残す**)**

最新問題**: 138**
次の表に示すリソースを含むAzureサブスクリプションがあります。

Name	Type
Group1	Group that has the Assigned membership type
App1	Enterprise application in Azure Active Directory (Azure AD)
Contributor	Azure subscription role
Role1	Azure Active Directory (Azure AD) role

どのリソースに対してアクセスレビューを作成できますか？

A. Group1、App1、Contributor、Role1

B. ホテルと寄稿者のみ

C. Group1、Role1、およびContributorのみ

D. グループ1のみ

Answer: (解答を表示する**)**

Access reviews require an Azure AD Premium P2 license.

Access reviews for Group1 and App1 can be configured in Azure AD Access Reviews.

Access reviews for the Contributor role and Role1 would need to be configured in Privileged Identity Management (PIM). PIM is included in Azure AD Premium P2.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review?toc=/azure/active-directory/governance/toc.json

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

最新問題**: 139**

デフォルトのアプリ登録設定を持つAzureActive Directory（Azure AD）テナントがあります。テナントには、次の表に示すユーザーが含まれています。

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

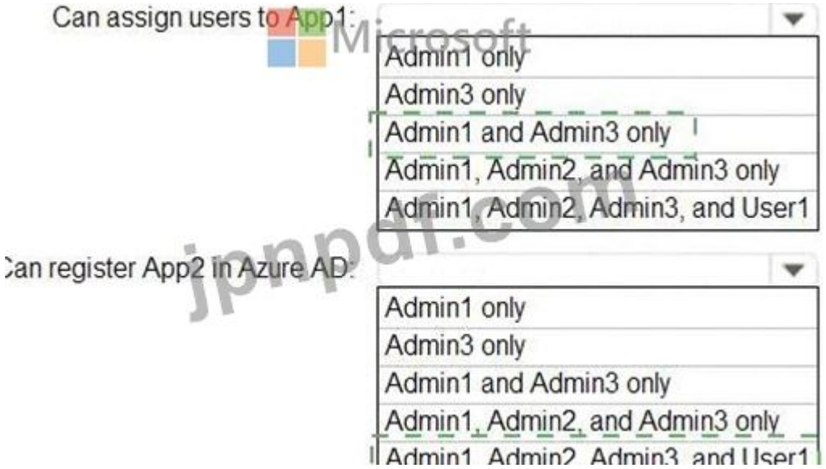
App1とApp2という名前の2つのクラウドアプリを購入します。グローバル管理者は、App1をAzureADに登録します。

ユーザーをApp1に割り当てることができるユーザーと、AzureADにApp2を登録できるユーザーを特定する必要があります。

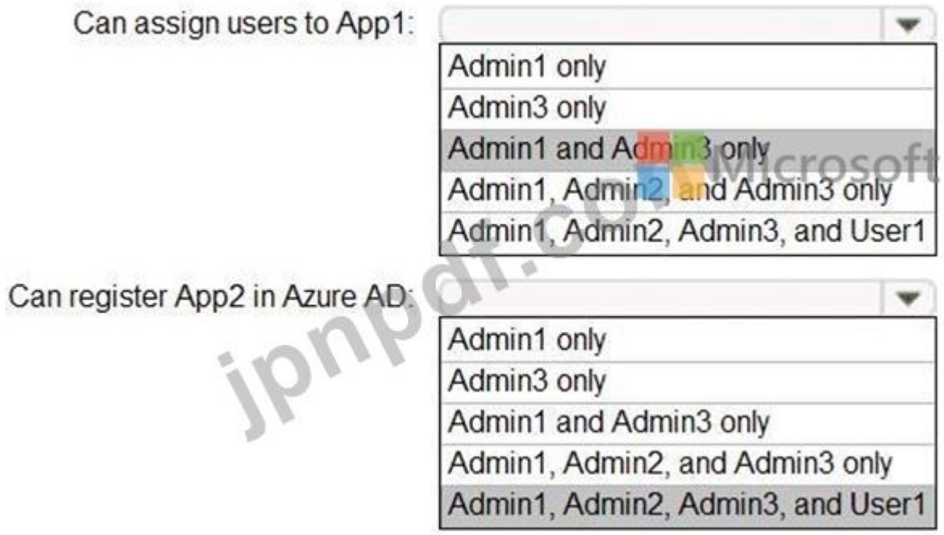
何を特定する必要がありますか？回答するには、回答エリアで適切なオプションを選択してください。

注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:



Explanation:



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

最新問題**: 140**
会社には、User 1 という名前のユーザーを含む Microsoft Entra テナントがあります。
同社にはマーケティングと財務という2つの部門があります。
マーケティング部門のユーザーのみを管理するには、User1 に権限を付与する必要があります。
最初に何を作成すべきでしょうか?
A. 管理グループ
B. a resource group
C. Microsoft 365 グループ
D. 行政単位

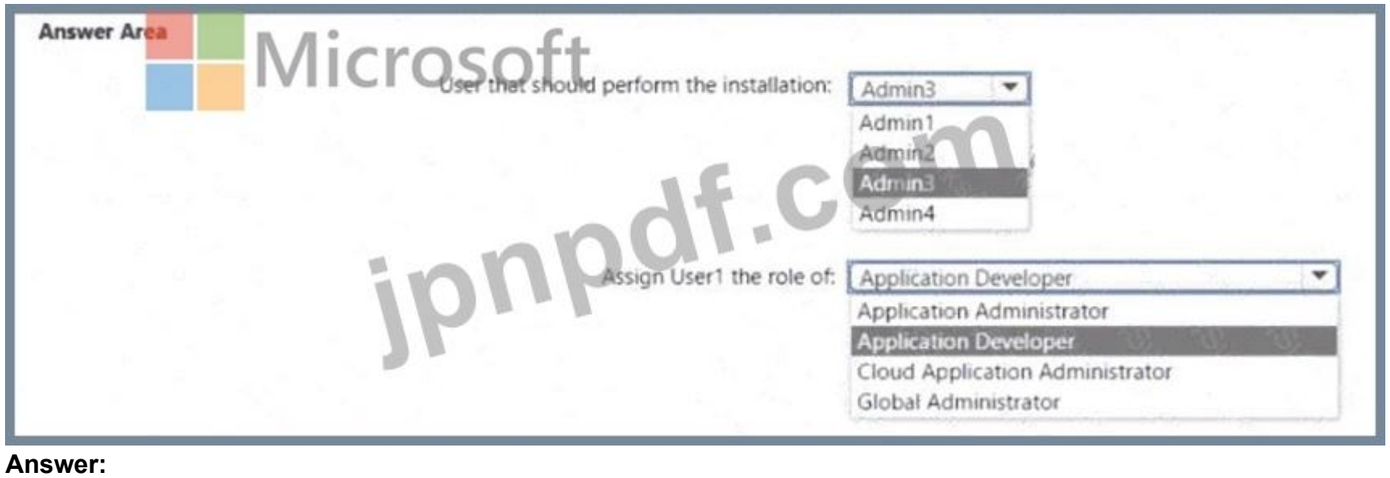
Answer: D (メーッセージを残す)

最新問題: **141**
ユーザーが High 70 サインイン アラートをトリガーしたときにアクセスをブロックする条件付きアクセス ポリシーを作成します。次の条件でポリシーをテストする必要があります。
* ユーザーが別の国からサインインします。
* ユーザーがサインイン リスクをトリガーします。
テストを完了するために何を使用する必要がありますか?
A. 条件付きアクセスの What If ツール
B. Azure AD のサインイン ログ
C. Azure AD のアクセス レビュー
D. Microsoft Defender for Cloud Apps のアクティビティ ログ
Answer: A (メーッセージを残す)

最新問題: **142**
次の表に示すユーザーを含むハイブリッド Microsoft 365 サブスクリプションがあります。

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

オンプレミスのアプリを展開する予定です1。App1 は Azure AD に登録され、Azure AD アプリケーション プロキシを使用します。
アプリケーション プロキシ コネクタのインストールを委任し、User1 が App1 を Azure AD に登録できるようにする必要があります。ソリューションでは、最小特権の原則を使用する必要があります。
どのユーザーがインストールを実行する必要がありますか?また、Users1 にはどの役割を割り当てる必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:

Explanation:

最新問題: **143**

タスク5

Windows 10/11 Enterprise E3 ライセンスを Sg-Retail グループに割り当てる必要があります。

Answer:

See the Explanation for the complete step by step solution

Explanation:

To assign a Windows 10/11 Enterprise E3 license to the Sg-Retail group, you can follow these steps:

Sign in to the Microsoft Entra admin center:

Make sure you have the role of Global Administrator or License Administrator.

Navigate to the licensing page:

Go to Billing > Licenses1.

Find the Windows 10/11 Enterprise E3 license:

Look for the Windows 10/11 Enterprise E3 license in the list of available products.

Assign licenses to the group:

Select the license and then choose Assign licenses.

Search for and select the Sg-Retail group.

Confirm the assignment and make sure that the correct number of licenses is available for the group.

Review and confirm the assignment:

Ensure that the licenses have been properly assigned to the Sg-Retail group without affecting other groups or users.
Monitor the license status:
Check the license usage and status to ensure that the Sg-Retail group members can utilize the Windows 10/11 Enterprise E3 features.
By following these steps, the Sg-Retail group should now have the Windows 10/11 Enterprise E3 licenses assigned to them.

最新問題**: 144**
監視要件を満たすには、多段階攻撃の検出を構成する必要があります。
何をすべきでしょうか?
A. Azure Sentinel ルールのロジックをカスタマイズします。
B. ワークブックを作成します。
C. Azure Sentinel データ コネクタを追加します。
D. Azure Sentinel プレイブックを追加します。
Answer: A (メーッセージを残す**)**
Topic 1, Litware, IncOverview
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.
Identity 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 gu est accounts in the litware.com tenant.
Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices 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.
On-premises Environment
The on-premises network contains the severs 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

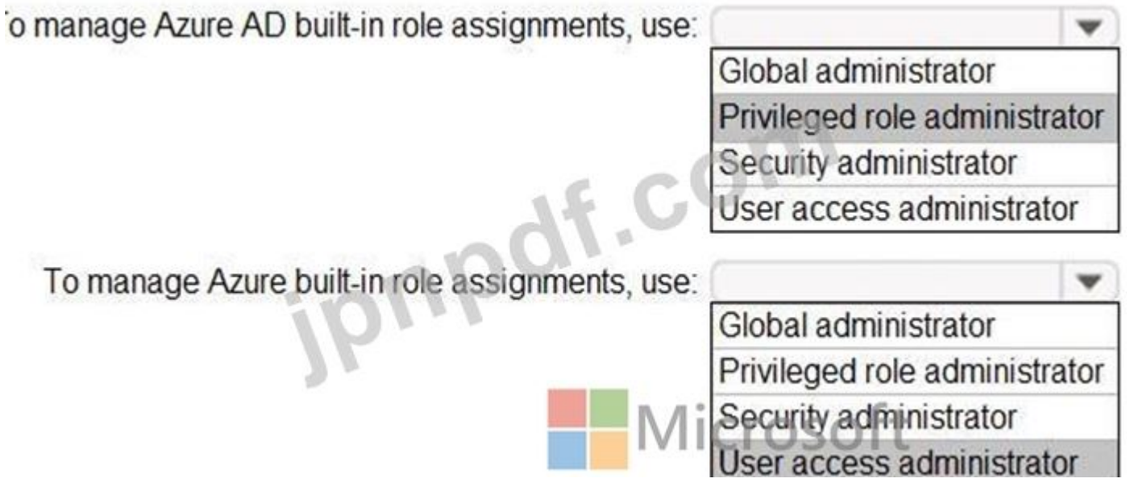
Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Delegation Requirements

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.
Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest.
Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft
365 group that he appropriate license assigned.
Management Requirement
Litware wants to create a group named LWGroup1 will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
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
Access 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.
Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

最新問題: **145**
役割の割り当てを管理するために使用する役割を特定する必要があります。ソリューションは、委任の要件を満たす必要があります。
あなたは何をするべきか？回答するには、回答エリアで適切なオプションを選択してください。
注：正しい選択はそれぞれ1ポイントの価値があります。

Answer:

Explanation:



Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
Topic 2, Contoso, LtdOverview
Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.
Existing Environment
The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces OU contains all users and computers.
The Contoso.com Active Directory domain contains the users shown in the following table.

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

Microsoft 365/Azure Environment

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

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS). Only the Contoso Resources OU is synced.

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

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

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

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

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

Security defaults are disabled for Contoso.com.

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

Problem Statements

Contoso identifies the following issues:

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

Planned Changes

Contoso plans to implement the following changes.

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

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

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

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

Technical Requirements

Contoso identifies the following technical requirements:

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

* Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
* Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
* The helpdesk administrators must be able to manage licenses for only the users in their respective office.
* Users must be forced to change their password if there is a probability that the users' identity was compromised.

最新問題: **146**
次の表に示すユーザーを含むAzureActive Directory（Azure AD）テナントがあります。

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

User1はGroup1の所有者です。
次の設定を持つアクセスレビューを作成します。
レビューするユーザー :グループのメンバー
範囲：全員
グループ :グループ1
レビュアー :メンバー（自己）
User3のアクセスレビューを実行できるユーザーはどれですか？
A. User1、User2、およびUser3
B. User3のみ
C. User1のみ
D. User1とUser2のみ
Answer: (解答を表示する**)**

最新問題: **147**
Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションを持っています。
サブスクリプションのアプリのセキュリティを強化する予定です。
ユーザー認証を必要としないアプリを特定する必要がある
Microsoft 365 Defender ポータルでは何をすべきですか?
A. OAuth ポリシーを作成し、アラートを確認します。
B. クラウド アプリ カタログを確認します。
C. スナップショット Cloud Discovery レポートを作成します。
D. 検出されたアプリのクエリを作成します。
Answer: D (メーッセージを残す**)**

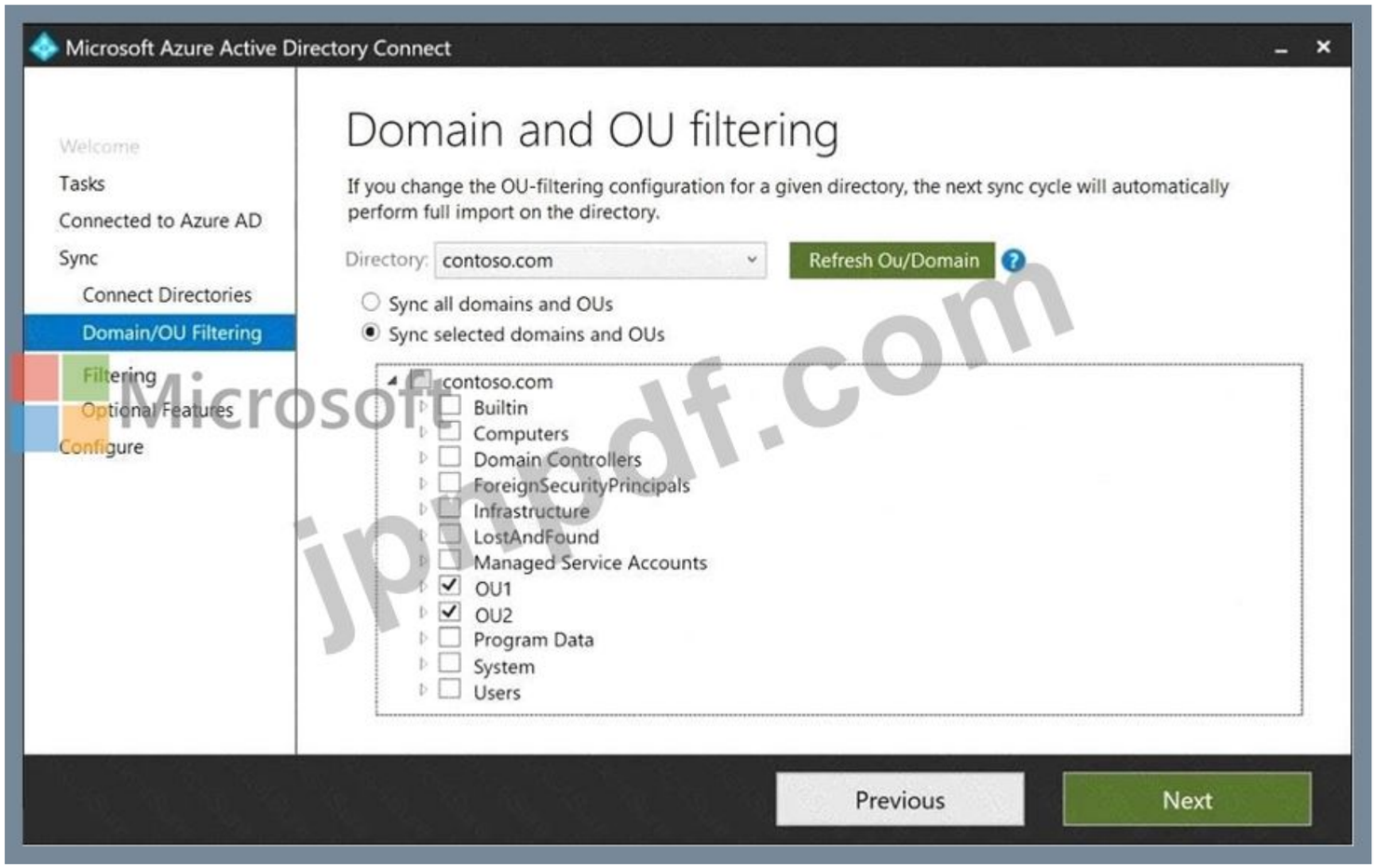
最新問題: **148**
Azure Monitorを使用して、Azure Active Directory（Azure AD）アクティビティログを分析します。
Yonは、テール付きのAzure AI）ユーザーのサインイン試行に対して、毎日100を超える電子メールアラートを受信します。
新しいセキュリティ管理者があなたの代わりにアラートを受信することを確認する必要があります。
解決策 :Azureモニターから、データ収集ルールを作成します。
これは目標を達成していますか？

A. いいえ
B. はい
Answer: A (メーッセージを残す**)**

最新問題**: 149**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。ドメインには、次の表に示すオブジェクトが含まれています。

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

Azure AD Connect をインストールします。「ドメインと OU のフィルタリング」の説明に従って、ドメインと OU のフィルタリング設定を構成します。([ドメインと OU フィルタリング] タブをクリックします。)

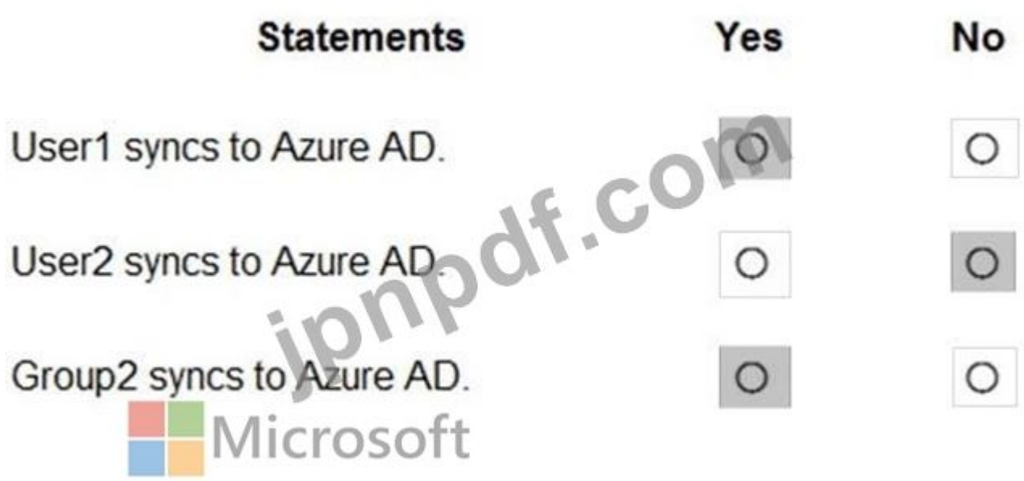


「ユーザーとデバイスのフィルター」の説明に従って、ユーザーとデバイスのフィルター設定を構成します。(「ユーザーとデバイスのフィルター」タブをクリックします。)

次の各ステートメントについて、そのステートメントが true の場合は [はい] を選択します。それ以外の場合は、「いいえ」を選択します。

Answer:

Explanation:



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

Reference:

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

最新問題: 150

次の表に示すリソースを含む contoso.com という名前の Azure AD テナントがあります。

Admin 1 という名前のユーザーを作成します。

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

管理者が contoso.com のセキュリティの既定値を有効にできることを確認する必要があります。
最初に何をすべきですか？
A. Identity Governance を構成します。
B. Package1 を削除します。
C. CAPolicy1 を削除します。
D. Admin1 に Au1 の認証管理者ロールを割り当てます。
Answer: (解答を表示する**)**
To enable Security defaults for contoso.com, you should first sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator. Then, browse to Azure Active Directory > Properties and select Manage security defaults. Set the Enable security defaults toggle to Yes and select Save.
After that, you can assign Admin1 the Identity Administrator role for Au1 to enable them to manage security defaults for the tenant.
https://practical365.com/what-are-azure-ad-security-defaults-and-should-you-use-them/