Microsoft.SC-300J.v2022-07-09.q43

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:	43
バージョン:	v2022-07-09
アクセス数:	471
ページビュー数:	430
https://www.jpnpdf.com/Microsoft.SC-300J.v2022-07-09.q43-mondaishu.html	

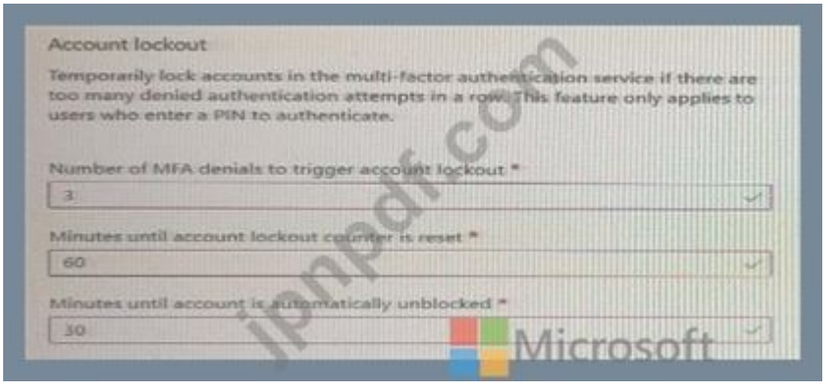
最新問題: **1**
条件付きアクセスポリシーを使用するAzureActive Directory（Azure AD）テナントがあります。
サードパーティのセキュリティ情報およびイベント管理（SIEM）を使用して、条件付きアクセスの使用状況を分析することを計画しています。
条件付きアクセスポリシーデータを含むAzureADログをダウンロードする必要があります。
Azure ADから何をエクスポートする必要がありますか？
A. JSON形式でのサインイン
B. CSV形式でのサインイン
C. JSON形式の監査ログ
D. CSV形式の監査ログ
Answer: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-audit-logs

最新問題: **2**
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**)**

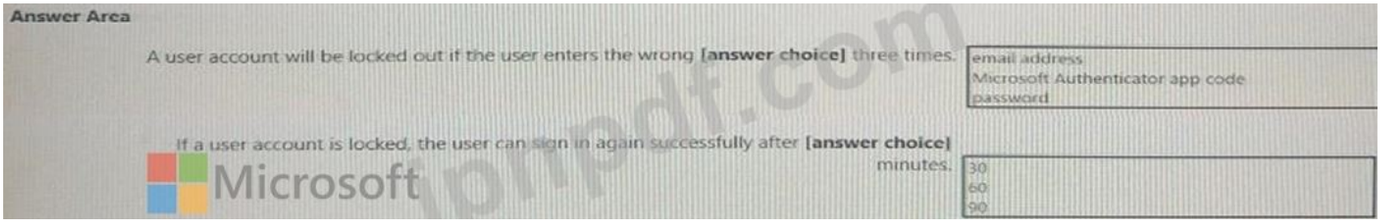
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

最新問題: 3
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

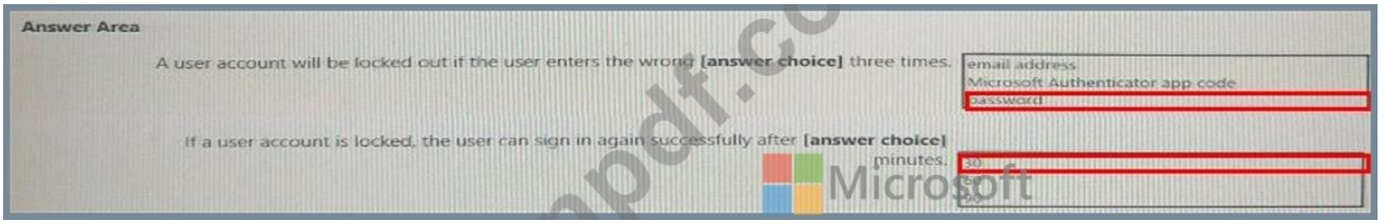
最新問題: 4
多要素認証（MFA）が有効になっているAzure Active Directory（Azure AD）テナントがあります。
アカウントのロックアウト設定は、次の図に示すように構成されています。



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。

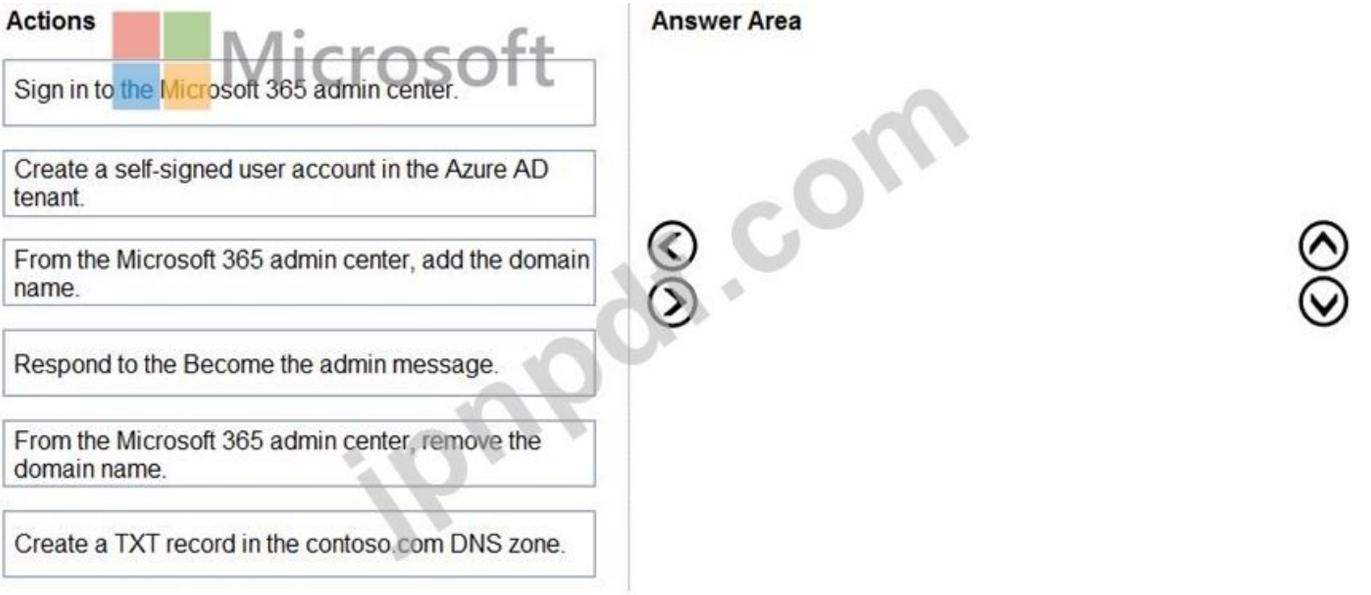


Answer:

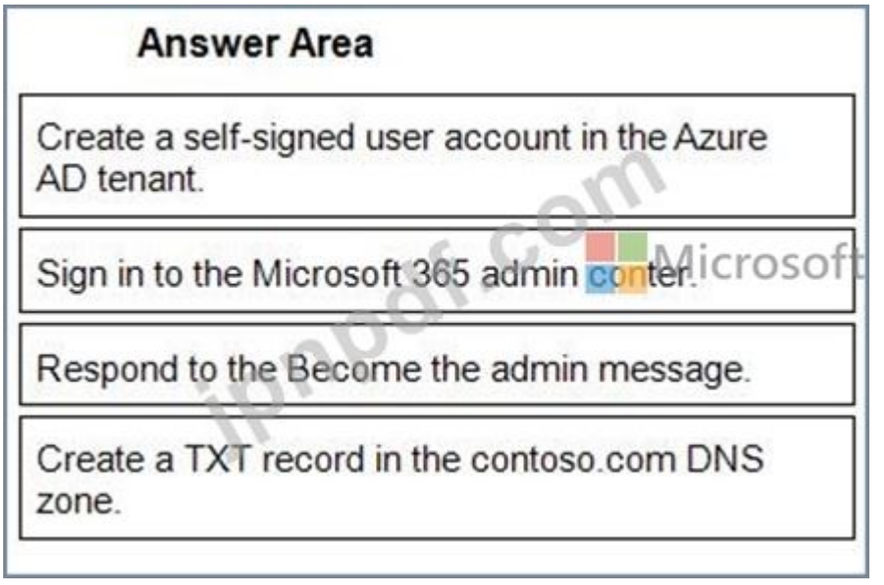


最新問題: **5**
Microsoft365テナントがあります。
Azure Active Directory（Azure AD）テナントは、オンプレミスのActiveDirectoryドメインに同期します。
Emergency1という名前の緊急アクセス管理アカウントを作成する予定です。Emergency1には、AzureADのグローバル管理者の役割が割り当てられます。Emergency1は、AzureAD機能の障害およびオンプレミスインフラストラクチャの障害が発生した場合に使用されます。
緊急時にEmergency1がサインインできなくなる可能性を減らす必要があります。
あなたは何をするべきか？
A. Emergency1に多要素認証（MFA）を要求するように条件付きアクセスポリシーを構成します。
B. Emergency1のグローバル管理者ロールのAzure AD特権ID管理（PIM）アクティベーションが必要です。
C. Emergency1のサインイン場所を企業ネットワークのみに制限する条件付きアクセスポリシーを構成します。
D. Emergency1が変更された場合、またはサインインした場合にアラートを生成するようにAzureMonitorを構成します。
Answer: D (メーッセージを残す**)**

最新問題: **6**
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:



1 - Create a self-signed user account in the Azure AD tenant.
2 - Sign in to the Microsoft 365 admin conter.
3 - Respond to the Become the admin message.
4 - Create a TXT record in the contoso.com DNS zone.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

最新問題**: 7**
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

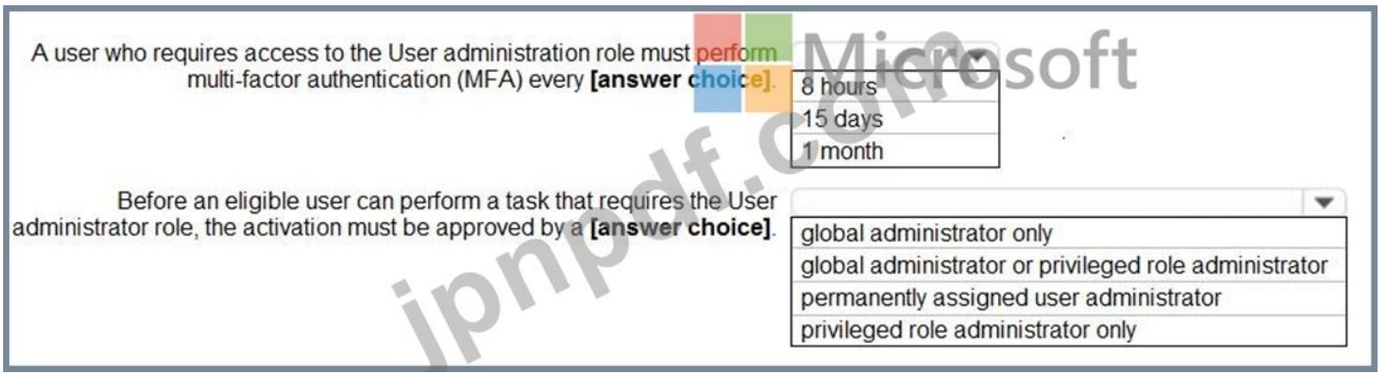
Answer: (解答を表示する**)**

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

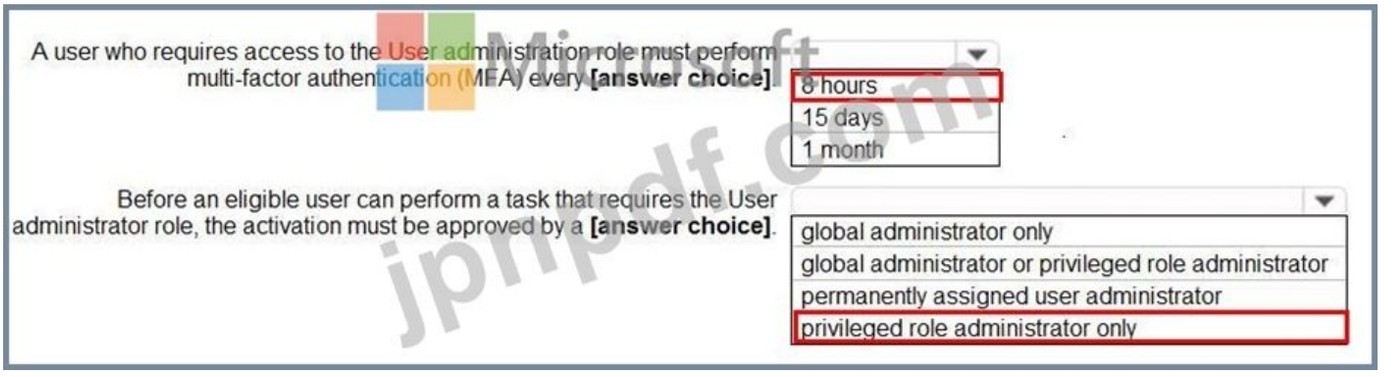
最新問題**: 8**

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。

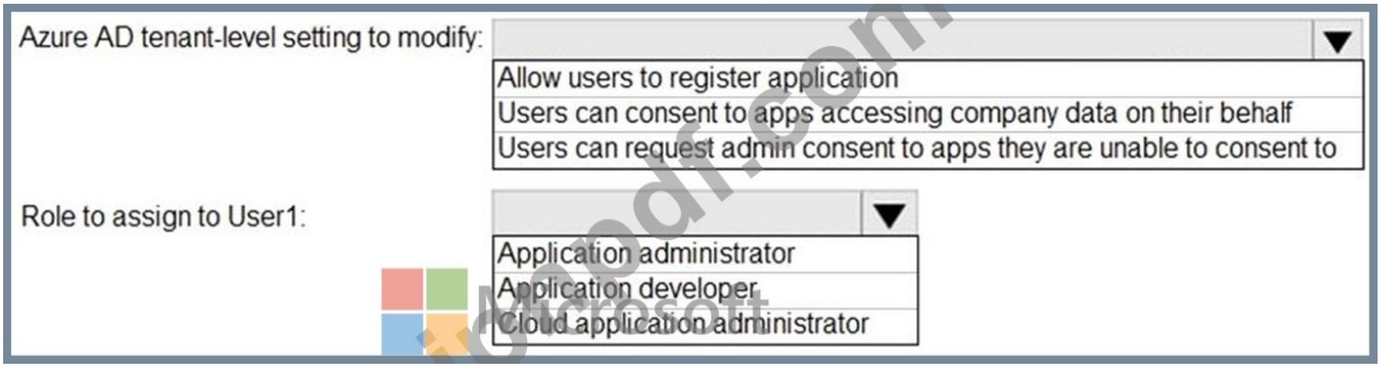


Answer:



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**: 9**
委任の要件を満たすには、AzureADでアプリの登録を構成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:

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

最新問題: **10**
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、アクショングループを変更します。
これは目標を達成していますか？
A. いいえ
B. はい
Answer: (解答を表示する)

最新問題: **11**
あなたの会社は最近、Azure Active Directory（Azure AD）特権ID管理（PIM）を実装しました。
PIMでの役割を確認すると、会社のIT部門の15人のユーザー全員が永続的なセキュリティ管理者権限を持っていることがわかります。
IT部門のユーザーが、必要な場合にのみセキュリティ管理者の役割にアクセスできるようにする必要があります。
セキュリティ管理者の役割の割り当てには何を構成する必要がありますか？
A. 役割設定の詳細から対象の割り当てを期限切れにします
B. 役割設定の詳細からアクティブな割り当てを期限切れにします
C. アクティブへの割り当てタイプ
D. 適格への割り当てタイプ
Answer: D (メーッセージを残す)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

最新問題: **12**
contoso.comのSMTPのアドレス空間を使用するMicrosoftExchange組織があります。

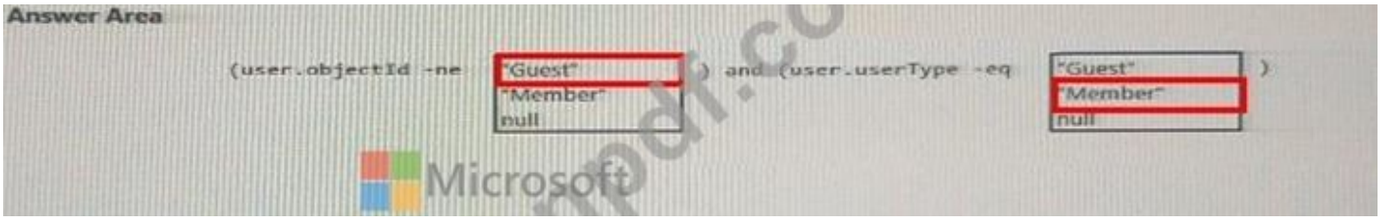
何人かのユーザーは、自分のcontoso.com電子メールアドレスを使用して、Azure Active Directory（Azure AD）へのセルフサービスサインアップを行います。
自己署名ユーザーを含むAzureADテナントに対するグローバル管理者特権を取得します。
Microsoft 365サービスへのセルフサービスサインアップのために、ユーザーがcontoso.com AzureADテナントでユーザーアカウントを作成できないようにする必要があります。
どのPowerShellコマンドレットを実行する必要がありますか？
A. Set-MsolCompanySettings
B. Set-MsolDomainFederationSettings
C. 更新-MsolfederatedDomain
D. Set-MsolDomain
Answer: A (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

最新問題**: 13**
Azure Active Directory（Azure AD）テナントがあります。
次の設定を持つHRAppsという名前のエンタープライズアプリケーションコレクションを作成します。
*アプリケーション：Appl。App？、App3
*所有者：管理者
*ユーザーとグループ：HRUsers
AH 3つのアプリには、次のプロパティ設定があります。
*ユーザーがサインインできるようにする：はい
*必要なユーザー割り当て：はい
*ユーザーに表示：はい
ユーザーは、My Appsポータルにアクセスすると、App1とApp2のみを訴えると報告しています。
ユーザーがApp3も表示できるようにする必要があります。App3から何をすべきですか？
App3から何をすべきですか？
A. ユーザーとグループから、HRUsersを追加します。
B. プロムのプロパティ、必要なユーザー割り当てを[いいえ]に変更します。
C. [権限]から、ユーザー同意の権限を確認します。
D. シングルサインオンから、サインオン方式を構成します。
Answer: A (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal
https://docs.microsoft.com/en-us/azure/active-directory/user-help/my-applications-portal-workspaces

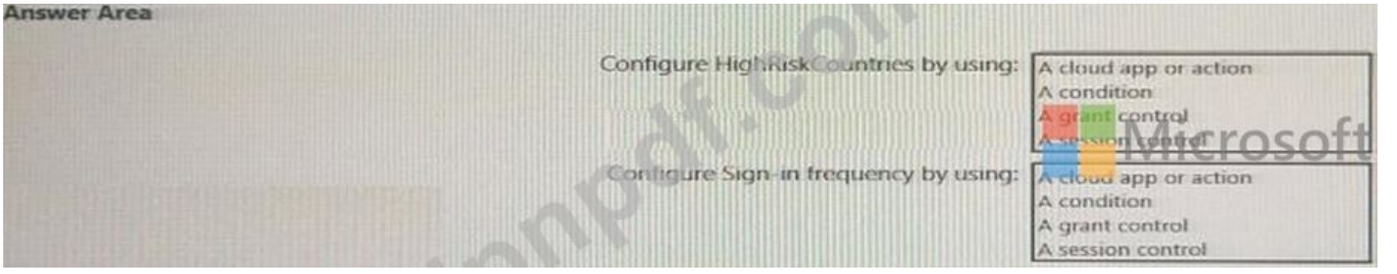
最新問題**: 14**

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:



最新問題: **15**
Microsoft36Sテナントがあります。
高リスクの国のリストを含むHighRiskCountriesという名前の場所を作成します。
リスクの高い国から接続する場合、ユーザーが認証を維持できる時間を制限する必要があります。
条件付きアクセスポリシー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:

最新問題: **16**

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: C (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

最新問題**: 17**
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**: 18**

ActiveDirectoryフォレストに同期するAzureActive Directory（Azure AD）テナントがあります。テナント認証を通じて使用します。
企業のセキュリティポリシーには、次のように記載されています。
ドメインコントローラーは、インターネットと直接通信してはなりません。
必要なソフトウェアのみをサーバーにインストールする必要があります。
Active Directoryドメインには、次の表に示すオンプレミスサーバーが含まれています。

Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

サーバーに障害が発生した場合に、ユーザーがAzureADに対して認証できることを確認する必要があります。
追加のパススルー認証エージェントをどのサーバーにインストールする必要がありますか？
A. Server1
B. Server2
C. Server4
D. Server3
Answer: A (メーッセージを残す)

最新問題: **19**
Microsoft365テナントがあります。
Azure Active Directory（Azure AD）では、利用規約を構成します。
利用規約に同意したユーザーのみがテナント内のリソースにアクセスできるようにする必要があります。他のユーザーはアクセスを拒否する必要があります。
何を設定する必要がありますか？
A. Microsoft Cloud AppSecurityのアクセスポリシー。
B. Microsoft EndpointManagerの利用規約。
C. AzureADの条件付きアクセスポリシー
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)
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/terms-of-use

最新問題: **20**
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**: 21**

次の表に示すオブジェクトを含むAzureActive Directory（Azure AD）テナントがあります。

Name	Type	Directly assigned license
User1	User	*None*
User2	User	Microsoft Office 365 Enterprise E5
Group1	Security group	Microsoft Office 365 Enterprise E5
Group2	Microsoft 365 group	*None*
Group3	Mail-enabled security group	*None*

Group3にメンバーとして追加できるオブジェクトはどれですか？

A. User2とGroup2のみ

B. User2、Group1、およびGroup2のみ

C. User1、User2、Group1、Group2

D. User1とUser2のみ

E. User2のみ

Answer: E (メーッセージを残す**)**

Reference:

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

最新問題**: 22**

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。ユーザーは、Windows 10を実行し、ドメインに参加しているコンピューターにサインインします。

Azure ADシームレスシングルサインオン（Azure ADシームレスSSO）を実装する予定です。

AzureADシームレスSSO用にコンピューターを構成する必要があります。

あなたは何をするべきか？
A. エンタープライズステートローミングを有効にします。
B. サインインオプションを構成します。
C. Azure ADConnect認証エージェントをインストールします。
D. イントラネットゾーンの設定を変更します。
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start

最新問題**: 23**
次の表に示すオブジェクトを含むAzureActive Directory（Azure AD）テナントがあります。

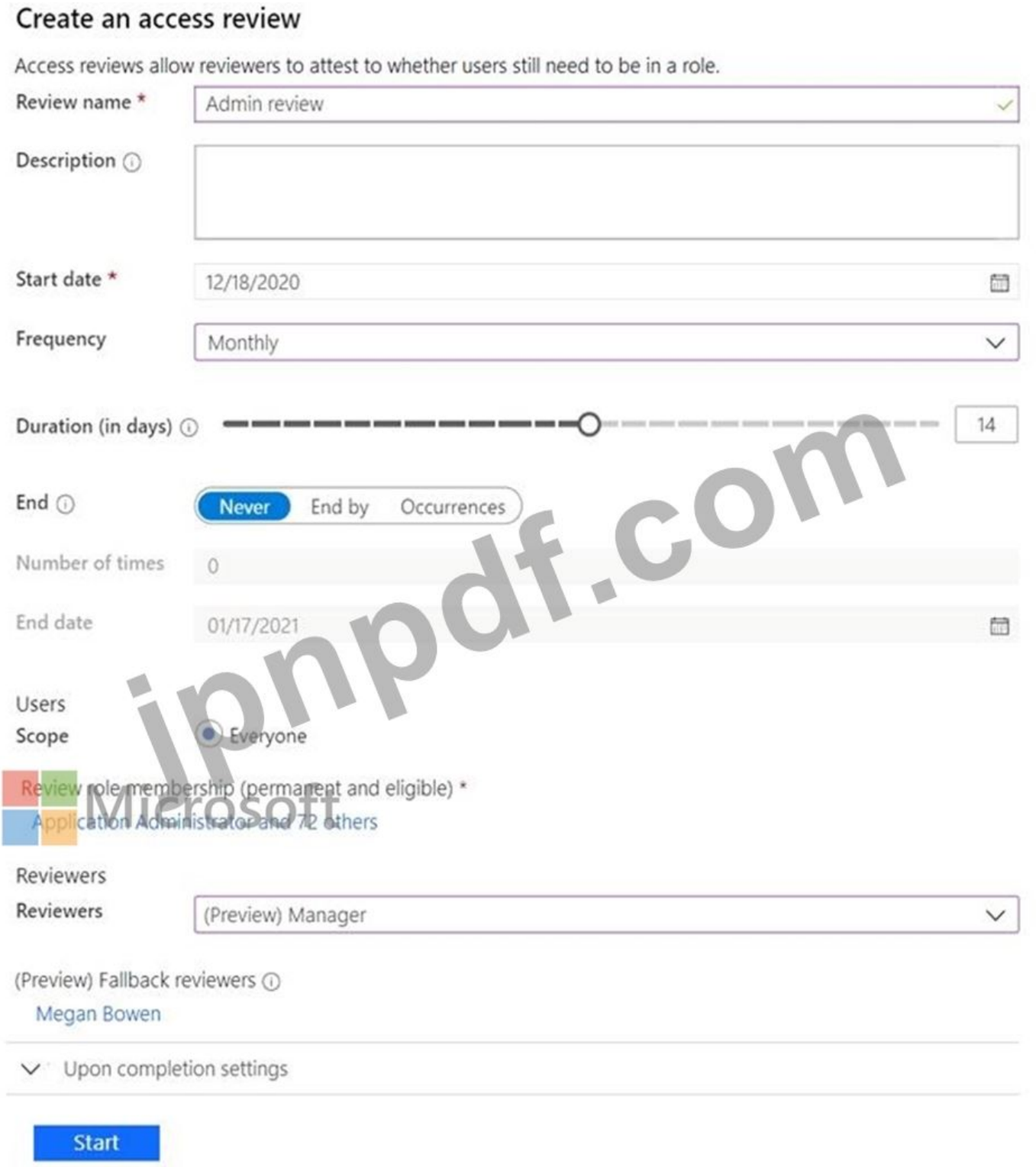
Name	Type
User1	User
Guest1	Guest
Identity1	Managed identity

Azure ADロールのAzure特権ID管理（PIM）に適格として追加できるオブジェクトはどれですか？
A. User1のみ
B. User1とIdentity1のみ
C. ユーザー1。Guest1、およびIdentity
D. User1とGuest1のみ
Answer: D (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-deployment-plan

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: 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: **25**
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している必要があります。
あなたは何をするべきか？
A. Microsoft Azure Active Directory接続ウィザードから、[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接続ウィザードから、[ユーザーサインインの変更]を選択します。
Answer: A (メーッセージを残す**)**
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

最新問題: **26**
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：役割ごとに個別のアクセスレビューを作成します。
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)
D18912E1457D5D1DDCBD40AB3BF70D5D
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

最新問題**: 27**
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:

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, Ltd
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**: 28**
Identity Governanceを使用して、アプリケーションアクセスの割り当てを追跡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。
あなたは最初に何をすべきですか？
A. エンタープライズアプリケーションのユーザー同意設定を変更します。
B. カタログを作成します。
C. プログラムを作成します。
D. エンタープライズアプリケーションの管理者同意要求設定を変更します。
Answer: B (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview Overview Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.
Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.
Topic 1, Litware, Inc

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 guest 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

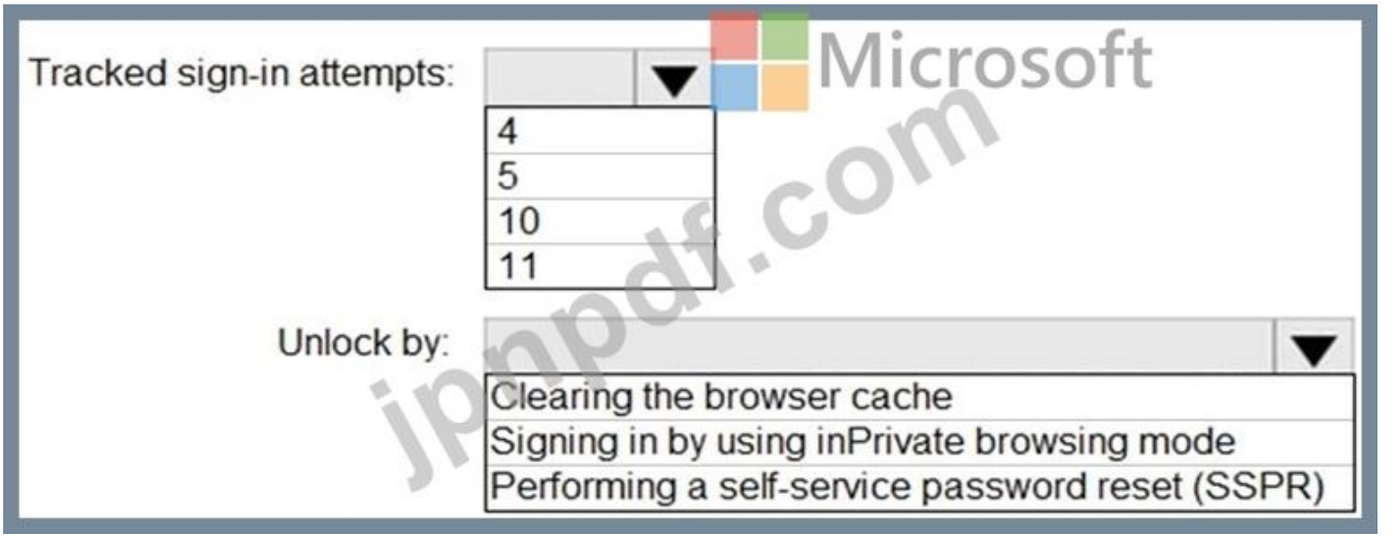
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to 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: **29**
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。
あなたは何をするべきか？
A. AzureSentinelルールロジックをカスタマイズします。
B. AzureSentinelデータコネクタを追加します。
C. AzureSentinelプレイブックを追加します。
D. ワークブックを作成します。
Answer: B (メーッセージを残す**)**

最新問題: **30**
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
Pa55w.rd123
Pa55word12
Pa55word12
Pa55word12
Pa55w.rd12

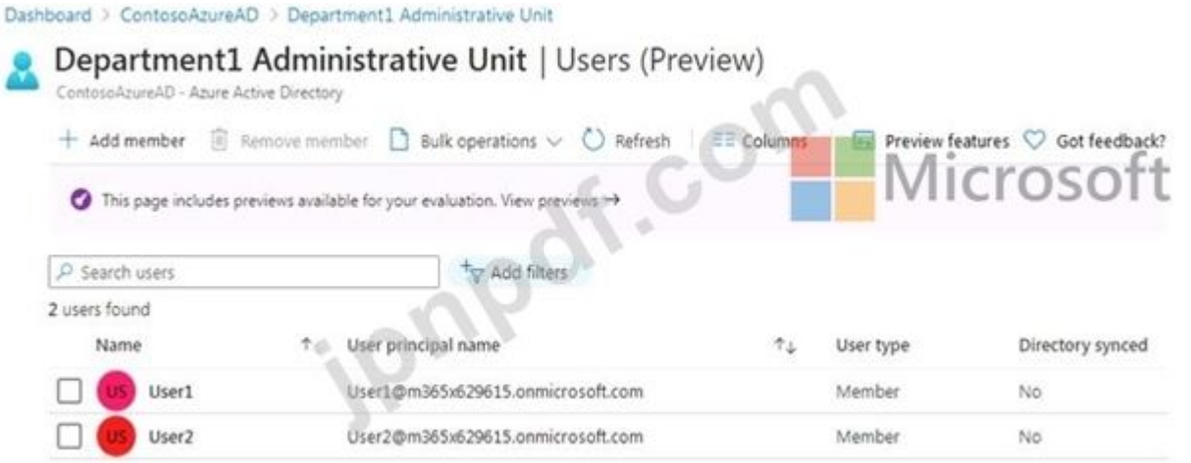
User1で追跡されたサインインの試行回数と、300秒のロックアウト期間が終了する前にUser1がアカウントのロックを解除する方法を特定する必要があります。
何を特定する必要がありますか？答えるには、適切なものを選択してください
注：正しい選択はそれぞれ1ポイントの価値があります。



Answer:

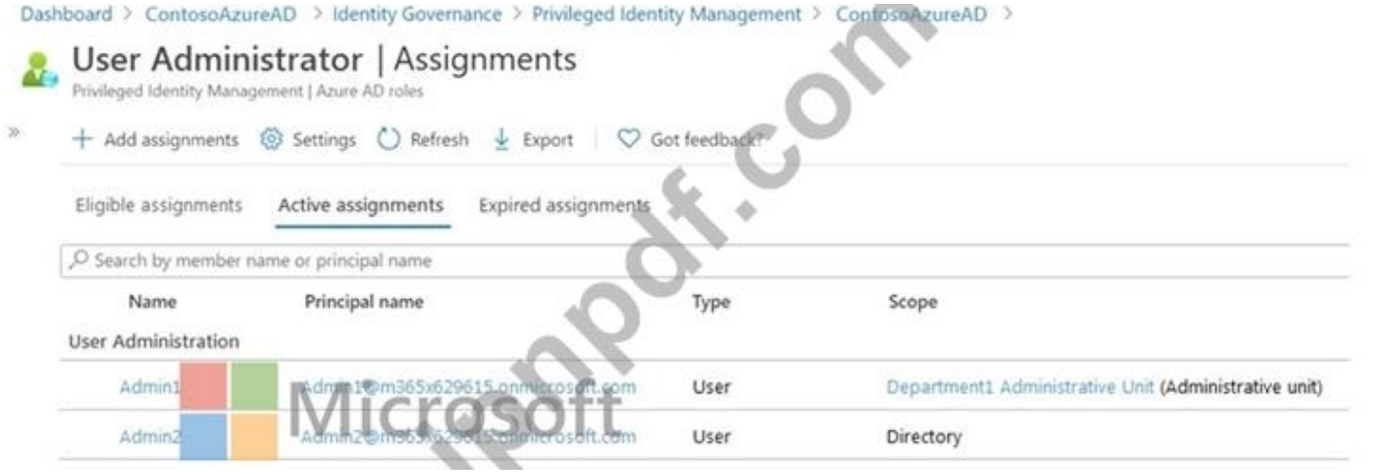
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

最新問題**: 31**
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.	○	○

Reference:

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

最新問題: **32**

User1という名前のユーザーと次の表に示すグループを含むAzureActive Directory（Azure AD）テナントがあります。

Name	Type	Membership type
Group1	Security	Assigned
Group2	Security	Dynamic User
Group3	Security	Dynamic Device
Group4	Microsoft 365	Assigned

テナントでは、次の表に示すグループを作成します。

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

GroupAとGroupBにどのメンバーを追加できますか？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。

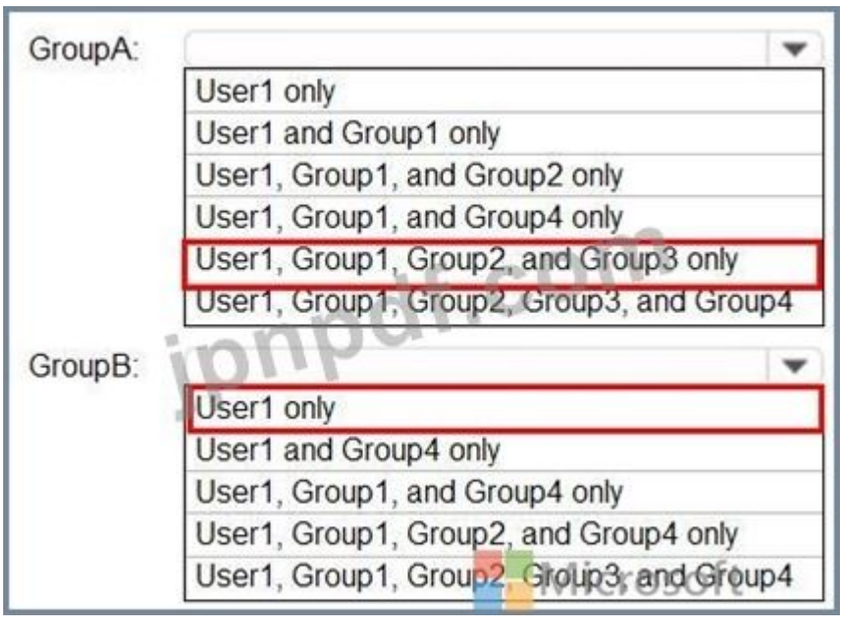
GroupA:

- User1 only
- User1 and Group1 only
- User1, Group1, and Group2 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group3 only
- User1, Group1, Group2, Group3, and Group4

GroupB:

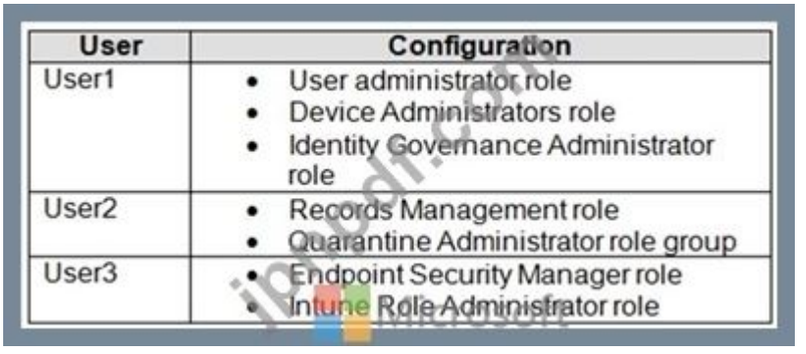
- User1 only
- User1 and Group4 only
- User1, Group1, and Group4 only
- User1, Group1, Group2, and Group4 only
- User1, Group1, Group2, Group3, and Group4

Answer:



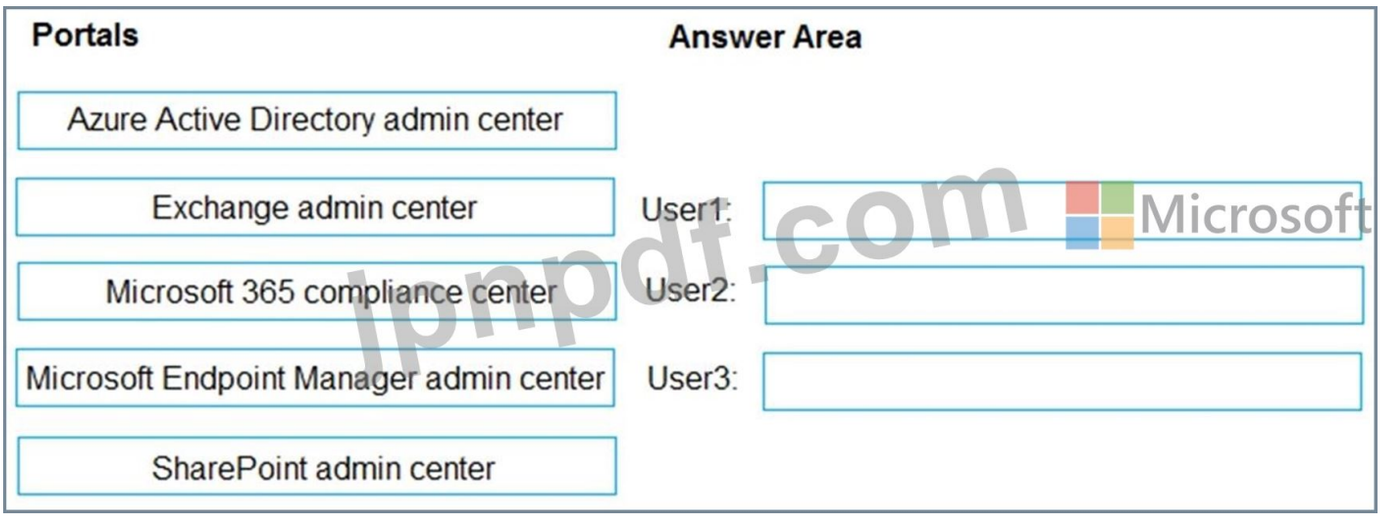
Reference:
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

最新問題**: 33**
User1、User2、およびUser3という名前の3人のユーザーを含むMicrosoft 365E5サブスクリプションがあります。
次の表に示すように、ユーザーを構成する必要があります。

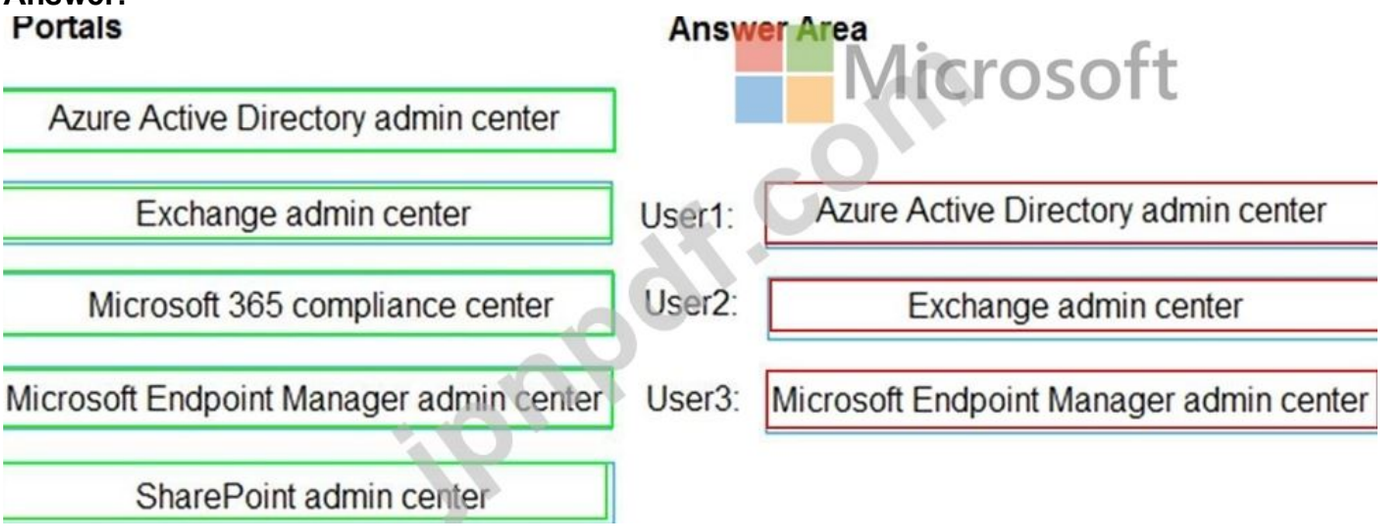


User	Configuration
User1	• User administrator role • Device Administrators role • Identity Governance Administrator role
User2	• Records Management role • Quarantine Administrator role group
User3	• Endpoint Security Manager role • Intune Role Administrator role

各ユーザーを構成するには、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、適切なポータルを適切なユーザーにドラッグします。各ポータルは、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、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:



最新問題: **34**

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. 組織内のアドレスへのメール

C. モバイルアプリコード

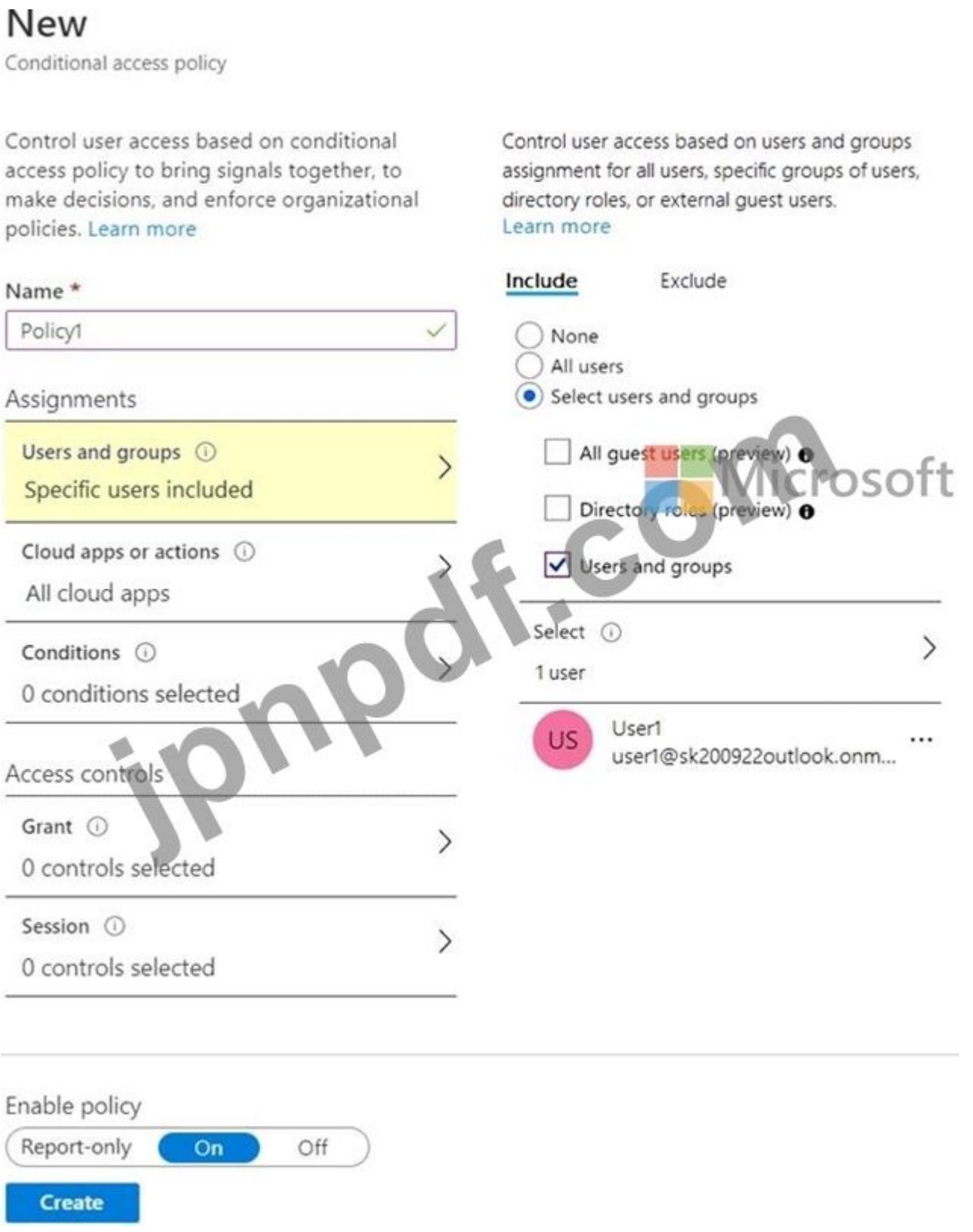
D. ホームプリオン

Answer: D (メーッセージを残す**)**

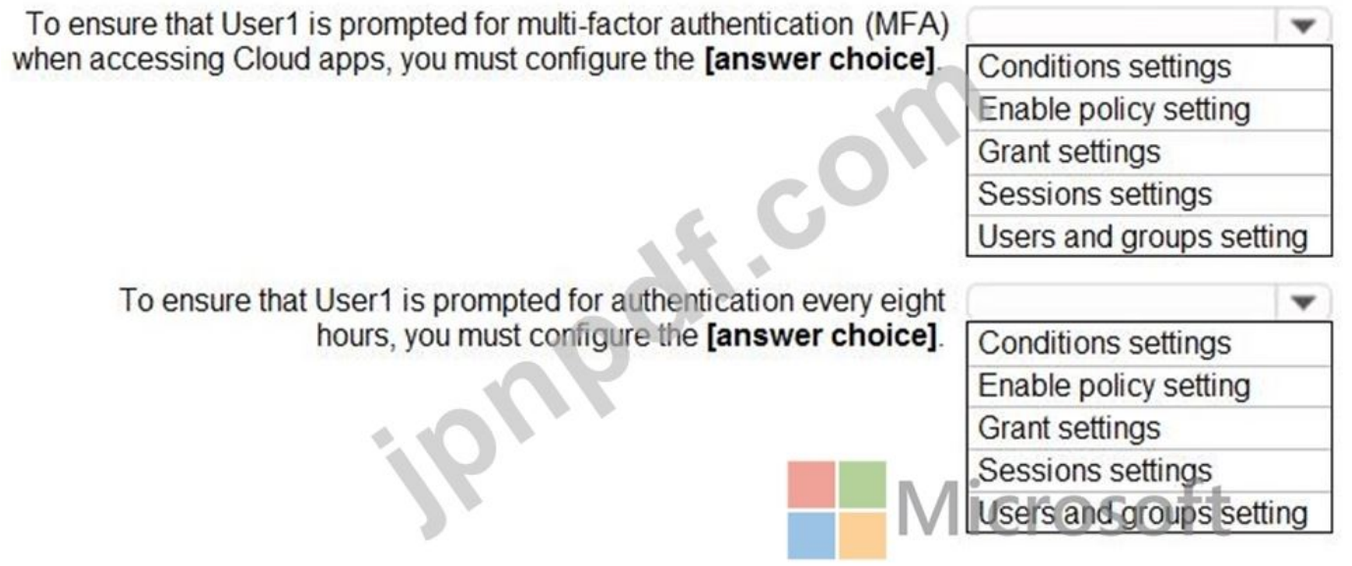
最新問題: **35**

セキュリティのデフォルトが無効になっているAzureActive Directory（Azure AD）テナントがあります。

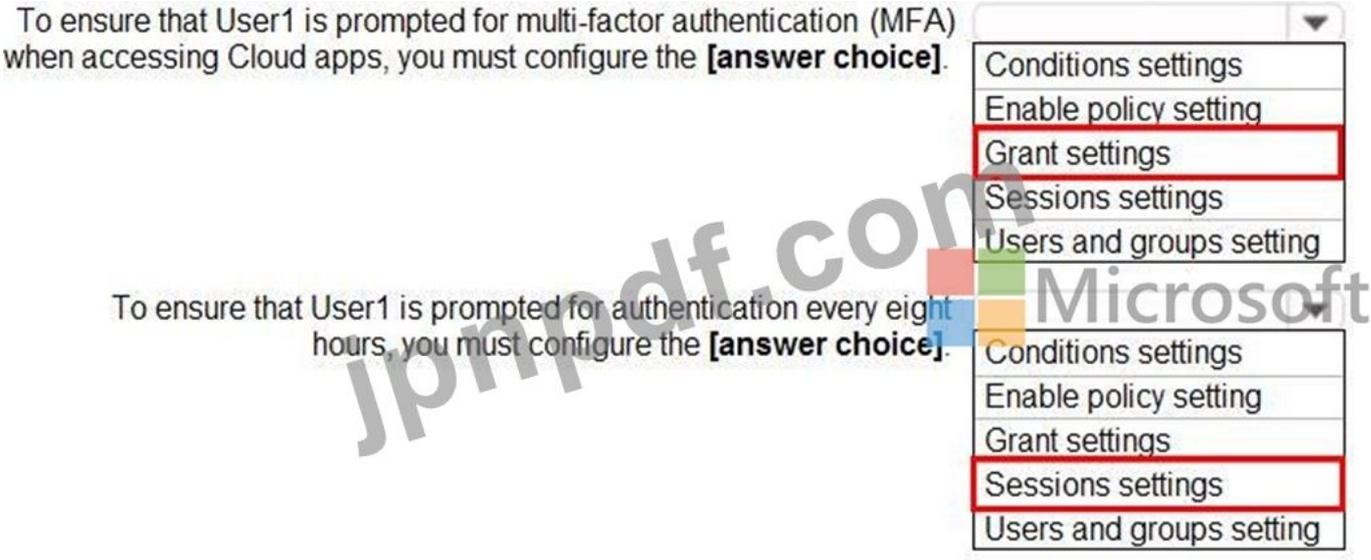
次の展示に示すように、条件付きアクセスポリシーを作成しています。



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:



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

最新問題**: 36**
Microsoft 365E5テナントがあります。
App1という名前のクラウドアプリを購入します。
Microsoft Cloud app Securityを使用して、App1のリアルタイムセッションレベルの監視を有効に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:

1 - Publish App1 in Azure Active Directory (Azure AD).
2 - From Microsoft Cloud App Security,modify the Connected apps settings for App1.
3 - From Microsoft Cloud App Security, create a session policy.
4 - Create a conditional access policy that has session controls configured.
Reference:
https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app
https://docs.microsoft.com/en-us/cloud-app-security/session-policy-aad

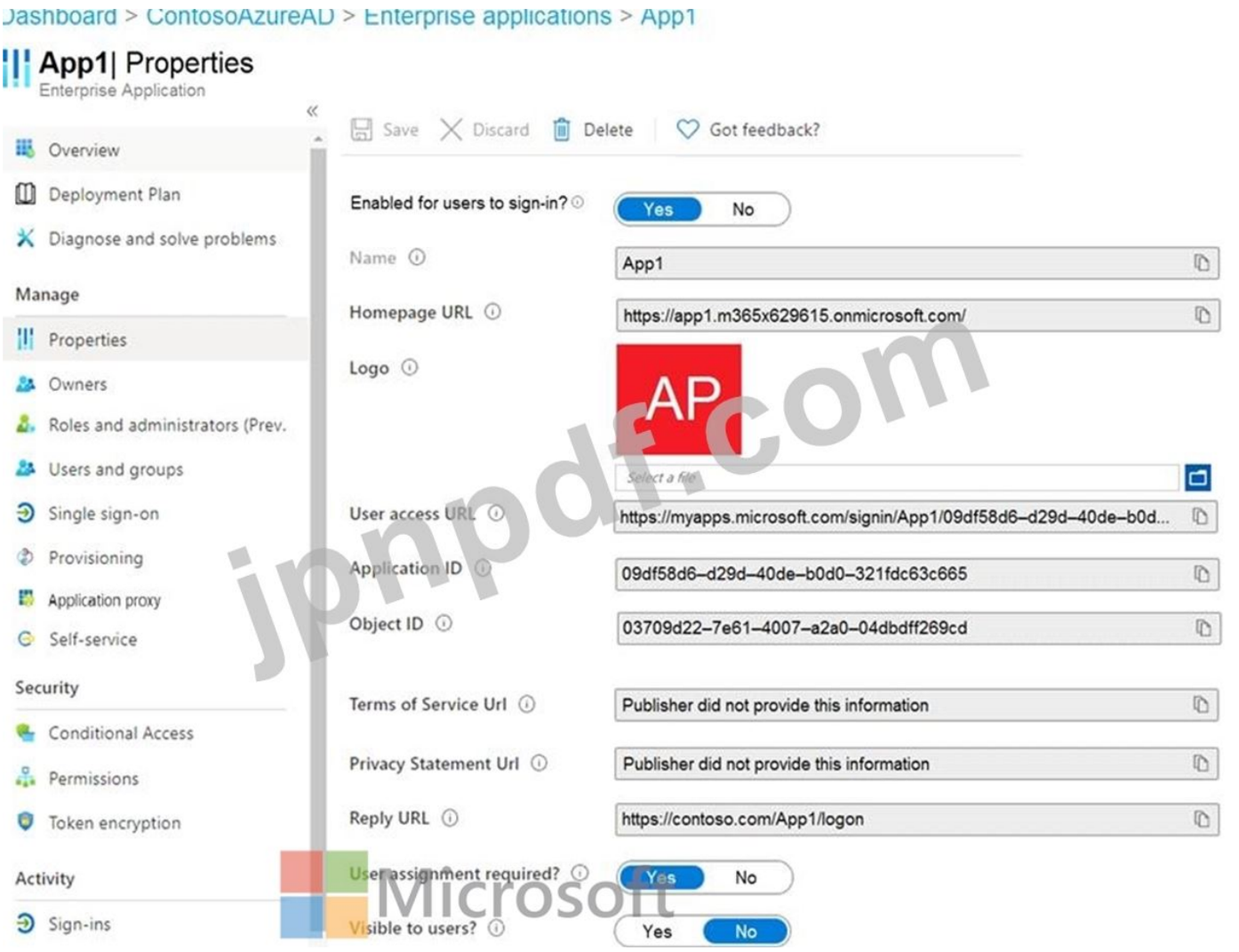
最新問題**: 37**
Microsoft365テナントがあります。
すべてのユーザーは携帯電話とラップトップを持っています。
ユーザーは、Wi-Fiアクセスや携帯電話接続がない遠隔地から頻繁に作業します。
ユーザーは、離れた場所から作業しているときに、ラップトップをインターネットにアクセスできる有線ネットワークに接続します。
多要素認証（MFA）を実装することを計画しています。
ユーザーがリモートロケーションから使用できるMFA認証方法はどれですか？
A. MicrosoftAuthenticatorアプリからの確認コード
B. セキュリティの質問
C. 声

D. SMS
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

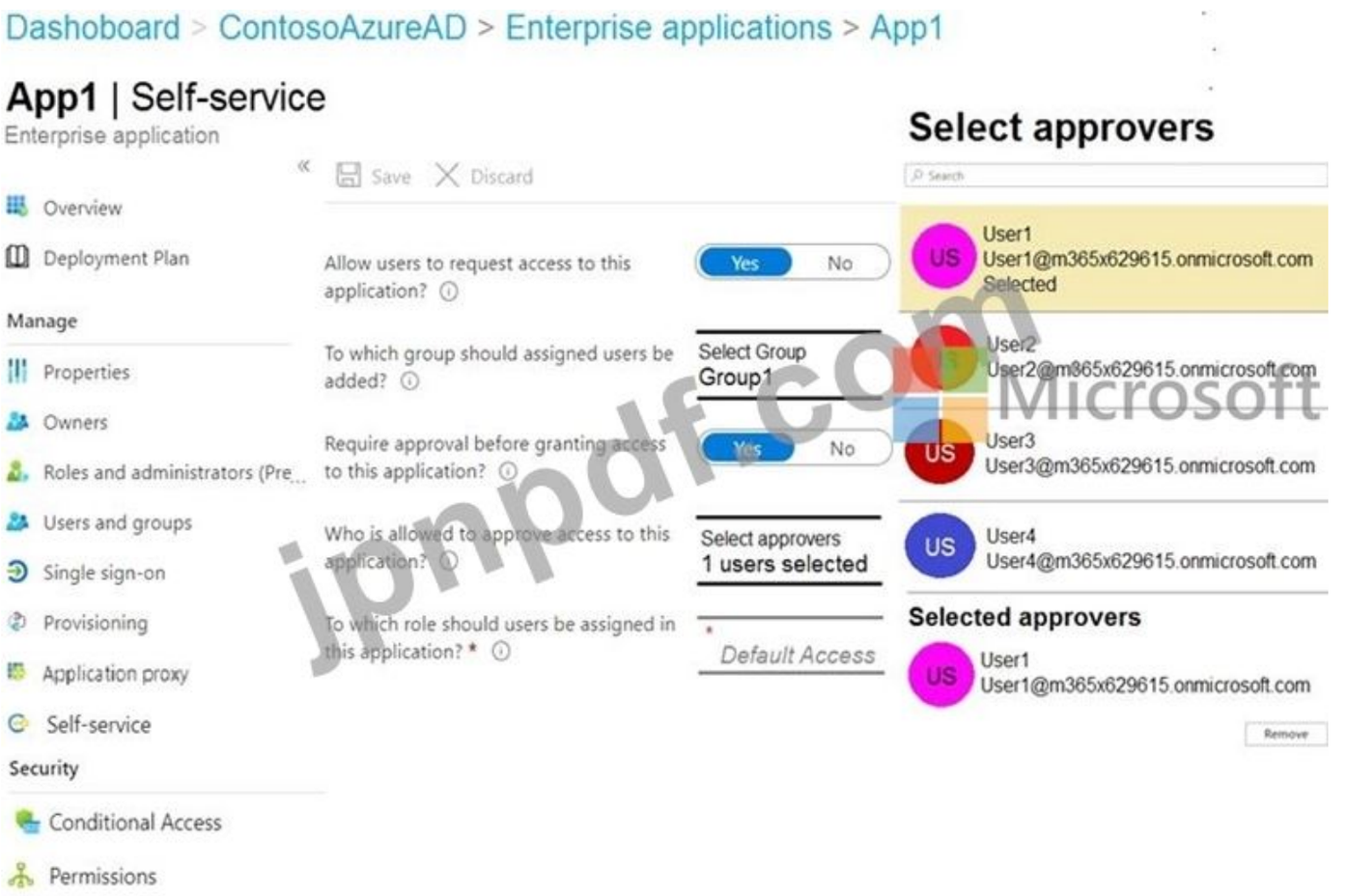
最新問題**: 38**
Azure Active Directory (Azure AD)テナントがあります。
リスク検出レポートを開きます。
どのリスク検出タイプがユーザーリスクとして分類されますか？
A. 不可能な旅行
B. 匿名IPアドレス
C. 非定型旅行
D. 漏洩したクレデンシャル
Answer: D (メーッセージを残す**)**
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

最新問題**: 39**
Group1の展示に示されているように、Group1という名前のグループを含むMicrosoft365テナントがあります。 [グループ1]タブをクリックします。）

App1プロパティの展示に示されているように、App1という名前のエンタープライズアプリケーションを作成します。 [App1のプロパティ]タブをクリックします。）



App1セルフサービスの展示に示されているように、App1のセルフサービスを構成します。 App1セルフサービス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。

Answer:

最新問題: **40**
contoso.comという名前のAzureActive Directory（Azure AD）テナントがあり、Azure AD IdentityProtectionポリシーが適用されています。
Azure Sentinelインスタンスを作成し、Azure ActiveDirectoryコネクタを構成します。
Azure Sentinelが、Azure AD IdentityProtectionによって発生したリスクアラートに基づいてインシデントを生成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. AzureSentinelデータコネクタを追加します。
B. Azure AD IdentityProtectionで通知設定を構成します。
C. AzureSentinelプレイブックを作成します。
D. AzureADの診断設定を変更します。
Answer: (解答を表示する**)**
Reference:
https://docs.microsoft.com/en-us/azure/sentinel/connect-azure-ad-identity-protection

最新問題: **41**
Microsoft365テナントがあります。
Azure Monitorを使用して、Azure Active Directory（Azure AD）監査ログ情報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. AzureAの診断設定を変更します
C. Get-AzureADAuditDirectoryLogsコマンドレットを実行します。
D. AzureADワークブックを作成します。
Answer: C (メーッセージを残す**)**

最新問題: **42**

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 ADから、管理者の役割でInsightsの割り当てを作成します。
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**)**

最新問題**: 43**
Microsoft365テナントがあります。
Azure Active Directory（Azure AD）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	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

AzureADの場合。Appl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追加します。
App1に割り当てることができるグループはどれですか？
A. Group1およびGroup
B. グループ2のみ
C. グループ1のみ
D. Group1およびGroup4
E. グループ3のみ
Answer: (解答を表示する**)**