Microsoft.SC-300.v2026-05-11.q345

試験コード:	SC-300
試験名称:	Microsoft Identity and Access Administrator
認定資格:	Microsoft
無料問題数:	345
バージョン:	v2026-05-11
アクセス数:	258
ページビュー数:	3450
https://www.jpnpdf.com/Microsoft.SC-300.v2026-05-11.q345-mondaishu.html	

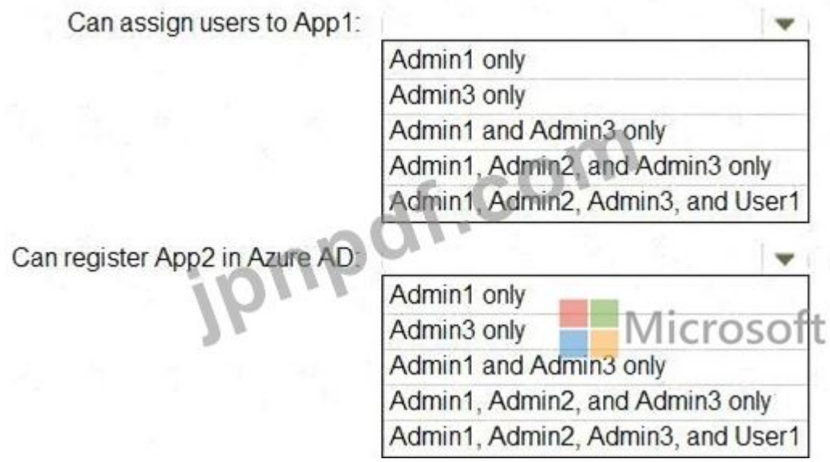
最新問題: **1**
既定のドメイン名 contosso.com を使用するように新しい Microsoft 36S テナントを構成します。
条件付きアクセス ポリシーを使用して、Microsoft 365 リソースへのアクセスを制御できることを確認する必要があります。
まず何をすべきでしょうか?
A. ユーザーの同意設定を無効にします。
B. セキュリティのデフォルトを無効にします。
C. 多要素認証 (MI A) 登録ポリシー 1 を構成します。
D. Windows Server Active Directory のパスワード保護を構成します。
Answer: B (メーッセージを残す**)**
Microsoft SC-300: Microsoft Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール 条件付きアクセス ポリシーの計画と実装」によると、条件付きアクセス ポリシーを有効化またはカスタマイズするには、Azure AD のセキュリティの既定値を無効にする必要があります。
セキュリティの既定値は、すべてのユーザーへのMFAの適用やレガシー認証のブロックなど、基本的なレベルの保護を提供します。ただし、セキュリティの既定値を有効にすると、サインインリスクとアクセス制御の両方を管理するため、カスタムの条件付きアクセスポリシーを作成することはできません。
Microsoft のドキュメントより:
条件付きアクセス ポリシーを使用するには、セキュリティの既定値を無効にする必要があります。条件付きアクセス ポリシーは、セキュリティの既定値よりも細分性と柔軟性に優れています。」したがって、条件付きアクセスを通じて Microsoft 365 リソースへのアクセスを制御する前に、まず Azure AD テナントでセキュリティの既定値を無効にする必要があります。

最新問題: **2**
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

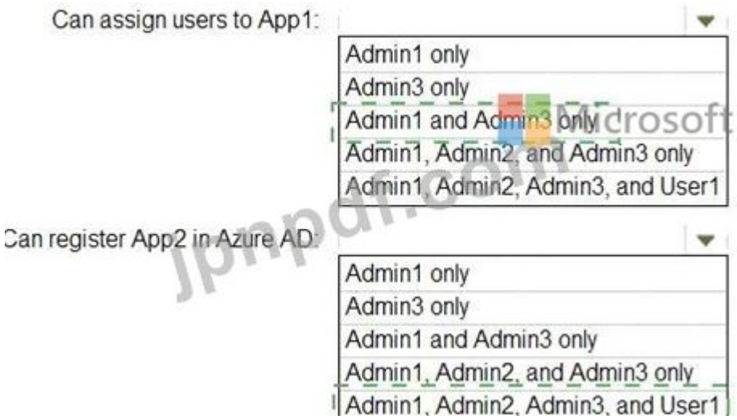
Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

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Azure ADに登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD 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。

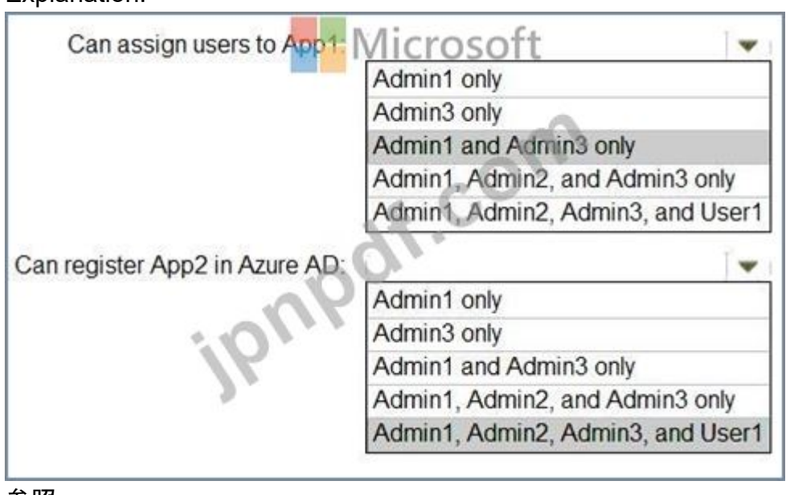
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

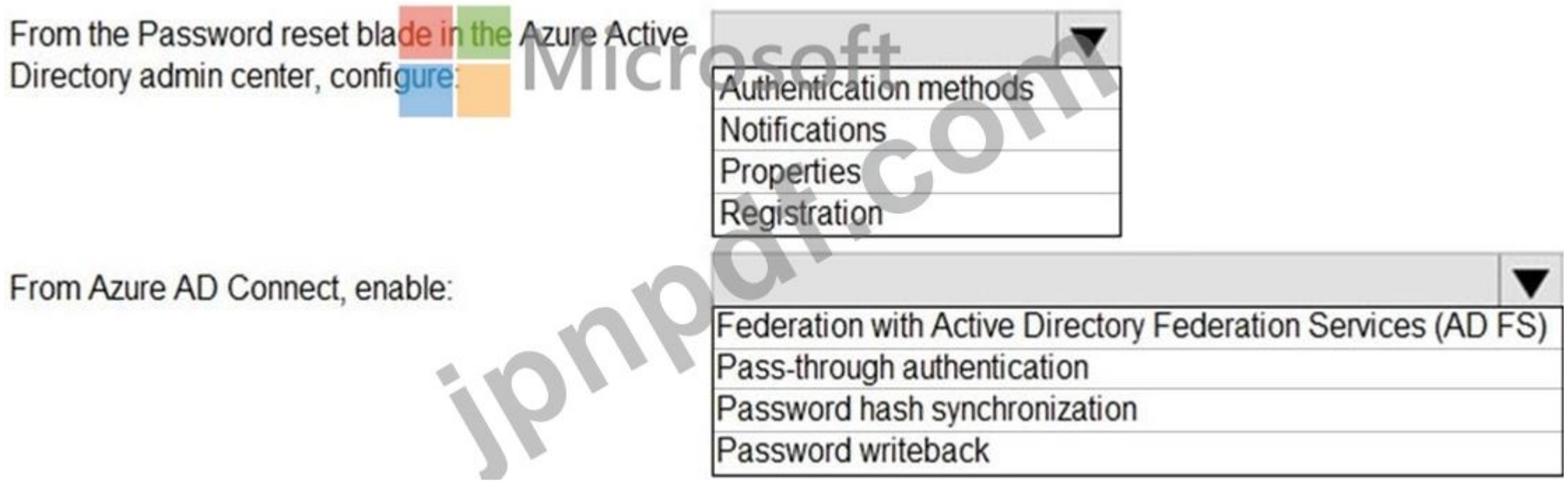


参照：

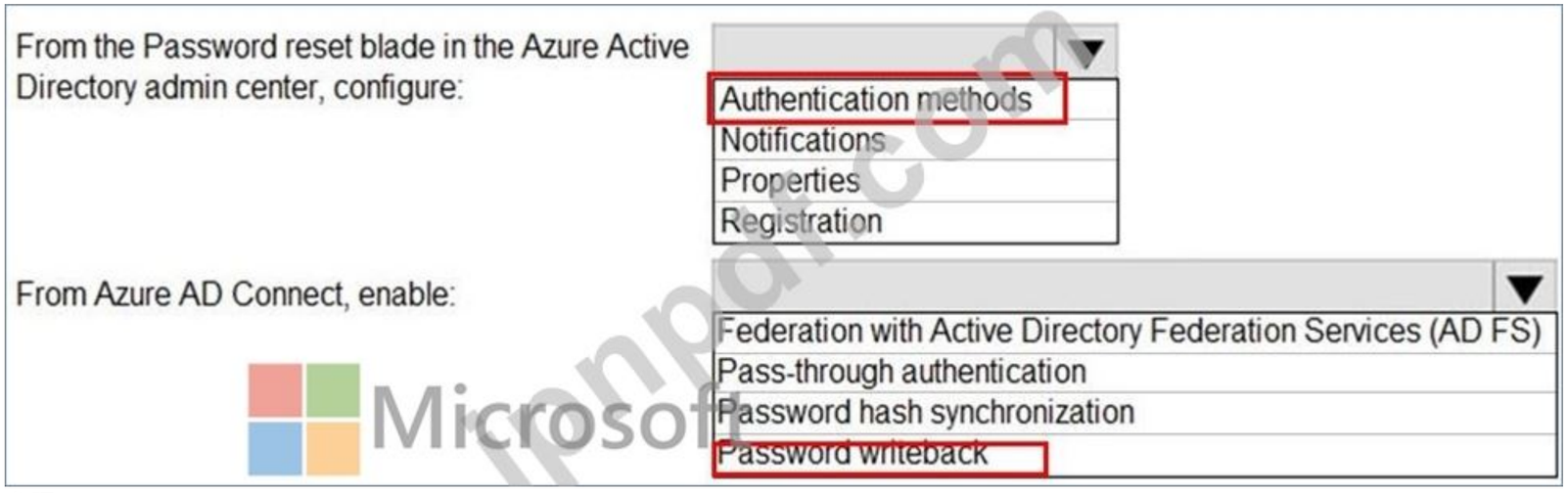
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

最新問題**: 3**
Microsoft 365 テナントと、adatum.com という名前の Active Directory ドメインがあります。
簡単設定を使用して Azure AD Connect をデプロイします。
次の要件を満たすようにセルフサービス パスワード リセット (SSPR) を構成する必要があります。
ユーザーがパスワードをリセットする場合、モバイル アプリの通知に応答するか、事前定義された 3 つのセキュリティの質問に答えるように要求される必要があります。
パスワードがリセットされた場所に関係なく、テナントとドメイン間でパスワードを同期する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題: **4**
Microsoft 365 E5 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。
どの 4 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、適切なアクションをアクション 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 - Azure Active Directory (Azure AD) で App1 を公開します。
2 - Microsoft Cloud App Security から、App1 の接続アプリの設定を変更します。
3 - Microsoft Cloud App Security からセッション ポリシーを作成します。
4 - セッション制御が構成された条件付きアクセス ポリシーを作成します。
参照：
https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app
https://docs.microsoft.com/ja-jp/cloud-app-security/session-policy-aad

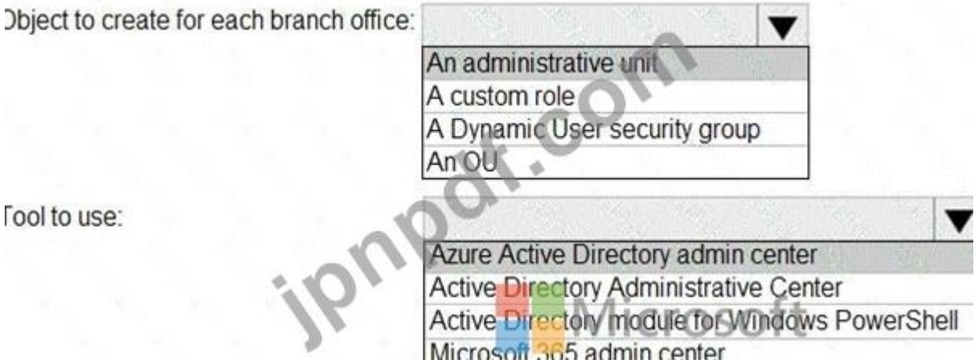
最新問題: **5**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明
テキストの説明は自動的に生成されます



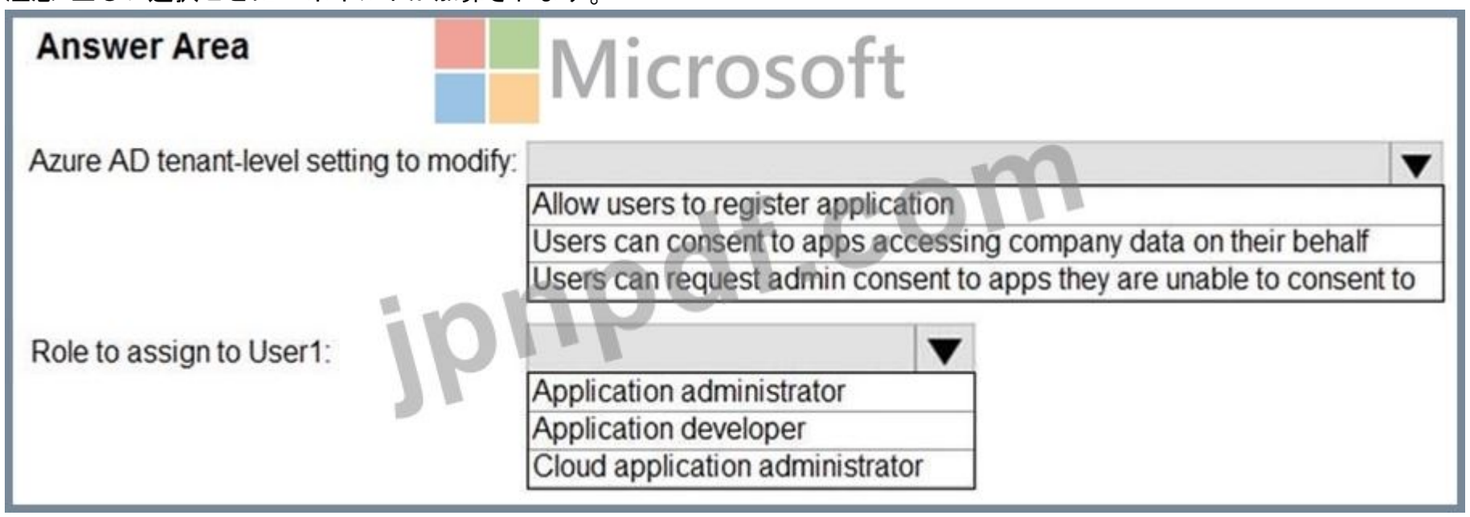
最新問題: **6**
ケーススタディ2 - Litware, Inc.
概要
Litware, Inc. は、Fabrikam, Inc. という子会社を持つ製薬会社です。
Litware はボストンとシアトルにオフィスを構えていますが、従業員は全米各地にいます。
従業員は、VPN 接続を使用してどちらかのオフィスにリモートで接続します。
既存の環境。環境を特定する
ネットワークには、litware.com という名前の Active Directory フォレストが含まれており、これは litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパススルー認証を使用し、パスワード ハッシュ同期は無効になっています。
Litware.com には、すべてのアプリケーション開発を監督する User1 というユーザーがいます。

Litware は Azure AD アプリケーション プロキシを実装します。
Fabrikam には fabrikam.com という Azure AD テナントがあります。Fabrikam のユーザーは、litware.com テナントのゲストアカウントを使用して litware.com のリソースにアクセスします。
既存環境。クラウド環境
Litware の全ユーザーは Microsoft 365 Enterprise E5 ライセンスを保有しています。Microsoft Cloud App Security に組み込まれている異常検出ポリシーはすべて有効になっています。
Litware には、litware.com Azure AD テナントに関連付けられた Azure サブスクリプションがあります。このサブスクリプションには、Azure Active Directory コネクタと Office 365 コネクタを使用する Azure Sentinel インスタンスが含まれています。Azure Sentinel は現在、Azure AD サインインログと監査ログを収集しています。
既存の環境。オンプレミス環境
オンプレミス ネットワークには、次の表に示すサーバーが含まれています。

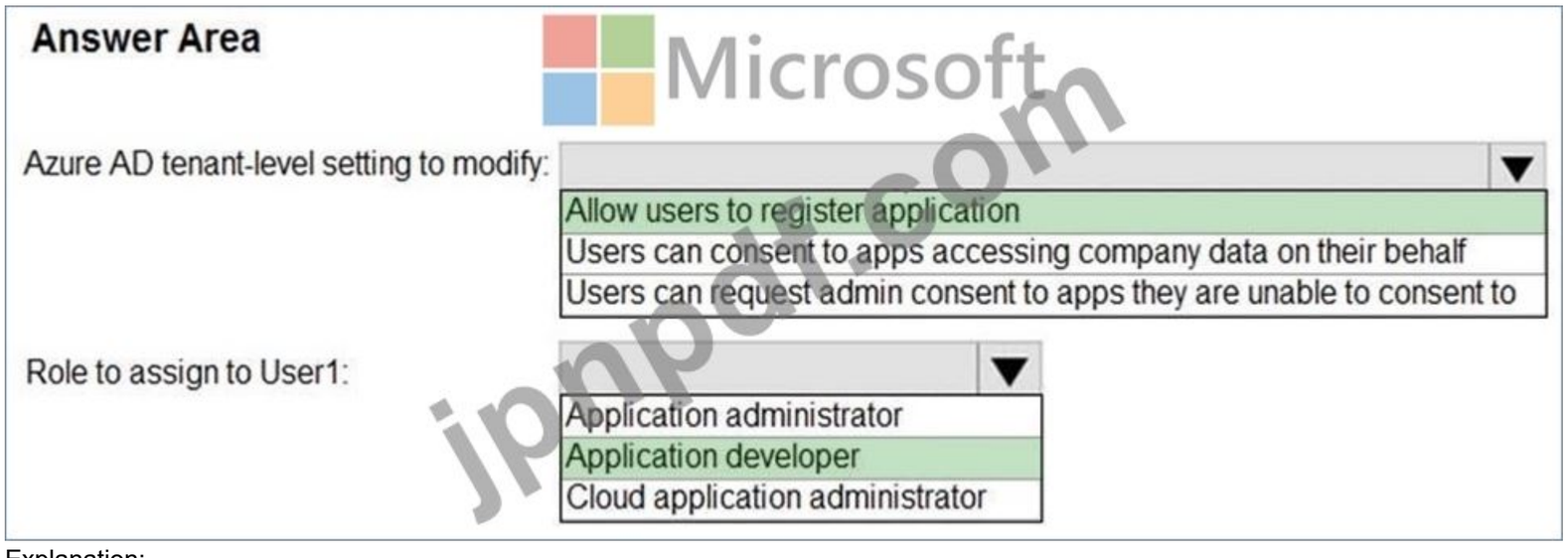
Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Litwareの両オフィスはインターネットに直接接続しています。両オフィスは、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのすべてのドメインコントローラーは、インターネットへのアクセスをブロックされています。
要件。委任要件
Litware では、次の委任要件が特定されています。
* Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
* 権限のないユーザーが litware.com Azure AD テナントにアプリケーションを登録できないようにします。
* アイデンティティ ガバナンスにはカスタム カタログとカスタム プログラムを使用します。
* User1 が Azure AD でエンタープライズ アプリケーションを作成できることを確認します。
* 最小権限の原則を使用します。
要件。ライセンス要件
Litware は最近、litware.com Active Directory フォレストに LWLicenses というカスタム ユーザー属性を追加しました。Litware は、LWLicenses 属性の値を変更することで、Azure AD ライセンスの割り当てを管理したいと考えています。LWLicenses に適切な値を持つユーザーは、適切なライセンスが割り当てられている Microsoft 365 グループに自動的に追加される必要があります。
要件。管理要件
Litware では、Litware のすべての Azure AD ユーザー アカウントを含み、すべての Azure AD ゲスト アカウントを除外する、LWGroup1 という名前のグループを作成したいと考えています。
要件。認証要件
Litware では、次の認証要件が識別されます。
* すべての Litware ユーザーに対して多要素認証 (MFA) を実装します。
* Litware のボストン オフィスから Azure AD への認証に MFA を使用するユーザーを除外します。
* litware.com フォレストの禁止パスワード リストを実装します。
* オンプレミスのアプリケーションにアクセスするときに MFA を適用します。
* 外部に漏洩した資格情報を自動的に検出し、修正します。
要件。アクセス要件
Litware では、次のアクセス要件が特定されています。
* 条件付きアクセス ポリシーを使用して、すべての Azure リソースと Azure AD アプリケーションへのすべてのアクセスを制御します。
* Microsoft SharePoint Online のセッション制御を備えた条件付きアクセス ポリシーを実装します。

* Azure AD のアクセス レビューを使用して、アプリケーションへの特権アクセスを制御します。
要件。監視要件
Litware は、Azure Sentinel の Fusion ルールを使用して、疑わしい Azure AD サインインとそれに続く異常な Microsoft Office 365 アクティビティの組み合わせを含む多段階の攻撃を検出したいと考えています。
ホットスポットに関する質問
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

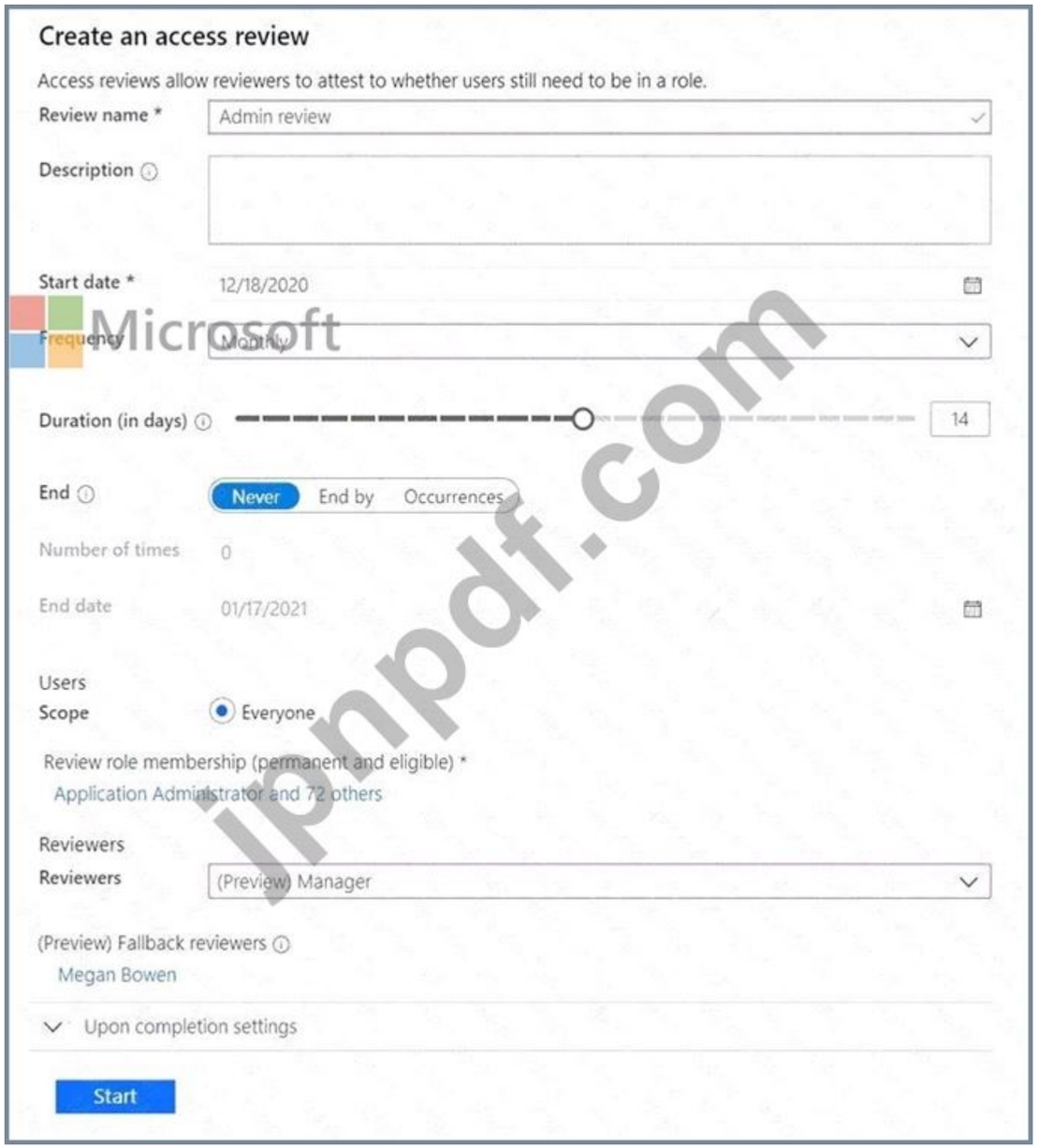


Answer:



Explanation:
1: 委任の要件には 「ユーザーがアプリケーションを登録できないようにする」と明記されています
2: ユーザー1は、アプリ開発者が 「最小権限の原則」を使用してテナントにアプリを登録する必要があります。
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

最新問題: **7**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントがあります。
100 人の IT 管理者が 10 の部門に分かれて所属しています。
展示に示されているアクセス 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 リクエストは Megan Bowen 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れ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担当者として追加します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: (解答を表示する**)**
展示と SC-300 学習ガイド (アクセス レビュー セクション) によると、アクセス レビューは、レビュー担当者の種類が (プレビュー) マネージャーに設定され、Megan Bowen がフォールバック レビュー担当者として構成されています。
Azure AD アクセスレビューでは、レビュー担当者の種類として 「マネージャー」が選択されている場合、各ユーザーの Azure AD で定義されたマネージャーがアクセスレビュー担当者として自動的に割り当てられます。ただし、ユーザーに Azure AD でマネージャーが割り当てられていない場合は、レビュータスクはデフォルトでフォールバックレビュー担当者 (この場合は Megan Bowen) に割り当てられます。
したがって、すべてのアクセス レビュー要求が Megan Bowen に送信される場合は、テナント内のユーザーに Azure AD ユーザー属性で適切に割り当てられたマネージャーが存在しないことを意味します。
部門マネージャーをフォールバック レビュー担当者として追加しても、フォールバック レビュー担当者は部門に基づいてではなく、マネージャーのいないユーザーのレビューのみを受信するため、問題は解決されません。
Microsoft のドキュメントには次のように記載されています。
レビュー担当者として 「マネージャー」を選択した場合、Azure AD のマネージャープロパティが使用されます。ユーザーにマネージャーがいない場合は、フォールバックレビュー担当者が使用されます。マネージャーをフォールバックレビュー担当者として追加しても、部門に基づいてレビューが割り当てられることはありません。

最新問題: 8
ホットスポットに関する質問
あなたの会社には、contoso.com という Azure Active Directory (Azure AD) テナントがあり、Fabrikam, Inc. というビジネス パートナーがいます。
Fabrikam は Azure AD を使用しており、fabrikam.com と litwareinc.com という 2 つの検証済みドメイン名を保有しています。どちらのドメイン名も Fabrikam のメール アドレスに使用されています。
Fabrikam のユーザーのみがアクセスできる、package1 という名前のアクセス パッケージを作成する予定です。
Fabrikam の接続された組織を作成します。
package1 に fabrikam.com の電子メール アドレスを持つユーザーのみがアクセスできるようにする必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

jpnpdf.com Microsoft

Answer:

Answer Area



To allow access for users who have fabrikam.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

To block access for users who have litwareinc.com email addresses, configure:

- An access package assignment in Identity Governance
- An access package policy in Identity Governance
- A conditional access policy in Azure AD
- The External collaboration settings in Azure AD

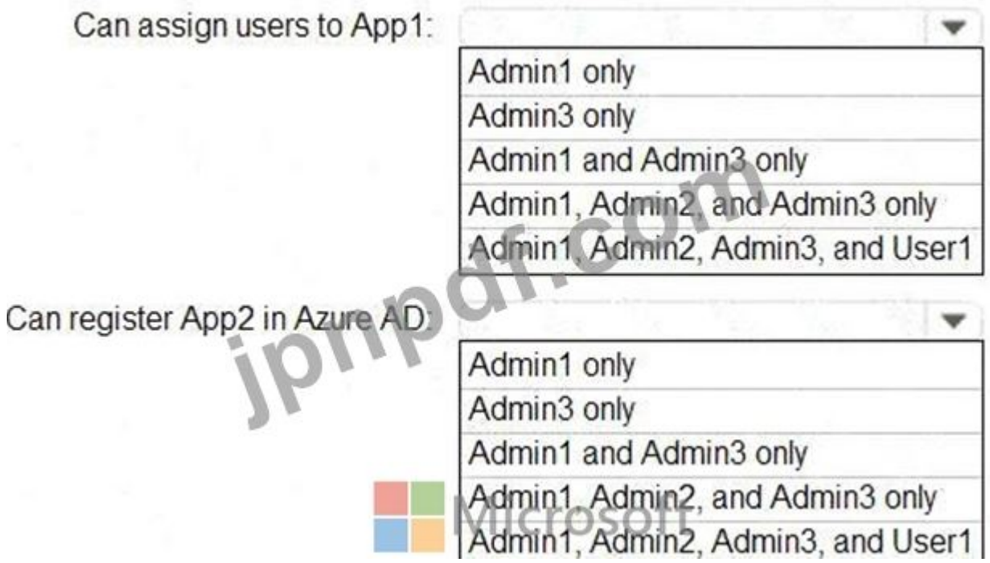
jpnpdf.com

Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-request-policy
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create

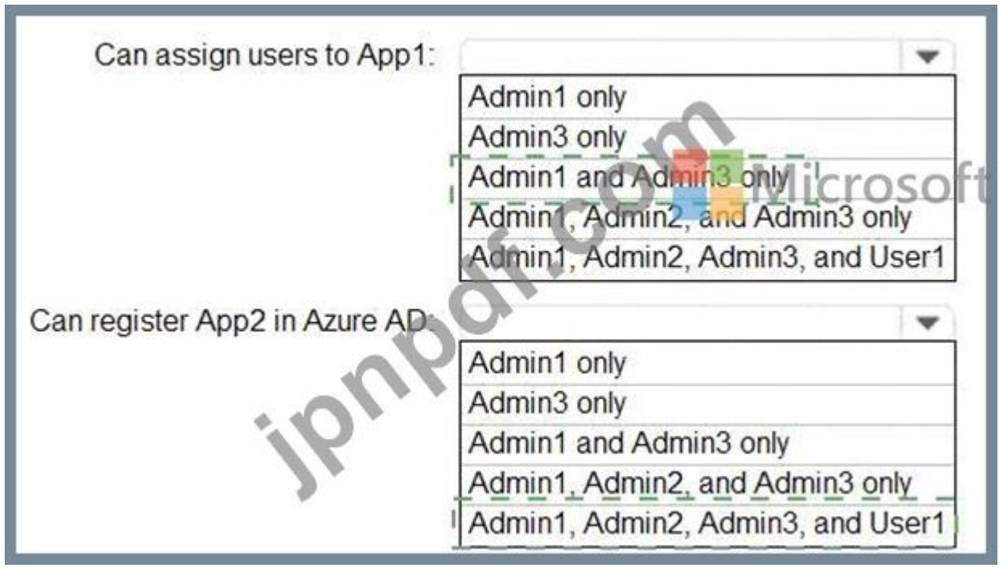
最新問題: 9
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

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

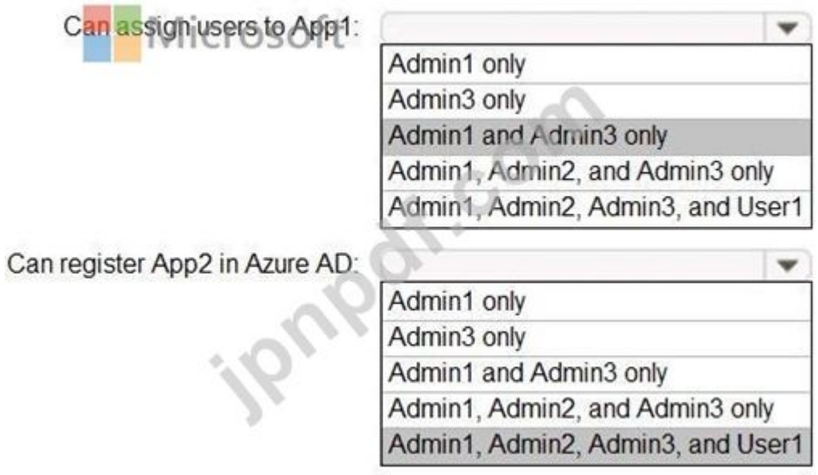
App1とApp2という2つのクラウドアプリを購入します。グローバル管理者はApp1をAzure ADに登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD に App2 を登録できるユーザーを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



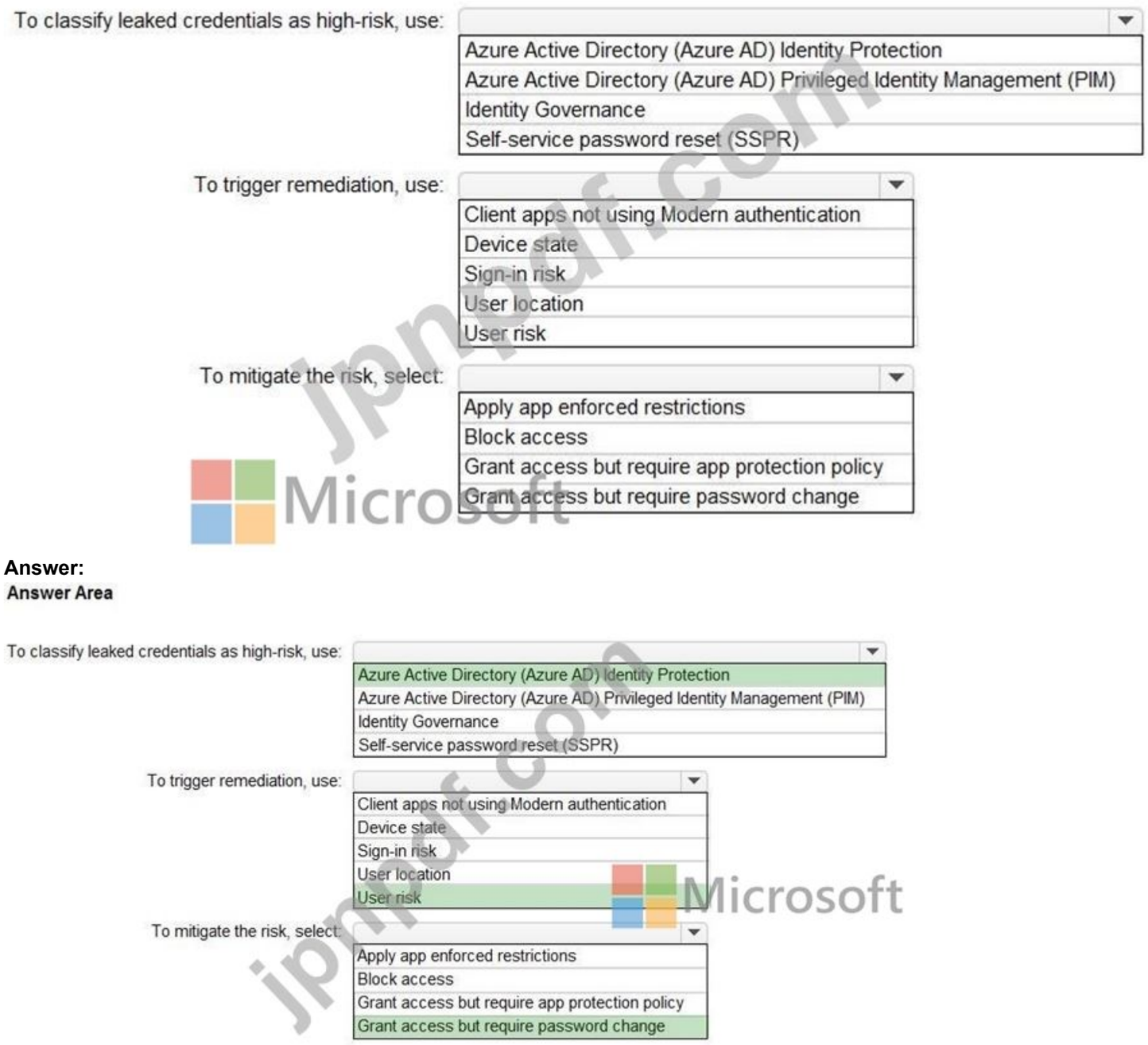
Explanation:



参照：
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**: 10**
ホットスポットに関する質問
Microsoft 365 テナントがあります。
認証情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。
- 漏洩の疑いのあるユーザーによるサインインを特定する
資格。
- サインインを高リスクイベントとしてフラグ付けします。
- リスクを軽減するための制御を直ちに実施する。
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ます。
何を使うべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:

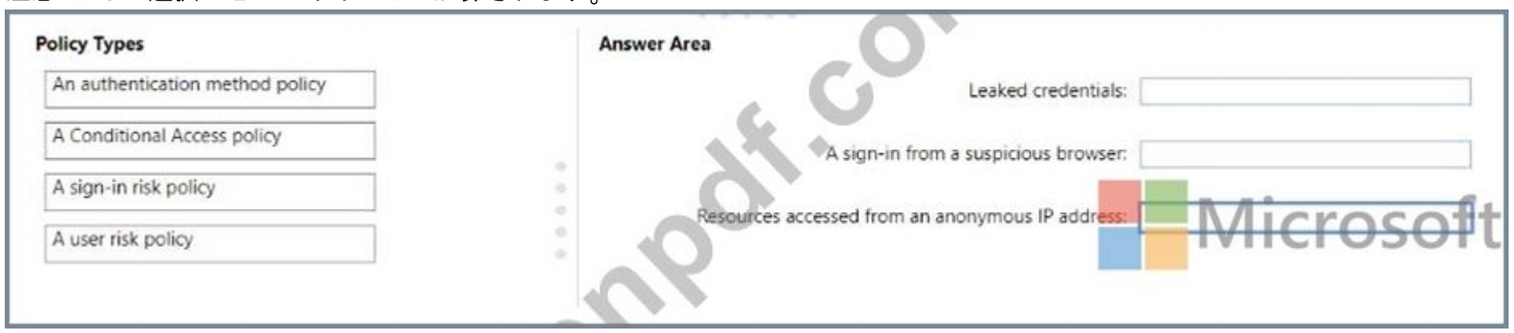
Answer Area

Explanation:

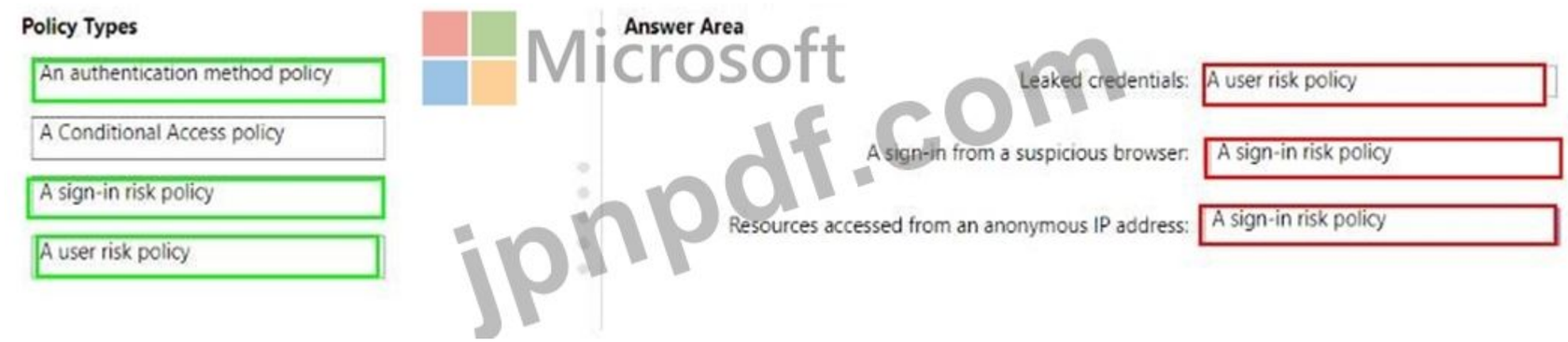
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

最新問題: 11

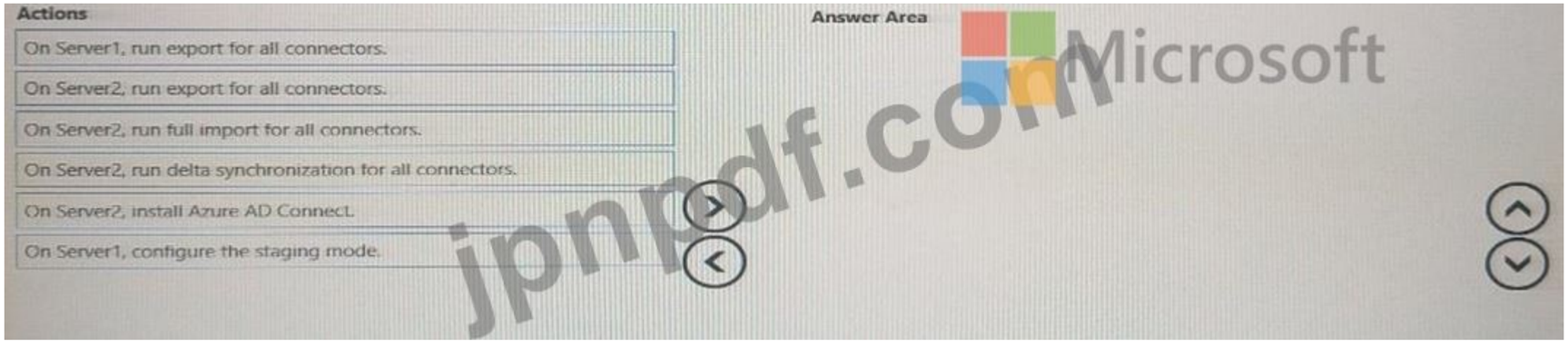
最近のセキュリティ インシデントの問題を解決する必要があります。
各インシデントに対してどのような設定を行うべきでしょうか？適切なポリシータイプを適切な問題にドラッグしてください。各ポリシータイプは、1回、複数回、または全く使用されない場合があります。
コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: 12
ネットワークには、Azure AD Connect を使用して contoso.com という名前の Azure Active Directory (Azure AD) テナントにリンクされている contoso.com という名前の Active Directory フォレストが含まれています。
Attire AD Connect は、Server 1 という名前のサーバーにインストールされています。
Windows Server 2019 を実行する Server? という名前の新しいサーバーを展開します。
Azure AD Connect 用のフェールオーバーサーバーを実装する必要があります。このソリューションでは、Server1 に障害が発生した場合にフェールオーバーにかかる時間を最小限に抑える必要があります。
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 リストから回答領域に移動し、正しい順序に並べます。

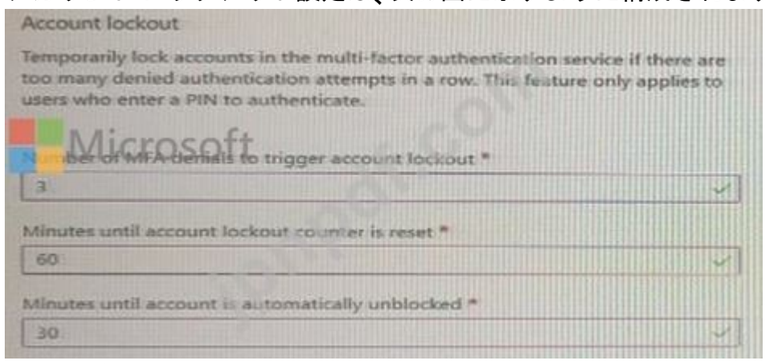


Answer:

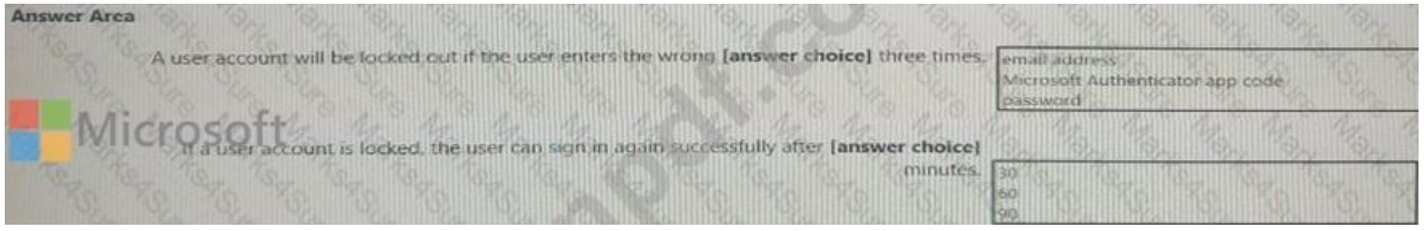


1 - Server2 で、すべてのコネクタに対してエクスポートを実行します。
2 - Server2 で、すべてのコネクタのデルタ同期を実行します。
3 - Server1 で、すべてのコネクタのエクスポートを実行します。

最新問題**: 13**
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 ロックアウト設定は、次の図に示すように構成されます。



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

アプリコード

60

https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#account- ロックアウト

最新問題: 14

User1 という名前のユーザーを含む contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

User1 には次の表に示すデバイスがあります。

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

2020 年 11 月 5 日に、contoso.com で次の設定の利用規約を作成して適用します。

* 名前: 用語1
* 表示名: Contoso 利用規約
* ユーザーに利用規約の拡張を要求する: オン
* すべてのデバイスでユーザーの同意を求める: オン
* 同意の有効期限: オン
* 有効期限 :2020年12月10日
* 頻度: 毎月

2020年11月15日に、ユーザー1はデバイス3で利用規約1に同意します。

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 ポイントが加算されます。



Answer:



説明



最新問題: **15**

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ストレージサービス暗号化

B. ユーザー アカウントと Azure Key Vault

C. ユーザー割り当てマネージド ID と Azure Key Vault
D. 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
Answer: C (メーッセージを残す)
SC-300資料では、Azureリソースのマネージドidは、Microsoft Entra IDで自動的に管理されるIDを提供し、アプリはこれを使用してトークンを要求できるため、 資格情報の管理が不要」になり、コード内のシークレットを回避できると説明されています。また、シークレットの推奨ストアはAzure Key Vaultであり、アプリは埋め込みキーではなくマネージドIDからEntraトークンを提示してKey Vaultにアクセスする必要があるとされています。複数の仮想マシンで同じワークロードを実行するシナリオでは、このガイダンスではユーザー割り当てマネージドIDが強調されています。これはスタンドアロンIDとして作成され、『つ以上のインスタンスに割り当てることができる」ため、共有IDへのKey Vaultアクセスを一度許可すれば、すべてのVMにアタッチできます。これにより、システム割り当てID（各VMライフサイクルに1対1で関連付けられている）と比較して、管理が最小限に抑えられます。このアプローチでは、VMはユーザー割り当てマネージドIDを介してEntraトークンを取得し、Azureリソースを呼び出し、Key Vaultで認証します。その後、アプリケーションは実行時にKey Vaultからサードパーティ APIシークレットを取得します。これにより、すべての要件が満たされます。シークレットは安全に保存され、コード内に資格情報は存在せず、VM は Entra 認証を使用し、VM フリート全体で単一の ID を再利用することで運用上の労力が削減されます。

最新問題**: 16**
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

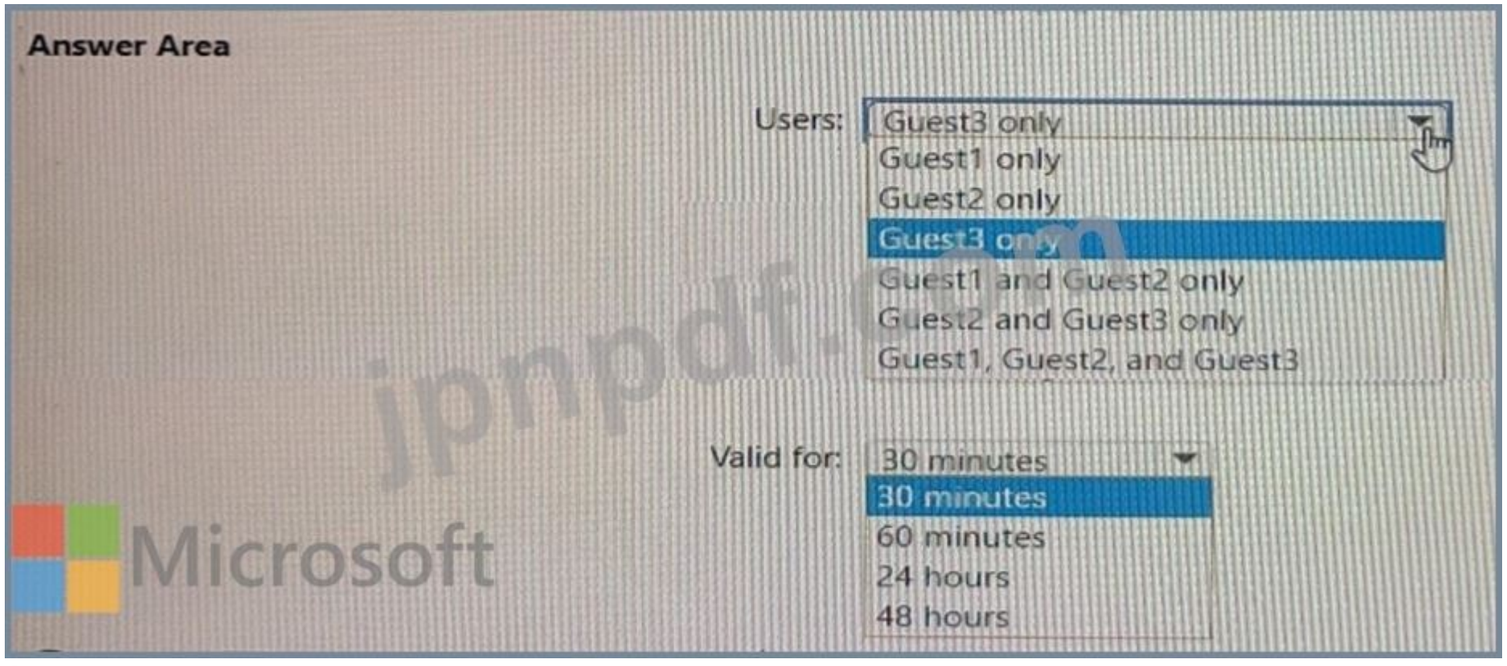
Azure ポータルを使用して、Role3 という名前のカスタム Azure サブスクリプション ロールを作成する必要があります。
Role3 は既存のロールのベースライン権限を使用します。
Role3 を作成するためにどのロールを複製できますか?
A. ロール2のみ
B. 組み込みの Azure サブスクリプション ロールのみ
C. 組み込みの Azure サブスクリプション ロールと Role2 のみ
D. 組み込みの Azure サブスクリプション ロールと組み込みの Azure AD ロールのみ
E. Role1、Role2 組み込み Azure サブスクリプション ロール、および組み込み Azure AD ロール
Answer: C (メーッセージを残す)
https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#clone-a- role

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

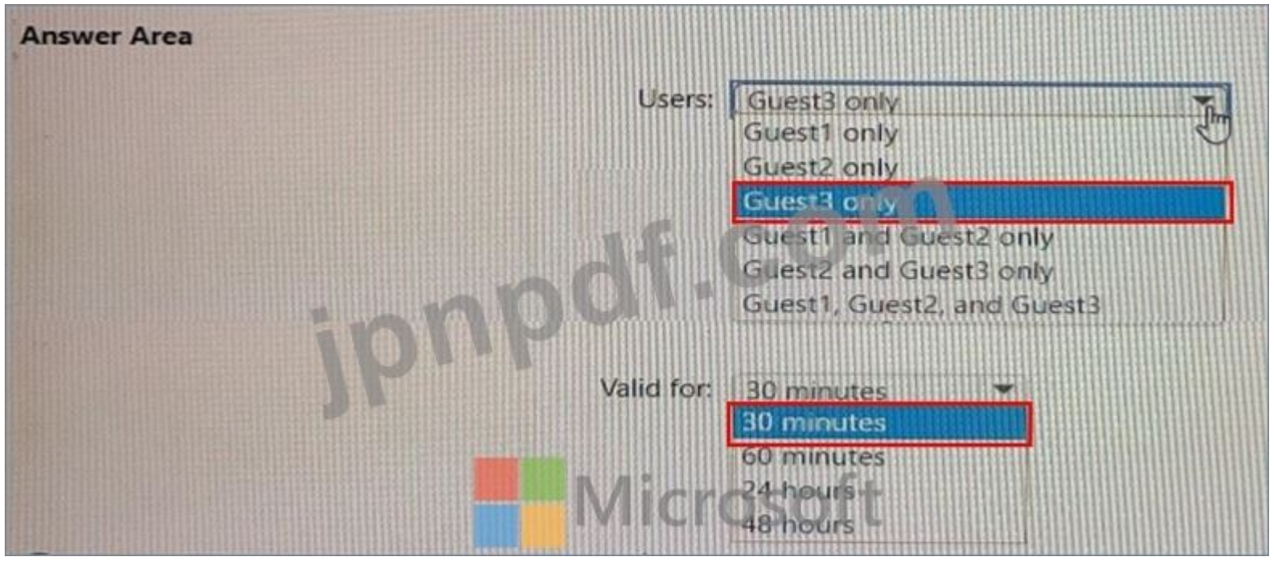
最新問題**: 17**
contoso.com という名前の Azure AD テナントがあり、ゲスト用のワンタイム パスコードを電子メールで送信することが [はい] に設定されています。
次の表に示すゲスト ユーザーを招待します。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

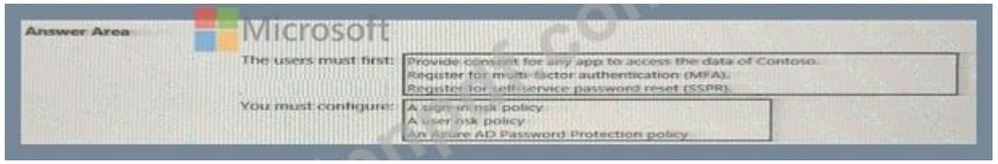
ワンタイム パスコードを受け取るユーザーは誰ですか? また、パスコードの有効期間はどのくらいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **18**
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **19**
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確実に行われるようにする必要があります。どのような設定を行い、どのようなツールを使用すればよいでしょうか？回答するには、回答欄から適切なオプションを選択してください。注：各選択肢は1ポイントです。
Answer Area



Answer:

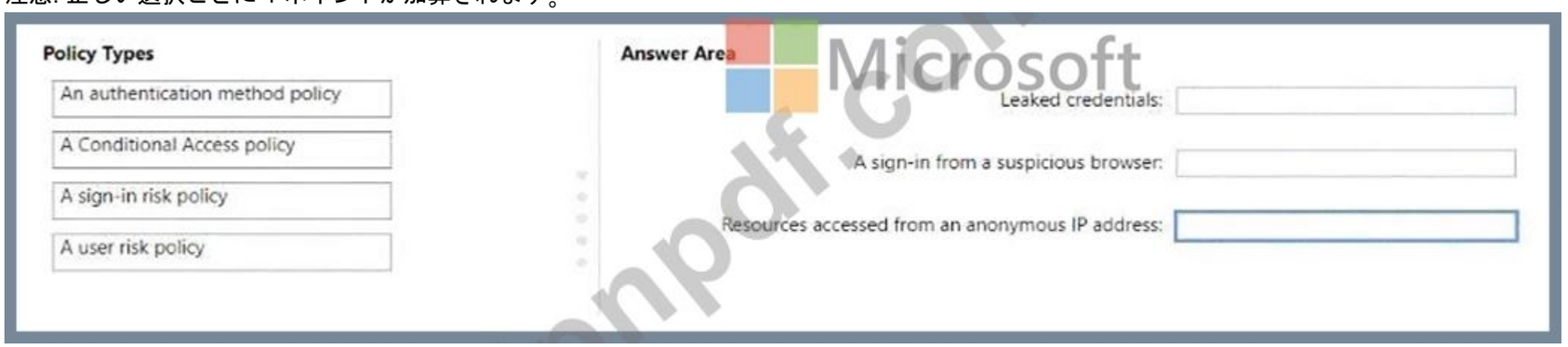


Explanation:



Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール 「Microsoft Entra Connect の実装と管理」によれば、組織がオンプレミスの Active Directory ドメイン サービス (AD DS) 環境に対して常に直接ユーザー パスワードを検証するための認証を必要とする場合、正しい構成はパススルー認証 (PTA) です。
理由は次のとおりです。
* パススルー認証 (PTA) により、ユーザーが Microsoft Entra ID (旧 Azure AD) にサインインしようとする際に、クラウドで資格情報が検証されることがなくなります。代わりに、認証要求はオンプレミスの認証エージェントに安全に渡され、オンプレミスの AD DS ドメイン コントローラーに対して資格情報がリアルタイムで検証されます。
* この構成により、オンプレミスのアカウントの状態が即座に反映されます。アカウントが無効化、ロックされたり、パスワードが変更されたりすると、それらの変更はクラウド認証にも即座に反映されます。
PTA を構成するには、オンプレミスのディレクトリを Microsoft Entra ID にリンクするハイブリッド ID 同期ツールである Microsoft Entra Connect を使用する必要があります。Entra Connect のセットアップ時に、管理者はサインイン方法としてパスワードハッシュ同期、パススルー認証、フェデレーションのいずれかを選択できます。
Microsoft のドキュメントには次のように明記されています。
「パススルー認証により、ユーザーはオンプレミスとクラウドベースの両方のアプリケーションに同じパスワードでサインインできます。認証はオンプレミスの Active Directory に対して行われます。」したがって、認証では常にオンプレミスの AD DS ドメインに対してパスワードを検証するという要件を満たすには、次の操作を行います。

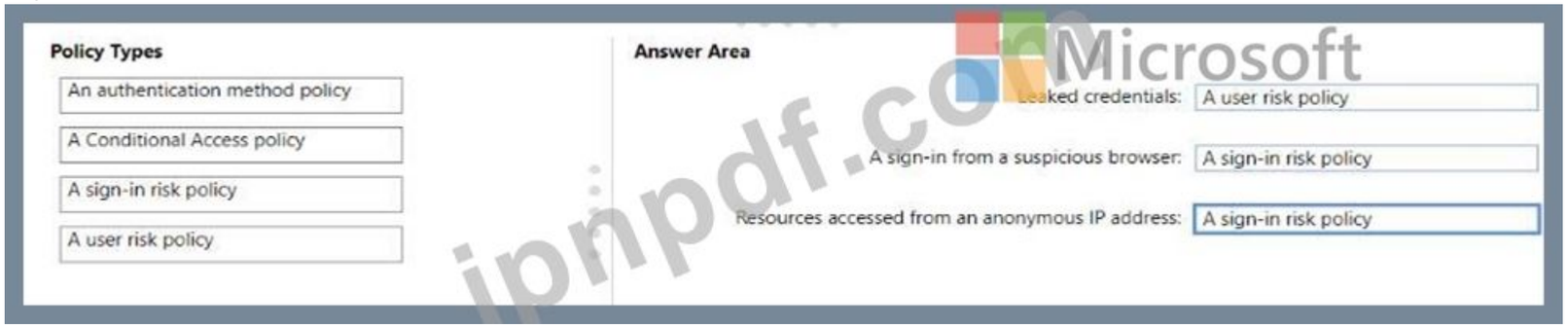
最新問題: 20
最近のセキュリティ インシデントの問題を解決する必要があります。
各インシデントに対してどのような設定を行うべきでしょうか？適切なポリシータイプを適切な問題にドラッグしてください。各ポリシータイプは、1回、複数回、または全く使用されない場合があります。
コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: **21**
A Datumユーザー向けのライセンスを特定する必要があります。ソリューションには技術要件が必要です。
どのようなタイプのオブジェクトを作成する必要がありますか?
A. Dynamoユーザーセキュリティグループ
B. 配布グループ
C. あなたの中に
D. 行政単位
Answer: D (メーッセージを残す**)**

最新問題: **22**
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
ユーザー1がグループのアクセスレビューを作成でき、ユーザー2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、最小権限の原則を適用する必要があります。
各ユーザーにどのロールを割り当てるべきですか？ 回答するには、適切なロールを正しいユーザーにドラッグしてください。各ロールは1回、複数回、または全く使用されない場合があります。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：正しい選択ごとに1ポイント獲得できます。



Answer:



最新問題: **23**
タスク2
Salesforce アプリへのアクセス権を持つゲストユーザーをレビューするプロセスを実装する必要があります。レビューは、以下の要件を満たす必要があります。
* レビューは毎月行う必要があります。
* 各ゲスト ユーザーの管理者はアクセスを確認する必要があります。
* 5 日以内にレビューが完了しない場合は、アクセスを削除する必要があります。
* ゲスト ユーザーにマネージャーがいない場合は、Megan Bowen がアクセスを確認する必要があります。
Answer:
完全なステップバイステップの解決策については説明を参照してください
Explanation:
Salesforceアプリへのゲストユーザーのアクセスを特定の要件に基づいてレビューするプロセスを実装するには、Microsoft EntraのIdentity Governanceアクセスレビュー機能を使用できます。手順は以下のとおりです。
適切な役割を割り当てます。
グローバル管理者、ユーザー管理者、または Identity Governance 管理者のいずれかのロールを持っていることを確認します1。
Identity Governance に移動します。
Microsoft Entra 管理センターにサインインします。
[アイデンティティ ガバナンス] > [アクセス レビュー] に移動します1。
新しいアクセスレビューを作成します。
[新しいアクセス レビュー]を選択します。
ゲスト ユーザーのアクセスを確認するには、Salesforce アプリを選択します1。
レビュー設定を構成します。
レビューの頻度を月次に設定します。
レビュー期間の期間を 5 日間に定義します1。
レビュー担当者を決定します。
各ゲスト ユーザーのマネージャーをレビュー担当者として割り当てます。
ゲスト ユーザーにマネージャーがいない場合は、Megan Bowen をレビュー担当者として割り当てます1。
削除プロセスを自動化します。
指定された期間内にレビューが完了しない場合にアクセスを自動的に削除するように設定を構成します1。

コンプライアンスの監視と強制:
アクセス レビューの結果を定期的に確認し、レビュー ポリシー 1 に準拠していることを確認します。
プロセスを伝える:
すべての関係者に新しいレビュー プロセスについて通知し、レビューを完了する方法についてのガイダンスを提供します。
これらの手順に従うことで、ゲスト ユーザーの Salesforce アプリへのアクセスが毎月レビューされ、マネージャがレビューの責任を負い、レビューが期限内に完了しない場合はアクセスが削除されるようにすることができます。

最新問題: **24**
VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。VM1 の構成は次のとおりです。
* プライベートIPアドレス: 172.16.1.5
* パブリックIPアドレス 10fl.143.16U5
* システム割り当てマネージドIDのステータス: オン
VM1 に App1 という名前のアプリをインストールします。
マネージドIDのアプリ専用アクセストークンをリクエストするようにApp1を設定する必要があります。リクエストにApp1が使用するIPアドレスはどれですか？
A. 169.254.169.254
B. 108.143.161.25
C. 127.0.0.1
D. 172.1615
Answer: (解答を表示する**)**

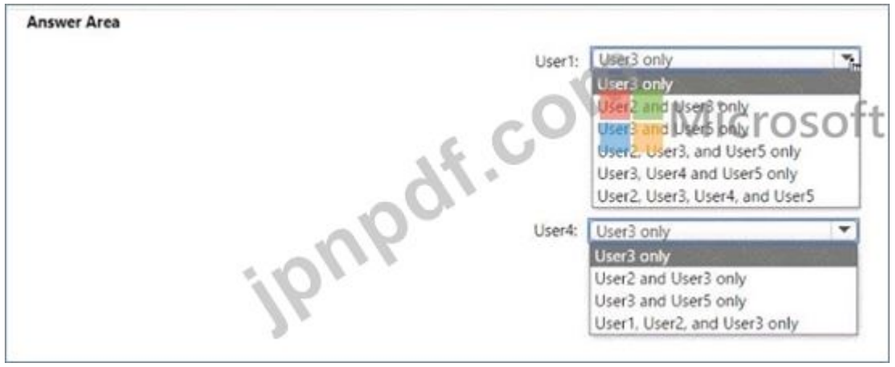
最新問題: **25**
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

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、次の表に示すロール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 はどのユーザーのパスワードをリセットできますか? 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:

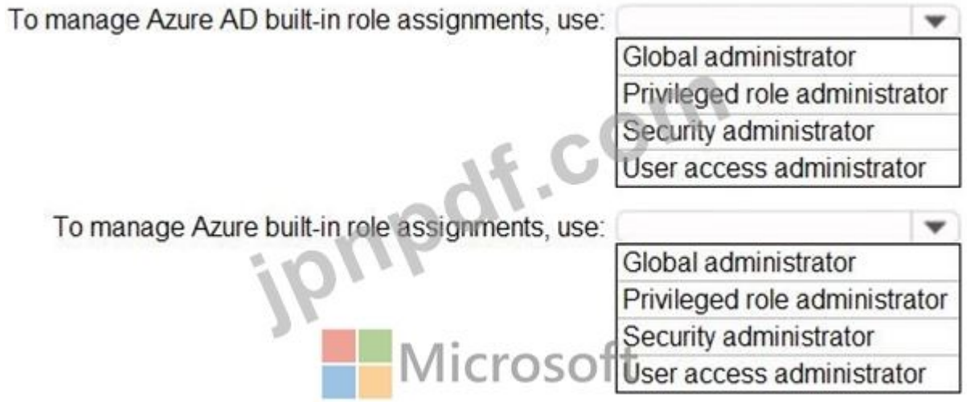


最新問題**: 26**

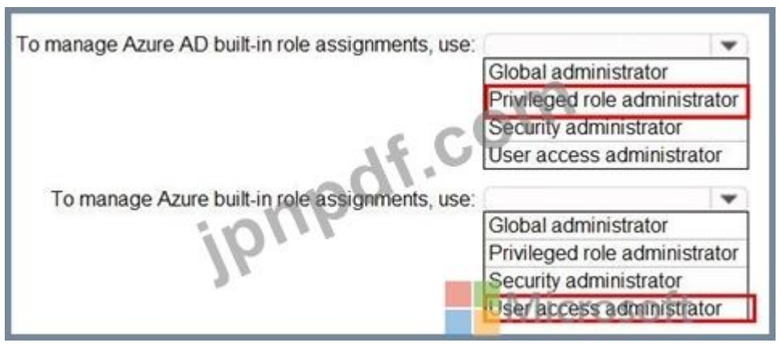
役割の割り当てを管理するために使用する役割を特定する必要があります。ソリューションは委任要件を満たす必要があります。

どうすればいいでしょうか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。

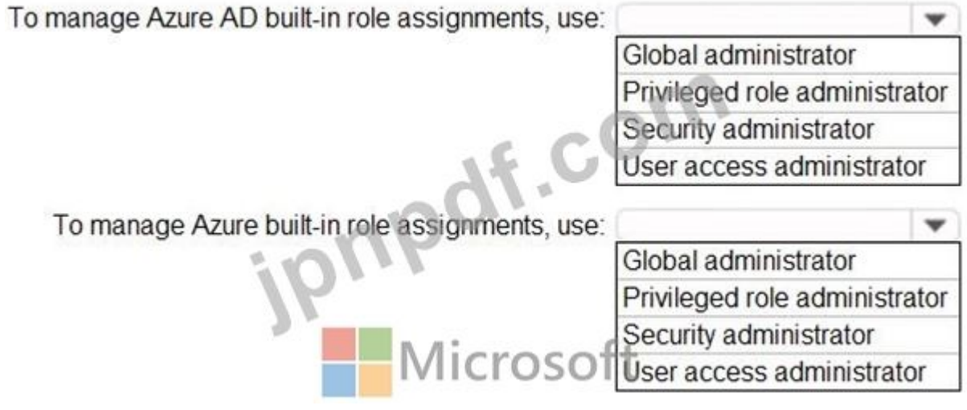


Answer:



参照：
https://docs.microsoft.com/en-us/azure/ロールベースのアクセス制御/ロール割り当てポータル
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

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要件を満たす必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



参照：
https://docs.microsoft.com/en-us/azure/ロールベースのアクセス制御/ロール割り当てポータル
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

最新問題: **28**
Admin1 という名前のユーザーを含む Azure AD テナントがあります。
Admin1 は、高リスク ユーザーのパスワード変更を要求するポリシー テンプレートを使用して、新しい条件付きアクセス ポリシーを作成します。
ポリシー割り当てにおいて、デフォルトで誰に含まれ、誰に除外されますか？ 適切なオプションを正しい対象にドラッグしてください。各オプションは、1回、複数回、または全く使用されない場合があります。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

白い背景に黒い文字の説明が自動的に生成されます



最新問題: 29

contoso.com の SMTP アドレス スペースを使用するオンプレミスの Microsoft Exchange 組織があります。

ユーザーが Microsoft 365 サービスへのセルフサービス サインアップに自分のメール アドレスを使用していることがわかりました。

自己署名ユーザーが含まれる Azure Active Directory (Azure AD) テナントに対するグローバル管理者権限を取得する必要があります。

どの 4 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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

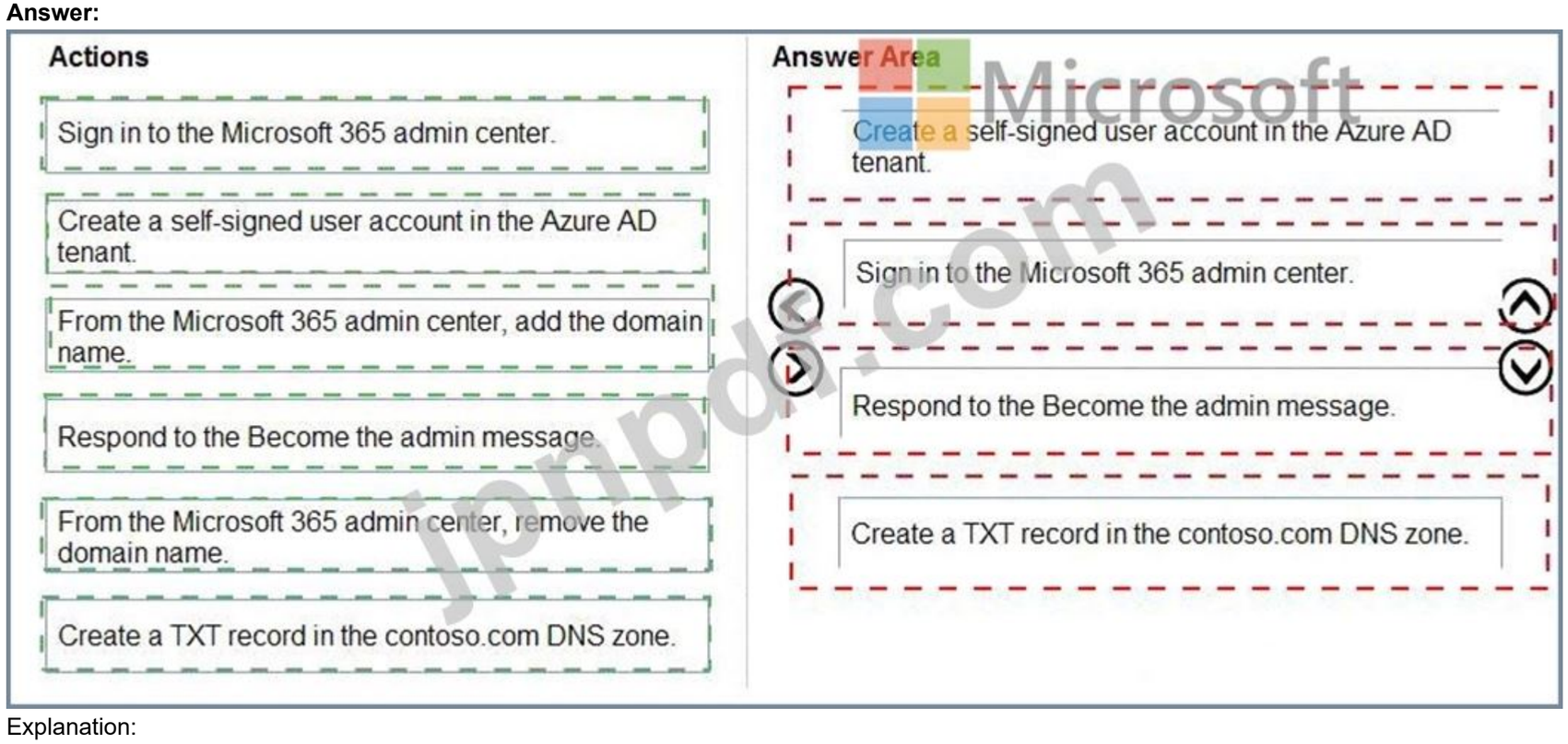
Actions

- Sign in to the Microsoft 365 admin center.
- Create a self-signed user account in the Azure AD tenant.
- From the Microsoft 365 admin center, add the domain name.
- Respond to the Become the admin message.
- From the Microsoft 365 admin center, remove the domain name.
- Create a TXT record in the contoso.com DNS zone.

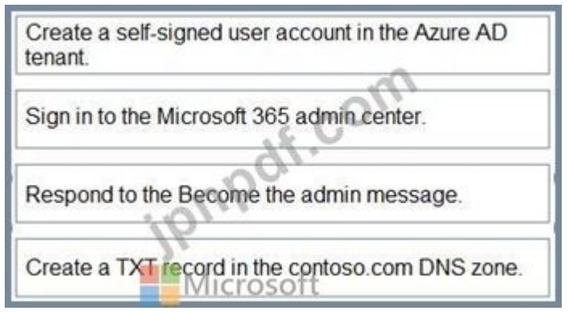
Answer Area



Answer:

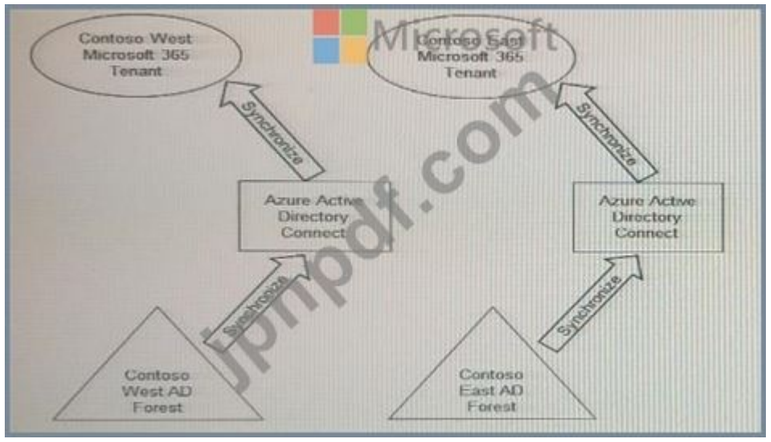


Explanation:



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

最新問題**: 30**
あなたの会社には、Contoso East と Contoso West という2つの部門があります。両部門の Microsoft 365 ID アーキテクチャは次の図に示されています。



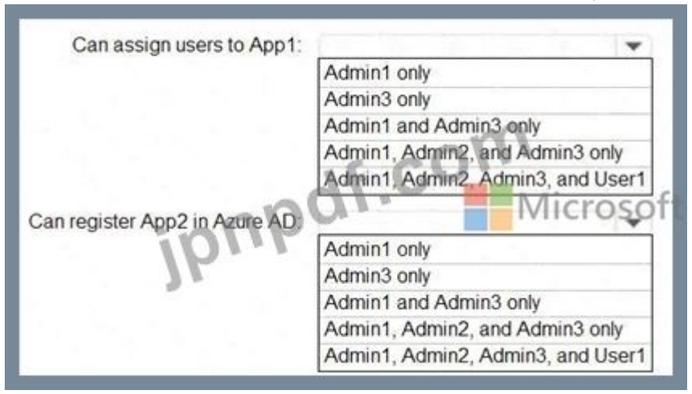
Contoso East部門のユーザーに、Contoso WestテナントのMicrosoft SharePoint Onlineサイトへのアクセスを割り当てる必要があります。このソリューションでは、追加のMicrosoft 3G5ライセンスは必要ありません。
何をすべきでしょうか?
A. West テナント内のすべての Contoso East ユーザーのゲスト アカウントを作成します。
B. Contoso West テナントで Azure AD アプリケーション プロキシを構成します。
C. Contoso Cast の既存の Azure AD Connect サーバーを構成して、Contoso East Active Directory フォレストを Contoso West テナントに同期します。
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**: 31**
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、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Azure ADに登録します。

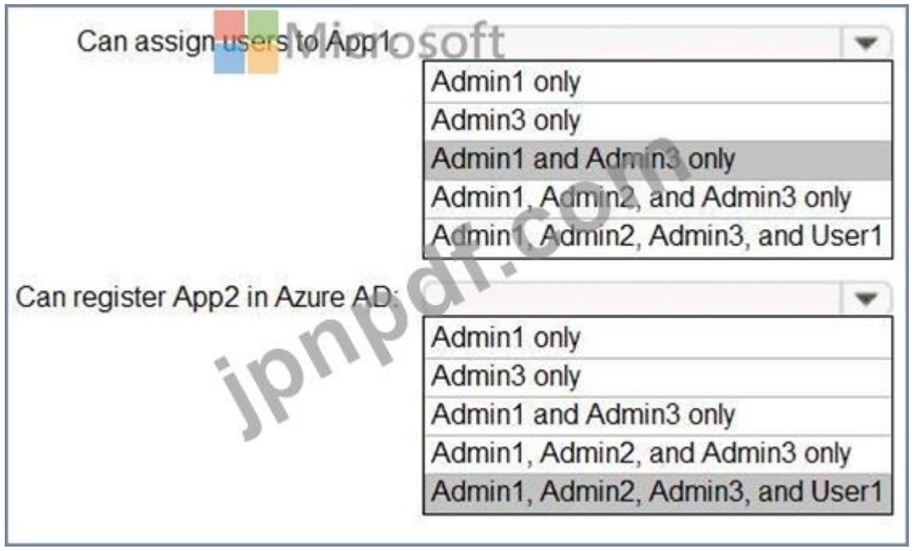
App1 にユーザーを割り当てることができるユーザーと、Azure AD に App2 を登録できるユーザーを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



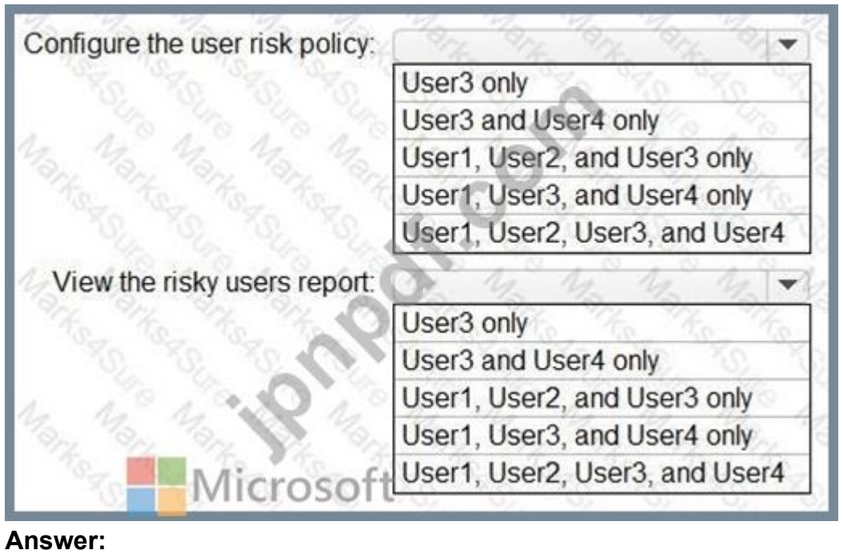
参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 32
次の表に示すユーザーを含む Azure Active 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 Identity Protection を実装する予定です。
ユーザー リスク ポリシーを構成できるのはどのユーザーですか。また、リスクのあるユーザー レポートを表示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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



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

最新問題**: 33**
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。このテナントには、App1という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。このテナントには、App2という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 2 つの資格情報はどれですか。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 ポイントが加算されます。
A. 証明書
B. マネージドID
C. 秘密
D. ユーザーアカウント

E. ワンタイムパスワード
Answer: (解答を表示する**)**
Microsoft Entra ID では、1 つのアプリケーション (App1) がユーザーの介入なしに別のアプリケーション (App2) の API に安全にアクセスする必要がある場合、アプリのみの認証 (クライアント資格情報フローとも呼ばれます) が使用されます。
アプリ間通信の場合:
* App1 には、App2 への権限を付与する必要があります (アプリケーション権限経由)。
* App1 は、Entra ID が認識する資格情報を使用して認証する必要があります。
有効な資格情報の種類は次のとおりです。
* 証明書 - X.509 証明書を使用したアプリ認証の安全な方法。
* クライアント シークレット - アプリの認証に使用されるテキストベースのキー (パスワード)。
Microsoft のドキュメントには次のように記載されています。
「アプリケーション ID は、クライアント資格情報フローでクライアント シークレットまたは証明書を使用して確立できます。」オプション B (マネージド ID) は、Azure リソース (登録済みアプリではない) にのみ適用されます。
オプション D (ユーザー アカウント) と E (ワンタイム パスワード) は対話型の資格情報であり、アプリのみのアクセスには無効です。
Microsoft Entra ID では、1 つのアプリケーション (App1) がユーザーの介入なしに別のアプリケーション (App2) の API に安全にアクセスする必要がある場合、アプリのみの認証 (クライアント資格情報フローとも呼ばれます) が使用されます。
アプリ間通信の場合:
* App1 には、App2 への権限を付与する必要があります (アプリケーション権限経由)。
* App1 は、Entra ID が認識する資格情報を使用して認証する必要があります。
有効な資格情報の種類は次のとおりです。
* 証明書 - X.509 証明書を使用したアプリ認証の安全な方法。
* クライアント シークレット - アプリの認証に使用されるテキストベースのキー (パスワード)。
Microsoft のドキュメントには次のように記載されています。
「アプリケーション ID は、クライアント資格情報フローでクライアント シークレットまたは証明書を使用して確立できます。」オプション B (マネージド ID) は、Azure リソース (登録済みアプリではない) にのみ適用されます。
オプション D (ユーザー アカウント) と E (ワンタイム パスワード) は対話型の資格情報であり、アプリのみのアクセスには無効です。

最新問題**: 34**
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、および Role1
B. ホテルと貢献者のみ
C. グループ1、ロール1、および貢献者のみ
D. グループ1のみ
Answer: A (メーッセージを残す**)**

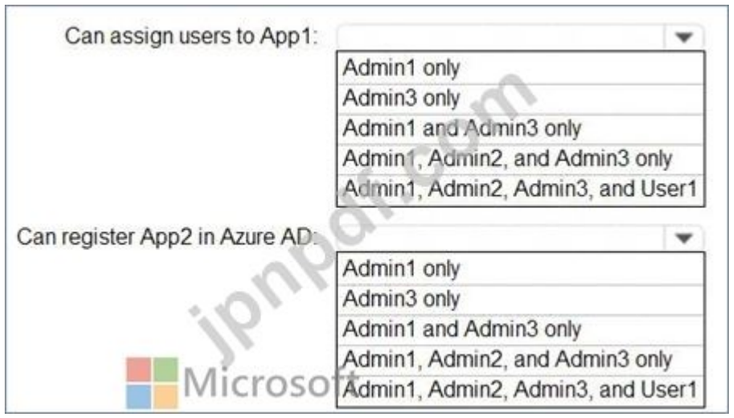
アクセス レビューには、Azure AD Premium P2 ライセンスが必要です。
Group1 と App1 のアクセス レビューは、Azure AD アクセス レビューで構成できます。
共同作成者ロールとロール1のアクセスレビューは、Privileged Identity Management (PIM) で構成する必要があります。PIM は Azure AD Premium P2 に含まれています。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-start- 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**: 35**
storage1 という名前のストレージ アカウントと WebApp1 という名前の Web アプリを含む Azure サブスクリプションがあります。WebApp1 はシステム割り当てのマネージド ID を使用します。
WebApp1 がシステム割り当てマネージド ID を使用して storage1 のファイルを読み書きできることを確認する必要があります。
Azure ポータルで storage1 に何を構成する必要がありますか?
A. ファイル共有設定
B. アクセス制御（午前時）設定
C. 共有アクセス署名 (SAS)
D. データ保護
E. アクセスキー
Answer: B (メーッセージを残す**)**
Microsoft SC-300 公式学習ガイドおよび Microsoft Learn モジュール 「マネージド ID を使用して ID を管理する」によれば、Web アプリがシステム割り当てのマネージド ID を使用する場合、Azure は Microsoft Entra ID 内にその ID を表すサービス プリンシパルを自動的に作成します。
Azure Storage アカウント内のファイルの読み取りと書き込みの権限をマネージド ID に付与するには、Azure ポータルの [アクセス制御 (IAM)] ブレードで、ロールベースのアクセス制御 (RBAC) 権限を構成する必要があります。具体的には、適切なリソース スコープ (ストレージ アカウントやコンテナーなど) で、マネージド ID にストレージ BLOB データ共同作成者やストレージ BLOB データ閲覧者などのロールを割り当てます。
SAS トークン、アクセス キー、ファイル共有設定などのその他のオプションは、キーベースまたは手動の認証方法に依存しており、これは最小権限とマネージド ID 自動化の原則に反します。
アクセス制御 (IAM) は、Azure AD を介した安全な ID ベースのアクセスを保証します。
正解: B. アクセス制御（IAM）設定

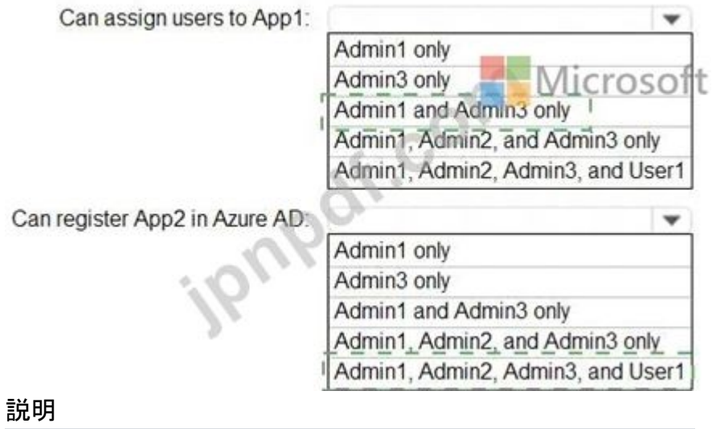
最新問題**: 36**
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

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

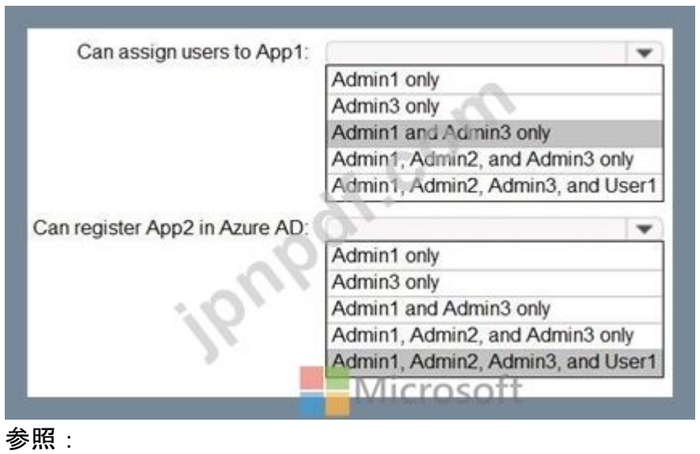
App1とApp2という2つのクラウドアプリを購入します。グローバル管理者はApp1をAzure ADに登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD に App2 を登録できるユーザーを特定する必要があります。
何を特定する必要がありますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明



参照：

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users

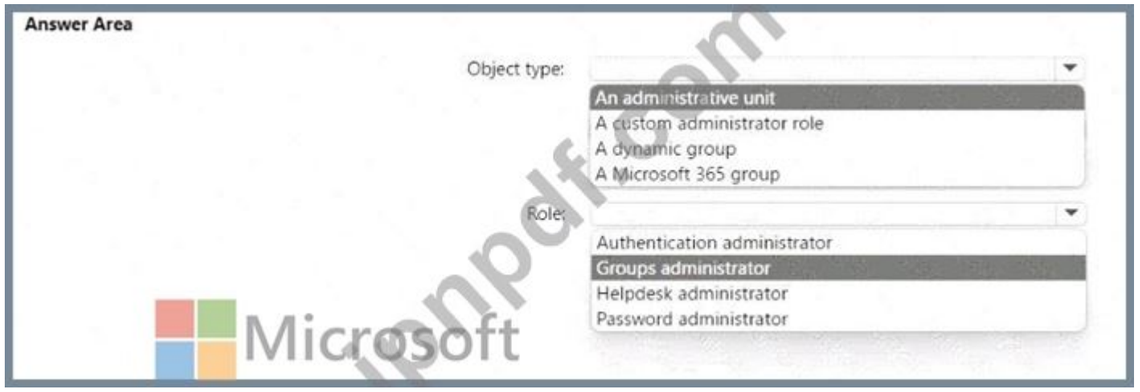
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

最新問題**: 37**

5,000人のユーザーがいるMicrosoft 365テナントがあります。そのうち100人は経営幹部で、経営幹部には専任のサポートチームがいます。

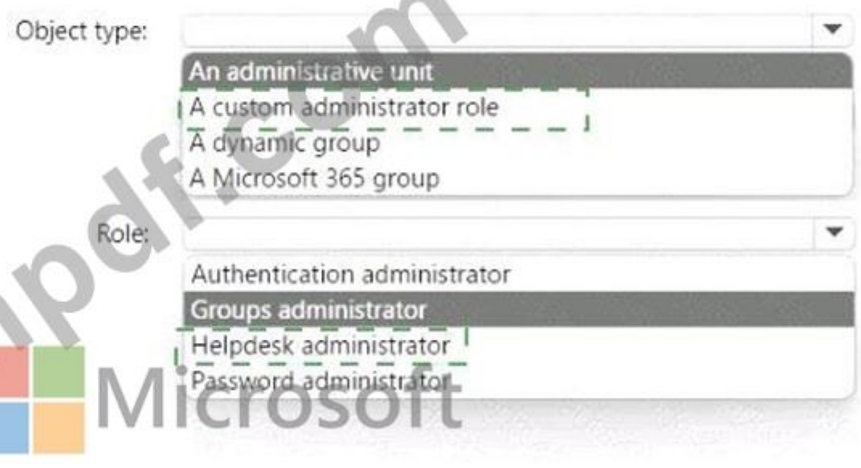
サポートチームが経営幹部のみを対象にパスワードのリセットと多要素認証（MFA）設定を管理できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。

どのオブジェクト タイプと Azure Active Directory (Azure AD) ロールを使用す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Answer Area



Explanation:



最新問題**: 38**

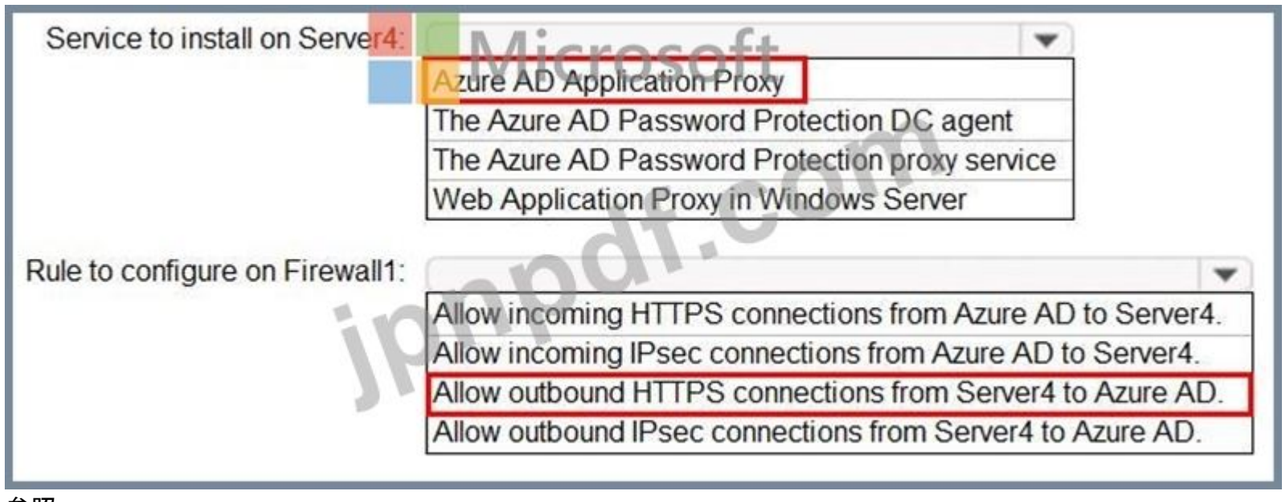
次の表に示すホストを含むオンプレミス データセンターがあります。

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

Active Directory フォレストと同期する Azure Active 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 Azure AD ユーザーに公開できることを確認する必要があります。
Server と Firewall1 で何を設定す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

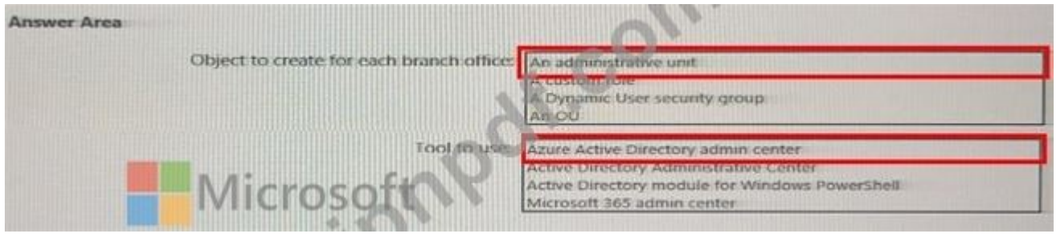


参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-proxy

最新問題**: 39**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **40**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、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試行が失敗すると、毎日 100 件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に代わってアラートを受信するように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)
診断設定ではなくアクション グループを変更するには、Azure モニターに移動する必要があります。

最新問題: **41**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションで質問に回答した後は、そのセクションに戻ることはできず、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。
Amazon Web Services (AWS) アカウント、Google Workspace サブスクリプション、GitHub アカウントをお持ちです。
Azureサブスクリプションを展開し、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、Microsoft Azure アプリ コネクタを追加します。
これは目標を満たしていますか?
A. はい

B. いいえ

Answer: (解答を表示する)

Microsoft Azure コネクタは、Azure リソース アクティビティを Defender for Cloud Apps に統合し、サードパーティ アプリ間の OAuth 認証要求ではなく、Azure 内のリソース管理操作とセキュリティ アラートに主に焦点を当てています。

Microsoft Defender for Cloud Apps の公式ドキュメントによると、次のとおりです。

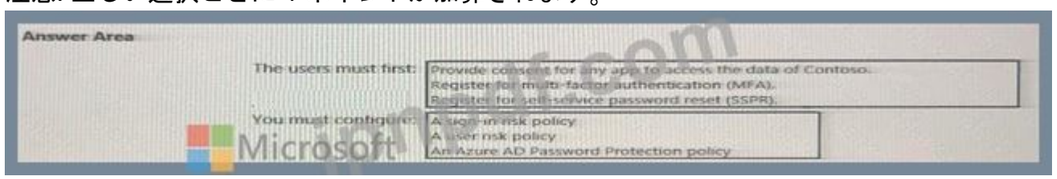
「Microsoft Azureコネクタを追加すると、Azure Resource Managerのアクティビティとアラートを可視化できますが、サードパーティのOAuth認証データは可視化できません。」OAuthアプリ認証の監視には、Azure自体ではなく、認証にOAuthを使用するクラウドアプリケーション（Google Workspace、AWS、GitHubなど）への接続が含まれます。したがって、Microsoft Azureコネクタを追加しても、ハイブリッド環境全体でOAuth認証リクエストを監視するという目標は達成されません。

最新問題**: 42**

ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。

ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題**: 43**

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 ポイントが加算されます。



Answer:



Explanation:

ユーザー 1 は、Microsoft 365 アプリにサインインするときに多要素認証 (MFA) を使用する必要があります。= はい ユーザー 2 は、Microsoft 365 アプリにサインインするときに多要素認証 (MFA) を使用する必要があります。= はい ユーザー 3 は、Microsoft 365 アプリにサインインするときに多要素認証 (MFA) を使用する必要があります。= いいえ すべての Microsoft SC-300: ID およびアクセス管理者ドキュメントによる包括的かつ詳細な説明: = 条件付きアクセスでは、適用は割り当て # ユーザーまたはワークロード ID (ポリシーの適用先を指定) とターゲット リソース (保護されるアプリ/リソースを指定) によって決定されます。

ポリシーの付与制御が 多要素認証を必要とする」に設定されている場合、ポリシーのユーザー割り当てスコープに含まれるすべてのIDは、対象リソースへのアクセス時に多要素認証を実行する必要があります。複数のグループのメンバーであっても適用が緩和されることはありません。ユーザーがいずれかのグループに属している場合、ポリシーが適用されます。

逆に、ポリシーのユーザー割り当てスコープに含まれていないユーザーは、特権ロールを保持している場合でも、そのポリシーによってMFAの入力を求められません。テナントがセキュリティの既定値を使用しているか、条件付きアクセスポリシーがその管理者アカウントまたはそのグループを対象としている場合を除き、グローバル管理者ロールを保持しているからといって、MFAが自動的に強制されるわけではありません。

これをシナリオに適用すると、Policy1 はすべてのクラウドアプリを対象としており つまり、アプリ側はユニバーサル)、グループのコンテキストを考慮すると、ユーザー割り当てのスコープは Group1 に設定されます。User1 Group1)と User2 Group1 と Group2)は両方ともスコープ内にあるため、MFA を実行する必要があります。User3 は Group2 のみに存在します。Group2 はポリシーのユーザー割り当て範囲外であるため、グローバル管理者ロールを持つ User3 には Policy1 が適用されません。したがって、次のようになります。

User1 の場合は 「はい」、User2 の場合は 「はい」、User3 の場合は 「いいえ」。

最新問題: **44**

I-.Group1の問題を解決する必要があります。まず何をすべきでしょうか？

A. IT-Group 1 グループを再作成します。

B. IT-Group1のメンバーシップタイプを動的デバイスに変更します

C. IT_Group1 に所有者を追加します。

D. IT-Group1のメンバーシップタイプを動的ユーザーに変更します

Answer: A (メーッセージを残す**)**

組み込みのディレクトリ ロール (デバイス管理者など) をグループに割り当てるには、ロールを割り当て可能なグループが必要です。

SC-300のドキュメントでは、 クラウドセキュリティグループにAzure ADロールを割り当てるには、 Azure ADロールをグループに割り当てることができます』という設定でグループを作成する必要があります」と説明されています。さらに、 この属性は変更できません。作成時に決定する必要があります。既存のグループを後からロール割り当て可能に変換することはできません」と強調されています。標準セキュリティグループがロール割り当て可能として作成されていない場合、ディレクトリロールを割り当てようとしたときにピッカーに表示されません。これは、 ロール割り当て可能でないグループ

は、Azure ADロールの割り当て対象として選択できません」という動作と全く同じです。したがって、最初の手順は、IT_Group1をロール割り当て可能なセキュリティグループ（「ロール割り当て対象」グループと呼ばれることが多い）として再作成し、そのグループにデバイス管理者ロールを割り当てることです。メンバーシップの種類（動的ユーザーまたは動的デバイス）を変更したり、所有者を追加したりしても、既存のグループがロール割り当て可能なグループに変換されないため、問題は解決されません。

最新問題: **45**
Azure AD Identity Protection を使用し、次の表に示すリソースを含む Azure AD テナントがあります。

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

Azure Multi-Factor Authentication (MFA) はすべてのユーザーに対して有効になっています。
User1 は、追加調査を必要とする中程度の重大度のアラートをトリガーします。
次回サインインするときに、User1 にパスワードをリセットさせる必要があります。ソリューションでは、管理の労力を最小限に抑える必要があります。
何をすべきでしょうか?
A. User1 の Azure MFA 登録をリセットします。
B. User1 を侵害ありとしてマークします。
C. サインイン リスク ポリシーを構成します。
D. 中程度または低程度の重大度でトリガーされるようにユーザー リスク ポリシーを再構成します。
Answer: B (メッセージを残す)

最新問題: **46**
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Azure AD tenant-level setting to modify:
- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:
- Application administrator
- Application developer
- Cloud application administrator

Answer:

jpnpdf.com



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

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 47
Sub1 という名前の Azure サブスクリプションがあり、そこには RG1 という名前のリソース グループが含まれています。RG1 には、Azure ロールベースのアクセス制御 (Azure RBAC) を使用する KV1 と KV2 という名前の 2 つの Azure キー コンテナーが含まれています。
サブスクリプションには、次の表に示すユーザーが含まれます。

Name	Role	Role scope
User1	Key Vault Administrator	Sub1
User2	Key Vault Reader	RG1
User3	Key Vault Secrets User	KV1

KV1 には Secret 1 という名前のシークレットが含まれています。KV2 には Secret2 という名前のシークレットが含まれています。
各シークレットの値を読み取ることが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:

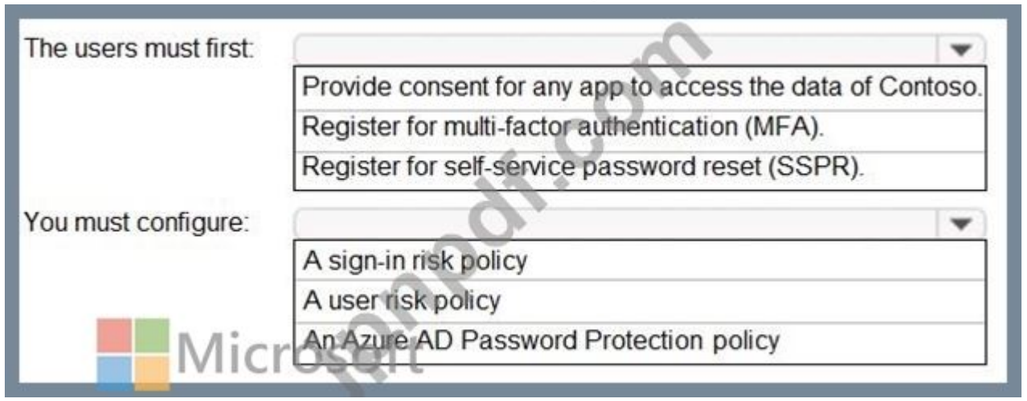


最新問題: **48**

ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。

ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。

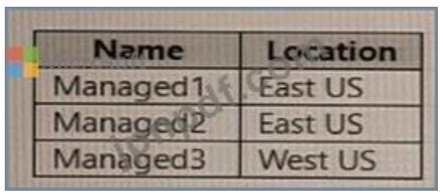


Answer:



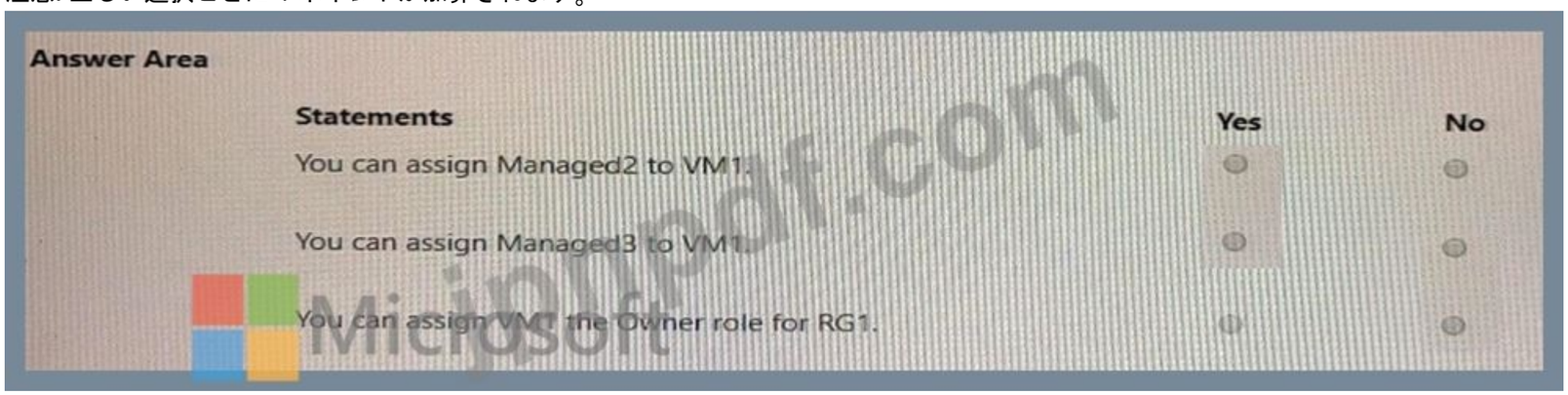
参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

最新問題: 49
次の仮想マシンが含まれる Azure サブスクリプションがあります。名前: 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。

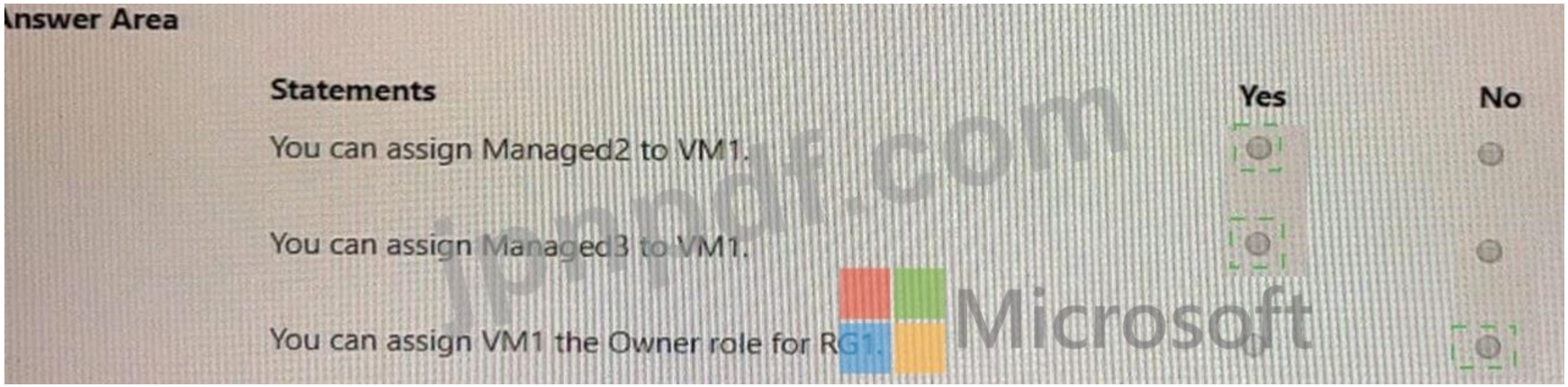


Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

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。
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 ポイントが加算されます。



Answer:



Explanation:



最新問題**: 50**

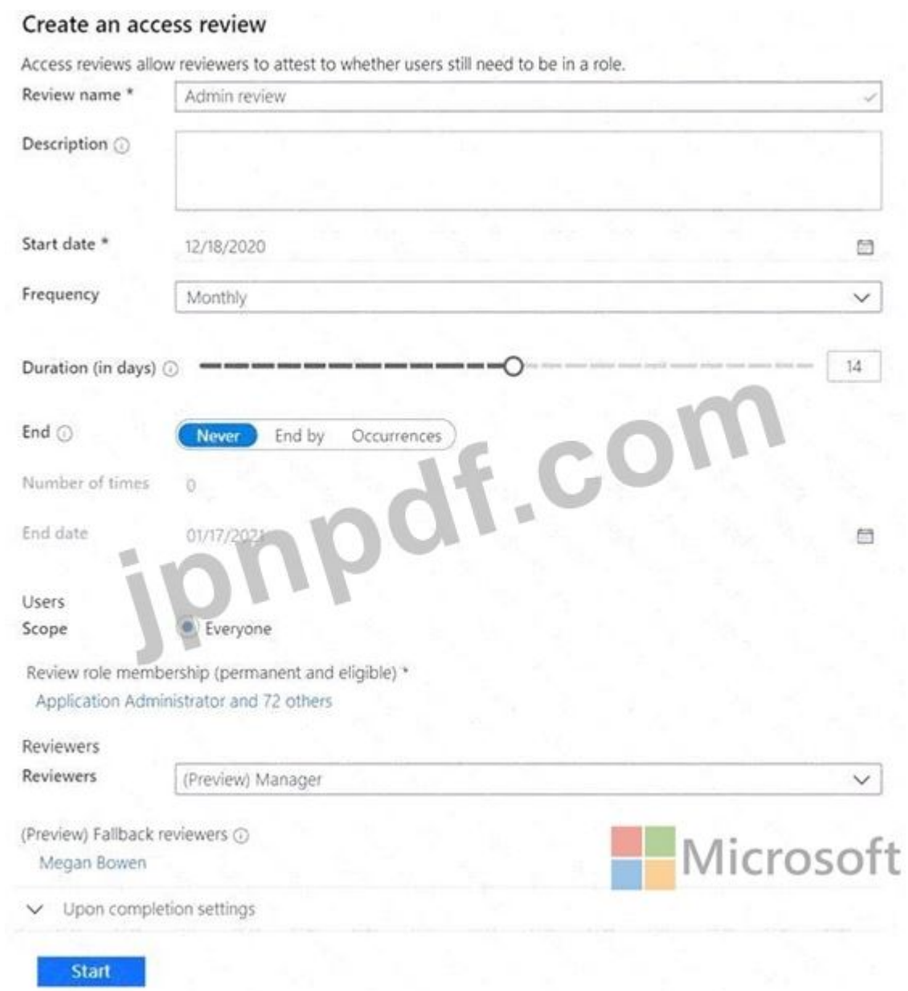
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。

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。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 テナントがあります。

100 人の IT 管理者が 10 の部門に分かれて所属しています。

展示に示されているアクセス レビューを作成します。([展示] タブをクリックします。)



jpnpdf.com

すべてのアクセス レビュー リクエストは Megan Bowen 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れ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 (自分) に設定します。
これは目標を満たしていますか?
A. いいえ
B. はい
Answer: A (メーッセージを残す**)**

最新問題**: 51**
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、Azure Active Directory (Azure AD) へのセルフサービス サインアップに contoso.com のメール アドレスを使用しています。
自己署名ユーザーを含む Azure AD 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 Azure AD 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. Set-MsolCompanySettings

B. Set-MsolDomainFederationSettings
C. Update-MsolfederatedDomain
D. Set-MsolDomain
Answer: A (メーッセージを残す)
Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn のコンテンツ「Azure AD テナントの管理とテナントプロパティの構成」によると、セルフサービス サインアップ（バイラル サインアップとも呼ばれます）を使用すると、ユーザーは既存の Azure AD テナントに関連付けられたメールドメインを使用して、そのテナントにアカウントを作成できます。この機能は、明示的に無効化されていない場合、外部ユーザーや管理されていないユーザーが ID を作成できるため、組織の名前空間で不正なアカウントが作成される可能性があります。
ユーザーが組織の検証済みドメイン (例: contoso.com) を使用してセルフサービス サインアップを実行できないようにします。
com）を使用している場合、管理者はPowerShellを使用してAzure Active DirectoryのAllowEmailVerifiedUsers設定を無効にする必要があります。この構成変更により、ユーザーがMicrosoft 365やその他のAzureサービスに登録する際に、組織のドメインでアカウントを自動的に作成することを防ぐことができます。
このようなテナント レベルの設定を構成するために使用されるコマンドレットは、MSOnline モジュールの Set-MsolCompanySettings です。
具体的な PowerShell コマンドは次のようになります。
Set-MsolCompanySettings -AllowEmailVerifiedUsers $false
このコマンドは、電子メールで確認されたユーザーのセルフサービス サインアップを無効にし、管理者のみがテナントにアカウントを作成できるようにします。
オプション内のその他のコマンドレットは、異なる目的に使用されます。
* Set-MsolDomainFederationSettings - ドメインのフェデレーション設定を構成するために使用されます。
* Update-MsolFederatedDomain - フェデレーション信頼設定を更新または修復するために使用されます。
* Set-MsolDomain - ドメイン固有のプロパティ (認証の種類など) を構成するために使用されます。
Microsoft の公式ドキュメントによると:
ユーザーが組織の検証済みドメインを使用してセルフサービス サインアップできないようにするには、Set-MsolCompanySettings を使用して AllowEmailVerifiedUsers を $false に設定します。

最新問題**: 52**
Microsoft Defender for Cloud Apps を使用する Microsoft 365 E5 サブスクリプションがあります。
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。ソリューションは管理作業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 Defender for Cloud Apps ポータルから、承認されていない Facebook。
B. Microsoft Endpoint Manager でアプリ構成ポリシーを作成します。
C. Defender for Cloud Apps アクセス ポリシーを作成します。
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)
質問は、管理作業を最小限に抑えながら、Microsoft Defender for Cloud Apps (MCAS) を使用して、デバイスやブラウザーから Facebook にアクセスしているユーザーを識別する方法を尋ねています。
内訳は次のとおりです。
* 目的: Facebook (クラウド アプリ) にアクセスするユーザーを識別する。
* ツール: Microsoft Defender for Cloud Apps。
* 要件: 制御ではなく可視性、つまり検出とレポート。
これを実現するための適切な最初のステップは、Defender for Cloud Apps にアクセス ポリシーを作成することです。
アクセスポリシーを使用すると、ユーザー、デバイス、場所、アプリの使用状況に基づいて、クラウドアプリへのリアルタイムセッションアクセスを監視および制御できます。アクセスポリシーには以下の機能があります。
* ユーザーが特定のアプリ (Facebook など) にサインインしたり使用したりしたことを検出します。

* 自動的にログに記録し、管理者に警告します。
* エンドポイントまたは条件付きアクセスの構成は不要 - 管理の労力を最小限に抑える」という要件を満たします。
Microsoft Defender for Cloud Apps のドキュメントより:
「アクセスポリシーはアプリのアクセスパターンを監視し、ユーザーが特定の承認済みまたは承認されていないクラウドアプリケーションにサインインまたはアクセスしたときにアラートをトリガーできます。」その他のオプションについては以下で説明します。
* (A) 非承認の Facebook はそれを禁止としてマークしますが、アクセスしているユーザーを特定しません。
* (B) Intune のアプリ構成ポリシーは、クラウド アプリのアクセスではなく、モバイル デバイスの設定を制御します。
* (D) 条件付きアクセス ポリシーでは、Facebook へのアクセスをブロックしたり条件を要求したりできますが、誰がアクセスしたかは報告されません。

最新問題: **53**
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	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

次の設定を持つユーザー リスク ポリシーがあります。
* 課題:
含める: グループ1
o 除外: グループ2
* サインインリスク 中以上
* アクセス制御:
o アクセスを許可する: パスワードの変更を要求する
ユーザーがサインインしようとすると、次の表に示すようにユーザーのリスク レベルが検出されます。

User	Risk level
User1	High
User2	Medium
User3	High

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。

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	○	○
User2 must change their password during sign in.	○	○
User3 must change their password during sign in.	○	○

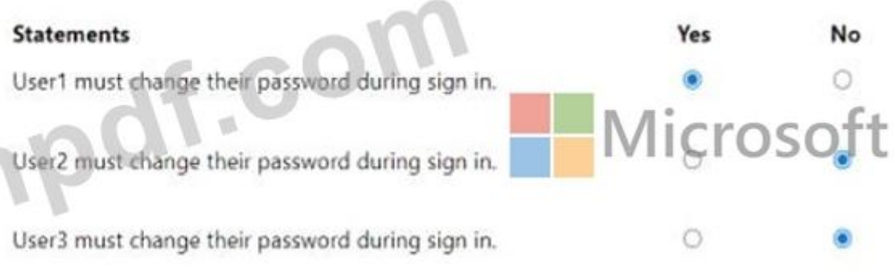
Answer:

Answer Area



Explanation:

Answer Area



最新問題: 54

Groups1、Group2、Group3 という 3 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	Role	Member of
User1	Global Administrator	Group1
User2	None	Group2
User3	Global Reader	Group2, Group3

次の設定を持つ CAT という名前の条件付きアクセス ポリシーを作成します。

* ユーザー

* 含む

#ユーザーとグループ: グループ1

o 除外

#ユーザーとグループ: グループ2

#ディレクトリの役割: グローバル管理者

o ターゲットリソース

#含める: すべてのクラウドアプリ

o アクセス制御

#Grant: 多要素認証を要求する

次の設定を持つ CA2 という名前の条件付きアクセス ポリシーを作成します。

* ユーザー

* 含む

#ユーザーとグループ: グループ2

o 除外

#ユーザーとグループ: グループ3
o ターゲットリソース
#含める: すべてのクラウドアプリ
o アクセス制御
#許可: アクセスをブロック
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 ポイントが加算されます。



Answer:



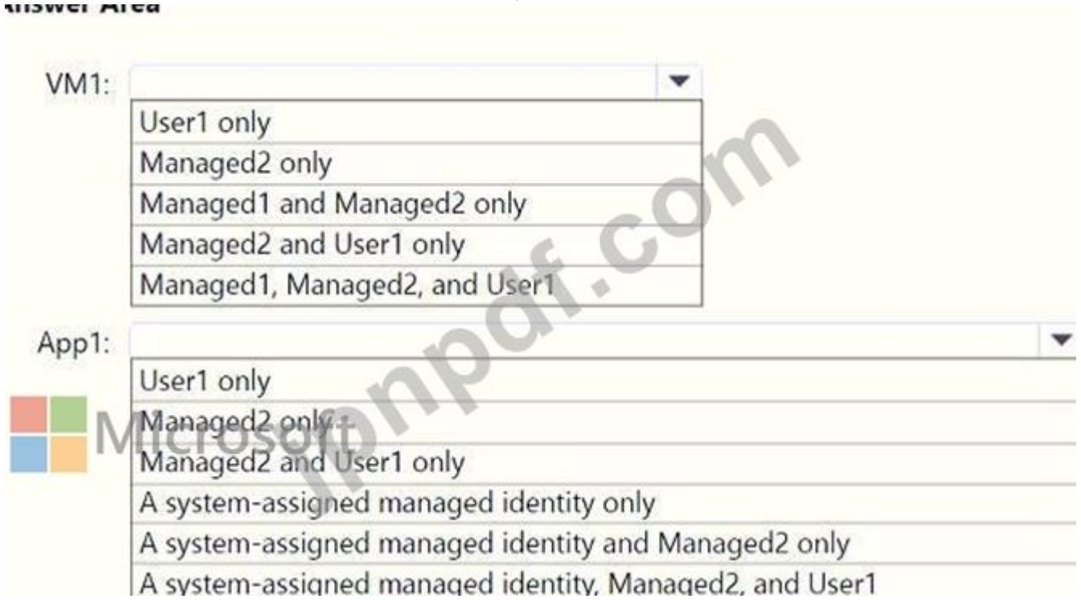
Explanation:



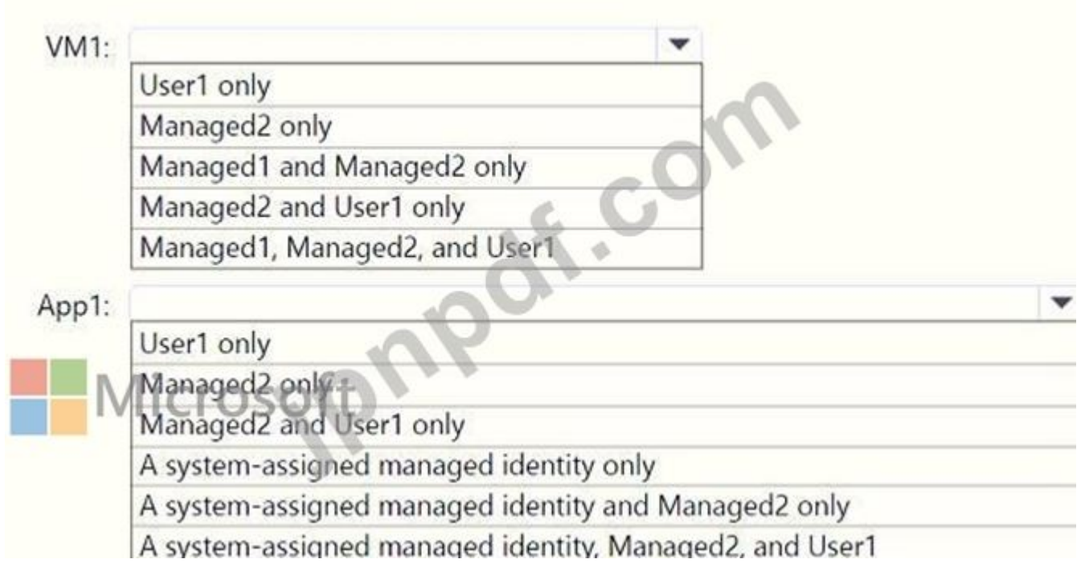
最新問題**: 55**
ホットスポットに関する質問
次の表に示すリソースを含む Azure サブスクリプションがあります。

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

User1 という名前の Microsoft Entra ユーザーを作成します。
VM1 と App1 に追加できる ID はどれですか。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。
注意: 正解ごとに 1 ポイントが加算されます。



Answer:



最新問題: **56**
ドラッグアンドドロップの質問
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Azure仮想マシンにサインインできることを確認する

Microsoft 365 の資格情報。
- 新しい仮想マシンを作成する権限を委任します。
各要件にはどのような機能を利用すべきでしょうか？ 適切な機能を正しい要件にドラッグして答えてください。各機能は1回、複数回、または全く使用されない場合があります。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad- windows#configure-role-assignments-for-the-vm

最新問題**: 57**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Fabrikam, Inc. という会社のユーザーにリソース アクセスを提供するために、権限管理を実装します。Fabrikam は fabrikam.com というドメインを使用します。
アクセスが不要になった場合、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。
次の設定を構成する必要があります。
- 外部ユーザーがこのディレクトリにサインインすることをブロックする: いいえ
- 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: 90
Identity Governance ブレードでは何を構成する必要がありますか?
A. アクセスパッケージ
B. 権限管理設定
C. 利用規約
D. アクセスレビュー
Answer: B (メーッセージを残す**)**
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management- external-users#manage-the-lifecycle-of-external-users

最新問題: **58**
次の表に示すユーザーを含む Azure Active 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。
- レビュー対象ユーザー: グループのメンバー
- 対象: 全員
- グループ: グループ1
- レビュー担当者: メンバー（自身）
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、ユーザー2、ユーザー3
B. ユーザー3のみ
C. ユーザー1のみ
D. ユーザー1とユーザー2のみ
Answer: (解答を表示する)
設定は自己レビューされたため、全員が自分自身でレビューすることになります。つまり、User3 は User3 によってレビューされます。
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how- to-start-security-review

最新問題: **59**
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要件を満たす必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



jpnpdf.com
Microsoft

Answer:



参照：
https://docs.microsoft.com/en-us/azure/ロールベースのアクセス制御/ロール割り当てポータル
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

最新問題: 60
contoso.com という名前の Microsoft 365 テナントがあります。
ゲストユーザーアクセスが有効になっています。
次の表に示すように、ユーザーは contoso.com との共同作業に招待されます。

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory 管理センターの外部コラボレーション設定から、次の図に示すようにコラボレーション制限設定を構成します。



ユーザーは、Microsoft SharePoint Online サイトから user3@adatum.com をサイトに招待します。
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 ポイントが加算されます。

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

Answer:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

最新問題**: 61**
パッケージに計画されている変更を実施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5のみ
B. ユーザー4とユーザー5
C. ユーザー3のみ
D. ユーザー3とユーザー4
E. ユーザー3とユーザー5
F. ユーザー4のみ
Answer: A (メーッセージを残す**)**

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード**: Freepdfdumps**)

最新問題**: 62**
次のグループを含む Azure Active Directory (Azure AD) テナントがあります。
* 名前: グループ1
* メンバー: ユーザー1、ユーザー2
* 所有者: ユーザー3
2021 年 1 月 15 日に、図に示すようにアクセス レビューを作成します。([図] タブをクリックします。)

Create an access review

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

Review name * Review1

Description ⓘ

Start date * 01/15/2021

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never | End by | Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope
- ○ Guest users only
- ◉ Everyone

Group *
Group1

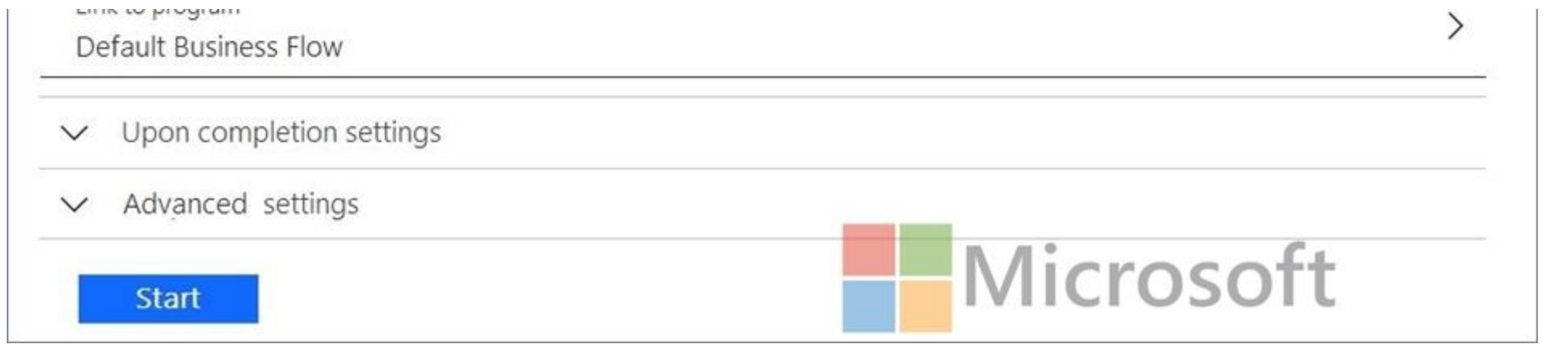
Reviewers

Reviewers Members (self)

Programs

Link to program

jpnpdf.com



ユーザーは、次の表に示すように Review1 の質問に回答します。

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 ポイントが加算されます。

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Answer:

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Explanation:

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

最新問題**: 63**

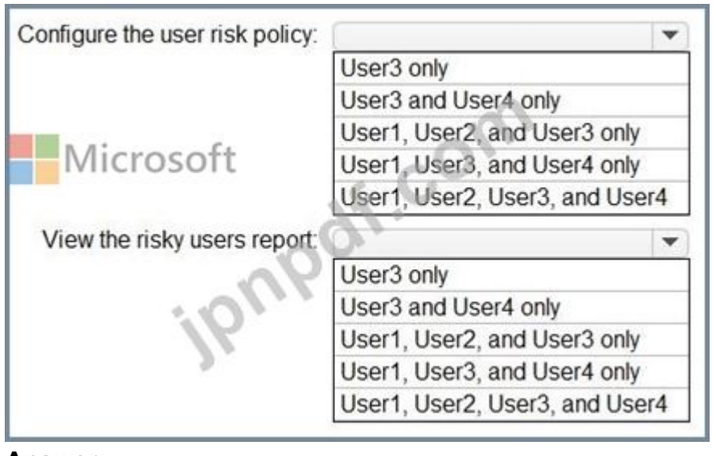
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

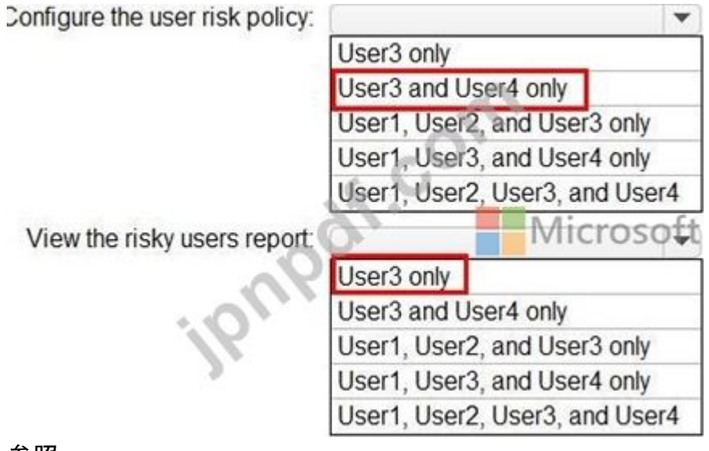
Azure AD Identity Protection を実装する予定です。

ユーザー リスク ポリシーを構成できるのはどのユーザーですか。また、リスクのあるユーザー レポートを表示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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題**: 64**
Azure Active Directory Premium P2 テナントがあります。
Log Analytics 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。
まず何をすべきでしょうか?
A. Set-AzureADTenantDetail コマンドレットを実行します。
B. Azure AD ブックを作成します。
C. Azure AD 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: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-integrate-activity-logs-with-lo

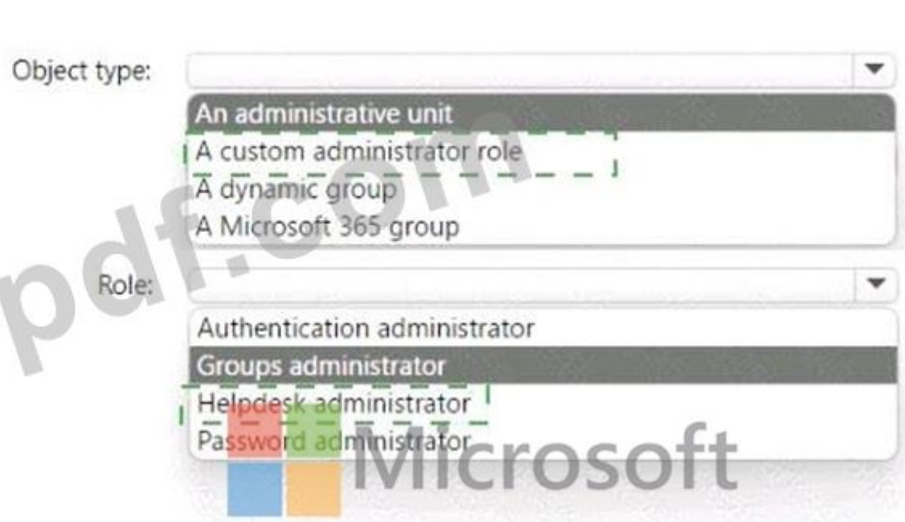
最新問題**: 65**
Microsoft 365 テナントがあります。
すべてのユーザーは、Microsoft 365 サービスにアクセスするときに、多要素認証 (MFA) に Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。
ユーザーが開始していない MFA リクエストを報告した場合、そのユーザーを自動的にブロックする必要があります。
解決策: Azure ポータルから、多要素認証 (MFA) のアカウント 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**)**
説明
不正行為警告設定を構成する必要があります。
参照：

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

最新問題: **66**
5,000人のユーザーがいるMicrosoft 365テナントがあります。そのうち100人は経営幹部で、経営幹部には専任のサポートチームがいます。
サポートチームがパスワードをリセットし、経営幹部のみの多要素認証（MFA）設定を管理できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのオブジェクト タイプと Azure Active Directory (Azure AD) ロールを使用す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:

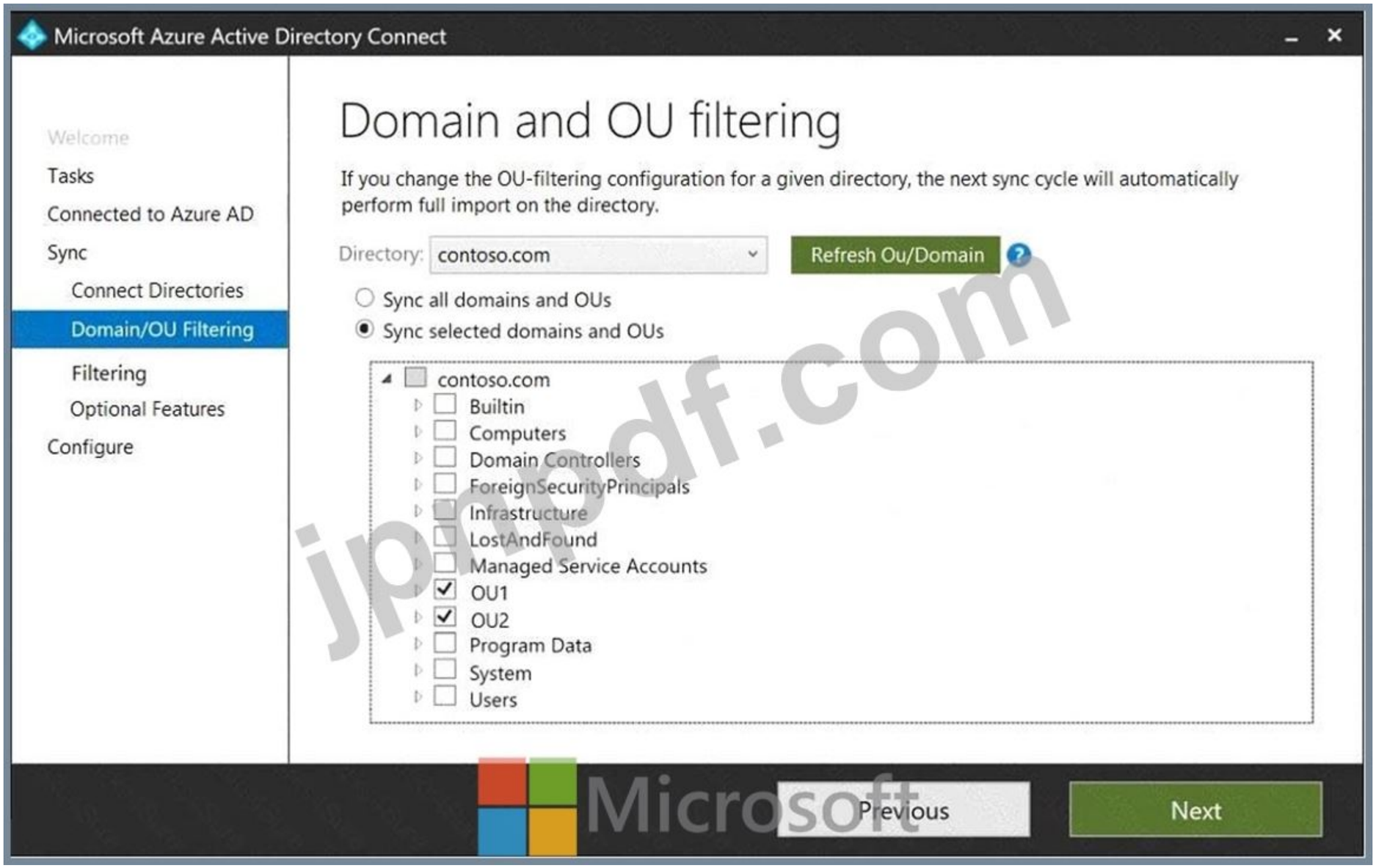


最新問題: **67**

ネットワークには、contoso.com というオンプレミスの Active Directory ドメインが含まれています。このドメインには、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」の図に示すように、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 のフィルタリング」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」設定は、「ユーザーとデバイスのフィルター」の図に示すように構成します。（「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。）



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 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Explanation:

Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

グループ1の直接のメンバーのみが同期されます。グループ2はグループ1の直接のメンバーであるため同期されますが、グループ2のメンバーは同期されません。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom
最新問題**: 68**

タスク10
Auditというグループを作成する必要があります。ソリューションでは、Auditのメンバーがセキュリティリーダーロールを有効化できるようにする必要があります。
Answer:
完全なステップバイステップの解決策については説明を参照してください
Explanation:
「監査」という名前のグループを作成し、そのメンバーがセキュリティ リーダー ロールをアクティブ化できるようにするには、次の手順に従います。
Microsoft Entra 管理センターを開きます。
セキュリティ管理者またはグローバル管理者の役割を持つアカウントでサインインします。
グループに移動します:
[チームとグループ] > [アクティブなチームとグループ] に移動します1。
セキュリティ グループを作成します。
セキュリティ グループの追加を選択します。
[基本設定] ページで、グループ名として「Audit」と入力します。
必要に応じて説明を追加し、[次へ1]を選択します。
設定を編集:
[設定の編集] ページで、Microsoft Entra ロールをこのグループに割り当て可能にするかどうかを選択し、[次へ] を選択します。
役割の割り当て:
グループを作成したら、「ロール」> 「すべてのロール」に移動します。
セキュリティ リーダー ロールを見つけて選択します。
[割り当て] の下で、[割り当て] を選択します。
「監査」グループを選択して、そのメンバーにロールを割り当てます2。
確認して終了:
設定を確認し、「監査」グループが作成され、そのメンバーがセキュリティ リーダー ロールをアクティブ化できることを確認します。
セットアップを終了し、変更を保存します。
これらの手順に従うことで、「監査」グループが作成され、そのメンバーがセキュリティ閲覧者ロールを有効化できるようになります。これにより、メンバーはセキュリティ関連情報を閲覧できますが、変更権限は付与されません。新しいグループとロールの割り当てについて、組織内の関係者に必ず伝えてください。

最新問題: **69**
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。
何を実装すべきでしょうか?
A. Microsoft Endpoint Manager で設定されたポリシー
B. Microsoft Endpoint Manager のアプリ構成ポリシー
C. Azure AD でのアプリ登録
D. Azure AD アプリケーション プロキシ
Answer: D (メーッセージを残す**)**
Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール「Azure AD アプリケーション プロキシを使用してリモート アクセス用にオンプレミス アプリを公開する」によると、Azure AD アプリケーション プロキシを使用すると、VPN アクセスを必要とせずに、内部のオンプレミス Web アプリケーションへの安全なリモート アクセスが可能になります。
このシナリオでは、App1 は Litware ネットワーク内でホストされているオンプレミス アプリケーションであり、技術要件では、Azure AD 認証を通じて内部ユーザーと外部ユーザー (Fabrikam ゲスト アカウントを含む) の両方が安全にアクセス可能である必要があると指定されています。
Microsoft の公式ドキュメントには次のように記載されています。

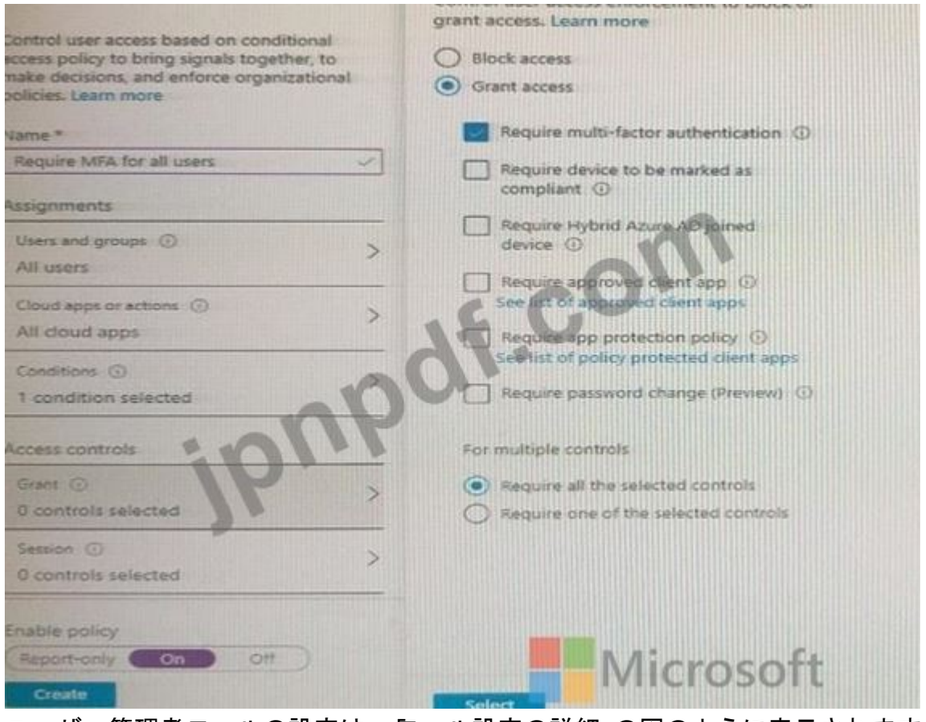
Azure AD アプリケーション プロキシは、オンプレミスの Web アプリケーションへの安全なリモート アクセスを提供し、Azure AD と統合してシングル サインオン (SSO) と条件付きアクセス ポリシーを実現します。」環境に既に Azure AD アプリケーション プロキシ コネクタを実行しているサーバー (SERVER1) が含まれており、Litware が App1 に対して Azure AD 条件付きアクセスと MFA を適用しようとしていることを考えると、Azure AD アプリケーション プロキシが適切な実装です。
その他のオプションは適切ではありません:
* A. Microsoft Endpoint Manager で設定されたポリシー: オンプレミス アプリの公開ではなく、デバイスのコンプライアンスとアプリの管理に使用されます。
* B. エンドポイント マネージャーのアプリ構成ポリシー: アクセスの公開ではなく、モバイル アプリの構成 (MAM ポリシーなど) に使用されます。
* C. Azure AD でのアプリの登録: 最新のクラウドまたは SaaS アプリの統合に使用されますが、App1 はオンプレミスであり、プロキシ アクセスが必要です。
D: Azure AD アプリケーション プロキシ
トピック1、Contoso, Ltd概要
Contoso 社は、モントリオールに本社を置き、ロンドンとシアトルにオフィスを構えるコンサルティング会社です。
Contoso は、Fabrikam, Inc という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。
既存の環境
Contoso 社のオンプレミスネットワークには、contos.com という Active Directory ドメインが含まれています。このドメインには、Contoso_Resources という組織単位 (OU) が含まれています。Contoso_Resoureces OU には、すべてのユーザーとコンピューターが含まれています。
Contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

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

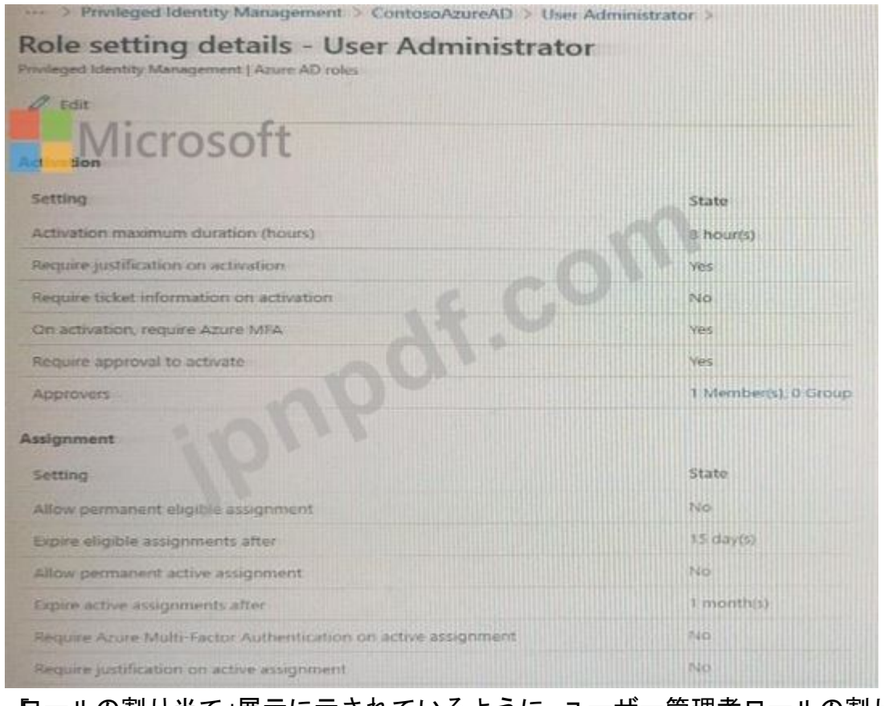
Microsoft 365/Azure 環境
Contoso には、次の関連ライセンスを持つ Contoso.com という名前の Azure AD テナントがあります。
マイクロソフト Office 365 エンタープライズ E5
エンタープライズモビリティ + セキュリティ
Windows 10 エンタープライズ E5
プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory Domain Serverless (AD DS) の間で構成されています。Contoso Resources OU のみが同期されます。
ヘルプデスク管理者は、通常、Microsoft 365 管理センターを使用してユーザー設定を管理します。
ユーザー管理者は現在、Microsoft 365 管理センターを使用してライセンスを手動で割り当てています。次の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
ロンドンオフィスのユーザーは、Microsoft 365 管理センターを使用して手動でライセンスを割り当てることができます。以下の例外を除き、すべてのユーザーにライセンスが割り当てられています。
ロンドン オフィスのユーザーには、Microsoft 365 電話システム ライセンスが割り当てられていません。
シアトル オフィスのユーザーには、Yammer Enterprise ライセンスが割り当てられていません。
Contoso.com ではセキュリティの既定値が無効になっています。
Contoso は、Azure AD Privileged Identity Management (PIM) を使用してプロジェクト管理者ロールを実行します。
問題ステートメント
Contoso は次の問題を特定しています。
* 現在、すべてのヘルプデスク管理者は、Microsoft 365 テナント全体のユーザー ライセンスを管理できます。
* ユーザー管理者は、Contoso オフィスごとに異なるライセンス要件を手動で構成するのは面倒だと報告しています。

* ヘルプデスク管理者は、必要な Microsoft 365 サービスとアプリへの内部アクセスとゲスト アクセスのプロビジョニングに多くの時間を費やしています。
* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
* Azure AD でログ ノードを選択すると、Log Analytics 統合が有効になっていないことを示すエラー メッセージが表示されます。
計画された変更
Contoso は次の変更を実装する予定です。
セルフサービスパスワードリセット（SSPR）を実装します。Azure Monitorを使用してAzure監査アクティビティログを分析し、テナントに追加された新規ユーザーへのライセンス割り当てを簡素化します。Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施します。ユーザー管理者ロールを構成し、アクティベーションに正当な理由と承認が必要になります。
App1 という名前のカスタム基幹業務 Azure Web アプリを実装します。App1 はインターネットからアクセスでき、Azure AD アカウントを使用して認証されます。
マーケティング部門の新規ユーザーに対して、自動承認ワークフローを実装して、Microsoft SharePoint Online サイト、グループ、アプリへのアクセスを提供します。
Contoso社はCorporation社という会社を買収する予定です。AdatumというActive Directory組織単位（OU）に、新たにA Datumユーザー100名が作成されます。ユーザーはロンドンとシアトルに拠点を置く予定です。
技術要件
Contoso では、次の技術要件を特定しています。
* AH ユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には、https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのみのライセンスを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。

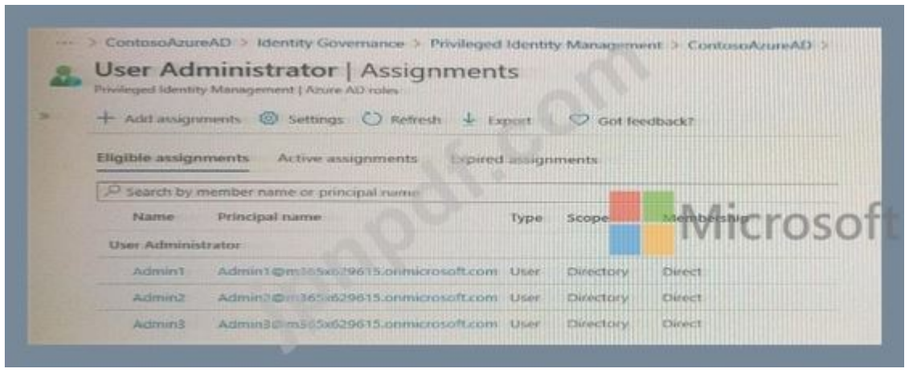
最新問題: 70
Microsoft 365 テナントがあります。
条件付きアクセス ポリシーは、条件付きアクセス ポリシーの図に示されているように構成します。([条件付きアクセス ポリシー] タブをクリックします。)



ユーザー管理者ロールの設定は、"ロール設定の詳細"の図のように表示されます。("ロール設定の詳細"タブをクリックします。)

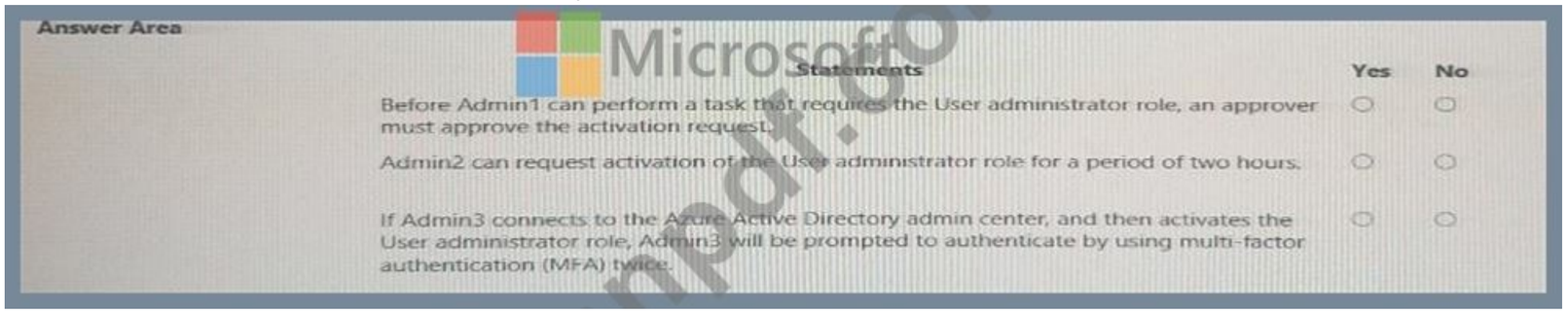


"ロールの割り当て"展示に示されているように、ユーザー管理者ロールの割り当てを表示します。("ロールの割り当て"ラボをクリックします。)

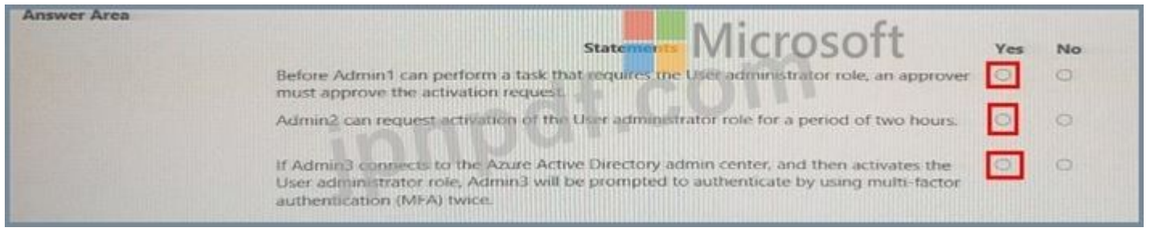


以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **71**

シミュレーション

必要に応じて次のログイン資格情報を使用します。

ユーザー名を入力するには、「サインイン」ボックスにカーソルを置き、下のユーザー名をクリックします。

パスワードを入力するには、「パスワードを入力」ボックスにカーソルを置き、下のパスワードをクリックします。

Microsoft 365 ユーザー名:admin@XXYyz112233.onmicrosoft.com

Microsoft 365 パスワード: =1122334455667788

Microsoft 365 ポータルがブラウザーに正常に読み込まれない場合は、Ctrl キーを押しながら K キーを押して、新しいブラウザー タブにポータルを再度読み込みます。

以下の情報は技術サポートのみを目的としています。

ラボインスタンス: 99999999

sg-Legal グループのユーザーがテナントによって管理されるクラウド アプリにアクセスするときは、12 時間ごとに再認証を行うようにする必要があります。

このタスクを完了するには、適切な管理センターにサインインします。

Answer:

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

Sign-in frequency control
Step 1: Sign in to the Microsoft Entra admin center as at least a Conditional Access Administrator.

Step 2: Browse to Protection > Conditional Access.

Step 3: Select Create new policy.

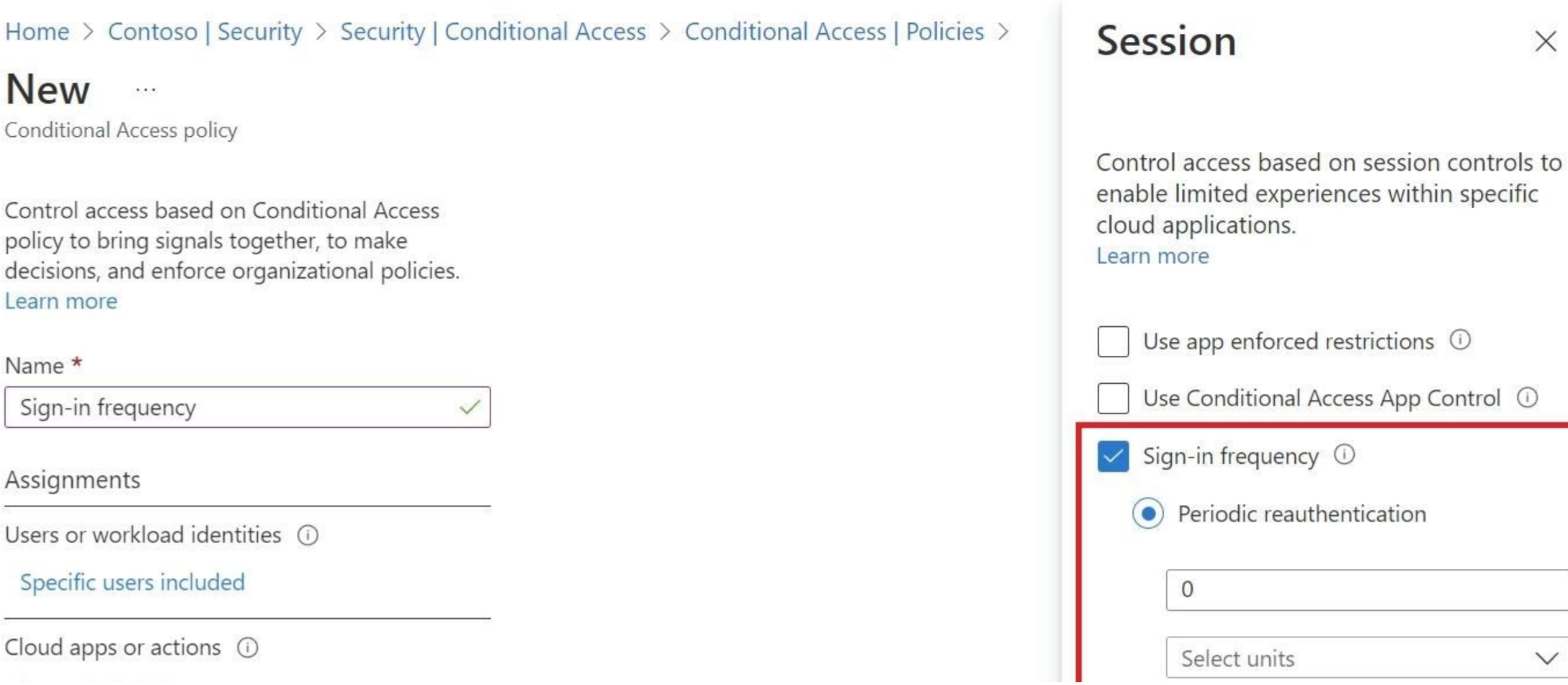
Step 4: Give your policy a name. We recommend that organizations create a meaningful standard for the names of their policies.

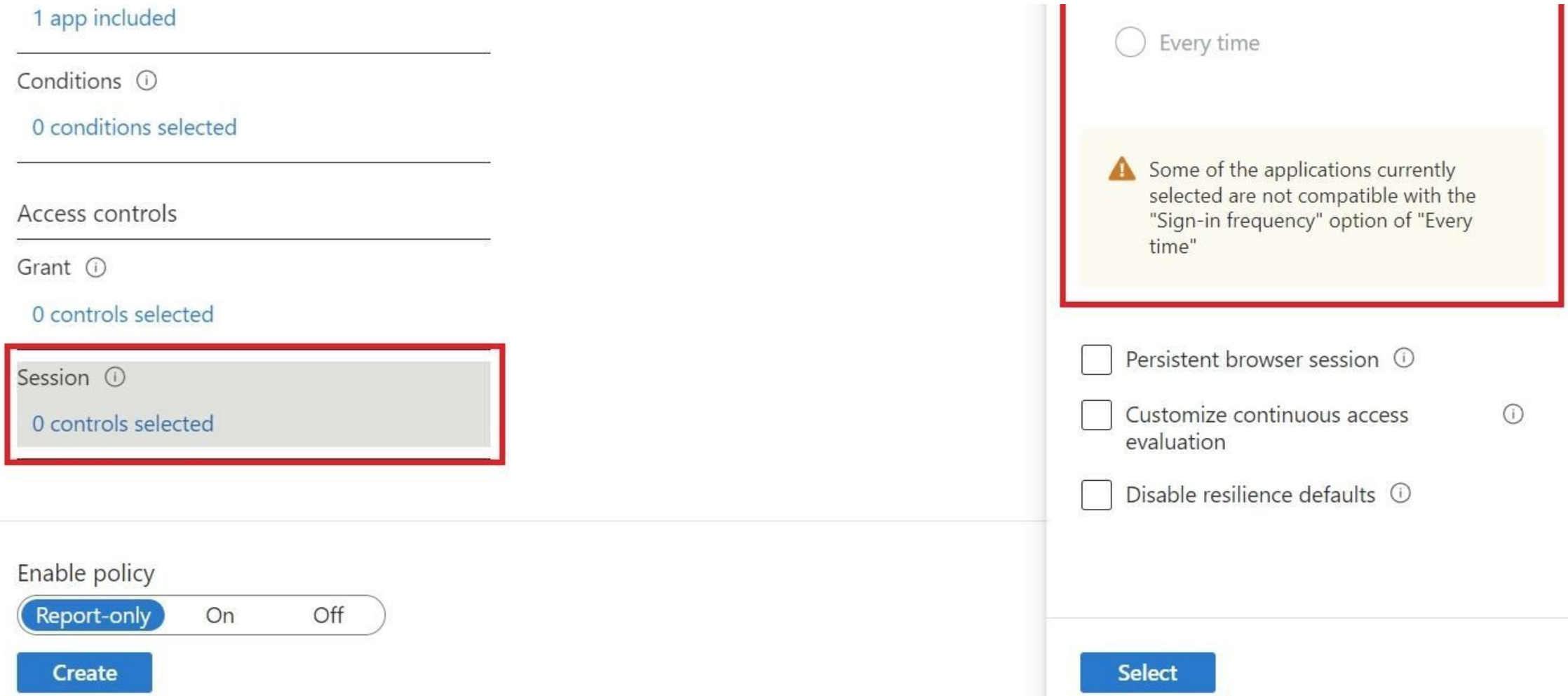
Step 5: Choose all required conditions for customer's environment, including the target cloud apps.

Step 6: Under Access controls > Session.

Step 6a: Select Sign-in frequency.

Step 6b: Choose Periodic reauthentication and enter a value of hours or days [Specify 12 hours: 12 + Hours as Unit] or select Every time.





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

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

Step 7: Click Create, and save your policy.

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

最新問題**: 72**
Microsoft 365 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 Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。

ユーザーが開始していない MFA リクエストを報告した場合、その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) のユーザーのブロック/ブロック解除設定を構成します。
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**)**
不正行為警告設定を構成する必要があります。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

最新問題**: 73**
次のオブジェクトを含む Azure Active Directory (Azure AD) テナントがあります。
* Device1という名前のデバイス
* User1、User2、User3、User4、User5という名前のユーザー
* Group1、Group2、Group3、Group4、Group5という名前のグループ
グループは次の表のように構成されます。

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

Microsoft Office 365 Enterprise E5 ライセンスを直接割り当てることができるのはどのグループですか?
A. グループ1とグループ4のみ
B. グループ1、グループ2、グループ3、グループ4、およびグループ5
C. グループ1とグループ2のみ
D. グループ1のみ
E. グループ1、グループ2、グループ4、グループ5のみ
Answer: C (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

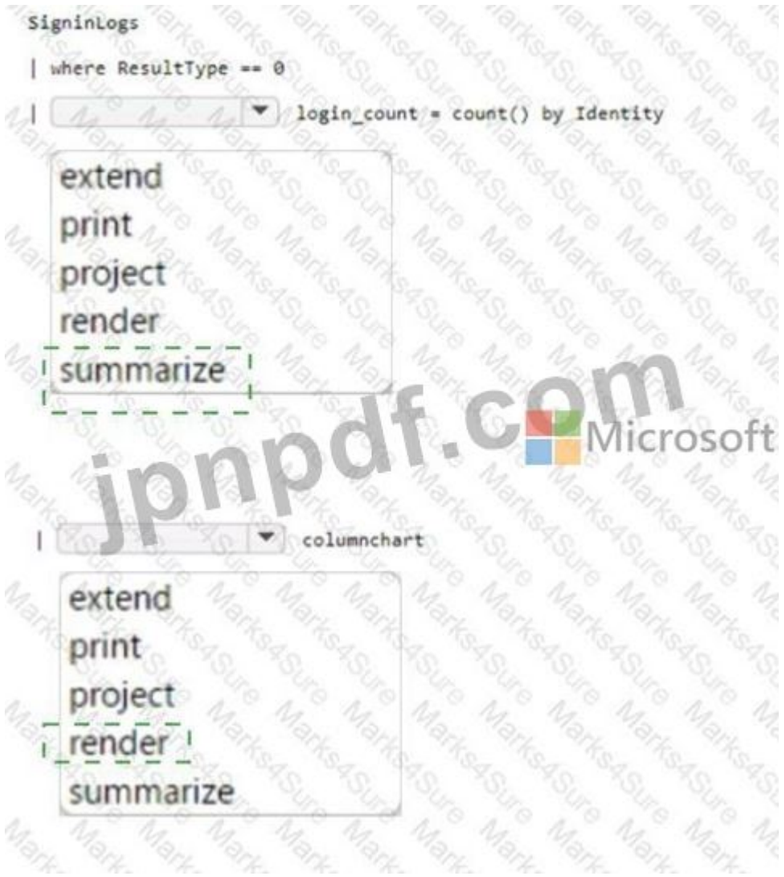
最新問題**: 74**
Appl という名前のエンタープライズ アプリケーションを含む contoso.com という名前の Microsoft Entra テナントがあります。
請負業者は user1@outlook.com の資格情報を使用します。
請負業者にApp1へのアクセスを提供できることを確認する必要があります。請負業者はuser1 @outlook.comとして認証できる必要があります。
何をすべきでしょうか?
A. New-Mguserコマンドレットを実行する
B. New-MgInvitationコマンドレットを実行します。
C. 外部コラボレーション設定を構成する
D. Microsoft Entra Connect 同期を実装します。
Answer: (解答を表示する**)**
外部ユーザー (請負業者など) にエンタープライズ アプリケーションなどの Microsoft Entra リソースへのアクセスを許可する場合、正しい方法は、そのユーザーをゲスト ユーザーとして招待することで

す。
Microsoft SC-300 学習ガイドには次のように記載されています。
既存のアカウント（Outlook.com、Gmail、または他のEntraテナントなど）を使用して認証する外部ユーザーと共同作業を行うには、Microsoft Graph APIまたはNew-MgInvitation PowerShellコマンドレットを使用して、ゲストユーザーとして招待する必要があります。このシナリオでは、請負業者は個人用のMicrosoftアカウントであるuser1@outlook.comを使用します。New-MgInvitationコマンドレットは、認証のために外部IDにリンクするゲストユーザーをテナントに作成します。

最新問題: **75**
Azure サブスクリプションをお持ちです。
Azure AD ログは Log Analytics ワークスペースに送信されます。
ログをクエリし、ユーザーごとのサインイン数をグラフで表示する必要があります。
クエリ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。



Answer:



jpnpdf.com
Microsoft

Explanation:
ボックス1
サインインログ
| ResultType == 0 の場合
| login_count = count() を ID 別に集計する
| 円グラフをレンダリングする
このクエリは、サインイン ログを取得し、成功したサインインをフィルターし、ユーザーごとのサインイン数を集計し、結果を円グラフとして表示します。
ボックス2 = レンダリング

最新問題: **76**
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。

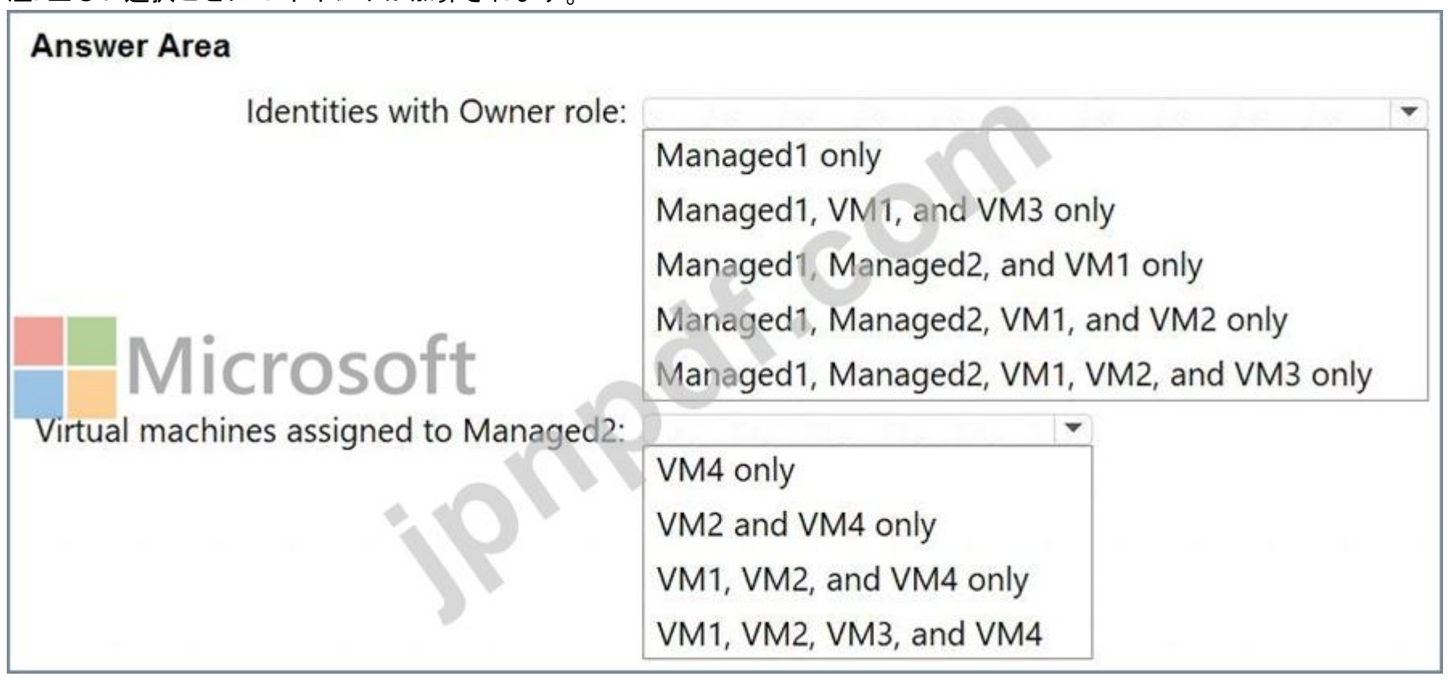
Name	Type	Location
RG1	Resource group	East US
Managed1	Managed identity	East US
Managed2	Managed identity	West US

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。

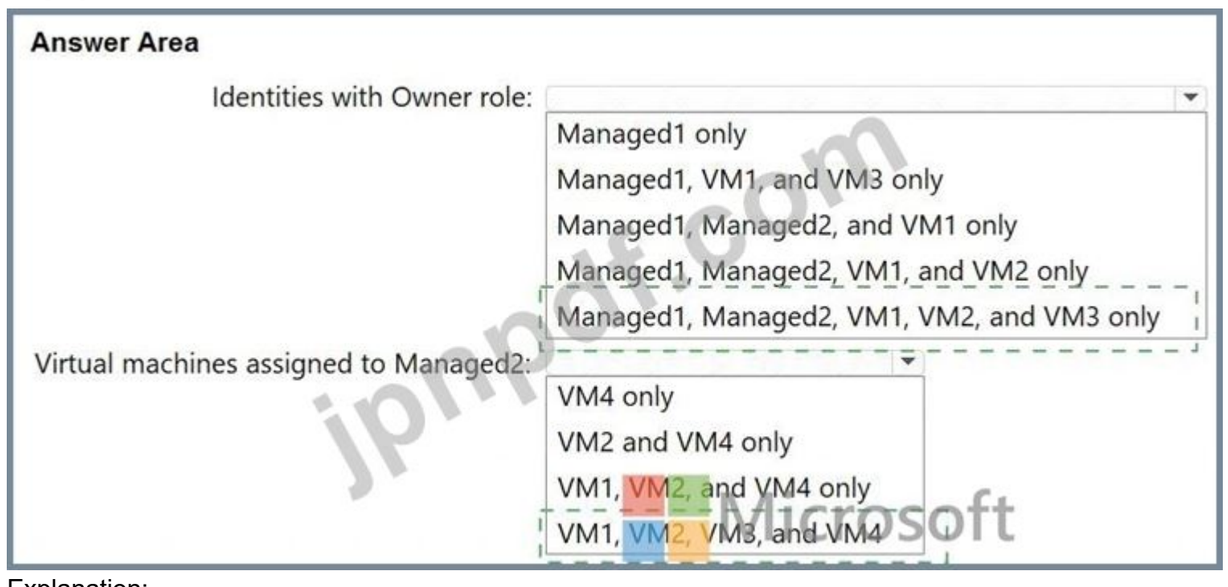


Name	Location	Identity
VM1	East US	System-assigned
VM2	West US	System-assigned
VM3	East US	Managed1
VM4	West US	None

RG1 の所有者ロールを割り当てることができる ID はどれですか。また、Managed2 を割り当てることができる仮想マシンはどれですか。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: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

ボックス1:Managed1、Managed2、VM1、VM2、VM3

Box2: VM1、VM2、VM3、VM4 この記事では、マネージド ID を複数の地域にわたって使用できることを確認します。
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-faq

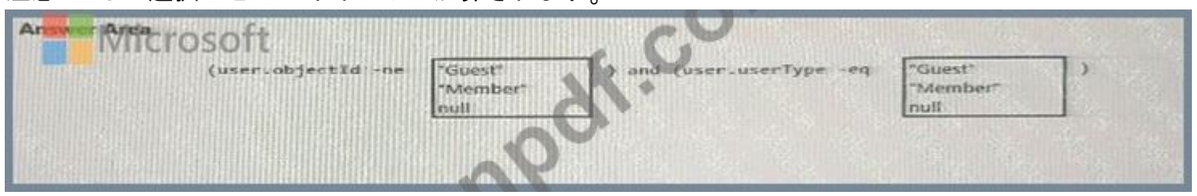
有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **77**
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や携帯電話の接続環境が整っていない遠隔地から頻繁に作業を行います。遠隔地で作業する際、ユーザーはノートパソコン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。
ユーザーはリモート ロケーションからどの MFA 認証方法を使用できますか?
A. Microsoft Authenticator アプリからの通知
B. アプリパスワード
C. Windows Hello for Business
D. SMS
Answer: C (メーッセージを残す)
Windows 10 では、Windows Hello for Business が PC とモバイルデバイスにおけるパスワードの代わりに強力な 2 要素認証を導入します。この認証は、デバイスに紐付けられ、生体認証または PIN を使用する新しいタイプのユーザー資格情報で構成されます。
登録時にユーザーの初期2段階認証を行うと、ユーザーのデバイスにWindows Helloがセットアップされ、Windowsはユーザーにジェスチャー（指紋などの生体認証やPINなど）の設定を求めます。ユーザーはジェスチャーを入力することで本人確認を行います。その後、WindowsはWindows Helloを使用してユーザーを認証します。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

最新問題: **78**
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がない遠隔地から作業することがよくあります。
ユーザーは、遠隔地から作業する際、インターネットにアクセスできる有線ネットワークにラップトップを接続します。
多要素認証 (MFA) を実装する予定です。
ユーザーはリモート ロケーションからどの MFA 認証方法を使用できますか?
A. Microsoft Authenticator アプリからの確認コード
B. セキュリティに関する質問
C. 音声
D. SMS

Answer: A (メッセージを残す)
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#

最新問題: **79**
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はどのように完成させるべきでしょうか？答えは、適切な値を正しいターゲットにドラッグすることです。各値は1回、複数回、または全く使用されない場合があります。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:
ヌル
"メンバー"

最新問題: **80**
ホットスポットに関する質問
Sub1 と Sub2 という 2 つの Azure サブスクリプションがあり、これらは Microsoft Entra テナントにリンクされています。テナントには、Group1、Group2、Group3 という 3 つのグループが含まれています。
サブスクリプションには、次の表に示すリソースが含まれています。

Name	Type	Subscription
VM1	Virtual machine	Sub1
VM2	Virtual machine	Sub2
Automation1	Azure Automation account	Sub2

テナントには次の表に示すユーザーが含まれます。

Name	Member of
User1	Group1
User2	Group2, Group3
User3	Group3

サブスクリプションの管理は、Microsoft Entra Permissions Management を使用します。Permissions Management は、次の表に示すように構成されています。

Name	Roles	Authorization System Name	Requestor for Other Identities
Group1	Viewer	Sub1	*None*
Group2	Controller	Sub2	User1
Group3	Approver	All Current and Future	*None*

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 ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can request access to VM2 by using Permissions Management.	○	○
User2 can create an access request to Automation1 on behalf of User1.	○	○
User3 can approve access requests for VM2.	○	○

jpnpdf.com
Microsoft

Answer:

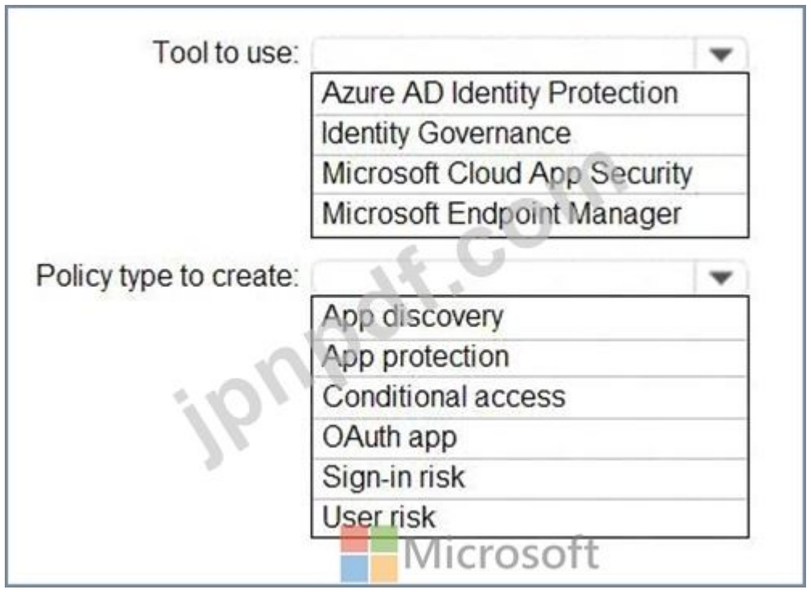
Answer Area

Statements	Yes	No
User1 can request access to VM2 by using Permissions Management.	○	●
User2 can create an access request to Automation1 on behalf of User1.	○	●
User3 can approve access requests for VM2.	●	○

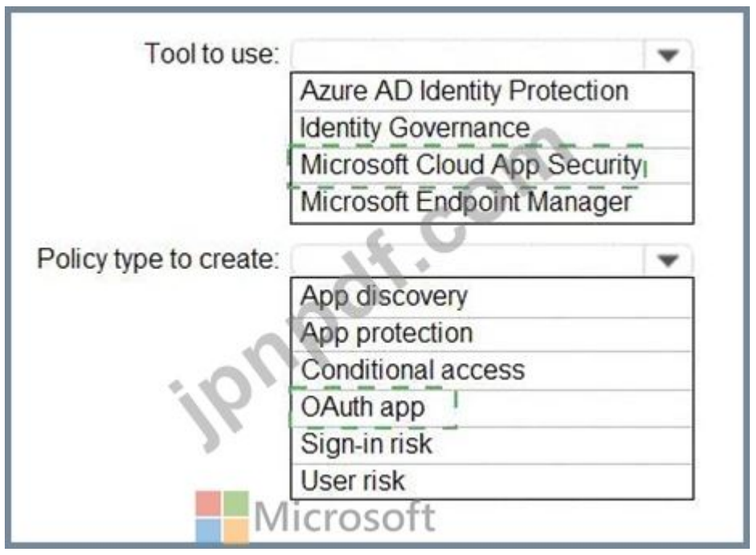
jpnpdf.com
Microsoft

Explanation:
いいえ - User1 は、sub1 へのアクセスをリクエストできるグループに属していますが、sub2 へのアクセスをリクエストすることはできません。いいえ - User1 は、user2 ではなく他の ID に代わって Sub1 へのアクセスをリクエストできます。はい - User3 のグループは、すべてのサブスクリプションへのアクセス リクエストを承認できます。

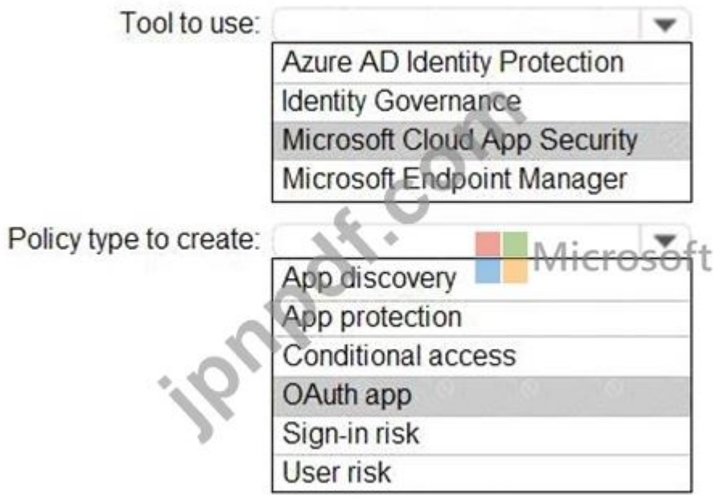
最新問題**: 81**
Microsoft 365 テナントがあります。
ユーザーは、Microsoft 365 データへの限定的なアクセスを必要とする外部のサードパーティ製アプリケーションを使用する場合があります。ユーザーは、これらのアプリケーションを Azure Active Directory (Azure AD) に登録します。
登録されたアプリケーションがユーザーの電子メールへの読み取りおよび書き込みアクセス権を取得した場合にアラートを受信する必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



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

最新問題**: 82**
contoso.com という名前の Azure AD テナントがあり、このテナントには All Company という名前のグループが含まれており、次の Identity Governance 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することをブロックする: 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 名称: All Company
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の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 リーダー ロールを 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。
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 ポイントが加算されます。

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:

Answer Area

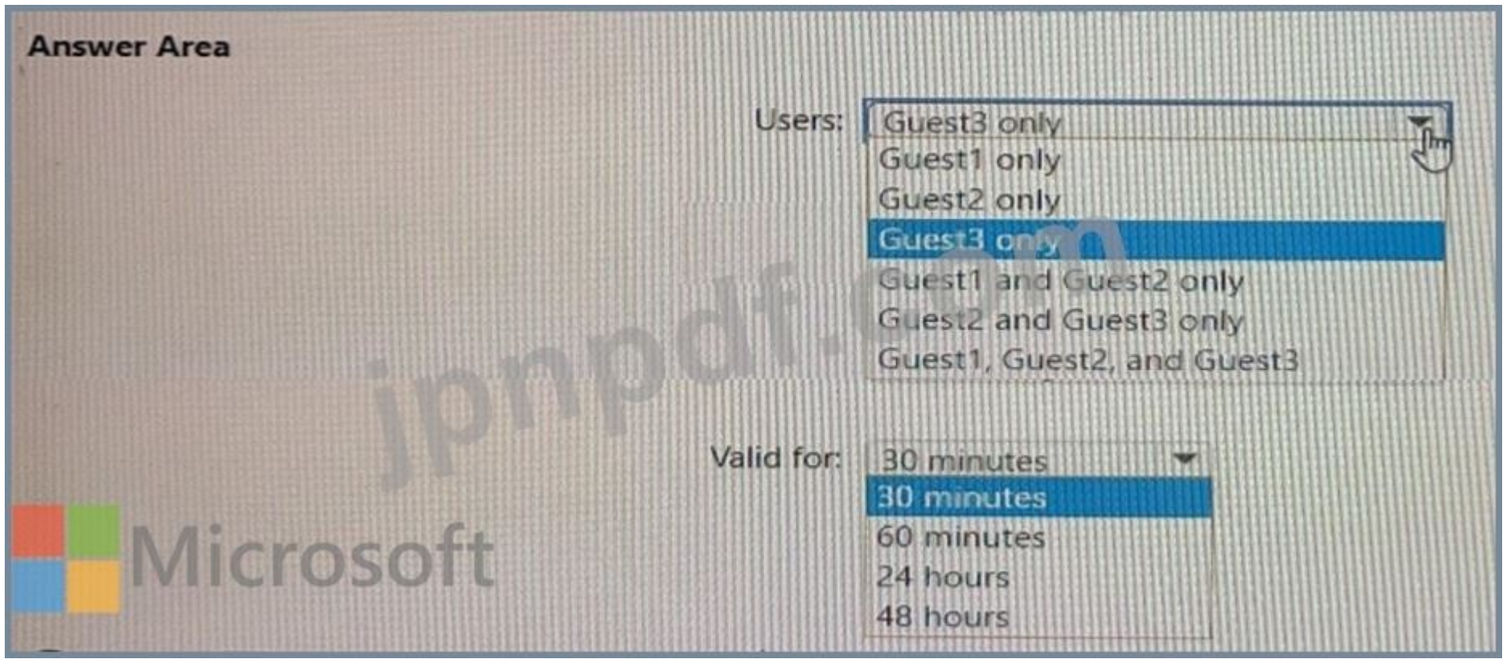
Statements	Yes	No
On May 5, 2022, the Guest1 account is in contoso.com.	○	●
On May 5, 2022, the Guest2 account is in contoso.com.	○	●
On May 5, 2022, the Guest3 account is in contoso.com.	●	○

最新問題: 83

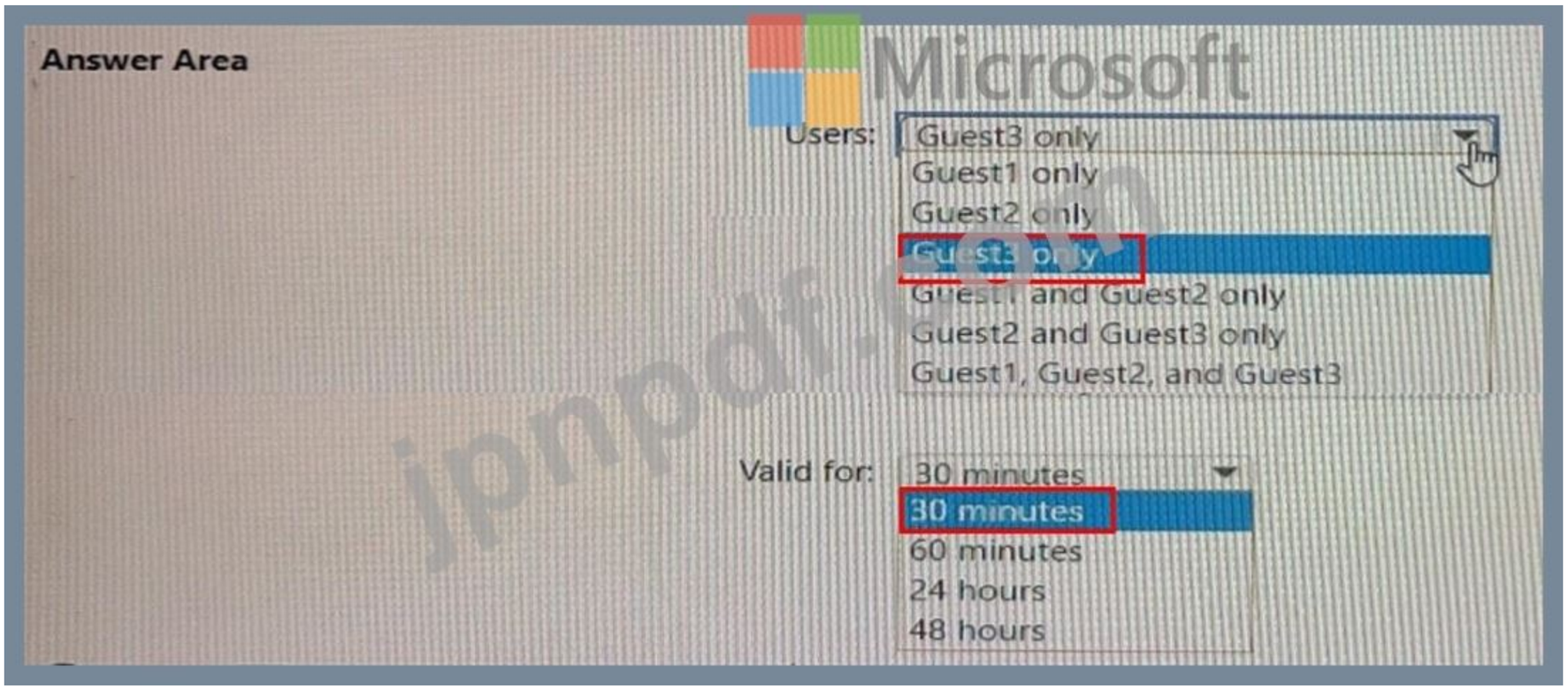
contoso.com という名前の Azure AD テナントがあり、ゲスト用のワンタイム パスコードを電子メールで送信することが [はい] に設定されています。
次の表に示すゲスト ユーザーを招待します。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

ワンタイム パスコードを受け取るユーザーは誰ですか? また、パスコードの有効期間はどのくらいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **84**

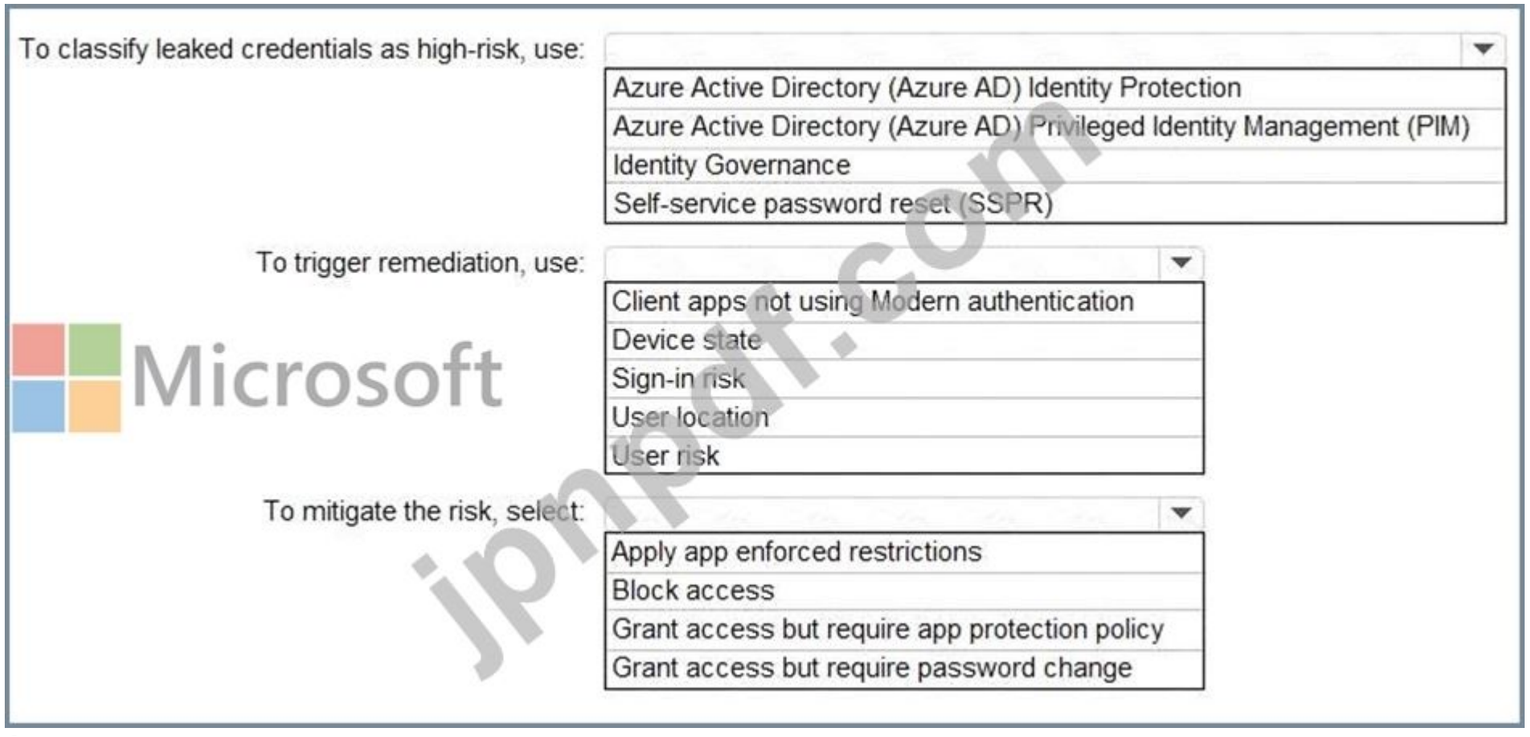
Microsoft 365 テナントがあります。

資格情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。

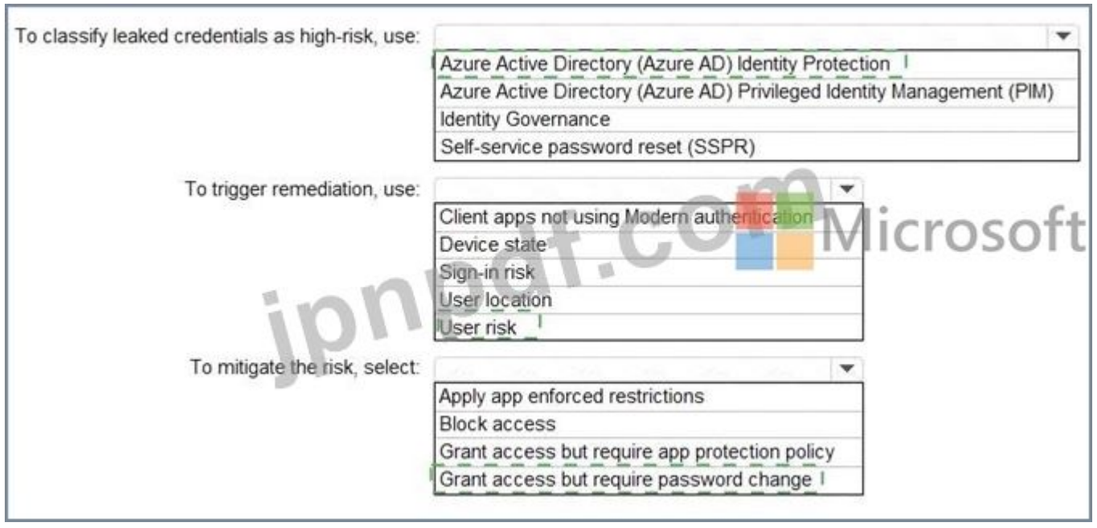
* 資格情報が漏洩した疑いのあるユーザーによる ID サインイン。
* サインインを高リスクイベントとして禁止します。
* ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。

何を使うべきでしょうか? 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。

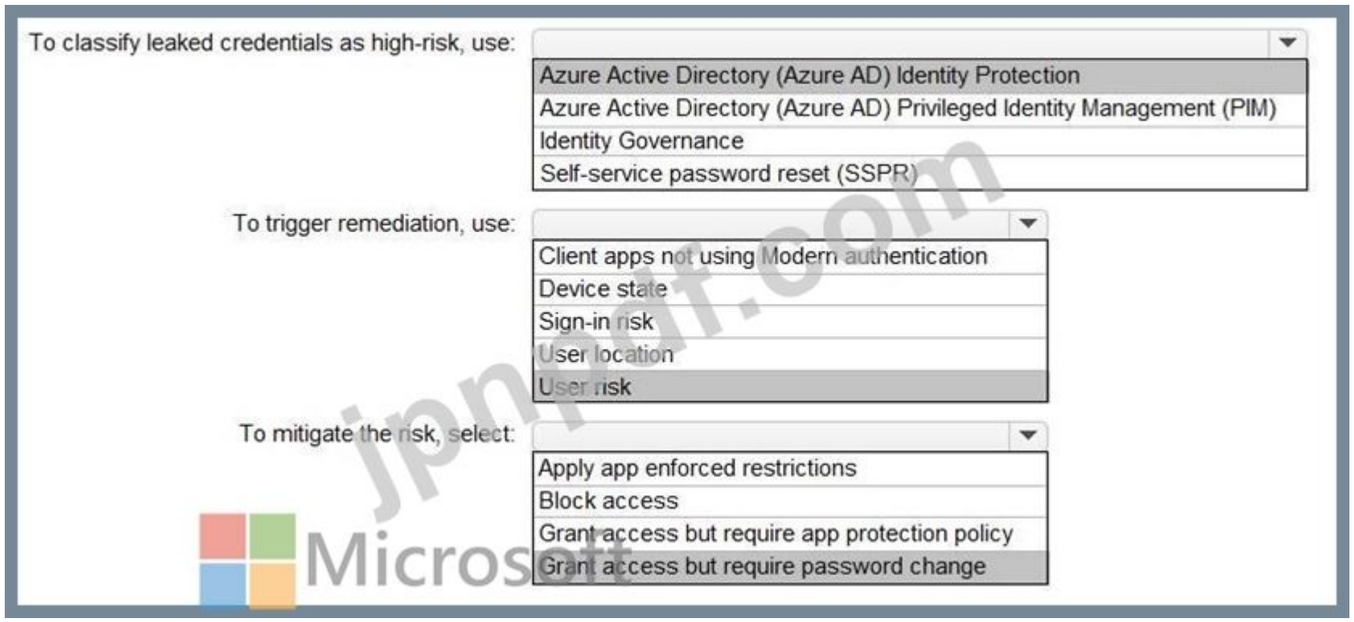
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

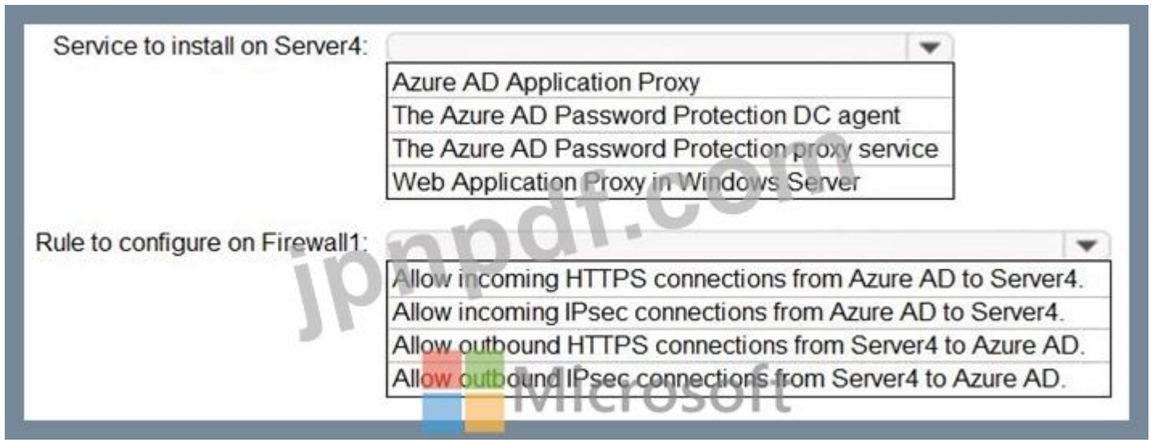


参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

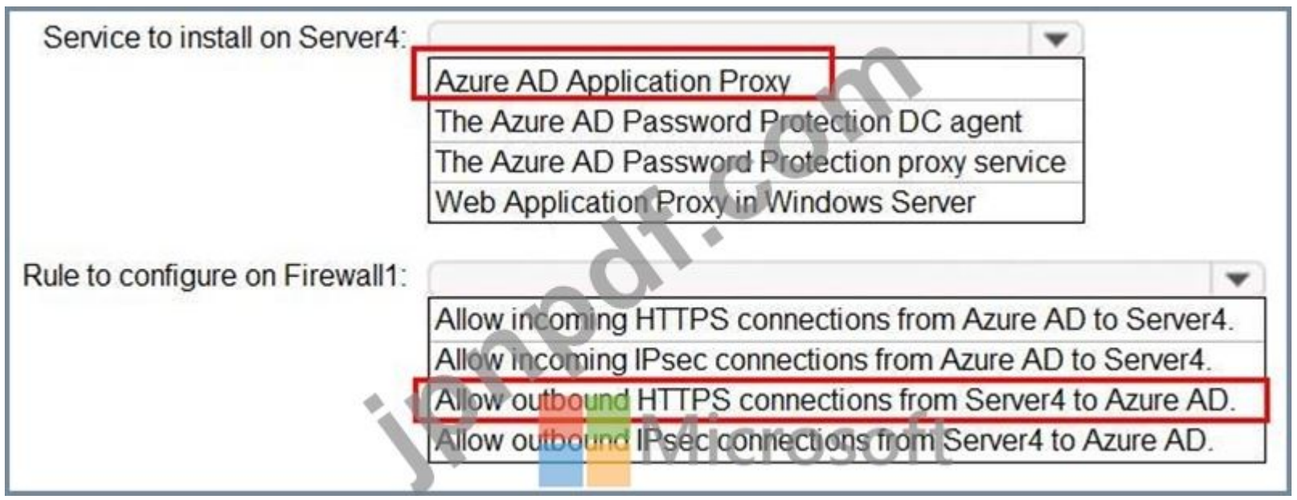
最新問題**: 85**
次の表に示すホストを含むオンプレミス データセンターがあります。

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

Active Directory フォレストと同期する Azure Active 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 Azure AD ユーザーに公開できることを確認する必要があります。
Server と Firewall1 で何を設定す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



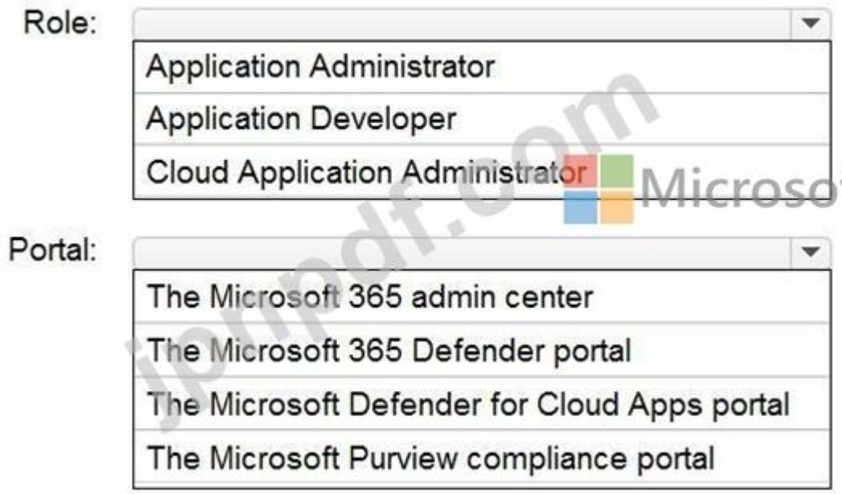
Answer:



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

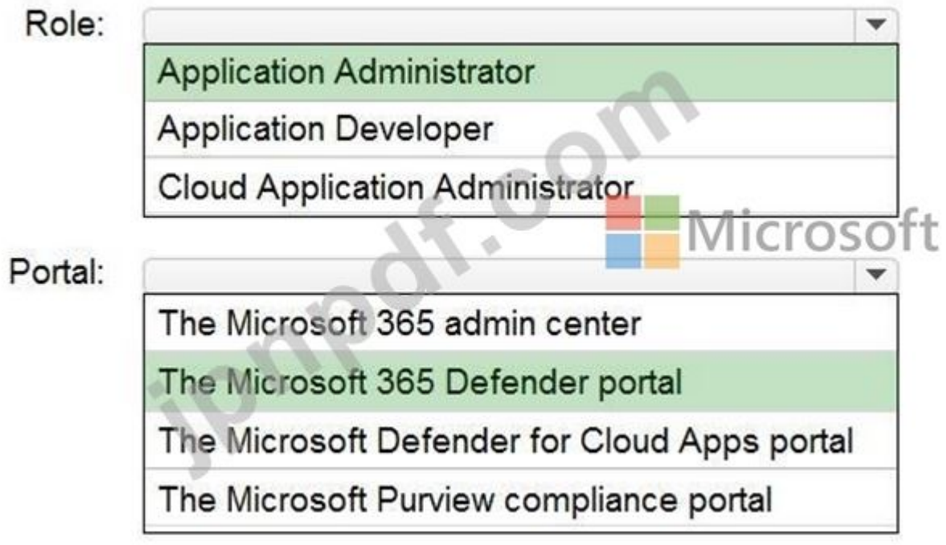
最新問題**: 86**
ホットスポットに関する質問
User1 という名前のユーザーを含む Microsoft 365 E5 サブスクリプションがあります。
アプリ ガバナンスの統合を構成します。
ユーザー1はアプリガバナンスダッシュボードを表示する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
User1 にはどのロールを割り当てる必要がありますか? また、User1 はダッシュボードを表示するためにどのポータルを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:

Answer Area

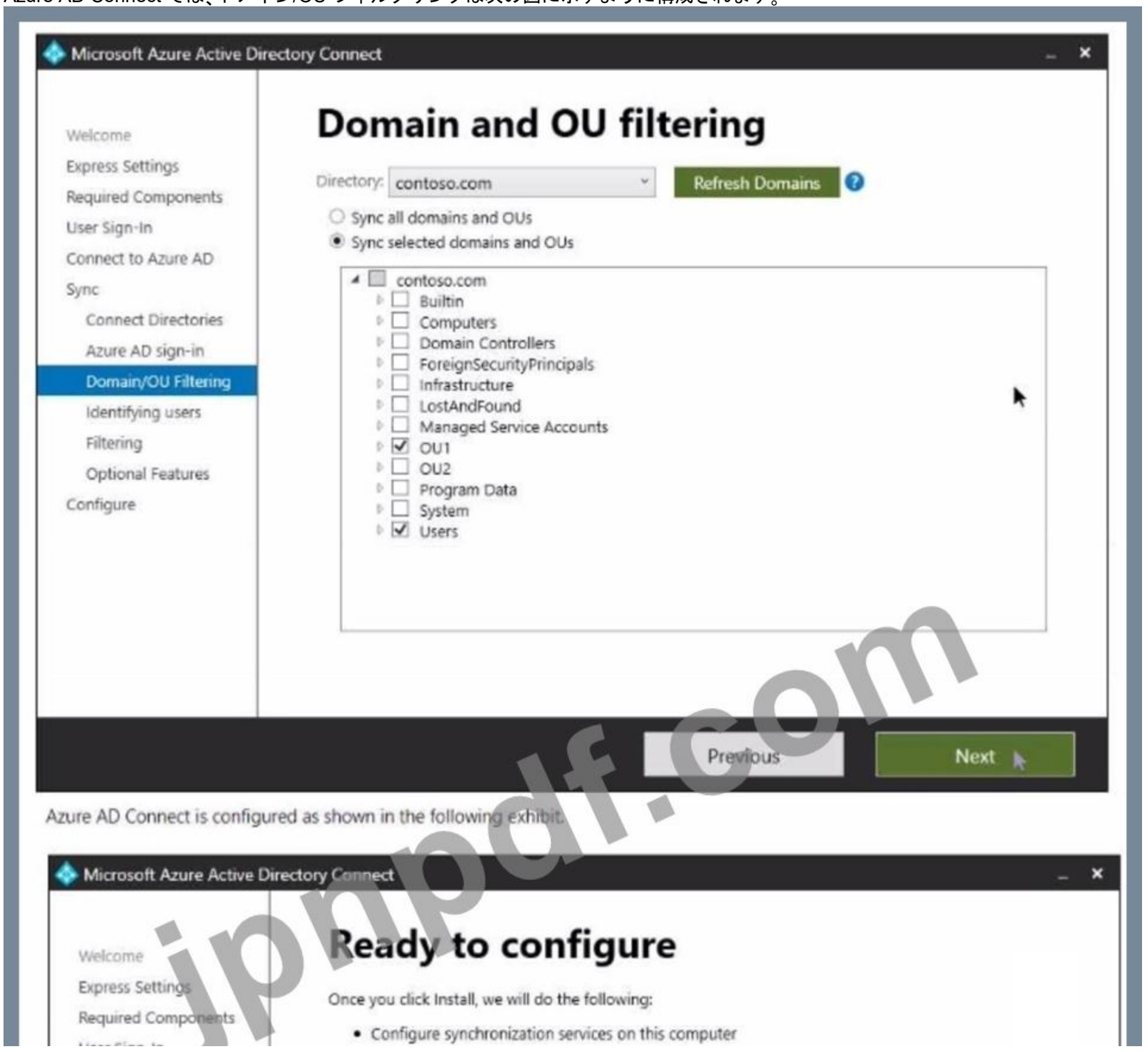


Explanation:
https://learn.microsoft.com/en-us/defender-cloud-apps/app-governance-get-started#roles

最新問題: 87
ネットワークには、Azure AD と同期し、次の表に示すユーザーを含むオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

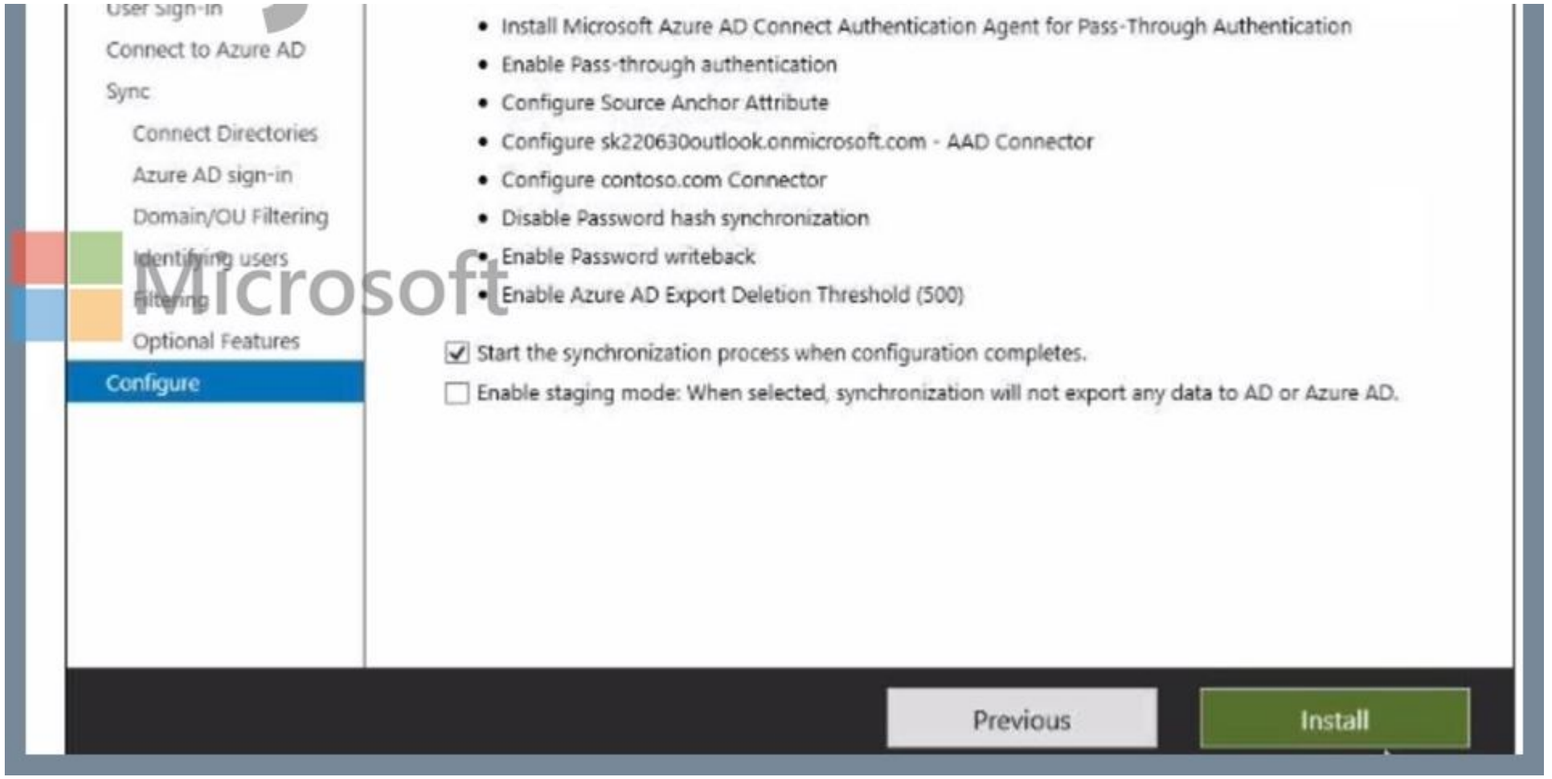
Name	Organizational unit (OU)
User1	OU1
User2	OU2

Azure AD Connect では、ドメイン/OU フィルタリングは次の図に示すように構成されます。



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

jpnpdf.com



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 ポイントが加算されます。



Answer:



Explanation:

最新問題: **88**

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 Azure Active 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

グループAとグループBに追加できるメンバーは誰ですか？ 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。

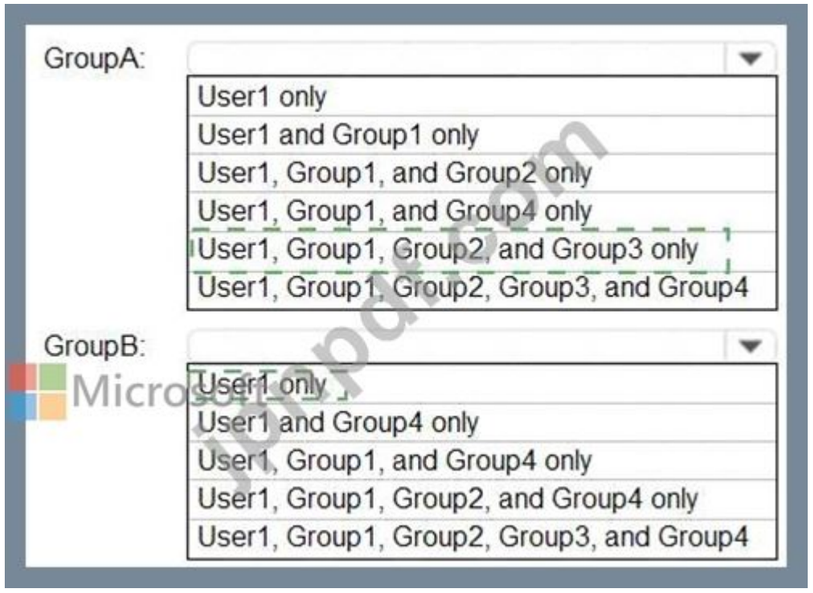
GroupA:

- 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

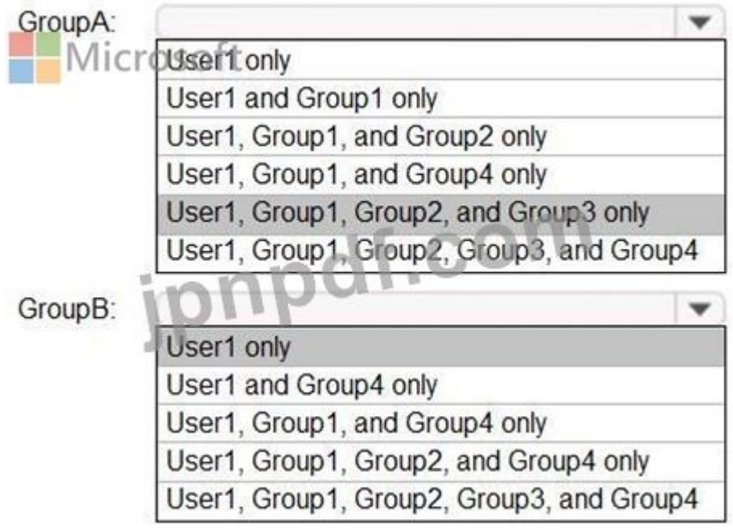
GroupB:

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

Answer:

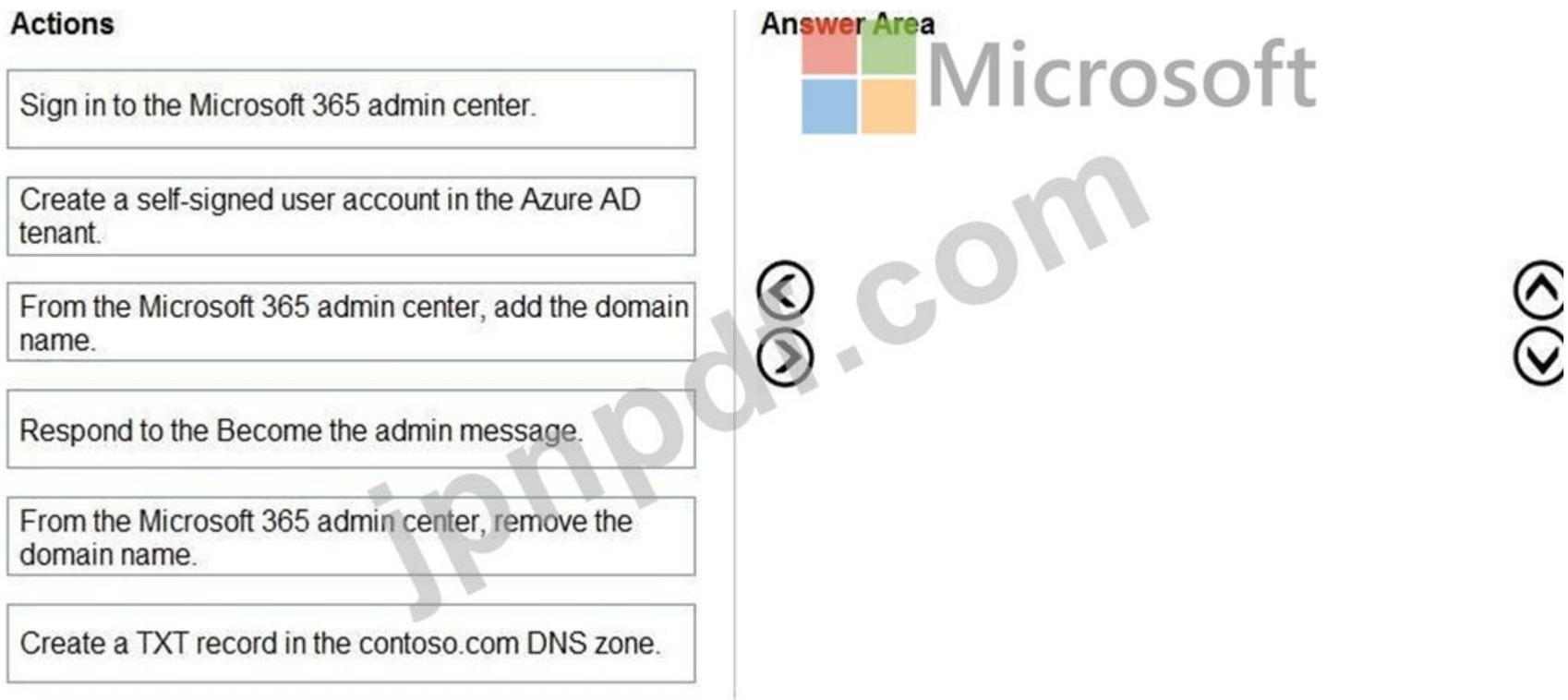


説明

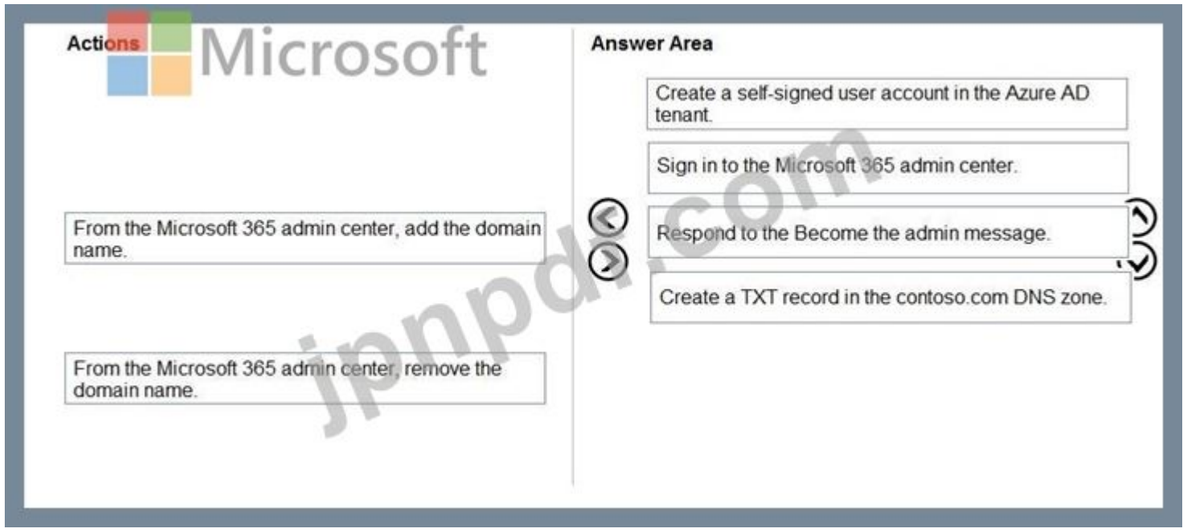


参照：
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

最新問題**: 89**
ドラッグアンドドロップの質問
contoso.com の SMTP アドレス スペースを使用するオンプレミスの Microsoft Exchange 組織があります。
ユーザーが Microsoft 365 サービスへのセルフサービス サインアップに自分のメール アドレスを使用していることがわかりました。
自己署名ユーザーが含まれる Azure Active Directory (Azure AD) テナントに対するグローバル管理者権限を取得する必要があります。
どの 4 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、適切なアクションをアクション 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:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-admin-takeover

最新問題**: 90**
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。

次のことを特定する必要があります。
* User1 のアカウントが削除されてから何日後にアカウントを復元できますか?
* 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?
何を特定すべきでしょうか？ 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：正解ごとに1ポイント獲得できます。



Answer:



Explanation:



最新問題: **91**
Active Directory フォレストと同期する Azure Active Directory (Azure AD) テナントがあります。テナントは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。
* サーバーには必要なソフトウェアのみを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。

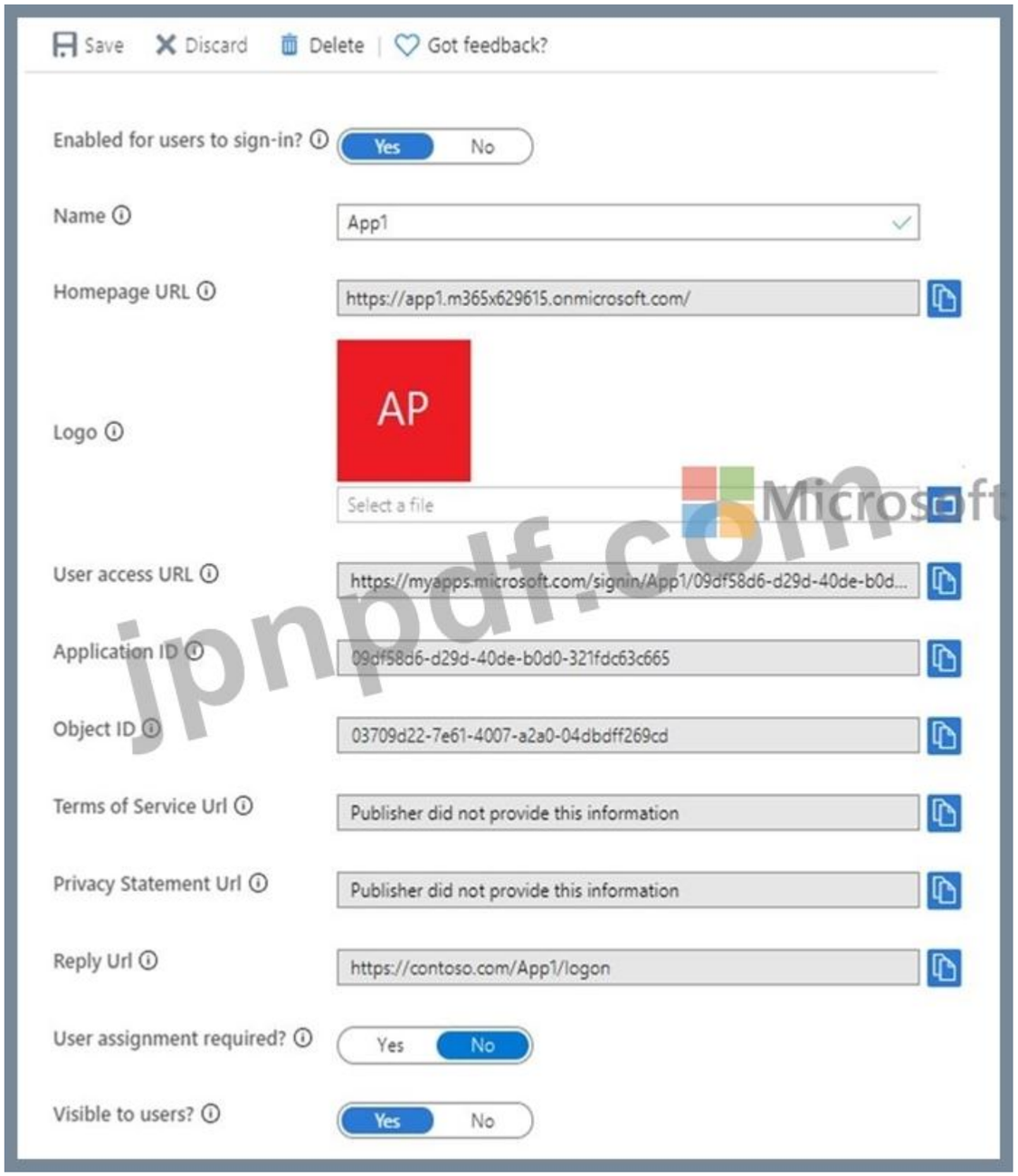
Name	Description
Server1	Domain controller (PDC emulator)
Server2	Domain controller (infrastructure master)
Server3	Azure AD Connect server
Server4	Unassigned member server

サーバーに障害が発生した場合でも、ユーザーが Azure AD 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. サーバー1
B. サーバー2
C. サーバー3
D. サーバー4
Answer: (解答を表示する**)**

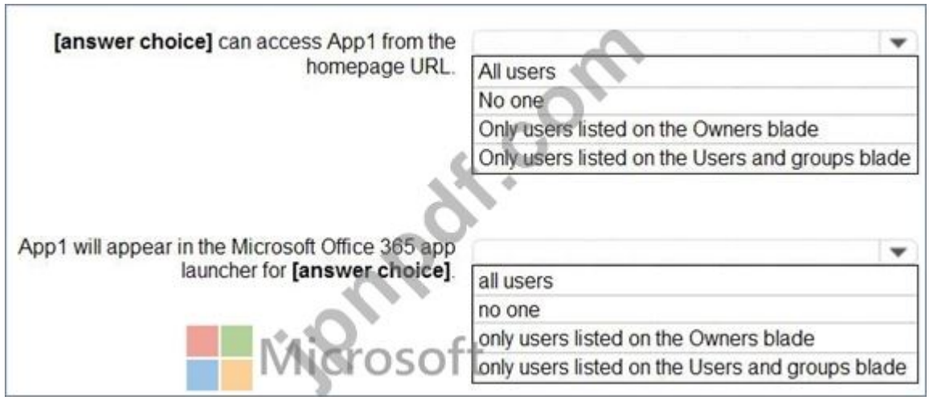
有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 92**
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、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

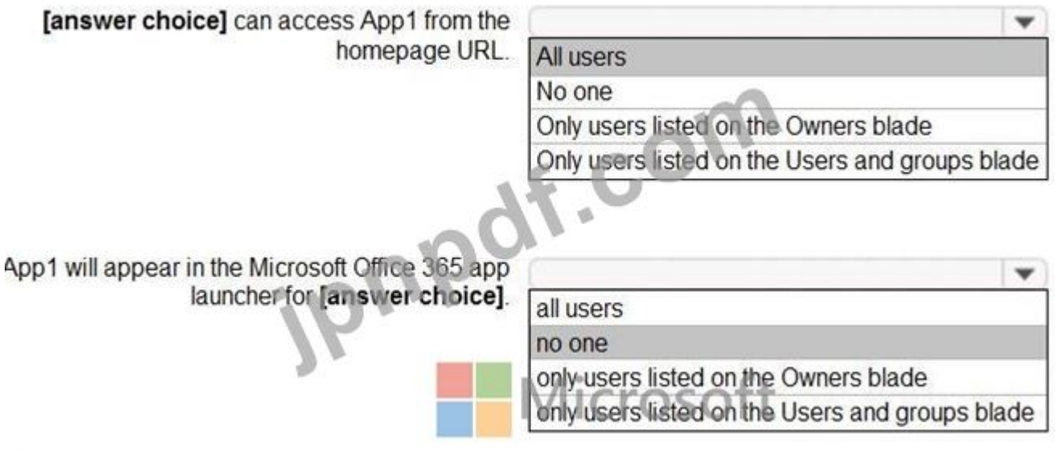
jpnpdf.com



Answer:



Explanation:



参照：

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/ユーザーまたはグループアクセスポータルの割り当て

最新問題**: 93**

ホットスポットに関する質問

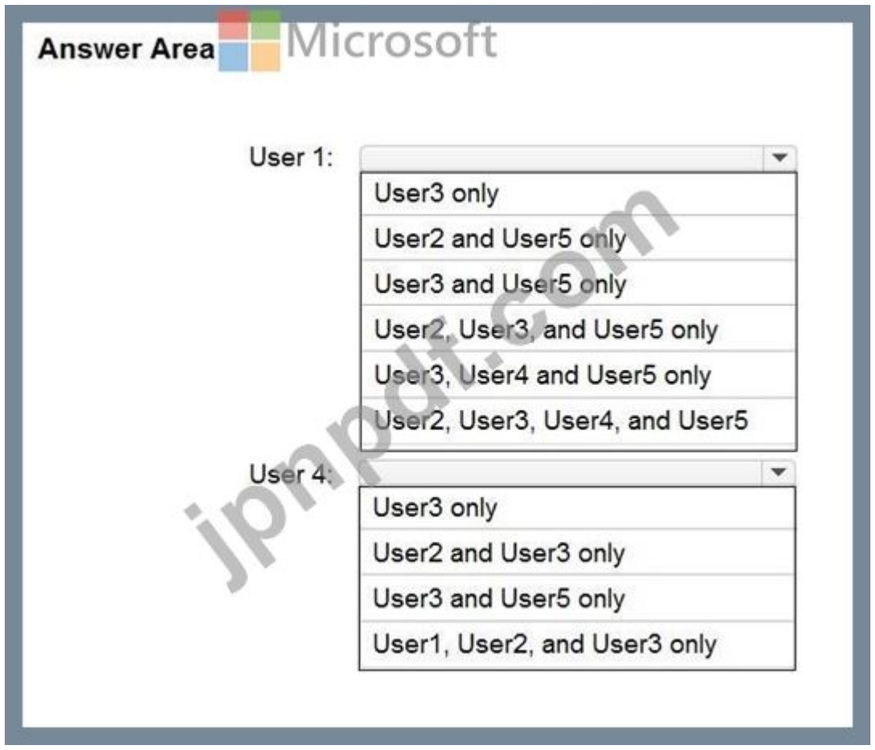
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

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、次の表に示すロール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 はどのユーザーのパスワードをリセットできますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

Answer Area

User 1:

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

User 4:

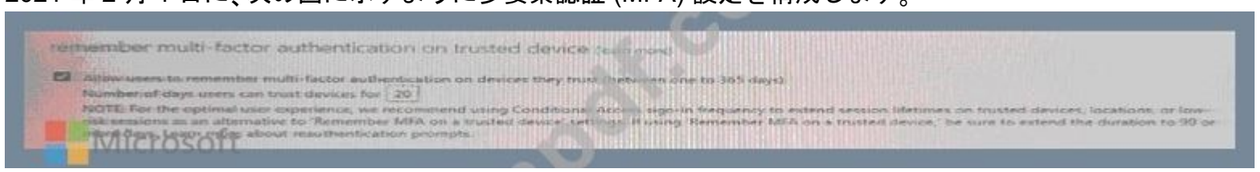
- User3 only
- User2 and User3 only
- User3 and User5 only
- User1, User2, and User3 only

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

最新問題**: 94**
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 へのユーザー認証。

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	Disabled
User2	Enabled
User3	Enforced

B.

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

C.

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

D.

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

Answer: C (メーッセージを残す**)**

最新問題**: 95**

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	Role
Admin1	Global Administrator
Admin2	Conditional Access Administrator
Admin3	Authentication Policy Administrator
Admin4	Global Administrator

Admin4 は、 Azure 管理に多要素認証を要求する」テンプレートを使用して、Policy1 という名前の条件付きアクセス ポリシーを作成します。

次回サインイン時に多要素認証 (MFA) の使用が求められるユーザーはどれですか?

A. Admin2とAdmin3のみ

B. Admin1とAdmin4のみ

C. Admin1、Admin2、Admin3のみ

D. 管理者1、管理者2、管理者3、管理者4

Answer: (解答を表示する**)**

包括的かつ詳細な説明：

Microsoft Identity and Access Administrator ドキュメントで説明されているように、Microsoft Entra ID 条件付きアクセス ポリシー、 Azure 管理には多要素認証が必要」テンプレート、およびユーザーに割り当てられたロールに基づいて、これを段階的に説明してみましょう。

Azure 管理に多要素認証を要求する」テンプレートについて理解する:

Microsoft Entra ID 条件付きアクセス ポリシーを使用すると、管理者は特定の条件に基づいて多要素認証 (MFA) を要求するなどのセキュリティ制御を適用できます。

Azure 管理に多要素認証を要求する」テンプレートは、Microsoft Entra ID の定義済み条件付きアクセス ポリシー テンプレートです。このテンプレートは、Azure ポータル、Azure PowerShell、Azure CLI、その他の Azure 管理エンドポイントなどの Azure 管理インターフェイスへのアクセスをセキュリティで保護するように設計されています。

テンプレートの主な詳細:

クラウドアプリまたはアクション: このテンプレートは Microsoft Azure 管理」クラウドアプリを対象としています。これにはすべての Azure 管理インターフェースが含まれますが、他のクラウドアプリ

Microsoft 365 アプリなど）には適用されません。
ユーザー: デフォルトでは、テンプレートは すべてのユーザー」に適用されますが、特定のユーザーまたはグループを追加または除外するように変更できます。質問では変更内容が指定されていないため、デフォルトの すべてのユーザー」が対象範囲であると想定します。
条件: 通常、変更されない限り、このテンプレートには特定の条件 (デバイスの状態、場所など) はありません。
許可制御: テンプレートは、アクセス制御として 多要素認証を要求する」ことを強制します。
したがって、このポリシーでは、Azure 管理インターフェイスにアクセスしようとするすべてのユーザーに対して MFA が要求されます。
ロールと Azure 管理との相互作用について理解する:
各ユーザーに割り当てられているロールと、それらのユーザーが Azure 管理インターフェイスと対話する可能性があるかどうかを確認しましょう。
管理者1: グローバル管理者
グローバル管理者には、Azure サブスクリプション、リソース、Azure ポータルを管理する機能を含む、すべての Microsoft Entra ID および Azure リソースへのフル アクセス権があります。
グローバル管理者は、管理タスクを実行するためにAzure管理インターフェース（Azureポータルなど）に頻繁にアクセスします。そのため、管理者1がAzure管理にアクセスするためにサインインする際には、条件付きアクセスポリシーが適用されます。
管理者2: 条件付きアクセス管理者
条件付きアクセス管理者は、Microsoft Entra ID で条件付きアクセス ポリシーを管理できますが、既定では Azure 管理インターフェイスに直接アクセスすることはできません。
このロールはMicrosoft Entra IDに重点を置いたものであり、Azureリソース管理には重点を置いていません。Admin2にAzureの追加ロール（共同作成者 所有者など）が付与されていない限り、Azure管理インターフェースにアクセスできない可能性があります。
質問では Admin2 の追加ロールは示されていないため、Azure 管理とやり取りしないものと想定します。
管理者3: 認証ポリシー管理者
認証ポリシー管理者は、Microsoft Entra ID の認証方法とポリシー (MFA 設定、パスワードレス認証など) を管理できます。
条件付きアクセス管理者と同様に、このロールはMicrosoft Entra IDに固有のものであり、デフォルトではAzure管理インターフェースへのアクセスを許可しません。Admin3は通常、追加のAzureロール（指定されていません）が割り当てられていない限り、Azure管理にアクセスできません。
管理者4: グローバル管理者
Admin1 と同様に、Admin4 はグローバル管理者であり、Azure 管理インターフェイスへのフルアクセス権を持ちます。
Admin4 は、Azure 管理にアクセスするときに条件付きアクセス ポリシーの対象となります。
条件付きアクセスポリシーの適用:
このポリシーは すべてのユーザー」(テンプレートの既定のスコープ) に適用され、 Microsoft Azure 管理」クラウド アプリを対象とします。
ポリシーでは、Azure 管理インターフェイスにアクセスするすべてのユーザーに対して MFA が要求されます。
Admin1 および Admin4 (グローバル管理者):
グローバル管理者として、Admin1 と Admin4 の両方が管理業務の一環として Azure 管理インターフェイス (Azure ポータルなど) にアクセスします。
次回 Azure 管理にアクセスするためにサインインすると、条件付きアクセス ポリシー (Policy1) によって MFA が適用されます。
Admin2 (条件付きアクセス管理者) と Admin3 (認証ポリシー管理者):
これらのロールは、本質的にAzure管理インターフェースへのアクセスを許可するものではありません。その責任は、条件付きアクセスポリシーや認証方法の管理など、Microsoft Entra ID関連のタスクに限定されます。
Admin2 または Admin3 が Azure 管理にアクセスしようとしない限り（デフォルトではアクセスが許可されていません）、このポリシーは適用されません。質問では 次回サインイン時」について尋ねられていますが、このポリシーでは対象のクラウドアプリ（Microsoft Azure 管理）にアクセスした場合にのみ MFA がトリガーされます。Admin2 と Admin3 が Microsoft Entra ID またはその他のアプリ（例：Microsoft 365）にサインインした場合、このポリシーは適用されません。
オプションの分析:
A). Admin2 と Admin3 のみ:
不正解です。Admin2 と Admin3 は、役割に基づいて Azure 管理インターフェイスにアクセスする可能性は低いため、ポリシーでは MFA を必要としません。

B). Admin1 と Admin4 のみ:
正解です。Admin1 と Admin4 は、Azure 管理インターフェイスにアクセスするグローバル管理者であり、次回これらのインターフェイスにサインインするときに MFA を要求するポリシーがトリガーされます。
C). Admin1、Admin2、Admin3 のみ:
不正解です。上記の理由により、Admin2 と Admin3 はポリシーの対象ではありません。
D). 管理者1、管理者2、管理者3、および管理者4:
不正解です。ポリシーは「すべてのユーザー」に適用されますが、Azure 管理インターフェイスにアクセスする可能性があるのは Admin1 と Admin4 (グローバル管理者) のみで、MFA 要件がトリガーされます。
追加の考慮事項:
Admin2 または Admin3 に、Azure 管理へのアクセスを許可する追加の Azure ロール（例共同作成者、所有者）が割り当てられている場合、彼らもポリシーの対象となります。しかし、質問にはそのようなロールは示されていません。
「次回サインイン時」という表現は誤解を招く可能性があります。このポリシーは、ユーザーが対象のクラウドアプリ（Microsoft Azure Management）にサインインした場合にのみMFAを適用します。Admin2またはAdmin3が別のアプリ（例Microsoft 365）にサインインした場合、このポリシーは適用されません。
ポリシーが変更され、別のクラウドアプリ（例：「すべてのアプリ」）を対象とするように、または特定のユーザーを含めるように変更された場合、回答は変わる可能性があります。ただし、この質問では、テンプレートのデフォルトの動作が指定されています。
結論：「Azure管理に多要素認証を要求する」テンプレートを使用して作成された条件付きアクセスポリシー（ポリシー1）は、Azure管理インターフェースにアクセスするユーザーに多要素認証を要求します。ユーザーの役割に基づき、以下のようになります。
Admin1 と Admin4 (グローバル管理者) は、次回 Azure 管理にサインインするときに MFA を使用する必要があります。
Admin2 と Admin3 (条件付きアクセス管理者と認証ポリシー管理者) は Azure 管理にアクセスする可能性は低いため、ポリシーは適用されません。したがって、正解は B です。
参考文献:
Microsoft Entra ID 条件付きアクセスのドキュメント: 「一般的な条件付きアクセス ポリシー - Azure 管理に MFA が必要」(Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-policy-common#require-mfa-for-azure-management) Microsoft Entra ID ロールのドキュメント: 「Microsoft Entra ID の管理者ロールのアクセス許可」(Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference) 条件付きアクセス ポリシーと、特定のロールおよびクラウド アプリへのその適用について説明した、Microsoft Identity and Access Administrator (SC-300) 試験の学習ガイド。

最新問題: **96**
次の表に示すグループを含む Microsoft Entra テナントがあります。

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

グループに対して Privileged Identity Management (PIM) を実装する必要があります。
PIM を使用して管理できるグループはどれですか?
A. グループ1とグループ2のみ
B. グループ3とグループ4のみ
C. グループ1のみ
D. グループ1とグループ3のみ
E. グループ1、グループ2、グループ3、グループ4
Answer: (解答を表示する**)**

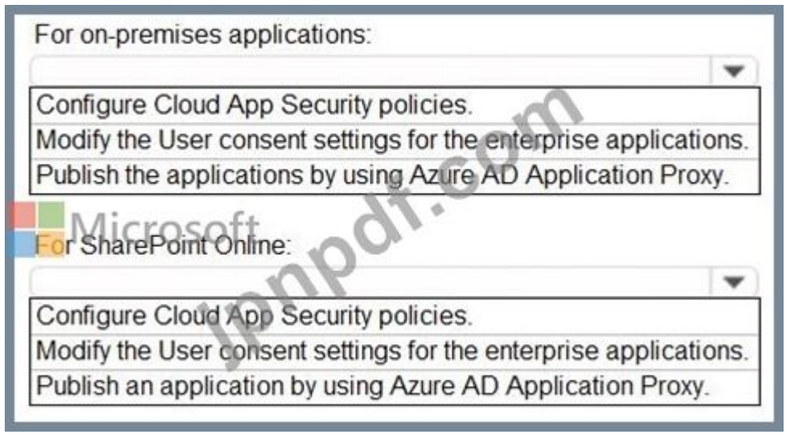
最新問題: **97**
Microsoft Entra テナントがあります。
サインイン失敗回数が 10 回を超えるとロックアウトしきい値が設定されるスマート ロックアウトを実装する必要があります。Microsoft Entra 管理センターで何を構成すればよいですか?
A. ユーザーリスクポリシー
B. パスワード保護
C. 認証の強度
D. サインインリスクポリシー
Answer: B (メーッセージを残す**)**
Microsoft SC-300 学習ガイドと Microsoft Learn モジュール 「スマート ロックアウトとパスワード保護の実装と管理」によると、スマート ロックアウトは Microsoft Entra Password Protection の機能であり、サインイン試行の失敗が繰り返されるとアカウントをロックアウトすることでブルート フォース攻撃を防ぐのに役立ちます。
Smart Lockout の構成には、次の 2 つの主要な設定が含まれます。
* ロックアウトしきい値 - アカウントがロックされるまでの失敗したサインインの回数。
* ロックアウト期間 - 別の試行が許可されるまでにアカウントがロックされている時間。
これらの設定は、ユーザーまたはサインイン リスク ポリシー (これらは Identity Protection の一部) や認証の強度ではなく、Entra 管理センターのパスワード保護で管理されます。
ロックアウトしきい値を 10 回のサインイン失敗に構成すると、要件を満たすことになります。

最新問題: **98**
次の表に示す Azure リソースがあります。

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

RG1 の Contributor ロールをどの ID に割り当てることができますか?
A. User1とGroup1のみ
B. ユーザー1、グループ1、VM1、およびApp1
C. User1、VM1、およびApp1のみ
D. User1とVM1のみ
E. ユーザー1のみ
Answer: B (メーッセージを残す**)**

最新問題: **99**
認証要件とアクセス要件を満たすには、オンプレミス アプリケーションと SharePoint Online の制限を実装する必要があります。
どうすればいいでしょうか? 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。



Answer:



最新問題: **100**
Microsoft 365 E5 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。
どの 4 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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

Actions

From Microsoft Cloud App Security, create a session policy.

Publish App1 in Azure Active Directory (Azure AD).

Create a conditional access policy that has session controls configured.

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

Answer Area

Publish App1 in Azure Active Directory (Azure AD).

From Microsoft Cloud App Security, modify the Connected apps settings for App1.

From Microsoft Cloud App Security, create a session policy.

Create a conditional access policy that has session controls configured.

Answer:

Answer Area

Publish App 1 in Azure Active Directory (Azure AD)

FROM Microsoft Cloud App Security , modify the Connected apps settings for App 1 .

From Microsoft Cloud App Security , create a session policy.

Create a conditional access policy that has session controls configured.

1 - Azure Active Directory (Azure AD) でアプリ 1 を公開する

2 - Microsoft Cloud App Security から、アプリ 1 の接続アプリの設定を変更します。

3 - Microsoft Cloud App Security からセッション ポリシーを作成します。
4 - セッション制御が構成された条件付きアクセス ポリシーを作成します。
参照：
https://docs.microsoft.com/en-us/cloud-app-security/proxy-deployment-any-app
https://docs.microsoft.com/ja-jp/cloud-app-security/session-policy-aad

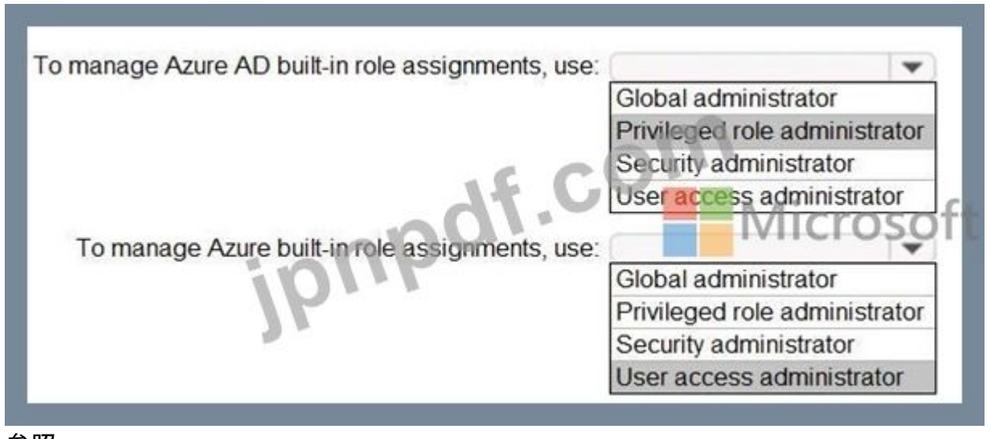
最新問題**: 101**
役割の割り当てを管理するために使用する役割を特定する必要があります。ソリューションは委任要件を満たす必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明



参照：
https://docs.microsoft.com/en-us/azure/ロールベースのアクセス制御/ロール割り当てポータル
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference
トピック1、Contoso株式会社
概要
Contoso 社は、モントリオールに本社を置き、ロンドンとシアトルにオフィスを構えるコンサルティング会社です。
Contoso は、Fabrikam, Inc という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。
既存の環境
Contoso 社のオンプレミスネットワークには、contos.com という Active Directory ドメインが含まれています。このドメインには、Contoso_Resources という組織単位 (OU) が含まれていま
す。Contoso_Resoureces OU には、すべてのユーザーとコンピューターが含まれています。
Contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

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 環境
Contoso には、次の関連ライセンスを持つ Contoso.com という名前の Azure AD テナントがあります。
* マイクロソフト Office 365 エンタープライズ E5
* エンタープライズモビリティ + セキュリティ
* Windows 10 エンタープライズ E5
* プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory Domain Serverless (AD DS) の間で構成されています。Contoso Resources OU のみが同期されます。
ヘルプデスク管理者は、通常、Microsoft 365 管理センターを使用してユーザー設定を管理します。
ユーザー管理者は現在、Microsoft 365 管理センターを使用してライセンスを手動で割り当てています。次の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
ロンドンオフィスのユーザーは、Microsoft 365 管理センターを使用して手動でライセンスを割り当てることができます。以下の例外を除き、すべてのユーザーにライセンスが割り当てられています。

* ロンドン オフィスのユーザーには、Microsoft 365 電話システム ライセンスが割り当てられていません。
* シアトル オフィスのユーザーには、Yammer Enterprise ライセンスが割り当てられていません。
Contoso.com ではセキュリティの既定値が無効になっています。
Contoso は、Azure AD Privileged Identity Management (PIM) を使用してプロジェクト管理者ロールを実行します。
問題ステートメント
Contoso は次の問題を特定しています。
* 現在、すべてのヘルプデスク管理者は、Microsoft 365 テナント全体のユーザー ライセンスを管理できます。
* ユーザー管理者は、Contoso オフィスごとに異なるライセンス要件を手動で構成するのは面倒だと報告しています。
* ヘルプデスク管理者は、必要な Microsoft 365 サービスとアプリへの内部アクセスとゲスト アクセスのプロビジョニングに多くの時間を費やしています。
* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
* Azure AD でログ ノードを選択すると、Log Analytics 統合が有効になっていないことを示すエラー メッセージが表示されます。
計画された変更
Contoso は次の変更を実装する予定です。
セルフサービス パスワード リセット (SSPR) を実装します。Azure Monitor を使用して Azure 監査アクティビティ ログを分析し、テナントに追加された新規ユーザーへのライセンス割り当てを簡素化します。Fabrikam のユーザーと協力して共同マーケティング キャンペーンを実施します。ユーザー管理者ロールを構成し、有効化に正当な理由と承認が必要になります。
App1 という名前のカスタム基幹業務 Azure Web アプリを実装します。App1 はインターネットからアクセスでき、Azure AD アカウントを使用して認証されます。
マーケティング部門の新規ユーザーに対して、自動承認ワークフローを実装して、Microsoft SharePoint Online サイト、グループ、アプリへのアクセスを提供します。
Contoso社はCorporation社という会社を買収する予定です。AdatumというActive Directory組織単位（OU）に、新たにA Datumユーザー100名が作成されます。ユーザーはロンドンとシアトルに拠点を置く予定です。
技術要件
Contoso では、次の技術要件を特定しています。
* AH ユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのみのライセンスを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。
トピック1、Litware社
概要
Litware, Inc.は、fabrikam, Inc.という子会社を持つ製薬会社です。Litwareはボストンとシアトルにオフィスを構えていますが、従業員は全米各地にいます。従業員はVPN接続を使用して、どちらのオフィスにもリモートで接続しています。
アイデンティティ環境
ネットワークには、litware.com という名前の Active Directory フォレストが含まれており、これは litware.com という名前の Azure Active Directory (Azure AD) テナントにリンクされています。Azure AD Connect はパススルー認証を使用し、パスワード ハッシュ同期は無効になっています。
Litware.com には、すべてのアプリケーション開発を監督する User1 というユーザーがいます。Litware は Azure AD アプリケーション プロキシを実装しています。
Fabrikam には fabrikam.com という Azure AD テナントがあります。Fabrikam のユーザーは、litware.com テナントのゲストアカウントを使用して litware.com のリソースにアクセスします。
クラウド環境
Litware の全ユーザーは Microsoft 365 Enterprise E5 ライセンスを保有しています。Microsoft Cloud App Security に組み込まれているすべての異常検出ポリシーが有効になっています。
Litware には、litware.com Azure AD テナントに関連付けられた Azure サブスクリプションがあります。このサブスクリプションには、Azure Active Directory コネクタと Office 365 コネクタを使用する

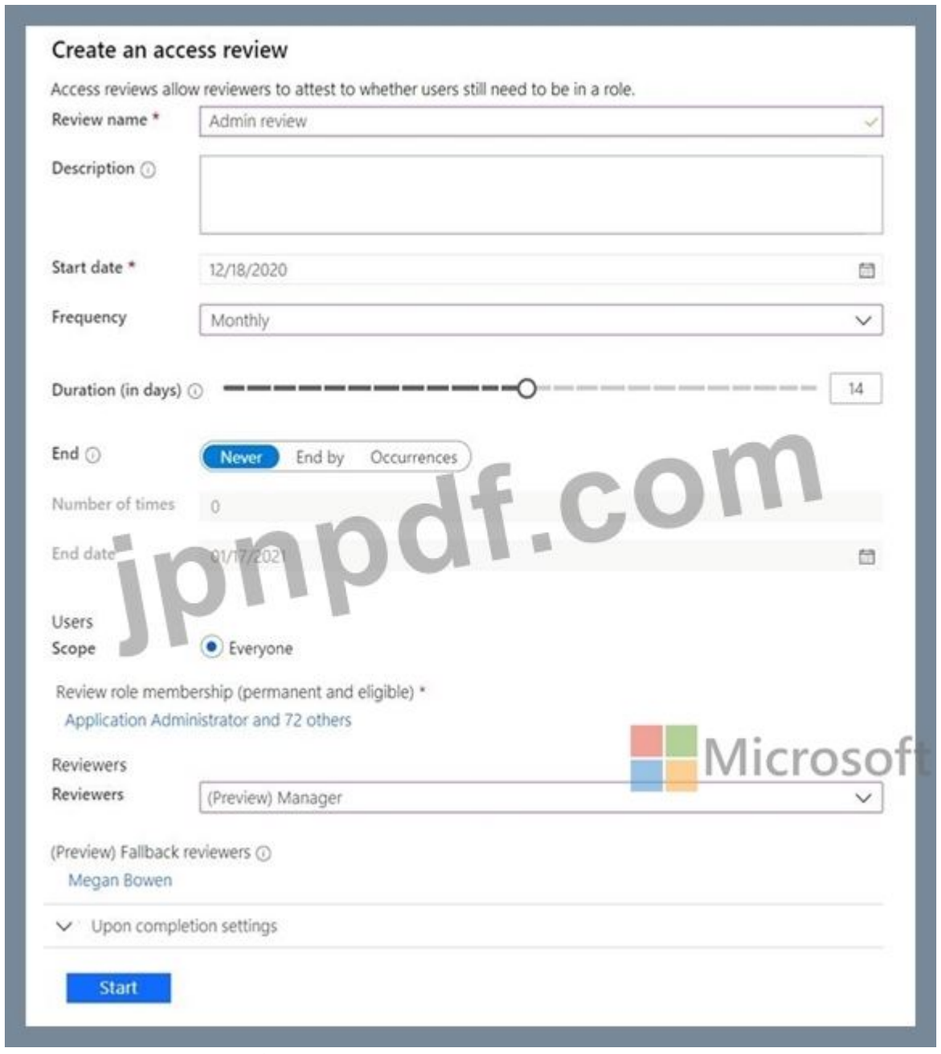
Azure Sentinel インスタンスが含まれています。
Azure Sentinel は現在、Azure AD サインイン ログと監査ログを収集します。
オンプレミス環境
オンプレミス ネットワークには、次の表に示すサーバーが含まれています。

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

Litwareの両オフィスはインターネットに直接接続しています。両オフィスは、サイト間VPN接続を使用してAzureサブスクリプション内の仮想ネットワークに接続しています。オンプレミスのすべてのドメインコントローラーは、インターネットへのアクセスをブロックされています。
委任要件
Litware では、次の委任要件が特定されています。
* Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
* 権限のないユーザーがlitware.com Azure ADテナントにアプリケーションを登録できないようにします。
* アイデンティティ ガバナンスにはカスタム カタログとカスタム プログラムを使用します。
* User1 が Azure AD でエンタープライズアプリケーションを作成できることを確認します。最小権限の原則を適用します。
ライセンス要件
Litware は最近、litware.com Active Directory フォレストに LWLicenses という名前のカスタム ユーザー属性を追加しました。
Litware は、LWLicenses 属性の値を変更することで、Azure AD ライセンスの割り当てを管理したいと考えています。LWLicenses に適切な値を持つユーザーは、適切なライセンスが割り当てられた Microsoft 365 グループに自動的に追加される必要があります。
管理要件
Litware は、Litware のすべての Azure AD ユーザー アカウントを含み、すべての Azure AD ゲスト アカウントを除外する LWGroup1 という名前のグループを作成したいと考えています。
認証要件
Litware では、次の認証要件が識別されます。
* すべての Litware ユーザーに対して多要素認証 (MFA) を実装します。
* Litware のボストン オフィスから Azure AD への認証に MFA を使用するユーザーを除外します。
* litware.com フォレストの禁止パスワード リストを実装します。
* オンプレミスのアプリケーションにアクセスするときに MFA を適用します。
* 外部に漏洩した資格情報を自動的に検出し、修復します
アクセス要件
Litware では、Litware のすべての Azure AD ユーザー アカウントを含み、すべての Azure AD ゲスト アカウントを除外する、LWGroup1 という名前のグループを作成したいと考えています。
監視要件
Litware は、Azure Sentinel の Fusion ルールを使用して、疑わしい Azure AD サインインとそれに続く異常な Microsoft Office 365 アクティビティの組み合わせを含むマルチステージの検出をしたいと考えています。

最新問題: **102**
AzureサブスクリプションにUser1というユーザーが登録されています。この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。User1にPermissions Managementへのアクセス権限を付与する必要があります。このソリューションは、以下の要件を満たす必要があります。
* 最小権限の原則に従ってください。
* 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. 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。
B. 権限管理の [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。
C. Microsoft Entra 管理センターから、User1 にロールを割り当てます。
D. 権限管理の [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。
Answer: C (メーッセージを残す)
Microsoft Entra Permissions Management (CIEMソリューション)へのオンボーディングでは、ユーザーがPermissions Management内の機能を実行する前に、Entraテナント内で適切なPermissions Managementロールを付与する必要があります。最小権限の原則に基づき、必要最小限のロール (Permissions Managementの承認者、閲覧者、管理者など)のみを付与する必要があります。SC-300の学習教材とMicrosoftのドキュメントでは、管理アクセスはEntra ID内でロールを割り当てることから始める必要があることが強調されています。
セキュリティ グループ (オプション A) を作成することは組織にとって便利な方法ですが、それだけでは権限管理内でユーザーに権限が付与されるわけではありません。
ロール/ポリシー テンプレート (オプション B) の作成は、権限スコープを定義することであり、ユーザー アクセスを許可するための最初のステップではありません。
[マイ リクエスト](オプション D) でリクエストを作成するには、User1 がリクエストを行う権限 (つまり、何らかのロール) をすでに持っていることが前提となりますが、実際にはまだその権限はありません。
したがって、最初のアクションは、Entra 管理センターから User1 に権限管理ロールを割り当て、最小限の権限を遵守しながら適切なアクセス権を付与することです。

最新問題: **103**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントがあります。
100 人の IT 管理者が 10 の部門に分かれて所属しています。
図に示すアクセス レビューを作成します。(図タブをクリックします。)



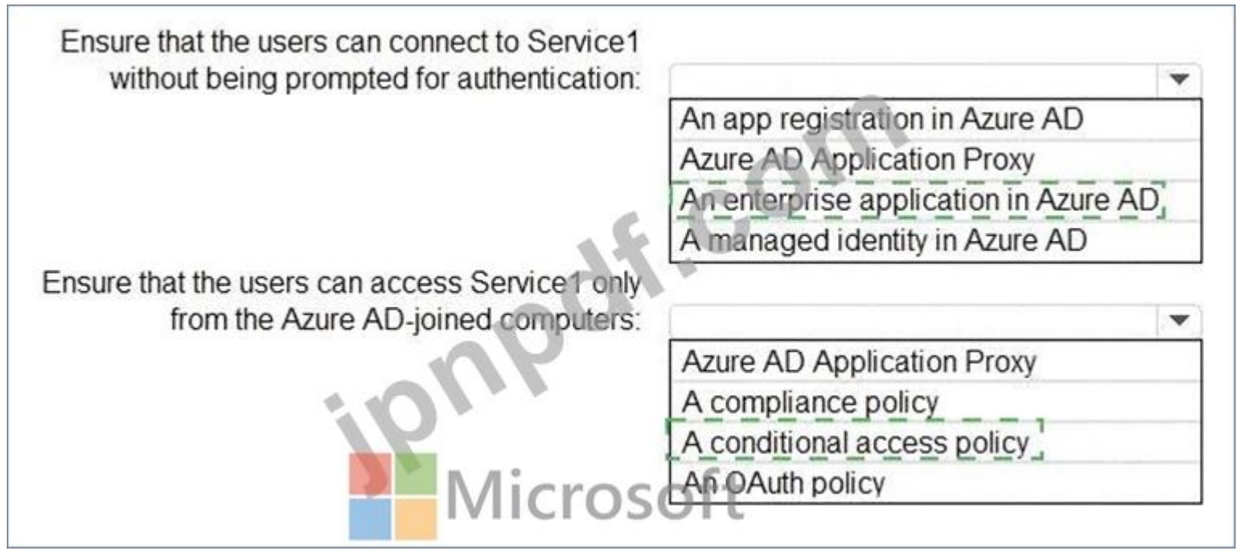
jpnpdf.com
Microsoft

すべてのアクセス レビュー リクエストは Megan Bowen 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れるようにする必要があります。
解決策: ロール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**)**
D18912E1457D5D1DDCBD40AB3BF70D5D
参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

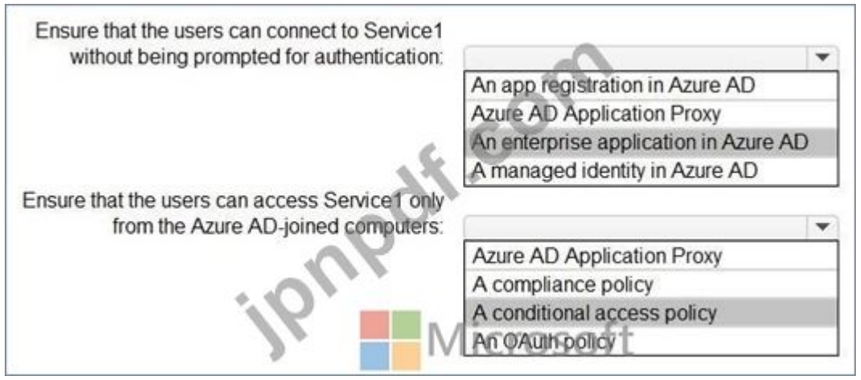
最新問題**: 104**
storage1 という名前のストレージ アカウントを含む Azure サブスクリプションがあります。
複数の仮想マシンでホストされるApp1というアプリを展開する予定です。仮想マシンは、シークレットを使用してサードパーティAPIに認証します。仮想マシン用の認証ソリューションを推奨する必要が

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ストレージサービス暗号化
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 Azure Key Vault
Answer: (解答を表示する**)**

最新問題**: 105**
会社には Microsoft 365 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所有しています。
会社はService1という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Azure AD認証と承認をサポートしています。Service1はAzure AD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、Azure ADに参加しているコンピューターからのみユーザーがService1にアクセスできるようにする必要があります。また、管理作業を最小限に抑える必要があります。
各要件に対して何を推奨しますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer:



Explanation:



参照：

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**: 106**

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。

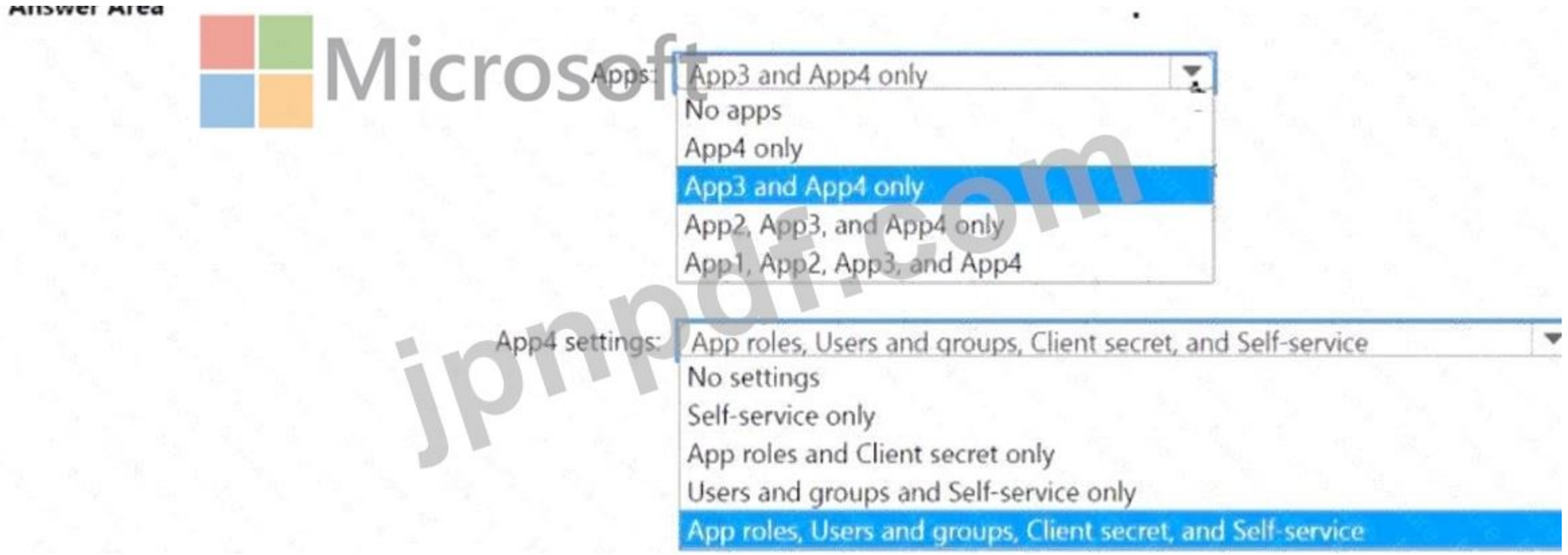
Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users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

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 107

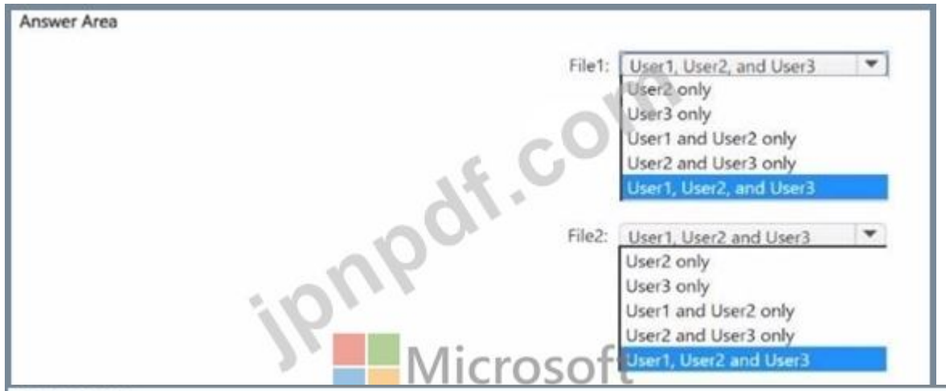
Sub1 という名前の Azure サブスクリプションがあり、そこには User1、User2、User3 という 3 人のユーザーが含まれています。Sub1 には storage1 という名前のストレージ アカウントがあり、次の表に示すリソースが含まれています。

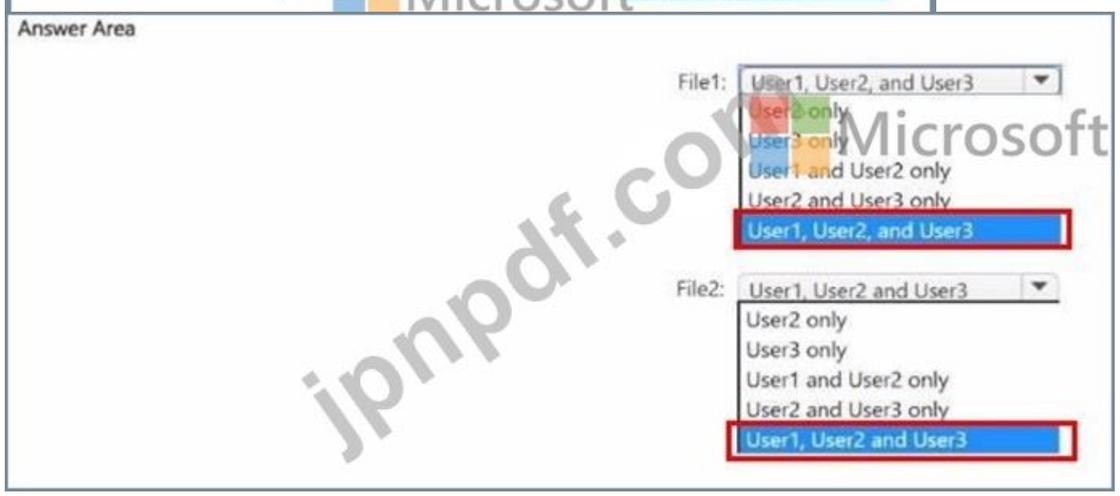
Name	Type	Contents
cont1	Container	File1
share1	File share	File2

Sub1 には、次の表に示すユーザーが含まれます。

Name	Role	Scope
User1	Reader	Sub1
User2	Reader	Sub1
User2	Storage Blob Data Reader	storage1
User3	Storage Contributor	storage1

File1 と File2 を読み取ることができるのはどのユーザーですか? 回答するには、回答で適切なオプション a を選択します。注: 正しい選択ごとに 1 ポイントが加算されます。





最新問題: 108

ケーススタディ 1 - Contoso 社
概要
Contoso 社は、モントリオールに本社を置き、ロンドンとシアトルに支社を持つコンサルティング会社です。
Contoso は、Fabrikam, Inc. という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。
既存の環境。既存の環境
Contoso のオンプレミス ネットワークには、contoso.com という名前の Active Directory ドメインが含まれています。
ドメインにはContoso_Resourcesという組織単位（OU）が含まれています。Contoso_Resources OUにはすべてのユーザーとコンピューターが含まれています。
contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

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

jpntpdf.com Microsoft

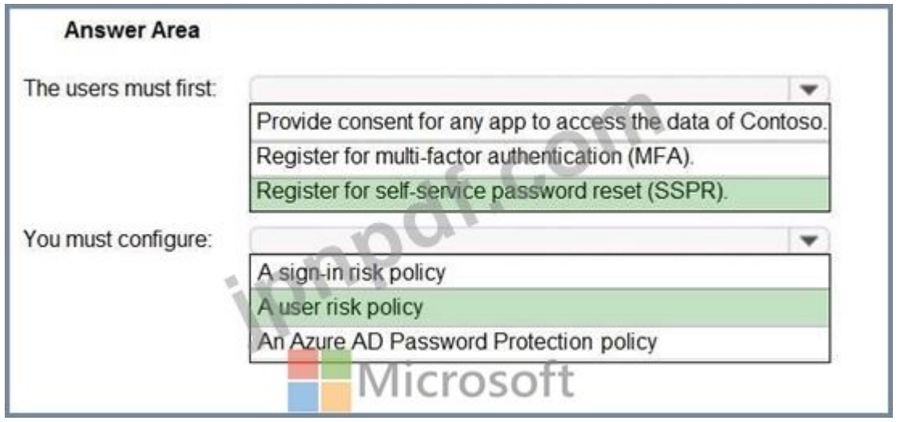
既存の環境。Microsoft 365/Azure 環境
Contoso には、次の関連ライセンスを持つ contoso.com という名前の Azure AD テナントがあります。
* マイクロソフト Office 365 エンタープライズ E5
* エンタープライズモビリティ + セキュリティ
* Windows 10 エンタープライズ E3
* プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory ドメイン サービス (AD DS) の間で構成されています。Contoso_Resources OU のみが同期されます。
ヘルプデスク管理者は、通常、Microsoft 365 管理センターを使用してユーザー設定を管理します。
ユーザー管理者は現在、Microsoft 365 管理センターを使用して手動でライセンスを割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
* ロンドン オフィスのユーザーには、Microsoft 365 電話システムのライセンスが割り当てられていません。
* シアトル オフィスのユーザーには、Yammer Enterprise ライセンスが割り当てられていません。
contoso.com のセキュリティの既定値は無効になっています。
Contoso では、Azure AD Privileged Identity Management (PIM) を使用して管理ロールを保護します。
既存の環境。問題の説明
Contoso は次の問題を特定しています。
* 現在、すべてのヘルプデスク管理者は、Microsoft 365 テナント全体のユーザー ライセンスを管理できます。
* ユーザー管理者は、Contoso オフィスごとに異なるライセンス要件を手動で構成するのは面倒だと報告しています。
* ヘルプデスク管理者は、必要な Microsoft 365 サービスとアプリへの内部アクセスとゲスト アクセスのプロビジョニングに多くの時間を費やしています。
* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
* Azure AD でログ ノードを選択すると、Log Analytics 統合が有効になっていないことを示すエラー メッセージが表示されます。
要件。計画された変更
Contoso は次の変更を実装する予定です。

* セルフサービス パスワード リセット (SSPR) を実装します。
* Azure Monitor を使用して Azure 監査アクティビティ ログを分析します。
* テナントに追加された新しいユーザーに対するライセンスの割り当てを簡素化します。
* Fabrikam のユーザーと協力して共同マーケティング キャンペーンを実施します。
* アクティブ化するには正当性と承認が必要となるようにユーザー管理者ロールを構成します。
* App1 という名前のカスタム基幹業務 Azure Web アプリを実装します。App1 はインターネットからアクセスでき、Azure AD アカウントを使用して認証されます。
* マーケティング部門の新規ユーザーに対して、自動承認ワークフローを実装し、Microsoft SharePoint Online サイト、グループ、アプリへのアクセスを提供します。
Contoso社はAdatum Corporationという会社を買収する計画を立てています。AdatumというActive Directory組織単位（OU）に、100人の新規ADatumユーザーが作成されます。ユーザーはロンドンとシアトルに拠点を置く予定です。
要件。技術要件
Contoso では、次の技術要件を特定しています。
* すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのみのライセンスを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。
ホットスポットに関する質問
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:



Explanation:

ユーザー リスクは、「ID」が侵害される可能性を計算します。

管理者は、Azure AD セルフサービス パスワード リセットを使用して、アクセスをブロックするか、アクセスを許可するか、アクセスは許可するがパスワードの変更を要求するかを選択できます。

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

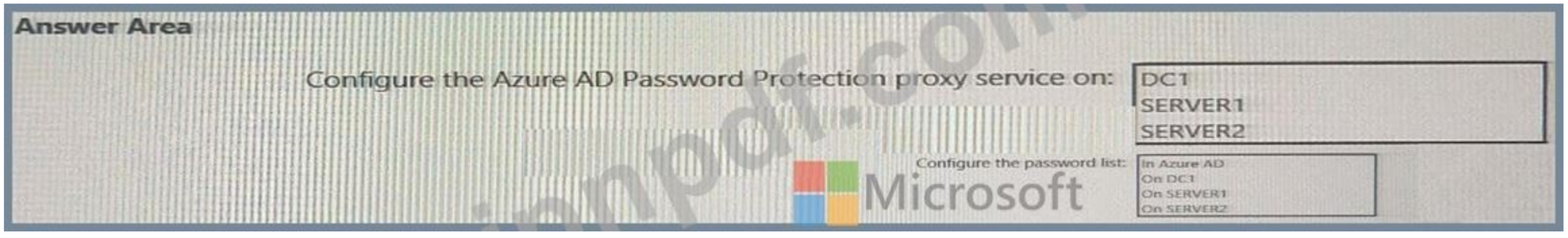
最新問題**: 109**

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 Azure AD パスワード保護 DC エージェントをインストールします。

次に何をすべきでしょうか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

サーバー1

DC1で

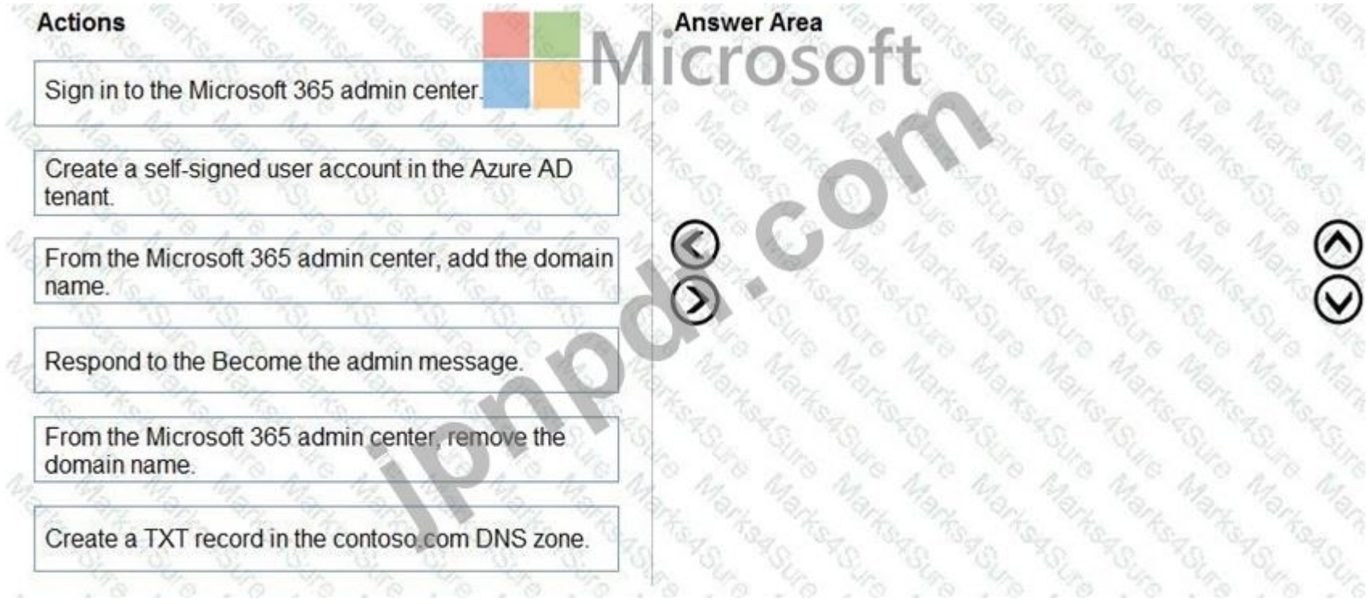
最新問題: **110**

contoso.com の SMTP アドレス スペースを使用するオンプレミスの Microsoft Exchange 組織があります。

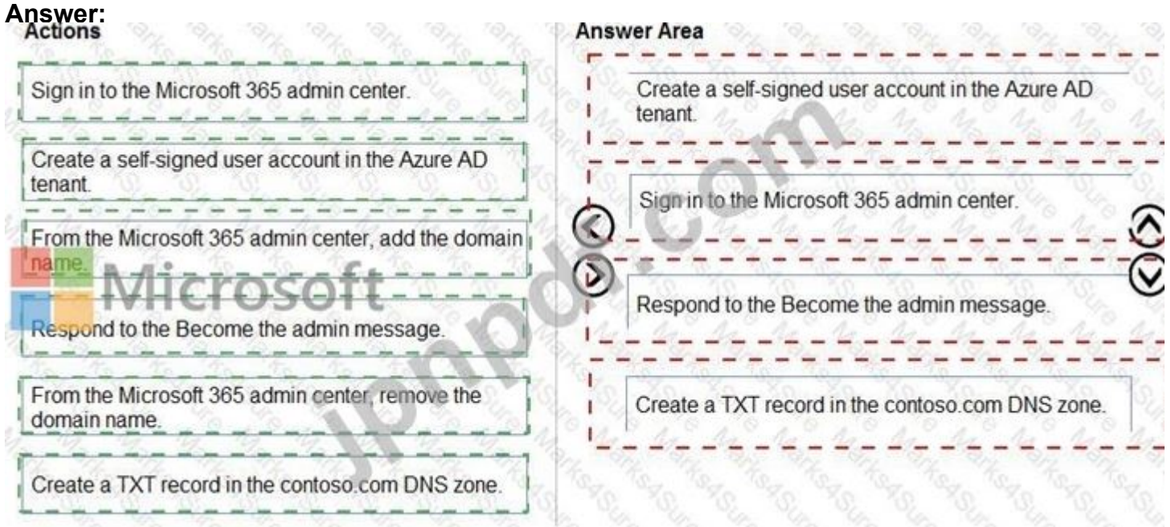
ユーザーが Microsoft 365 サービスへのセルフサービス サインアップに自分のメール アドレスを使用していることがわかりました。

自己署名ユーザーが含まれる Azure Active Directory (Azure AD) テナントに対するグローバル管理者権限を取得する必要があります。

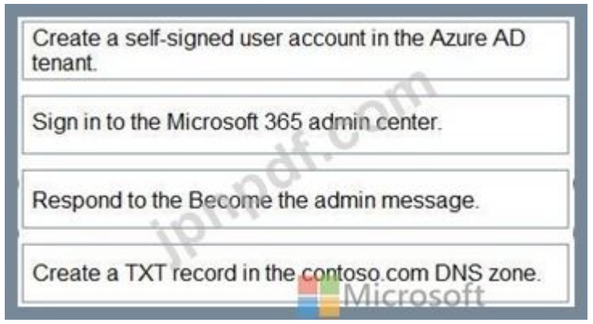
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:



Explanation:



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

最新問題**: 111**
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。
各インシデントに対してどのような設定を行うべきでしょうか？適切なポリシータイプを適切な問題にドラッグしてください。各ポリシータイプは、1回、複数回、または全く使用されない場合があります。
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。



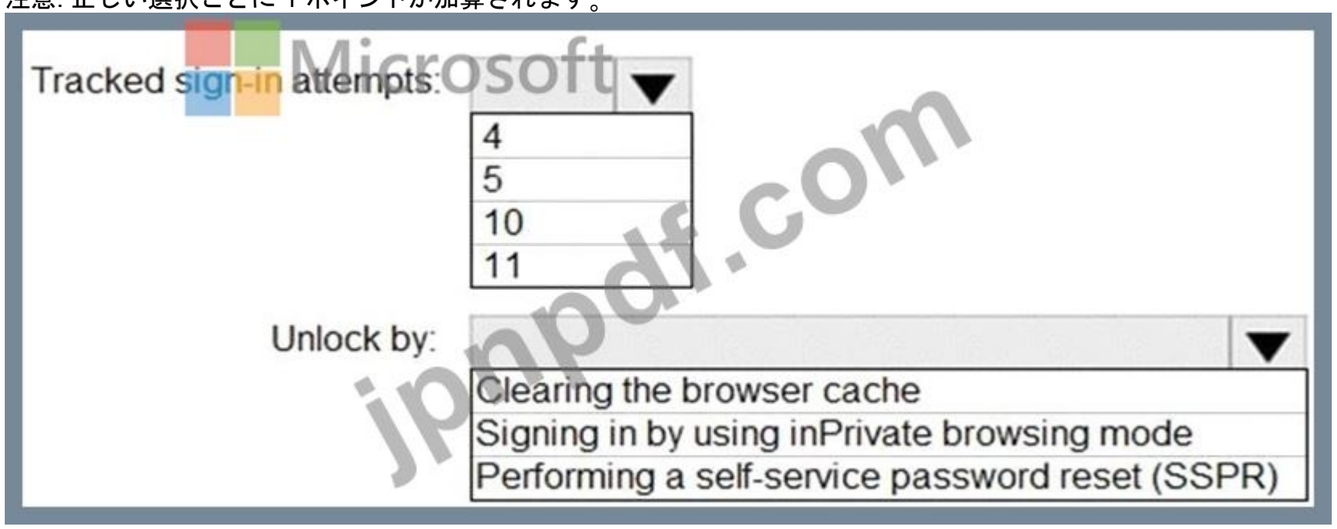
Answer:



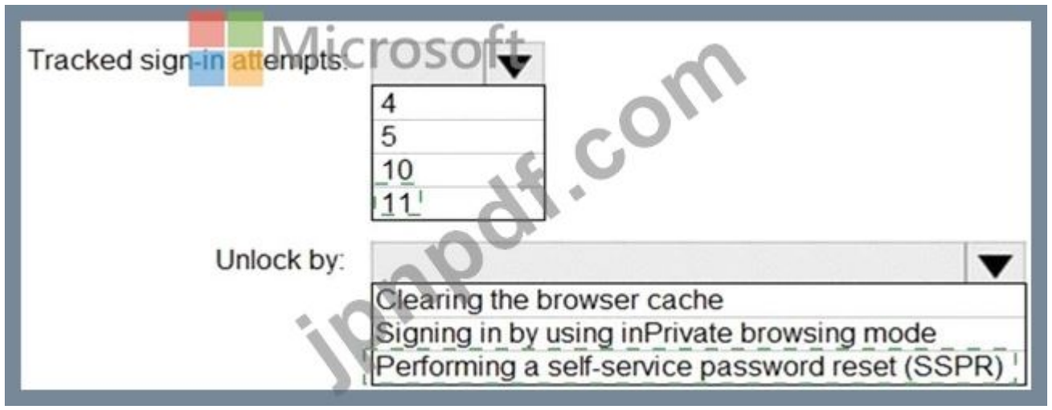
Explanation:



最新問題: **112**
User1 というユーザーが、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す。
Pa55w0rd12
Pa55w0rd12
Pa55w0rd12
Pa55w.rd12
Pa55w.rd123
Pa55w.rd123
Pa55w.rd123
Pa55word12
Pa55word12
Pa55word12
Pa55w.rd12
User1 に対して追跡されたサインイン試行の回数と、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。
何を特定すべきでしょうか？ 回答するには、適切なものを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。

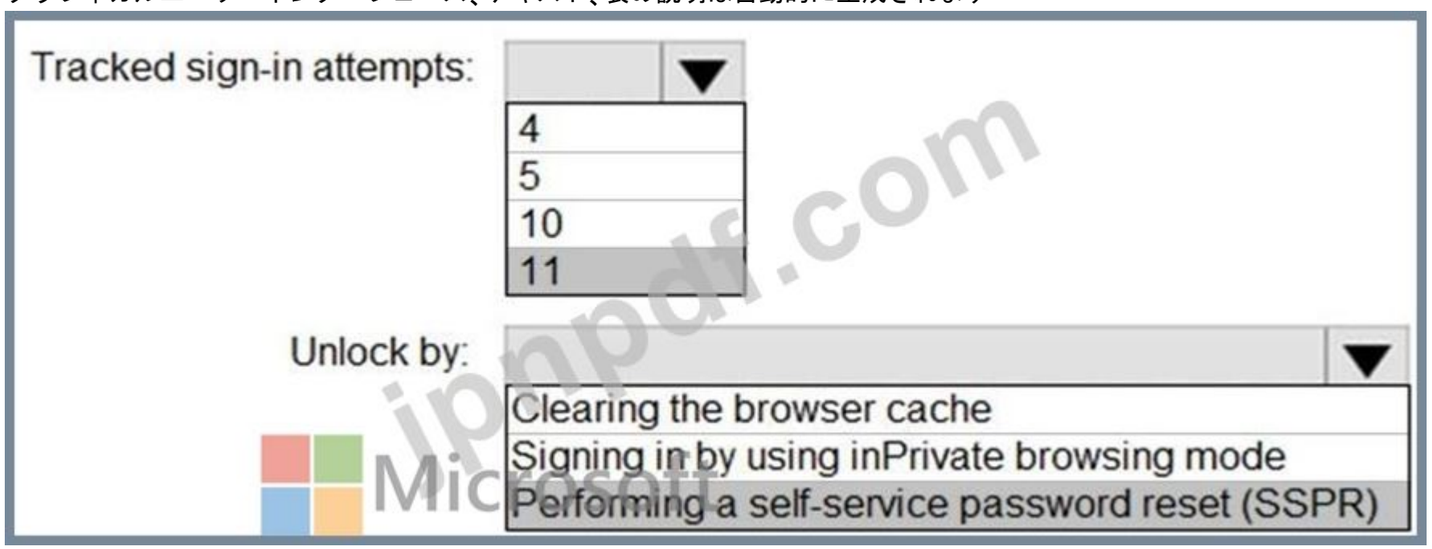


Answer:



説明

グラフィカルユーザーインターフェース、テキスト、表の説明は自動的に生成されます



参照：

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

最新問題: 113

Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。

ユーザー1がグループのアクセスレビューを作成でき、ユーザー2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、最小権限の原則を適用する必要があります。

各ユーザーにどのロールを割り当てるべきですか？ 回答するには、適切なロールを正しいユーザーにドラッグしてください。各ロールは1回、複数回、または全く使用されない場合があります。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：正しい選択ごとに1ポイント獲得できます。



Answer:



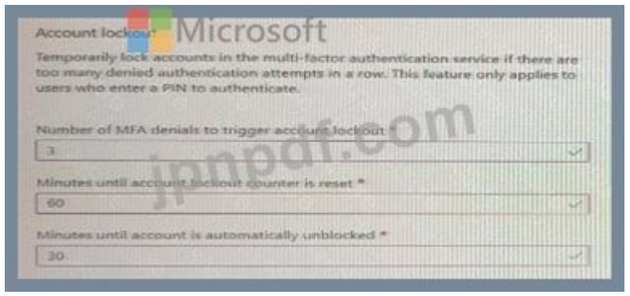
説明



最新問題: **114**

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 ロックアウト設定は、次の図に示すように構成されます。

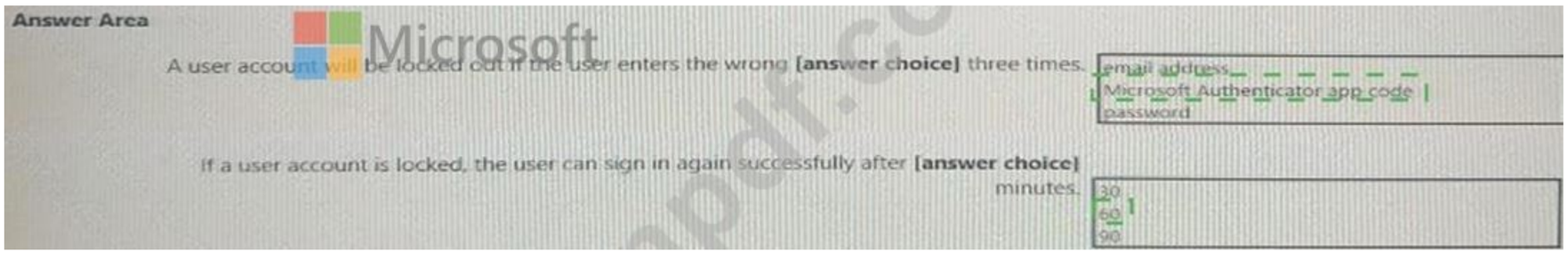


ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

アプリコード

60

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

最新問題**: 115**

contoso.com という名前の Microsoft 365 テナントがあります。

ゲストユーザーアクセスが有効になっています。

次の表に示すように、ユーザーは contoso.com との共同作業に招待されます。

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory 管理センターの外部コラボレーション設定から、次の図に示すようにコラボレーション制限設定を構成します。



ユーザーは、Microsoft SharePoint Online サイトから user3@adatum.com をサイトに招待します。
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 ポイントが加算されます。

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

Answer:

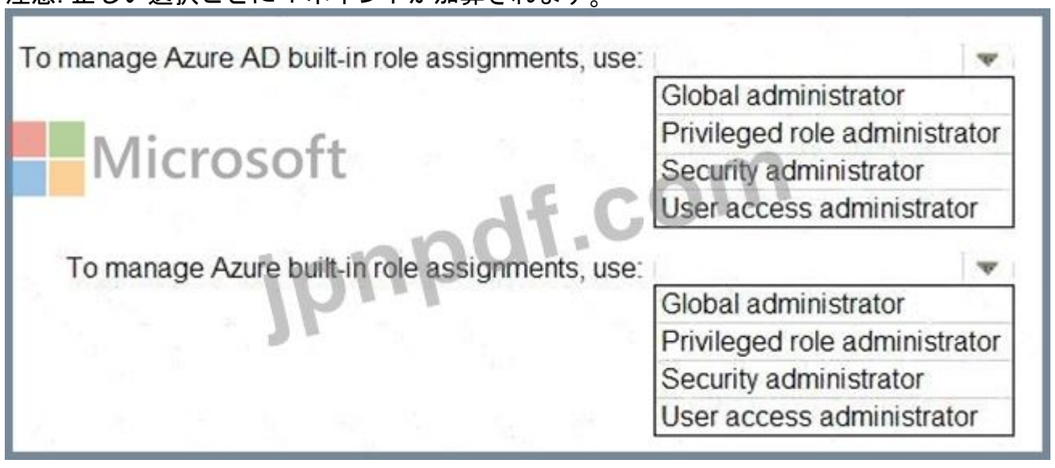
Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

説明

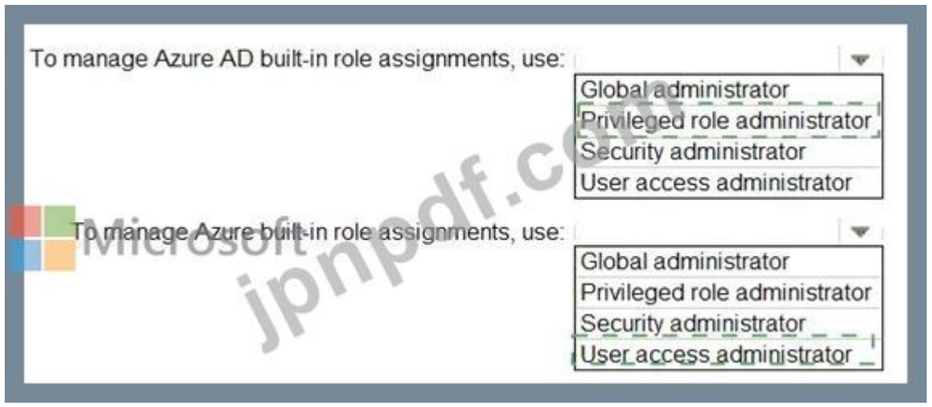


ボックス1: はい
招待はoutlook.comにのみ送信できます。そのため、User1は招待を承諾し、アプリケーションにアクセスできます。
ボックス2. はい
招待はoutlook.comにのみ送信できます。ただし、User2はすでに招待を受け取って承諾しているため、アプリケーションにアクセスできます。
ボックス3. いいえ
招待状はoutlook.comにのみ送信できます。そのため、User3は招待状を受け取りません。

最新問題**: 116**
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要件を満たす必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール 「Azure AD ロールの実装と管理」および 「Privileged Identity Management (PIM) の実装」によれば、Azure AD 組み込みロールと Azure (リソースベース) 組み込みロールには明確な違いがあります。

* Azure AD の組み込みロールは、Azure Active Directory (Entra ID) のユーザー、グループ、エンタープライズ アプリ、セキュリティ設定の管理など、ディレクトリ レベルのアクセスを制御します。特権ロール管理者ロールを使用すると、ユーザーは、PIM によるロールのアクティブ化など、Azure AD のディレクトリ ロールのロール割り当てを管理できます。グローバル管理者にもこの機能がありますが、特権ロール管理者は、シナリオで述べられている最小権限の原則に沿って、委任要件を満たす最小権限ロールです。ドキュメントには次のように記載されています。

「特権ロール管理者は、Azure AD Privileged Identity Management を通じてロールをアクティブ化および割り当てる機能を含む、Azure AD でのロールの割り当てを管理します。」

* 一方、Azure の組み込みロールは、サブスクリプション、リソース グループ、個々のリソースなど、Azure リソース レベルでのアクセスを制御するために使用されます。これらの割り当てを管理するロールは、ユーザー アクセス管理者です。このロールは、Azure RBAC (ロールベースのアクセス制御) 内でロールの割り当てを管理することにより、Azure リソースへのアクセスを許可または取り消すことができます。Microsoft のドキュメントには次のように記載されています。

「ユーザー アクセス管理者は、Azure リソースへのユーザー アクセスを管理できます。リソース、サブスクリプション、管理グループに対して Azure RBAC のロールを割り当てることができます。」したがって、次のようになります。

Azure AD の組み込みロールの割り当てを管理するには # 特権ロール管理者

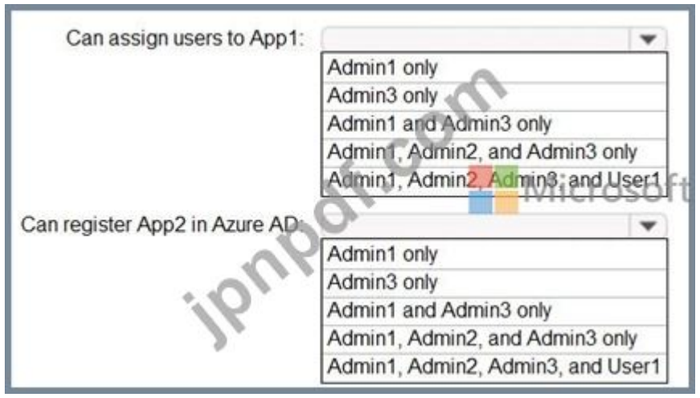
Azure 組み込みロールの割り当てを管理するには # ユーザー アクセス管理者 このアプローチでは、各種類のロール管理タスクに必要な最小限の権限のロールを割り当てることで、シナリオで説明されている委任要件を満たします。

最新問題: 117

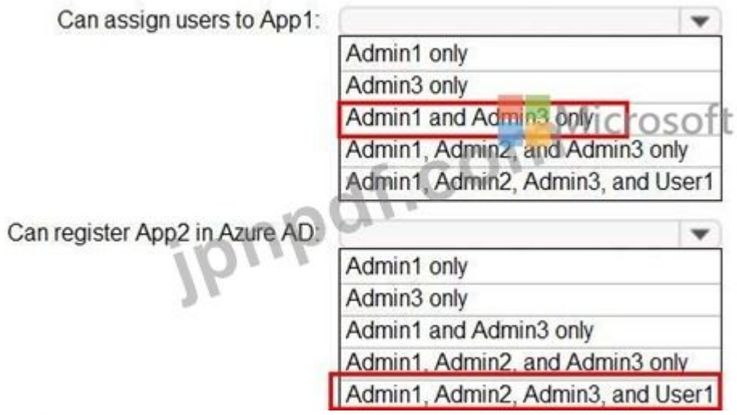
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

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Azure ADに登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

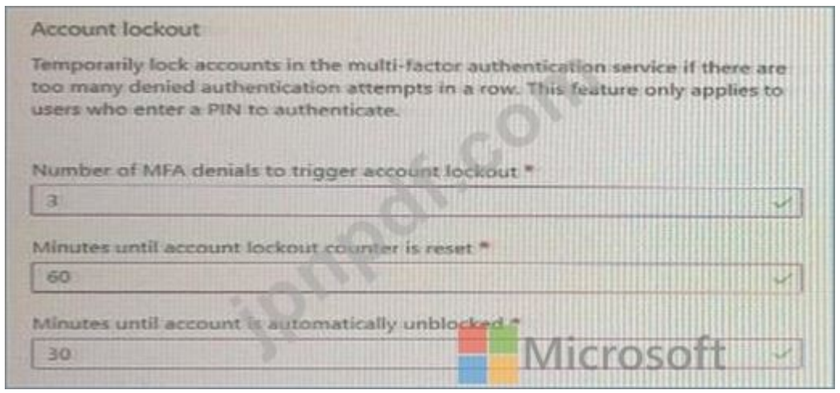


Answer:

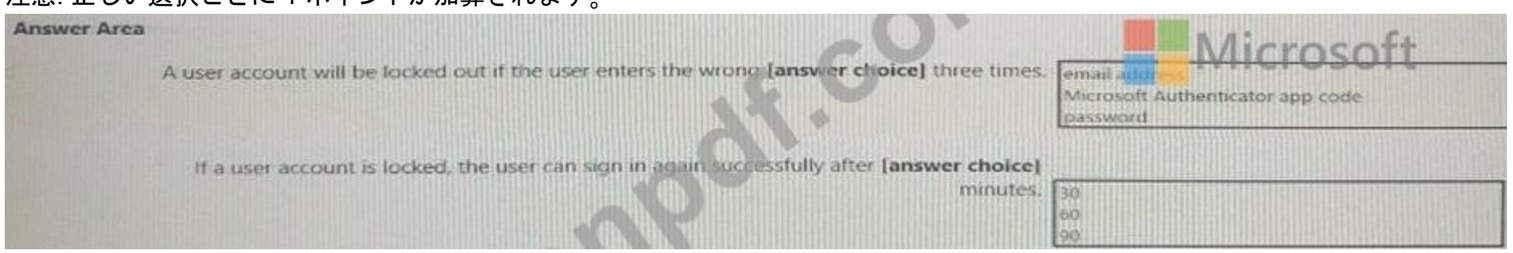


参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

最新問題**: 118**
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 ロックアウト設定は、次の図に示すように構成されます。



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



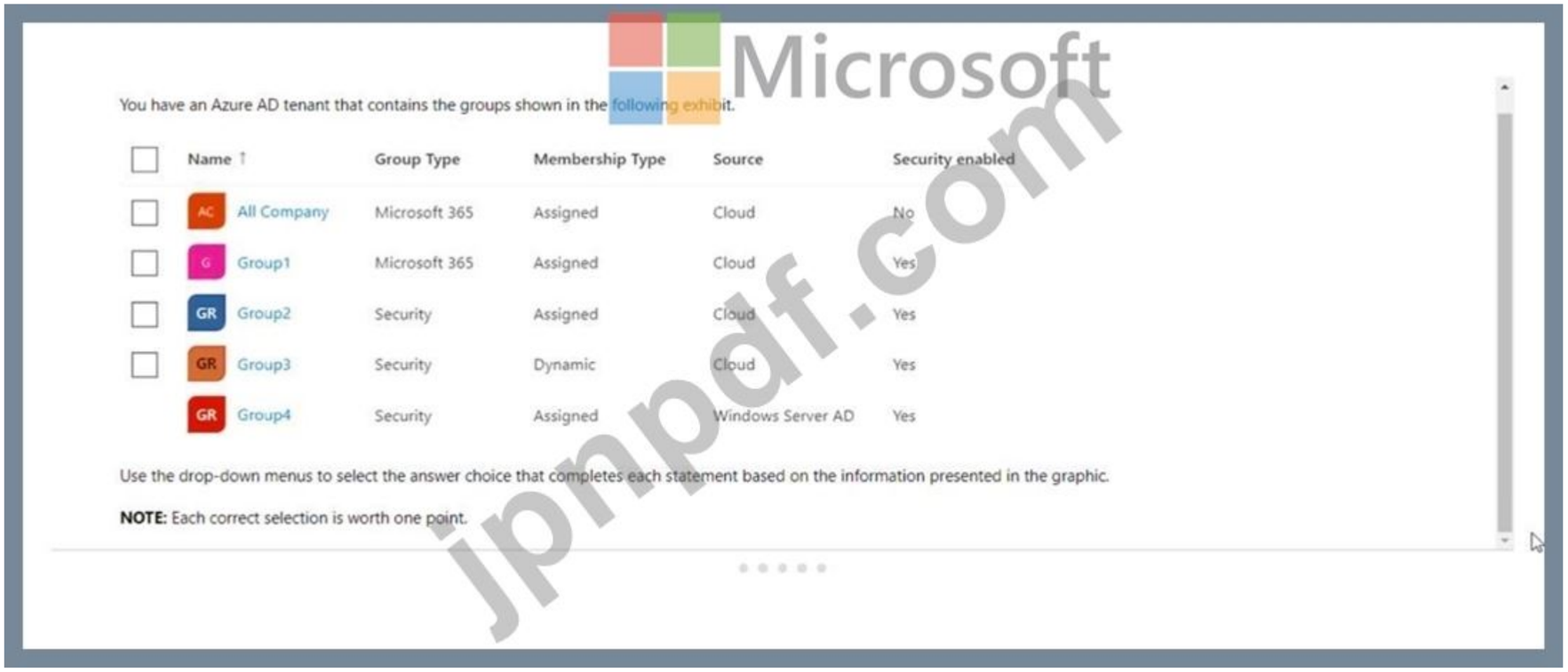
Answer:



最新問題: **119**
Microsoft 365 E5 サブスクリプションをお持ちです。
アプリ ガバナンス アドオン ライセンスを購入します。
アプリ ガバナンスの統合を有効にする必要があります。
どのポータルを使用すればよいですか?
A. Microsoft Defender for Cloud Apps ポータル
B. Microsoft 365 管理センター
C. Microsoft 365 Defender
D. Azure Active Directory 管理センター
E. Microsoft Purview コンプライアンス ポータル
Answer: C (メーッセージを残す**)**
Microsoft の Microsoft 365 向けアプリ ガバナンス ガイダンスに記載されているように、アプリ ガバナンスは、Microsoft 365 と統合された OAuth 対応アプリケーションに対する可視性とポリシー ベースの制御を提供するセキュリティおよびコンプライアンス アドオンです。アプリ ガバナンス ライセンスを購入して割り当てると、この機能の統合と管理は Microsoft 365 Defender ポータルを通じて実行されます。

Defenderポータルでは、管理者は 「権限とアプリ」セクションの 「アプリガバナンス」にアクセスして、統合を有効にし、インサイトを確認し、ポリシーを構成できます。Microsoftのドキュメントには次のように記載されています。
アプリ ガバナンス機能は、Microsoft 365 Defender ポータル (https://security.microsoft.
com) では、Microsoft 365 データに接続された危険なアプリの動作を監視、警告、および修復できます。」したがって、統合と監視は、Azure AD、Purview、または Defender for Cloud Apps ではなく、Microsoft 365 Defender でのみ管理されます。

最新問題: 120
ホットスポットに関する質問次の図に示すグループを
含む 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、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

You can add a managed identity to **<answer choice>**.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

You can add an Azure AD cloud user to **<answer choice>**.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

jpnpdf.com

Microsoft

Answer:

Answer Area



You can add a managed identity to **<answer choice>**.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

You can add an Azure AD cloud user to **<answer choice>**.

- Group2 only
- All Company and Group1 only
- Group2, Group3, and Group4 only
- All Company, Group1, and Group2 only
- All Company, Group1, Group2, Group3, and Group4

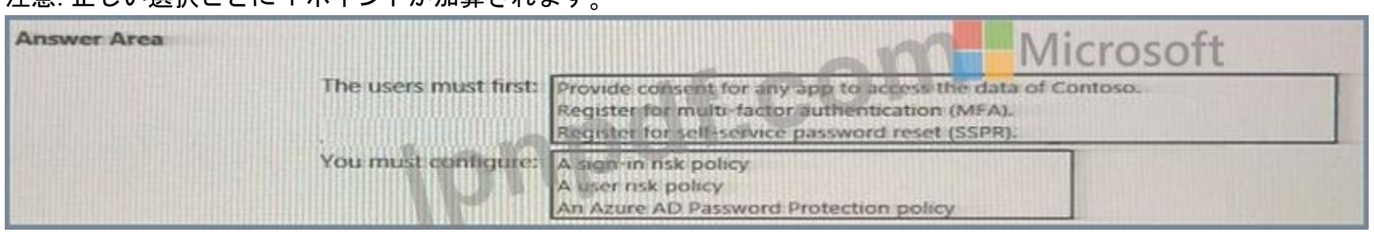
jpnpdf.com

最新問題: **121**

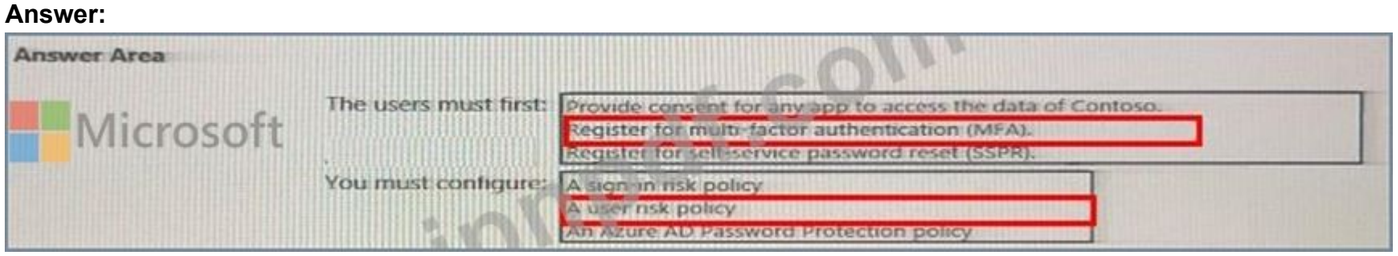
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。

ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

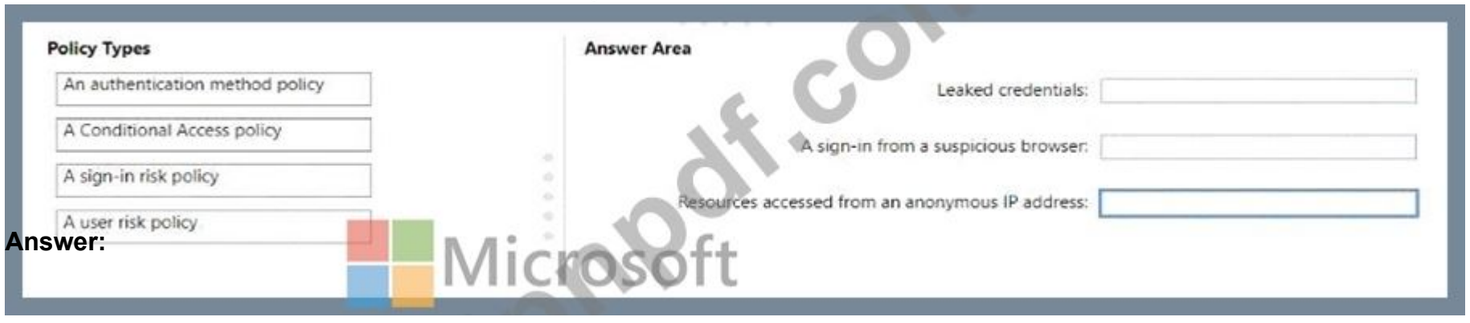
最新問題: **122**
Microsoft 36S テナントがあります。
高リスク国のリストを含む、HighRiskCountries という名前の名前付き場所を作成します。
高リスクの国から接続する場合、ユーザーが認証された状態を維持できる時間を制限する必要があります。
条件付きアクセス ポリシーでは何を構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **123**
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。
各インシデントに対してどのような設定を行うべきでしょうか？適切なポリシータイプを適切な問題にドラッグしてください。各ポリシータイプは、1回、複数回、または全く使用されない場合があります。
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:

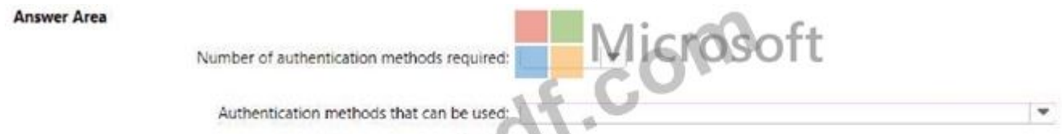


最新問題: 124

SSPR の計画された変更を実装します。

User3 が SSPR を使用しようとすると何が起こりますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。

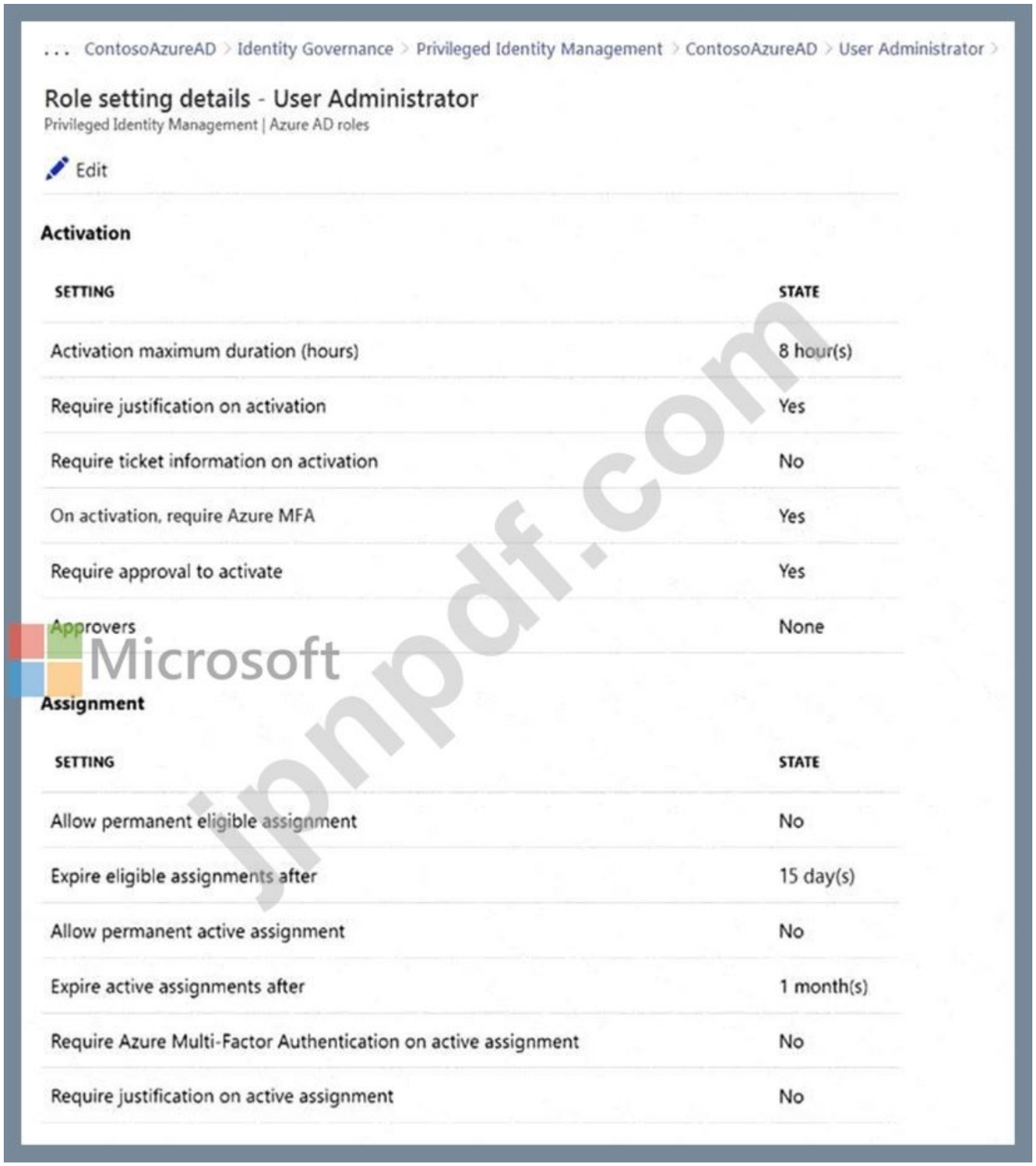


Answer:



最新問題: 125

次の図に示すように、ユーザー管理者ロールの Azure AD Privileged Identity Management (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、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

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

- 8 hours
- 15 days
- 1 month

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

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

Answer:

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

- 8 hours
- 15 days
- 1 month

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

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

Azure AD Privileged Identity Management (PIM) では、ロールのアクティブ化時に MFA を適用できます。『アクティブ化時に Azure MFA を要求する: はい」に設定すると、ユーザーはロールをアクティブ化するたびに MFA を完了する必要があります。

『アクティベーションの最大期間（時間)』は8時間であるため、この期間を超えてユーザー管理者ロールを必要とするユーザーは、ロールを再アクティベートし、MFAを再度実行する必要があります。学習ガイドでは、『アクティベーション時にMFAを要求することで、権限が昇格された瞬間に強力な検証が確実に実行されます」と説明されています。また、『アクティベーションの最大期間は、ユーザーがロールを再アクティベートするまでの期間を制御します」とも記載されています。承認については、ロール設定に 『アクティベートに承認が必要 :はい」と 『承認者 :なし」と表示されています。Azure ADロールのPIM動作は、『ロールに承認者リストが構成されていない場合、アクティベーション要求は特権ロール管理者とグローバル管理者にルーティングされます」です。試験教材では、『特権ロール管理者は、承認ワークフローを含むロール設定を管理し、対象となるアクティベーションを承認できます。また、明示的に承認者が定義されていない場合、グローバル管理者も承認権限を持ちます」と強調されています。したがって、MFA 『アクティベーション期間ごと』は8時間、承認者は明示的に割り当てられていない場合はグローバル管理者または特権ロール管理者を選択するのが正解です。

最新問題**: 126**
次のグループを含む Azure Active Directory (Azure AD) テナントがあります。
名前: グループ1
メンバー: ユーザー1、ユーザー2
所有者: ユーザー3
2021 年 1 月 15 日に、図に示すようにアクセス レビューを作成します。([図] タブをクリックします。)

Create an access review

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

Review name * Review1

Description ⓘ

Start date * 01/15/2021

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never | End by | Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope

- ○ Guest users only
- ◉ Everyone

Group *

Group1

Jpnpdf.com

Microsoft



ユーザーは、次の表に示すように Review1 の質問に回答します。

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 ポイントが加算されます。

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Microsoft
jpnpdf.com

Answer:

参照：

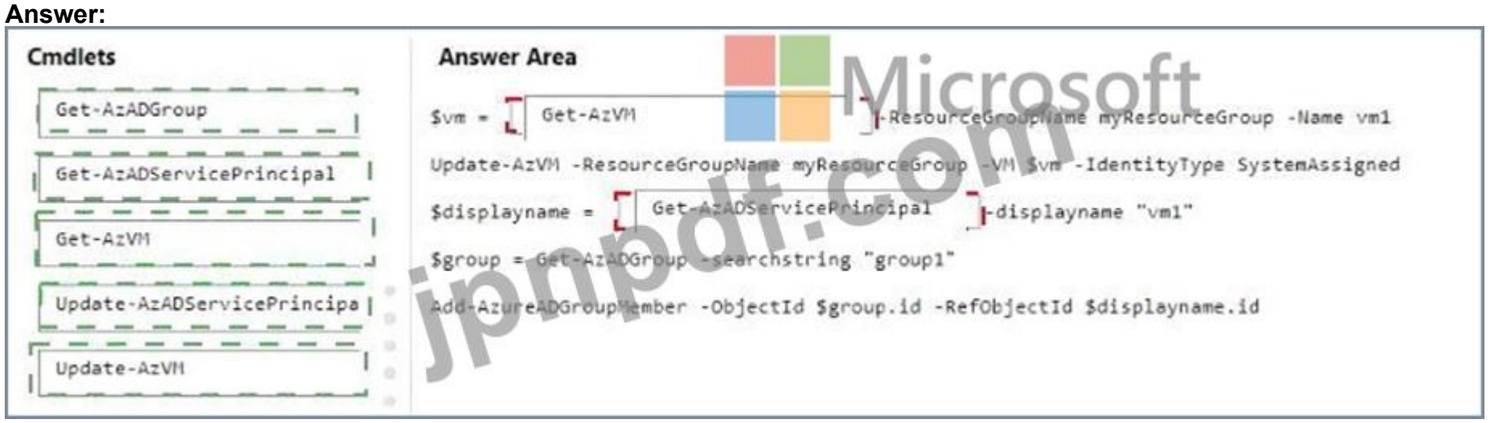
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

最新問題: **127**

contoso.com という 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。このサブスクリプションには、Group1 というグループと VM1 という仮想マシンが含まれています。
次の要件を満たす必要があります。
* VM1 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。
* VM1 を Group1 に追加します。
PowerShellスクリプトはどのように完成させるべきでしょうか？適切なコマンドレットを適切なターゲットにドラッグしてください。各コマンドレットは1回、複数回、または全く使用されない場合があります。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:

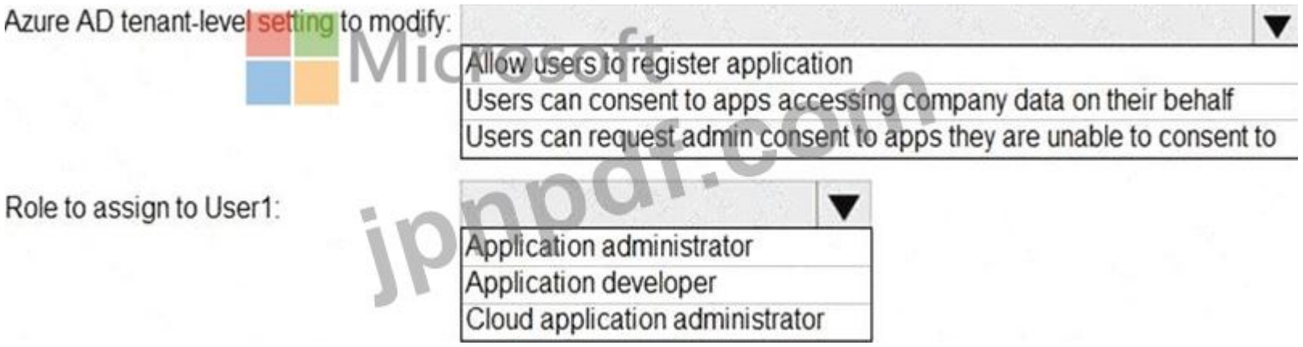


最新問題: 128

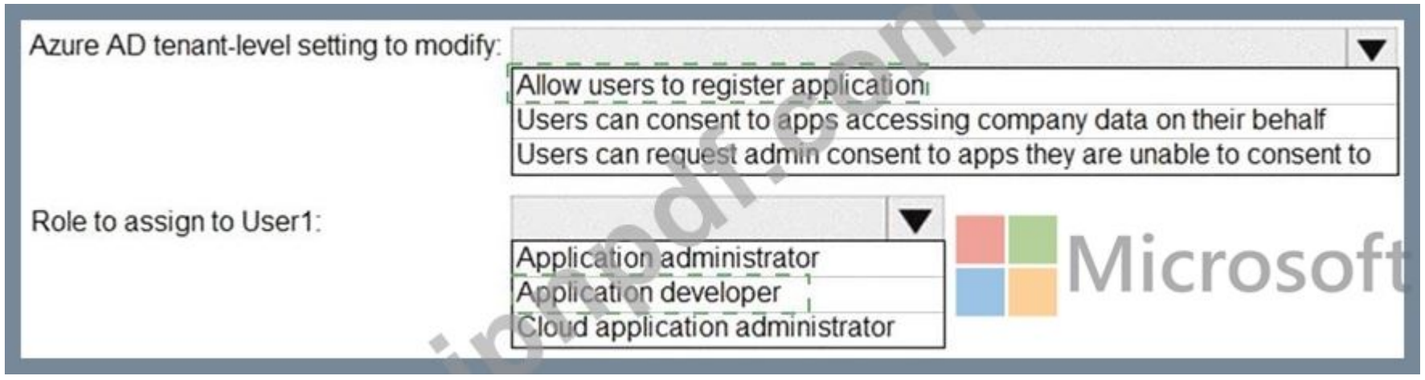
A へのライセンスを見つける必要があります。
Datumユーザー。ソリューションには技術要件が必要です。
どのようなタイプのオブジェクトを作成する必要がありますか?
A. 配布グループ
B. Dynamoユーザーセキュリティグループ
C. あなたの中に
D. 行政単位
Answer: B (メーッセージを残す**)**

最新問題**: 129**
多要素認証 (MFA) が適用され、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 が複合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 ポイントが加算されます。
A. ハードウェアトークン
B. ワンタイムパスコードメール
C. Microsoft Authenticator アプリ
D. FID02 セキュリティキー
E. Windows Hello for Business
Answer: (解答を表示する**)**

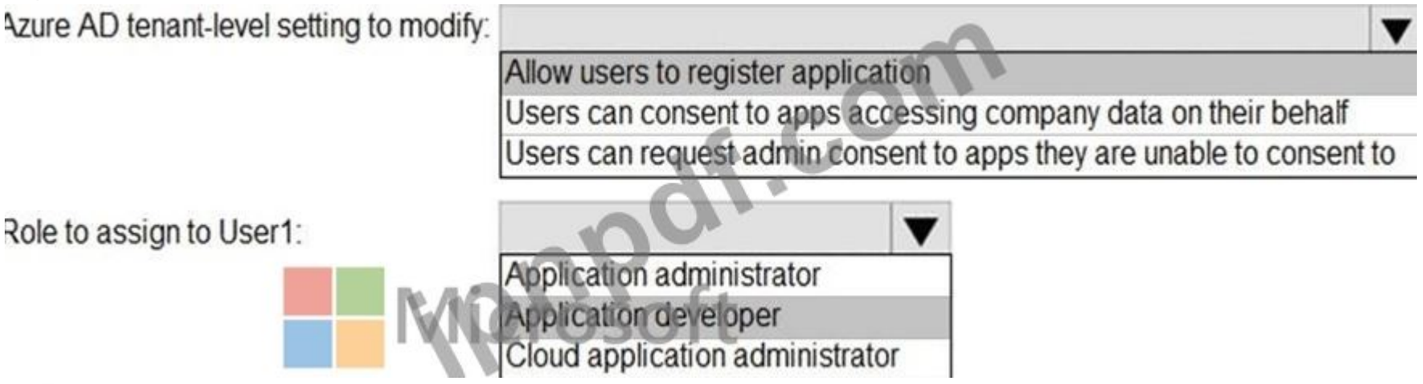
最新問題**: 130**
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



参照：

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

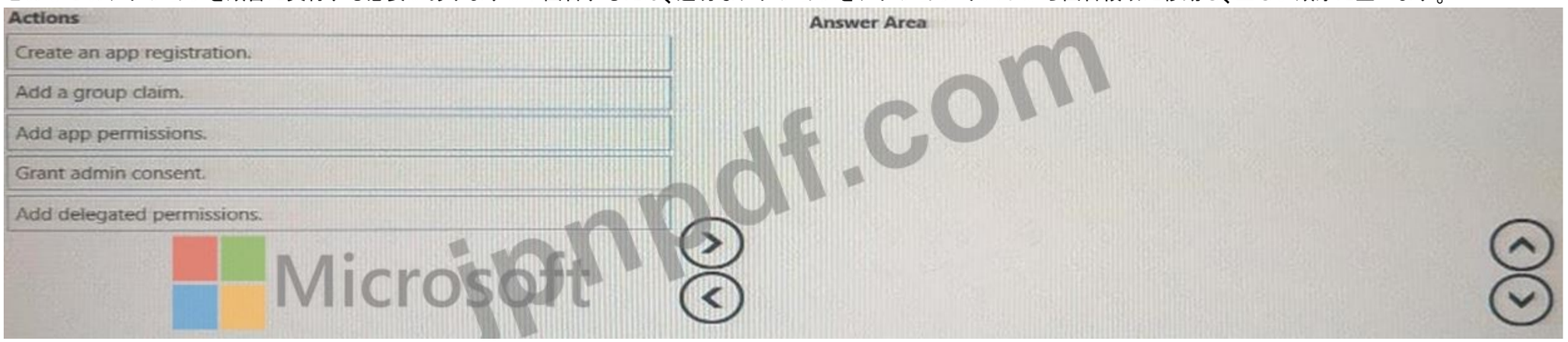
最新問題**: 131**

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。

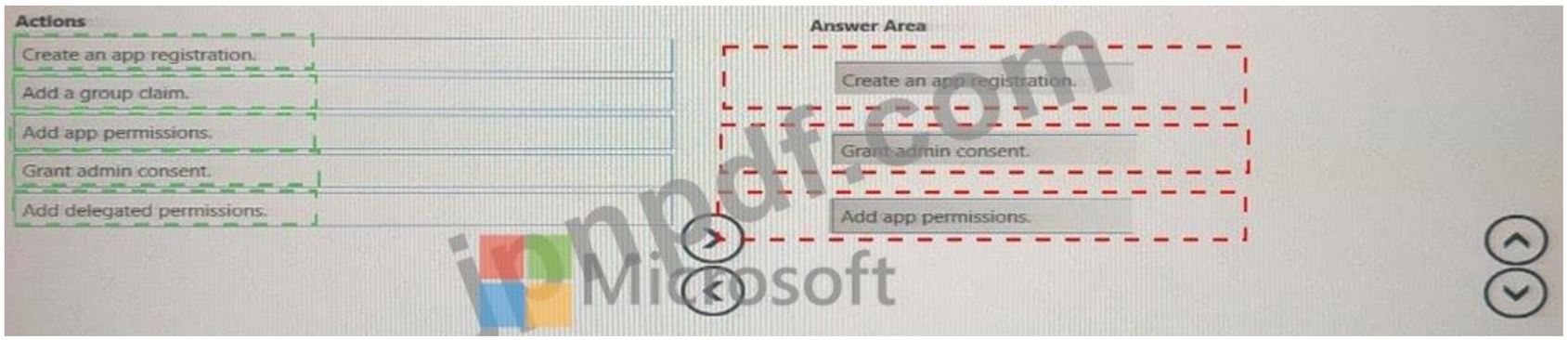
同社はApp1というWebサービスを開発しています。

App1 が Microsoft Graph を使用して contoso.com 内のディレクトリ 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。

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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:



説明

グラフィカルユーザーインターフェース、テキスト、アプリケーションの説明が自動的に生成される



アプリ登録を作成します。

アプリは、Microsoft ID プラットフォームに登録され、必要な Microsoft Graph リソースへのアクセスをユーザーまたは管理者によって承認される必要があります。

管理者の同意を与える:

より高い権限には管理者の同意が必要です。

アプリの権限を追加します:

アプリの権限への同意後、アプリはアクセストークンを取得できます。アクセストークンは、アプリがリソースに対して何らかの形でアクセスする権限を表します。アクセストークンには、アプリがそのリソースに対して付与されているすべての権限がエンコードされています。

参照：

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

最新問題**: 132**

次の表に示す Azure リソースがあります。

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

RG1 の Contributor ロールをどの ID に割り当てることができますか?

A. User1とVW1のみ

B. User1、Group1、Vm1、およびApp1

C. User1、VM1、およびApp1のみ

D. ユーザー1のみ

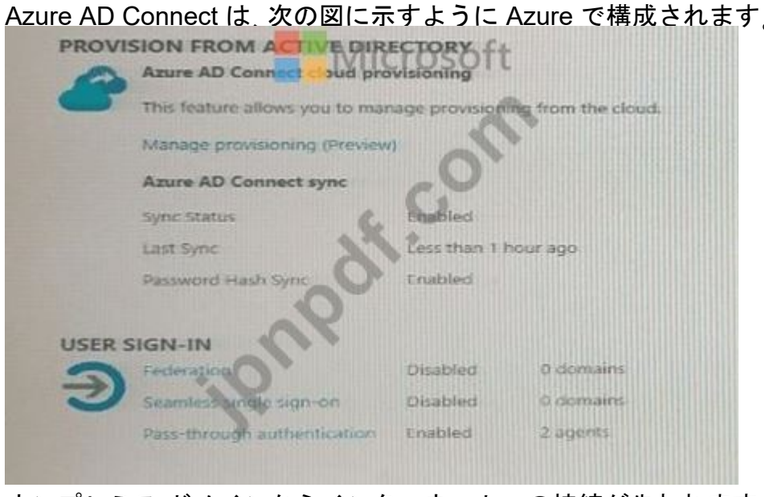
E. User1とGroup1のみ
Answer: B (メーッセージを残す)

最新問題: **133**
Azure AD テナントがあります。
特定の外部ドメインのユーザーのみをテナントにゲストとして招待できるようにする必要があります。
どのような設定を構成する必要がありますか?
A. リンクされたサブスクリプション
B. テナント間アクセス設定
C. すべてのIDプロバイダー
D. 外部コラボレーション設定
Answer: D (メーッセージを残す)

最新問題: **134**
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。
Azure AD Connect は、次の図に示すように Azure で構成されます。



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 Azure AD 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. ユーザー1とユーザー2のみ
C. ユーザー1、ユーザー2、ユーザー3
D. ユーザー1のみ
Answer: (解答を表示する)

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	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

次の表に示す場所があります。

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

テナントには、次の構成を持つ名前付き場所が含まれています。
* 名前: location1
* 信頼できる場所としてマーク: 有効
* IPv4範囲: 10.10.0.0/16
MFA には、193.17.17.0/24 の信頼できる iPad ドレス シリーズがあります。
次の設定を持つ条件付きアクセス ポリシーがあります。
* 名前: CAPolicy1
* 課題
o ユーザーまたはワークロード ID: グループ 1
o クラウドアプリまたはアクション: すべてのクラウドアプリ
* 条件
* 場所 信頼できるすべての場所
* アクセス制御
o と
* アクセスを許可する: 多要素認証を要求する
セッション: 選択されたコントロールは 0 件です
* ポリシーを有効にする: オン
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：正しい選択は1つにつき1点となります。



Answer:

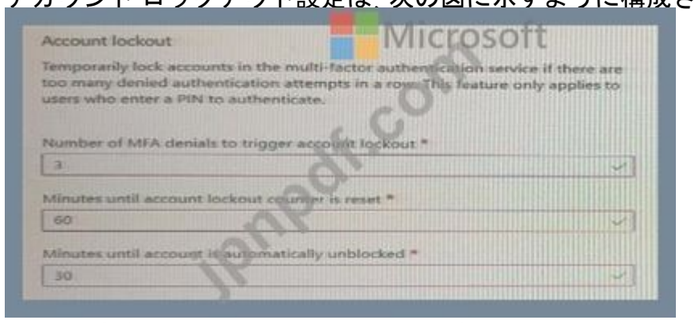


Explanation:

Answer Area

Statements	Yes	No
If User1 connects to the tenant from IP address 10.10.0.150, the user will be prompted for MFA.	○	●
If User2 connects to the tenant from IP address 10.10.1.160, the user will be prompted for MFA.	○	●
If User2 connects to the tenant from IP address 192.168.1.20, the user will be prompted for MFA.	●	○

最新問題**: 136**
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 ロックアウト設定は、次の図に示すように構成されます。



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **137**
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。
追跡された Azure Al) ユーザーのサインイン試行に関する電子メール アラートを毎日 100 件以上受信します。
新しいセキュリティ管理者があなたに代わってアラートを受信するように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。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: (解答を表示する**)**
最新問題: **138**
Microsoft 365 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 Active Directory ドメインと同期します。このドメインには、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への通信ができなくなります。
Server1 と Server2 に Azure AD パスワード保護を実装します。
Windows Server 2019 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。
1 台のサーバーに障害が発生した場合でも、Azure AD 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 コネクト
B. Azure AD 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. Azure AD 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**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premisesdeploy

最新問題: **139**
ホットスポットに関する質問
Sub1 という名前の Azure サブスクリプションがあり、そこには storage1 と storage2 という 2 つのストレージ アカウントと、次の表に示す BLOB コンテナーが含まれています。

Name	In storage account	Contains blob named
cont1	storage1	blob1
cont2	storage1	blob2
cont1	storage2	blob3

Sub1 には、次の表に示すユーザーが含まれます。

Name	Role	Scope	Role assignment condition
User1	Reader	Sub1	*Not applicable*
	Storage Blob Data Reader	Sub1	Condition1
User2	Reader	Sub1	*Not applicable*
	Storage Blob Data Owner	storage1	Condition2

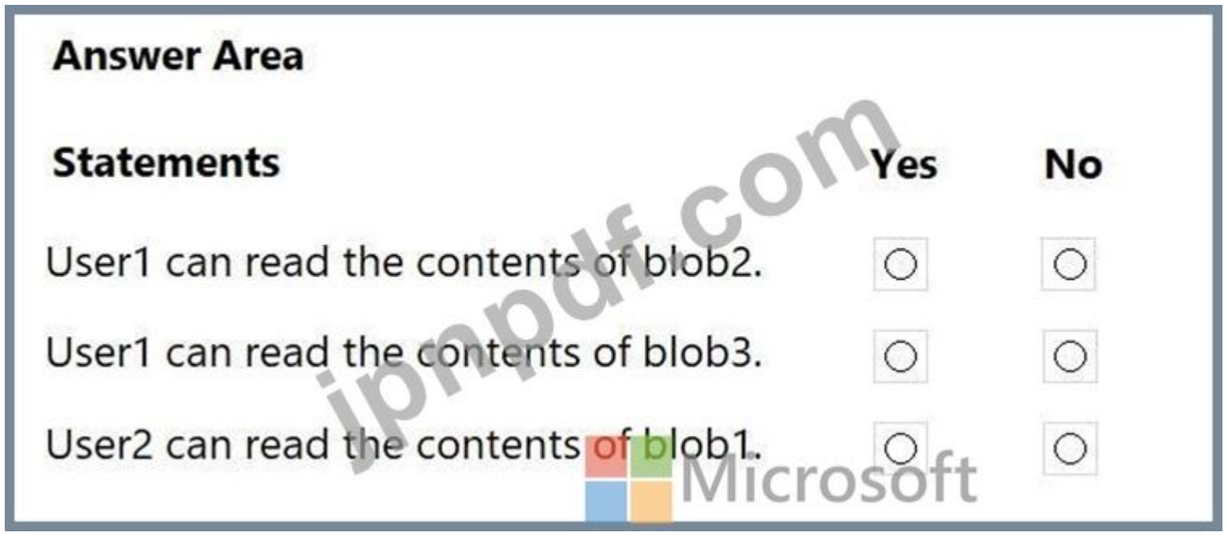
条件1の定義は次のとおりです。

```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read'})
 )
 OR
 (
  @Resource[Microsoft.Storage/storageAccounts/blobServices/containers:name] StringEquals 'cont1'
 )
)
```

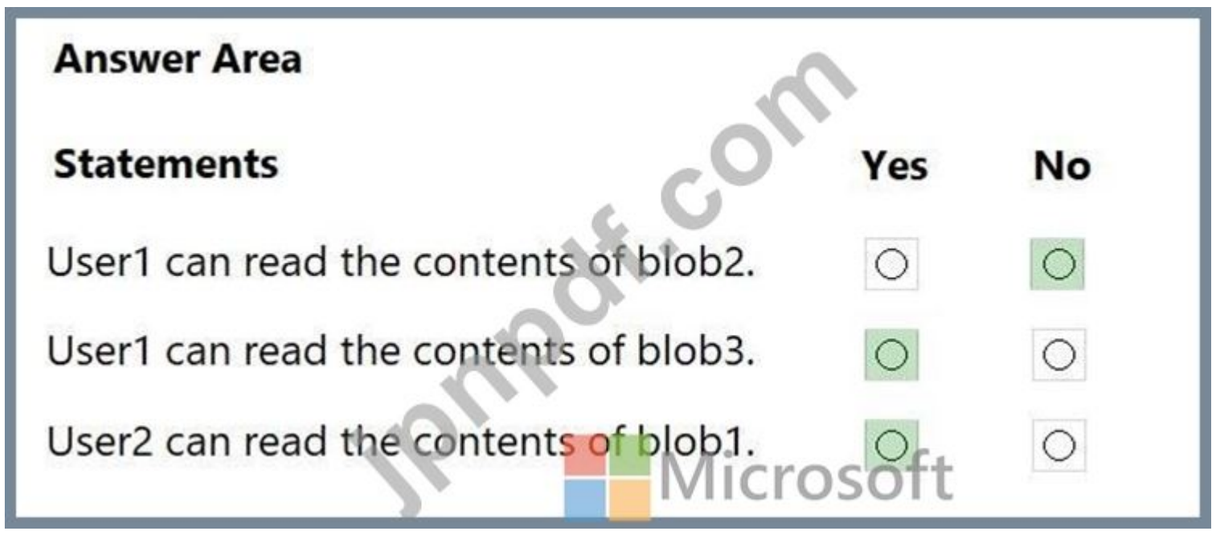
Condition2 has the following definition:

```
(
 (
  !(ActionMatches{'Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write'})
 )
 OR
 (
  @Resource[Microsoft.Storage/storageAccounts/blobServices/containers/blobs:path] StringLike '*2*'
 )
)
```

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



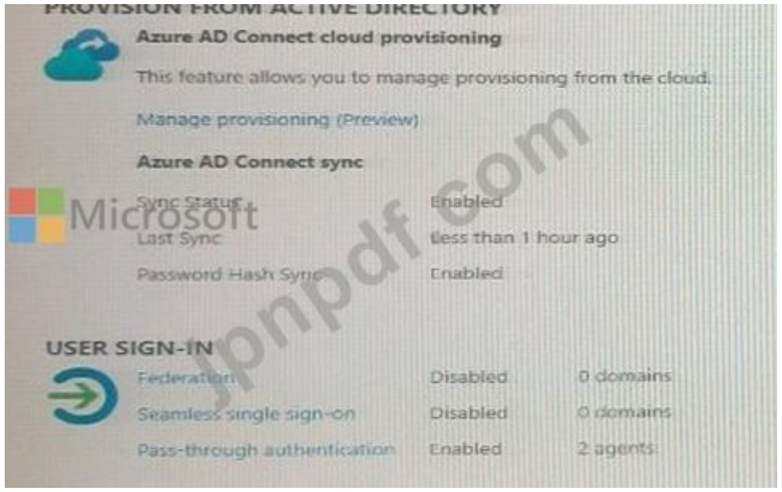
Explanation:
ボックス1: いいえ
User1 は Reader ロールを持っています。BLOB コンテナーには適用されません。
User1 には、Condition1 の Storage Blob Data Reader もあります。
Blob2 は Cont2 にあります。
条件1は偽になります:
アクションは..blob/readsです
リソース名はcont1ではなくcont2です
注: ストレージ BLOB データ リーダー
Azure Storage コンテナーと BLOB を読み取り、一覧表示します。
ボックス2: はい
Blob3はcont1にあります。条件1は真になります。
ボックス3: はい

User2 は Reader ロールを持っています。BLOB コンテナーには適用されません。
User2 には、Condition2 のストレージ BLOB データ所有者ロールもあります。
blob1はcont1にあります
アクションは書き込みではなく読み取りなので、条件 2 は true になります。

最新問題: **140**
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。
Azure AD Connect は、次の図に示すように Azure で構成されます。



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 Azure AD にサインインできますか?
A. ユーザー1のみ
B. ユーザー1とユーザー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**)**

最新問題: **141**
Active Directory フォレストと同期する Azure Active Directory (Azure AD) テナントがあります。テナントは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。
サーバーには必要なソフトウェアのみを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でも、ユーザーが Azure AD 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. サーバー2
B. サーバー4
C. サーバー1
D. サーバー3
Answer: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/pta クイックスタートへの接続方法

最新問題**: 142**
次の表に示すオブジェクトを含む Azure Active 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. ユーザー2とグループ2のみ
B. ユーザー2、グループ1、グループ2のみ
C. ユーザー1、ユーザー2、グループ1、グループ2
D. ユーザー1とユーザー2のみ
E. ユーザー2のみ
Answer: E (メーッセージを残す**)**
M365 管理センターでは、メールが有効なセキュリティ グループに追加できるのはユーザーのみです。
グループに追加できるのはライセンスを持つユーザーのみで、ライセンスを持たないユーザーはメンバー選択ページにも表示されません。
参照：
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups- nesting/

最新問題**: 143**
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

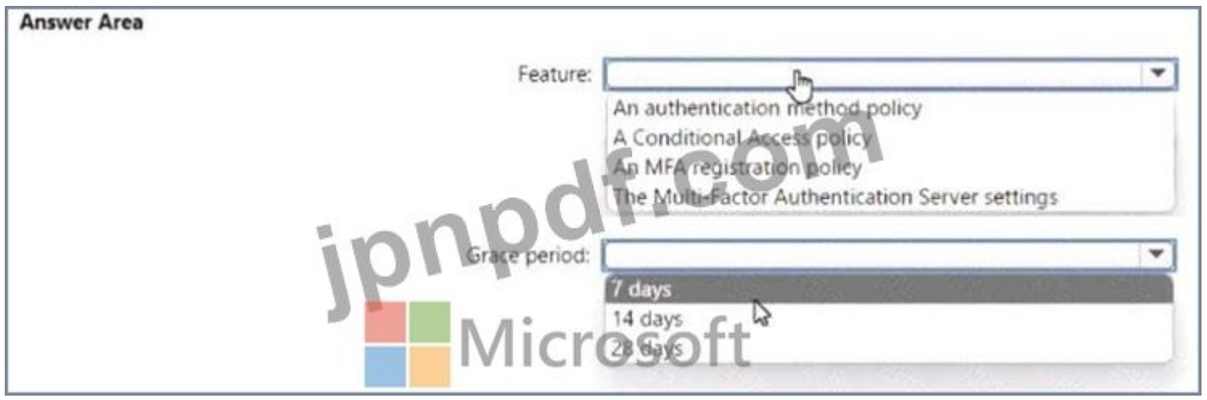


Explanation:



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

最新問題**: 144**
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、ユーザーはどのくらいの時間前に登録を完了す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**: 145**

Sub1 という名前の Azure サブスクリプションがあります。

Microsoft Entra Permissions Management を展開する予定です。

権限管理がSub1にアクセスできることを確認する必要があります。ソリューションは最小権限の原則に従う必要があります。

PowerShell コマンド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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



Microsoft Entra Permissions Management（旧称CloudKnox）では、Azureサブスクリプションのオンボーディングでは、Permissions Managementサービスプリンシパルに、そのサブスクリプション全体のID、ロール、およびアクセス許可を検出するために必要な最小限の権限を付与する必要があります。SC-300資料では、オンボーディングにおける最小権限の原則が強調されています。サブスクリプションスコープで閲覧者（Reader）を割り当て、サービスがリソースとアクセス許可のインベントリを作成できるようにし、変更権限は付与しないようにします。オンボーディング後、自動修復/適正化が必要な場合は、ユーザーアクセス管理者（User Access Administrator）を追加で付与（または手動で変更）できますが、オンボーディングとデータ収集のみにこの権限の昇格は必要ありません。
したがって、New-AzRoleAssignment を使用して、サブスクリプション スコープでアプリケーション（サービス プリンシパル）の RBAC 割り当てを作成し、-RoleDefinitionName Reader を指定することで、PowerShell を完了できます。新しいカスタム ロール (New-AzRoleDefinition) の作成は不要であり、New-AzTag は RBAC とは無関係です。Owner または Contributor を選択すると、オンボーディングに必要なアクセス権限を超え、最小権限ガイダンスに違反します。したがって、正しい最小限の構成は、New-AzRoleAssignment を使用して、/subscriptions/<SubscriptionId> スコープで Permissions Management アプリケーションに Reader を割り当てることです。

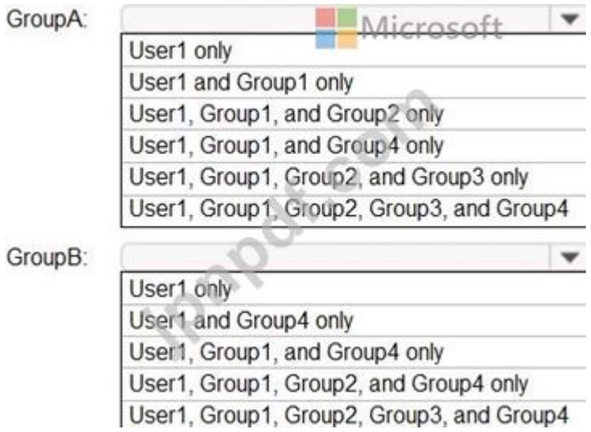
最新問題: **146**
User1 という名前のユーザーと、次の表に示すグループを含む Azure Active Directory (Azure AD) テナントがあります。

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

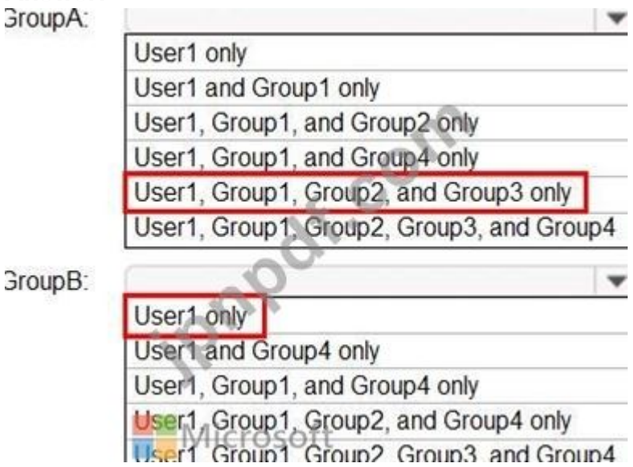
テナントでは、次の表に示すグループを作成します。

Name	Type	Membership type
GroupA	Security	Assigned
GroupB	Microsoft 365	Assigned

グループAとグループBに追加できるメンバーは誰ですか？ 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題**: 147**
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	Privileged Authentication Administrator
User3	Global Administrator

Azure AD Privileged Identity Management (PIM) では、次の図に示すようにグローバル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、グローバル管理者ロールの対象となります。
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 ポイントが加算されます。

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.	○	○
User2 and User3 can edit the Global Administrator role assignment.	○	○

Answer:

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.	○	○
User2 and User3 can edit the Global Administrator role assignment.	○	○

jpnpdf.com
Microsoft

Explanation:



最新問題**: 148**

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

Azure AD で、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追加します。

App1 に割り当てることができるグループは何ですか?

A. グループ1とグループ3

B. グループ2のみ

C. グループ3のみ

D. グループ1のみ

E. グループ1とグループ4

Answer: E (メーッセージを残す**)**

グループベースの割り当てには、Azure Active Directory Premium P1 または P2 エディションが必要です。グループベースの割り当ては、セキュリティ グループでのみサポートされます。

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

最新問題**: 149**

Microsoft 365 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 Active Directory ドメインと同期します。

ユーザーは、社内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 の資格情報を使用してファイアウォールに認証します。

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。

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には、ファイアウォール ログを使用する必要があります。

情報を収集するには何を使用すればよいですか?

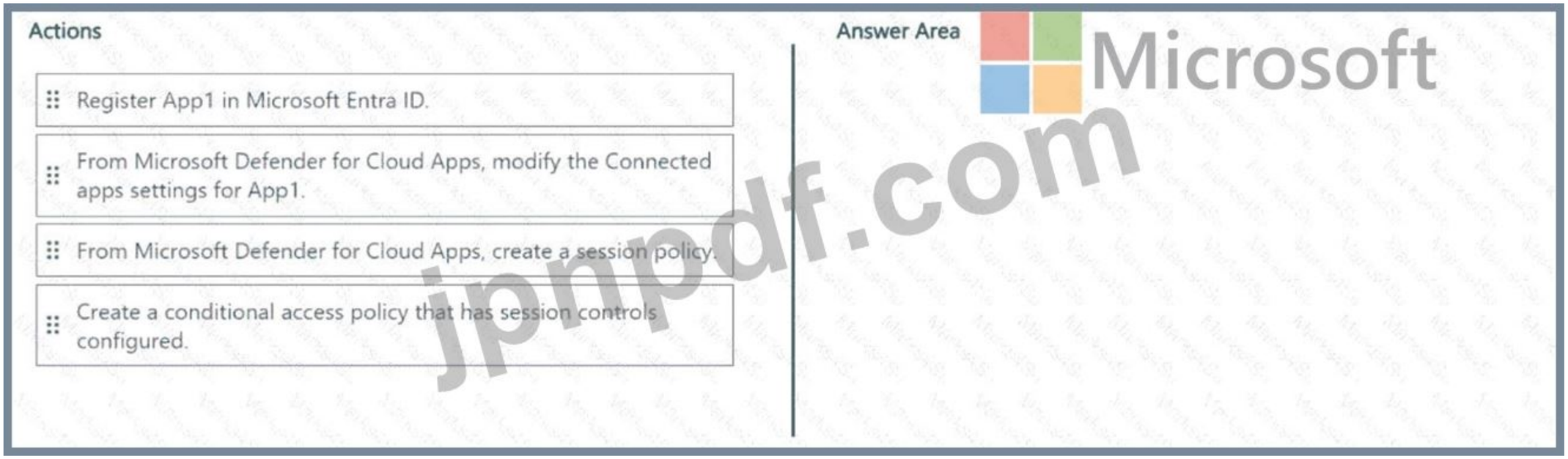
A. Azure Monitor の Application Insights

B. Azure AD のアクセスレビュー

C. Microsoft Cloud App Security の Cloud App Discovery

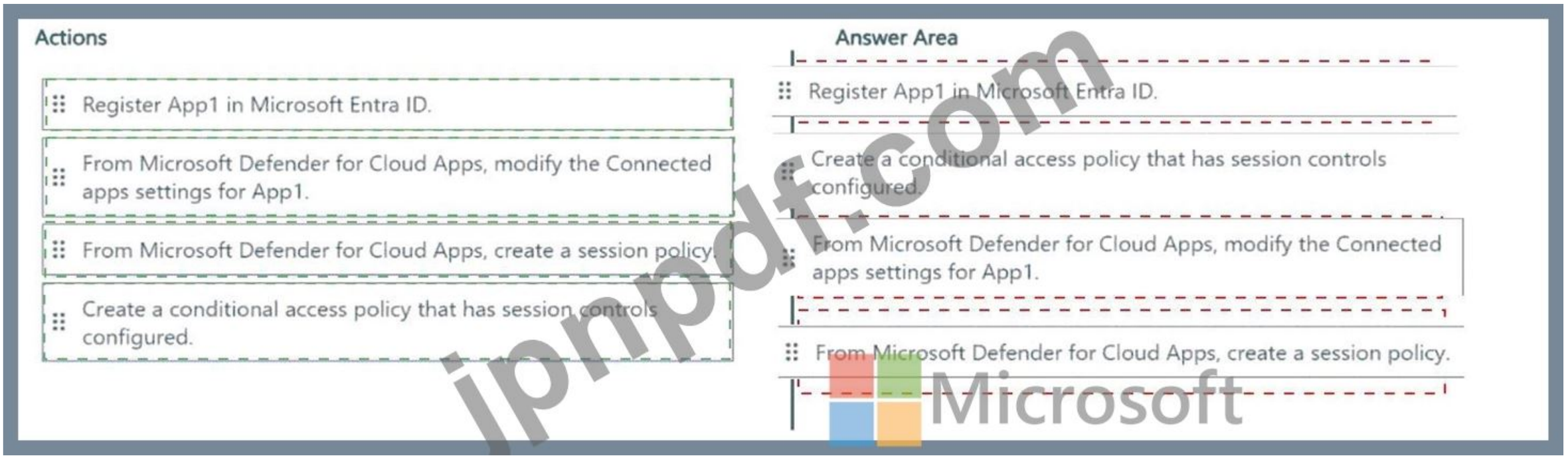
D. Azure AD のエンタープライズ アプリケーション
Answer: C (メーッセージを残す**)**
https://docs.microsoft.com/en-us/cloud-app-security/create-snapshot-cloud-discovery- reports#using-traffic-logs-for-cloud-discovery

最新問題**: 150**
Microsoft 365 E5 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 Defender for Cloud Apps 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。
どの順序でアクションを実行すればよいですか? 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、正しい順序に並べます。



Microsoft
jpnpdf.com

Answer:



ipnpdf.com

Explanation:

App1をMicrosoft Entra IDに登録します。

セッション制御が構成された条件付きアクセス ポリシーを作成します。

Microsoft Defender for Cloud Apps から、App1 の接続アプリの設定を変更します。

Microsoft Defender for Cloud Apps からセッション ポリシーを作成します。

Microsoft Identity and Access Administrator ドキュメントで概説されているように、リアルタイムのセッション レベルの監視を有効にするために、Microsoft Defender for Cloud Apps (MDCA) と Microsoft Entra ID の統合に基づいて、これを段階的に説明してみましょう。

目標を理解する: Microsoft Defender for Cloud Apps によるリアルタイムのセッション レベル監視:

Microsoft Defender for Cloud Apps (MDCA) は、クラウド アプリケーションの可視性、制御、脅威からの保護を提供するクラウド アクセス セキュリティ ブローカー (CASB) ソリューションです。

リアルタイムのセッションレベル監視により、MDCAはアクティブセッション中にクラウドアプリ（この場合はApp1）内のユーザーアクティビティを検査・制御できます。そのためには、Microsoft Entra IDとの統合と、条件付きアクセスポリシーを使用してセッションをMDCA経由でルーティングし、監視する必要があります。

Microsoft 365 E5 テナントには、この機能に必要な Microsoft Entra ID P2 と Microsoft Defender for Cloud Apps のライセンスが含まれています。

アクションのステップバイステップの分析: リアルタイムのセッション レベルの監視を有効にするには、クラウド アプリを MDCA と統合するための Microsoft の推奨ワークフローに沿った論理的な順序でアクションを実行する必要があります。

ステップ 1: Microsoft Entra ID に App1 を登録します。

App1 を MDCA で監視するには、Microsoft Entra ID にアプリケーションとして登録する必要があります。この手順では、テナントのエンタープライズ アプリケーションに App1 を追加し、Microsoft Entra ID がアプリの認証と承認を管理できるようにします。

アプリを Microsoft Entra ID に登録すると、シングル サインオン (SSO) が有効になり、セッション レベルの監視の前提条件である条件付きアクセス ポリシーでアプリを管理できるようになります。

App1 が Microsoft Entra ID によって認識されなければ、他のアクションを続行できないため、これが最初のステップとなります。

手順 2: セッション制御が構成された条件付きアクセス ポリシーを作成します。

Microsoft Defender for Cloud Apps は、Microsoft Entra ID 条件付きアクセスと統合され、セッションレベルの監視を実施します。App1 をターゲットとし、ユーザーセッションを MDCA 経由でルーティングするセッション制御を含む条件付きアクセスポリシーを作成する必要があります。

条件付きアクセスポリシーの「セッション」制御で、「条件付きアクセスアプリ制御を使用する」オプションを有効にします。これはMDCAと統合されます。これにより、MDCAはセッションをリアルタイムで監視および制御できるようになります。
条件付きアクセスポリシーは既存のアプリを対象とする必要があるため、この手順はMicrosoft Entra IDにアプリを登録した後に実行する必要があります。また、セッション制御統合によってMicrosoft Entra IDとMDCA間の接続が確立されるため、この手順はMDCA固有の手順よりも前に実行する必要があります。
手順 3: Microsoft Defender for Cloud Apps から、App1 の接続アプリの設定を変更します。
条件付きアクセスポリシーによってセッションがMDCAにルーティングされた後、MDCA内でApp1の「接続アプリ」設定を変更して構成する必要があります。この手順では、App1がMDCAに正しく接続されていることを確認する必要があります。これには、APIコネクタの構成や、MDCAがアプリのアクティビティを監視できるかどうかの確認などが含まれる場合があります。
この手順は、MDCA が App1 を監視するために必要な権限と構成を持っていることを確認するために必要です。条件付きアクセス ポリシーによって統合が有効になり、アプリを処理するために MDCA を設定する必要があるため、この手順は条件付きアクセス ポリシーの後に行われます。
手順 4: Microsoft Defender for Cloud Apps からセッション ポリシーを作成します。
最後に、MDCA でセッションポリシーを作成し、App1 のリアルタイム監視および制御ルールを定義します。MDCA のセッションポリシーを使用すると、ユーザーアクティビティ（ファイルのダウンロード、データ共有など）を監視し、事前定義された条件に基づいてアクション（ブロック、通知など）を適用できます。
この手順は最後の手順です。これは、前の手順に依存しているためです。つまり、アプリを登録し、条件付きアクセスポリシーでセッションをMDCAにルーティングし、MDCAがApp1を認識できるように接続アプリの設定を構成する必要があります。これらが完了したら、リアルタイム監視を適用するためのセッションポリシーを定義できます。
なぜこの注文なのですか?
この順序により論理的な流れが保証されます。
アプリを Microsoft Entra ID に登録すると、テナント内にアプリの ID が確立されます。
条件付きアクセス ポリシーは、セッションを MDCA 経由でルーティングすることで MDCA との統合を可能にします。
MDCA の接続アプリの設定を変更すると、アプリが監視用に適切に設定されるようになります。
MDCA でセッション ポリシーを作成すると、リアルタイムのセッション レベル監視の特定の監視および制御ルールが定義されます。
この順序から外れるとエラーが発生します。例えば、Microsoft Entra ID にアプリを登録する前に MDCA でセッションポリシーを作成すると、MDCA がアプリを認識できないため失敗します。
追加の考慮事項:
Microsoft 365 E5 ライセンスには Microsoft Entra ID P2 と Microsoft Defender for Cloud Apps が含まれているため、このシナリオでは追加のライセンスは必要ありません。
App1 が MDCA のアプリ コネクタでサポートされているアプリでない場合は、追加の手順 (カスタム アプリ コネクタの使用など) が必要になる可能性がありますが、質問では、App1 は標準プロセスで監視できることが示唆されています。
MDCA のセッション ポリシーには、ダウンロードのブロックやステップアップ認証の要求などのアクションを含めることができ、これらはユーザーのセッション中にリアルタイムに適用されます。
結論: Microsoft Defender for Cloud Apps 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正しい順序は次のとおりです。
App1をMicrosoft Entra IDに登録します。
セッション制御が構成された条件付きアクセス ポリシーを作成します。
Microsoft Defender for Cloud Apps から、App1 の接続アプリの設定を変更します。
Microsoft Defender for Cloud Apps からセッション ポリシーを作成します。
参考文献:
Microsoft Defender for Cloud Apps のドキュメント: 「Microsoft Defender for Cloud Apps を使用したセッション制御」(Microsoft Learn:https://learn.microsoft.com/en-us/defender-cloud-apps/session-policy)
Microsoft Entra ID 条件付きアクセスのドキュメント: 「条件付きアクセスでのセッション制御」(Microsoft Learn:https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-session) Microsoft Identity and Access Administrator (SC-300) 試験の学習ガイド。セッション レベルの監視のために Microsoft Defender for Cloud Apps と Microsoft Entra ID を統合する方法について説明します。

最新問題**: 151**
Sub1 という Azure サブスクリプションがあり、そこには RG1 と RG2 という 2 つのリソース グループが含まれています。Sub1 には、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Sub1 には、次の表に示すリソースが含まれています。

Name	Type	In resource group
VM1	Virtual machine	RG1
Vault1	Azure Key Vault	RG1
Vault2	Azure Key Vault	RG2

次の表に示すロールベースのアクセス制御 (RBAC) ロールの割り当てを作成します。

Role	Member of	Scope
Reader	Group1	Sub1
Key Vault Secrets User	Group2	RG2
Owner	Group3	RG1

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：正しい選択は1つにつき1点です。

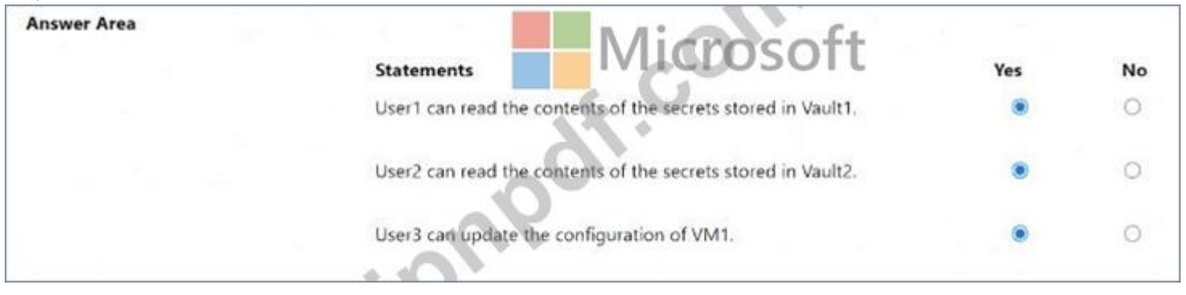
Answer Area

Statements	Yes	No
User1 can read the contents of the secrets stored in Vault1.	○	○
User2 can read the contents of the secrets stored in Vault2.	○	○
User3 can update the configuration of VM1.	○	○

Answer:



Explanation:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 152

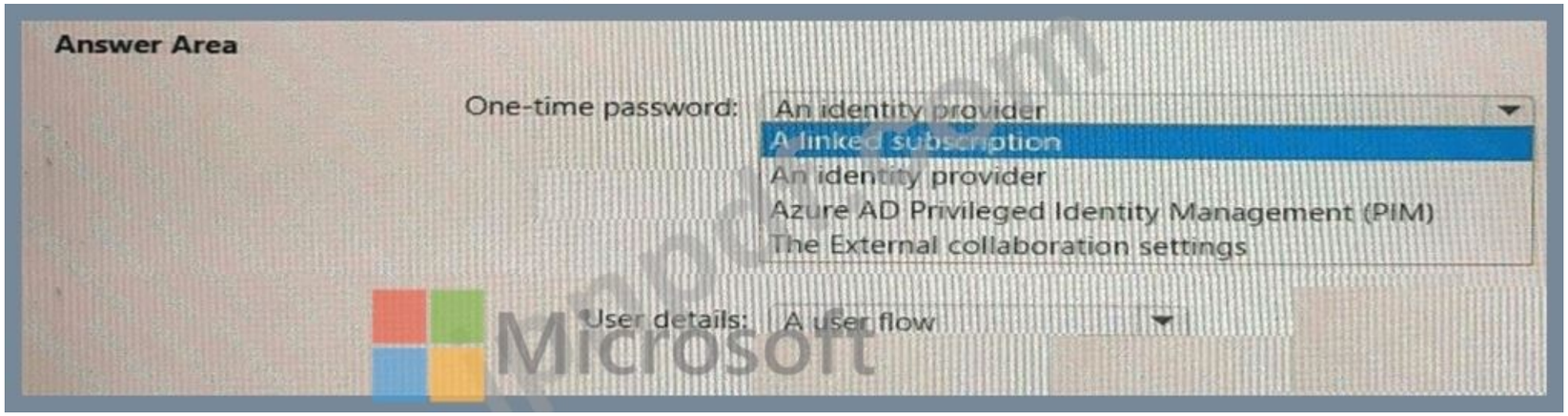
Azure AD テナントと、App1 という名前の Azure Web アプリがあります。

ゲストユーザーにApp1のセルフサービスサインアップを提供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。

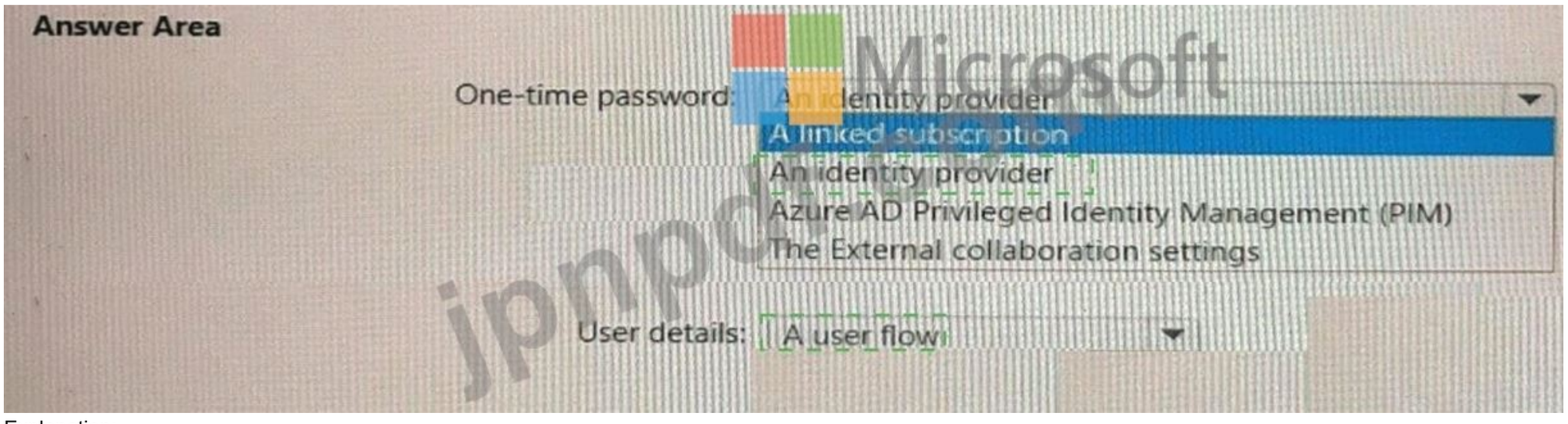
* ゲスト ユーザーは、ワンタイム パスワードを使用してサインアップできる必要があります。
* ユーザーはサインアップ時に、名、姓、市区町村、電子メール アドレスを入力する必要があります。

各要件に対して、Azure Active Directory 管理センターで何を構成す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。

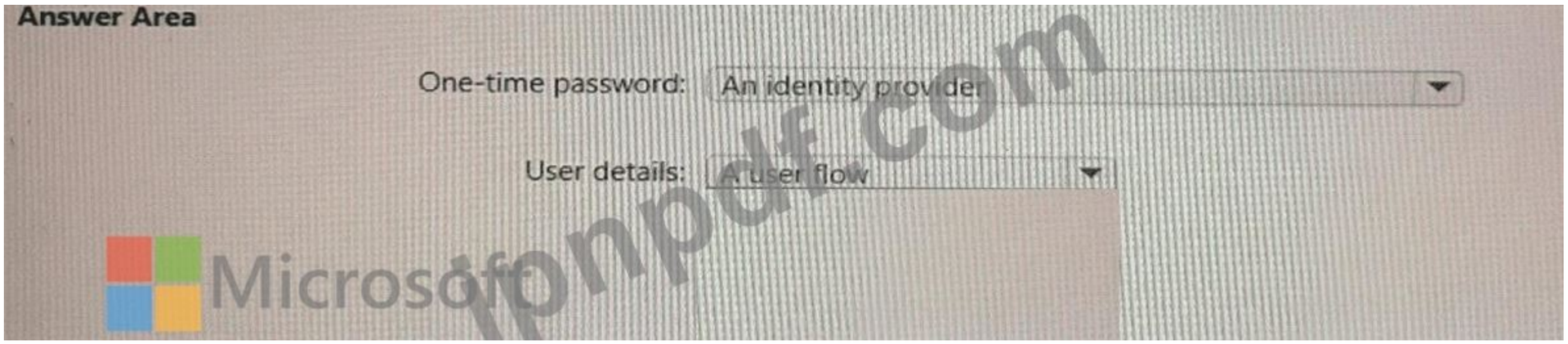
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



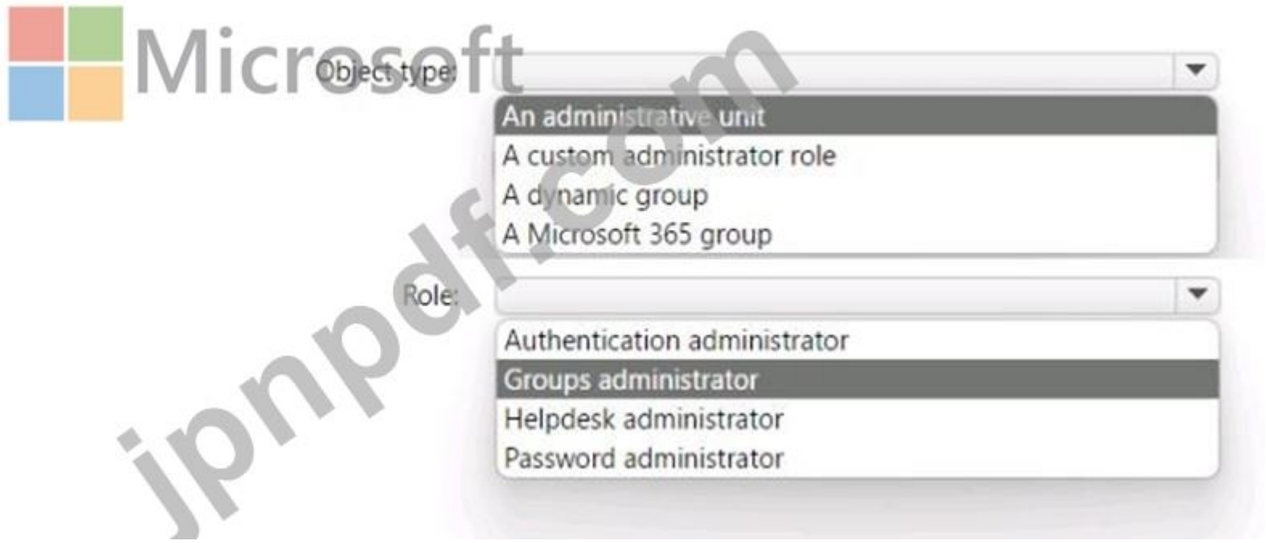
Explanation:



最新問題**: 153**
VM1 という名前の仮想マシンを含む Azure サブスクリプションがあります。VM1 の構成は次のとおりです。
- プライベートIPアドレス: 172.16.1.5
- パブリックIPアドレス: 108.143.161.25
- システム割り当てマネージドIDのステータス: オン
VM1 に App1 という名前のアプリをインストールします。
マネージド ID アプリ専用アクセス トークンを要求するように App1 を構成する必要があります。
App1 はリクエストにどの IP アドレスを使用する必要がありますか?
A. 108.143.161.25
B. 127.0.0.1
C. 169.254.169.254
D. 172.16.1.5
Answer: C (メーッセージを残す**)**
169.254.169.254 は、Azure Instance Metadata Service (IMDS) に使用される特別な IP アドレスであり、VM に関する情報を提供し、マネージド ID のトークンを要求できるようにします。

最新問題**: 154**
5,000人のユーザーがいるMicrosoft 365テナントがあります。そのうち100人は経営幹部で、経営幹部には専任のサポートチームがいます。
サポートチームがパスワードをリセットし、経営幹部のみの多要素認証（MFA）設定を管理できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
どのオブジェクト タイプと Azure Active Directory (Azure AD) ロールを使用す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



Answer:

Answer Area



jpnpdf.com

最新問題**: 155**

Department1 という名前の管理単位を含む Azure Active Directory (Azure AD) テナントがあります。

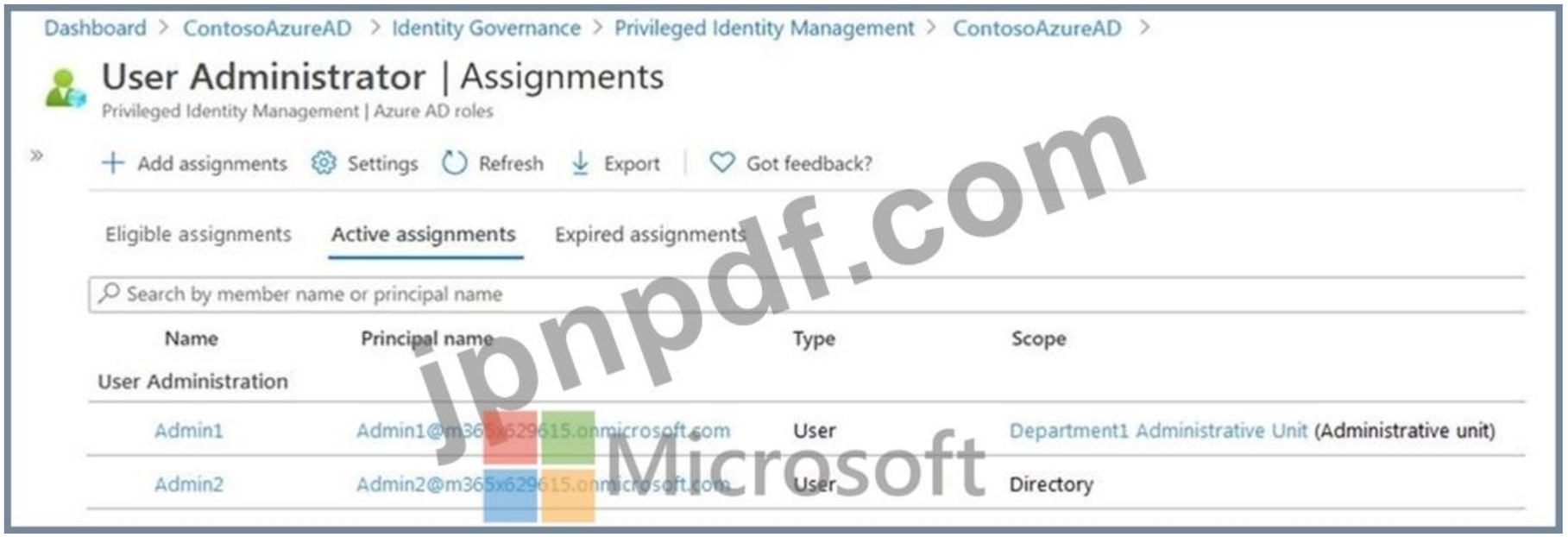
Department1 には、[ユーザー] 展示に示されているユーザーがいます。([ユーザー] タブをクリックします。)



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、[割り当て] 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。)



グループ2のメンバーはグループ2の展示に表示されます。(ヴグループ2」タブをクリックします。)



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 ポイントが加算されます。

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 Group2	○	○
Admin 2 can reset the password of User1.	○	○

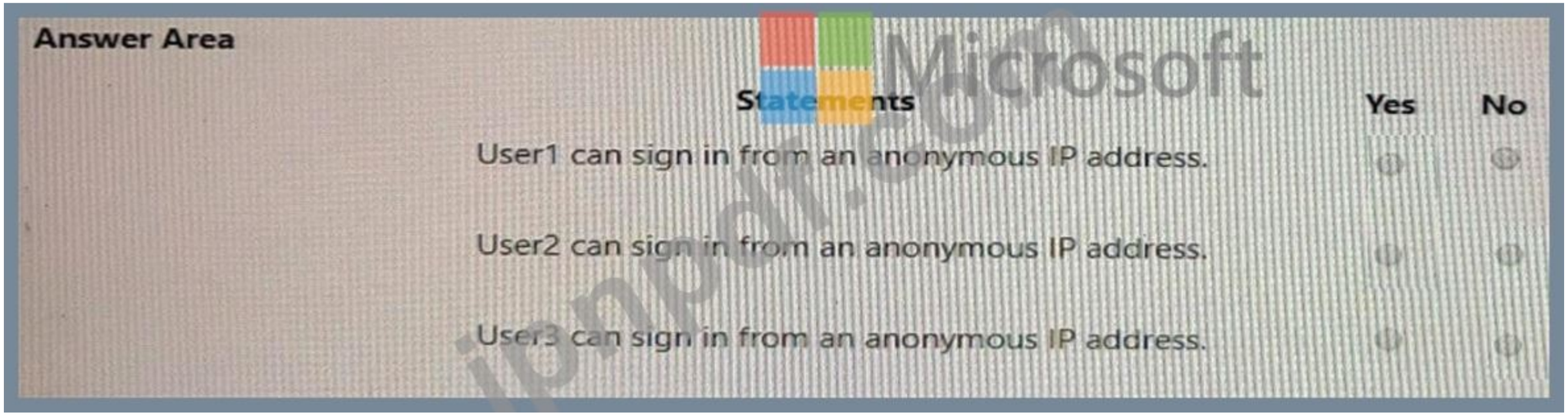
参照：
https://docs.microsoft.com/en-us/azure/active-directory/roles/管理ユニット

最新問題: **156**
次の表に示すユーザーを含む Azure AD テナントがあります。

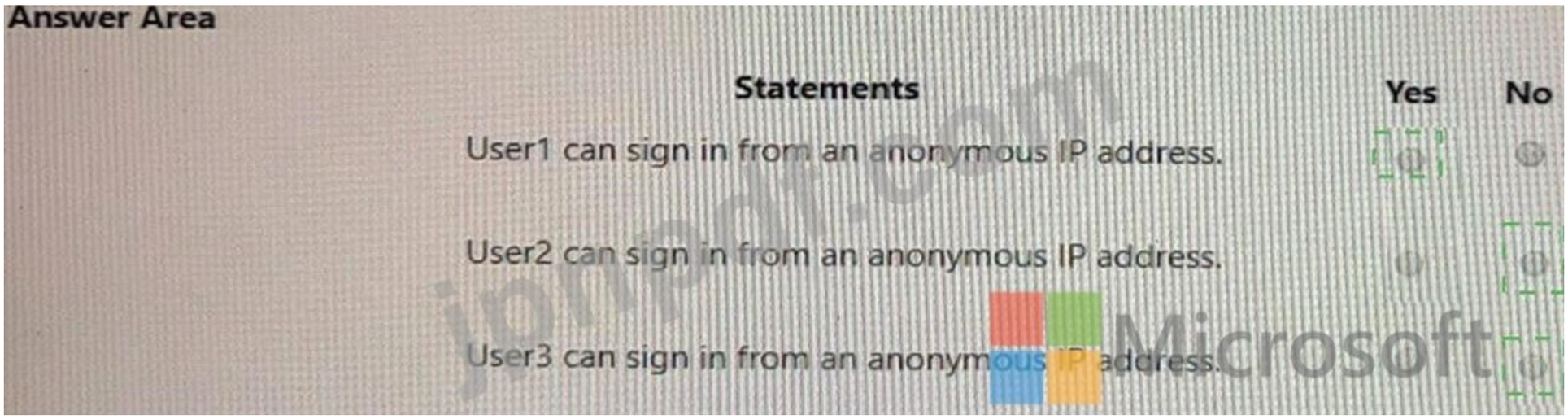
Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Enabled but never used
User2	Group2	Disabled
User3	Group1, Group2	Enforced and used

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。
* 課題:
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する
* 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。
* 課題:
o ユーザー: グループ2
o サインインリスク: 低以上
* コントロール:
o アクセス: 多要素認証を要求する
* ポリシーを強制する。オン
次の設定:
設定:
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。

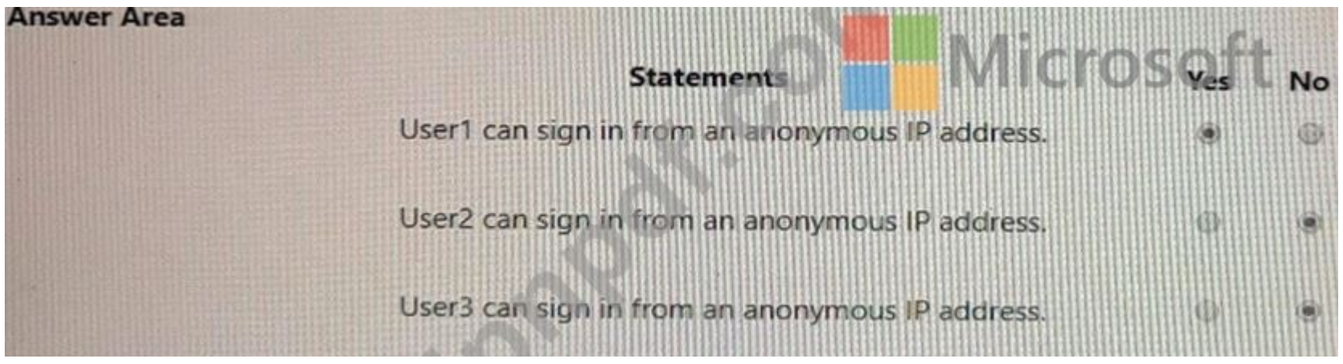
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明



最新問題: **157**

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 Area



Answer:



Explanation:



最新問題: 158

Microsoft 365 テナントがあります。

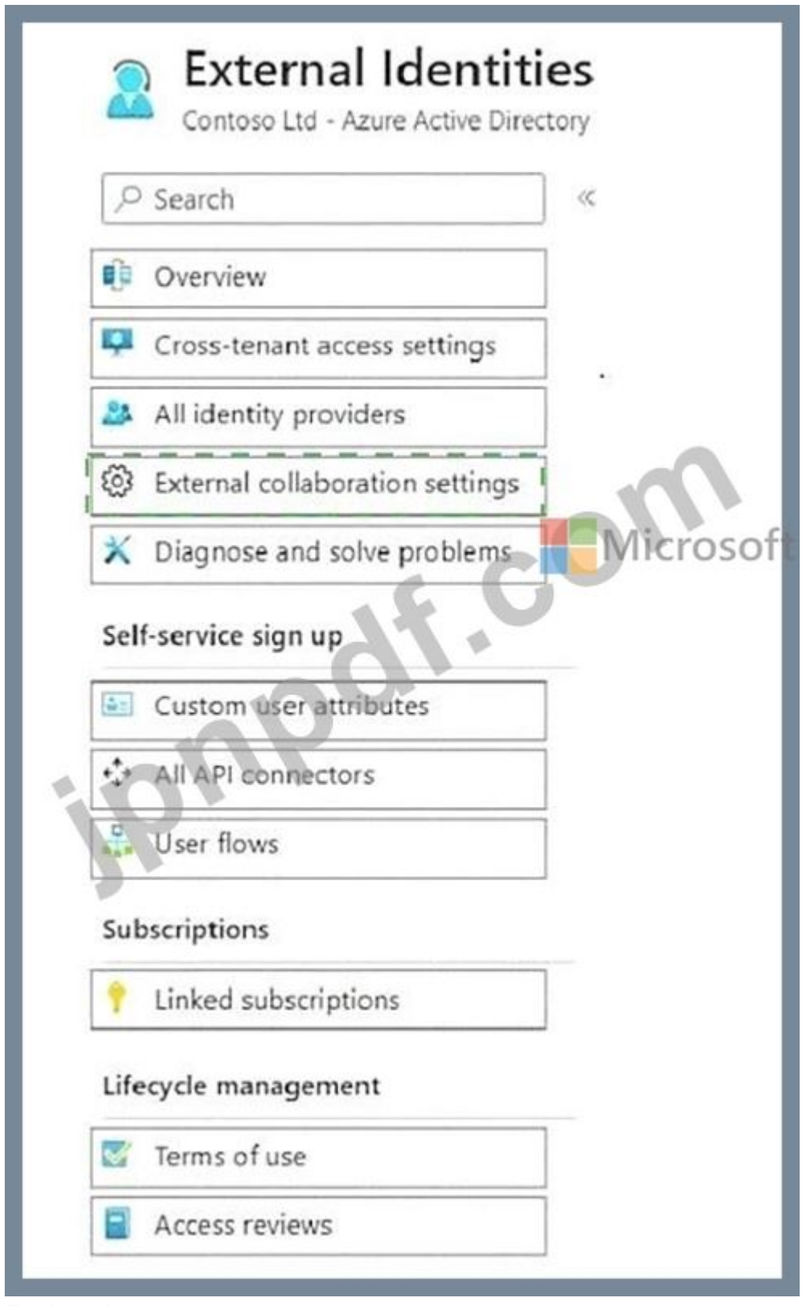
現在、基本認証を使用する電子メール クライアントが Microsoft Exchange Online に接続できるようにしています。
ユーザーが最新の認証プロトコルを使用する電子メール クライアントからのみ Exchange に接続できるようにする必要があります。
何を実装すべきでしょうか?
A. Microsoft Defender for Cloud Apps の OAuth ポリシー
B. Azure Active Directory (Azure AD) の条件付きアクセス ポリシー
C. Microsoft Endpoint Manager のコンプライアンス ポリシー
D. Microsoft Endpoint Manager のアプリケーション制御プロファイル
Answer: B (メーッセージを残す**)**
https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy- 認証

最新問題**: 159**
Microsoft Entra テナントがあります。
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
* 月間アクティブユーザー数 (MAU)に基づく価格設定
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 ポイントが加算されます。



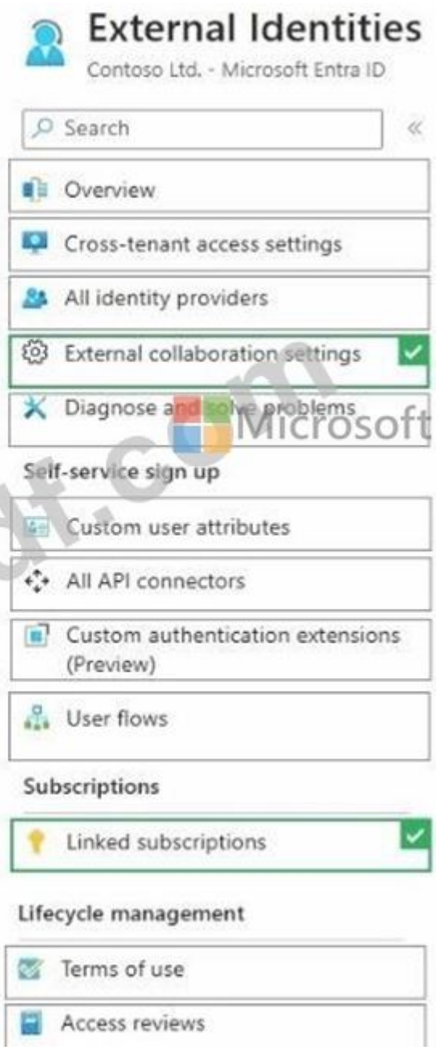
Microsoft
jpnpdf.com

Answer:



jpnpdf.com
Microsoft

Explanation:



jpnpdf.com
Microsoft

最新問題: **160**

あなたの会社には、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	Application administrator
User2	None
User3	Exchange administrator
User4	Cloud application administrator

次の表に示すアプリ登録があります。

App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

会社のポリシーにより、ユーザー権限の変更は禁止されています。
社内の各ユーザーのカレンダーに予定を作成できるのはどのユーザーですか?

A. ユーザー4
B. ユーザー1
C. ユーザー2
D. ユーザー3

Answer: D (メーッセージを残す)

最新問題**: 161**
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いくつですか？ 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：正しい選択ごとに1ポイントが加算されます。

Answer Area



Answer:
Answer Area



説明
Answer Area

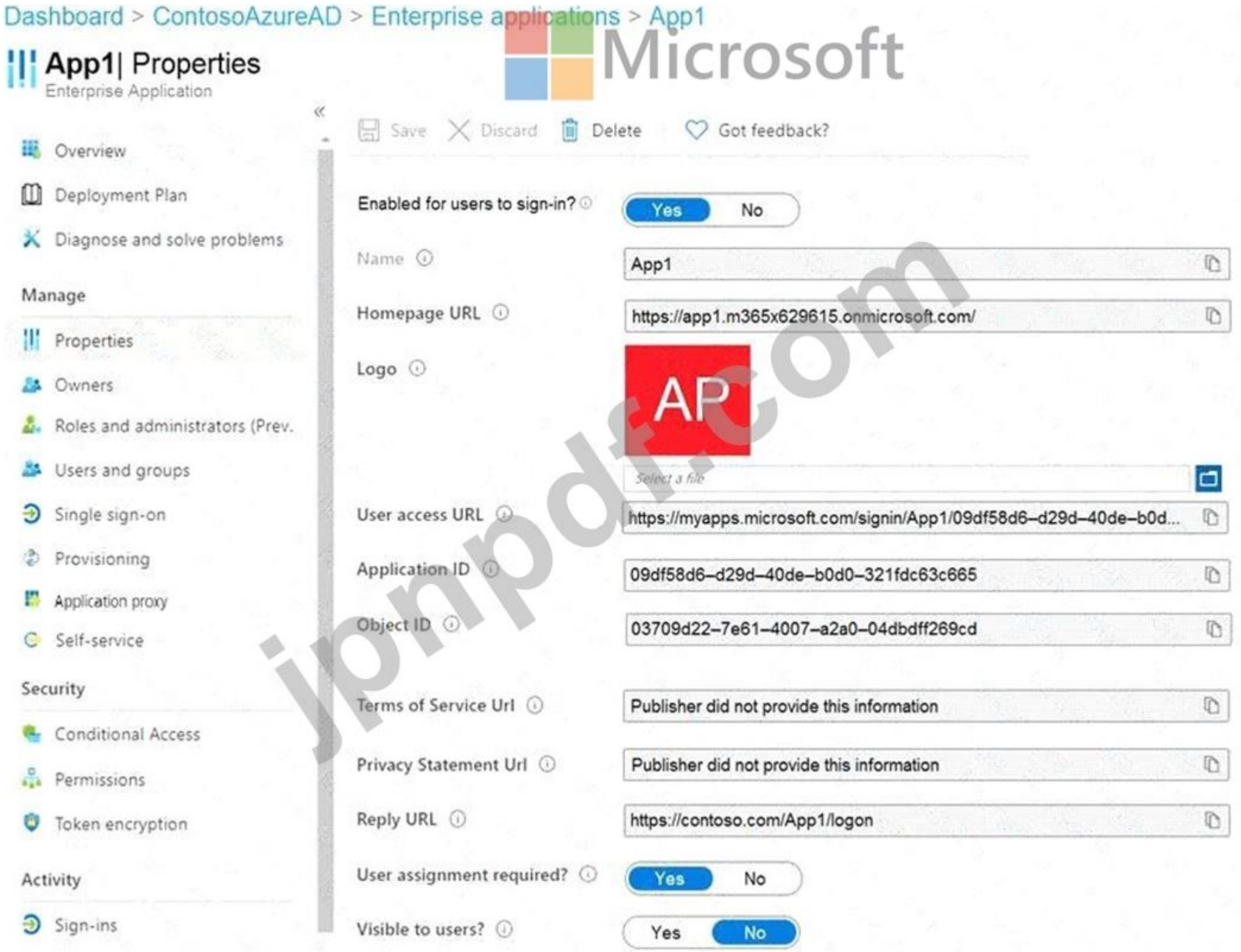


最新問題: **162**
Group1 の図に示すように、Group1 という名前のグループを含む Microsoft 365 テナントがあります。([Group1] タブをクリックします。)

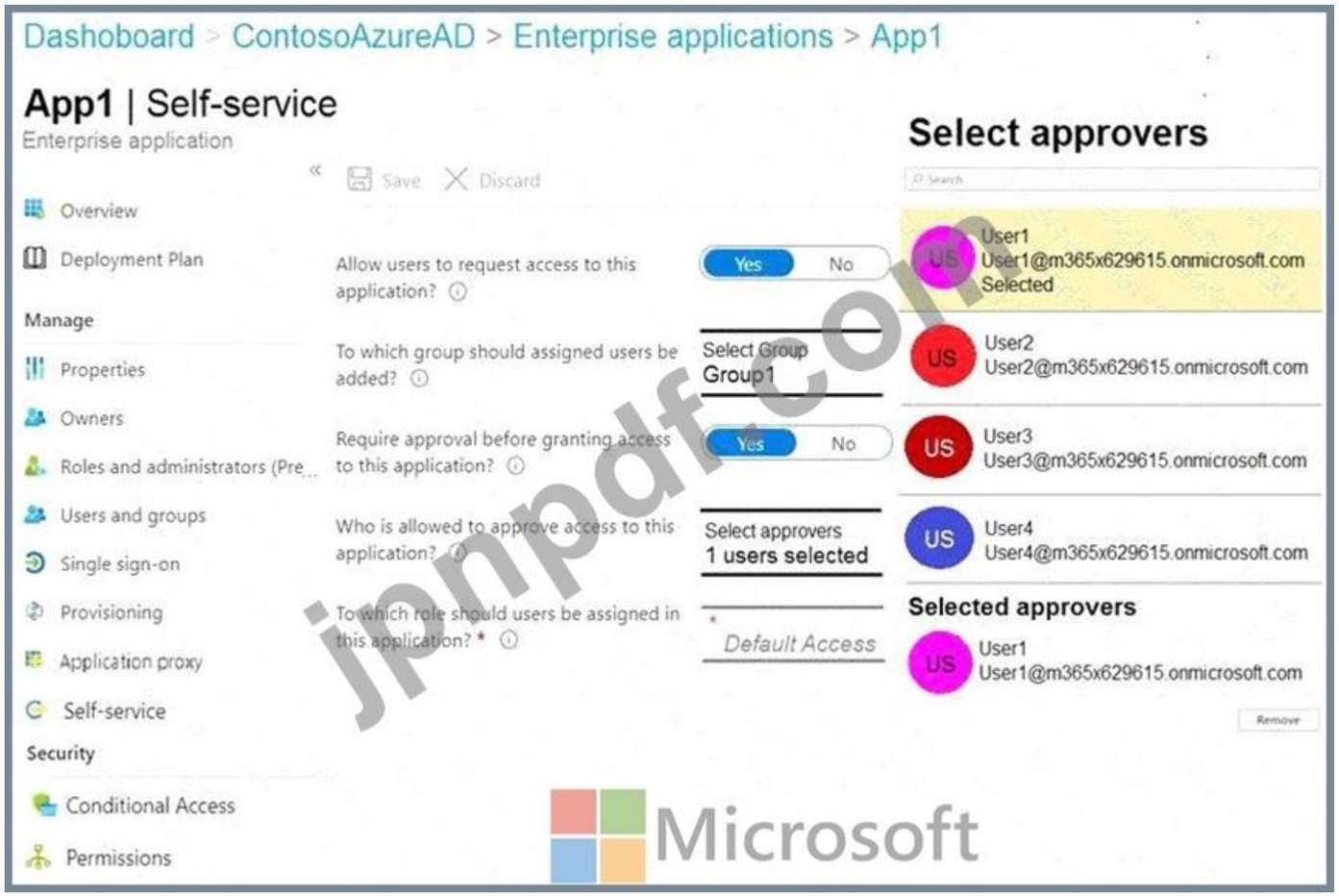


Microsoft
jpnpdf.com

App1 のプロパティ」の図に示すように、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 のセルフサービスは、App1 セルフサービス」の図に示すように構成します。(App1 セルフサービス」タブをクリックします。)



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 ポイントが加算されます。



Answer:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Explanation:
いいえ
いいえ
はい
a) アプリケーションにグループを割り当てると、そのグループ内のユーザーのみがアクセスできるようになります。割り当てはネストされたグループには適用されません。
b) ラボでテスト済み。既存の所有者は置き換えられます。また、リソース所有者への直接割り当ては最小限の権限のパスとなります。(テストで再現済み) c) アプリケーション設定の 凸ユーザーに表示」が 「いいえ」に設定されているため、ユーザーのマイアプリポータルとO365ランチャーにこのアプリケーションは表示されません。
参照
a)https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal b)おそらくhttps://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage- groups c)https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users

最新問題: **163**
ユーザー ID が侵害される可能性に関する技術要件を満たす必要があります。
ユーザーはまず何をすべきでしょうか、また何を設定すべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

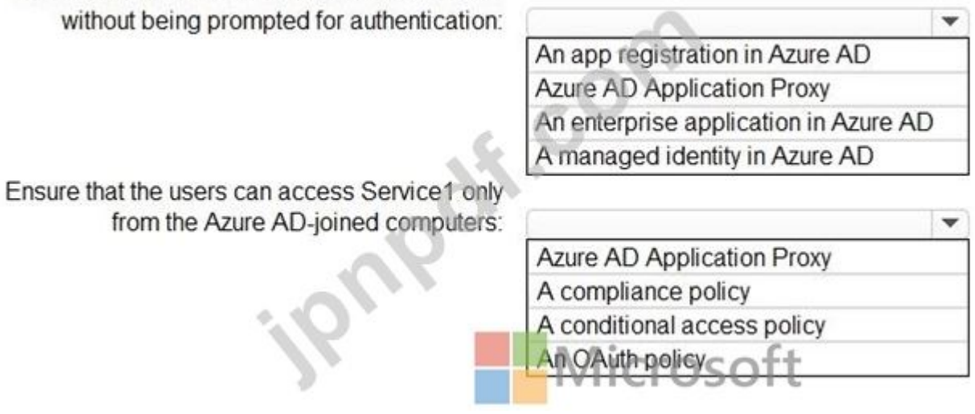


Answer:

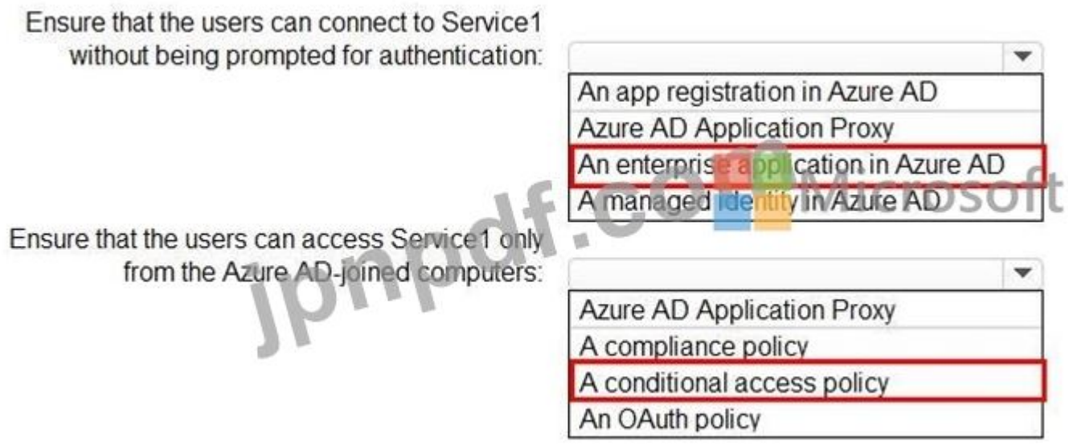


参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

最新問題: **164**
会社には Microsoft 365 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所有しています。
会社はService1という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Azure AD認証と承認をサポートしています。Service1はAzure AD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、Azure ADに参加しているコンピューターからのみユーザーがService1にアクセスできるようにする必要があります。また、管理作業を最小限に抑える必要があります。
各要件に対して何を推奨しますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

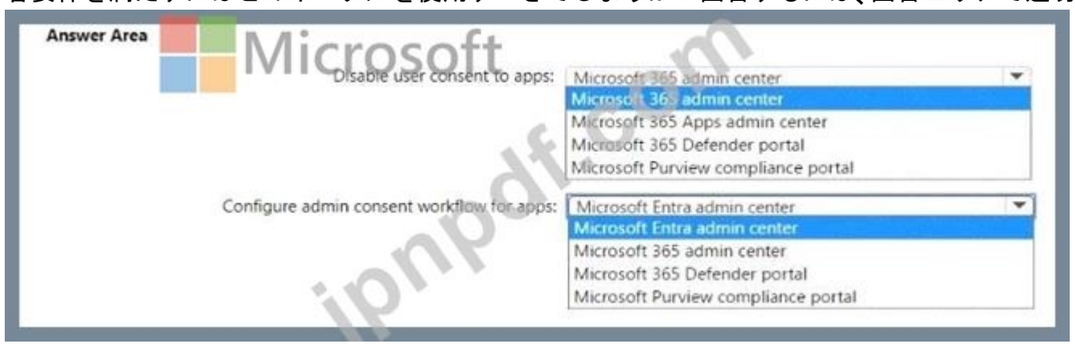


Answer:



参照：
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**: 165**
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のアプリ同意を設定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している必要があります。
* 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。
各要件を満たすにはどのポータルを使用すべきでしょうか？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：正解は1点です。



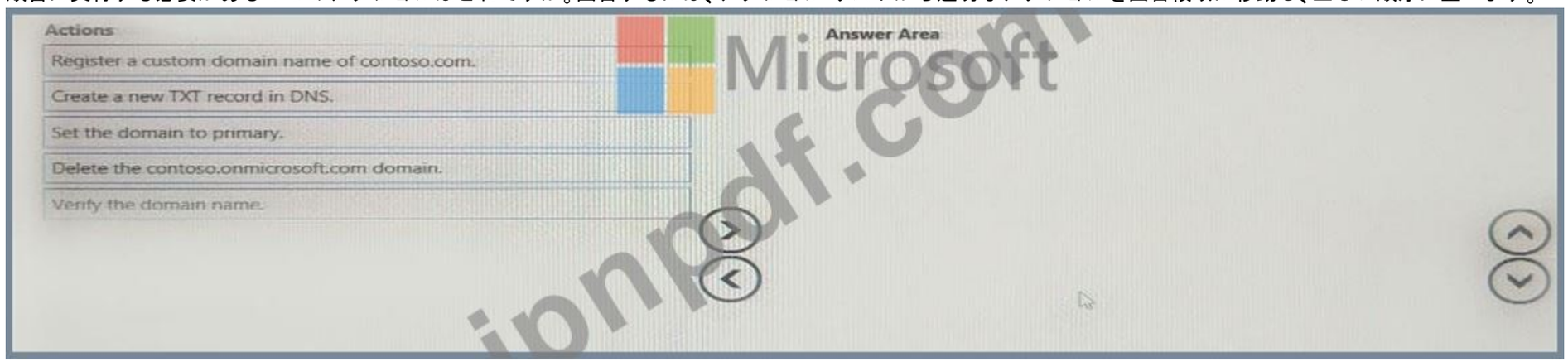
Answer:



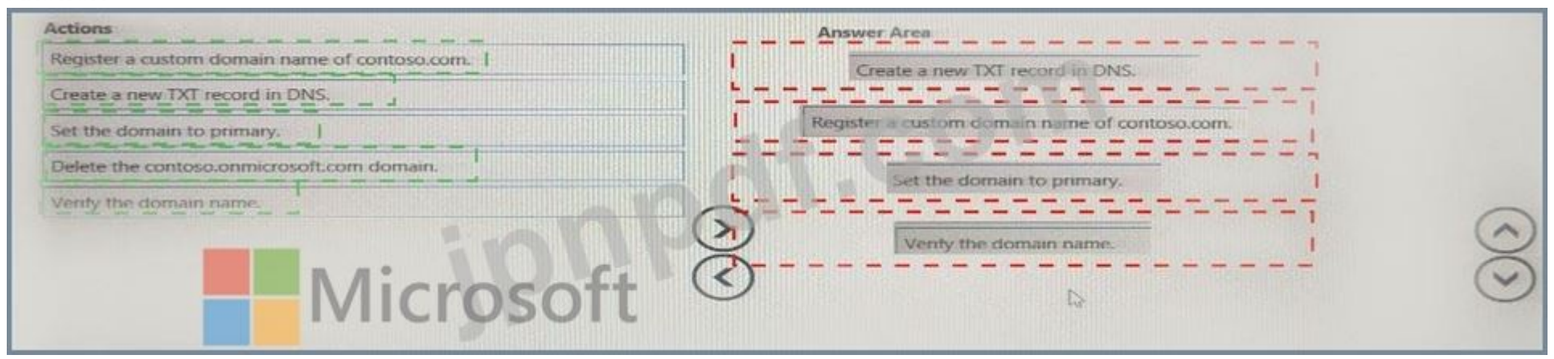
Explanation:



最新問題: **166**
contoso.conmicrosoft.com というドメイン名を使用する新しい Microsoft 365 テナントがあります。
ドメイン レジストラに contoso.com という名前を登録します。
新しい Microsoft 365 ユーザーの既定のドメイン名として contoso.com を使用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、アクション リストから適切なアクションを回答領域に移動し、正しい順序に並べます。



Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **167**
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要件を満たす必要があります。
まず何をすべきでしょうか?

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の同意要求設定を変更します。
Answer: B (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview 概要 Contoso, Ltd は、モントリオールに本社があり、ロンドンとシアトルにオフィスがあるコンサルティング会社です。
Contoso は、Fabrikam, Inc という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。

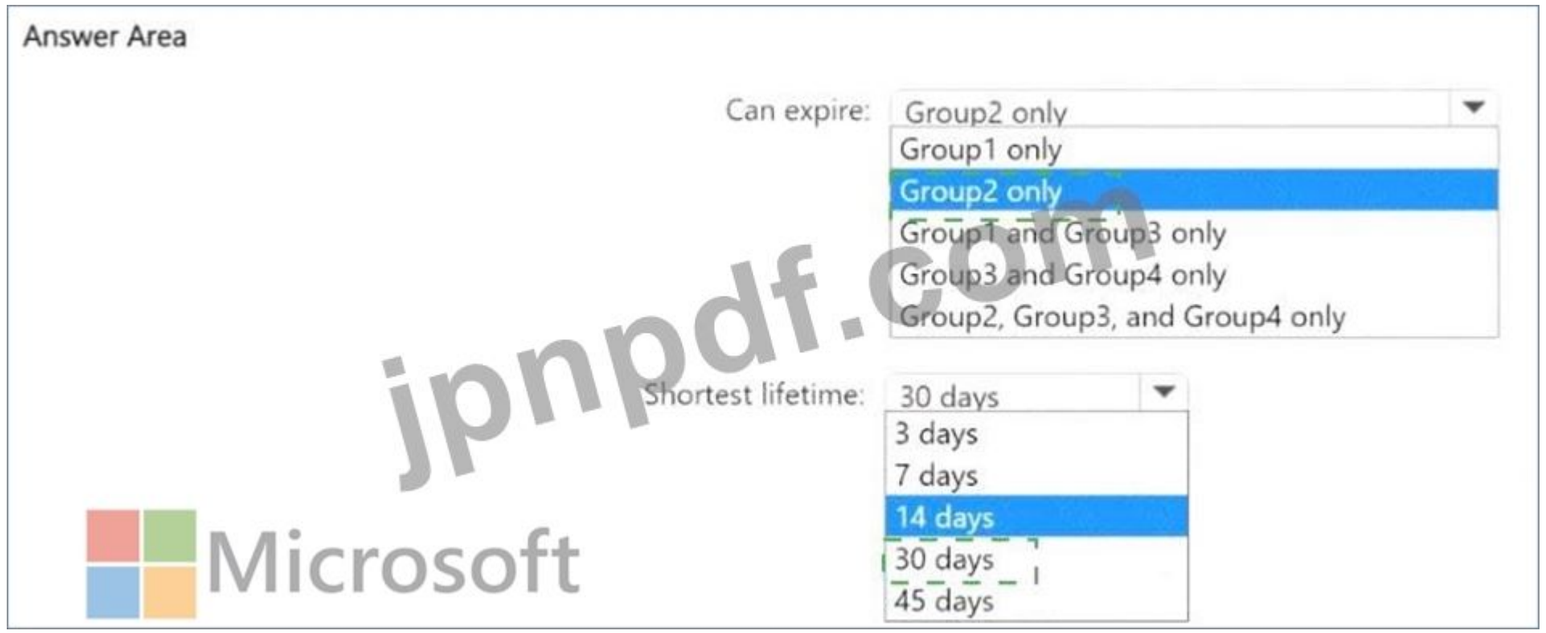
最新問題**: 168**
次の表に示すグループを含む Microsoft 365 E5 サブスクリプションがあります。

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

グループのライフサイクルを管理する予定です。
どのグループに有効期限を設定できますか。また、設定できるグループの有効期間の最短はどれくらいですか。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area



Answer:



Explanation:

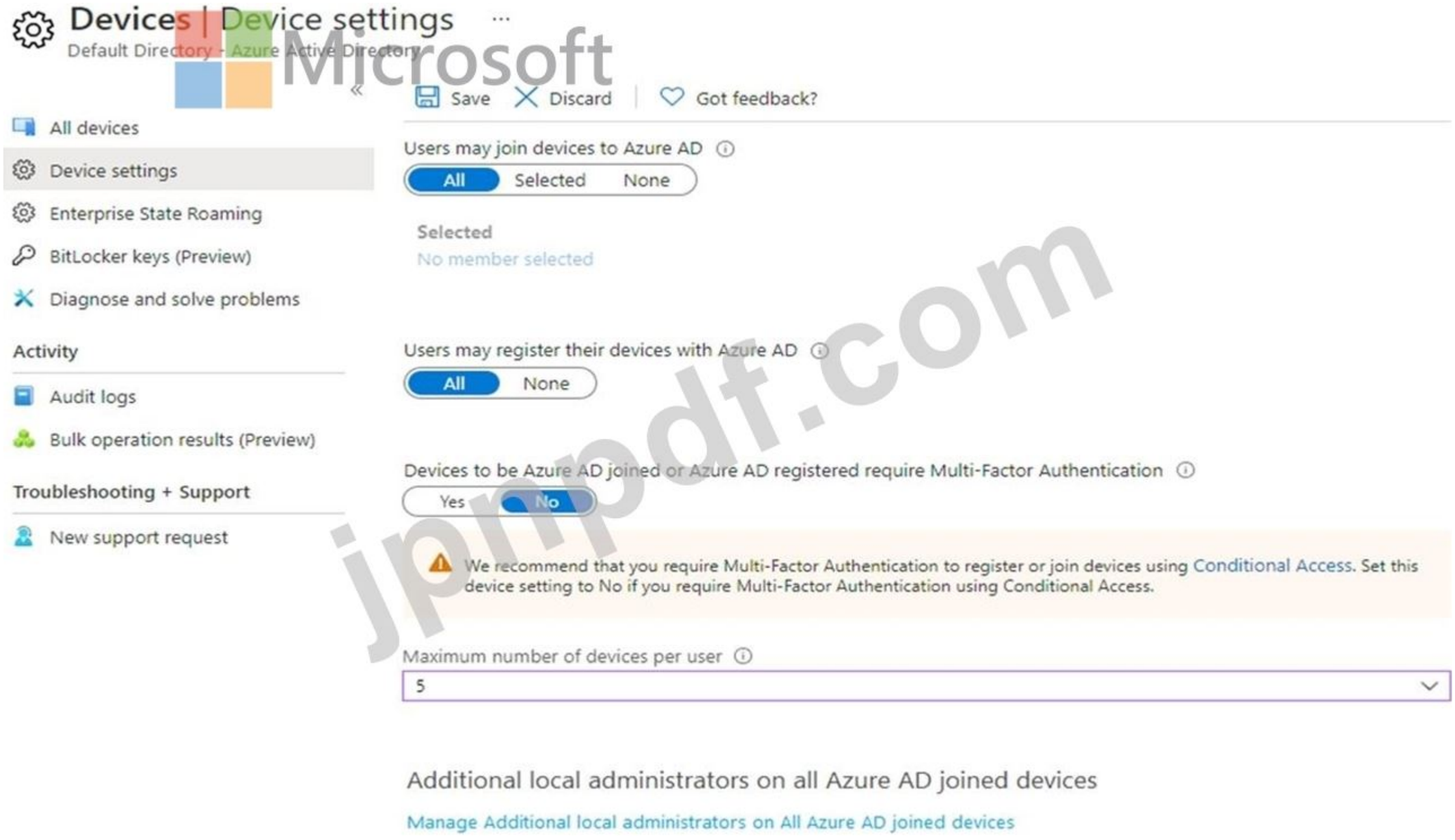


最新問題: 169

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。このテナントには、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

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 ポイントが加算されます。



Answer:



Explanation:
ボックス1: はい
ユーザーは 5 台のデバイスを Azure AD に参加させることができます。
ボックス2: はい
ボックス3: いいえ
追加のローカルデバイス管理者が適用されていません
参照：
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

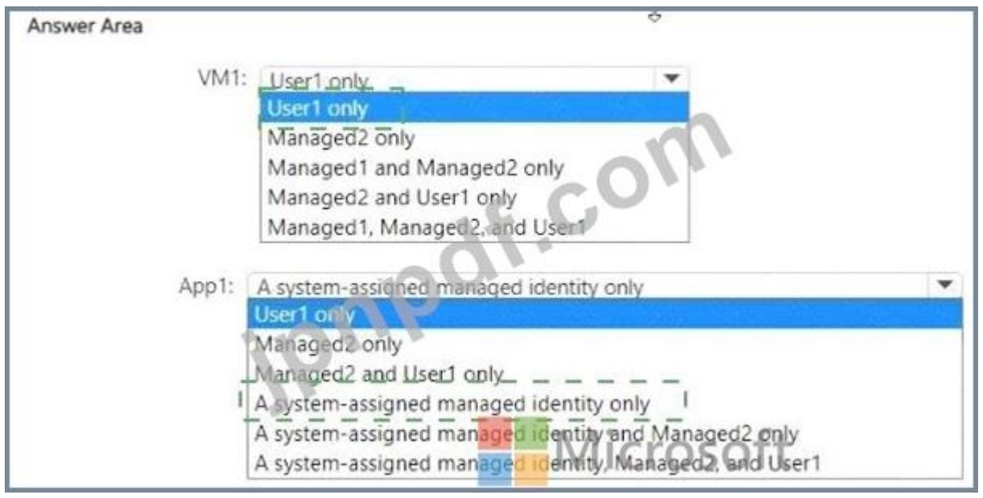
最新問題**: 170**
次の表に示すリソースを含む Azure サブスクリプションがあります。

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

User1 という名前の Microsoft Entra ユーザーを作成します。
VM1 と App1 に追加できる ID はどれですか。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。
注意: 正解ごとに 1 ポイントが加算されます。



Answer:



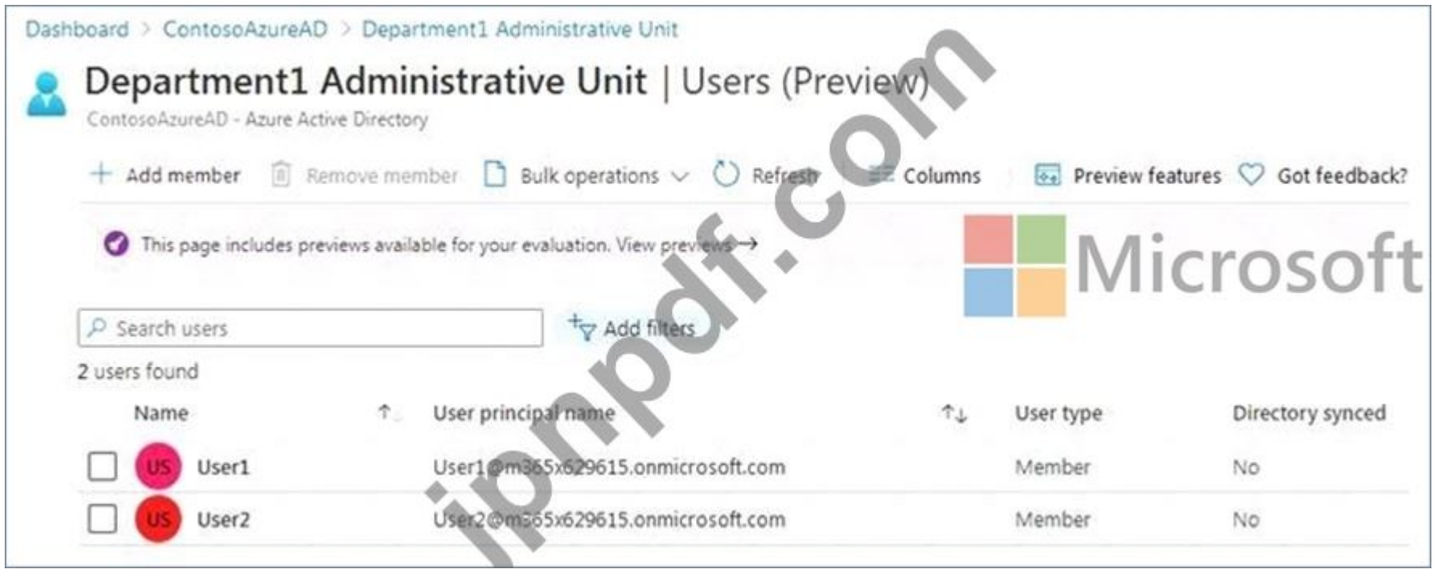
Explanation:



最新問題**: 171**

Department1 という名前の管理単位を含む Azure Active Directory (Azure AD) テナントがあります。

Department1 には、[ユーザー] 展示に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。)

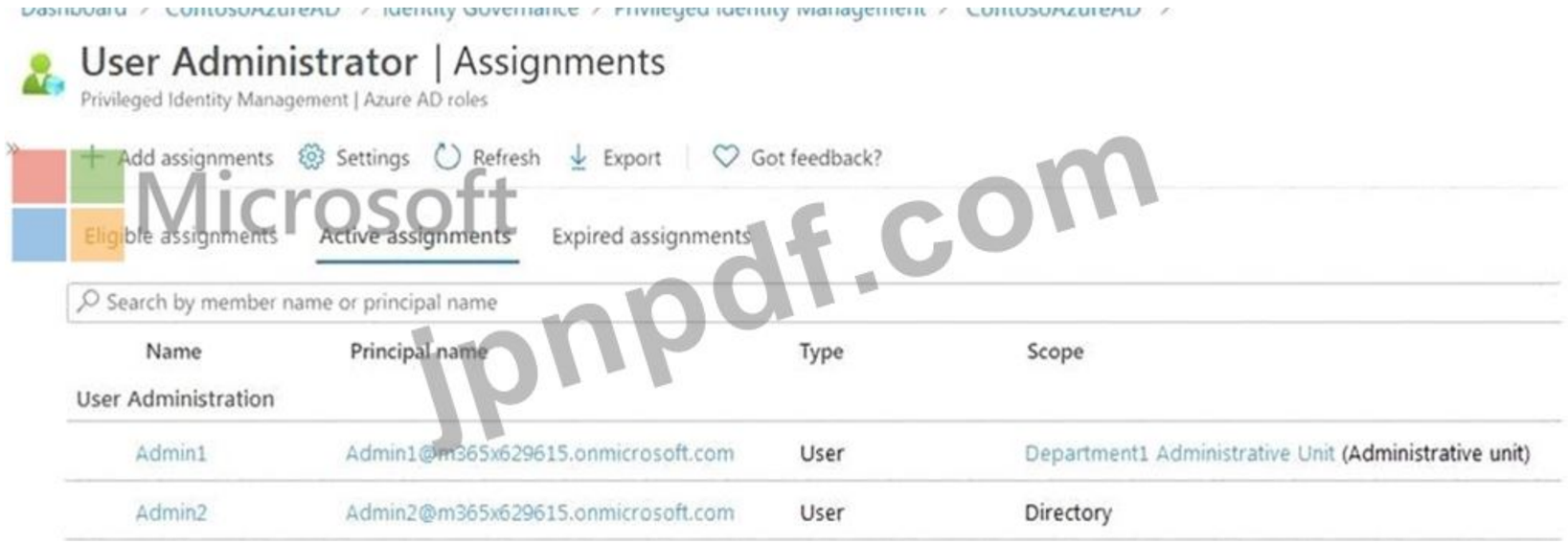


Department1 には、[グループ] 展示に示されているグループがあります。([グループ] タブをクリックします。)



Department1 には、[割り当て] 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。)

jpnpdf.com



Group2 のメンバーは、Group2 展示に表示されます。(Group2 タブをクリックします。)



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 ポイントが加算されます。

Microsoft
jpnpdf.com

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.	○	○

参照：

https://docs.microsoft.com/en-us/azure/active-directory/roles/管理ユニット

最新問題: 172

Azure Active Directory (Azure AD) テナントがあります。
過去に発生したサインインを調査するには、Azure AD サインイン ログを確認する必要があります。
Azure AD はサインイン ログにイベントをどのくらいの期間保存しますか?
A. 14日間
B. 30日間
C. 90日間
D. 365日
Answer: A (メーッセージを残す)
Azure AD の監視とレポートのドキュメントと SC-300 学習ガイド (モジュール: ID とアクセスの監視とレポート) では、Azure Active Directory のサインイン ログは既定で 14 日間保持されます。
サインインログには、アプリケーションの使用状況、条件付きアクセスポリシー、多要素認証の詳細など、ユーザーのサインインアクティビティに関する情報が含まれます。これらのログには、Azure Portal # Azure Active Directory # サインイン、またはMicrosoft Graphを介してプログラムでアクセスできます。
Microsoft は次のように指定します:
「Azure AD は、サインイン アクティビティを既定で 14 日間保存します。より長い保持期間を設定するには、Azure Monitor (Log Analytics)、Azure Storage、または Event Hub と統合する必要があります。」
この 14 日間の保持期間制限は、追加のプレミアム ログ保持ソリューションを導入していないテナントに適用されます。

最新問題**: 173**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Azure Active Directory (Azure AD) 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 Azure AD 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 Azure AD に対して認証されないようにする必要があります。
解決策: Azure AD パスワード保護を構成します。
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)
Azure AD パスワード保護は、アカウントが無効化された後のサインインを制御するようには設計されていません。SC-300 資料と Microsoft のドキュメントでは、これをパスワード強化機能として説明しています。「Azure AD パスワード保護は、グローバルな禁止パスワードリストとカスタム禁止パスワードの追加機能を提供し、ユーザーが脆弱なパスワードや侵害されたパスワードを使用することを防ぎます。」この機能は、パスワードの選択とリセットポリシーを管理するものであり、同期されたユーザーアカウントのリアルタイムの認証状態を管理するものではありません。
ご指摘の遅延は、Azure AD Connect 同期スケジューラによるものです。同期に関する試験内容において、Microsoft は「デフォルトでは、スケジューラは 30 分ごとに実行されます。変更内容のインポート、同期、エクスポートには差分同期が実行されます」と述べています。無効化操作はオンプレミスの Active Directory で行われるため、Azure AD では次回の同期サイクルが完了するまでその変更が反映されません。そのため、最近無効化されたユーザーは、その間隔まで認証を続行できる可能性があります。
したがって、パスワード保護を有効にしても、Azure AD 認証を即座に阻止するという目標は達成されません。SC-300 ガイダンスでは、即時の効果を実現するために、パスワード保護を構成するのではなく、オンデマンドの差分同期を開始する、Azure AD でアカウントを直接無効化する、Entra ID 経由でサインインセッション/トークンを取り消すなどのアクションが示されています。

最新問題**: 174**
次の表に示すグループを含む Azure Active 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
Group5	Microsoft 365	Dynamic User

どのグループに対してアクセス レビューを作成できますか?

A. グループ1のみ

B. グループ1とグループ4のみ

C. グループ1とグループ2のみ

D. グループ1、グループ2、グループ4、グループ5のみ

E. グループ1、グループ2、グループ3、グループ4、グループ5

Answer: D (メーッセージを残す**)**

デバイス グループのアクセス レビューを作成することはできません。

参照：

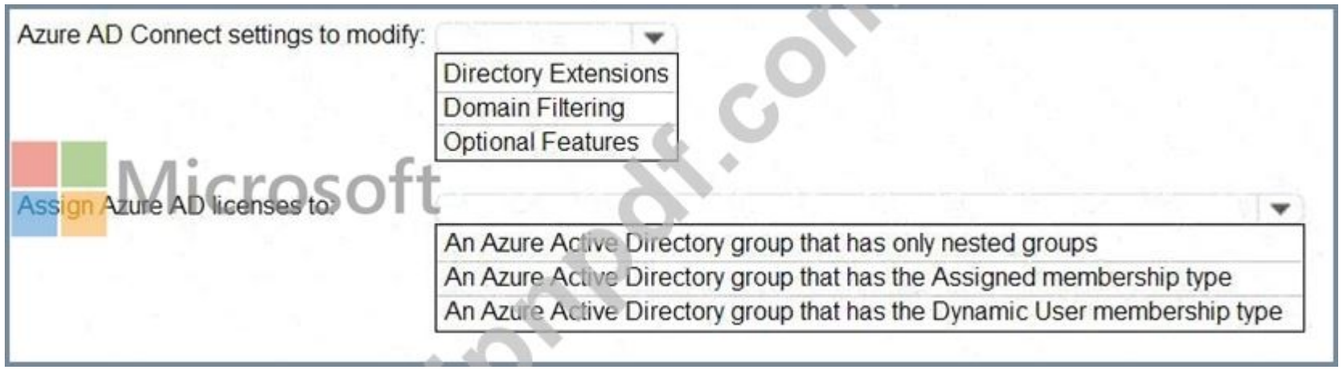
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

最新問題**: 175**

Litware ユーザーへの Azure AD ライセンスの割り当てを構成する必要があります。ソリューションはライセンス要件を満たしている必要があります。

どうすればいいでしょうか? 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。

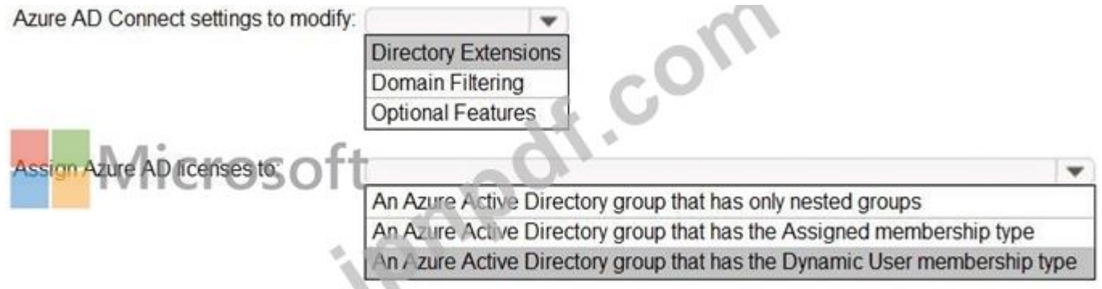
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



Litware は最近、litware.com Active Directory フォレストに LWLicenses という名前のカスタム ユーザー属性を追加しました。
Litware は、LWLicenses 属性の値を変更することで、Azure AD ライセンスの割り当てを管理したいと考えています。LWLicenses 属性に適切な値を持つユーザーは、適切なライセンスが割り当てられている Microsoft 365 グループに自動的に追加される必要があります。
トピック2、Contoso株式会社
概要
Contoso 社は、モントリオールに本社を置き、ロンドンとシアトルにオフィスを構えるコンサルティング会社です。
Contoso は、Fabrikam, Inc という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。
既存の環境
Contoso 社のオンプレミスネットワークには、contos.com という Active Directory ドメインが含まれています。このドメインには、Contoso_Resources という組織単位 (OU) が含まれています。Contoso_Resoureces OU には、すべてのユーザーとコンピューターが含まれています。
Contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

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

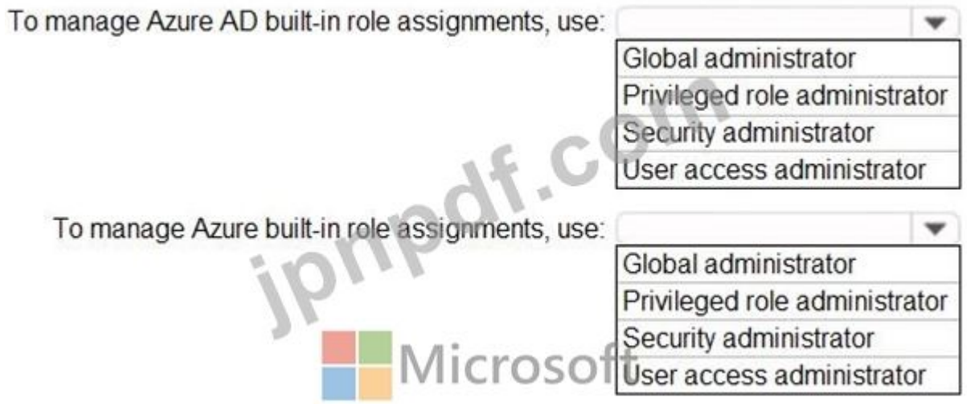
Microsoft 365/Azure 環境
Contoso には、次の関連ライセンスを持つ Contoso.com という名前の Azure AD テナントがあります。
* マイクロソフト Office 365 エンタープライズ E5
* エンタープライズモビリティ + セキュリティ
* Windows 10 エンタープライズ E5
* プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory Domain Serverless (AD DS) の間で構成されています。Contoso Resources OU のみが同期されます。
ヘルプデスク管理者は、通常、Microsoft 365 管理センターを使用してユーザー設定を管理します。
ユーザー管理者は現在、Microsoft 365 管理センターを使用してライセンスを手動で割り当てています。次の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
ロンドンオフィスのユーザーは、Microsoft 365 管理センターを使用して手動でライセンスを割り当てることができます。以下の例外を除き、すべてのユーザーにライセンスが割り当てられています。
* ロンドン オフィスのユーザーには、Microsoft 365 電話システム ライセンスが割り当てられていません。
* シアトル オフィスのユーザーには、Yammer Enterprise ライセンスが割り当てられていません。
Contoso.com ではセキュリティの既定値が無効になっています。

Contoso は、Azure AD Privileged Identity Management (PIM) を使用してプロジェクト管理者ロールを実行します。
問題ステートメント
Contoso は次の問題を特定しています。
* 現在、すべてのヘルプデスク管理者は、Microsoft 365 テナント全体のユーザー ライセンスを管理できます。
* ユーザー管理者は、Contoso オフィスごとに異なるライセンス要件を手動で構成するのは面倒だと報告しています。
* ヘルプデスク管理者は、必要な Microsoft 365 サービスとアプリへの内部アクセスとゲスト アクセスのプロビジョニングに多くの時間を費やしています。
* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
* Azure AD でログ ノードを選択すると、Log Analytics 統合が有効になっていないことを示すエラー メッセージが表示されます。
計画された変更
Contoso は次の変更を実装する予定です。
セルフサービスパスワードリセット (SSPR) を実装します。Azure Monitorを使用してAzure監査アクティビティログを分析し、テナントに追加された新規ユーザーへのライセンス割り当てを簡素化します。Fabrikamのユーザーと協力して共同マーケティングキャンペーンを実施します。ユーザー管理者ロールを構成し、アクティベーションに正当な理由と承認が必要になります。
App1 という名前のカスタム基幹業務 Azure Web アプリを実装します。App1 はインターネットからアクセスでき、Azure AD アカウントを使用して認証されます。
マーケティング部門の新規ユーザーに対して、自動承認ワークフローを実装して、Microsoft SharePoint Online サイト、グループ、アプリへのアクセスを提供します。
Contoso社はCorporation社という会社を買収する予定です。AdatumというActive Directory組織単位 (OU) に、新たにA Datumユーザー100名が作成されます。ユーザーはロンドンとシアトルに拠点を置く予定です。
技術要件
Contoso では、次の技術要件を特定しています。
* AH ユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのみのライセンスを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。

最新問題: **176**
Microsoft Entta ID P2 ライセンスを持つ Microsoft Entra テナントがあり、Log Analytics ワークスペースを作成します。
Azure Monitor を使用して Microsoft Entra ID 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。
まず何をすべきでしょうか?
A. Microsoft Entra ID ブックを作成します。
B. Microsoft Entra ID の診断設定を変更します。
C. update-ngoomain コマンドレットを実行します。
D. update-Mgorganization コマンドレットを実行します。
Answer: B (メーッセージを残す)
Microsoft SC-300 学習ガイドおよび Microsoft Learn モジュール 「Microsoft Entra ID の監視とトラブルシューティング」によれば、Azure Monitor (および Log Analytics ワークスペース) で Microsoft Entra ID 監査ログ情報を表示するには、まず Microsoft Entra ID の診断設定を構成する必要があります。
デフォルトでは、Entra ID 監査ログは Microsoft Entra ポータル内に 30 日間 (P1 の場合) または 180 日間 (P2 の場合) 保持されます。これらのログを Azure Monitor に統合して高度な分析、アラート、および保持を行うには、管理者が診断設定を通じてログのエクスポートを明示的に有効にし、指示する必要があります。
手順は次のとおりです:

* Microsoft Entra 管理センターで、[監視] # [診断設定] に移動します。
* 監査ログ (およびオプションでサインイン ログ) を選択します。
* [Log Analytics ワークスペースに送信] を選択し、目的のワークスペースを選択します。
この構成により、Entra ID 監査データを Azure Monitor に継続的にストリーミングし、Kusto クエリ言語 (KQL) を使用してクエリできるようになります。
ワークブックの作成や PowerShell コマンドレット (update-MgOrganization または update-ngoomain) の実行などの他のオプションでは、ログ転送は開始されません。

最新問題: 177
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要件を満たす必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



参照：
https://docs.microsoft.com/en-us/azure/ロールベースのアクセス制御/ロール割り当てポータル
https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

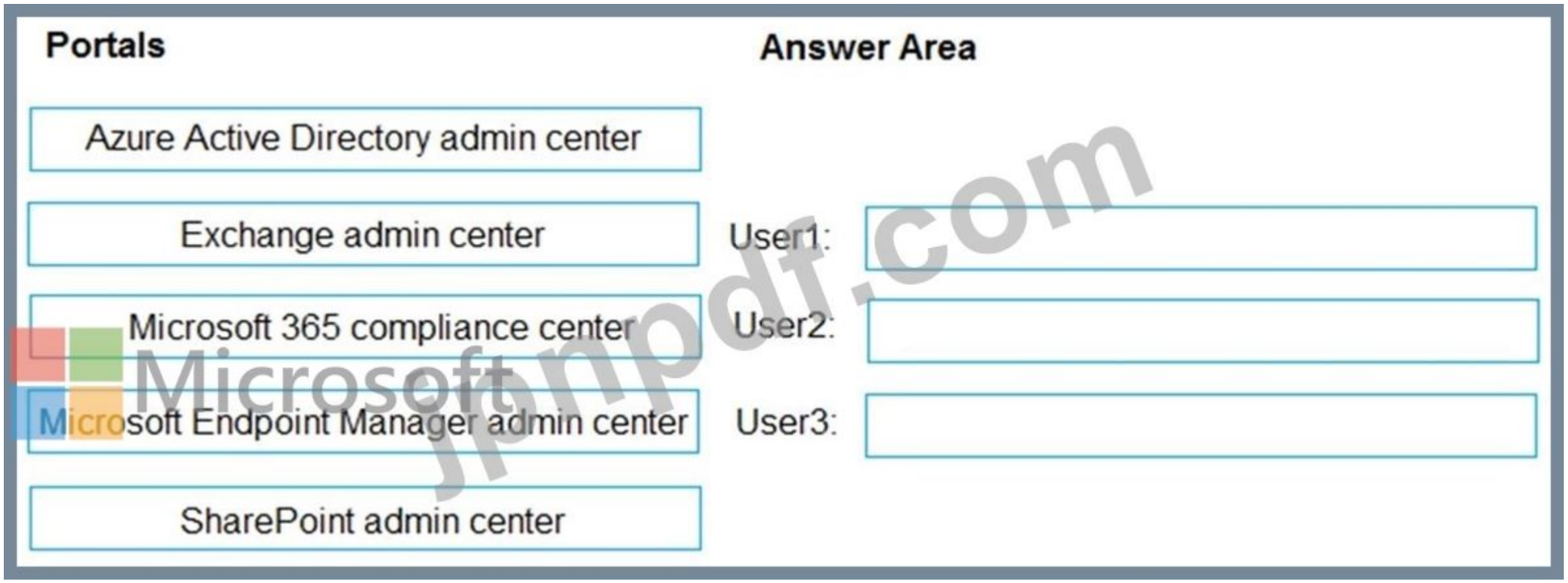
最新問題: 178
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Defender for Cloud Apps セッション ポリシーを作成する必要があります。

まず何をすべきでしょうか?
A. Microsoft Defender for Cloud Apps ポータルから、ユーザーの監視を選択します。
B. Microsoft Defender for Cloud Apps ポータルから、[アプリのオンボード/メンテナンス] を選択します。
C. Azure Active Directory 管理センターから、条件付きアクセス ポリシーを作成します。
D. Microsoft Defender for Cloud Apps ポータルから継続的なレポートを作成します。
Answer: C (メーッセージを残す)
Microsoft Identity and Access Administrator (SC-300) 学習ガイド、試験参照番号 SC-300、および Microsoft Defender for Cloud Apps (MDCA) のドキュメントによると、Defender for Cloud Apps (旧称 Microsoft Cloud App Security) のセッション ポリシーは、ユーザー セッションをリアルタイムで監視および制御するために使用されます。
これらのポリシーは、ダウンロードの制限、アップロードのブロック、Defender for Cloud Apps と統合された SaaS アプリケーションでのユーザー アクティビティの監視など、きめ細かいセッション レベルのアクセス制御を提供します。
ただし、セッションポリシーが機能するには、アプリの条件付きアクセス制御機能を有効にする必要があります。この統合により、Azure Active Directory (Azure AD) と Microsoft Defender for Cloud Apps が接続され、条件付きアクセスポリシーを通じてセッション制御を適用できるようになります。
SC-300 公式トレーニング コンテンツの 『Microsoft Defender for Cloud Apps の実装と構成」には、次のように記載されています。
Microsoft Defender for Cloud Apps を使用してセッション制御を適用するには、まずAzure AD で条件付きアクセス ポリシーを構成し、ユーザーセッションを Defender for Cloud Apps にルーティングして検査する必要があります。この手順を実行した後にのみ、Defender for Cloud Apps ポータル内でセッションポリシーを定義できます。したがって、正しい最初の手順は、Azure AD で 条件付きアクセス アプリ制御を使用する」オプションを使用する条件付きアクセス ポリシーを作成することです。このアクションにより、Defender for Cloud Apps のセッション制御ポリシーが有効になるために必要な接続パスが確立されます。

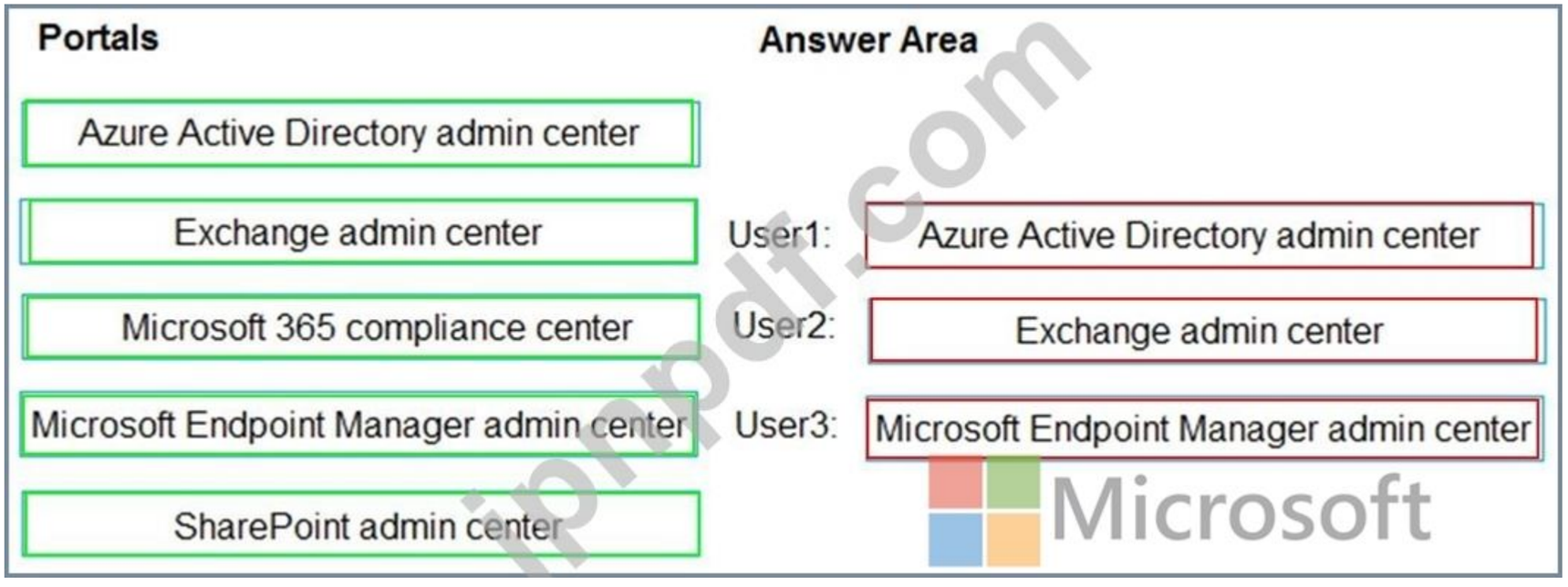
最新問題: **179**
Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
次の表に示すようにユーザーを構成する必要があります。

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

各ユーザーを設定するにはどのポータルを使用すればよいでしょうか？適切なポータルを適切なユーザーにドラッグしてください。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **180**

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

* Device1という名前のデバイス
* User1、User2、User3、User4、User5という名前のユーザー

* グループ1、グループ2、グループ3、Ciroup4、グループ5という5つのグループ
グループは次の表のように構成されます。

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	Group5
Group5	Microsoft 365	Assigned	User5

Microsoft Office 365 Enterprise E5 ライセンスを Group1 に割り当てた場合、使用されるライセンスの数はいくつですか?

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

Answer: B (メーッセージを残す**)**

参照：
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

最新問題**: 181**
次の表に示すホストを含むオンプレミス 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

Active Directory フォレストと同期する Azure Active 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 Azure AD ユーザーに公開できることを確認する必要があります。
Server と Firewall1 で何を設定す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **182**
Azure Active Directory (Azure AD) テナントがあります。
テナントの場合、ユーザーはアプリケーションを登録できますが、[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 Azure AD に App1 を登録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、最小権限の原則を適用する必要があります。
Admin1 に割り当てるべきロールはどれですか?
A. Azure AD のアプリケーション開発者
B. サブスクリプション1のアプリ構成データ所有者
C. サブスクリプション1の管理対象アプリケーション共同作成者
D. Azure AD 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**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール Azure AD でのアプリケーション登録の管理」によると、Azure Active Directory にアプリケーションを登録する機能は、ユーザー設定の下にあるテナントレベルの設定 「ユーザーはアプリケーションを登録できる」によって制御されます。
アプリの登録。
この設定を 「いいえ」に設定すると、アプリ登録権限を持つ特定のロールのみがアプリ登録を作成または管理できます。最小権限の原則に従うため、適切なロールにはアプリケーションの登録権限のみを付与し、より広範な管理権限は付与しないでください。
アプリケーション登録に関連する権限を持つロールには次のものがあります。
アプリケーション開発者 - ユーザーが所有するアプリケーションの登録と管理を許可します。このロールは、テナント設定が無効になっている場合にアプリ登録を作成する必要があるユーザー向けに特別

に設計されています。
クラウド アプリケーション管理者とアプリケーション管理者 - このシナリオに必要な最小限の範囲を超える、すべてのアプリケーション、資格情報、およびアクセス許可の管理を含む、より広範な権限を付与します。
マネージド アプリケーション共同作成者とアプリ構成データ所有者 - Azure リソース レベルのロールであり、Azure AD アプリケーションの登録とは関係ありません。
Microsoft のドキュメントより:
「ユーザーはアプリケーションを登録できます」が「いいえ」に設定されている場合、アプリを登録する必要があるユーザーにアプリケーション開発者ロールを割り当てます。」したがって、最小権限の原則に従いながら Admin1 が App1 を登録できるようにするには、アプリケーション開発者ロールを割り当てます。

最新問題**: 183**
次の表に示すユーザーを含む AzureAD テナントがあります。

Name	Member of	Multi-factor authentication (MFA)
User1	Group1	Disabled
User2	Group2	Enforced

次の表に示す場所があります。

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

テナントには、次の構成を持つ名前付き場所が含まれます。
* 名前: location1
* 信頼できる場所としてマーク: 有効
* IPv4範囲: 10.10.0.0/16
MFA には、193.17.17.0/24 の信頼できる iPad ドレス シリーズがあります。
次の設定を持つ条件付きアクセス ポリシーがあります。
* 名前: CAPolicy1
* 課題
o ユーザーまたはワークロード ID: グループ 1
o クラウドアプリまたはアクション: すべてのクラウドアプリ
* 条件
* 場所 信頼できるすべての場所
* アクセス制御
o と
* アクセスを許可する: 多要素認証を要求する
セッション: 選択されたコントロールは 0 件です
* ポリシーを有効にする: オン
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：正しい選択は1つにつき1点となります。



Answer:



最新問題**: 184**

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	Disabled
User2	Group2	Enforced

次の表に示す場所があります。

Name	Private address space	Public NAT address space
Location1	10.10.0.0/16	20.93.15.0/24
Location2	192.168.0.0/16	193.17.17.0/24

テナントには、次の構成を持つ名前付き場所が含まれています。

* 名前: location1
* 信頼できる場所としてマーク: 有効
* IPv4範囲: 10.10.0.0/16

MFA には、193.17.17.0/24 の信頼できる iPad ドレス シリーズがあります。

次の設定を持つ条件付きアクセス ポリシーがあります。

* 名前: CAPolicy1
* 課題

o ユーザーまたはワークロード ID: グループ 1

o クラウドアプリまたはアクション: すべてのクラウドアプリ

* 条件
* 場所 信頼できるすべての場所
* アクセス制御

o と

* アクセスを許可する: 多要素認証を要求する

セッション: 選択されたコントロールは 0 件です
* ポリシーを有効にする: オン
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：正しい選択は1つにつき1点となります。



Answer:



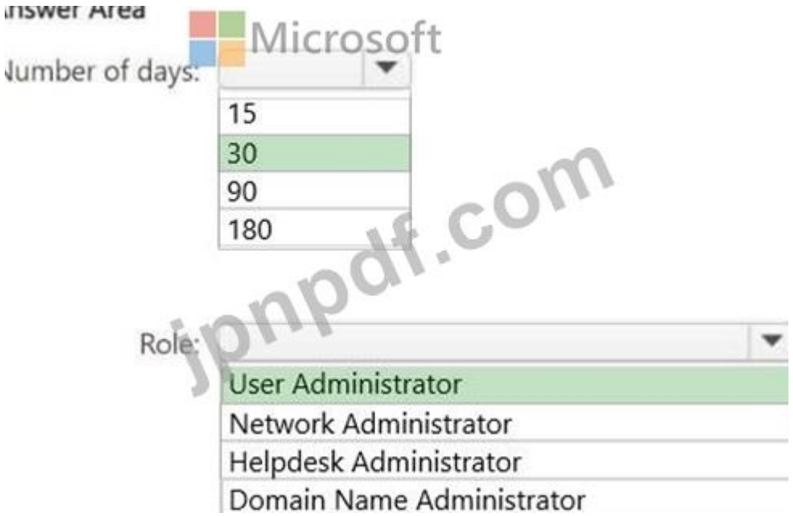
Explanation:



最新問題: **185**
ホットスポットに関する質問
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。
- 選択できる最大日数は？
User1 アカウントを復元しますか?
- 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てください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



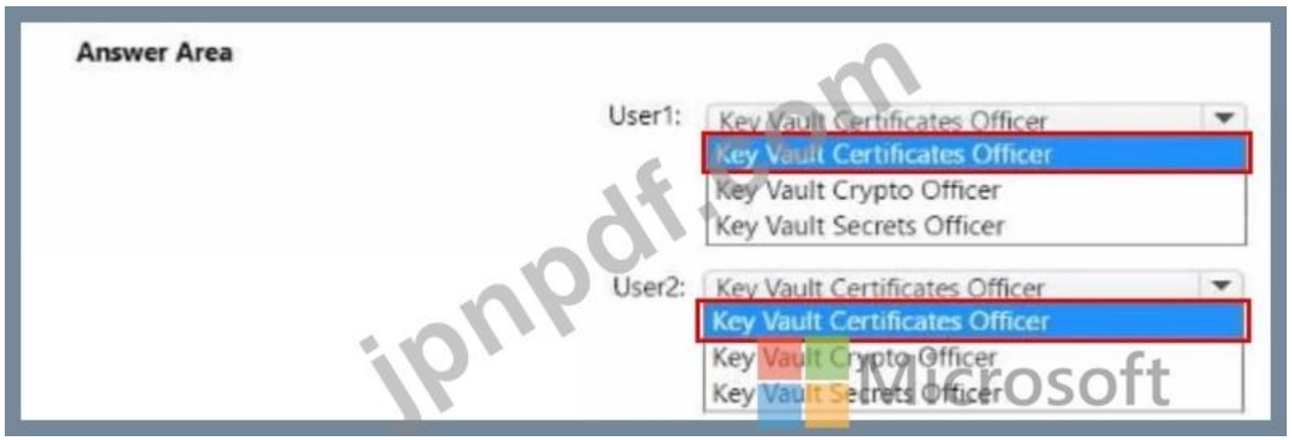
Explanation:
ボックス1: 30
Microsoft Entra ID（旧Azure AD）では、削除されたユーザーは30日以内であれば復元できます。30日を過ぎるとアカウントは完全に削除され、復元できなくなります。
ボックス2: ユーザー管理者
ユーザー管理者の役割は、Microsoft Entra ID で削除されたユーザーアカウントを復元するために必要な権限を持つ、最も権限の少ない役割です。ネットワーク管理者やドメイン名管理者などの他の役割には、ユーザーアカウントを管理するために必要な権限がありません。

最新問題**: 186**
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。ソリューションは以下の要件を満たしている必要があります。
* 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。

* 最小権限の原則を使用します。
各ユーザーにはどのような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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: 187
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、次の表に示すユーザーが含まれています。

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。
Azure AD Connect は、次の図に示すように Azure AD で構成されます。



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 Azure AD 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. ユーザー1のみ

C. ユーザー1、ユーザー2、ユーザー3

D. ユーザー1とユーザー2のみ

Answer: (解答を表示する**)**

参照：

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/pta への接続方法 - 現在の制限

最新問題**: 188**

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	Group
User1	Group1
User2	Group1
User3	Group2
User4	Group2
User5	None

Au1 という名前の管理単位があります。Group1、User2、および User3 は Au1 のメンバーです。

User5 には Au1 のユーザー管理者ロールが割り当てられます。

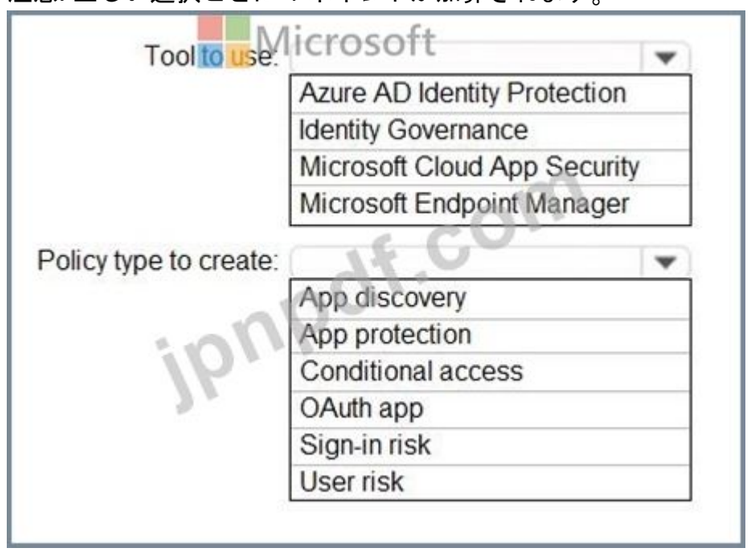
User5 はどのユーザーのパスワードをリセットできますか?

A. ユーザー2とユーザー3のみ

B. ユーザー1、ユーザー2、ユーザー3
C. ユーザー3とユーザー4のみ
D. ユーザー1とユーザー2のみ
Answer: (解答を表示する**)**

最新問題**: 189**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
このセクションで質問に回答した後は、そのセクションに戻ることはできず、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。
Amazon Web Services (AWS) アカウント、Google Workspace サブスクリプション、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、Google Workspace アプリ コネクタを追加します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: (解答を表示する**)**

最新問題**: 190**
Microsoft 365 テナントがあります。
ユーザーは、Microsoft 365 データへの限定的なアクセスを必要とする外部のサードパーティ製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、これらの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権を取得した場合にアラートを受信する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題**: 191**
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 Azure AD パスワード保護 DC エージェントをインストールします。
次に何をすべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



トピック3、
概要
データム環境
A. Datum のオンプレミス ネットワークには、adatum.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれています。
テナントには次の表に示すユーザーが含まれます。
問題ステートメント
* 営業部門の複数のユーザーが最大5台のデバイスを所有しています。営業部門のユーザーからは、デバイス数の上限に達したため、Azure ADテナントにデバイスを追加するためにサポート部門に連絡しな

ければならないことがあるという報告があります。
* 最近のセキュリティインシデントでは、複数のユーザーが認証情報を漏洩し、サインインに疑わしいブラウザが使用され、匿名のIPアドレスからリソースにアクセスされたことが明らかになりました。
* デバイス管理者ロールを IT_Group1 に割り当てようとすると、選択リストにグループが表示されません。
* 組織内の誰でも、他のゲストや管理者以外のユーザーも含め、ゲスト ユーザーを招待できます。
* ヘルプデスクはユーザーのパスワードのリセットに時間がかかりすぎます。
* 現在、ユーザーは認証にパスワードのみを使用します。
要件
A、Datum は以下の変更を実施する予定です。
* セルフサービス パスワード リセット {SSPR} を構成します。
* すべてのユーザーに対して多要素認証 (MFA) を構成します。
* Package1 という名前のアクセス パッケージのアクセス レビューを構成します。
* 組織データへのアプリケーション アクセスには管理者の承認が必要です。
* AD DS ユーザーと groupsoflitware.com を Azure AD テナントと同期します。
* 特定の管理者ロールが割り当てられているユーザーのみがゲスト ユーザーを招待できるようにします。
* Azure AD に参加または登録できるデバイスの最大数を 10 に増やします。
技術要件
* ユーザー管理者ロールを割り当てられたユーザーは、最大 1 年間、必要に応じてロールを使用する権限をリクエストできる必要があります。
* ユーザーには MFA への登録を促すプロンプトが表示され、猶予期間中に登録をバイパスするオプションが提供される必要がある。
* SSPRを使用してパスワードをリセットするには、ユーザーは1つの認証方法を提供する必要があります。利用可能な方法には以下が含まれます。
* メールアドレス
* 電話
* セキュリティに関する質問
* Microsoft Authenticator アプリ
* adatum.com と litware.com AD DS ドメイン間に信頼関係を確立してはなりません。
* 最小権限の原則を使用する必要があります。

最新問題: **192**
App1 という名前のオンプレミス アプリがあります。
Microsoft Entra テナントがあります。
Microsoft Entra Private Access を使用して App1 を公開する予定です。
プライベート アクセス プロファイルを有効にする必要があります。
Microsoft Entra 管理センターではどのブレードを使用する必要がありますか?
A. リモートネットワーク
B. トラフィック転送
C. セキュリティプロファイル
D. コネクタ
Answer: (解答を表示する**)**
プライベートアクセストラフィック転送プロファイルを有効にする
「Global Secure Access」>「Connect」>「Traffic forwarding」の順に選択し、「Private Access profile」のチェックボックスをオンにします。

最新問題: **193**

次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

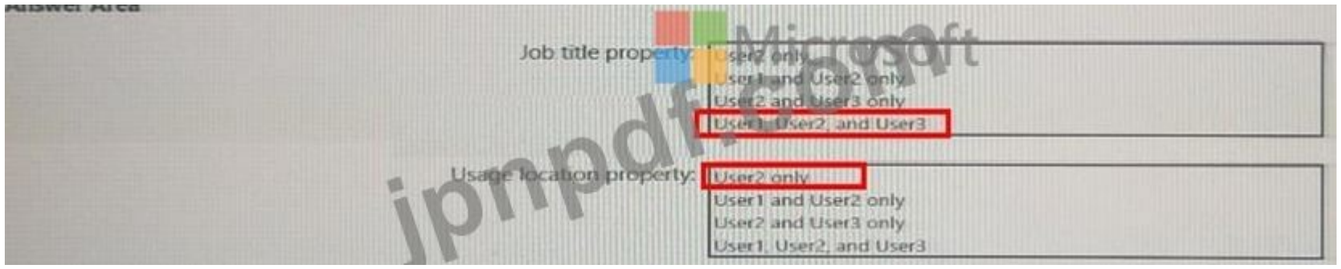
Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

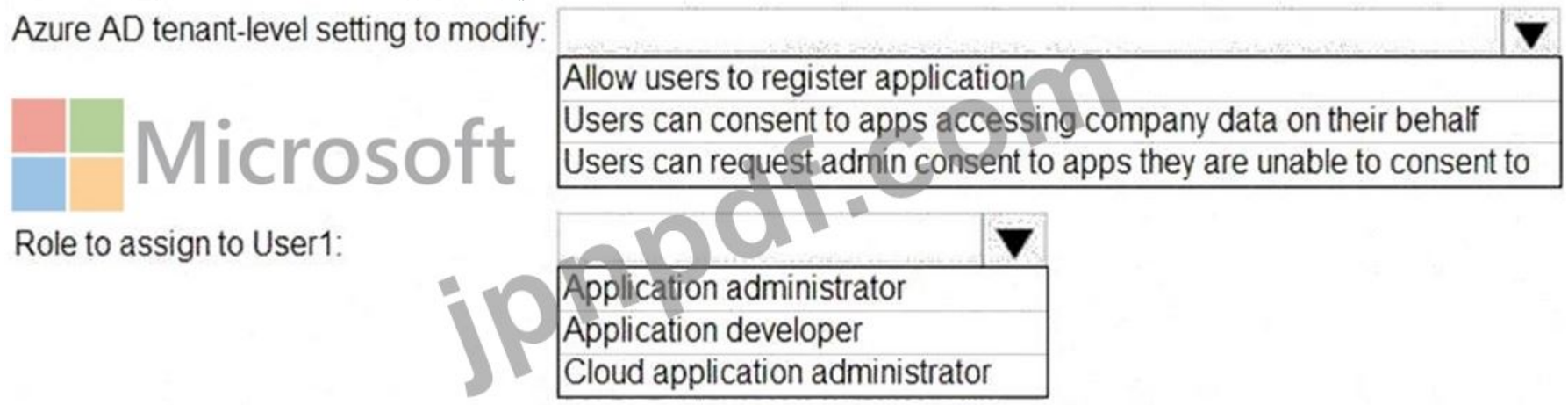


最新問題: **194**

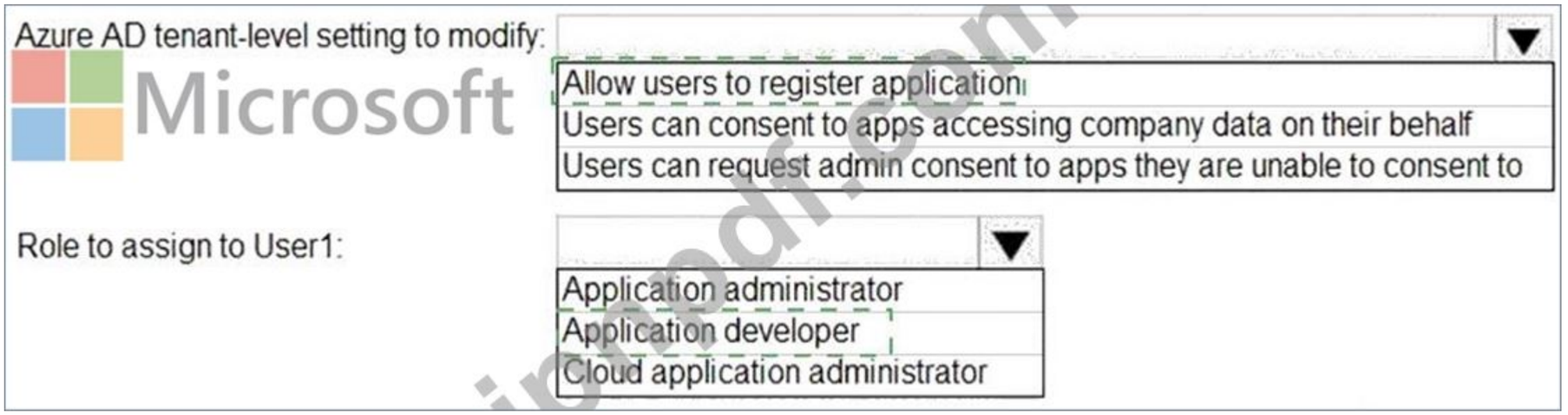
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。

どうすればいいでしょうか? 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。

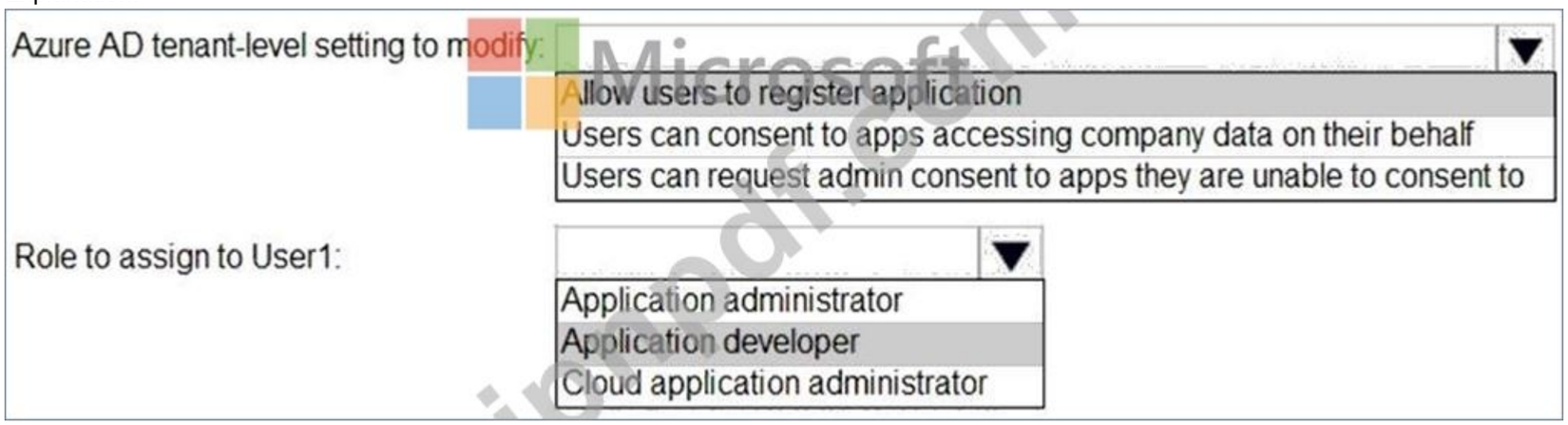
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

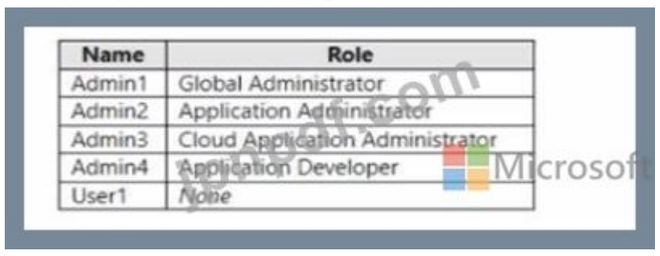


参照：

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

最新問題**: 195**

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 app1 を展開する予定です。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 Azure AD に App1 を登録できるようにする必要があります。このソリューションでは、最小権限の原則を適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し、Users1 にどのロール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:



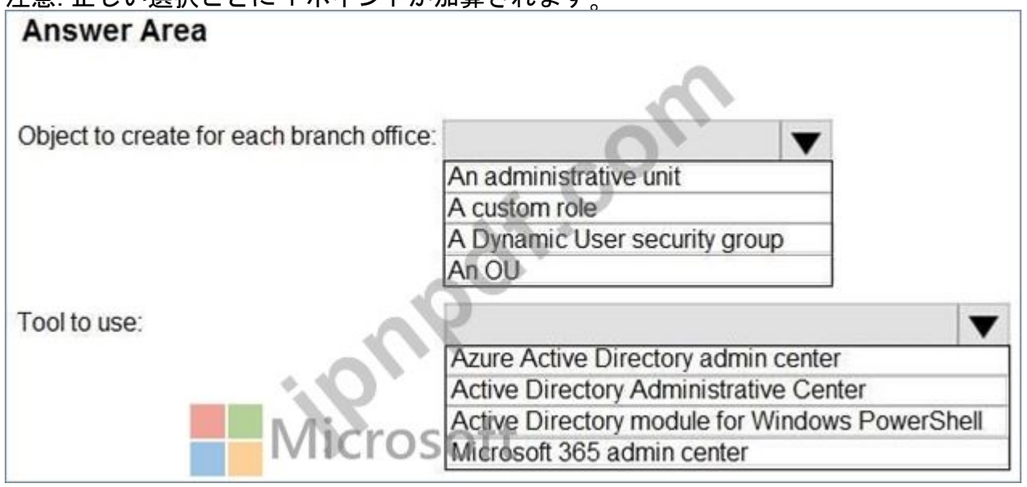
最新問題: **196**
ケーススタディ 1 - Contoso 社
概要
Contoso 社は、モントリオールに本社を置き、ロンドンとシアトルに支社を持つコンサルティング会社です。
Contoso は、Fabrikam, Inc. という会社と提携しています。Fabrikam には、fabrikam.com という Azure Active Directory (Azure AD) テナントがあります。
既存の環境。既存の環境
Contoso のオンプレミス ネットワークには、contoso.com という名前の Active Directory ドメインが含まれています。

ドメインにはContoso_Resourcesという組織単位（OU）が含まれています。Contoso_Resources OUにはすべてのユーザーとコンピューターが含まれています。
contoso.com Active Directory ドメインには、次の表に示すユーザーが含まれています。

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

既存の環境。Microsoft 365/Azure 環境
Contoso には、次の関連ライセンスを持つ contoso.com という名前の Azure AD テナントがあります。
* マイクロソフト Office 365 エンタープライズ E5
* エンタープライズモビリティ + セキュリティ
* Windows 10 エンタープライズ E3
* プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory ドメイン サービス (AD DS) の間で構成されています。Contoso_Resources OU のみが同期されます。
ヘルプデスク管理者は、通常、Microsoft 365 管理センターを使用してユーザー設定を管理します。
ユーザー管理者は現在、Microsoft 365 管理センターを使用して手動でライセンスを割り当てています。以下の例外を除き、すべてのユーザーにすべてのライセンスが割り当てられています。
* ロンドン オフィスのユーザーには、Microsoft 365 電話システムのライセンスが割り当てられていません。
* シアトル オフィスのユーザーには、Yammer Enterprise ライセンスが割り当てられていません。
contoso.com のセキュリティの既定値は無効になっています。
Contoso では、Azure AD Privileged Identity Management (PIM) を使用して管理ロールを保護します。
既存の環境。問題の説明
Contoso は次の問題を特定しています。
* 現在、すべてのヘルプデスク管理者は、Microsoft 365 テナント全体のユーザー ライセンスを管理できます。
* ユーザー管理者は、Contoso オフィスごとに異なるライセンス要件を手動で構成するのは面倒だと報告しています。
* ヘルプデスク管理者は、必要な Microsoft 365 サービスとアプリへの内部アクセスとゲスト アクセスのプロビジョニングに多くの時間を費やしています。
* 現在、ヘルプデスク管理者は、正当な理由や承認なしに、ユーザー管理者ロールを使用してタスクを実行できます。
* Azure AD でログ ノードを選択すると、Log Analytics 統合が有効になっていないことを示すエラー メッセージが表示されます。
要件。計画された変更
Contoso は次の変更を実装する予定です。
* セルフサービス パスワード リセット (SSPR) を実装します。
* Azure Monitor を使用して Azure 監査アクティビティ ログを分析します。
* テナントに追加された新しいユーザーに対するライセンスの割り当てを簡素化します。
* Fabrikam のユーザーと協力して共同マーケティング キャンペーンを実施します。
* アクティブ化するには正当性と承認が必要となるようにユーザー管理者ロールを構成します。

* App1 という名前のカスタム基幹業務 Azure Web アプリを実装します。App1 はインターネットからアクセスでき、Azure AD アカウントを使用して認証されます。
* マーケティング部門の新規ユーザーに対して、自動承認ワークフローを実装し、Microsoft SharePoint Online サイト、グループ、アプリへのアクセスを提供します。
Contoso社はAdatum Corporationという会社を買収する計画を立てています。AdatumというActive Directory組織単位 (OU)に、100人の新規ADatumユーザーが作成されます。ユーザーはロンドンとシアトルに拠点を置く予定です。
要件。技術要件
Contoso では、次の技術要件を特定しています。
* すべてのユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのみのライセンスを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。
質問
ホットスポットに関する質問
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

https://learn.microsoft.com/en-us/azure/active-directory/roles/administrative-units 管理単位は、ロールの権限を組織内の定義した任意の部分に制限します。例えば、管理単位を使用してヘルプデスク管理者のロールを地域のサポートスペシャリストに委任し、担当する地域のユーザーのみを管理できるようにすることができます。

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**37030%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 197

会社には Microsoft 365 テナントがあります。

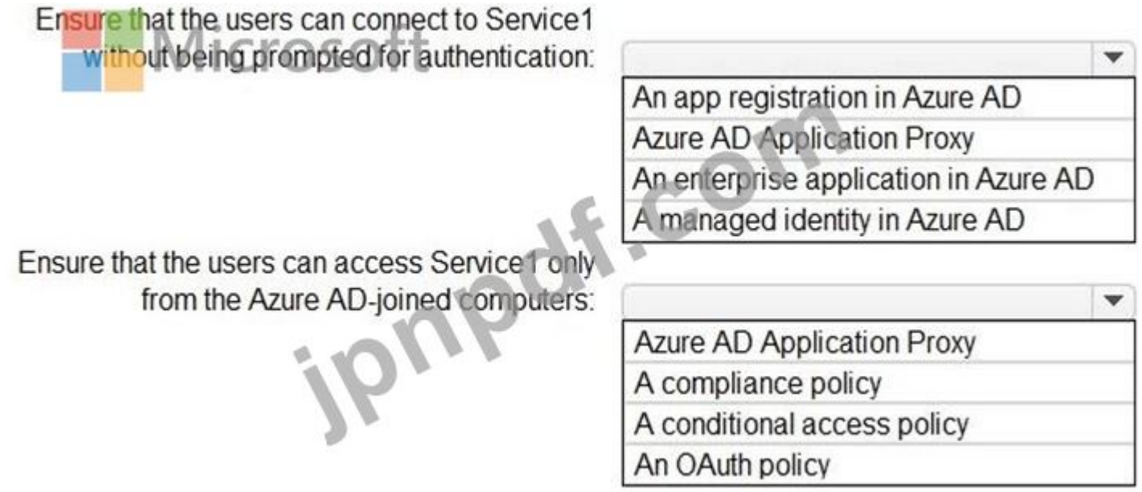
すべてのユーザーは、Windows 10 を実行し、Azure Active Directory (Azure AD) テナントに参加しているコンピューターを所有しています。

会社はService1という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Azure AD認証と承認をサポートしています。Service1はAzure ADギャラリーに公開されています。

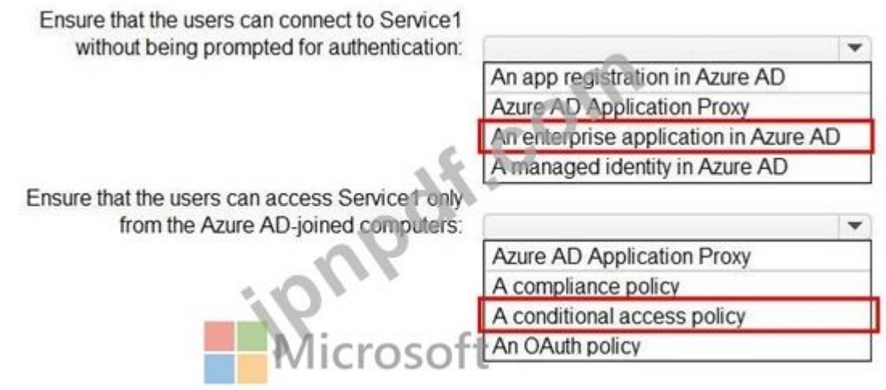
ユーザーが認証を求められることなくService1に接続できるようにするソリューションを推奨する必要があります。このソリューションでは、Azure ADに参加しているコンピューターからのみユーザーがService1にアクセスできるようにする必要があります。また、管理作業を最小限に抑える必要があります。

各要件に対して何を推奨しますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



参照：
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**: 198**
contoso.onmicrosoft.com というドメイン名を使用する新しい Microsoft 365 テナントがあります。
ドメイン レジストラに contoso.com という名前を登録します。
新しい Microsoft 365 ユーザーの既定のドメイン名として contoso.com を使用する必要があります。
どの 4 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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:

Answer Area

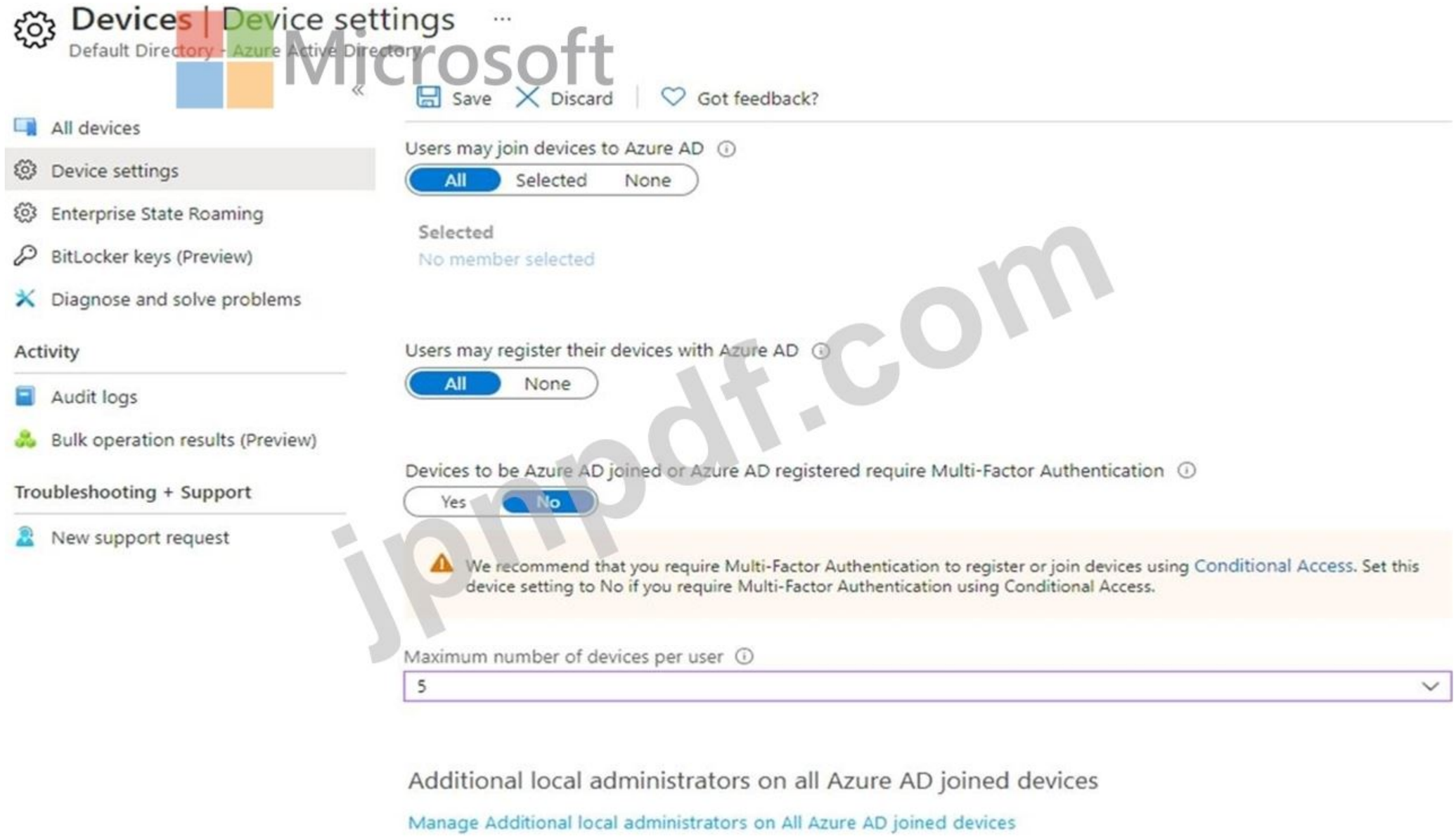
- Register a custom domain name of contoso.com.
- Create a new TXT record in DNS.
- Verify domain name.
- Set the domain to primary.

1 - contoso.com のカスタム ドメイン名を登録します。
2 - DNS に新しい TXT レコードを作成します。
3 - ドメイン名を確認します。
4 - ドメインをプライマリに設定します。
参照：
https://practical365.com/office-365 でカスタムドメインを構成する/

最新問題**: 199**
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。このテナントには、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**

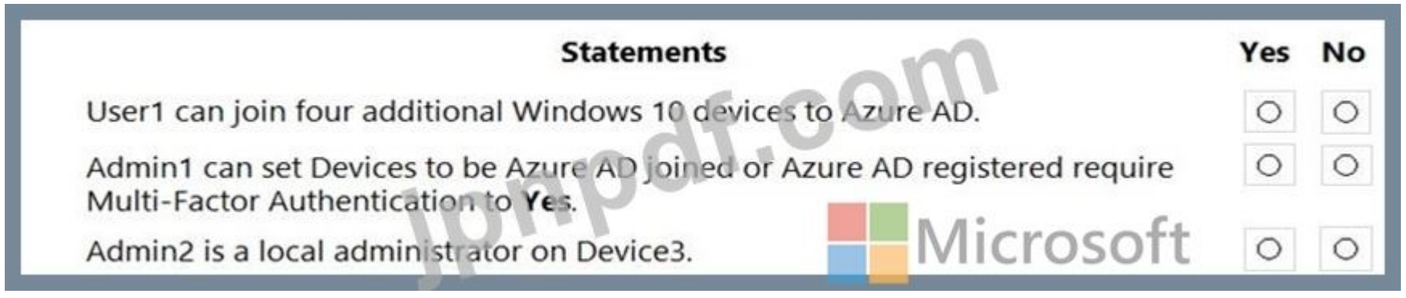
次の図に示すデバイス設定があります。



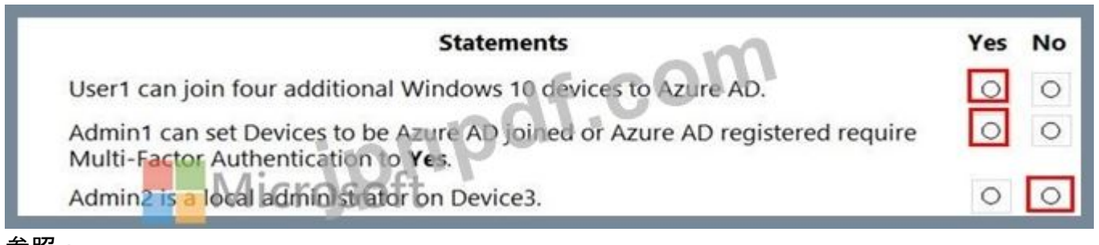
User1 には次の表に示すデバイスがあります。

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 ポイントが加算されます。



Answer:



参照：

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

最新問題**: 200**

貴社では現在、業務手順の見直しと効率化の方法を模索しています。懸念事項の一つは、ヘルプデスク管理者がユーザーの問題対応に費やす時間です。ヘルプデスク管理者への問い合わせやチケット発行を削減するために導入できるサービスは何でしょうか？

A. アクティブディレクトリ接続

B. セルフサービスパスワードリセット

C. 多要素認証

D. アプリケーションプロキシ

Answer: B (メーッセージを残す**)**

最新問題**: 201**

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 app1 を展開する予定です。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。

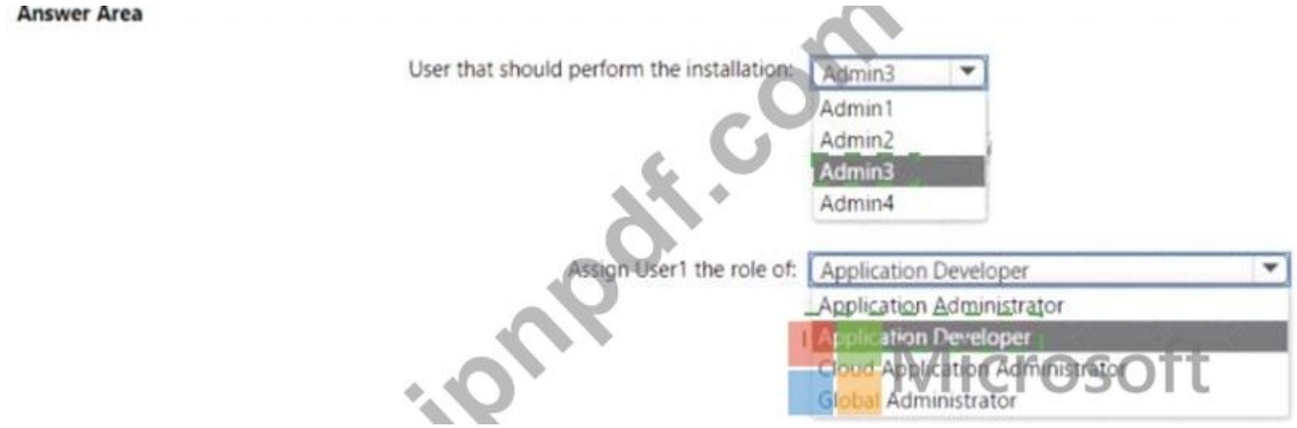
アプリケーションプロキシコネクタのインストールを委任し、User1 が Azure AD に App1 を登録できるようにする必要があります。このソリューションでは、最小権限の原則を適用する必要があります。

どのユーザーがインストールを実行し、Users1 にどのロール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: 202

次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

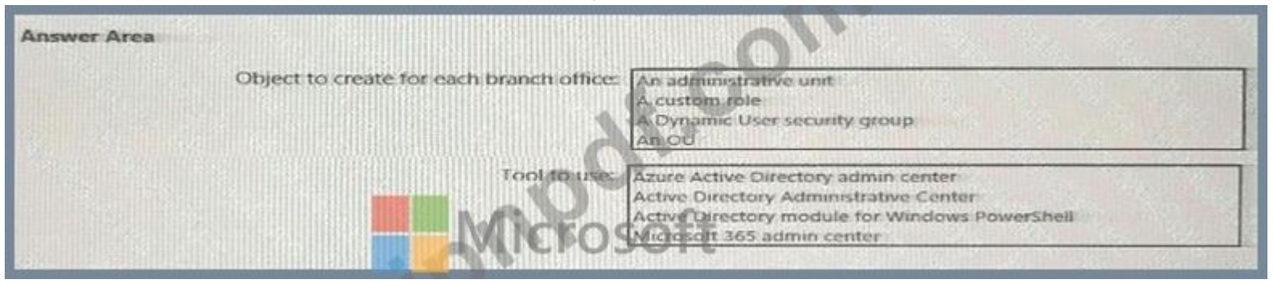


最新問題: **203**

ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。

最初に何を作成し、どのツールを使用すればよいですか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

Object to create for each branch office:

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

Tool to use:

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

最新問題**: 204**

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
User1	Group1
User2	Group2
User3	Group3

テナントには次の表に示す認証方法があります。

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

アプリに表示される番号と携帯電話に表示される番号を照合してクラウド アプリにサインインするユーザーは誰でしょうか?

A. ユーザー2とユーザー3のみ

B. ユーザー1とユーザー2のみ

C. ユーザー2のみ

D. ユーザー3のみ

E. ユーザー1のみ

Answer: E (メーッセージを残す**)**

最新問題**: 205**

次の図に示すように、ユーザー管理者ロールの Azure AD Privileged Identity Management (PIM) ロール設定を含む Azure Active Directory (Azure AD) テナントがあります。

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

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

Assignment

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

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

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

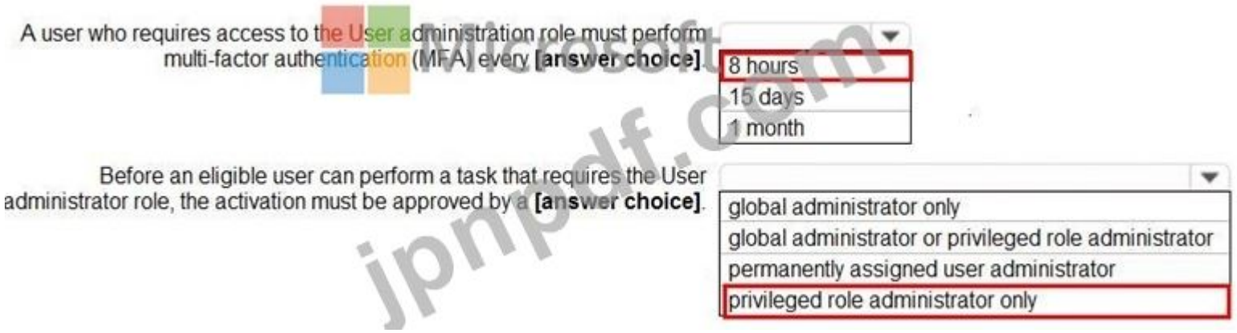
- 8 hours
- 15 days
- 1 month

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

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

Answer:

jpnpdf.com



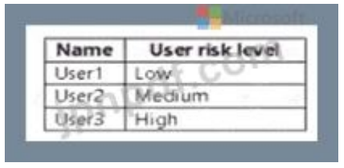
参照：

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**: 206**

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

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 ポイントが加算されます。

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.	○	○

Microsoft
jpnpdf.com

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.	○	○

Microsoft
jpnpdf.com

Explanation:

ユーザー1は多要素認証（MFA）を使用してサインインできます: いいえ

ユーザー2は多要素認証（MFA）を使用してサインインできます: いいえ

ユーザー3は匿名IPアドレスからサインインできる: いいえ

このシナリオは、Azure AD Identity Protection とその 2 つのコア条件付きアクセス メカニズムに基づいています。

* ユーザー リスク ポリシー - ユーザーの ID が侵害される可能性を評価します。
* サインイン リスク ポリシー - サインイン試行が正当なユーザーによって実行されない可能性を評価します。

提供された表に基づいて、段階的に分析してみましょう。

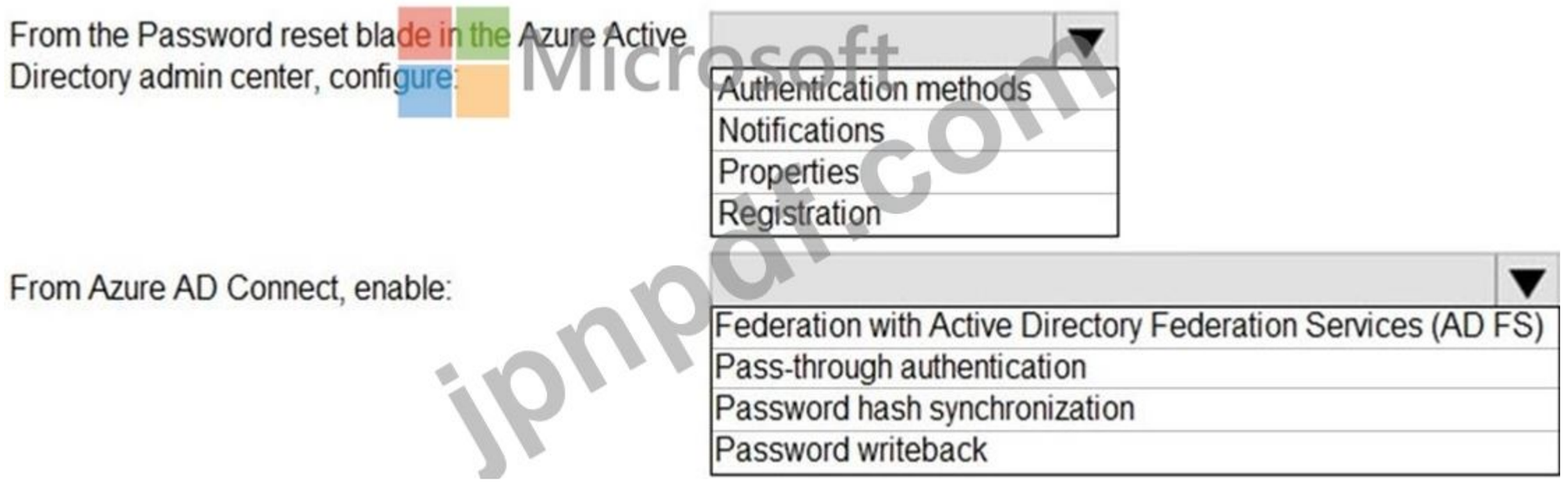
* リスクレベル: 低
* ユーザー リスク ポリシー: 低レベル以上 (つまり、低、中、高レベルのユーザー) に適用されます。
* 制御: アクセスをブロックします。
* 実行されたアクション: ユーザーのセキュリティが侵害されたことを確認します。ユーザーがセキュリティが侵害されたことを確認すると、ユーザーが修復されるまで (つまり、パスワードのリセット)、そのユーザーのリスク レベルが維持または増加します。ポリシーによって、ユーザー リスクが「低以上」の場合にアクセスがブロックされるため、User1 のサインインはブロックされ、MFA は要求されず、アクセスは拒否されます。

ユーザー1 MFAサインイン: いいえ

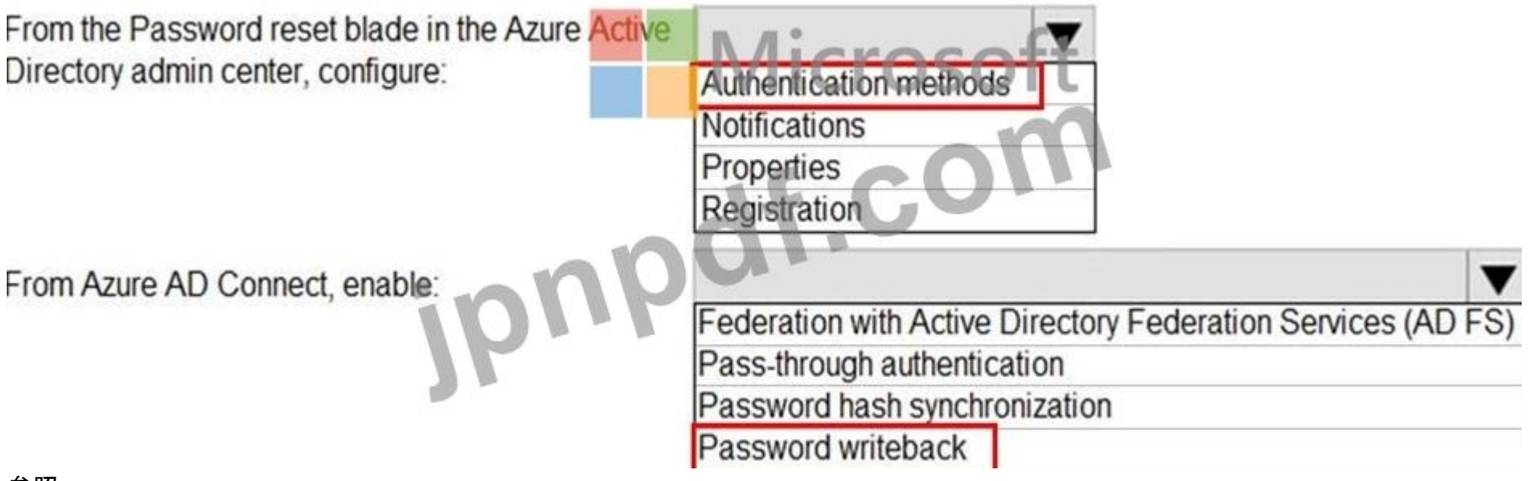
* 初期リスクレベル: 中
* 実行されたアクション:
* サインインの安全を確認 # サインインのリスクをクリアします。
* ユーザーのセキュリティが侵害されたことを確認すると、ユーザー リスクが再び「高」に引き上げられます。
* 適用されるポリシー:

* ユーザー リスク ポリシー (低以上): アクセスをブロックします。
* サインイン リスク ポリシー: 高レベルのサインインにのみ適用されます (ここでは関係ありません)。
ユーザー2のユーザーリスクは、侵害が確認された後に 高」に設定されているため、ユーザーリスクポリシーは、
低くて上。」
したがって、MFA は許可されません (セッションは完全に拒否されます)。
ユーザー2 MFAサインイン: いいえ
* ユーザーリスク: 高
* 実行されたアクション: ユーザー リスクを無視 # は、ユーザー リスクを 『リスクなし」にリセットします。
* サインイン ポリシー: 高いサインイン リスク # アクセスをブロックします。User3 が匿名 IP からサインインすると、Azure AD Identity Protection はこれを高いサインイン リスクとして検出します (Microsoft ドキュメントによる)。サインイン リスク ポリシーによってすべての高いサインインがブロックされるため、アクセスがブロックされます。
ユーザー3 匿名 IP サインイン: いいえ

最新問題**: 207**
Microsoft 365 テナントと、adatum.com という名前の Active Directory ドメインがあります。
簡単設定を使用して Azure AD Connect をデプロイします。
次の要件を満たすようにセルフサービス パスワード リセット (SSPR) を構成する必要があります。
ユーザーがパスワードをリセットする場合、モバイル アプリの通知に応答するか、事前定義された 3 つのセキュリティの質問に答えるように要求される必要があります。
パスワードがリセットされた場所に関係なく、テナントとドメイン間でパスワードを同期する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題**: 208**
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、Azure AD へのセルフサービス サインアップに contoso.com のメール アドレスを使用しています。
自己署名ユーザーを含む Azure AD 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 Azure AD 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-MgOrganization
B. Update-MgPolicyPermissionGrantPolicyExclude
C. 更新-MgDomain
D. Update-MgDomainFederationConfiguration
Answer: (解答を表示する**)**
Update-MgPolicyPermissionGrantPolicyExclude コマンドレットは、特定のユーザーグループへのポリシーの適用を除外するために使用されます。この場合、このコマンドレットを使用して、contoso.com SMTP アドレス空間を持つユーザーへのセルフサービスサインアップポリシーの適用を除外できます。

最新問題**: 209**
次のグループを含む Azure Active Directory (Azure AD) テナントがあります。
名前: グループ1
メンバー: ユーザー1、ユーザー2
所有者: ユーザー3
2021 年 1 月 15 日に、図に示すようにアクセス レビューを作成します。([図] タブをクリックします。)



Description ⓘ

Start date * 01/15/2021

Frequency Monthly

Duration (in days) ⓘ 14

End ⓘ Never | End by | Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope
- Guest users only
- Everyone

Group *
Group1

Reviewers

Reviewers Members (self)

Programs

jpnpdf.com

Microsoft



ユーザーは、次の表に示すように Review1 の質問に回答します。

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 ポイントが加算されます。

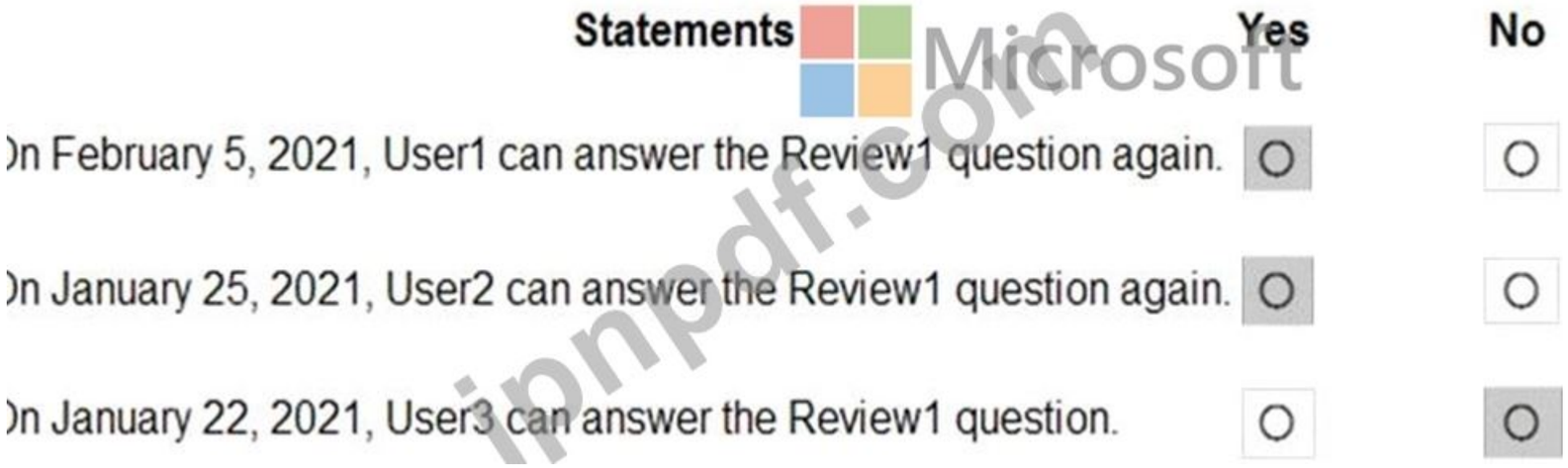
Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Answer:

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

jpnpdf.com
Microsoft

説明
コンピュータのスクリーンショット 低い信頼度で自動生成された説明



参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/review-your-access

最新問題: 210
次の表に示すグループを含む Azure Active 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
Group5	Microsoft 365	Dynamic User

どのグループに対してアクセス レビューを作成できますか?
A. グループ1のみ
B. グループ1とグループ4のみ
C. グループ1とグループ2のみ
D. グループ1、グループ2、グループ4、グループ5のみ
E. グループ1、グループ2、グループ3、グループ4、グループ5
Answer: D (メーッセージを残す)
SC-300公式学習ガイドとMicrosoft Learn: アクセスレビューの管理では、Azure ADのアクセスレビューはユーザーベースのグループ、Azure ADロール、エンタープライズアプリケーションを対象とできることが確認されています。ただし、動的デバイスグループはアクセスレビューではサポートされていません。

最新問題: 211
Admin1 という名前のユーザーを含む Azure AD テナントがあります。
Admin1 は、高リスク ユーザーのパスワード変更を要求するポリシー テンプレートを使用して、新しい条件付きアクセス ポリシーを作成します。
ポリシー割り当てにおいて、デフォルトで誰に含まれ、誰に除外されますか？ 適切なオプションを正しい対象にドラッグしてください。各オプションは、1回、複数回、または全く使用されない場合があります。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **212**

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

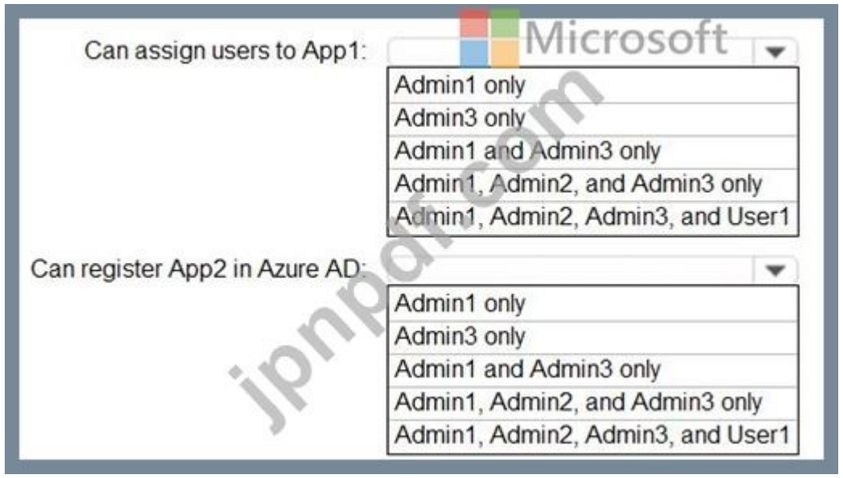
Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

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Azure ADに登録します。

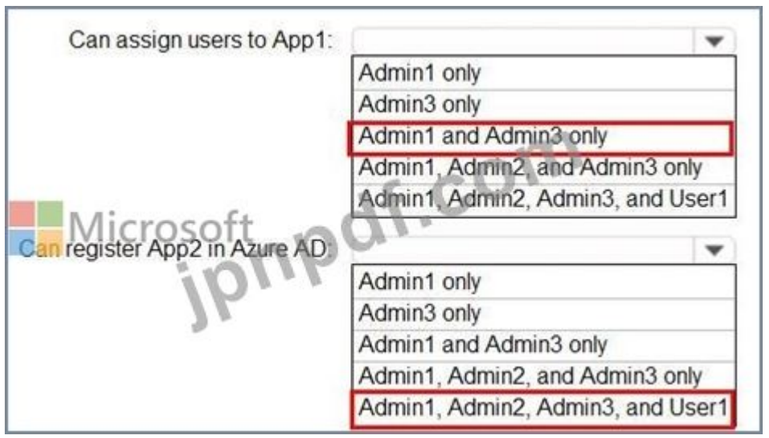
App1 にユーザーを割り当てることができるユーザーと、Azure AD に App2 を登録できるユーザーを特定する必要があります。

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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



参照：

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: **213**

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 ポイントが加算されます。



Answer:



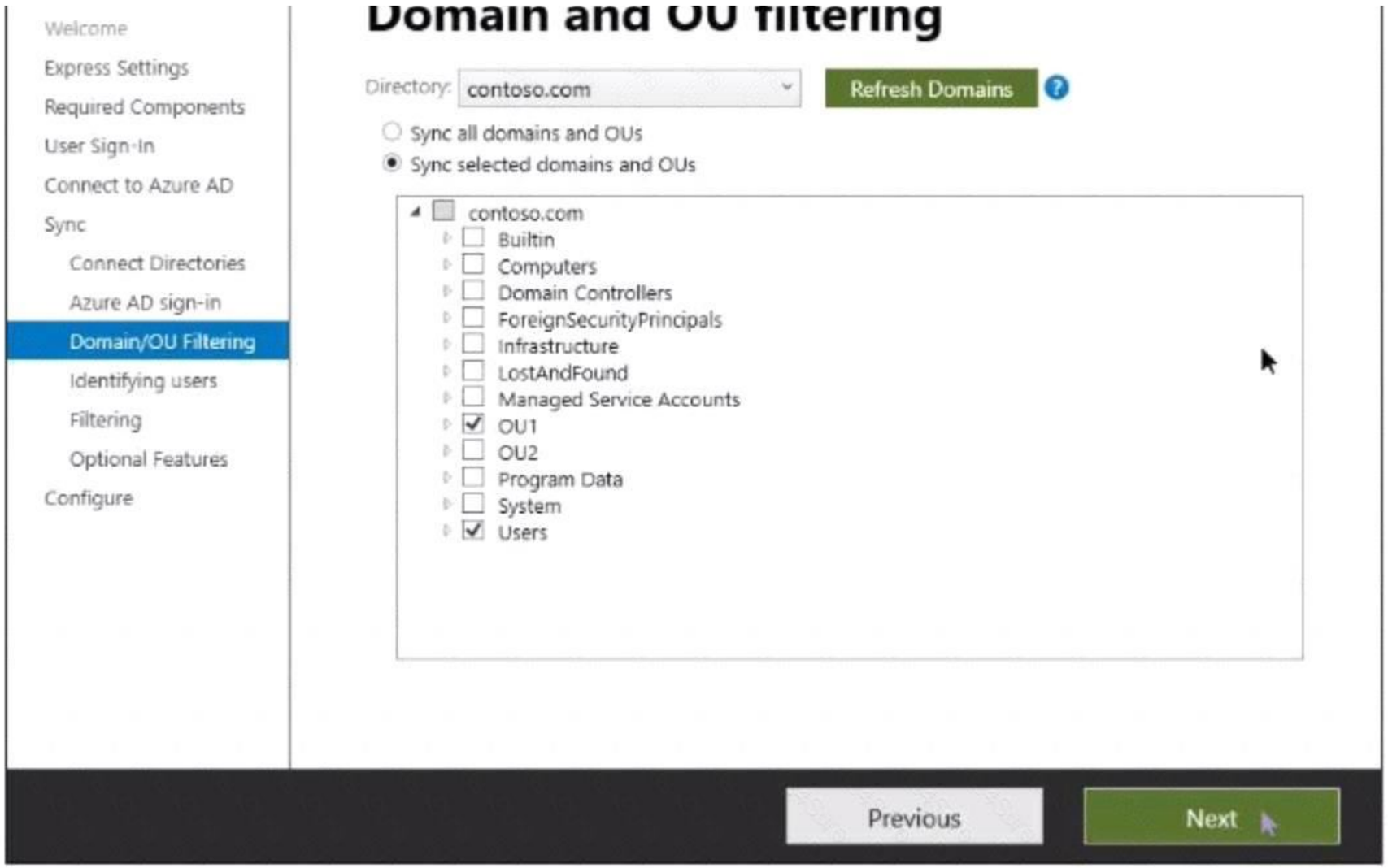
Explanation:
はい、いいえ、はい

最新問題**: 214**
ネットワークには、Azure AD と同期し、次の表に示すユーザーを含むオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。

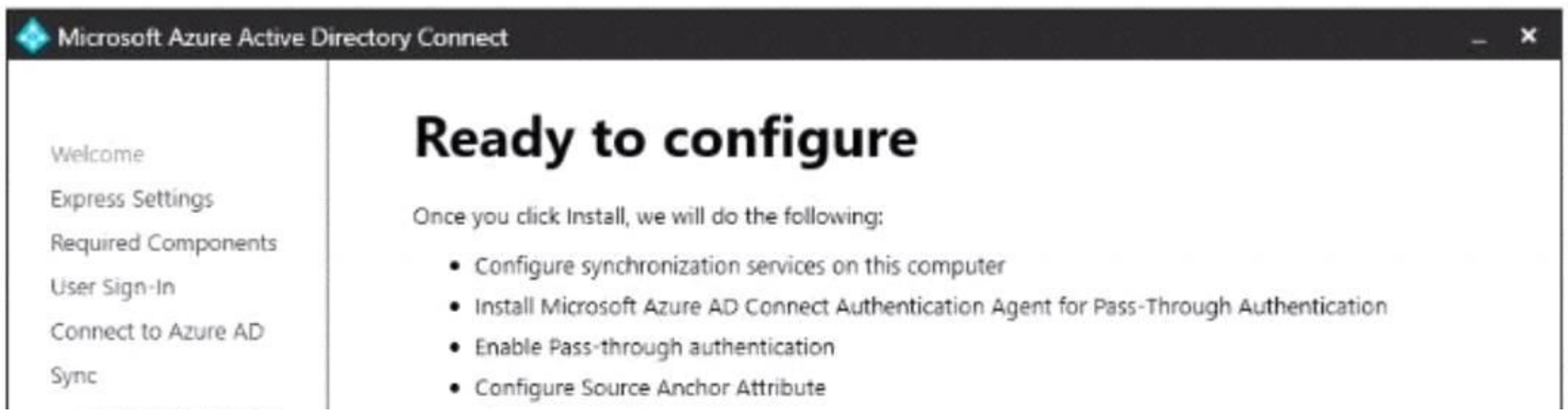
Name	Organizational unit (OU)
User1	OU1
User2	OU2

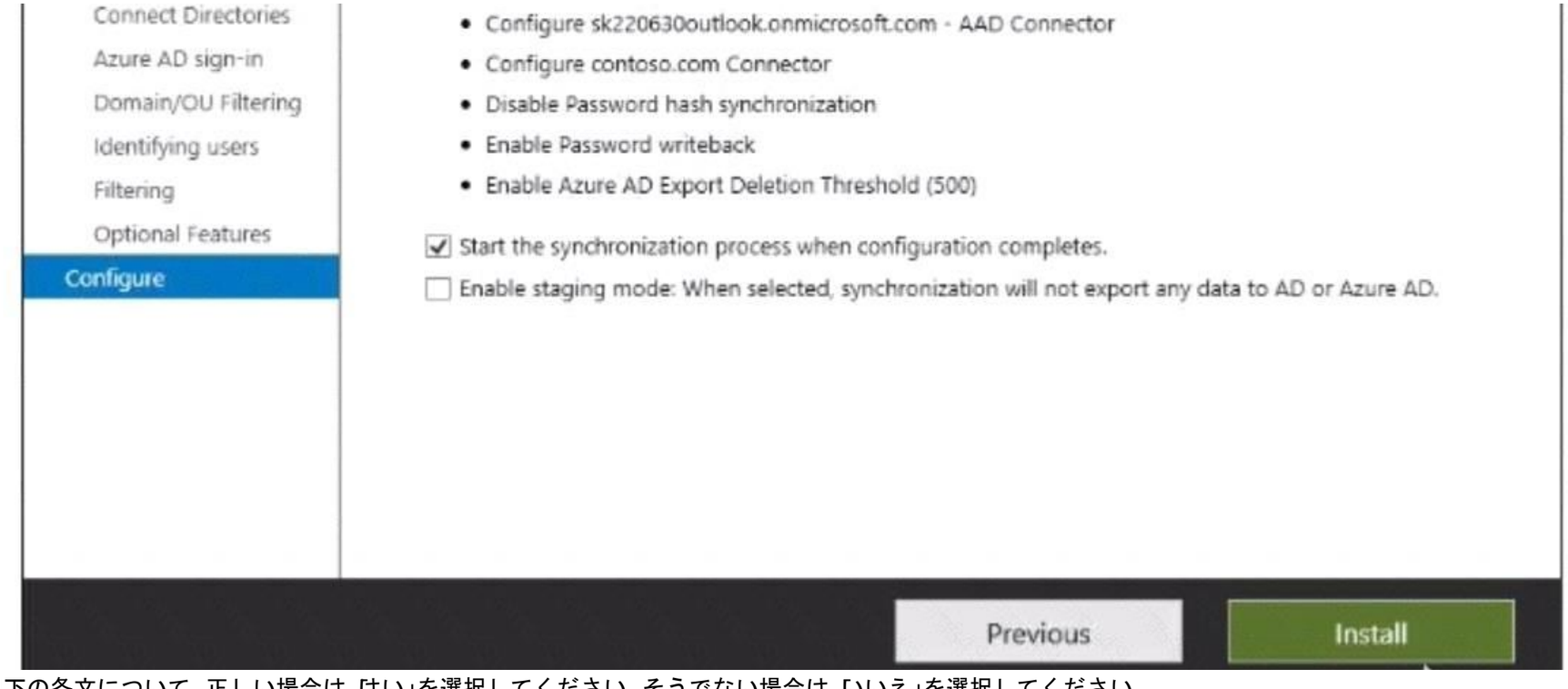
Azure AD Connect では、ドメイン/OU フィルタリングは次の図に示すように構成されます。





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





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 ポイントが加算されます。

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:



説明



jpnpdf.com
Microsoft

最新問題: **215**

ドラッグアンドドロップの質問

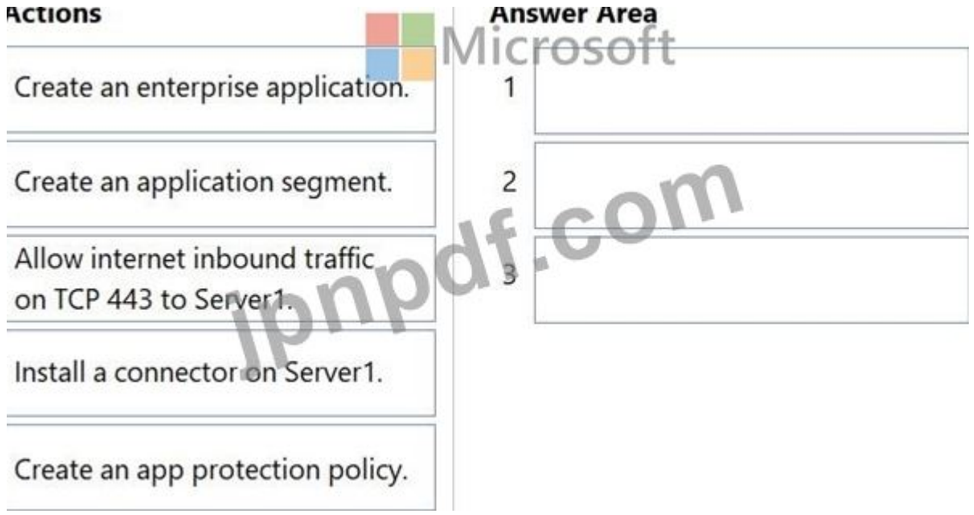
オンプレミスネットワークには、Active Directory ドメインサービス (AD DS) ドメインが含まれています。このドメインには、Windows Server を実行する Server1 というサーバーがあり、Share1 という共有フォルダをホストしています。このドメインには、Windows 11 を実行するデバイスが 500 台含まれています。

ドメインと同期する Microsoft 365 E5 サブスクリプションがあります。

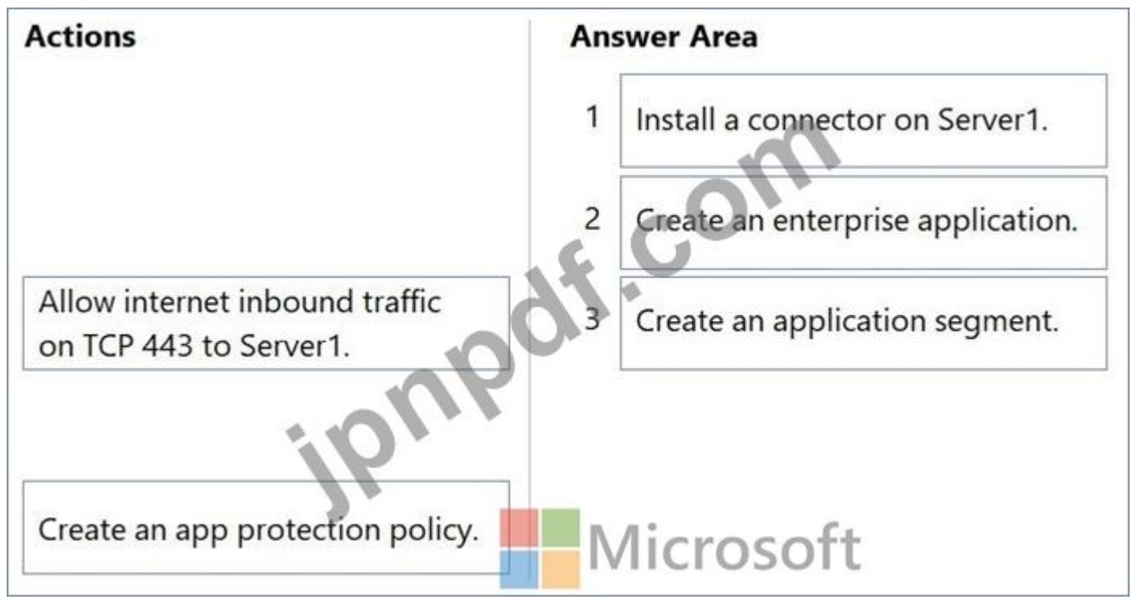
Global Secure Access から、プライベート アクセス プロファイルを有効にし、Global Secure Access クライアントをすべてのデバイスに展開します。

Global Secure Access を使用して、デバイスがリモートで Share1 に接続できることを確認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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。

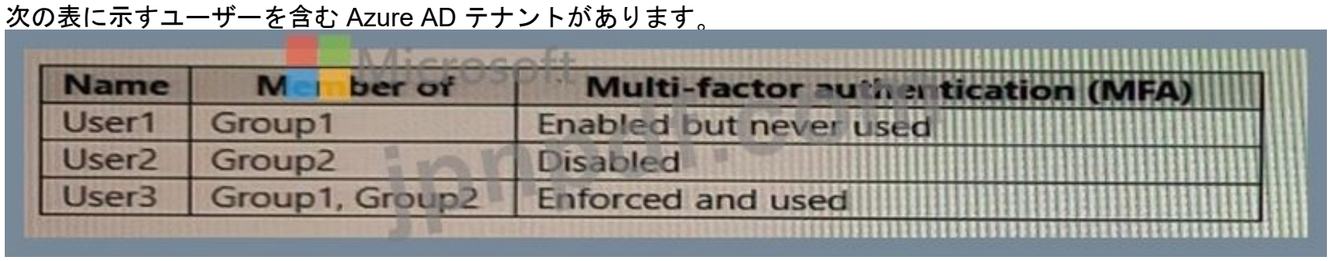


Answer:



最新問題: 216

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。

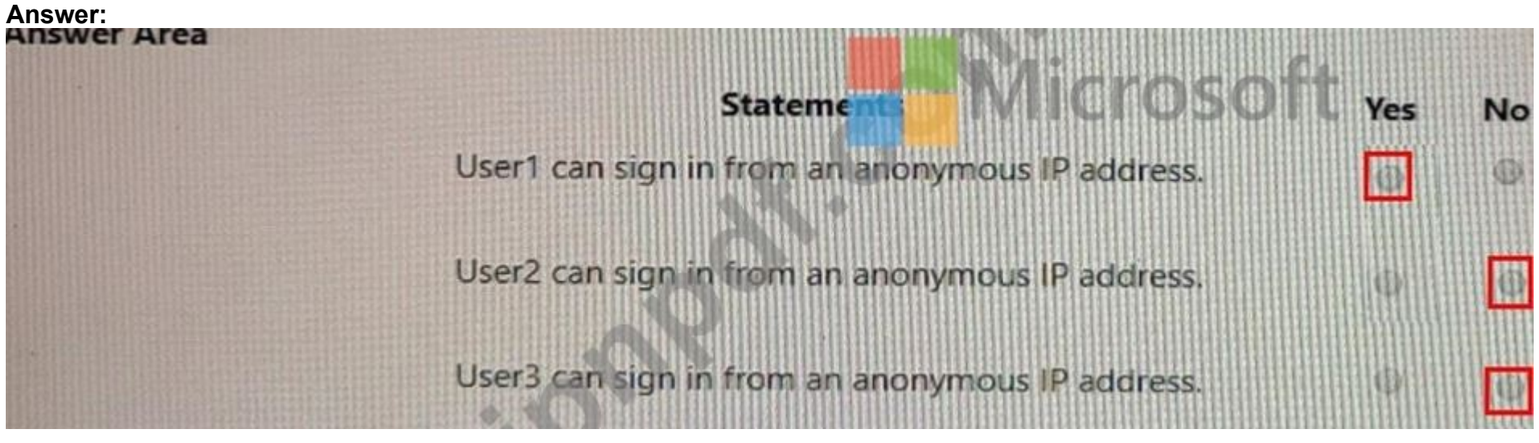
* 課題:

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する
* 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。
* 課題:
o ユーザー: グループ2
o サインインリスク: 低以上
* コントロール:
o アクセス: 多要素認証を要求する
* ポリシーを強制する。オン
次の設定:
設定:
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 ポイントが加算されます。



Answer:



最新問題: 217
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在す

る場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Active Directory フォレストと同期する Azure Active 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 Azure AD 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 Azure AD に対して認証されないようにする必要があります。
解決策: パスワード ライトバックを構成します。
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**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

最新問題**: 218**
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がない遠隔地から作業することがよくあります。
ユーザーは、遠隔地から作業する際、インターネットにアクセスできる有線ネットワークにラップトップを接続します。
多要素認証 (MFA) を実装する予定です。
ユーザーはリモート ロケーションからどの MFA 認証方法を使用できますか?
A. Microsoft Authenticator アプリからの確認コード
B. セキュリティに関する質問
C. 音声
D. SMS
Answer: A (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-authenticator-app#mobile-app からの検証コード

最新問題**: 219**
Microsoft 365 E5 サブスクリプションと Azure サブスクリプションをお持ちの場合、以下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権限を委任します。
各要件にはどのような機能を利用すべきでしょうか？ 適切な機能を正しい要件にドラッグして答えてください。各機能は1回、複数回、または全く使用されない場合があります。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。



Answer:



最新問題**: 220**

Active Directory ドメインと同期する Azure Active Directory (Azure AD) テナントがあります。

オンプレミスネットワークには、オンプレミスの Active Directory ドメインへの認証を行う VPN サーバーが含まれています。この VPN サーバーは Azure Multi-Factor Authentication (MFA) をサポートしていません。

VPN 接続に Azure MFA を提供するソリューションを推奨する必要があります。

推薦書には何を含めるべきでしょうか?

A. Azure AD アプリケーション プロキシ

B. Azure AD パスワード保護プロキシ

C. ネットワーク ポリシー サーバー (NPS)

D. パススルー認証プロキシ

Answer: C (メーッセージを残す**)**

NPS (ネットワーク ポリシーとアクセス サービス) は、VPN クライアントと Azure MFA の間の仲介役のようなものです。NPS ロールは、ドメインに参加しているサーバーまたはドメイン コントローラーにインストールされ、VPN クライアントからの RADIUS 要求を認証および承認するように構成されます。

VPN は、RADIUS 認証を使用し、NPS サーバーをポイントするように構成する必要があります。

MFA NPS拡張機能は、VPNサーバー以外の任意の場所にインストールされます。ユーザー/VPNクライアントが認証を試みると、VPN経由でNPSサーバーにRADIUS要求が送信され、NPSサーバーでプライマリ認証が実行され、その後、NPS拡張機能によるセカンダリ認証が実行されます。

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

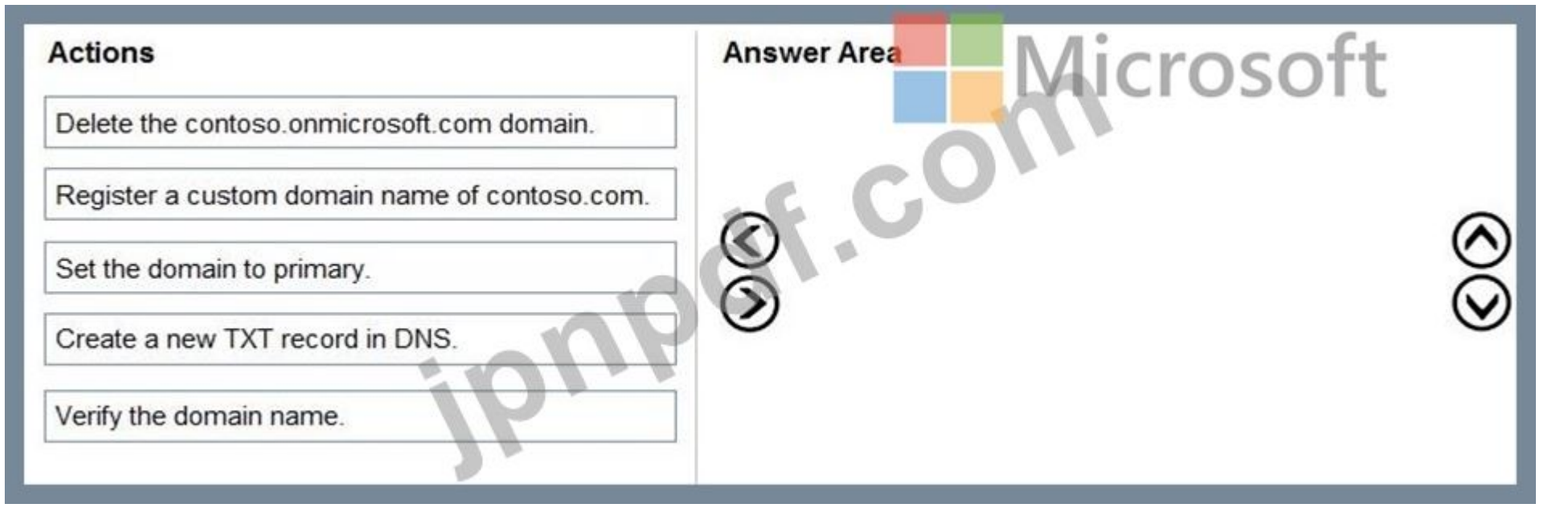
最新問題**: 221**

contoso.onmicrosoft.com というドメイン名を使用する新しい Microsoft 365 テナントがあります。

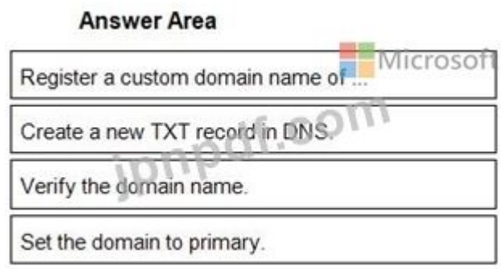
ドメイン レジストラに contoso.com という名前を登録します。

新しい Microsoft 365 ユーザーの既定のドメイン名として contoso.com を使用する必要があります。

どの 4 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、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:

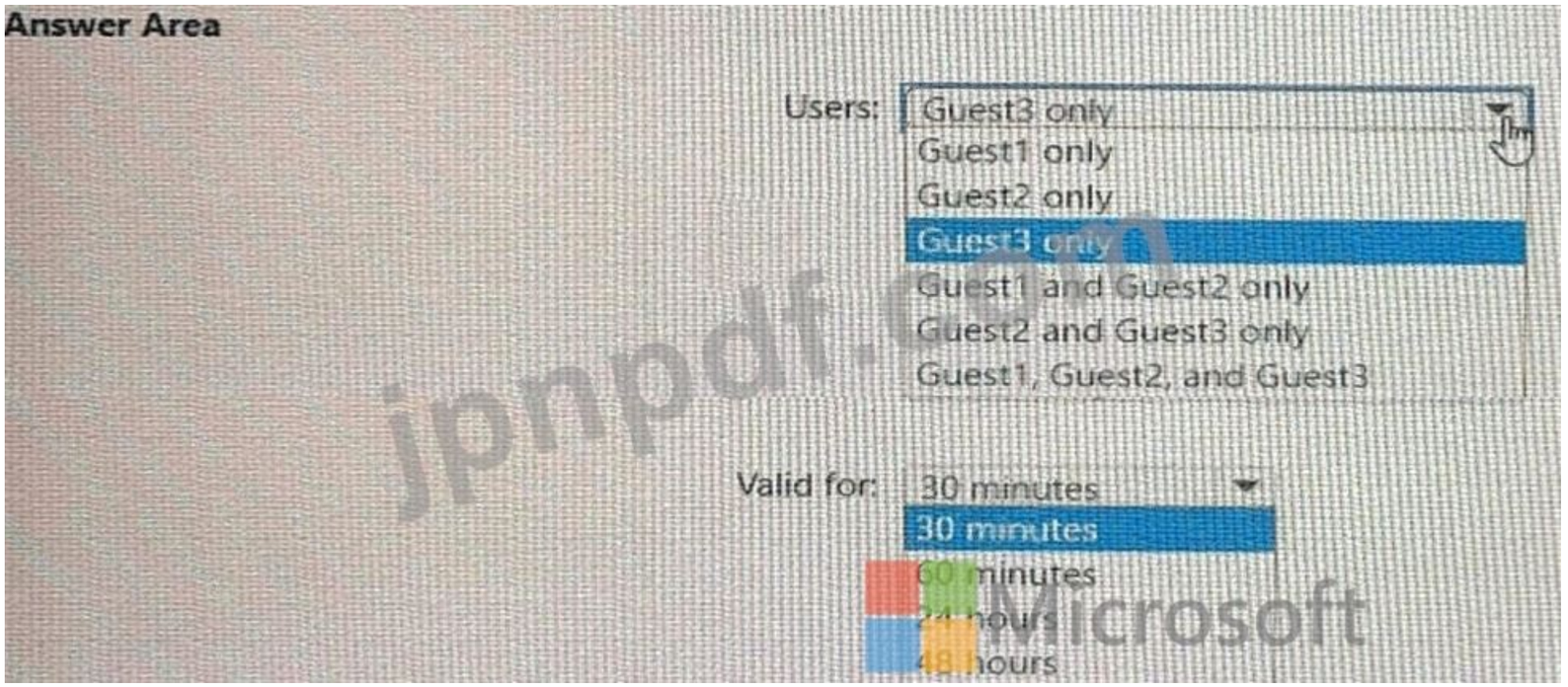


1 - ...のカスタムドメイン名を登録します。
2 - DNS に新しい TXT レコードを作成します。
3 - ドメイン名を確認します。
4 - ドメインをプライマリに設定します。
参照：
https://practical365.com/office-365 でカスタムドメインを構成する/

最新問題: 222
contoso.com という名前の Azure AD テナントがあり、ゲスト用のワンタイム パスコードを電子メールで送信することが [はい] に設定されています。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

ワンタイム パスコードを受け取るユーザーは誰ですか? また、パスコードの有効期間はどのくらいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



Microsoft SC-300 学習ガイド、試験参照 SC-300、および Microsoft Entra (Azure AD B2B コラボレーション) のドキュメントによると、ゲストが Azure AD テナントに招待され、「ゲストにワンタイム パスコードを電子メールで送信」設定が有効になっている場合、Azure AD はゲストのアカウントの種類に基づいて認証方法を決定します。
ロジックの適用方法は次のとおりです。
* Guest1 (adatum.com - Azure AD アカウント)
* adatum.com は Azure AD 管理ドメインであるため、Guest1 は自分の組織の Azure AD 資格情報を使用して認証します。
* ゲストのサインインはホームテナントにフェデレーションされるため、ワンタイムパスコード (OTP) は送信されません。
* ゲスト2 (outlook.com - Microsoft アカウント)
* @outlook.com のメール アドレスを持つユーザーには、Microsoft アカウント (MSA) があります。
* Microsoft アカウントは、Microsoft の ID システムを介して直接認証できます。
* したがって、ワンタイム パスコードは送信されず、ユーザーは Microsoft アカウントの資格情報を使用してサインインします。
* ゲスト3 (gmail.com - 個人のGoogleアカウント)
* @gmail.com アドレスは Microsoft アカウントではなく、既定ではどの Azure AD テナントにもリンクされていません。
* この場合、テナントの設定 「ゲスト用のワンタイム パスコードをメールで送信」が有効になっているため、Azure AD は認証のためにゲストのメール アドレスにワンタイム パスコード (OTP) を自動的に送信します。
* Microsoft のドキュメントでは、OTP は 30 分間有効で、1 回限りの使用であると規定されています。
有効期限が切れると、次回の認証試行時に新しいコードが発行されます。
これは、Microsoft の公式 Entra ID ドキュメントでも確認されています。
「ゲスト用のワンタイム パスコードをメールで送信する」設定を有効にすると、Azure AD または Microsoft アカウントを持たないゲストは、30 分間有効なワンタイム パスコードを使用して認証します。

最新問題**: 223**
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
ユーザー1がグループのアクセスレビューを作成でき、ユーザー2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、最小権限の原則を適用する必要があります。
各ユーザーにどのロールを割り当てるべきですか？ 回答するには、適切なロールを正しいユーザーにドラッグしてください。各ロールは1回、複数回、または全く使用されない場合があります。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：正しい選択ごとに1ポイント獲得できます。



Answer:



Explanation:



最新問題**: 224**

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 Area



Answer:



Explanation:



最新問題: **225**
あなたはPass4test Inc.のクラウド管理者であり、全ユーザーに多要素認証を実装する任務を負っています。この準備として、全ユーザーが多要素認証に適切に登録されていることを確認する必要があります。以下の選択肢のうち、認証方法として使用できないものはどれですか？
A. SMS
B. 音声通話
C. Microsoft Authenticator アプリ
D. セキュリティの質問

E. FIDO2 セキュリティキー
Answer: D (メーッセージを残す)

最新問題**: 226**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 227**
次の表に示すユーザーを含む Microsoft Entra テナントがあります。

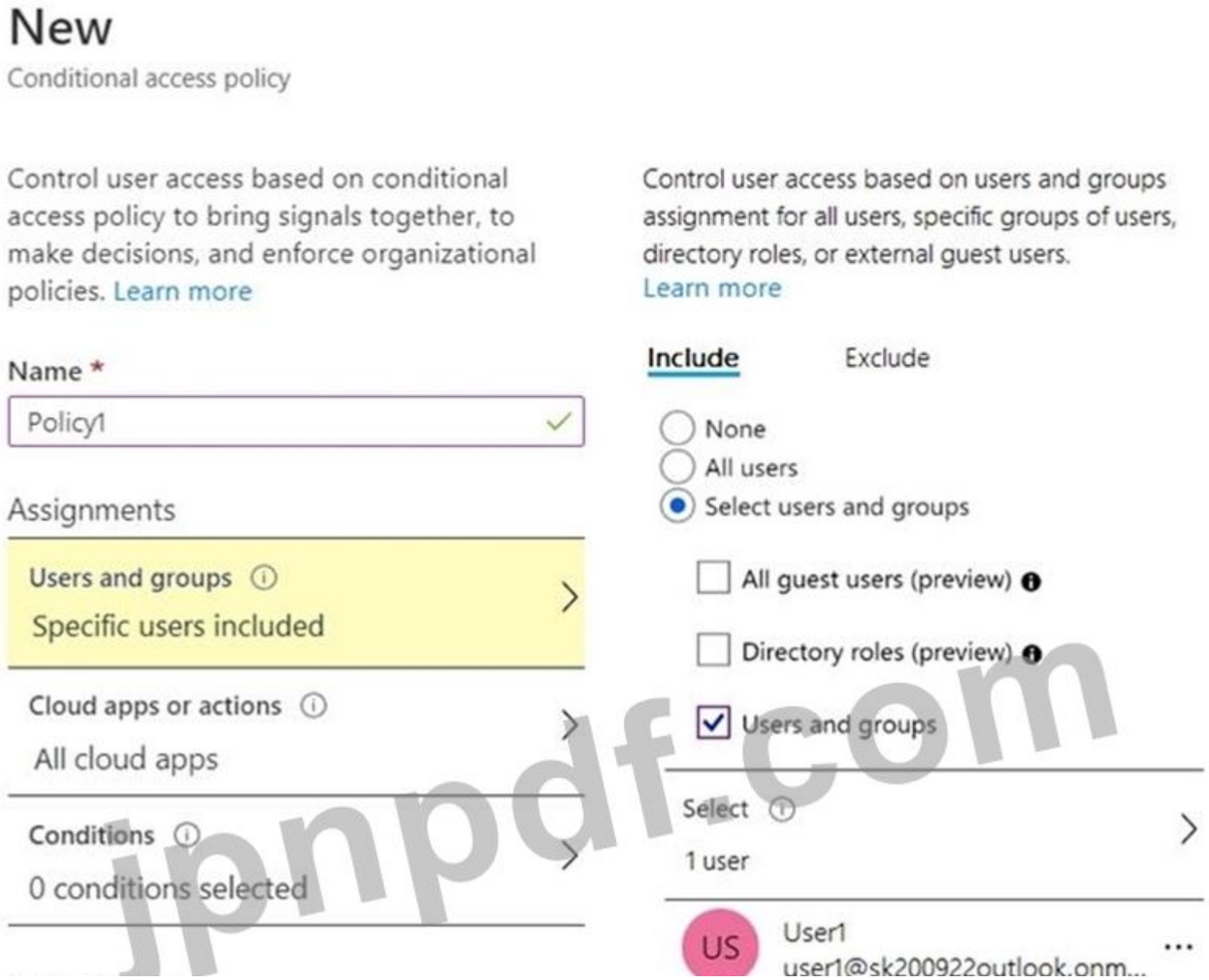
Name	User type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

User1 は Group1 の所有者です。

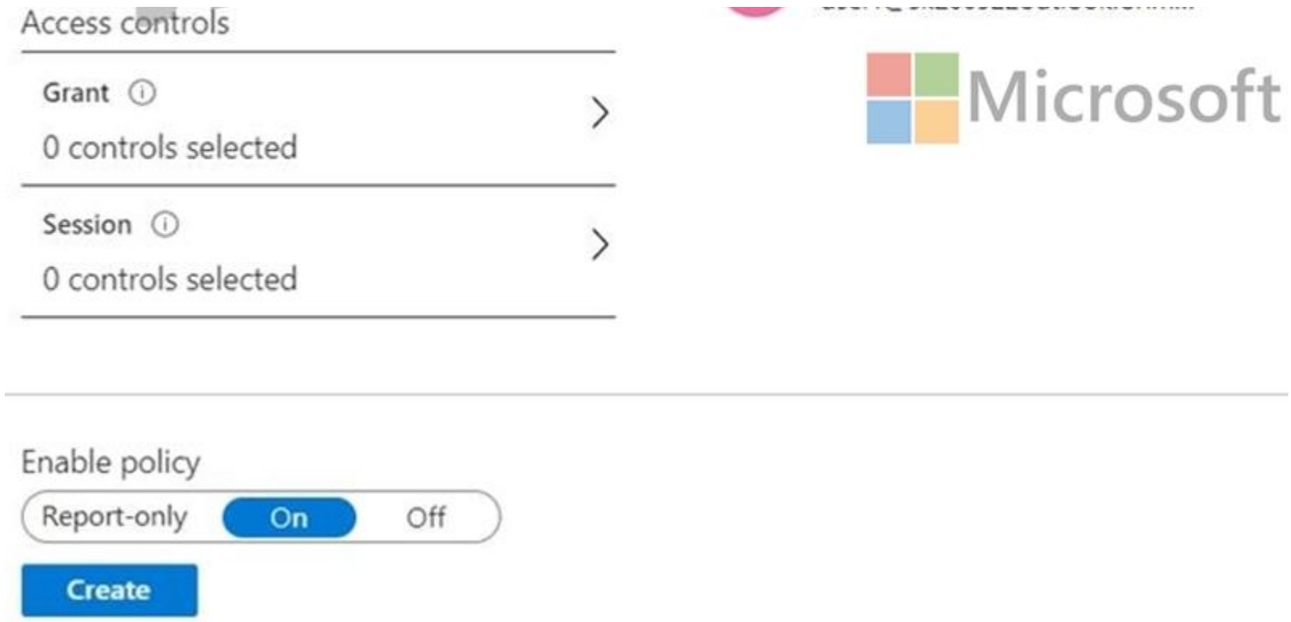
次の設定を持つアクセス レビューを作成します。
確認すべき点: チーム + グループ
対象: すべてのユーザー
グループ: グループ1
レビュー担当者: ユーザーは自分のアクセスをレビューします
User3 のアクセスレビューを実行できるのはどのユーザーですか?
A. ユーザー1のみ
B. ユーザー3のみ
C. ユーザー1とユーザー2のみ
D. ユーザー1、ユーザー2、ユーザー3
Answer: (解答を表示する**)**
包括的かつ詳細な説明：
Microsoft Entra アクセス レビュー設定と、Microsoft Identity and Access Administrator ドキュメントに記載されている原則に基づいて、これを段階的に説明してみましょう。
アクセスレビュー設定について:
レビュー対象: Teams + Groups これは、アクセス レビューが Microsoft Entra テナント内の Teams と Groups のメンバーシップを評価することを示します。指定されたグループは Group1 であるため、レビューは Group1 のメンバーシップに重点を置きます。
スコープ: すべてのユーザースコープはレビュー対象者を定義します。この 「すべてのユーザー」は

最新問題**: 228**
検証済みの回答:
Answer:
* VM1: Managed1 と Managed2 のみ
* App1: システム割り当てマネージドIDとManaged2のみ
すべての Microsoft SC-300: Identity and Access Administrator ドキュメントの包括的かつ詳細な説明:
この質問に答えるには、Azure リソースのマネージド ID の原則を適用する必要があります。マネージド ID は、Microsoft Entra 認証をサポートするリソース (Azure Key Vault や SQL など) への接続時にアプリケーションが使用できる、Microsoft Entra ID で自動的に管理される ID を提供します。
1. アイデンティティの種類を理解する:
* ユーザーオブジェクト (User1): 標準ユーザーアカウントは、人間のサインインに使用されます。標準ユーザーオブジェクト (User1 など) を Azure リソース (VM や App Service など) の ID として割り当てることはできません。リソースはサービスプリンシパルまたはマネージド ID を使用する必要があります。したがって、User1 を含むオプションは正しくありません。
* ユーザー割り当てマネージド ID (Managed1、Managed2): これらは、1 つ以上の Azure リソース (VM や App Services など) に割り当てることができるスタンドアロンの Azure リソースです。
* システム割り当てマネージド ID: これらはリソース自体で直接有効化され、リソースのライフサイクルを共有します。
2. VM1の分析:
* Azure Virtual Machines は、ユーザー割り当てマネージド ID をサポートします。
* 1 つの VM に複数のユーザー割り当て ID を割り当てることができます。
* VM1 のドロップダウン オプションを確認します。
* User1 のオプションは無効です。
* これにより、Managed2 のみ、または Managed1 と Managed2 のみ残ります。
* Managed1 と Managed2 はどちらもサブスクリプションで使用できる有効なユーザー割り当て ID であるため、両方を割り当てることができます。
* 結論: Managed1 と Managed2 のみを選択します。
3. App1の分析:

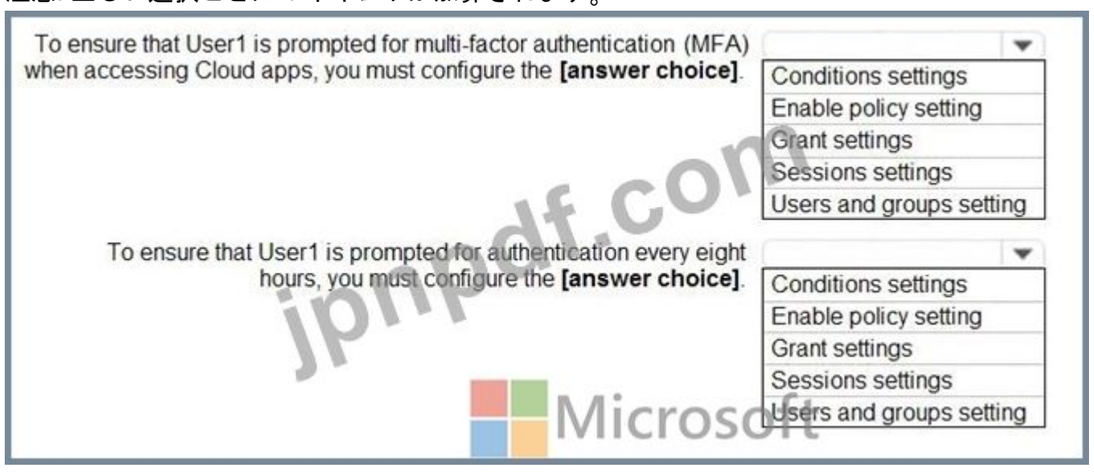
* Azure App Services は、システム割り当てマネージド ID とユーザー割り当てマネージド ID の両方を同時にサポートします。
* App1 のドロップダウン オプションを確認します。
* User1 のオプションは無効です。
* Managed1 がドロップダウン オプションに表示されていません (マネージド ID はリソースと同じリージョンに存在する必要があります。多くの場合、この質問はリージョンの不一致を意味しているか、単に選択肢を制限しています)。
* Managed2 は有効なユーザー割り当てオプションとしてリストされます。
* システム割り当てマネージド ID が有効なオプションとしてリストされます。
* システム割り当て ID とユーザー割り当て ID の両方を同時に使用するように App Service を構成できるため、最も完全な正解は、使用可能なすべての ID を識別します。
* 結論: システム割り当てマネージド ID と Managed2 のみを選択します。
参考抜粋:
Azure リソースのマネージド ID は、Azure Active Directory で自動的に管理される ID を Azure サービスに提供します... マネージド ID には、システム割り当てとユーザー割り当ての 2 種類があります...
[Azure Virtual Machines および Azure App Service] にユーザー割り当てマネージド ID を割り当てることができます。(出典: Microsoft Learn - Azure リソースのマネージド ID とは何ですか?)
最新問題**: 229**
セキュリティの既定値が無効になっている Azure Active Directory (Azure AD) テナントがあります。
次の図に示すように、条件付きアクセス ポリシーを作成します。



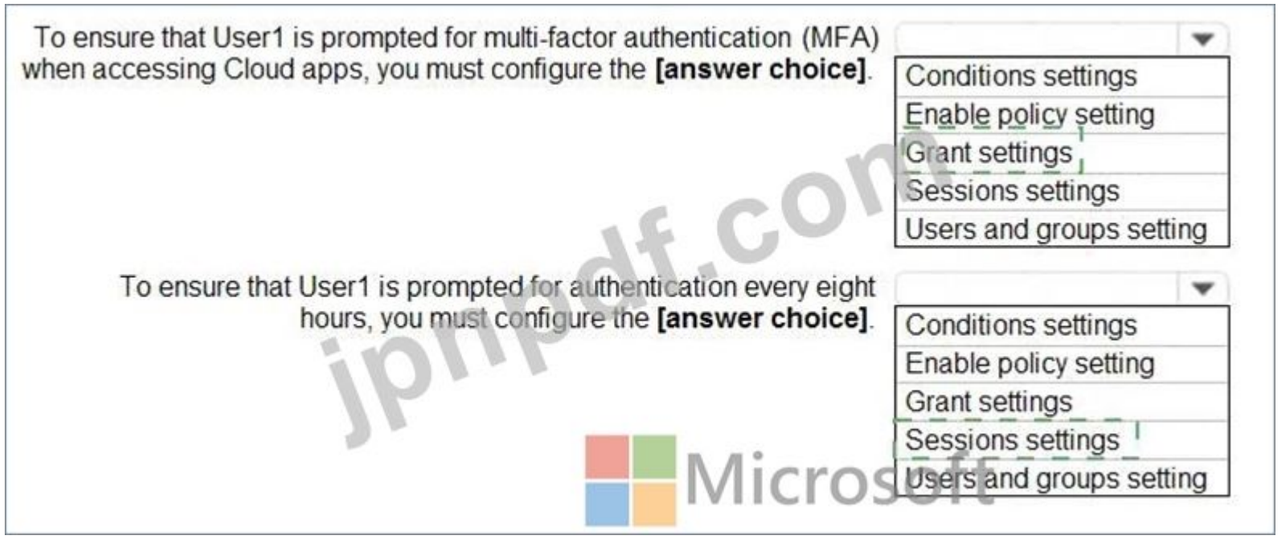
Jpnpdf.com



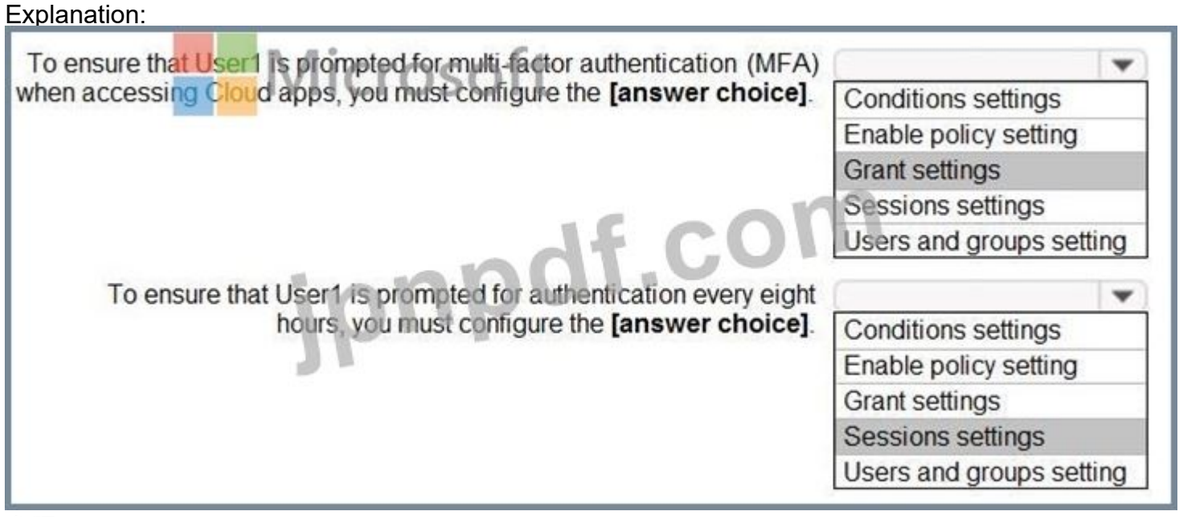
ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



参照：

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

最新問題: 230

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、グループ1、グループ2

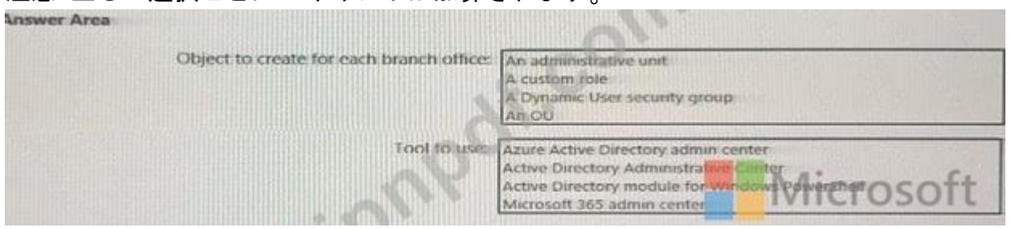
B. User1とGroup1のみ

C. ユーザー1とGtoup2のみ

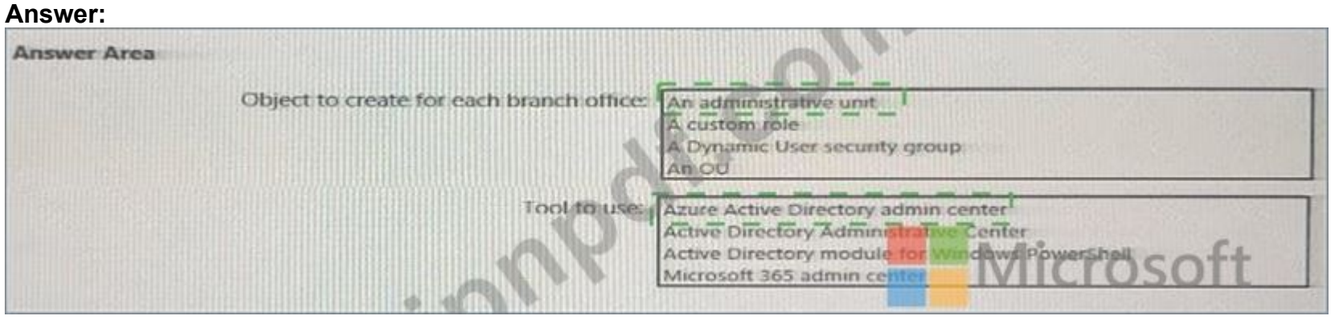
D. ユーザー1のみ

Answer: (解答を表示する)

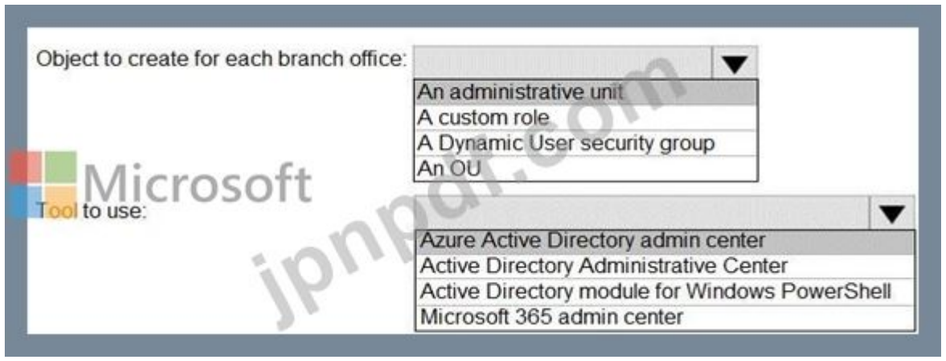
最新問題: **231**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明
テキストの説明は自動的に生成されます



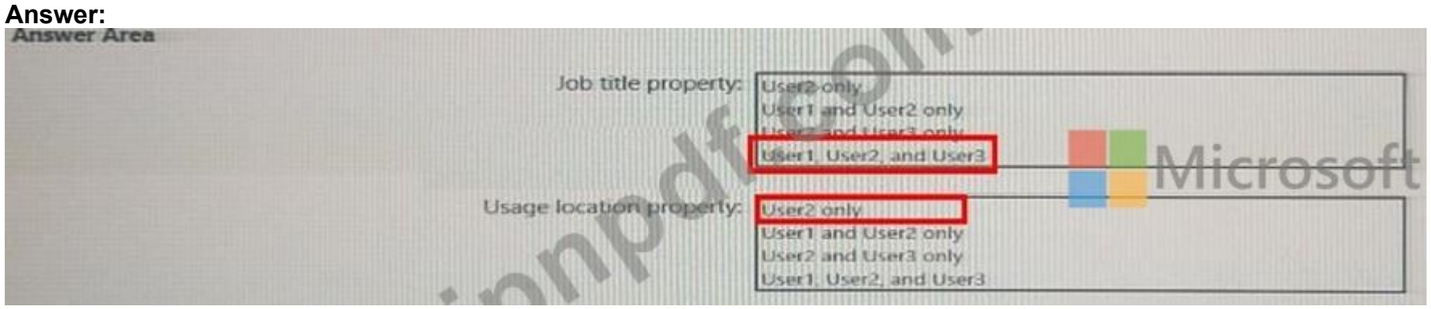
最新問題: **232**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

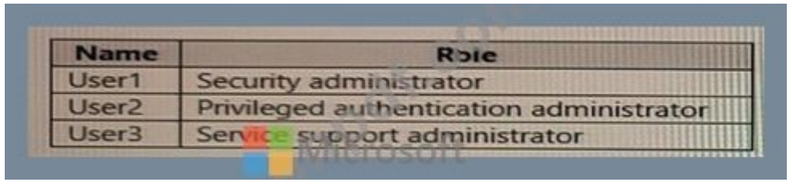


Answer:



最新問題: **233**

次の表に示すユーザーを含む Azure AD テナントがあります。

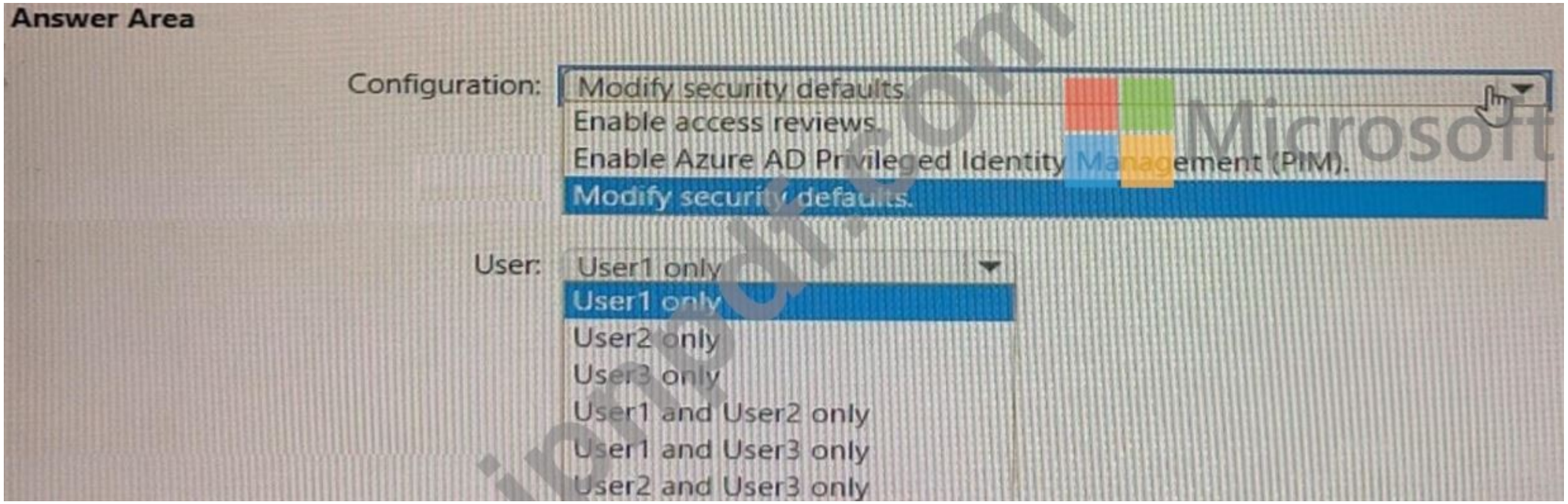


Name	Role
User1	Security administrator
User2	Privileged authentication administrator
User3	Service support administrator

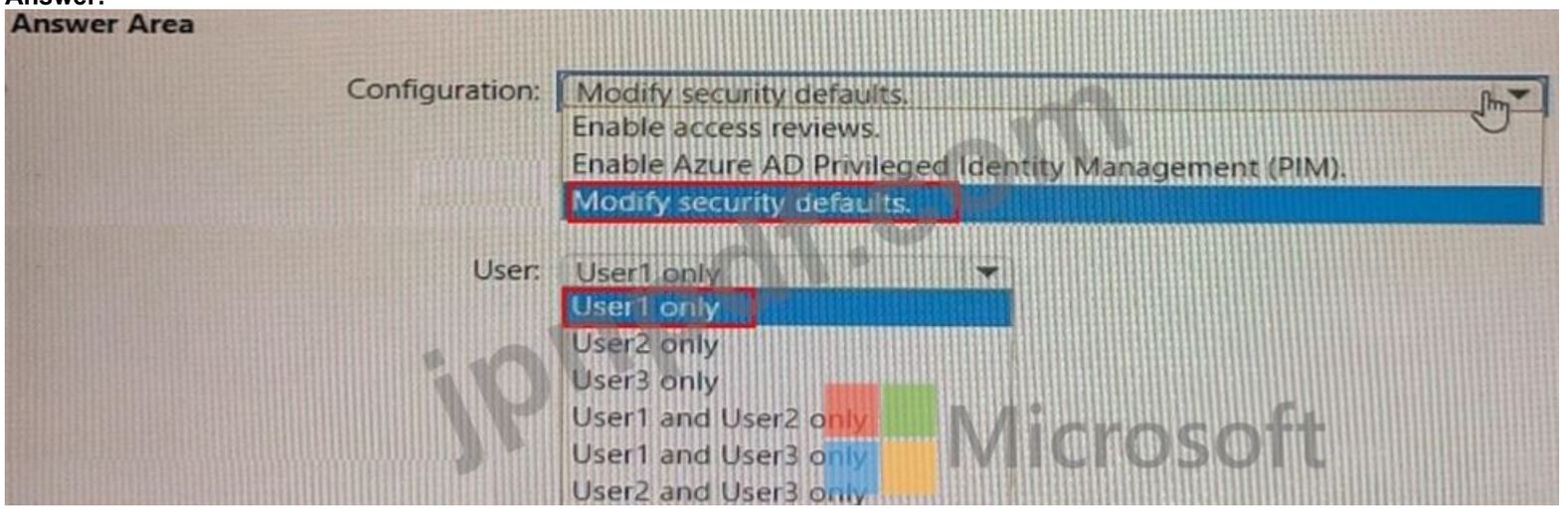
User2 は、Microsoft Authenticator アプリを使用するには多要素認証 (MFA) のみを構成できると報告しています。

User2 が代替 MFA 方法を構成できることを確認する必要があります。

どのような構成が必要で、どのユーザーが構成を実行す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。



Answer:

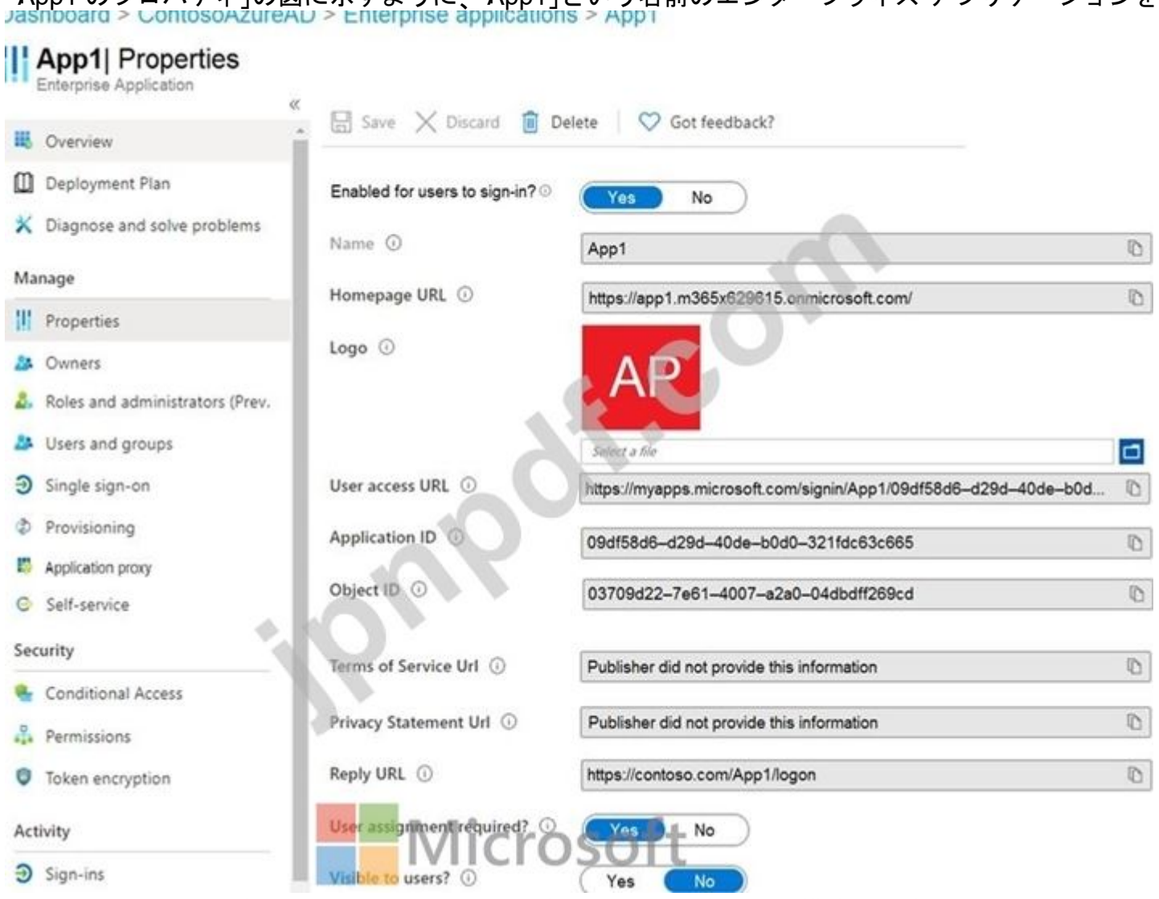


最新問題: 234

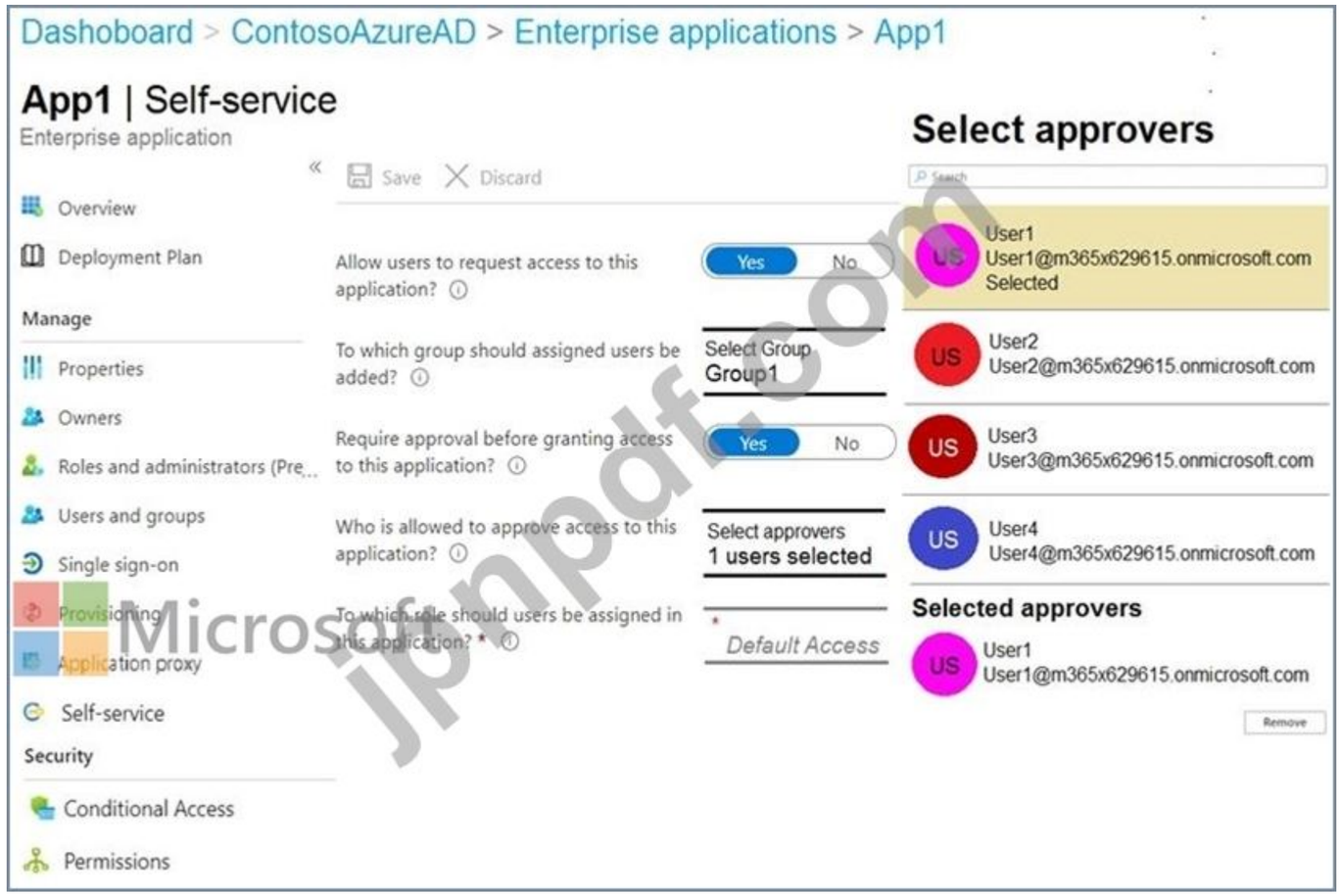
Group1 の図に示すように、Group1 という名前のグループを含む Microsoft 365 テナントがあります。([Group1] タブをクリックします。)



App1 のプロパティ」の図に示すように、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 のセルフサービスは、App1 セルフサービス」の図に示すように構成します。(App1 セルフサービス」タブをクリックします。)



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 ポイントが加算されます。

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Explanation:
いいえ
いいえ
はい
a) アプリケーションにグループを割り当てると、そのグループ内のユーザーのみがアクセスできるようになります。割り当てはネストされたグループには適用されません。
b) ラボでテスト済み。既存の所有者は置き換えられます。また、リソース所有者への直接割り当ては最小限の権限のパスとなります。(テストで再現済み) c) アプリケーション設定の 「ユーザーに表示」が「いいえ」に設定されているため、ユーザーのマイアプリポータルとO365ランチャーにこのアプリケーションは表示されません。
参照
a) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal b) おそらく https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-manage- groups c) https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/application-properties#visible-to-users

最新問題: **235**
次の表に示すキー コンテナーを含む Azure サブスクリプションがあります。

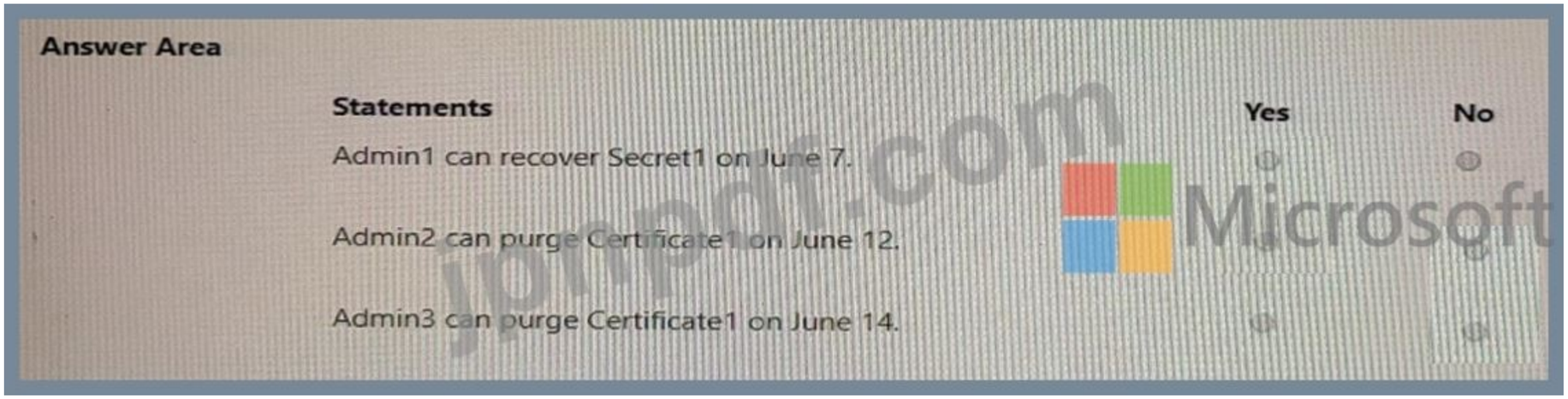
Name	In resource group	Number of days to retain deleted key vaults	Purge protection
KeyVault1	RG1	15	Enabled
KeyVault2	RG1	10	Disabled

サブスクリプションには、次の表に示すユーザーが含まれます。

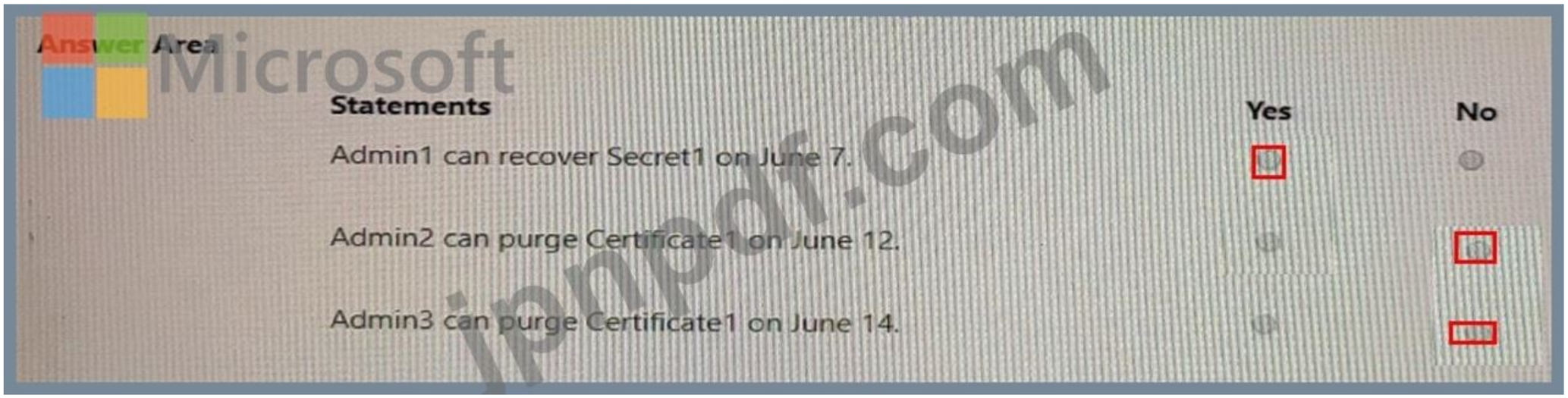
Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

6月1日に、Admin4は次のアクションを実行します。
* Key Vault1からCertificate!という名前の証明書を削除します

* KeyVault2からSecret1という名前のシークレットを削除します
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 ポイントが加算されます。



Answer:

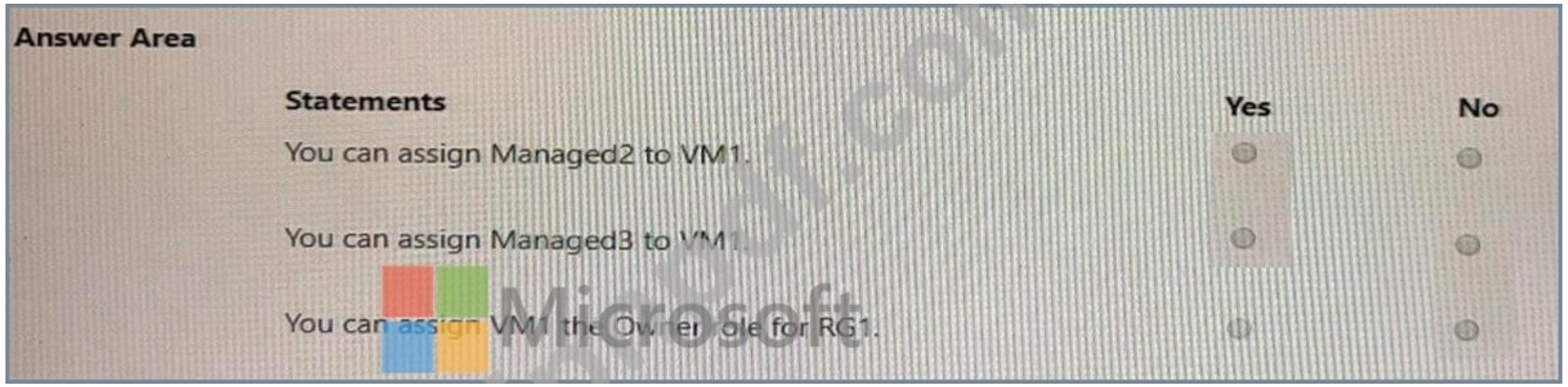


最新問題: 236
次の仮想マシンが含まれる Azure サブスクリプションがあります。名前: VM1、Azure リージョン: 米国東部、システム割り当てマネージド ID: 無効。次の表に示すマネージド ID を作成します。

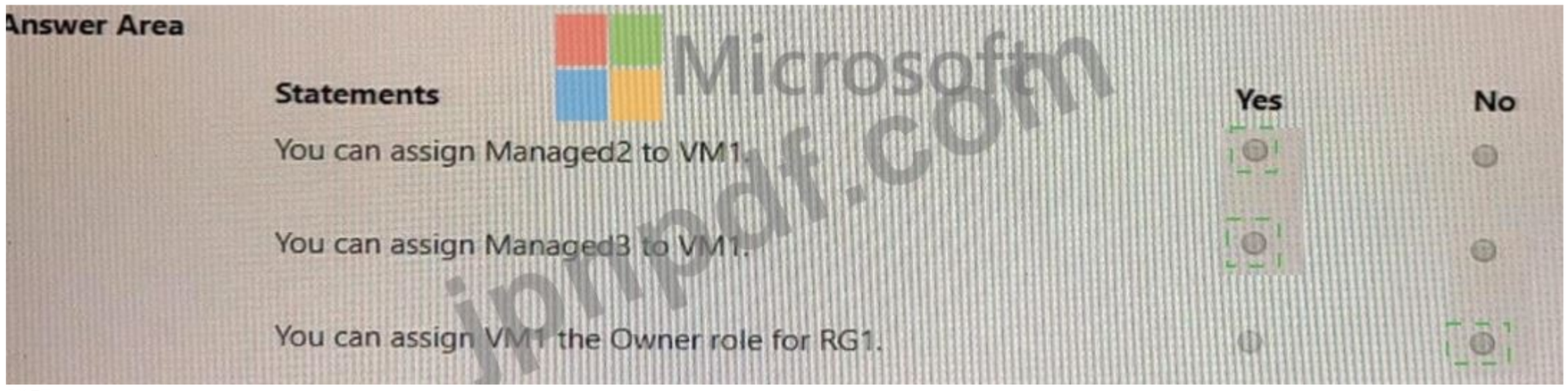
Name	Location
Managed1	East US
Managed2	East US
Managed3	West US

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。
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。

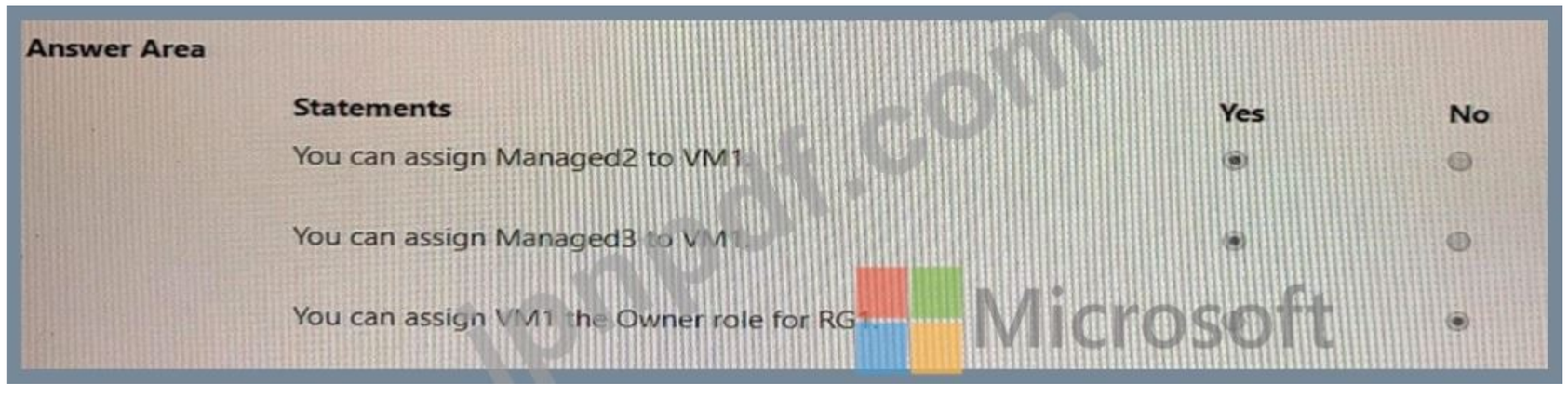
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明



最新問題: **237**

次の表に示すホストを含むオンプレミス データセンターがあります。

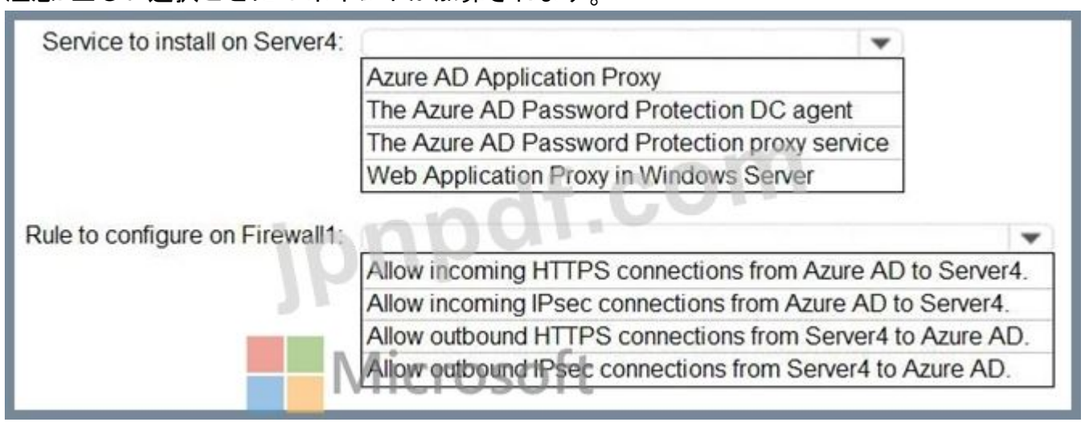
Name	Description
Server1	Domain controller that runs Windows Server 2019
Server2	Server that runs Windows Server 2019 and has Azure AD Connect deployed
Server3	Server that runs Windows Server 2019 and has a Microsoft ASP.NET application named App1 installed
Server4	Unassigned server that runs Windows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

Active Directory フォレストと同期する Azure Active 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。

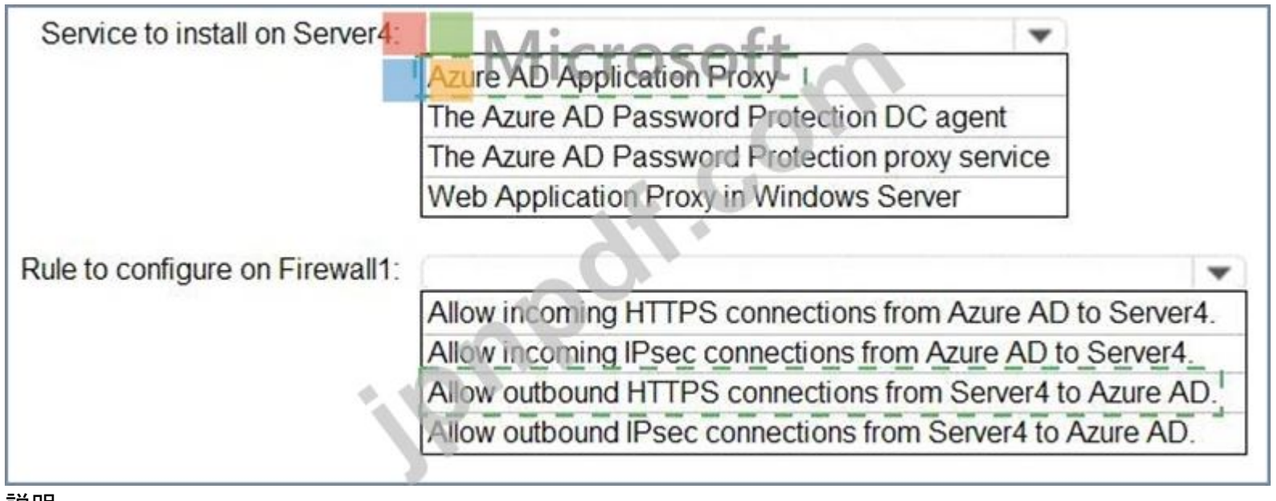
App1 を Azure AD ユーザーに公開できることを確認する必要があります。

Server と Firewall1 で何を設定す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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明

Service to install on Server4:

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

Rule to configure on Firewall1:

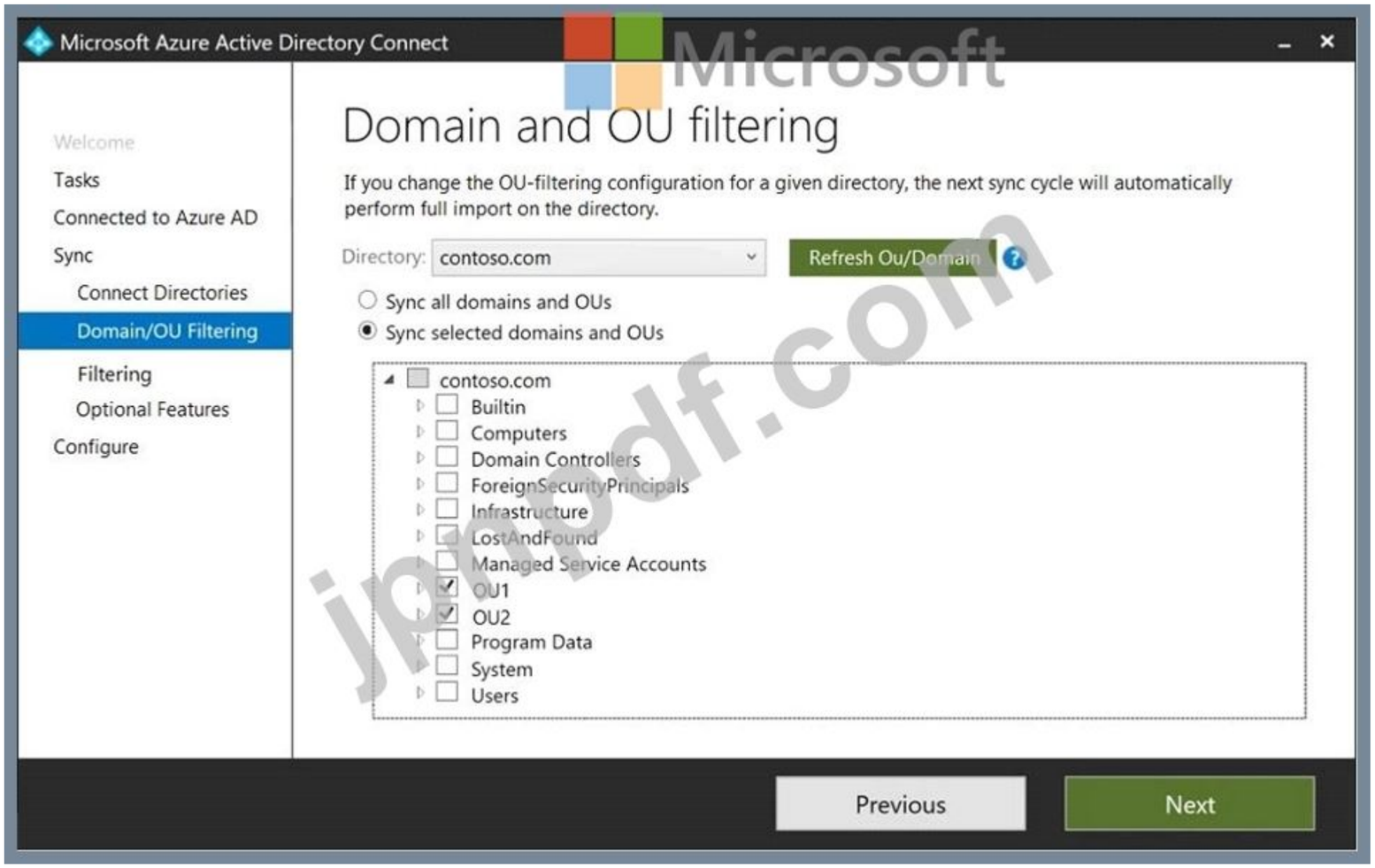
- Allow incoming HTTPS connections from Azure AD to Server4.
- Allow incoming IPsec connections from Azure AD to Server4.
- Allow outbound HTTPS connections from Server4 to Azure AD.
- Allow outbound IPsec connections from Server4 to Azure AD.

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

最新問題: 238
ネットワークには、contoso.com というオンプレミスの Active Directory ドメインが含まれています。このドメインには、次の表に示すオブジェクトが含まれています。

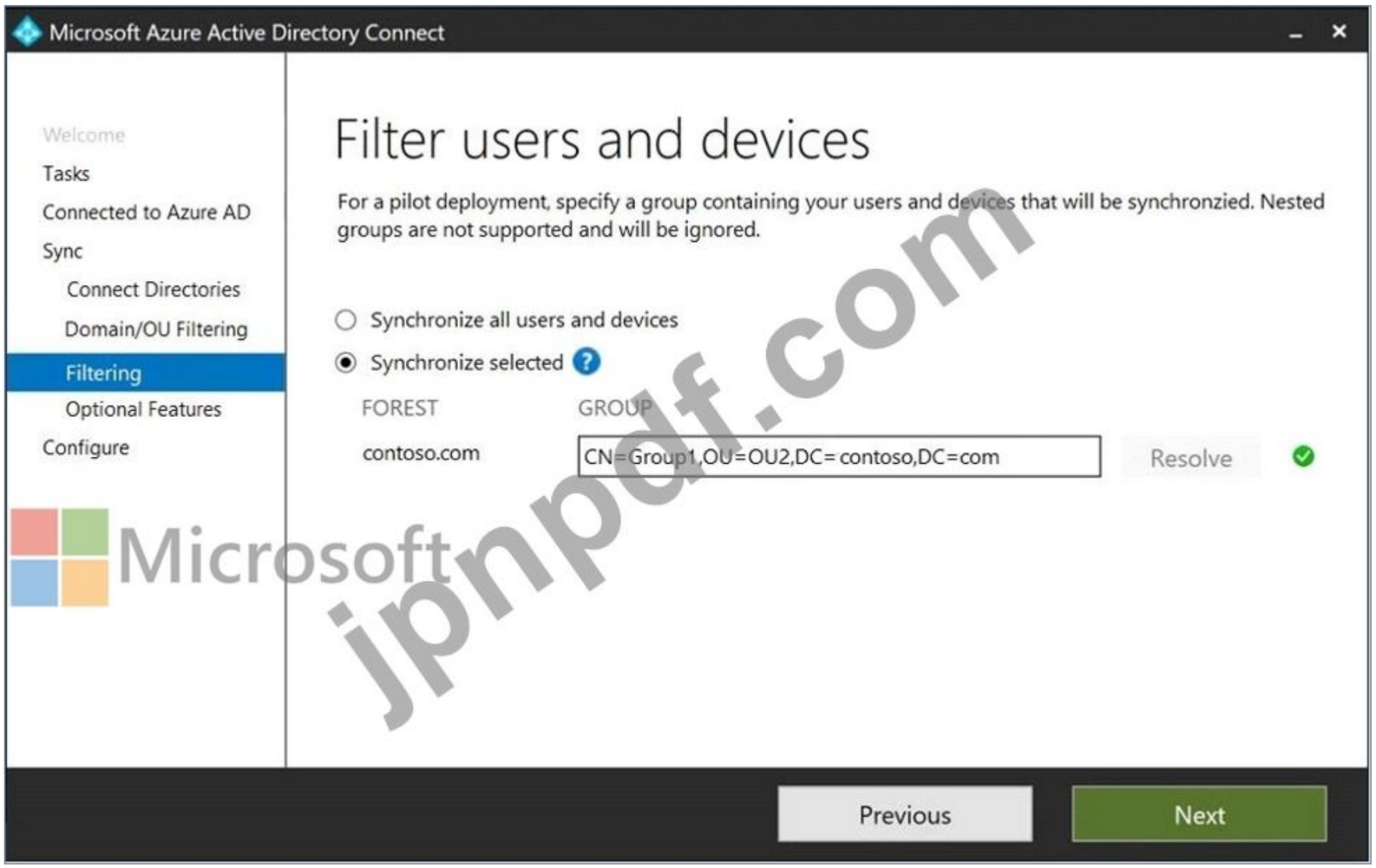
Name	Type	In organizational unit (OU)	Description
User1	User	OU1	User1 is a member of Group1.
User2	User	OU1	User2 is not a member of any groups.
Group1	Security group	OU2	User1 and Group2 are members of Group1.
Group2	Security group	OU1	Group2 is a member of Group1.

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」の図に示すように、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 のフィルタリング」タブをクリックします。)



jpbpdf.com

凸ーザーとデバイスのフィルター」設定は、凸ーザーとデバイスのフィルター」の図に示すように構成します。(凸ーザーとデバイスのフィルター」タブをクリックします。)



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 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:

Microsoft
jpnpdf.com



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

最新問題: **239**
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

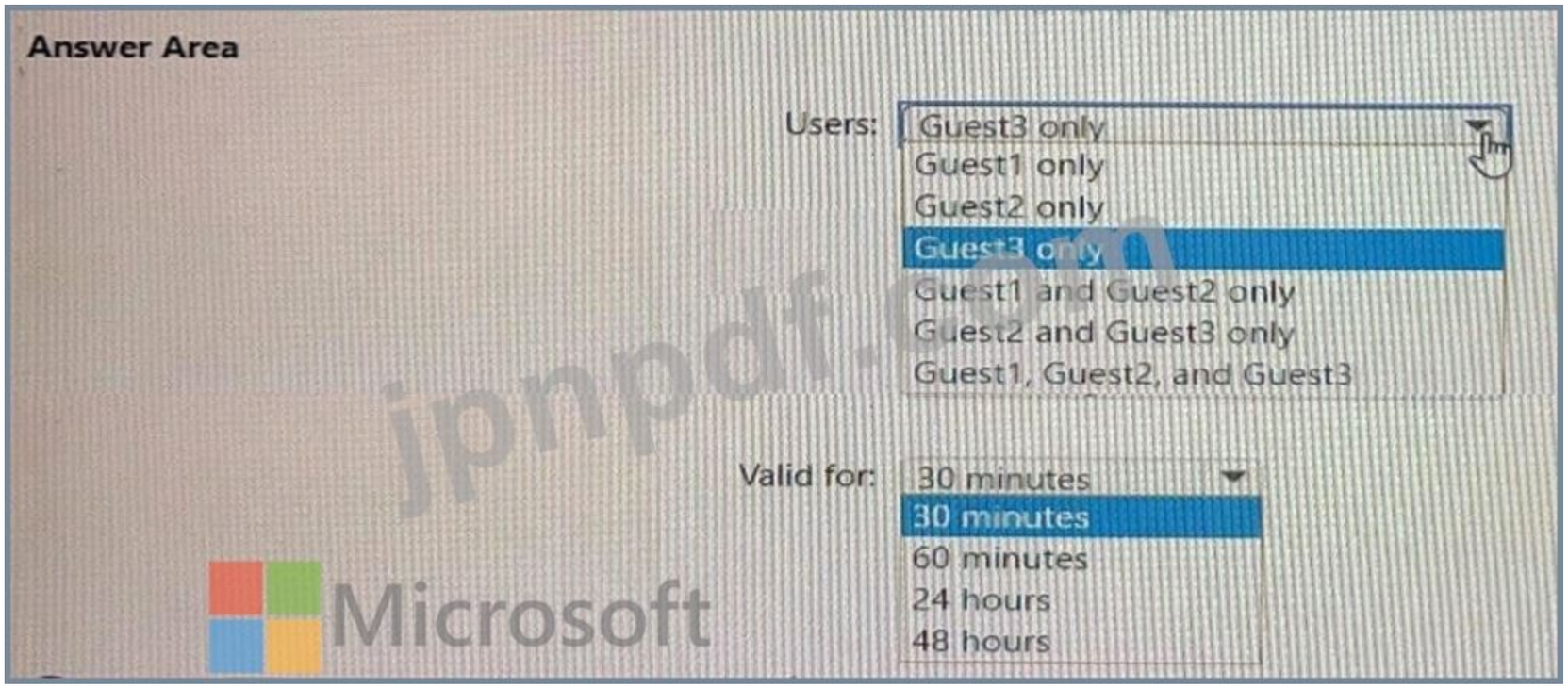
Azureポータルを使用して、Role3というカスタムAzureサブスクリプションロールを作成する必要があります。Role3は既存のロールのベースライン権限を使用します。Role3を作成するには、どのロールを複製すればよいですか？

A. ロール2のみ
B. 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
C. 組み込みの Azure サブスクリプション ロールと Role2 のみ
D. 組み込みの Azure サブスクリプション ロールのみ
E. 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
Answer: C (メーッセージを残す)

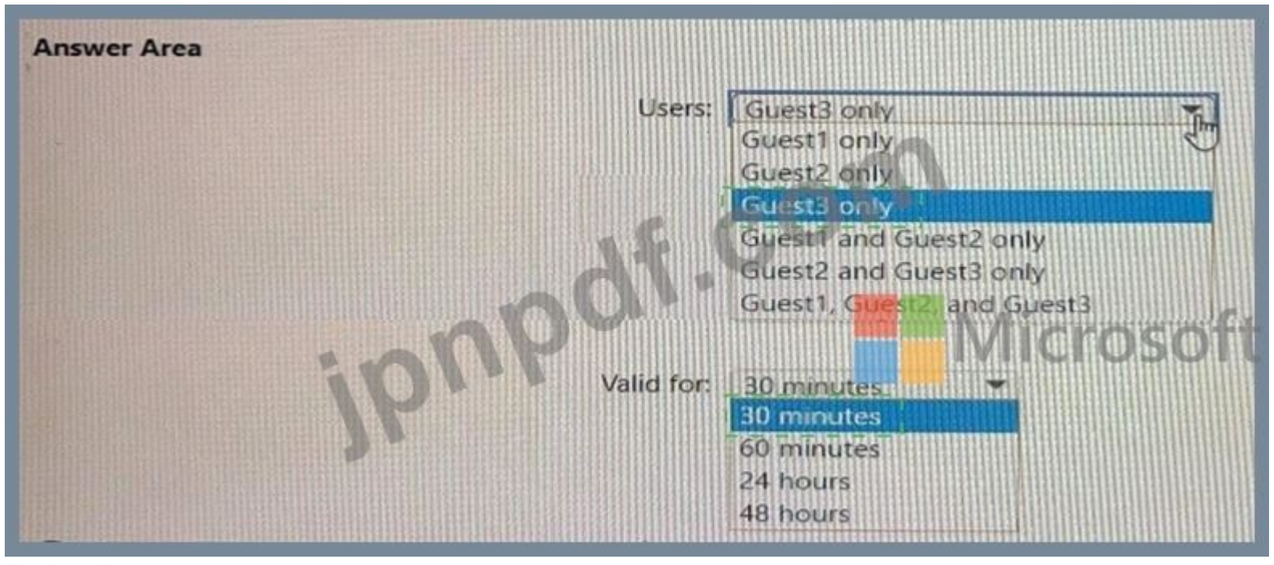
最新問題: **240**
contoso.com という名前の Azure AD テナントがあり、ゲスト用のワンタイム パスコードを電子メールで送信することが [はい] に設定されています。
次の表に示すゲスト ユーザーを招待します。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

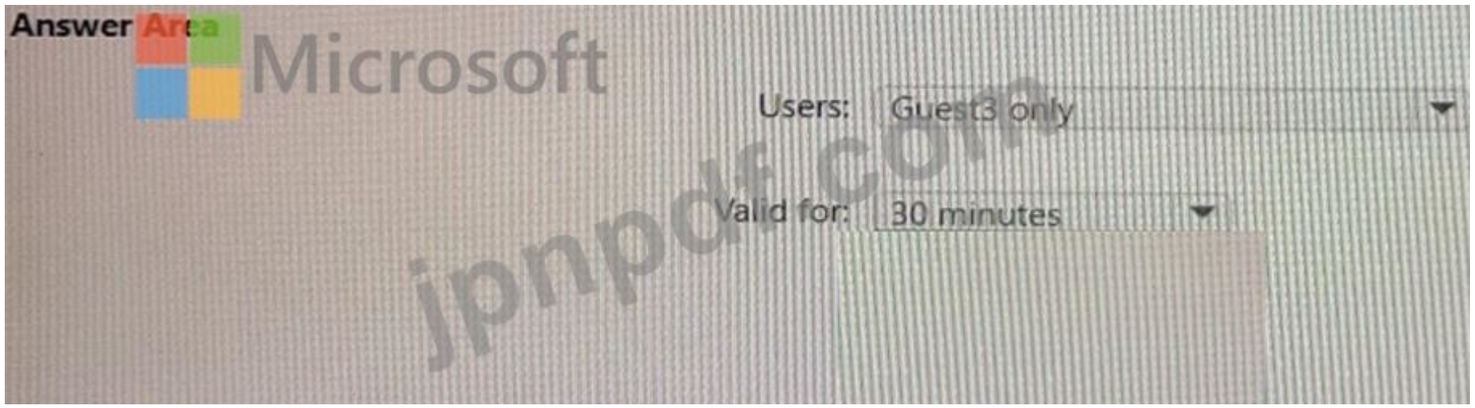
ワンタイム パスコードを受け取るユーザーは誰ですか? また、パスコードの有効期間はどのくらいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: **241**
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。
どのユーザーが PIM を使用してロール権限をアクティブ化できますか?
A. Admin3のみ
B. 管理者2のみ
C. Admin2 と Admin3 のみ
D. 管理者1、管理者2、管理者3
E. 管理者のみ
F. Admin1 と Admin2 のみ
Answer: F (メーッセージを残す**)**

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **242**
contoso.com という名前の Microsoft 365 テナントがあります。
ゲストユーザーアクセスが有効になっています。
次の表に示すように、ユーザーは contoso.com との共同作業に招待されます。

User email	User type	Invitation accepted	Shared resource
User1@outlook.com	Guest	No	Enterprise application
User2@fabrikam.com	Guest	Yes	Enterprise application

Azure Active Directory 管理センターの外部コラボレーション設定から、次の図に示すようにコラボレーション制限設定を構成します。



ユーザーは、Microsoft SharePoint Online サイトから user3@adatum.com をサイトに招待します。

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 ポイントが加算されます。

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

Answer:

Statements	Yes	No
User1 can accept the invitation and gain access to the enterprise application.	○	○
User2 can access the enterprise application.	○	○
User3 can accept the invitation and gain access to the SharePoint site.	○	○

最新問題: **243**

ホットスポットに関する質問

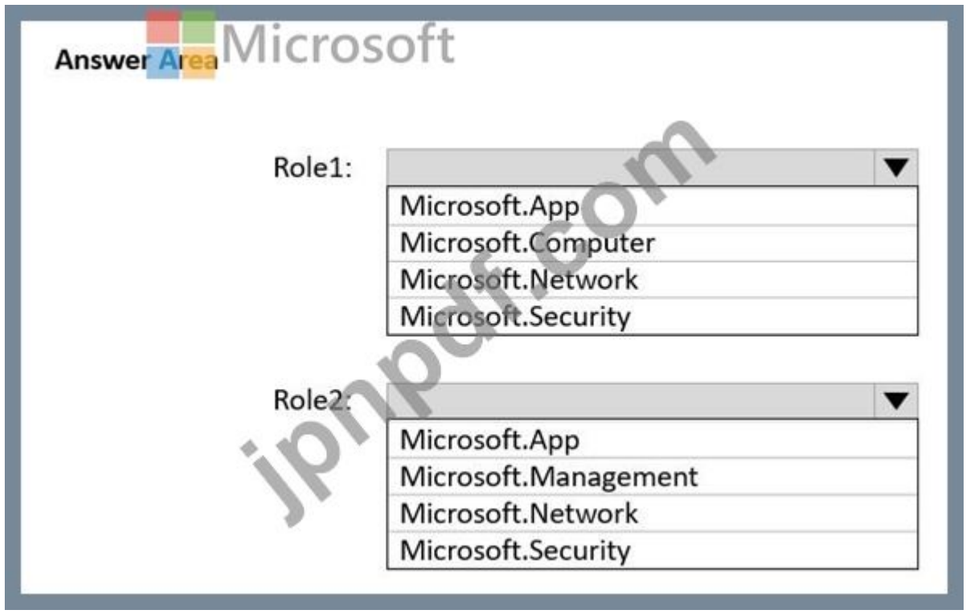
Azure サブスクリプションをお持ちです。

Role1とRole2という2つのカスタムロールを作成する必要があります。ソリューションは以下の要件を満たす必要があります。

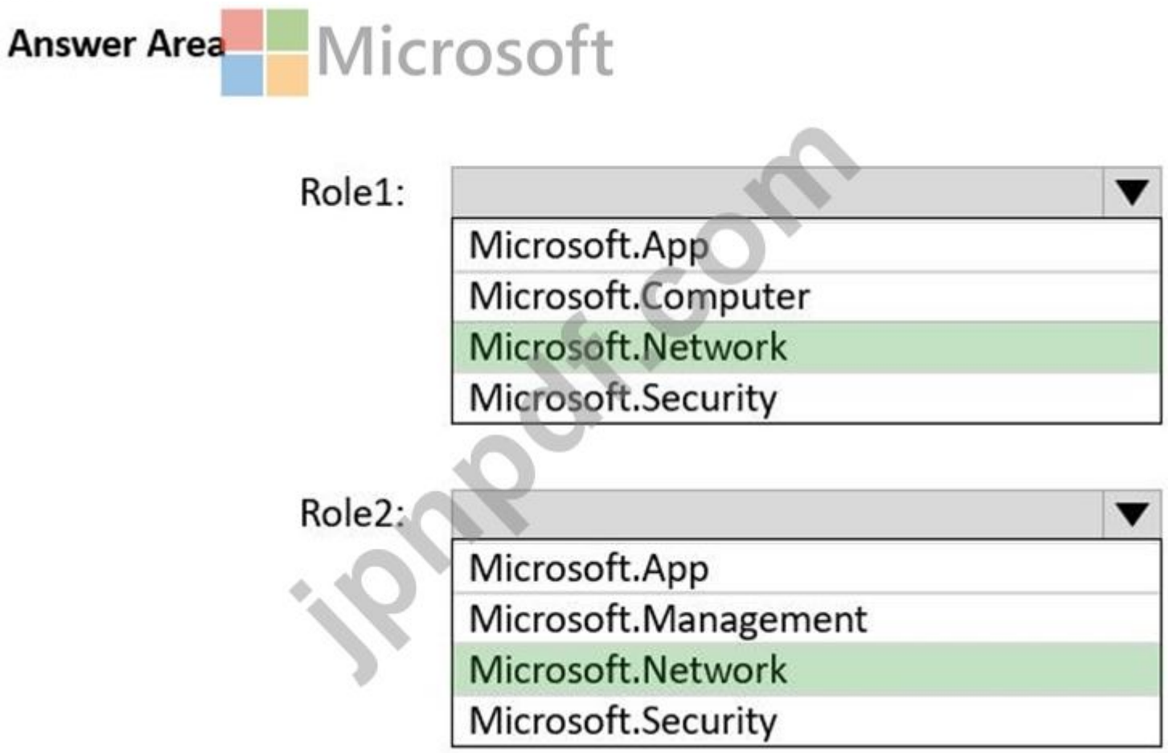
- Role1 が割り当てられたユーザーは、アプリケーション セキュリティ グループを管理できます。
- Role2 が割り当てられたユーザーは Azure Firewall を管理できます。

各ロールにはどのリソース プロバイダーのアクセス許可が必要ですか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/role-based-access-control/resource-provider- operations#microsoftnetwork

最新問題**: 244**
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	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

次の設定を持つユーザー リスク ポリシーがあります。
* 課題:
含める: グループ1
o 除外: グループ2
* サインインリスク 中以上
* アクセス制御:
o アクセスを許可する: パスワードの変更を要求する
ユーザーがサインインしようとすると、次の表に示すようにユーザーのリスク レベルが検出されます。

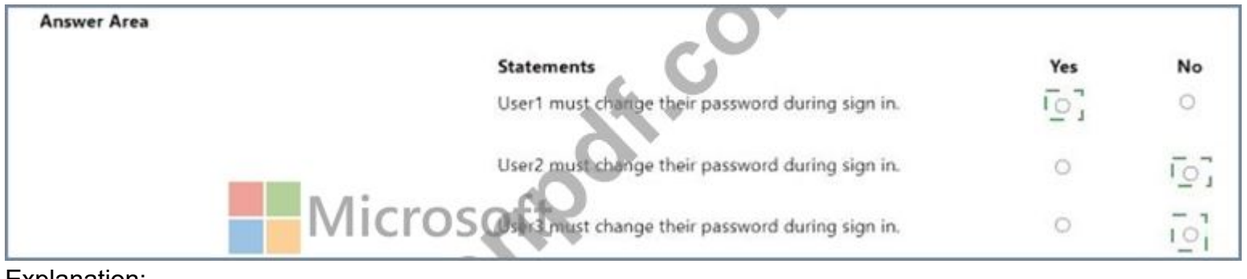


User	Risk level
User1	High
User2	Medium
User3	High

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。



Answer:

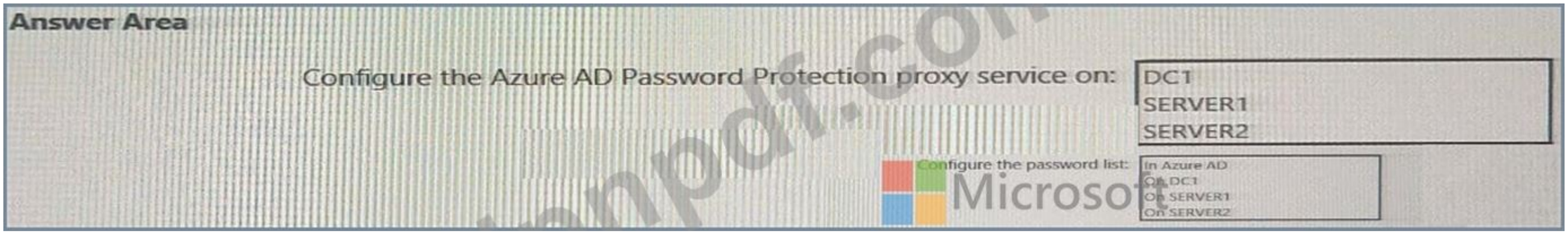


Explanation:

Answer Area

Statements	Yes	No
User1 must change their password during sign in.	●	○
User2 must change their password during sign in.	○	●
User3 must change their password during sign in.	○	●

最新問題**: 245**
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 Azure AD パスワード保護 DC エージェントをインストールします。
次に何をすべきでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

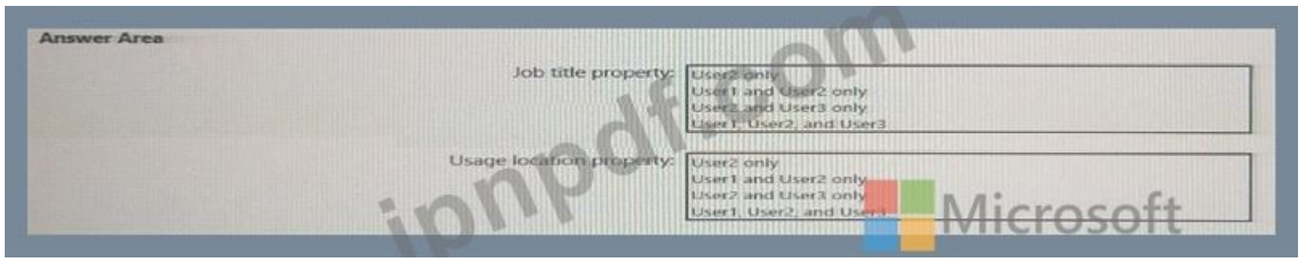


Explanation:
サーバー1
DC1で

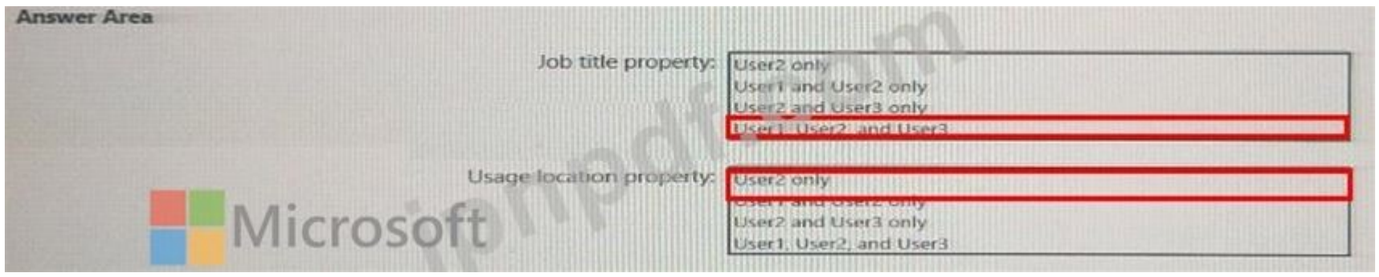
最新問題**: 246**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

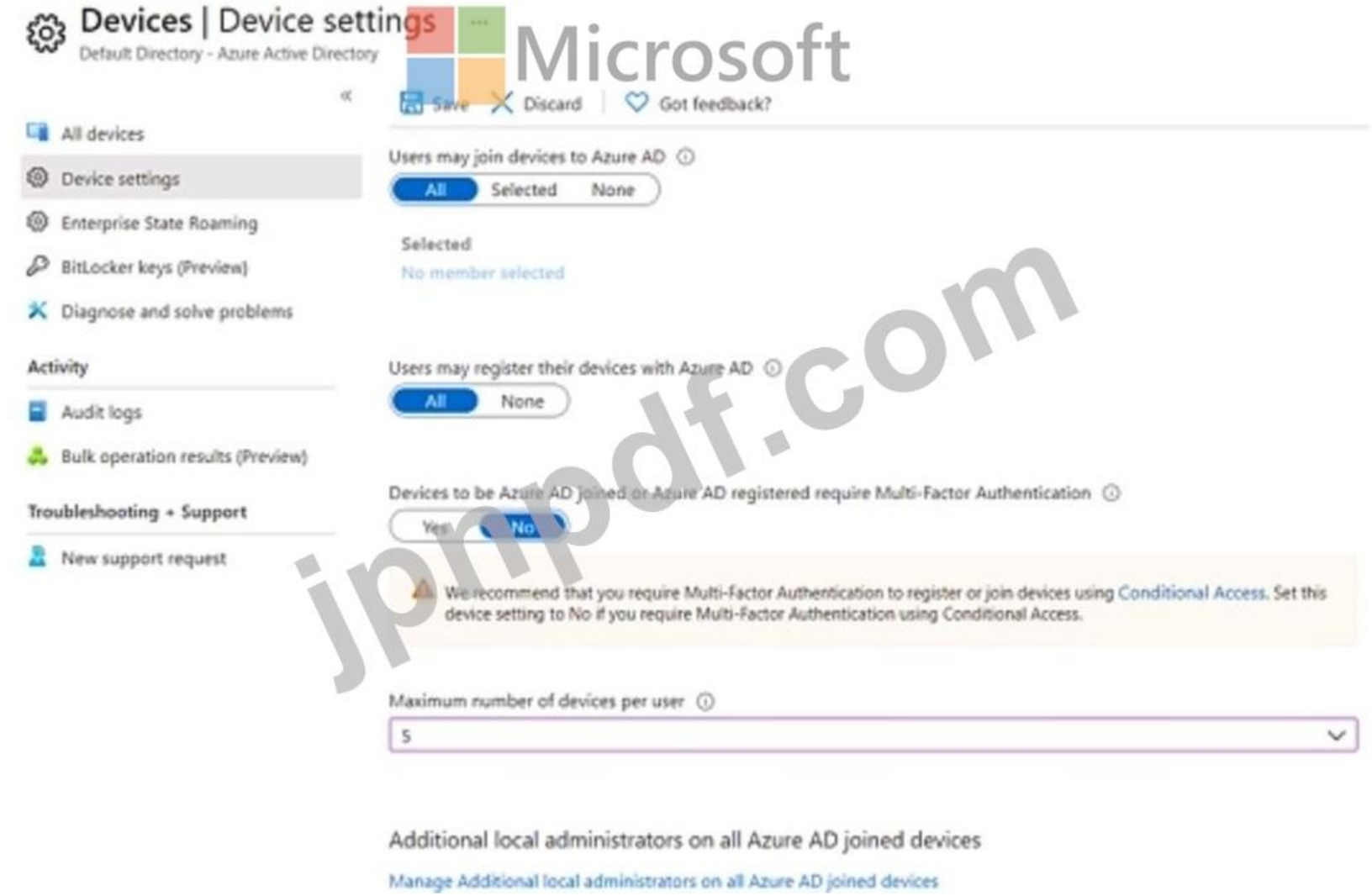


最新問題**: 247**
会社が Microsoft 365 E5 サブスクリプションを購入します。
User1 というユーザーには、セキュリティ管理者ロールが割り当てられています。
User1 が Microsoft Defender for Cloud Apps セッション ポリシーを作成できることを確認する必要があります。
まず何をすべきでしょうか?
A. 条件付きアクセス ポリシーを作成し、アプリ保護ポリシーを必要とするを選択します。
B. 条件付きアクセス ポリシーを作成し、条件付きアクセス アプリ制御の使用を選択します。
C. クラウド アプリケーション管理者のロールを User1 に割り当てます。
D. Cloud App Security 管理者ロールを User1 に割り当てます。
Answer: B (メーッセージを残す**)**
https://learn.microsoft.com/en-us/defender-cloud-apps/セッションポリシー-aad

最新問題**: 248**
ホットスポットに関する質問
Microsoft Entra ID P2 サービスプランをご利用の Microsoft Entra テナントがあります。このテナントには、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	Microsoft Entra Joined Device Local 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	Microsoft Entra joined
Device2	iOS	Microsoft Entra registered
Device3	Windows 10	Microsoft Entra registered
Device4	Android	Microsoft Entra registered

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 ポイントが加算されます。

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	○
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	○	○
Admin2 is a local administrator on Device3.	○	○

Answer:

Answer Area

Statements	Yes	No
User1 can join four additional Windows 10 devices to Microsoft Entra ID.	○	●
Admin1 can set Devices to be Microsoft Entra joined or Microsoft Entra registered require Multi-Factor Authentication to **Yes**.	●	○
Admin2 is a local administrator on Device3.	○	●

最新問題: **249**

Sub1 という名前の Azure サブスクリプションがあります。

Microsoft Entra Permissions Management を展開する予定です。

権限管理がSub1にアクセスできることを確認する必要があります。ソリューションは最小権限の原則に従う必要があります。

PowerShell コマンド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: 250

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

過去に発生したサインインを調査するには、Azure AD サインイン ログを確認する必要があります。

Azure AD はサインイン ログにイベントをどのくらいの期間保存しますか?

A. 14日間

B. 30日間

C. 90日間

D. 365日

Answer: B (メーッセージを残す)

参照：

https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/reference-reports-dataretention# azure-ad がデータを保存する期間

最新問題: 251

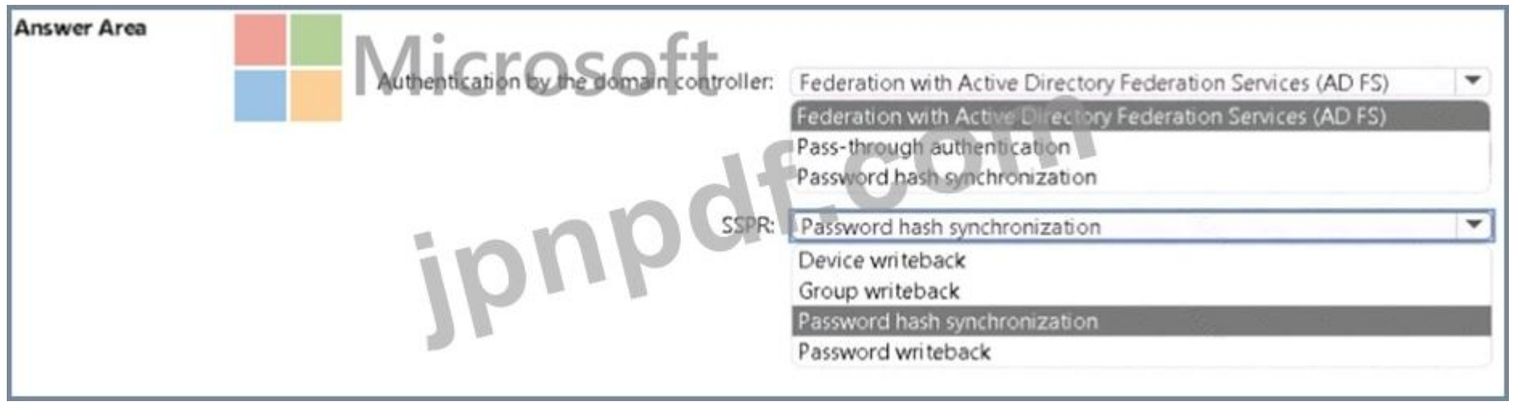
オンプレミスネットワークには、Azure AD Connect を使用して Azure AD テナントと同期する Active Directory ドメインが含まれています。以下の要件を満たすように Azure AD Connect を構成する必要があります。

* 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**: 252**

次の図に示すように、ユーザー管理者ロールの Azure AD Privileged Identity Management (PIM) ロール設定を含む Azure Active Directory (Azure AD) テナントがあります。

Role setting details - User Administrator

Privileged Identity Management | Azure AD roles

Edit

Activation

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

Assignment

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

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

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

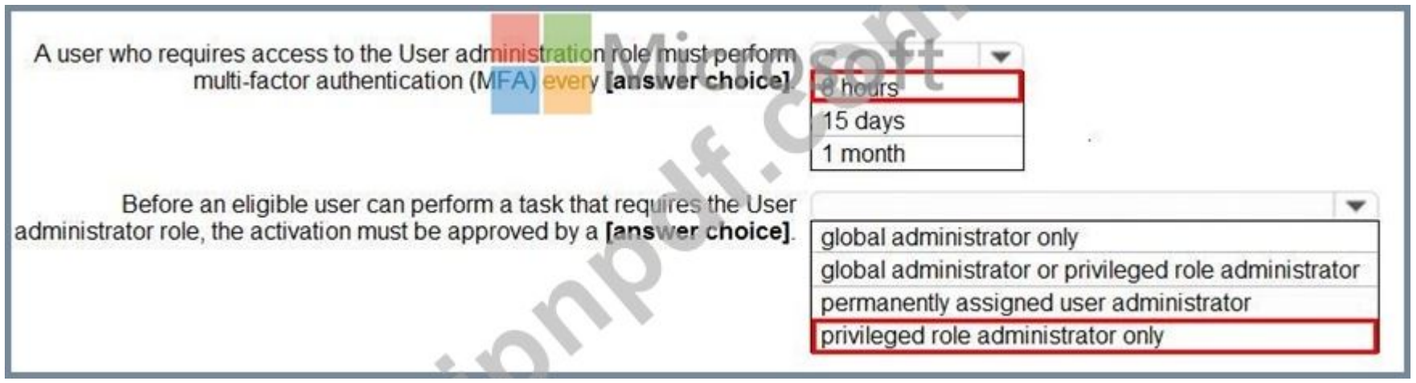
- 8 hours
- 15 days
- 1 month

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

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

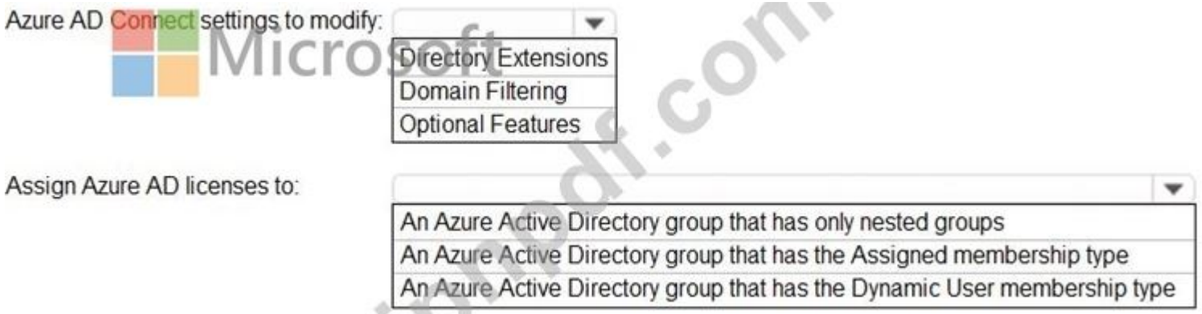
Answer:

jpnpdf.com



参照：
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**: 253**
Litware ユーザーへの Azure AD ライセンスの割り当てを構成する必要があります。ソリューションはライセンス要件を満たしている必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



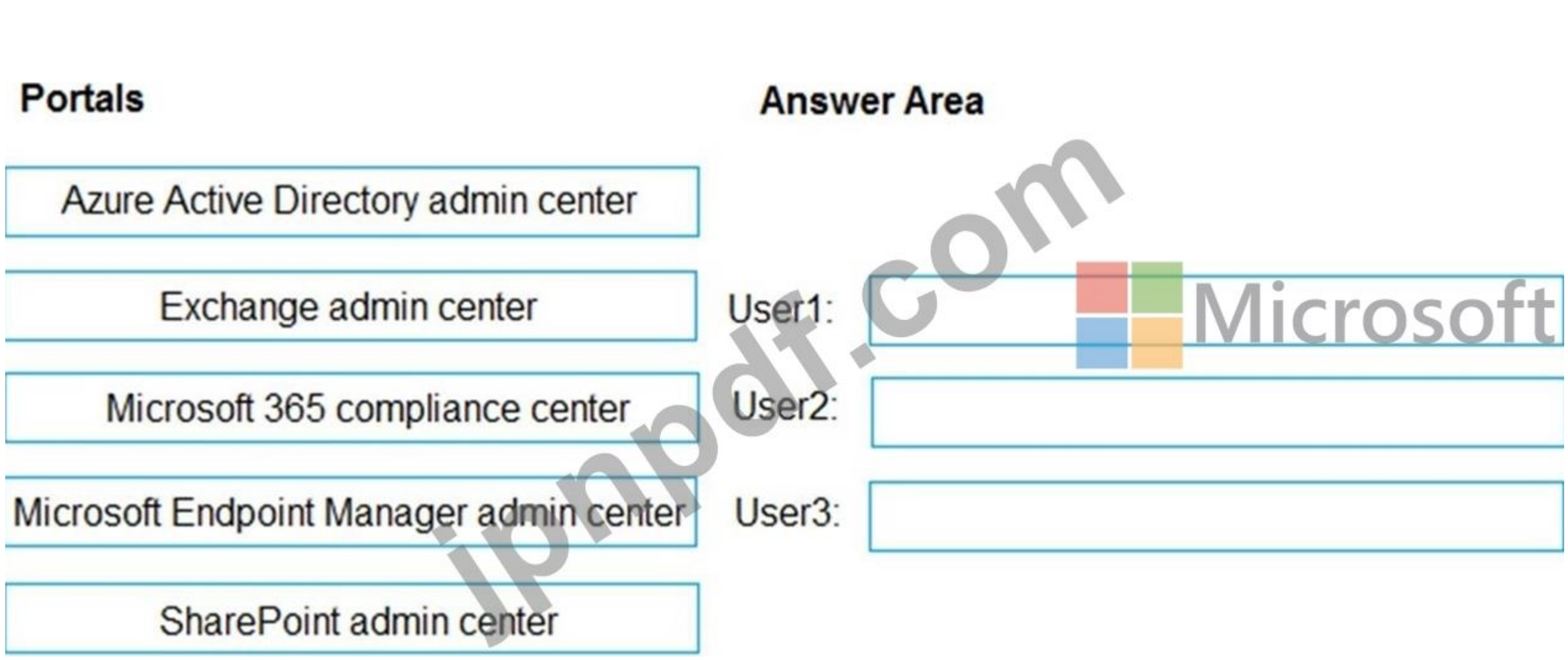
最新問題**: 254**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Azure AD 企業間 (B2B) コラボレーション ユーザーを一括招待する予定です。

一括招待を作成するときに含める必要がある 2 つのパラメータはどれですか。正解はそれぞれソリューションの一部を示します。注: 正解を選択するごとに 1 ポイントが加算されます。
A. メールアドレス
B. リダイレクトURL
C. ユーザー名
D. 共有キー
E. パスワード
Answer: A,B (メーッセージを残す)
必要な値は次のとおりです。
招待するメールアドレス - 招待を受け取るユーザー
リダイレクトURL - 招待を承諾したユーザーが転送されるURL。ユーザーを 『マイアプリ」ページに転送したい場合は、この値を次のように変更する必要があります。
https://myapps.microsoft.com または https://myapplications.microsoft.com。
参照 :
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite#invite-guest-users-in-bulk

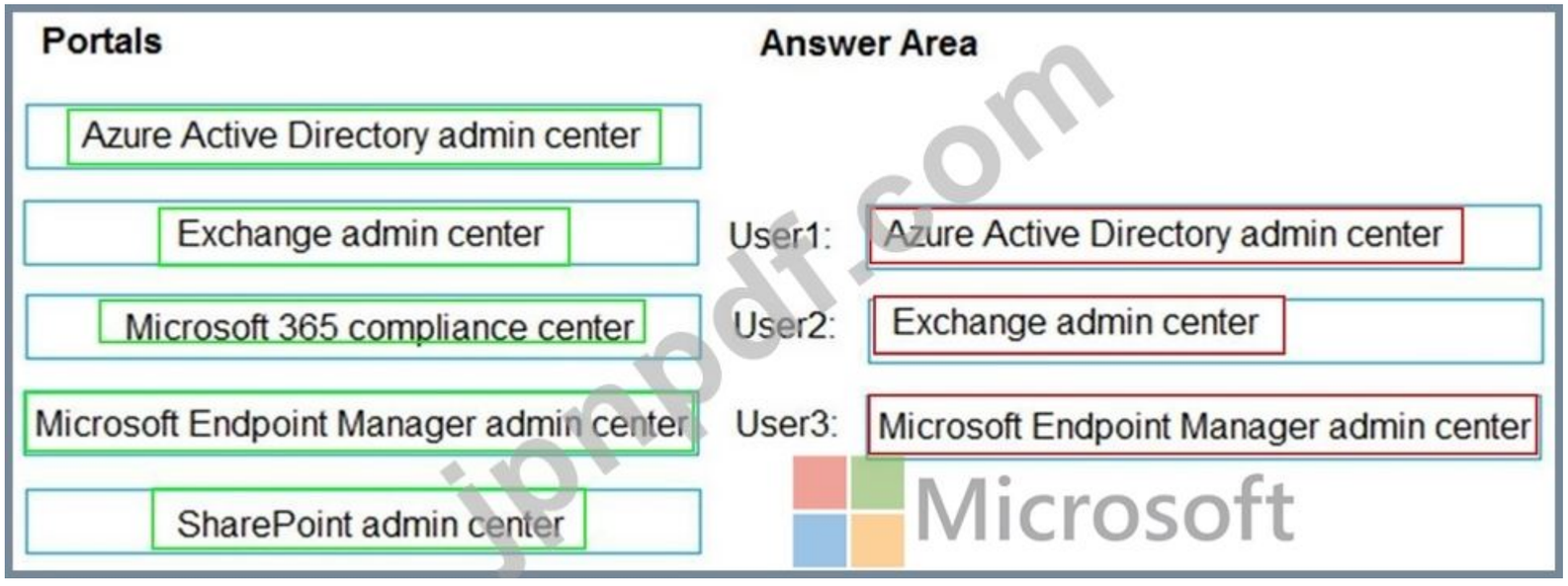
最新問題**: 255**
Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
次の表に示すようにユーザーを構成する必要があります。

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

各ユーザーを設定するにはどのポータルを使用すればよいでしょうか？適切なポータルを適切なユーザーにドラッグしてください。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



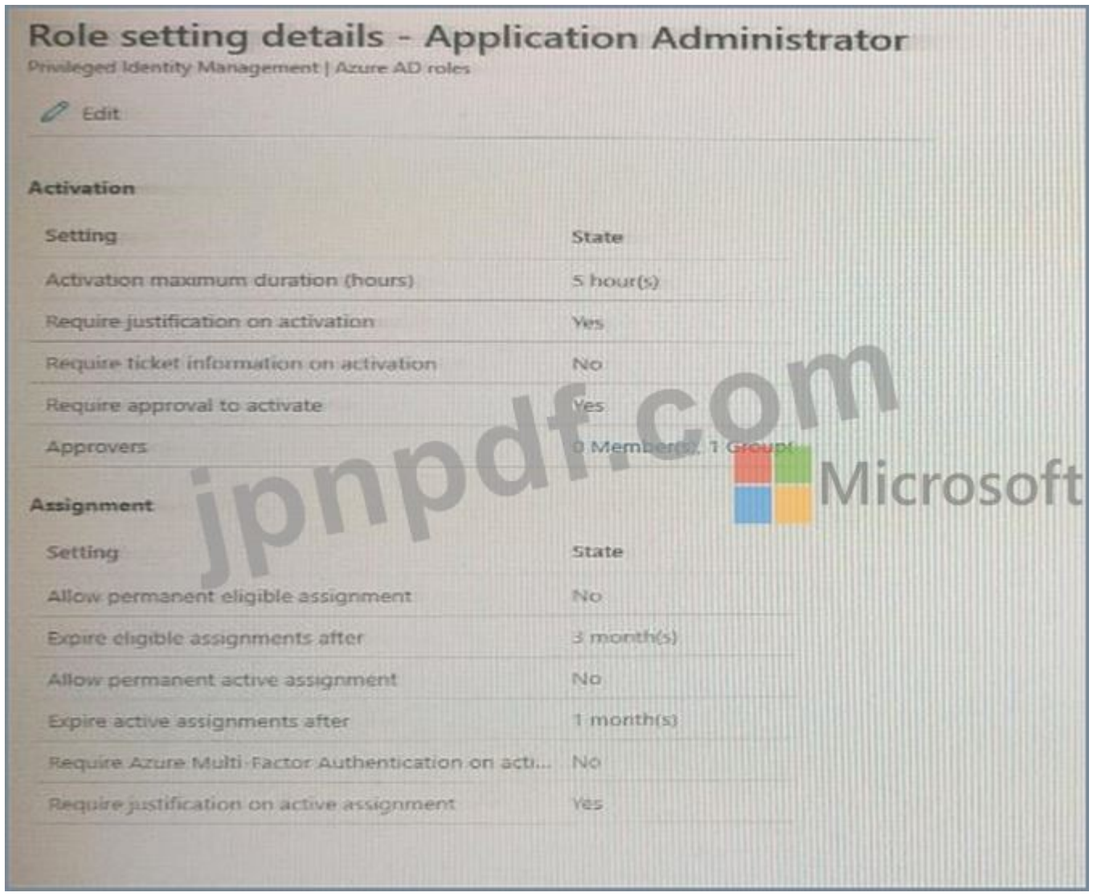
Answer:



最新問題: 256

Azure Active Directory (Azure AD) テナントに、User1、User2、User3 という 3 人のユーザーが含まれています。Group1 という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図に示されているように、Azure AD Privileged Identity Management (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ています。

User2 をアプリケーション管理者ロールの資格を持つように構成します。

User1 については、 割り当て」の図に示すように、アプリケーション管理者ロール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)



次の各文について、正しい場合は はい」を選択し、そうでない場合は いいえ」を選択します。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: 257

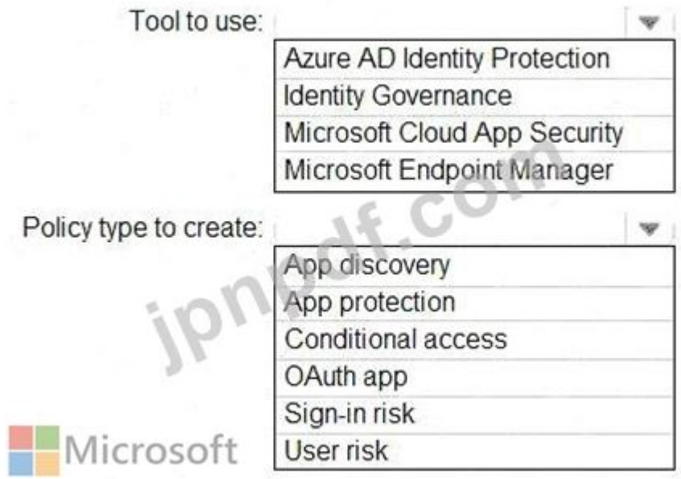
Microsoft 365 テナントがあります。

ユーザーは、Microsoft 365 データへの限定的なアクセスを必要とする外部のサードパーティ製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、これらの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権を取得した場合にアラートを受信する必要があります。

どうすればいいでしょうか? 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。

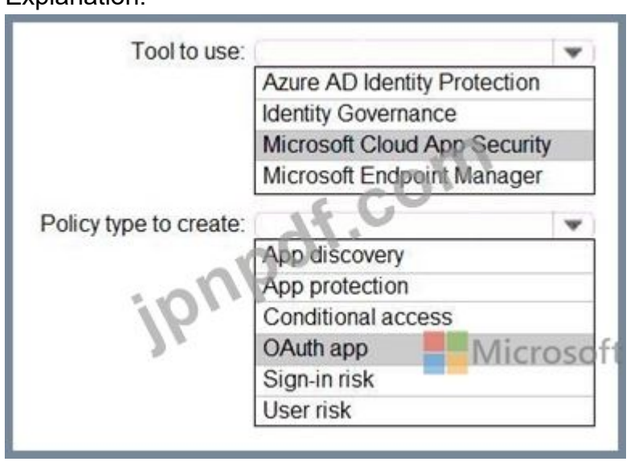
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



参照：

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

最新問題: **258**

次の表に示すホストを含むオンプレミス 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

Active Directory フォレストと同期する Azure Active 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 Azure AD ユーザーに公開できることを確認する必要があります。

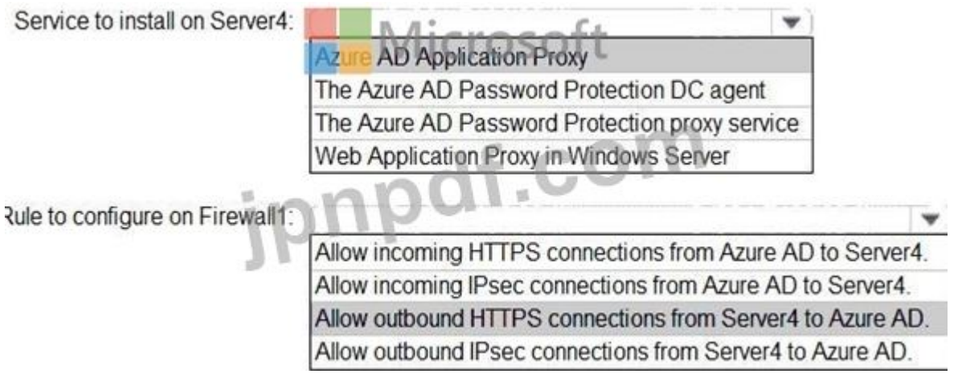
Server と Firewall1 で何を設定する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:





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

最新問題: 259
Sub1 という Azure サブスクリプションがあり、そこには RG1 と RG2 という 2 つのリソース グループが含まれています。Sub1 には、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Sub1 には、次の表に示すリソースが含まれています。

Name	Type	In resource group
VM1	Virtual machine	RG1
Vault1	Azure Key Vault	RG1
Vault2	Azure Key Vault	RG2

次の表に示すロールベースのアクセス制御 (RBAC) ロールの割り当てを作成します。

Role	Member of	Scope
Reader	Group1	Sub1
Key Vault Secrets User	Group2	RG2
Owner	Group3	RG1

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：正しい選択は1つにつき1点です。



Answer:
Explanation:



最新問題: **260**
Microsoft Entra 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. 見慣れないサインインプロパティ
B. パスワードスプレー
C. Microsoft Entra 脅威インテリジェンス
D. 匿名IPアドレス
Answer: C (メーッセージを残す**)**

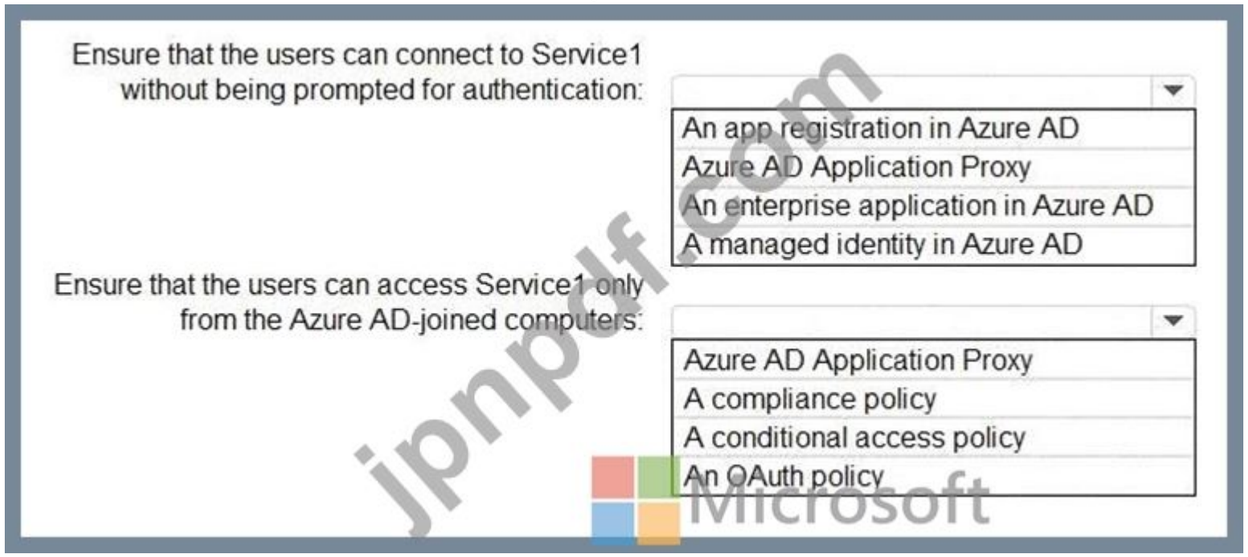
最新問題: **261**
Microsoft 365 E5 サブスクリプションがあり、そこには User1 と User2 という 2 人のユーザーが含まれています。
ユーザー1がグループのアクセスレビューを作成でき、ユーザー2が完了したすべてのアクセスレビューの履歴レポートを確認できることを確認する必要があります。このソリューションでは、最小権限の原則を適用する必要があります。
各ユーザーにどのロールを割り当てるべきですか？ 回答するには、適切なロールを正しいユーザーにドラッグしてください。各ロールは1回、複数回、または全く使用されない場合があります。コンテンツを表示するには、ペイン間の分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：正しい選択ごとに1ポイント獲得できます。



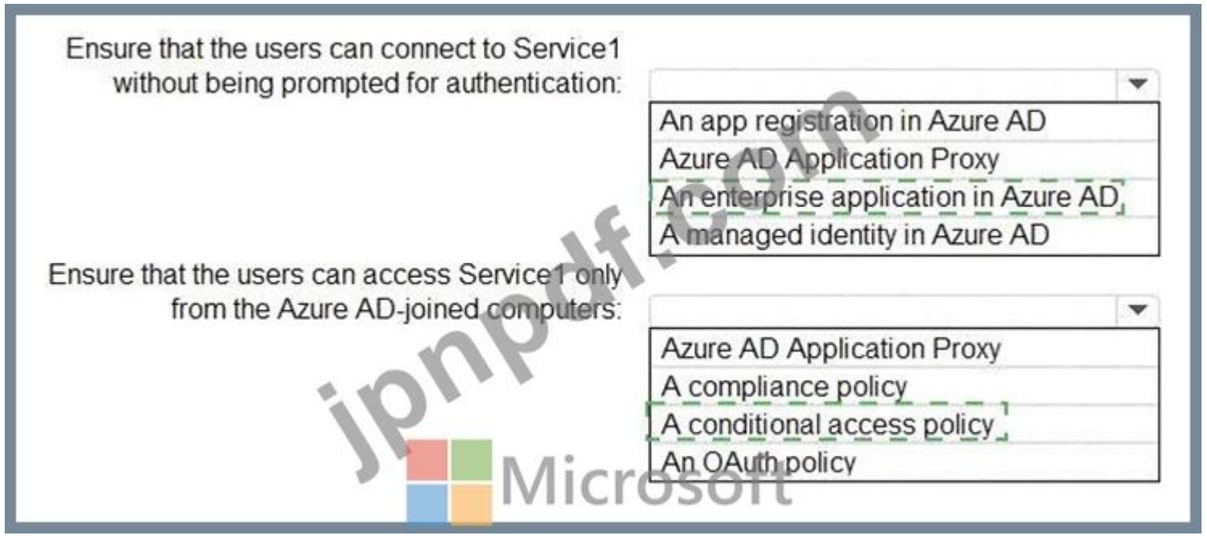
Answer:



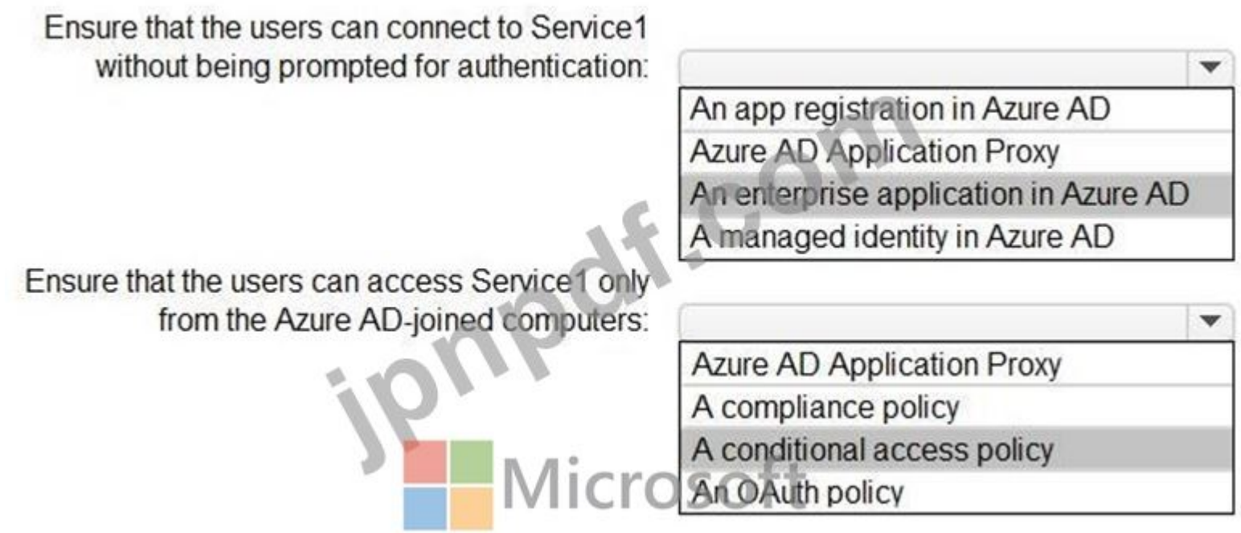
最新問題: **262**
会社には Microsoft 365 テナントがあります。
すべてのユーザーは、Windows 10 を実行し、Azure Active Directory (Azure AD) テナントに参加しているコンピューターを所有しています。
会社はService1というサードパーティのクラウドサービスに加入しています。Service1は、OAuthに基づくAzure AD認証と承認をサポートしています。Service1はAzure ADギャラリーに公開されています。
ユーザーが認証を求められることなくService1に接続できるようにするソリューションを推奨する必要があります。このソリューションでは、Azure ADに参加しているコンピューターからのみユーザーがService1にアクセスできるようにする必要があります。また、管理作業を最小限に抑える必要があります。
各要件に対して何を推奨しますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



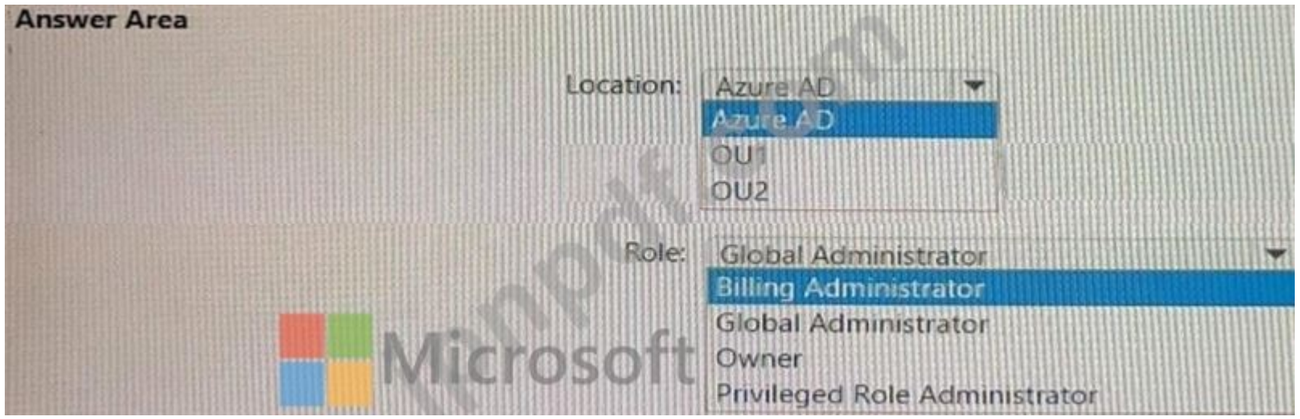
参照：
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices

最新問題**: 263**
ネットワークには、Azure AD 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 ドメインには、次の表に示す組織単位 (OU) が含まれています。

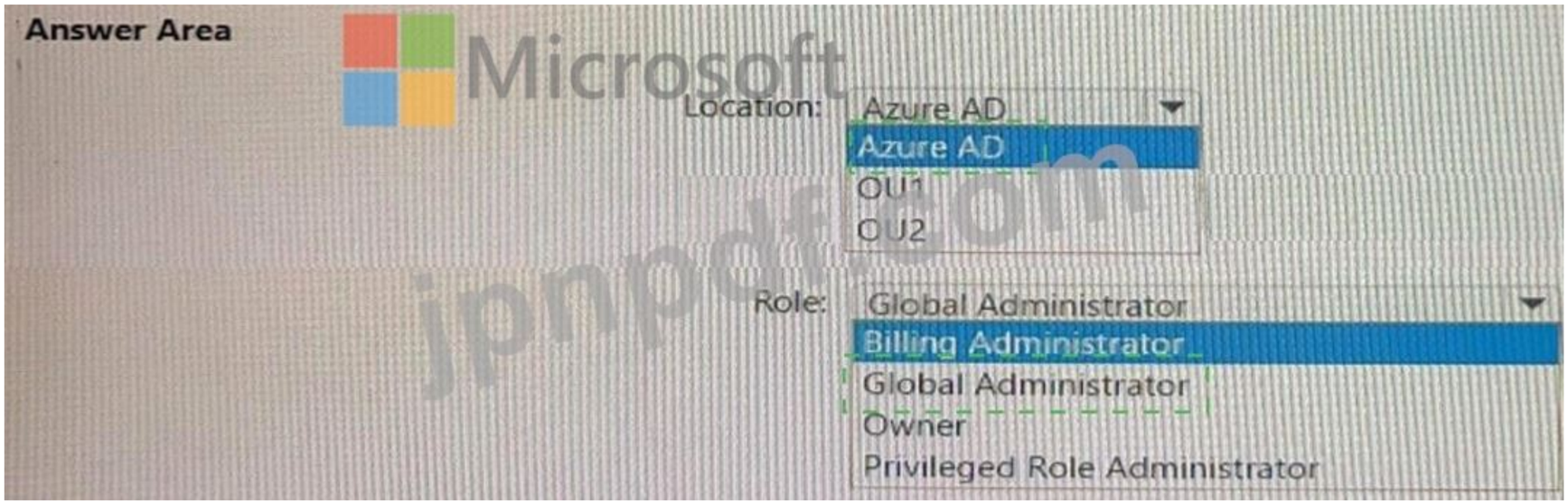
Name	Description
OU1	Syncs with Azure AD
OU2	Does **NOT** sync with Azure AD

BreakGlass という名前の Break-Glass アカウントを作成する必要があります。

BreakGlass はどこで作成し、BreakGlass にはどのようなロール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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

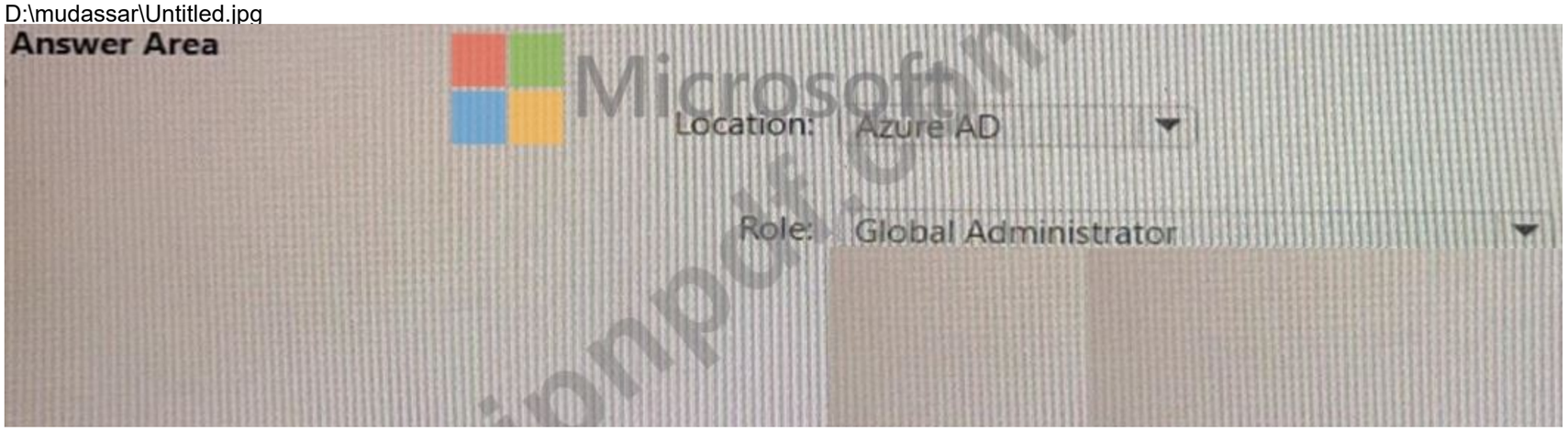


Answer:



説明

D:\mudassar\Untitled.jpg



最新問題: **264**

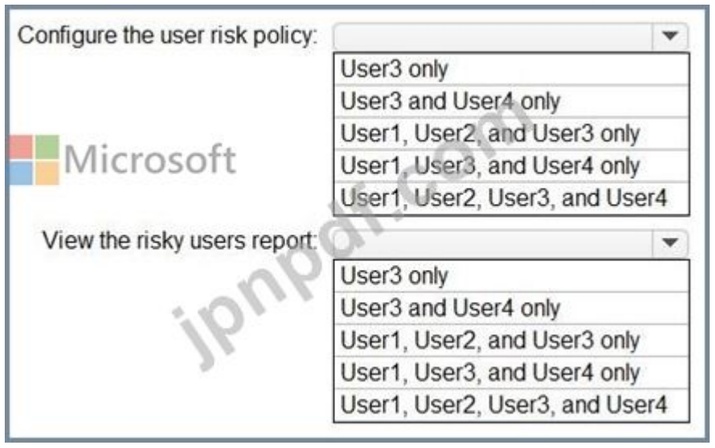
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD Identity Protection を実装する予定です。

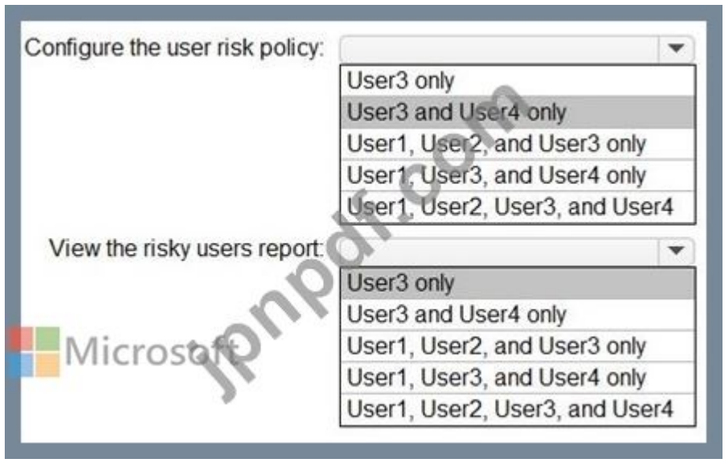
ユーザー リスク ポリシーを構成できるのはどのユーザーですか。また、リスクのあるユーザー レポートを表示できるのはどのユーザーですか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:





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

最新問題**: 265**
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、次の表に示すユーザーが含まれています。

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

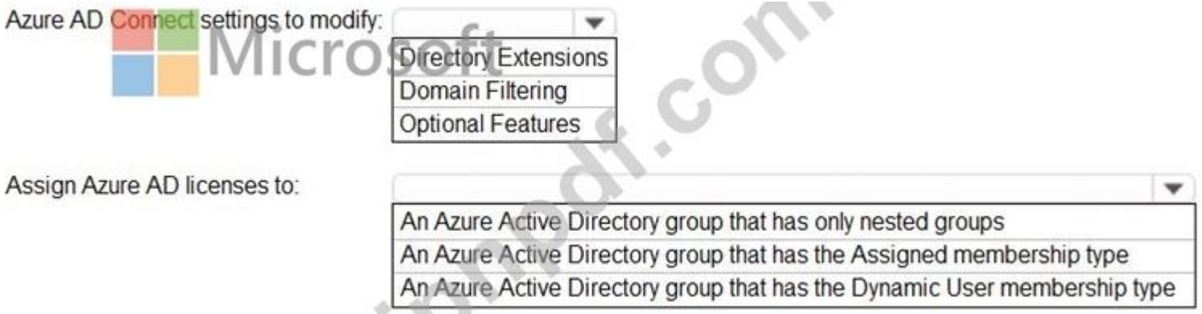
すべてのユーザーはリモートで作業します。
Azure AD Connect は、次の図に示すように Azure AD で構成されます。



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 Azure AD 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. ユーザー1のみ
C. ユーザー1、ユーザー2、ユーザー3
D. ユーザー1とユーザー2のみ
Answer: A (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/pta への接続方法 - 現在の制限

最新問題**: 266**
Litware ユーザーへの Azure AD ライセンスの割り当てを構成する必要があります。ソリューションはライセンス要件を満たしている必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題**: 267**
SSPR の計画された変更を実装します。
User3 が SSPR を使用しようとすると何が起こりますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

下記の説明の回答を参照してください。

Explanation:



最新問題**: 268**

ホットスポットに関する質問

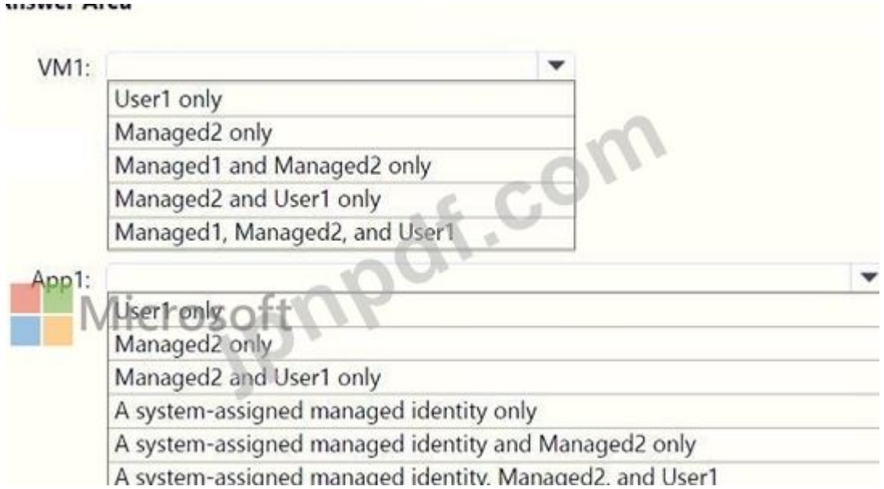
次の表に示すリソースを含む Azure サブスクリプションがあります。

Name	Type	Name	Type
VM1	Virtual machine	VM1	Virtual machine
App1	Azure App Service web app	App1	Azure App Service web app
Managed1	Managed identity	Managed1	Managed identity
Managed2	Managed identity	*Not applicable*	*Not applicable*

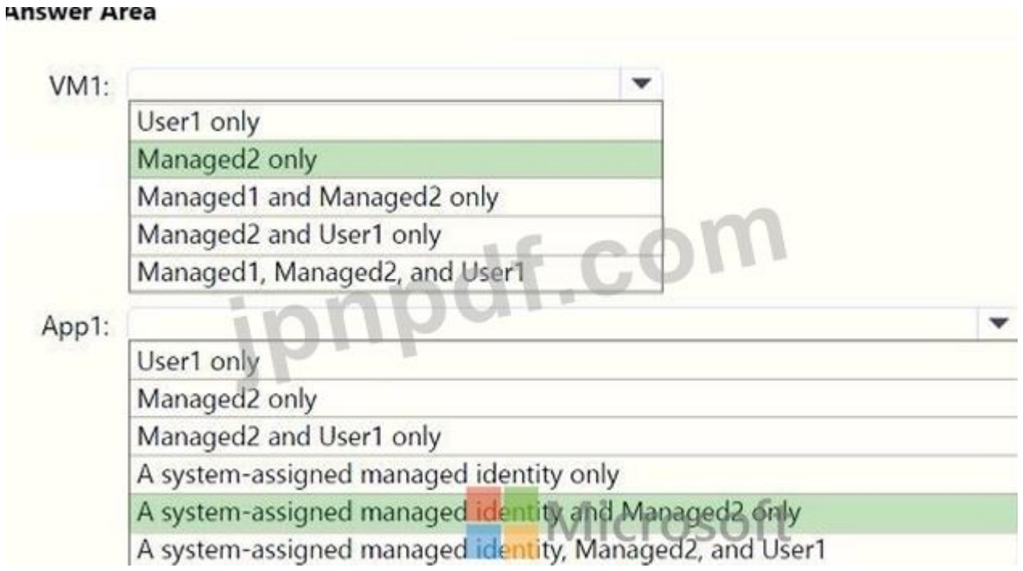
User1 という名前の Microsoft Entra ユーザーを作成します。

VM1 と App1 に追加できる ID はどれですか。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。

注意: 正解ごとに 1 ポイントが加算されます。



Answer:



最新問題: **269**

Microsoft Entra テナントがあります。

セルフサービス パスワード リセット (SSPR) は、次の設定で構成します。

* サインイン時にユーザー登録を要求する: はい
* リセットに必要な方法の数: 1

ユーザーが利用できる有効な認証方法は何ですか?

A. スマートカード

B. モバイルアプリのコード

C. FIDO2 セキュリティ トークン

D. Windows Hello PIN

Answer: (解答を表示する**)**

包括的かつ詳細な説明 :

Microsoft Identity and Access Administrator ドキュメントで概説されているように、Microsoft Entra ID セルフサービス パスワード リセット (SSPR) 設定と利用可能な認証方法に基づいて、これを段階的に説明してみましょう。
* Microsoft Entra ID のセルフサービス パスワード リセット (SSPR) について理解する:
* セルフサービス パスワード リセット (SSPR) を使用すると、ユーザーは管理者の介入なしにパスワードをリセットできるため、セキュリティが向上し、ヘルプデスクの作業負荷が軽減されます。
* 提供される設定は次のとおりです。
* サインイン時にユーザーの登録を要求する: はい - ユーザーは初めてサインインするときに認証方法 (電話番号、メール、セキュリティの質問など) を登録する必要があります。これにより、SSPR で使用できる方法が確保されます。
* リセットに必要な認証方法の数 :1 - ユーザーはパスワードをリセットするために、1つの認証方法を使用して本人確認を行う必要があります。これは必要な認証方法の最小数であり、ユーザーは少なくとも1つの認証方法を登録する必要があり、リセットプロセスではそのうちの1つの方法を使用します。
* SSPR で利用可能な認証方法:
* Microsoft Entra ID SSPR は、パスワードリセット時にユーザーが本人確認に使用できる特定の認証方法をサポートしています。これらの方法は、管理者が Microsoft Entra 管理センターの「パスワードリセット」設定で設定します。
* SSPR で使用できるデフォルトの認証方法は次のとおりです。
* メール: ユーザーは別のメールアドレスに送信されたコードを受け取ります。
* 携帯電話 (SMS): ユーザーは登録した携帯電話に SMS 経由でコードを受信します。
* モバイル アプリ コード: ユーザーは、Microsoft Authenticator アプリ (または互換性のある別の認証アプリ) によって生成されたコードを使用します。
* モバイル アプリ通知: ユーザーは、Microsoft Authenticator アプリでリセットを承認するためのプッシュ通知を受け取ります。
* セキュリティの質問: ユーザーは登録時に設定した定義済みのセキュリティの質問に答えます。
* 重要事項: スマートカード、FIDO2 セキュリティ トークン、Windows Hello などの認証方法は SSPR ではサポートされていません。これらの認証方法は通常、サインイン時の認証（MFA やパスワードレスサインインなど）に使用され、SSPR プロセスには使用されません。
* オプションの分析:
* A. スマートカード:
* スマートカードは、Windowsデバイスや VPNへのサインインによく使用される証明書ベースの認証方式です。物理カードとリーダーが必要で、通常はSSPRではなくプライマリ認証に使用されます。
* Microsoft Entra ID SSPR は、パスワードリセットの認証方法としてスマートカードをサポートしていません。SSPR の構成設定では、スマートカードは利用可能な方法として表示されません。
* 結論:これは誤りです。
* B. モバイルアプリコード:
* モバイル アプリ コードとは、Microsoft Authenticator アプリなどの認証アプリによって生成される時間ベースのワンタイム パスワード (TOTP) を指します。
* これは、Microsoft Entra ID の SSPR でサポートされている方法です。ユーザーは Microsoft Authenticator アプリ（または他の互換性のあるアプリ）を登録し、生成されたコードを使用してパスワードのリセット時に本人確認を行うことができます。
* 「リセットに必要な方法の数: 1」という設定は、必要な方法が 1 つだけであることを意味するため、ユーザーが登録している場合はモバイル アプリ コードが有効なオプションになります。
* 結論:これは正しいです。
* C. FIDO2 セキュリティ トークン:
* FIDO2 セキュリティ トークン（例:YubiKey）は、Microsoft Entra ID のパスワードレス認証をサポートするハードウェアベースのセキュリティキーです。Microsoft のパスワードレス認証戦略の一部であり、サインインに使用できます。
* ただし、FIDO2 セキュリティ トークンは SSPR ではサポートされていません。SSPR プロセスでは、メール、SMS、アプリベースのコードなど、よりシンプルでアクセスしやすい方法でリセットするように設計されているため、ユーザーは FIDO2 セキュリティキーを使用して本人確認を行うことができません。
* 結論:これは誤りです。
* D. Windows Hello PIN:
* Windows Hello PIN は、Windows デバイスへのサインインに使用されるデバイス固有の認証方法です。これは、生体認証（顔認証、指紋認証など）も含まれる Windows Hello の一部です。

* Windows Hello PINは、Microsoft Entra IDのSSPRではサポートされていません。SSPRプロセスはWebベースのポータル（例aka.ms/sspr）で実行され、Windows Helloのようなデバイス固有の認証方法とは統合されません。また、Windows Hello PINは特定のデバイスに関連付けられていますが、SSPRはデバイスに依存しないように設計されています。
* 結論:これは誤りです。
* 追加の考慮事項:
* 「サインイン時にユーザー登録を要求する :はい」という設定により、ユーザーは少なくとも1つの認証方法を登録していることが保証されます。ただし、この質問では管理者がどの方法を有効にしているかは指定されていません。Microsoft Entra IDでは、SSPRのデフォルトで有効な方法には、通常、メール、携帯電話 (SMS)、モバイルアプリコード、モバイルアプリ通知が含まれます。
セキュリティ上の懸念から、セキュリティの質問も有効にすることができますが、あまり一般的ではありません。
* 管理者が特定のメソッド（例モバイルアプリのコード）を無効にしている場合、回答は変更される可能性があります。ただし、質問にはそのような制限は記載されていないため、デフォルトのメソッドが利用可能であると想定しています。
* 「リセットに必要な方法の数 :1」設定は、ユーザーがパスワードをリセットするのに1つの方法だけを使用すればよいことを意味しますが、複数の方法を登録することもできます。質問は「ユーザーが利用できる有効な認証方法」であるため、SSPR がサポートする方法を特定する必要があります。
* 結論:SSPR 設定と Microsoft Entra ID でサポートされている認証方法に基づいて:
* モバイル アプリ コード (オプション B) は、デフォルトでサポートされており、構成と一致しているため、SSPR の有効な認証方法です。
* スマートカード、FIDO2 セキュリティ トークン、Windows Hello PIN は SSPR ではサポートされていません。
したがって正解はBです。
参考文献:
Microsoft Entra ID ドキュメント: 「セルフサービス パスワード リセット認証方法」(Microsoft Learn: https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#authentication- methods) Microsoft Entra ID ドキュメント: 「セルフサービス パスワード リセットを構成する」(Microsoft Learn:https://learn.
SSPR の構成とサポートされている認証方法について説明した Microsoft Identity and Access Administrator (SC-300) 試験学習ガイド (microsoft.com/en-us/entra/identity/authentication/howto-sspr-deployment)。

最新問題: **270**
シミュレーション
必要に応じて次のログイン資格情報を使用します。
ユーザー名を入力するには、「サインイン」ボックスにカーソルを置き、下のユーザー名をクリックします。
パスワードを入力するには、「パスワードを入力」ボックスにカーソルを置き、下のパスワードをクリックします。
Microsoft 365 ユーザー名:admin@XXYyz112233.onmicrosoft.com
Microsoft 365 パスワード: =1122334455667788
Microsoft 365 ポータルがブラウザーに正常に読み込まれない場合は、Ctrl キーを押しながら K キーを押して、新しいブラウザー タブにポータルを再度読み込みます。
以下の情報は技術サポートのみを目的としています。
ラボインスタンス: 99999999
次の要件を満たすようにグループ管理者ロールを構成する必要があります。
A. Allan Deyoung がロールをアクティブ化するリクエストを承認および拒否できることを確認します。
B. Christie Cline がロールのアクティブ化を要求できることを確認します。
C. 最小権限の原則を使用します。
D. このタスクを完了するには、適切な管理センターにサインインしてください。
Answer: A (メーッセージを残す**)**


Microsoft 365 portal approve and reject requests to activate the role

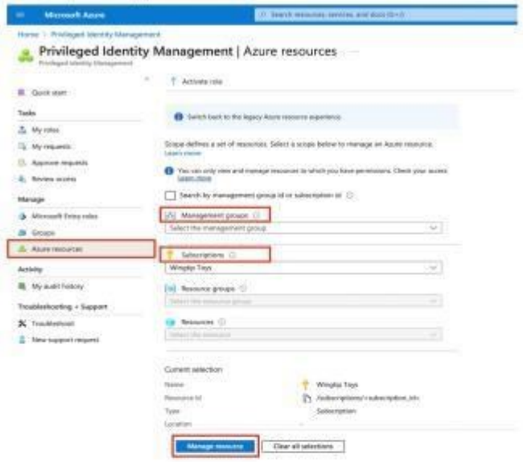
Note: Groups admin role in Azure Active Directory (Azure AD) is now generally available. This new Azure Active Directory role enables you to perform group management tasks for and Azure AD security groups without requiring Global administrator permissions.

Part 1: Ensure that Allan Deyoung can approve and reject requests to activate the role.
Assign a role
Follow these steps to make a user eligible for an Azure resource role.

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

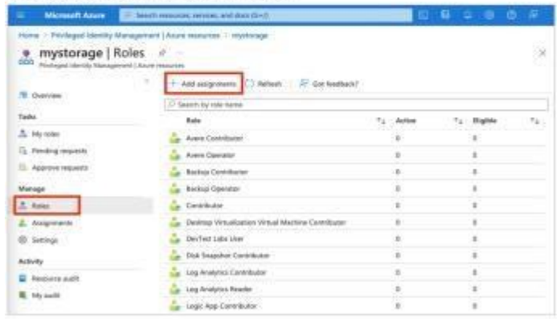
Step 2: Browse to Identity governance > Privileged Identity Management > Azure resources.

Step 3: Select the resource type you want to manage. Start at either the Management group dropdown or the Subscriptions dropdown, and then further select Resource groups or Resources as needed. Click the Select button for the resource you want to manage to open its overview page.



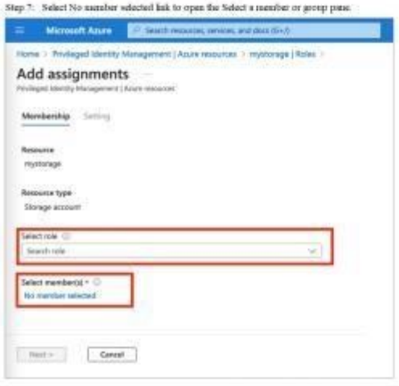
Step 4: Under Manage, select Roles to see the list of roles for Azure resources.

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

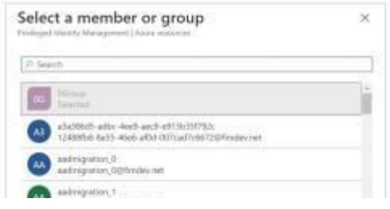


Step 6: Select a Role you want to assign. [Here: Select the Group Administrator role]

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

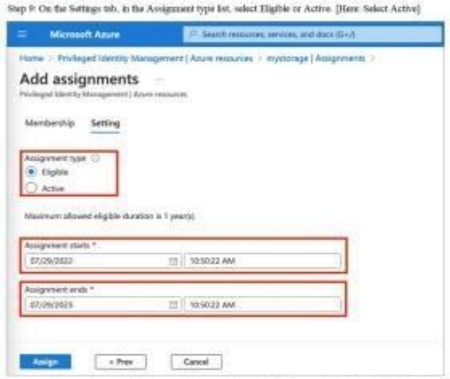


Step 8: Select a member or group you want to assign to the role and then choose Select. [Here: select Allan Deyoung]





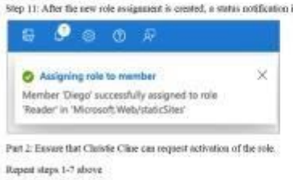
Step 9: On the Settings tab, in the Assignment type list, select Eligible or Active. [Here: Select Active]



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

Step 10: When finished, select Assign.

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



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

Repeat steps 1-7 above.

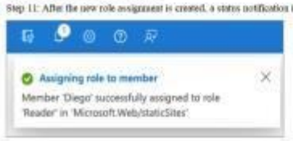
Step 8: Select a member or group you want to assign to the role and then choose Select. [Here: select Christie Cline]

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

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

Step 10: When finished, select Assign.

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



Reference:

https://techcommunity.microsoft.com/t5/microsoft-365-groups/introducing-the-groups-admin-role/m-p/973995

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

最新問題: **271**

既定のドメイン名 contoso.com を使用するように新しい Microsoft 365 テナントを構成します。

条件付きアクセス ポリシーを使用して、Microsoft 365 リソースへのアクセスを制御できることを確認する必要があります。

まず何をすべきでしょうか?

A. ユーザーの同意設定を無効にします。

B. セキュリティのデフォルトを無効にします。

C. 多要素認証 (MFA) 登録ポリシーを構成します。

D. Windows Server Active Directory のパスワード保護を構成します。

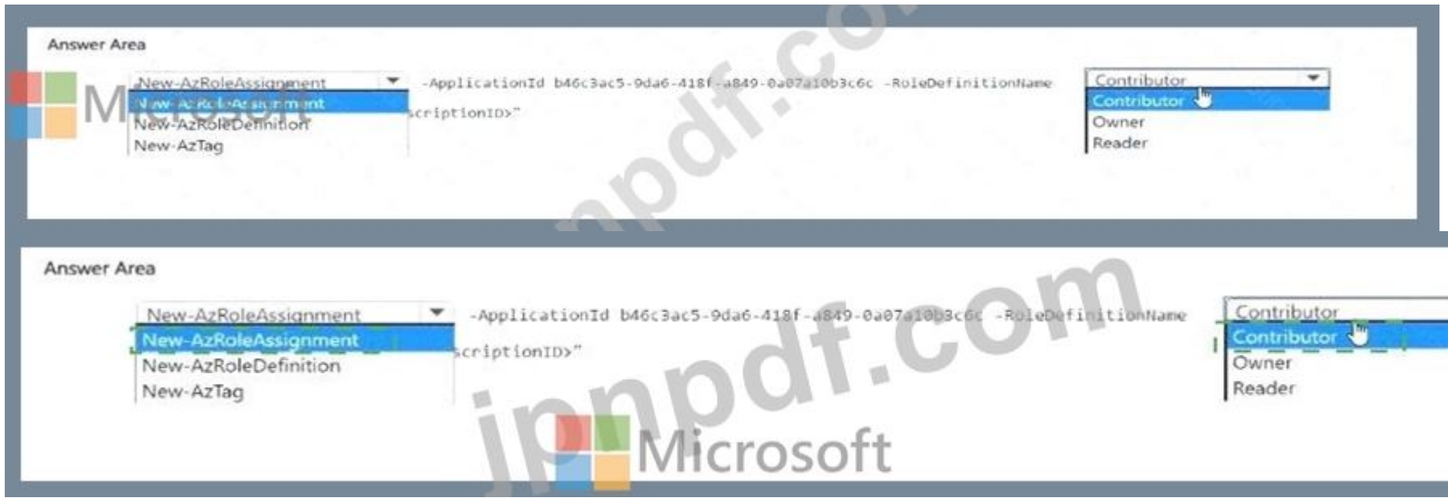
Answer: (解答を表示する**)**

2019年10月22日以降にテナントを作成された場合、セキュリティデフォルトが既に有効になっている可能性があります。すべてのユーザーを保護するため、新たに作成されるすべてのテナントにセキュリ

ティデフォルトが展開されます。
CAP を有効にするには、セキュリティのデフォルトを無効にする必要があります。
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals- セキュリティ デフォルト

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **272**
Sub1 という名前の Azure サブスクリプションがあります。
Microsoft Entra Permissions Management を展開する予定です。
権限管理がSub1にアクセスできることを確認する必要があります。ソリューションは最小権限の原則に従う必要があります。
PowerShell コマンド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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



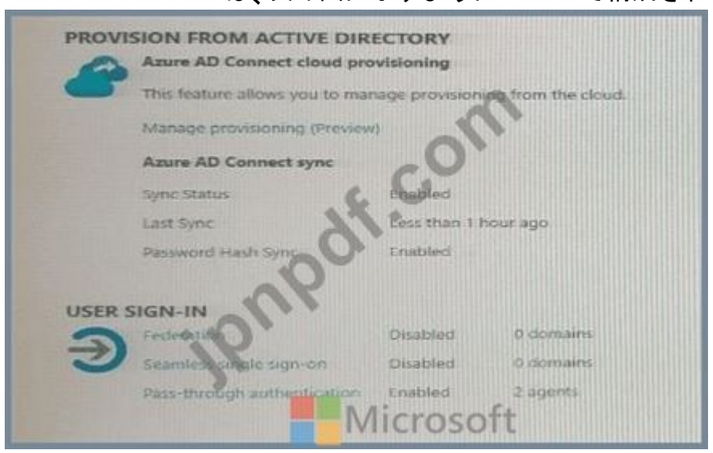
Explanation:



最新問題: **273**
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。
Azure AD Connect は、次の図に示すように Azure で構成されます。



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 Azure AD にサインインできますか?
A. ユーザー1のみ
B. ユーザー1とユーザー3のみ
C. ユーザー1、ユーザー2、ユーザー3
D. ユーザー1とユーザー2のみ
Answer: B (メーッセージを残す)

最新問題: **274**
RG1というリソースグループと、User1、User2、User3、User4という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。RG1に対して、これらのユーザーに以下のロールを割り当てる予定です。
* ユーザー1: 読者
* ユーザー2: 貢献者
* ユーザー3: ストレージBLOBデータリーダー
* ユーザー4: 仮想マシン コントリビューター
属性ベースアクセス制御 (ABAC)の使用を検討しています。ABACの使用をサポートするユーザーロールはどれですか？
A. ユーザー1
B. ユーザー2
C. ユーザー3
D. ユーザー4
Answer: C (メーッセージを残す)
Azure の属性ベースのアクセス制御 (ABAC) は、ユーザー、リソース、または環境の属性に基づいて条件を追加することで、ロールベースのアクセス制御 (RBAC) を強化します。
現在、ABAC は、ストレージ BLOB データ リーダー、ストレージ BLOB データ コントリビューター、ストレージ BLOB データ オーナーなどの適切なデータ プレーン ロールで使用される場合にのみ、Azure Storage (BLOB およびキュー) でサポートされます。
シナリオでは :

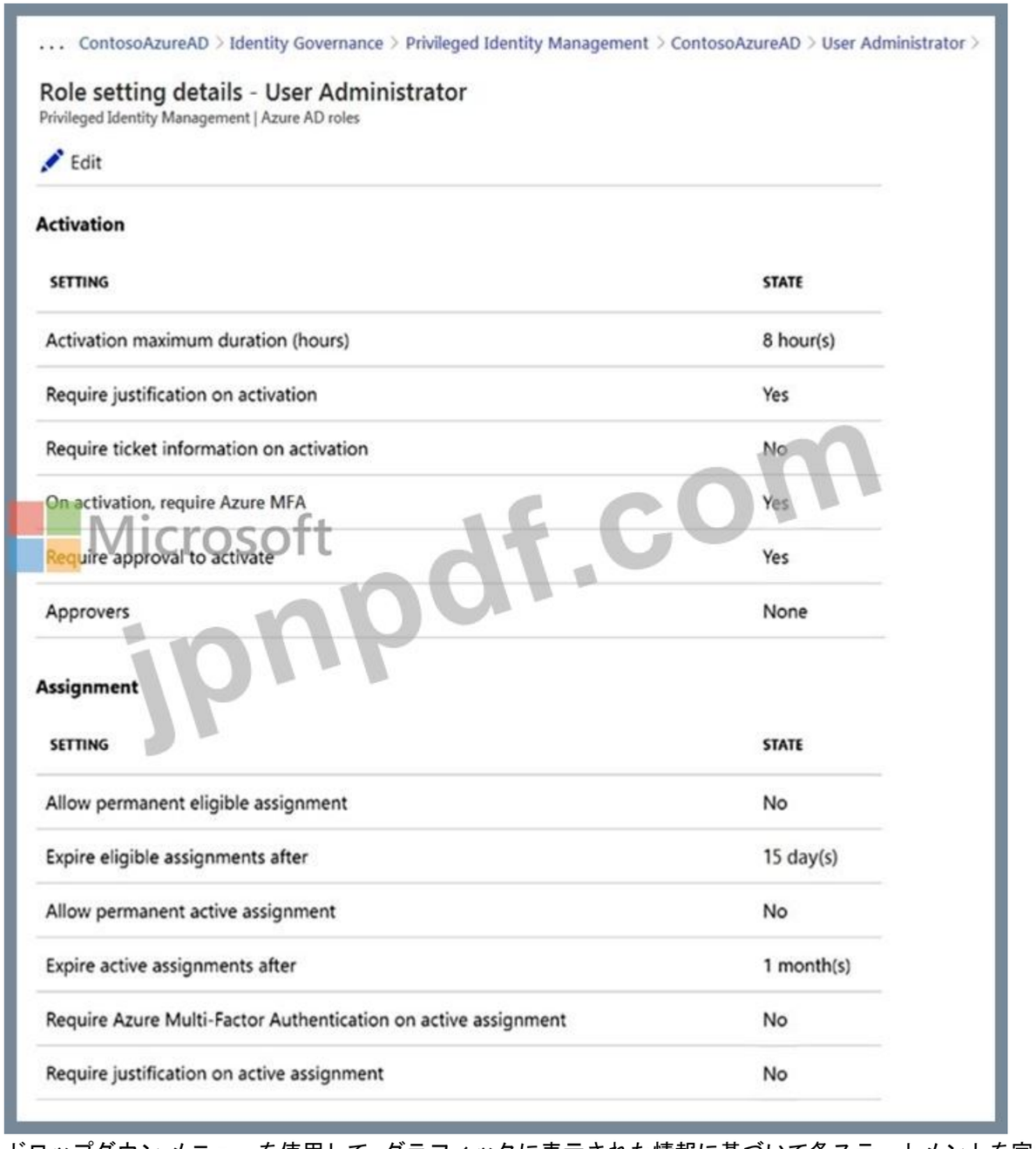
* User1 (リーダー) と User2 (コントリビューター) には、ABAC でサポートされているデータ ロールではなく、管理プレーン ロールが割り当てられています。
* User3 (ストレージ BLOB データ リーダー) には、ABAC をサポートするデータ プレーン ロールが割り当てられています。
* User4 (仮想マシン コントリビューター) にも管理プレーンのロールがあります。
したがって、User3 のロールだけが ABAC をサポートします。
Microsoft のドキュメントでは次のことが確認されています:
「ストレージ BLOB データ閲覧者や共同作成者などの Azure RBAC ロールを使用する場合、現在 Azure Storage で ABAC がサポートされています。ABAC では、きめ細かなアクセスのためにユーザーまたはリソース属性に条件を設定できます。」

最新問題: **275**
次のオブジェクトを含む Azure Active Directory (Azure AD) テナントがあります。
- Device1という名前のデバイス
- User1、User2、User3、User4、User5 という名前のユーザー
- Group1、Group2、Group3、Group4、Group5という名前のグループ
グループは次の表のように構成されます。

Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group3
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	User4
Group5	Microsoft 365	Dynamic User	User5

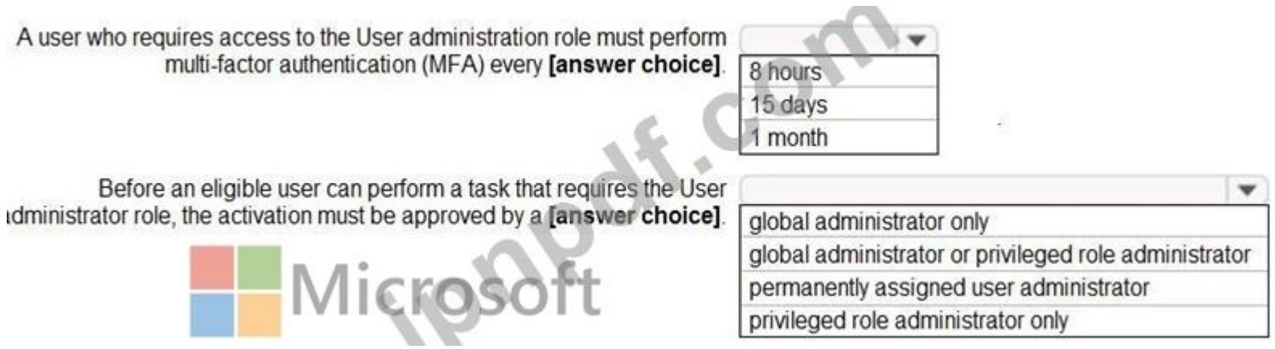
Microsoft Office 365 Enterprise E5 ライセンスを直接割り当てることができるのはどのグループですか?
A. グループ1とグループ4のみ
C. グループ1とグループ2のみ
B. グループ1、グループ2、グループ3、グループ4、およびグループ5
D. グループ1のみ
E. グループ1、グループ2、グループ4、グループ5のみ
Answer: C (メーッセージを残す**)**
グループ3はデバイスグループであるため、ライセンスを割り当てることはできません。デバイスグループにライセンスを割り当てることはできません。
グループ 4 とグループ 5 にライセンスを割り当てることはできません。Microsoft 365 グループにライセンスを割り当てることはできません。
https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group- advanced

最新問題: **276**
次の図に示すように、ユーザー管理者ロールの Azure AD Privileged Identity Management (PIM) ロール設定を含む Azure Active Directory (Azure AD) テナントがあります。

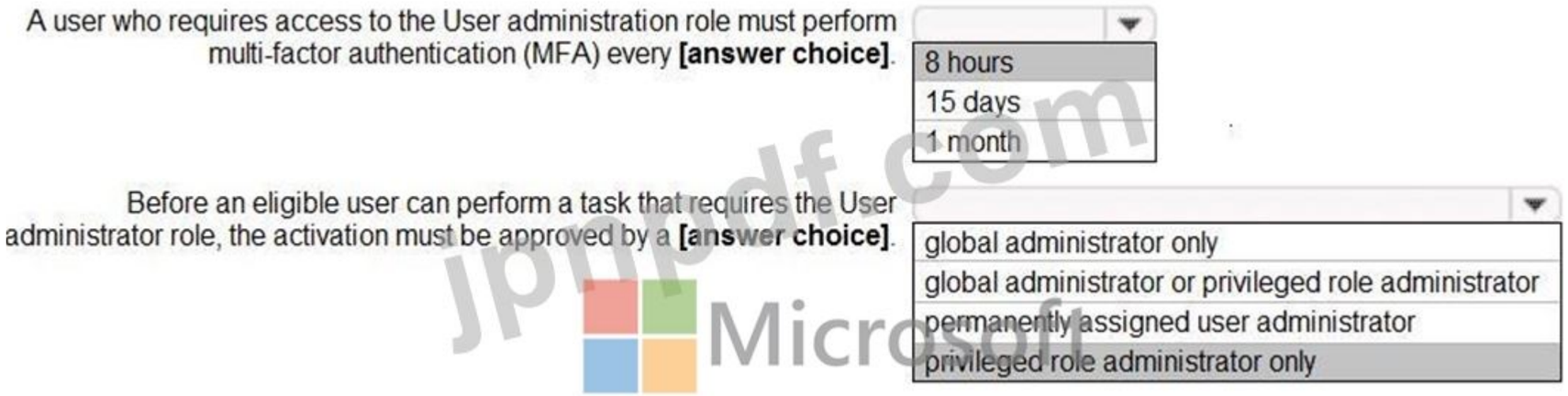


Microsoft
jpnpdf.com

ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。

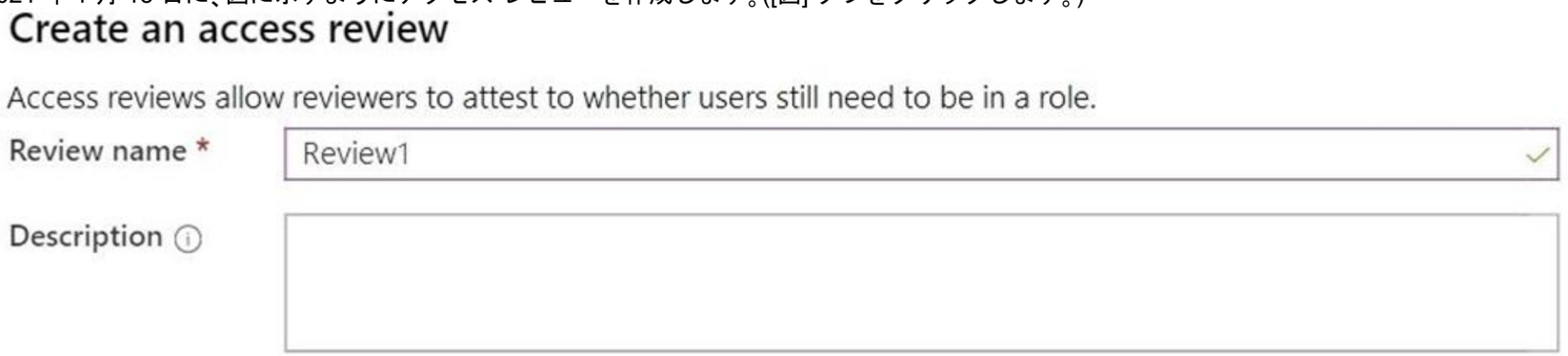


Answer:



参照：
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**: 277**
次のグループを含む Azure Active Directory (Azure AD) テナントがあります。
名前: グループ1
メンバー: ユーザー1、ユーザー2
所有者: ユーザー3
2021 年 1 月 15 日に、図に示すようにアクセス レビューを作成します。([図] タブをクリックします。)



Start date * 01/15/2021

Frequency Monthly

Duration (in days) 14

End Never | End by | Occurrences

Number of times 0

End date * 02/15/2021

Users

Users to review Members of a group

Scope
- Guest users only
- Everyone

Group *
Group1

Reviewers

Reviewers Members (self)

Programs

Link to program
Default Business Flow

Upon completion settings

Microsoft
jpnpdf.com



ユーザーは、次の表に示すように Review1 の質問に回答します。

User	Date	Do you still need access to Group1?
User1	January 17, 2021	Yes
User2	January 20, 2021	No

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 ポイントが加算されます。

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

Answer:

Statements	Yes	No
On February 5, 2021, User1 can answer the Review1 question again.	○	○
On January 25, 2021, User2 can answer the Review1 question again.	○	○
On January 22, 2021, User3 can answer the Review1 question.	○	○

参照：

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

最新問題**: 278**

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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。

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。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 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 Microsoft Authenticator アプリを使用する必要があります。
一部のユーザーから、サインイン要求を開始せずに Microsoft Authenticator アプリで MFA プロンプトを受け取ったという報告があります。
ユーザーが開始していない MFA リクエストを報告した場合は、その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)
Azure AD MFA 構成に関する SC-300 資料では、Microsoft は通知（Microsoft Authenticator がプッシュ通知を送信するかどうかを制御）と不正行為アラート設定（ユーザーが予期しない通知を報告した場合の動作を決定）を区別しています。学習ガイドでは、通知によって「アプリへのプッシュ承認が可能になる」と説明されていますが、ユーザーが疑わしい通知を報告した場合には、通知はアクションを実行しません。「ユーザーが開始していない MFA リクエストを報告した場合に、自動的にユーザーをブロックする」という要件を満たすには、不正行為アラートオプションを使用する必要があります。資料には、管理者は「ユーザーが不正行為アラートを送信できるようにする」と「不正行為を報告したユーザーをブロックする」ことで、「報告されたアカウントは管理者がブロックを解除するまで直ちにブロックされる」と記載されています。これらのオプションは、テナントの MFA サービス設定の一部であり、通知セクションではありません。つまり、通知を設定するだけでは、Microsoft Authenticator で「報告」をタップしたユーザーを自動的にブロックすることはできません。不正行為が報告された際にユーザーをブロックするには、設定を明示的に有効にする必要があります。したがって、提案されているソリューション（通知設定を変更する）は目的を達成しません。正しい方法は、不正行為の警告を有効にし、不正行為を報告するユーザーをブロックするを選択して、ユーザーが予期しない MFA プロンプトを報告したときに自動保護を確実にすることです。

最新問題: **279**
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 Azure Active 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

グループAとグループBに追加できるメンバーは誰ですか？ 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

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:

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

Explanation:

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

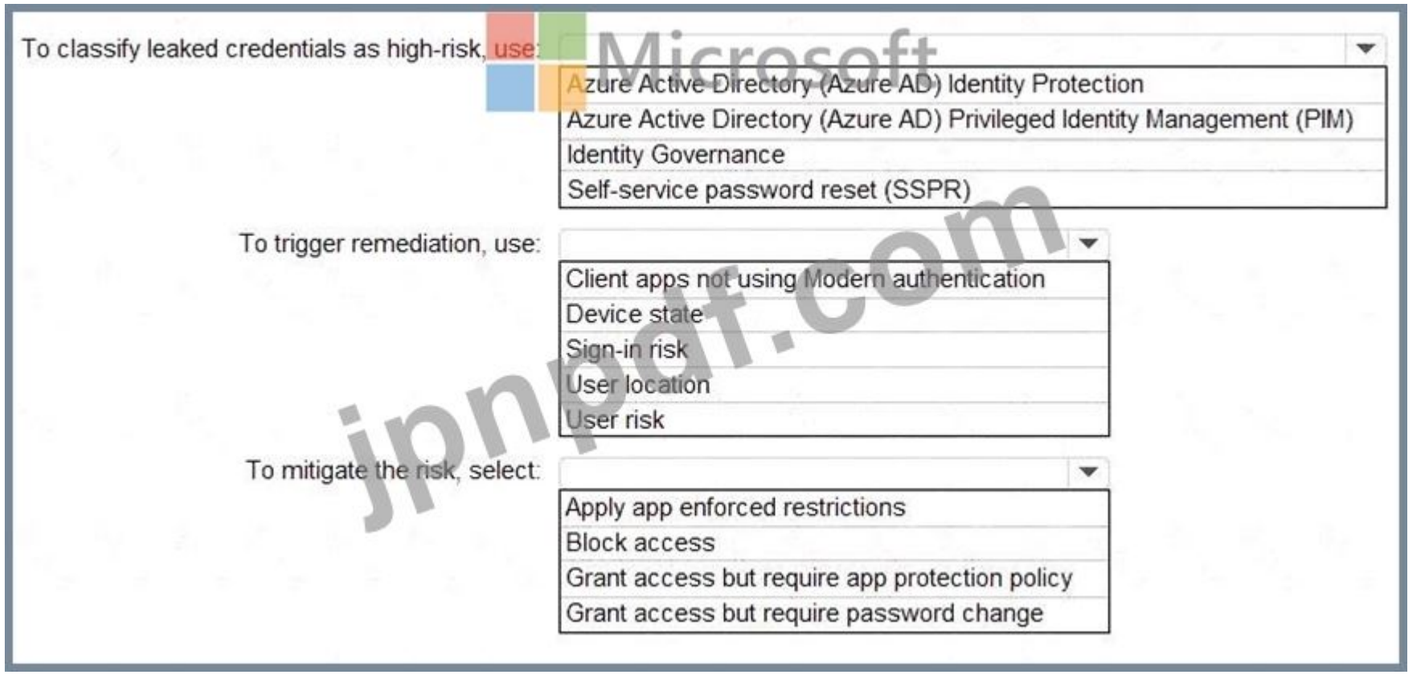
参照：
https://bitsizedbytes.wordpress.com/2018/12/10/distribution-security-and-office-365-groups-nesting/

最新問題**: 280**
Microsoft 365 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。

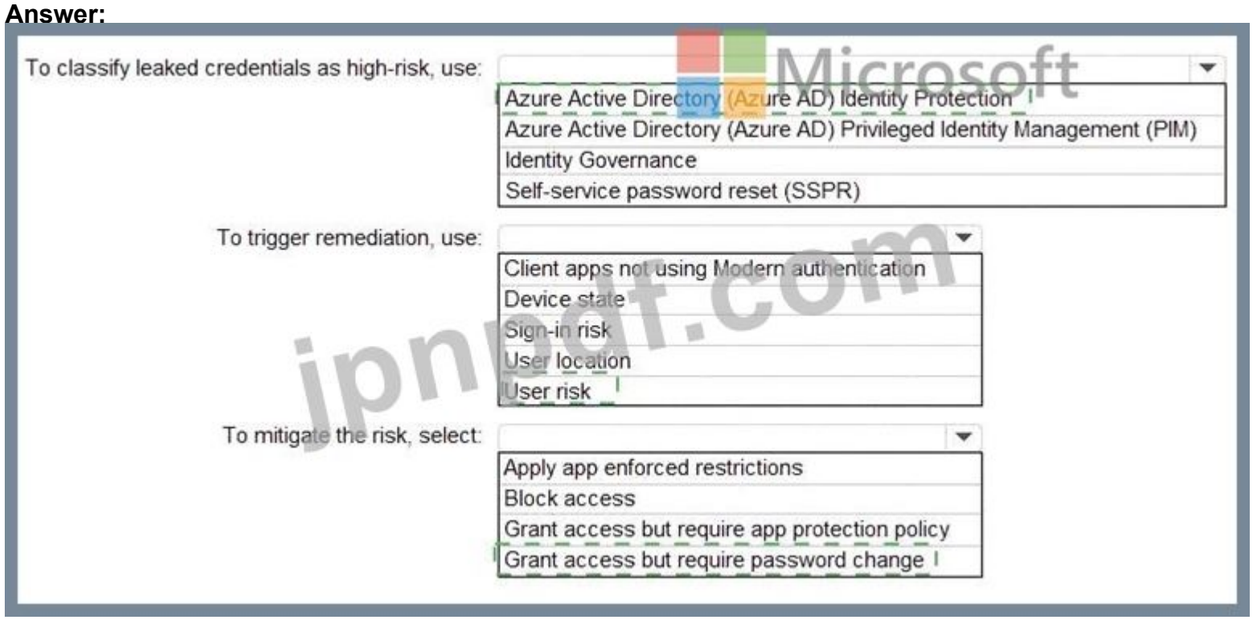
Name	Type
Group1	Security
Group2	Distribution
Group3	Microsoft 365
Group4	Mail-enabled security

Azure AD で、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何ですか?
A. グループ3のみ
B. グループ1のみ
C. グループ1とグループ4
D. グループ1とグループ
E. グループ2のみ
Answer: D (メーッセージを残す**)**

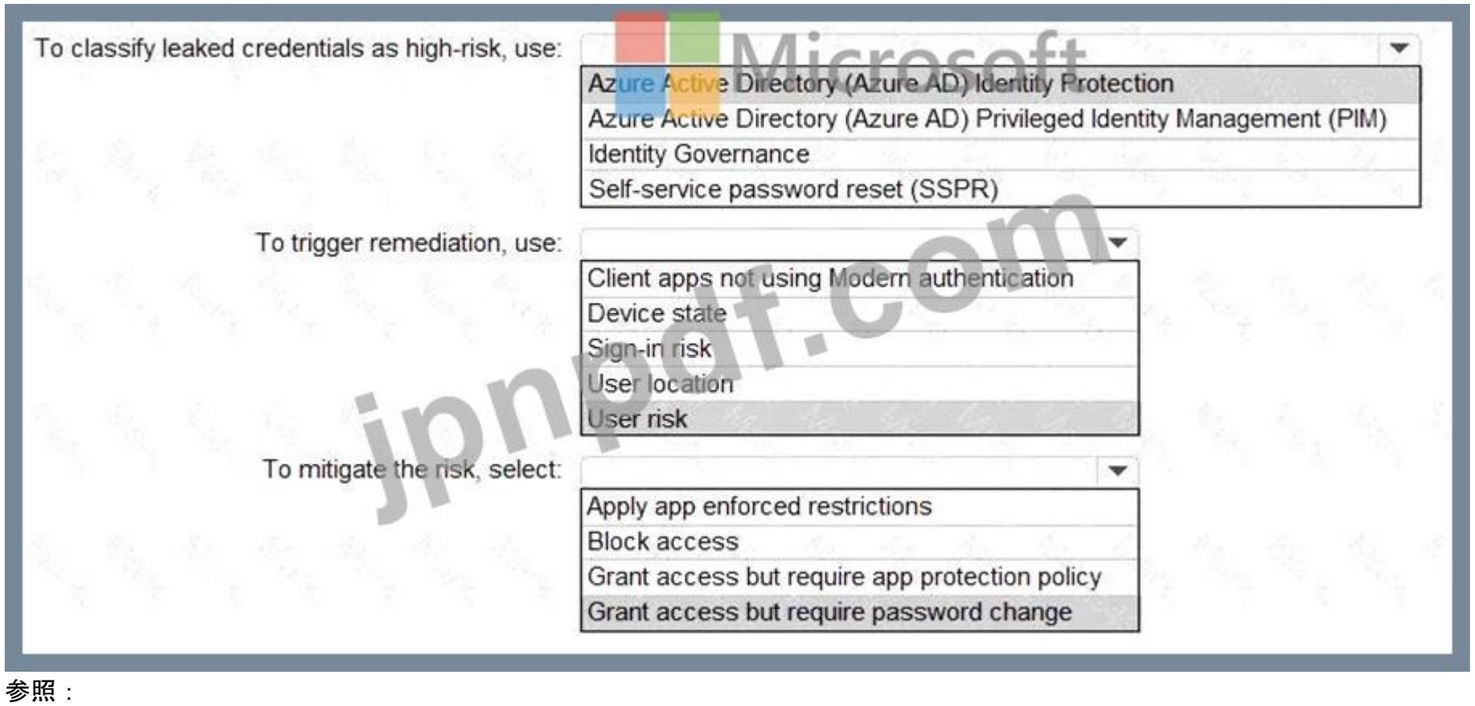
最新問題**: 281**
Microsoft 365 テナントがあります。
資格情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。
* 資格情報が漏洩した疑いのあるユーザーによる ID サインイン。
* サインインを高リスクイベントとして禁止します。
* ユーザーがアプリケーションにアクセスできるようにしながら、リスクを軽減するための制御を直ちに実施します。
何を使うべきでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



参照：

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

最新問題: 282

User1 という名前のユーザーを含む contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

User1 には次の表に示すデバイスがあります。

2020 年 11 月 5 日に、contoso.com で次の設定の利用規約を作成して適用します。

名前: 用語1

表示名: Contoso 利用規約

ユーザーに利用規約の拡張を要求する: オン

すべてのデバイスでユーザーの同意を求める: オン

同意の有効期限: オン

有効期限: 2020年12月10日

頻度: 毎月

2020年11月15日に、ユーザー1はデバイス3で利用規約1に同意します。

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 ポイントが加算されます。

Answer:

2020年11月16日 デバイス1: はい

2020年12月15日のデバイス3: はい

2020年11月20日 デバイス3: いいえ

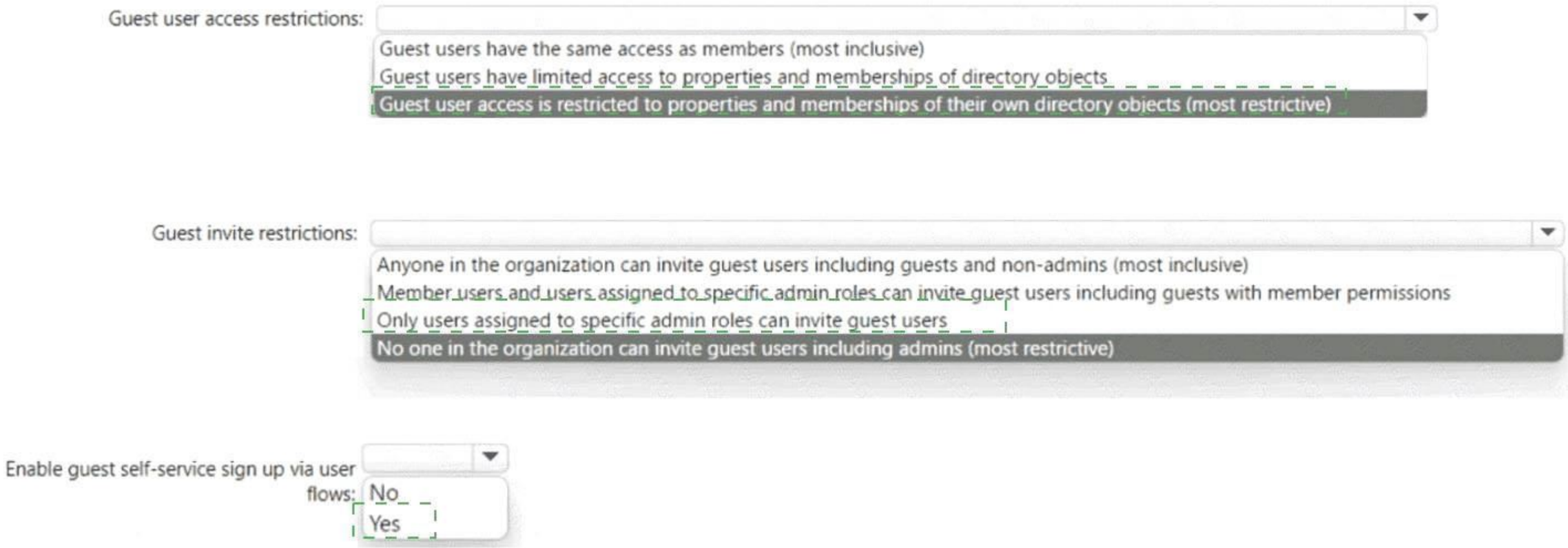
Microsoft の公式ドキュメントと SC-300: Identity and Access Administrator 学習ガイド (アイデンティティ ガバナンスとコンプライアンスのセクション) によると、Azure Active Directory の利用規約 (ToU) は条件付きアクセス ポリシーに基づいて管理され、リソースへのアクセスを許可する前にユーザーの承認が強制されます。

シナリオからの主要な構成設定:
* ユーザーに利用規約の拡張を要求する: オン # ユーザーは同意する前にドキュメントを開く必要があります。
* すべてのデバイスでユーザーの同意を要求する: オン # デバイスごとに個別の承認が必要です (同意はデバイスごとに保存されます)。
* 同意の有効期限: オン
* 有効期限 :2020年12月10日
* 頻度: 毎月 # ユーザーは最初の同意後、毎月利用規約に再度同意する必要があります。
とすれば :
*Terms1は2020年11月5日に作成されました。
* ユーザー1は、2020年11月15日にデバイス3でのみ利用規約に同意しました。
* 承認はデバイスごとに行われます。つまり、デバイス 1 とデバイス 2 ではまだ承認が記録されていません。
したがって :
* 2020年11月16日（翌日）ユーザー1がデバイス1からサインインするときに、利用規約1に同意する必要があります。# はい。
* 規約は 2020 年 12 月 10 日から毎月期限切れになるため、2020 年 12 月 15 日までに、ユーザー 1 はデバイス 3 で規約に再度同意する必要があります。# はい。
* 2020 年 11 月 20 日は、最初の承認 (11 月 15 日) と同じ月内であり、まだ期間が終了していません。# いいえ、すぐに再承認する必要はありません。
これは Microsoft のドキュメントの抜粋と一致しています:
「すべてのデバイスでユーザーの同意を要求する」を有効にすると、各デバイスへのサインインごとに個別の同意が必要になります。有効期限が設定されている場合、ユーザーは指定された日付から定義された頻度に基づいて利用規約に再度同意する必要があります。

最新問題**: 283**
User1 という名前のユーザーを含む Azure AD テナントがあります。User1 には、ユーザー管理者ロールが割り当てられています。
次の要件を満たすように、テナントの外部コラボレーション設定を構成する必要があります。|
*ゲスト ユーザーがスタッフの電子メール アドレスを照会できないようにする必要があります。
*ゲスト ユーザーは、User1 によって招待された場合にのみテナントにアクセスできる必要があります。
どの 3 つの設定を構成する必要がありますか? 回答するには、回答領域で適切な設定を選択してください。


Guest user access restrictions:
Guest users have the same access as members (most inclusive)
Guest users have limited access to properties and memberships of directory objects
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)
Guest invite restrictions:
Anyone in the organization can invite guest users including guests and non-admins (most inclusive)
Member users and users assigned to specific admin roles can invite guest users including guests with member permissions
Only users assigned to specific admin roles can invite guest users
No one in the organization can invite guest users including admins (most restrictive)
nable guest self-service sign up via user
flows: No
Yes

Answer:



Explanation:
Box1 = ユーザーアクセスは、自身のディレクトリオブジェクトのプロパティとメンバーシップに制限されます（最も制限が厳しい）。この設定により、ゲストユーザーはスタッフのメールアドレスを照会できず、User1 から招待された場合にのみテナントにアクセスできます。
Box2 = 特定の管理者ロールに割り当てられたユーザーのみがゲストユーザーを招待できます。この設定により、ゲストユーザーはUser1から招待された場合にのみテナントにアクセスできるようになります。
Box3 = この設定により、ゲスト ユーザーは、User1 から招待された場合にのみテナントにサインアップできるようになります。

最新問題**: 284**
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。
最初に何を作成し、どのツールを使用すればよいですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **285**

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
VM1	Virtual machine
App1	Azure App Service web app
Managed1	Managed identity
Managed2	Managed identity

User1 という名前の Microsoft Entra ユーザーを作成します。

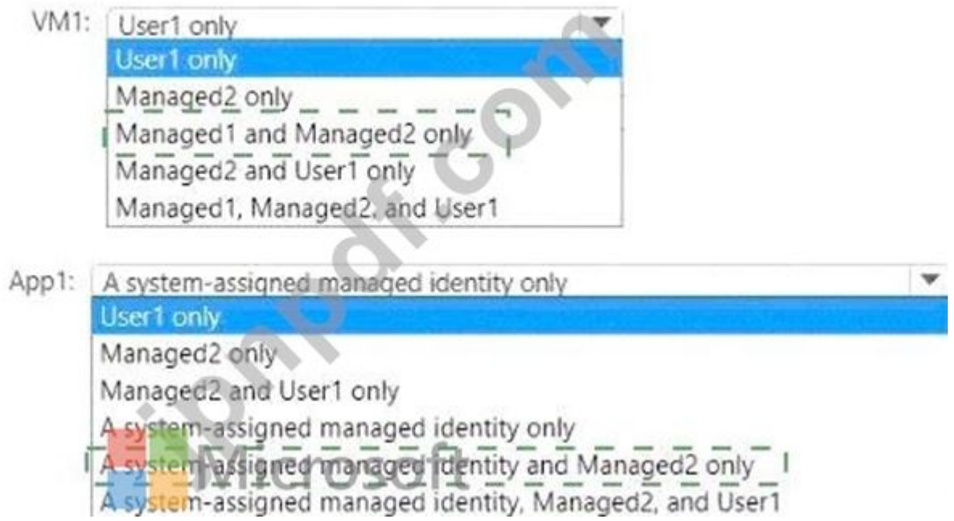
VM1 と App1 に追加できる ID はどれですか。回答するには、回答領域で適切なオプションを選択してください。

注意: 正解ごとに 1 ポイントが加算されます。



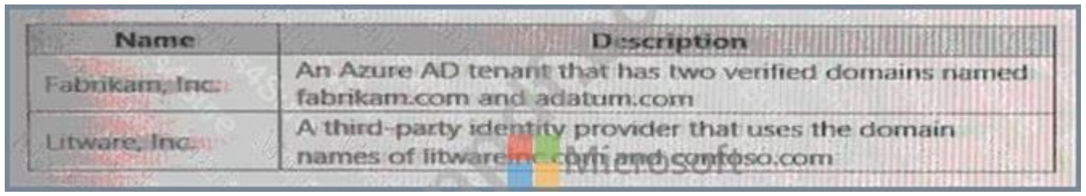
Answer:

Answer Area



Explanation:
VM1: Managed1 と Managed2 のみ
App1: システム割り当てマネージド ID と Managed2 のみ

最新問題: 286
あなたの会社には、contosri.com という Azure Active Directory (Azure AD) テナントがあり、次の表に示すビジネス パートナーが存在します。



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 litware.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リクエストできます。
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。
Fabrikam および litware の接続された組織を構成して、その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する必要があります。
作成する必要がある最小限の接続組織は何ですか。
A. 2
B. 1
C. 4
D. 3
Answer: (解答を表示する**)**

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **287**
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

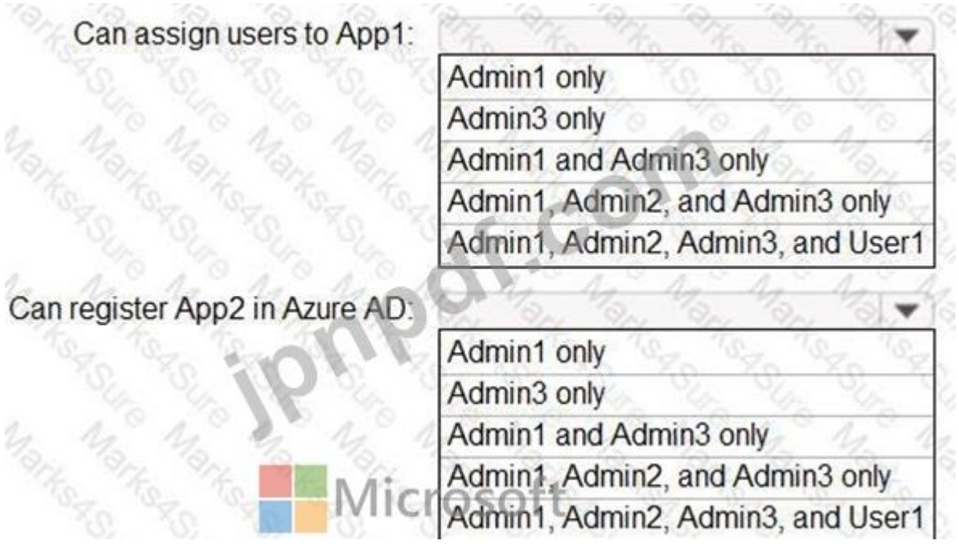
どのリソースに対してアクセス レビューを作成できますか?
A. Group1、App1、Contributor、および Role1
B. ホテルと貢献者のみ
C. グループ1、ロール1、および貢献者のみ
D. グループ1のみ
Answer: A (メーッセージを残す**)**
アクセス レビューには、Azure AD Premium P2 ライセンスが必要です。
Group1 と App1 のアクセス レビューは、Azure AD アクセス レビューで構成できます。
共同作成者ロールとロール1のアクセスレビューは、Privileged Identity Management (PIM) で構成する必要があります。PIM は Azure AD Premium P2 に含まれています。
参照：
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 Microsoft Identity and Access Administrator (SC-300) 公式学習ガイドと Microsoft Learn トレーニング モジュール 『アクセス レビューの管理』によると、Azure AD アクセス レビューを使用すると、管理者は Azure AD と Azure 全体の重要なリソースへのユーザー アクセスを定期的に評価できます。
試験の目標には、次のリソース タイプに適用されるアクセス レビュー機能が明示的にリストされています。
グループ (Microsoft 365 またはセキュリティグループ) - アクセスレビューを使用して、グループメンバーシップが最新であることを確認できます。この場合、Group1 は割り当て済みメンバーシップタイプであるため、アクセスレビューの対象となります。つまり、Group1 のメンバーをアクセスレビューの対象とすることができます。
エンタープライズ アプリケーション (App1) - アクセス レビューでは、Azure AD に登録されているエンタープライズ アプリケーションへのアクセス権を持つユーザーを評価し、適切なユーザーのみがアプリケーション アクセスを保持できるようにします。
Azure AD ロール (Role1) - 特権ディレクトリ ロール (グローバル管理者や Role1 などのカスタム ロールなど) のアクセス レビューを作成して、昇格されたアクセス許可の継続的な必要性を検証できます。
Azure サブスクリプション ロール (共同作成者) - Azure AD Privileged Identity Management (PIM) と統合すると、Azure リソースと管理グループにもアクセス レビューを適用できます。これにより、 共同作成者」などのロールをレビューすることで、最小限の権限によるアクセスが確保されます。Microsoft のドキュメントに基づき、以下の点に留意してください。
『アクセス レビューは、Azure AD グループ、エンタープライズ アプリケーション、Azure AD ロール、および Azure リソース ロールに対して構成でき、アクセス権が適切に維持されていることを確認できます。』つまり、Group1、App1、Contributor、および Role1 の 4 つすべてが、アクセス レビューのサポート対象となります。

最新問題: **288**
デフォルトのアプリ登録設定を持つAzure Active Directory (Azure AD) テナントがあります。このテナントには、次の表に示すユーザーが含まれています。

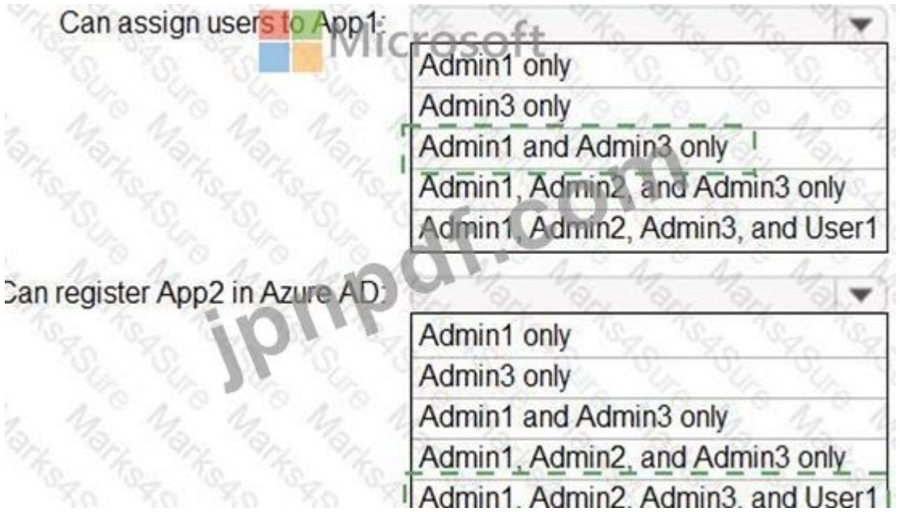
Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

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Azure ADに登録します。
App1 にユーザーを割り当てることができるユーザーと、Azure AD 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。

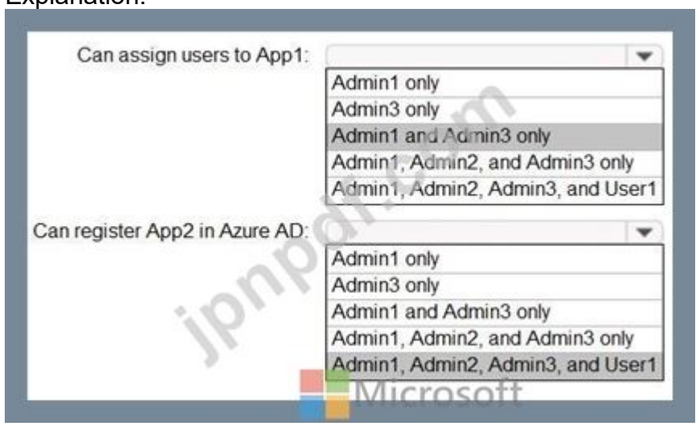
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:

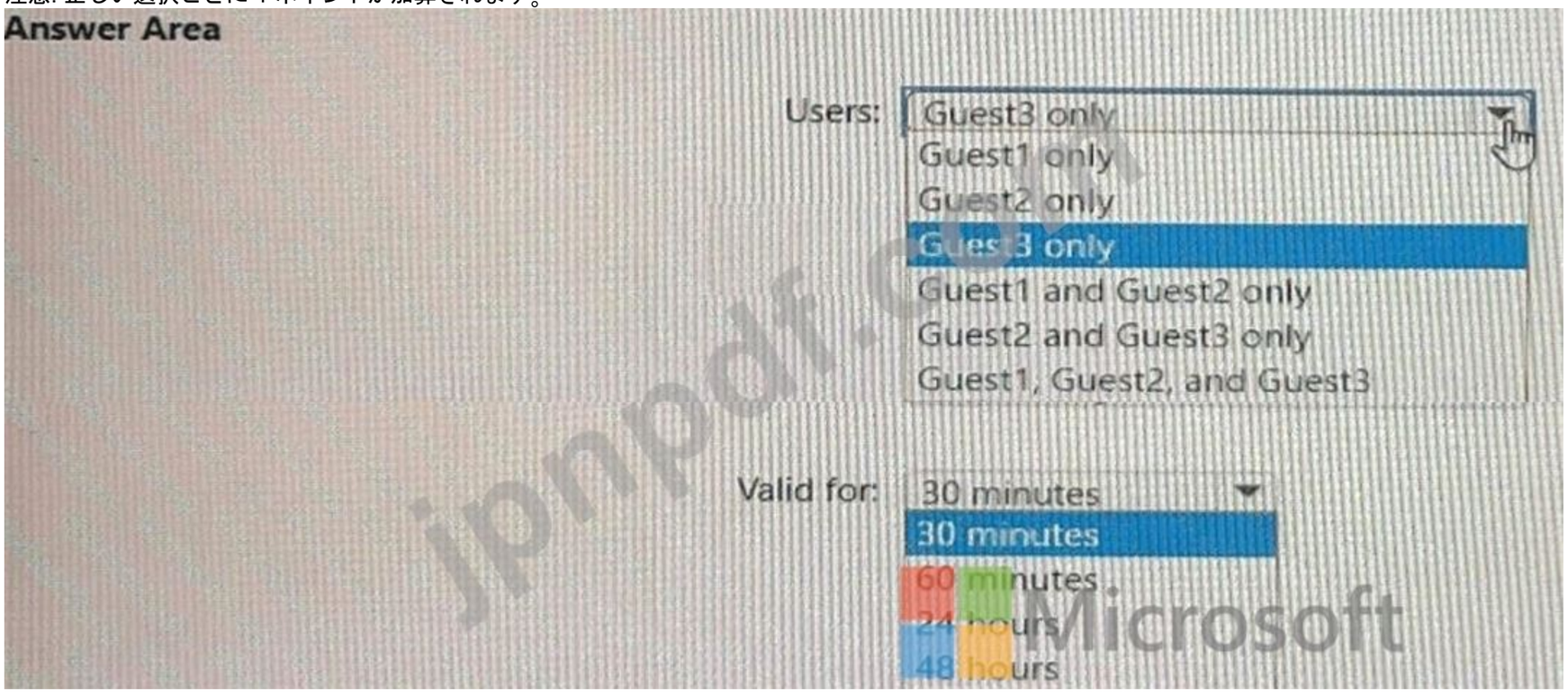


参照：
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-assign-users
https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

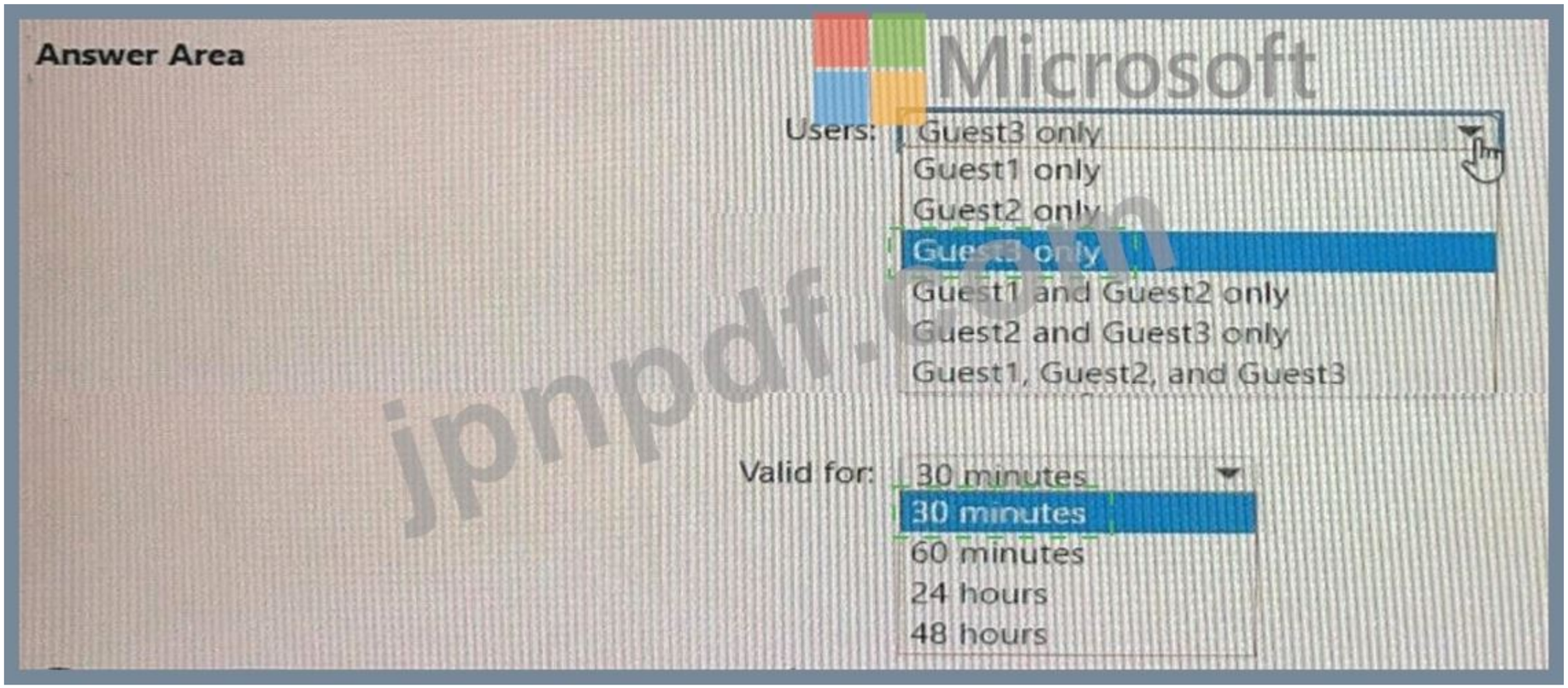
最新問題**: 289**
contoso.com という名前の Azure AD テナントがあり、ゲスト用のワンタイム パスコードを電子メールで送信することが [はい] に設定されています。
次の表に示すゲスト ユーザーを招待します。

Name	Email domain	Account type
Guest1	adatum.com	Azure AD account
Guest2	outlook.com	Microsoft account
Guest3	gmail.com	Personal Google account

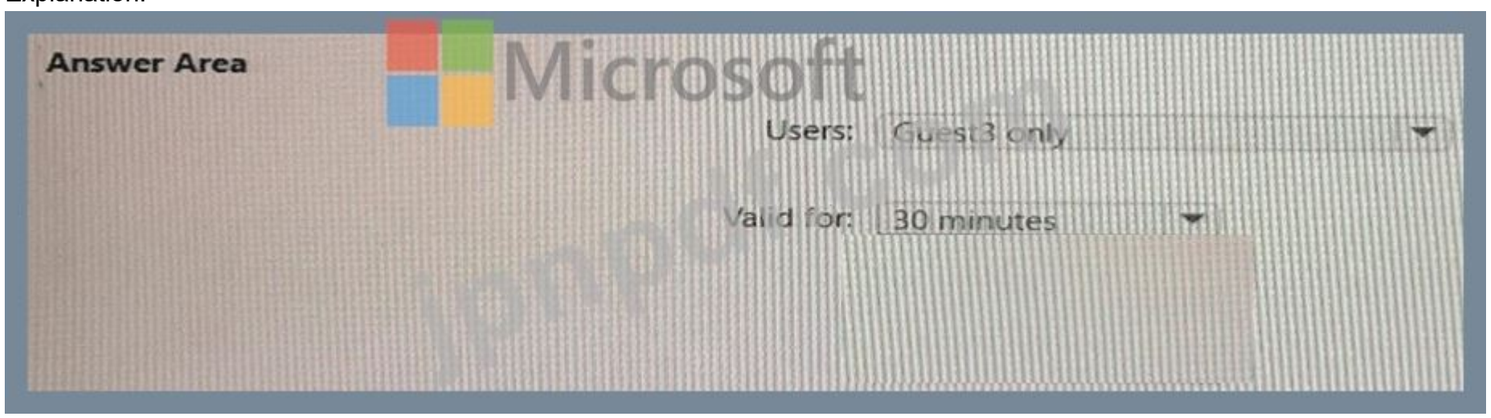
ワンタイム パスコードを受け取るユーザーは誰ですか? また、パスコードの有効期間はどのくらいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Explanation:



最新問題: 290

ホットスポットに関する質問

次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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グローバル管理者ロールを構成します。

Edit

Setting	State
Activation maximum duration (hours)	1 hour(s)
vRequire 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

jpnpdf.com

Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

User1 は、グローバル管理者ロールの対象となります。
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 ポイントが加算されます。



Answer:

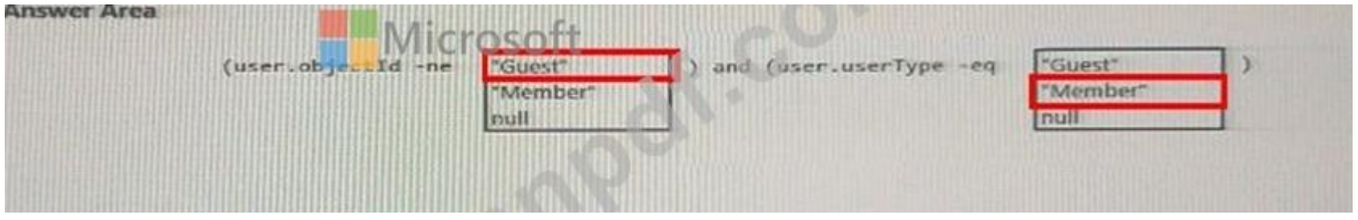


Explanation:
ボックス1: はい
アクティベーションにはMFAが必要です
ボックス2: いいえ
特権認証管理者は、グローバル管理者を含むすべてのユーザーに対して、任意の認証方法を設定またはリセットできます。
特権ロール管理者は、Azure Active Directory および Azure AD Privileged Identity Management におけるグローバル管理者ロールを含むロールの割り当てを管理できます。さらに、このロールでは、Privileged Identity Management と管理単位のあらゆる側面を管理できます。
ボックス3: いいえ
特権認証管理者は、グローバル管理者を含むすべてのユーザーに対して、任意の認証方法を設定またはリセットできます。
特権ロール管理者は、Azure Active Directory および Azure AD Privileged Identity Management におけるグローバル管理者ロールを含むロールの割り当てを管理できます。さらに、このロールでは、Privileged Identity Management と管理単位のあらゆる側面を管理できます。

最新問題**: 291**
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はどのように完成させるべきでしょうか？答えは、適切な値を正しいターゲットにドラッグすることです。各値は1回、複数回、または全く使用されない場合があります。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: **292**

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。

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 ポイントが加算されます。



Answer:



Explanation:



Microsoft
jpnpdf.com

最新問題: **293**
App1 という名前の登録済みアプリを含む Azure サブスクリプションがあります。
App1 のサインインアクティビティを確認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している必要があります。
* 失敗したサインインの数を特定します。
* サインインの成功率を特定します。
* 管理上の労力を最小限に抑えます。
何を使うべきでしょうか?
A. 監査ログ
B. サインインログ
C. アクセスレビュー
D. 使用状況と分析情報
Answer: D (メーッセージを残す)

最新問題: **294**
Microsoft 365 E5 サブスクリプションをお持ちです。
アプリ ガバナンス アドオン ライセンスを購入します。
アプリ ガバナンスの統合を有効にする必要があります。
どのポータルを使用すればよいですか?
A. Microsoft Defender for Cloud Apps ポータル
B. Azure Active Directory 管理センター
C. Microsoft 365 管理センター
D. Microsoft 365 Defender
E. Microsoft Purview コンプライアンス ポータル
Answer: A (メーッセージを残す)

最新問題: **295**
ボストンオフィスから接続するユーザーに対して、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す必要があります。
何を設定すればよいでしょうか?
A. プライベートIPアドレス範囲を持つ名前付き場所
B. パブリックIPアドレス範囲を持つ名前付き場所
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: B (メーッセージを残す)

参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition 場所オファーの国設定、IP 範囲、MFA 信頼済み IP、企業ネットワーク VPN ゲートウェイ IP アドレス:
これは、オンプレミス ネットワークの VPN デバイスのパブリック IP アドレスです。VPN デバイスには IPv4 パブリック IP アドレスが必要です。接続先の VPN デバイスの有効なパブリック IP アドレスを指定してください。Azure クライアントからアクセスできる必要があります。アドレス空間: このゲートウェイ経由でローカル オンプレミス ネットワークにルーティングする IP アドレス範囲を一覧表示します。複数のアドレス空間範囲を追加できます。ここで指定する範囲は、仮想ネットワークが接続する他のネットワークの範囲や、仮想ネットワーク自体のアドレス範囲と重複しないようにしてください。

最新問題**: 296**
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

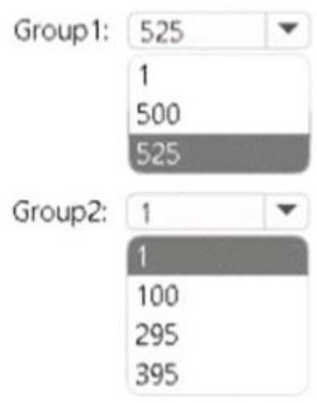
次の表に示すように、Group1 のアクセス レビューを作成します。

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。

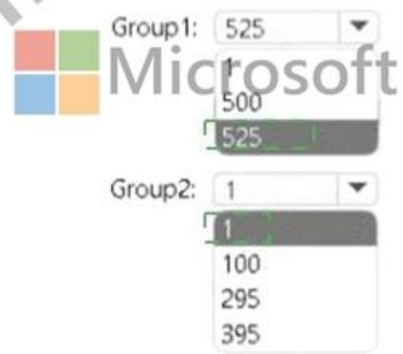
Setting	Value
Review type	Teams + Groups
Review scope	Guest users only
Reviewers	Group owner

各グループに必要なAzure AD Premium P2ライセンスの最小数はいくつですか？ 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：正しい選択ごとに1ポイントが加算されます。
Answer Area



Answer:

Answer Area



説明

Answer Area



最新問題: 297

SSPR の計画された変更を実装します。

User3 が SSPR を使用しようとすると何が起こりますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題: 298

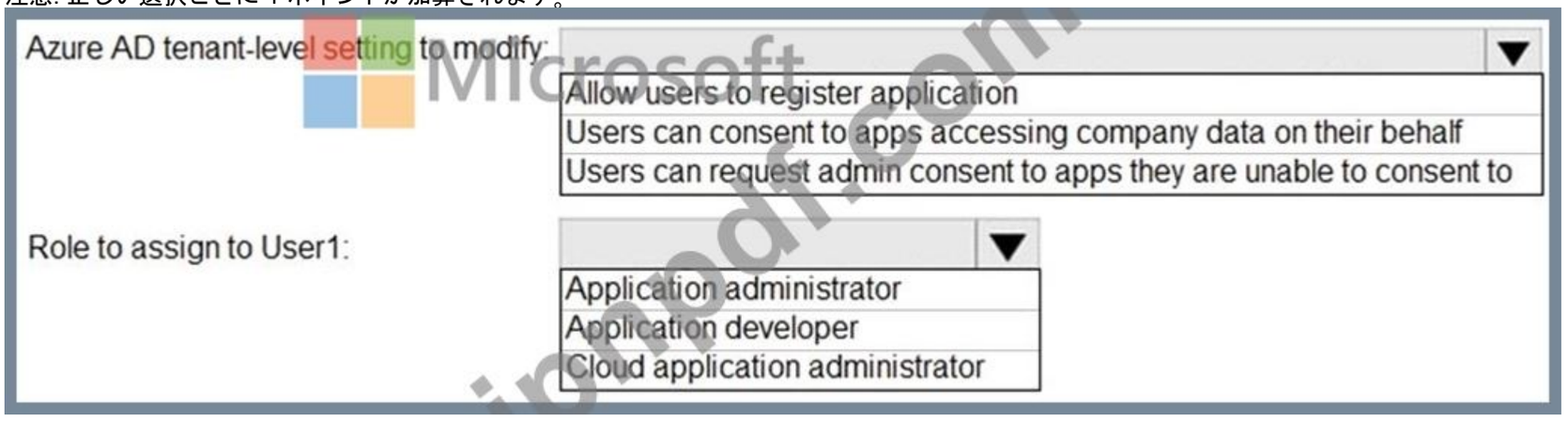
次の表に示すオブジェクトを含む Azure Active Directory (Azure Azure) テナントがあります。

* Device1という名前のデバイス
* User1、User2、User3、User4、User5という名前のユーザー
* グループ1、グループ2、グループ3、Ciroup4、グループ5という5つのグループ
グループは次の表のように構成されます。

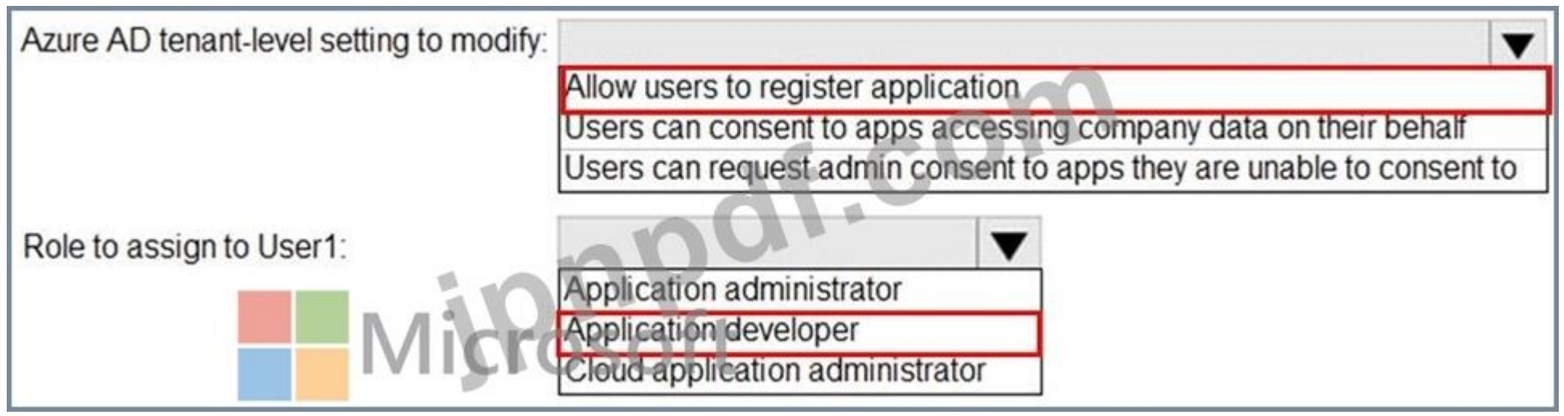
Name	Type	Membership type	Members
Group1	Security	Assigned	User1, User3, Group2, Group4
Group2	Security	Dynamic User	User2
Group3	Security	Dynamic Device	Device1
Group4	Microsoft 365	Assigned	Group5
Group5	Microsoft 365	Assigned	User5

Microsoft Office 365 Enterprise E5 ライセンスを Group1 に割り当てた場合、使用されるライセンスの数はいくつですか?
A. 0
B. 2
C. 3
D. 4
Answer: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/licensing-group-advanced

最新問題**: 299**
委任要件を満たすには、Azure AD でアプリの登録を構成する必要があります。
どうすればいいでしょうか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



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

最新問題**: 300**
条件付きアクセス ポリシーを使用する Azure Active Directory (Azure AD) テナントがあります。
条件付きアクセスの使用状況を分析するために、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) を使用する予定です。
条件付きアクセス ポリシー データを含む Azure AD 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形式のサインイン
B. CSV形式のサインイン
C. JSON形式の監査ログ
D. CSV形式の監査ログ
Answer: A (メーッセージを残す**)**
Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび公式 Microsoft Learn コンテンツ 『レポートとログを使用した Azure AD の監視とトラブルシューティング』に記載されているように、条件付きアクセス ポリシーのデータは Azure Active Directory 内のサインイン ログに記録されます。各サインイン レコードには、評価された条件付きアクセス ポリシー、適用されたポリシー、およびその適用結果（『アクセスを許可する』、『ブロックする』、『MFA を要求する』など）など、認証プロセスに関する詳細情報が含まれます。
一方、Azure AD の監査ログは、ポリシーの作成、変更、管理アクションといったディレクトリレベルの変更を追跡しますが、ユーザー認証や条件付きアクセスの評価データは含まれません。そのため、外部の SIEM システムで条件付きアクセスのアクティビティを分析するには、条件付きアクセスの評価の詳細を含むサインインログをエクスポートする必要があります。
Microsoft のドキュメントでは、サードパーティの SIEM システムとの統合には JSON 形式でのエクスポートが推奨されています。これは、JSON では CSV 形式では完全に表現できないネストされたポリシー評価データ構造が保持されるためです。CSV エクスポートでは、詳細な条件付きアクセス結果（ポリシー ID やポリシーごとの結果など）が省略されるため、自動解析や詳細な分析には適していません。
したがって、Microsoft の公式ドキュメントに基づくと、次のようになります。
『条件付きアクセス ポリシーの評価結果はサインイン ログでのみ使用可能であり、SIEM 統合のために JSON 形式でエクスポートする必要があります。』
正解: A. JSON形式のサインイン

最新問題**: 301**
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。

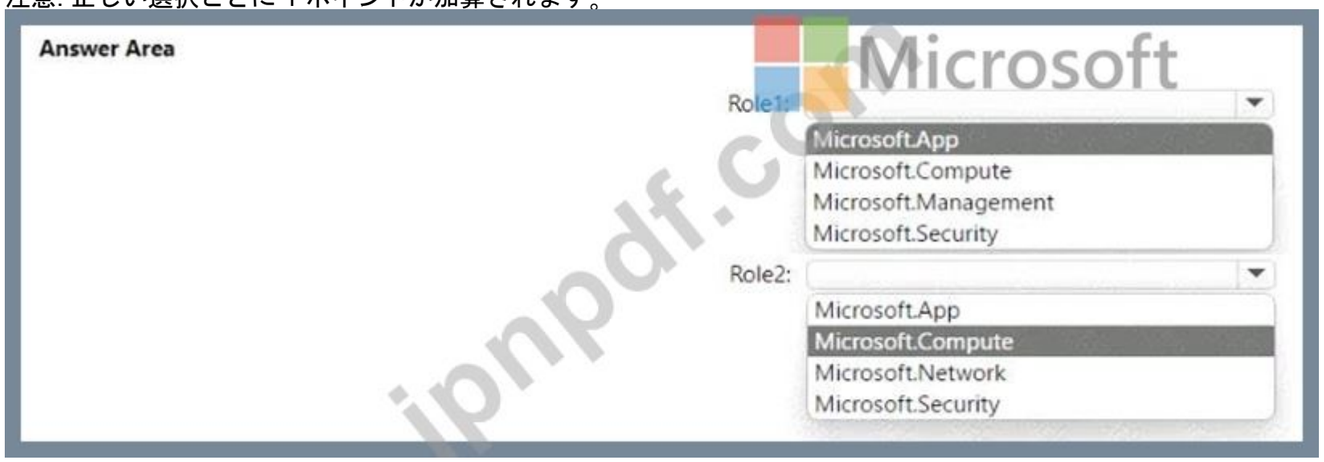
```
user.usageLocation -in ["US","AU"] -and (user.department -eq "Sales") -and -not (user.jobTitle -eq "Manager") -or (user.jobTitle -eq "SalesRep")
```

どのユーザーがグループに追加されますか?

A. ユーザー2のみ
B. ユーザー1とユーザー3のみ
C. ユーザー1とユーザー2のみ
D. ユーザー1のみ
E. ユーザー3のみ
F. ユーザー1、ユーザー2、ユーザー3
Answer: C (メーッセージを残す)

有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題: **302**
Azure サブスクリプションをお持ちです。
Role1とRole2という2つのカスタムロールを作成する必要があります。ソリューションは以下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。
各ロールにはどのリソース プロバイダーのアクセス許可が必要ですか? 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**: 303**

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。このテナントには、App1という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。このテナントには、App2という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 2 つの認証情報はどれですか? 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 ポイントが加算されます。

A. マネージドID

B. ユーザーアカウント

C. ワンタイムパスワード

D. 秘密

E. 証明書

Answer: (解答を表示する**)**

最新問題**: 304**

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Site1へのアクセスをリクエストできるように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。

- グループに基づいてユーザーからのリクエストを自動的に承認する
メンバーシップ。
- 30 日後にアクセスが自動的に削除されます。

何をすべきでしょうか?

A. 条件付きアクセス ポリシーを作成します。

B. アクセス パッケージを作成します。

C. Azure AD Privileged Identity Management でロール設定を構成します。

D. Microsoft 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**)**

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

最新問題**: 305**
Microsoft 365 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 Active Directory ドメインと同期します。このドメインには、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への通信ができなくなります。
Server1 と Server2 に Azure AD パスワード保護を実装します。
Windows Server 2019 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。
1 台のサーバーに障害が発生した場合でも、Azure AD 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 コネクト
B. Azure AD 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. Azure AD 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**)**
Microsoft SC-300 公式試験リファレンスと Microsoft の公式ドキュメントによると、Azure AD パスワード保護は、クラウド環境とオンプレミス環境の両方に対してパスワード ポリシーの適用と禁止パスワードの保護を提供します。
このソリューションには、次の 2 つの主要コンポーネントが必要です。
* ドメイン コントローラー (DC エージェント) - ドメイン内でパスワード ポリシーを適用します。
* プロキシ サービス (Azure AD パスワード保護プロキシ) - Azure AD と通信して最新のパスワード ポリシーと禁止パスワード リストをダウンロードし、DC エージェントと共有します。
このシナリオでは、Server1 と Server2 は既に Azure AD パスワード保護がインストールされているドメインコントローラーですが、インターネットに直接通信できません。つまり、Azure AD への安全な接続には、別のサーバーで実行されているプロキシ サービスに依存しています。
高可用性を確保するため、Microsoft は少なくとも 2 台のプロキシ サーバーを導入することを推奨しています。これにより、1 台のプロキシ サーバーに障害が発生しても、パスワード ポリシーの継続的な同期が確保されます。
Microsoft のドキュメントより:
冗長性を確保するために、少なくとも 2 台のプロキシ サーバーを展開します。プロキシ サービスは、Azure AD からグローバルおよびカスタムの禁止パスワード リストを取得し、DC エージェントを実行しているすべてのドメイン コントローラーに複製します。したがって、Server4 に Azure AD パスワード保護プロキシ サービスをインストールすると、プロキシ サーバーの 1 つに障害が発生した場合でもサービスの継続性が確保されます。

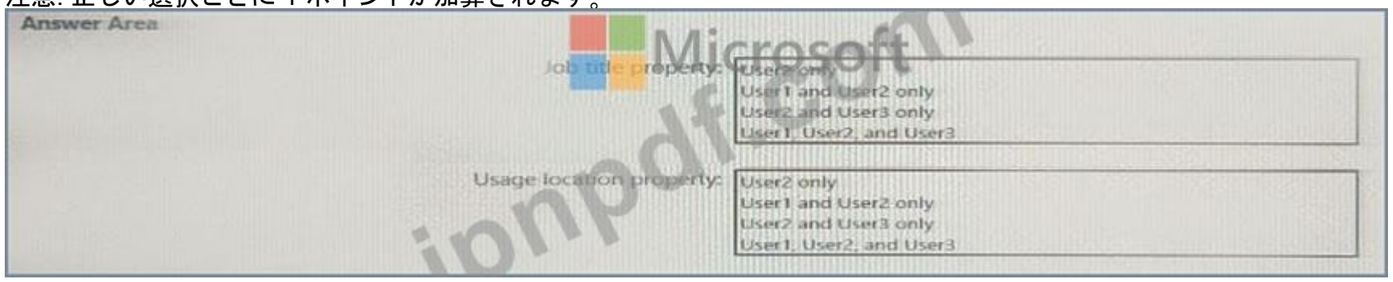
最新問題**: 306**
Microsoft 365 テナントがあります。
すべてのユーザーは携帯電話とラップトップを持っています。
ユーザーは、Wi-Fi アクセスや携帯電話接続がない遠隔地から作業することがよくあります。
ユーザーは、遠隔地から作業する際、インターネットにアクセスできる有線ネットワークにラップトップを接続します。
多要素認証 (MFA) を実装する予定です。
ユーザーはリモート ロケーションからどの MFA 認証方法を使用できますか?

A. Microsoft Authenticator アプリからの通知
B. アプリパスワード
C. Windows Hello for Business
D. SMS
Answer: (解答を表示する**)**
説明
Windows 10 では、Windows Hello for Business が PC とモバイルデバイスにおけるパスワードの代わりに強力な 2 要素認証を導入します。この認証は、デバイスに紐付けられ、生体認証または PIN を使用する新しいタイプのユーザー資格情報で構成されます。
登録時にユーザーの最初の 2 段階認証を実行すると、ユーザーのデバイスに Windows Hello が設定され、Windows はユーザーにジェスチャ (指紋などの生体認証または PIN) を設定するように求めます。ユーザーはジェスチャで本人確認を行います。その後、Windows は Windows Hello を使用してユーザーを認証します。
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods
https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-overview

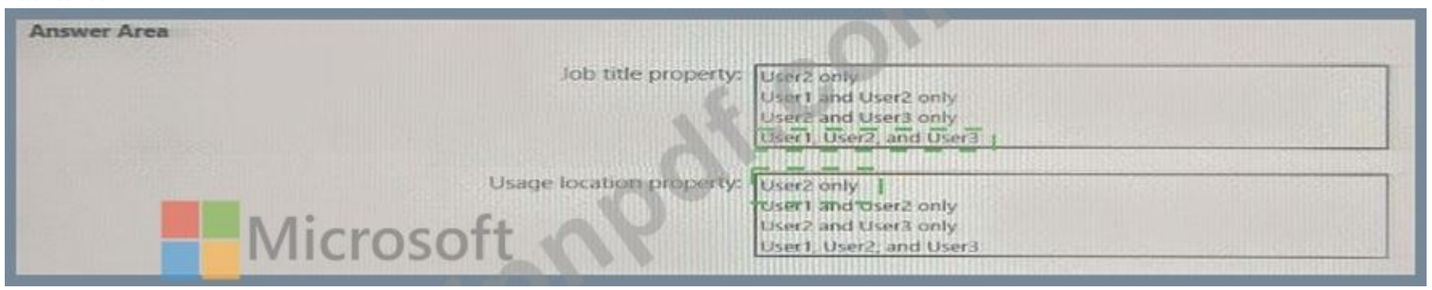
最新問題**: 307**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:

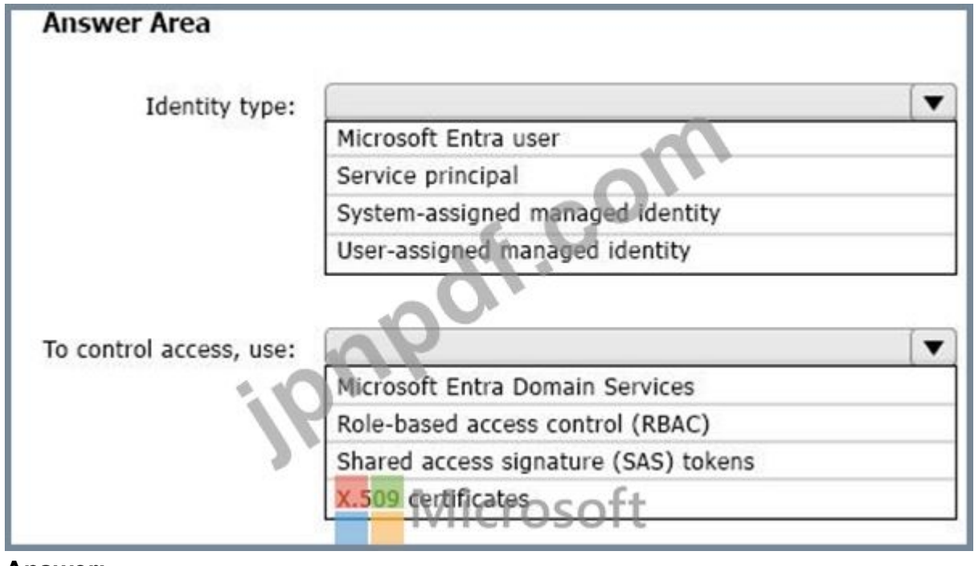


最新問題**: 308**
Microsoft 365 テナントがあります。
Azure Active Directory (Azure AD) テナントは、オンプレミスの Active Directory ドメインと同期します。このドメインには、次の表に示すサーバーが含まれています。

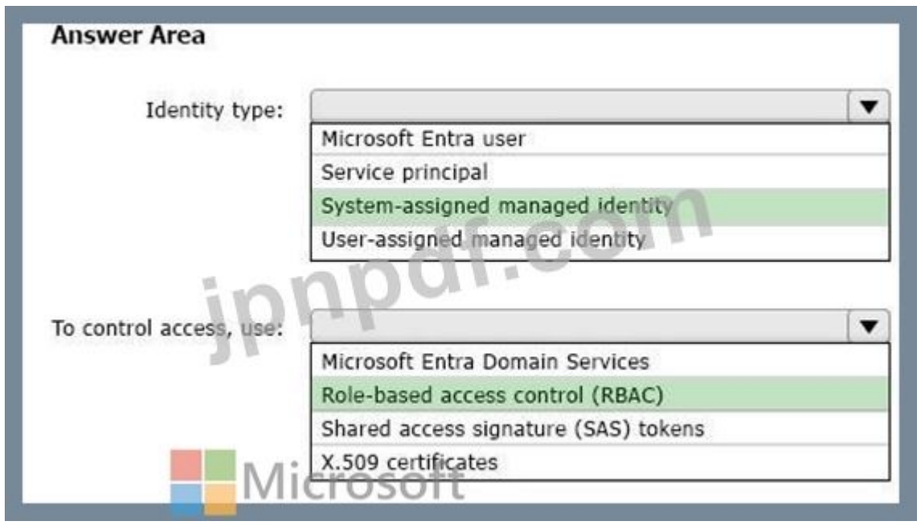
Name	Operating system	Configuration
Server1	Windows Server 2019	Domain controller
Server2	Windows Server 2019	Domain controller
Server3	Windows Server 2019	Azure AD Connect

ドメイン コントローラーはインターネットへの通信ができなくなります。
Server1 と Server2 に Azure AD パスワード保護を実装します。
Windows Server 2019 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。
1 台のサーバーに障害が発生した場合でも、Azure AD 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 コネクト
B. Azure AD 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. Azure AD パスワード保護プロキシ サービス
Answer: (解答を表示する**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on- premisesdeploy

最新問題**: 309**
ホットスポットに関する質問
複数のストレージ アカウントを含む Microsoft Entra テナントがあります。
ストレージ アカウントへのアクセスを必要とする複数の Azure App Service アプリをデプロイする予定です。
アプリにストレージアカウントへのアクセスを提供するためのID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は、管理の手間を最小限に抑えるものでなければなりません。
ストレージ アカウントへのアクセスを制御するために、どのような種類の ID を推奨しますか。また、何を使用することをお勧めしますか。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。

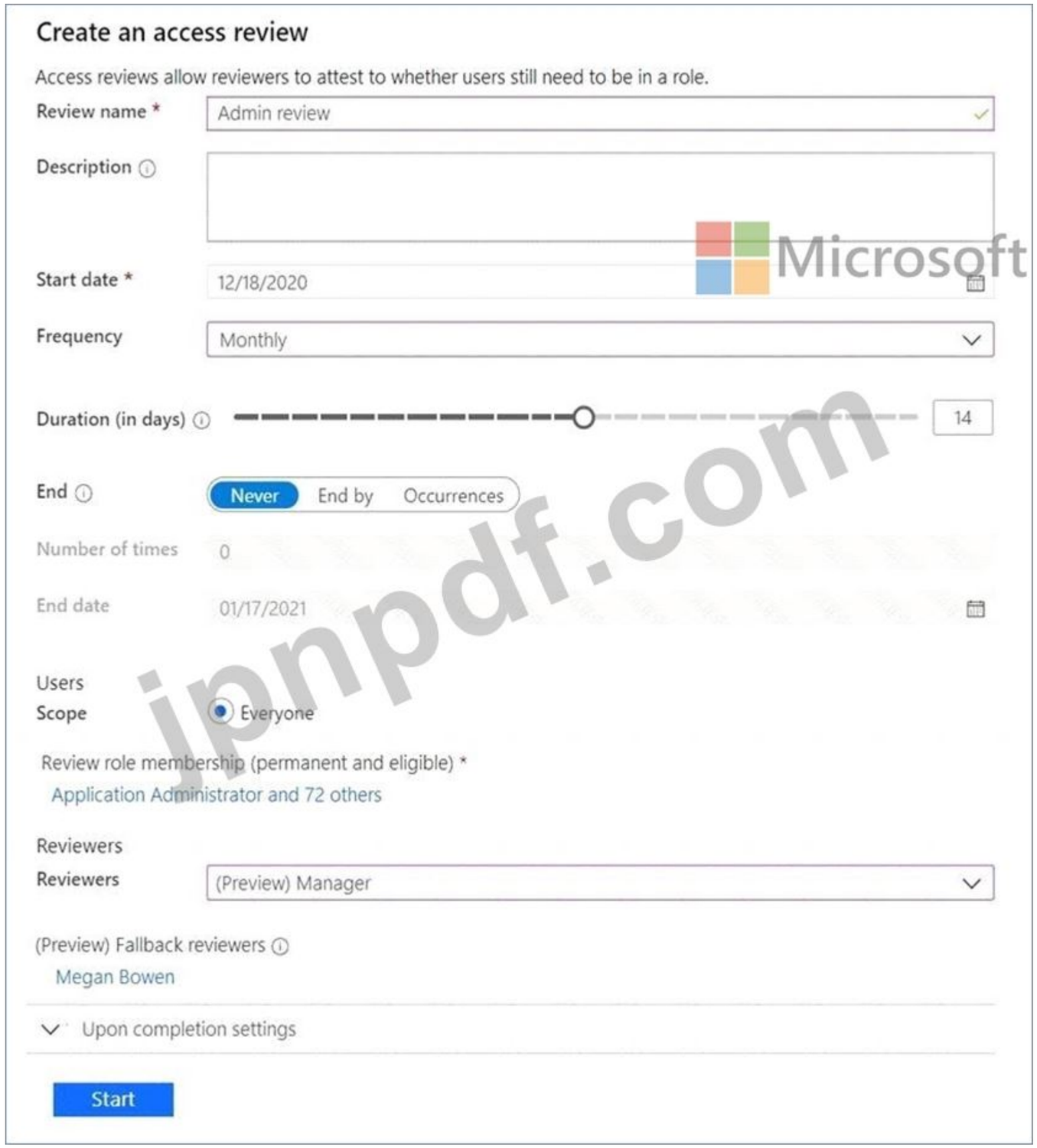


Answer:



Explanation:
https://learn.microsoft.com/en-us/azure/app-service/scenario-secure-app-access-storage?tabs=azure-portal

最新問題**: 310**
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可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Microsoft 365 テナントがあります。
100 人の IT 管理者が 10 の部門に分かれて所属しています。
図に示すアクセス レビューを作成します。(図タブをクリックします。)



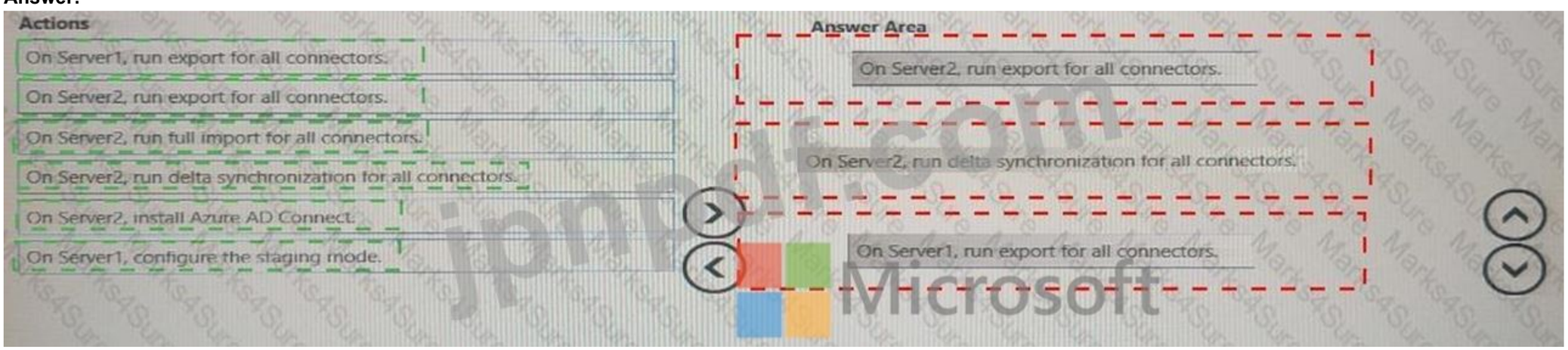
すべてのアクセス レビュー リクエストは Megan Bowen によって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取れるようにする必要があります。

解決策: 各マネージャーをフォールバックレビュー担当者として追加します。
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)
参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

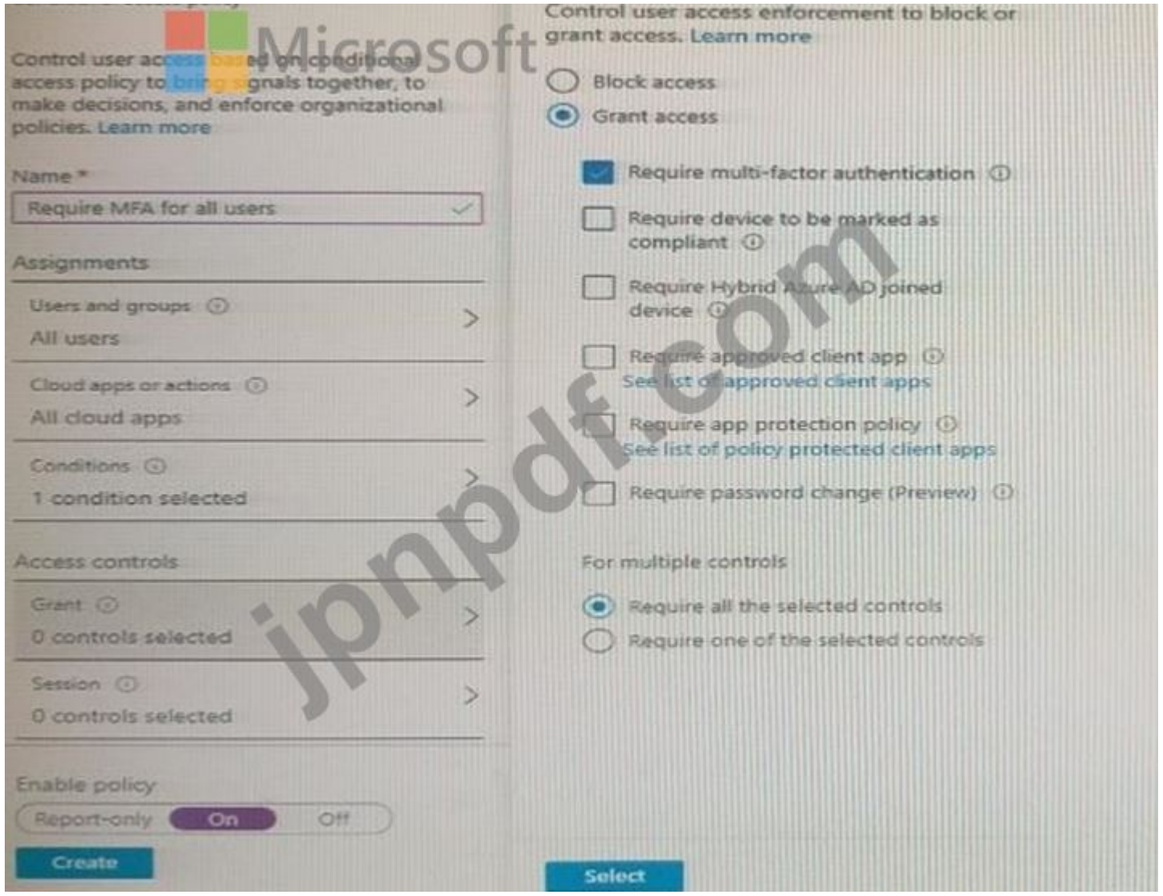
最新問題**: 311**
ネットワークには、Azure AD Connect を使用して contoso.com という名前の Azure Active Directory (Azure AD) テナントにリンクされている contoso.com という名前の Active Directory フォレストが含まれています。
Attire AD Connect は、Server 1 という名前のサーバーにインストールされています。
Windows Server 2019 を実行する Server? という名前の新しいサーバーを展開します。
Azure AD Connect 用のフェールオーバーサーバーを実装する必要があります。このソリューションでは、Server1 に障害が発生した場合にフェールオーバーにかかる時間を最小限に抑える必要があります。
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 リストから回答領域に移動し、正しい順序に並べます。



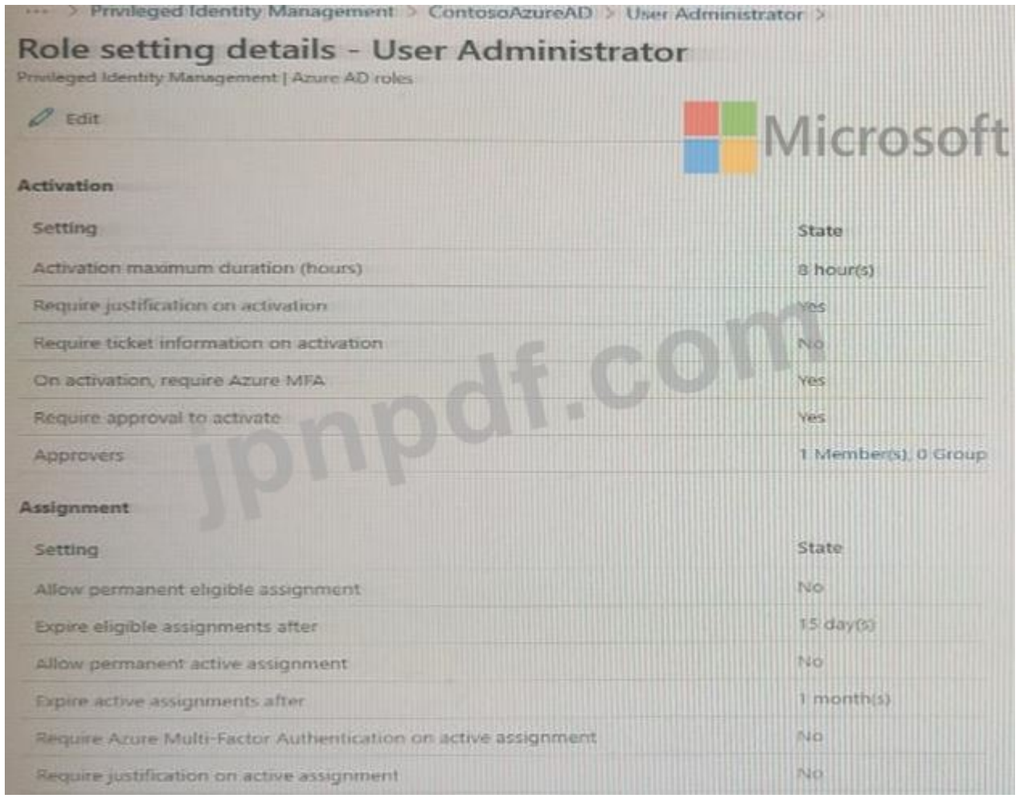
Answer:



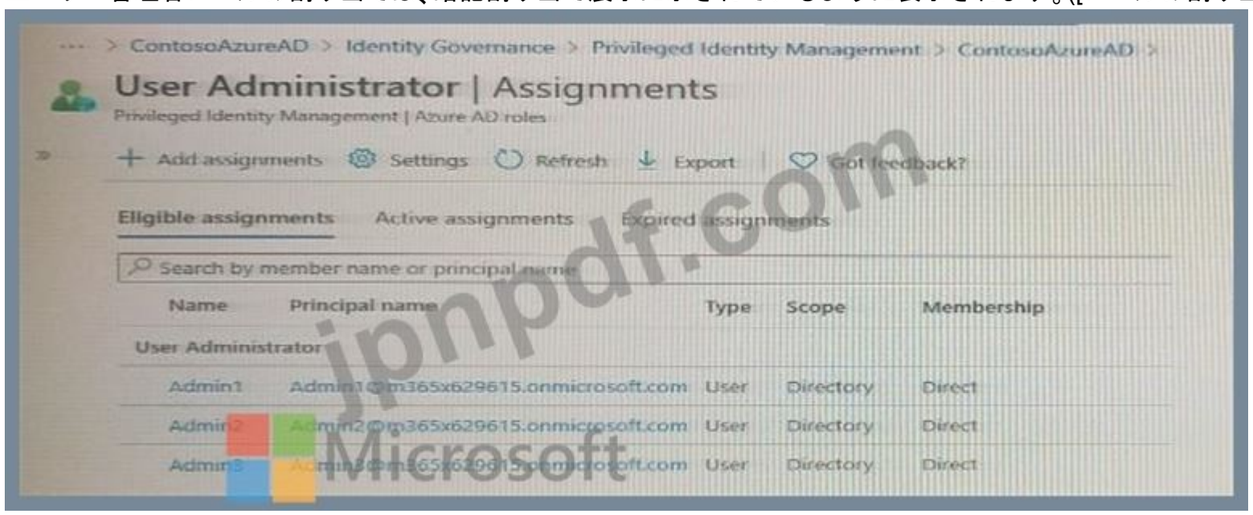
最新問題**: 312**
Microsoft 365 テナントがあります。
条件付きアクセス ポリシーは、条件付きアクセス ポリシーの図に示されているように構成します。([条件付きアクセス ポリシー] タブをクリックします。)



ユーザー管理者ロールの設定は、"ロール設定の詳細"の図のように表示されます。("ロール設定の詳細"タブをクリックします。)



ユーザー管理者ロールの割り当ては、暗記割り当て展示に示されているように表示されます。([ロールの割り当て] ラボをクリックします。)



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 ポイントが加算されます。



Answer:



最新問題: **313**

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セキュリティ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. User3とUser4のみ

B. ユーザー1、ユーザー2、ユーザー3、ユーザー4

C. ユーザー4のみ

D. User1とUser4のみ

E. User1、User3、User4のみ

Answer: A (メーッセージを残す)

最新問題: **314**

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
User1	Group1
User2	Group2
User3	Group3

テナントには次の表に示す認証方法があります。

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

アプリに表示される番号と携帯電話に表示される番号を照合してクラウド アプリにサインインするユーザーは誰でしょうか?

A. ユーザー1のみ

B. ユーザー2のみ

C. ユーザー3のみ

D. ユーザー1とユーザー2のみ

E. ユーザー2とユーザー3のみ

Answer: (解答を表示する**)**

Microsoft の SC-300: Microsoft Identity and Access Administrator 学習ガイドおよび試験番号 SC-300 によると、サインインプロセスの動作は、ユーザーまたはそのグループに対して有効になっている認証方法によって異なります。Azure AD は、Microsoft Authenticator アプリ、FIDO2、SMS など、特定のユーザーグループを対象にできる複数の強力な認証方法をサポートしています。

質問では、テナントの構成によって次の方法が有効になることが指定されています。

* FIDO2 # グループ2 (はい)

* Microsoft Authenticator アプリ # グループ 1 (はい)

* SMS # グループ3 (はい)

ユーザーのメンバーシップは次のとおりです。

* ユーザー1 # グループ1

* ユーザー2 # グループ2

* ユーザー3 # グループ3

質問のキーフレーズは次のとおりです。

「アプリに表示される番号と携帯電話に表示される番号を照合して、クラウド アプリにサインインします。」この特定のサインイン エクスペリエンスは、Microsoft Authenticator アプリの番号照合機能を指します。

* 番号の照合は、Azure AD MFA のセキュリティ強化であり、ユーザーはサインイン画面に表示される番号と Microsoft Authenticator アプリの通知に表示される番号を照合してサインインを確認する必要があります。

* Microsoft Learn によると:

「Microsoft AuthenticatorアプリをMFAに使用する場合、ユーザーは画面に表示される番号を入力するか、一致する番号を入力するよう求められます。この機能は、誤認証を防ぐことで認証を強化します。」そのため、

* Group1 (Microsoft Authenticator アプリが有効になっているグループ) のメンバーである User1 のみが、サインイン時に番号の一致を体験します。

* ユーザー2 は、番号照合ではなく、ハードウェア キーまたは生体認証を採用した FIDO2 を使用します。

* ユーザー 3 は SMS を使用しますが、これにはワンタイム パスコード (OTP) が含まれますが、この場合も番号の照合は行われません。

したがって、番号マッチングを使用してクラウド アプリにサインインするのは User1 のみになります。

最新問題**: 315**

Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
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

各ユーザーを設定するにはどのポータルを使用すればよいでしょうか？適切なポータルを適切なユーザーにドラッグしてください。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

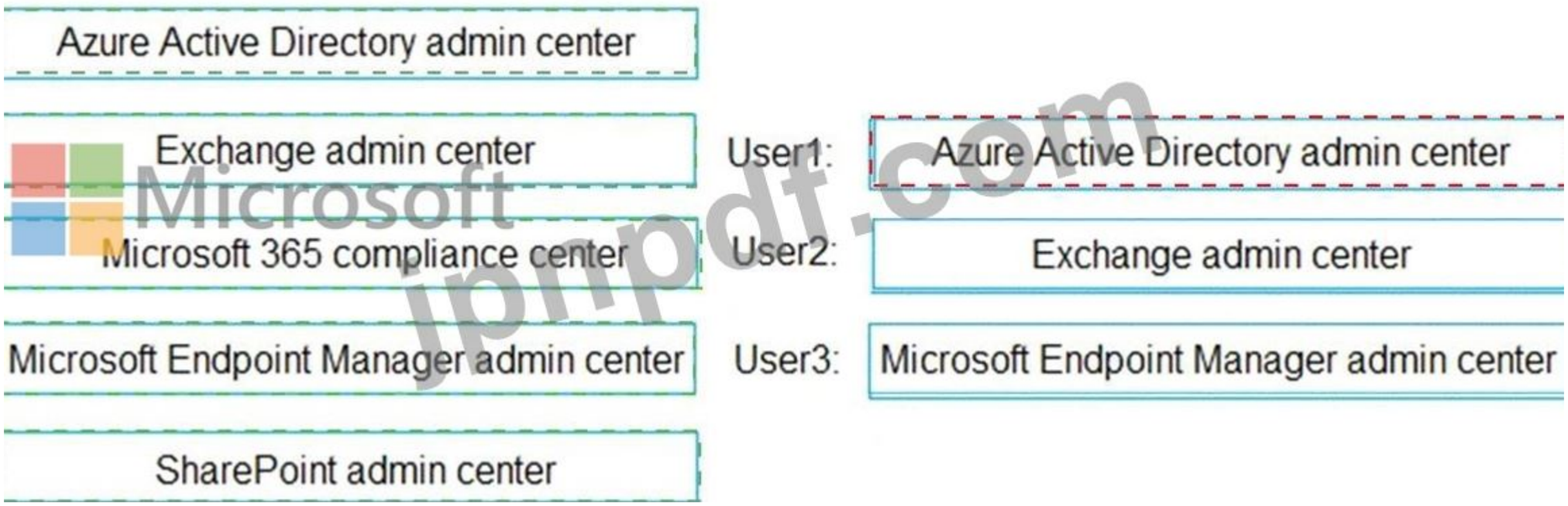
Portals

- Azure Active Directory admin center
- Exchange admin center
- Microsoft 365 compliance center
- Microsoft Endpoint Manager admin center
- SharePoint admin center

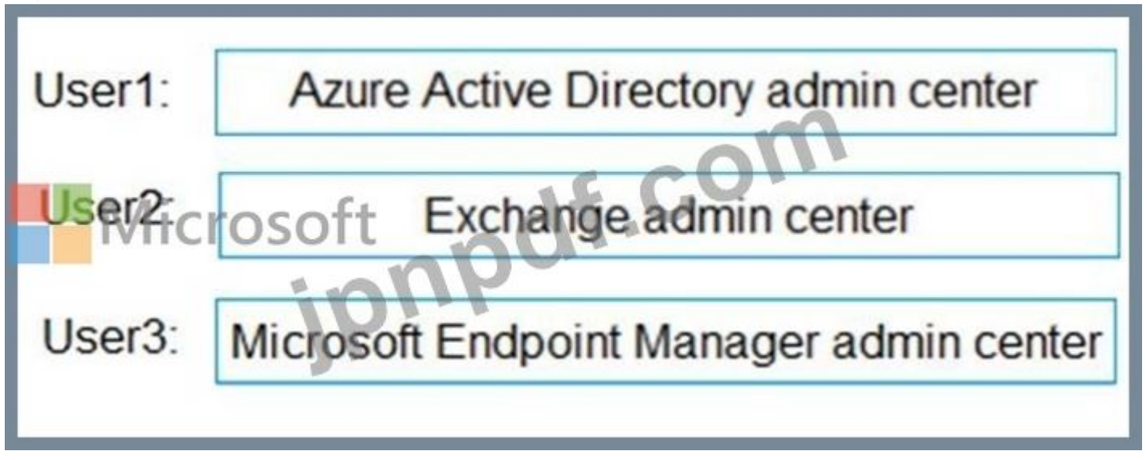
Answer Area

User1: [ ]
User2: [ ]
User3: [ ]

Answer:



Explanation:



最新問題: 316

Azure サブスクリプションをお持ちです。

Azure AD ログは Log Analytics ワークスペースに送信されます。

ログをクエリし、ユーザーごとのサインイン数をグラフで表示する必要があります。

クエリ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。

```
SigninLogs
| where ResultType == 0
|  login_count = count() by Identity
```

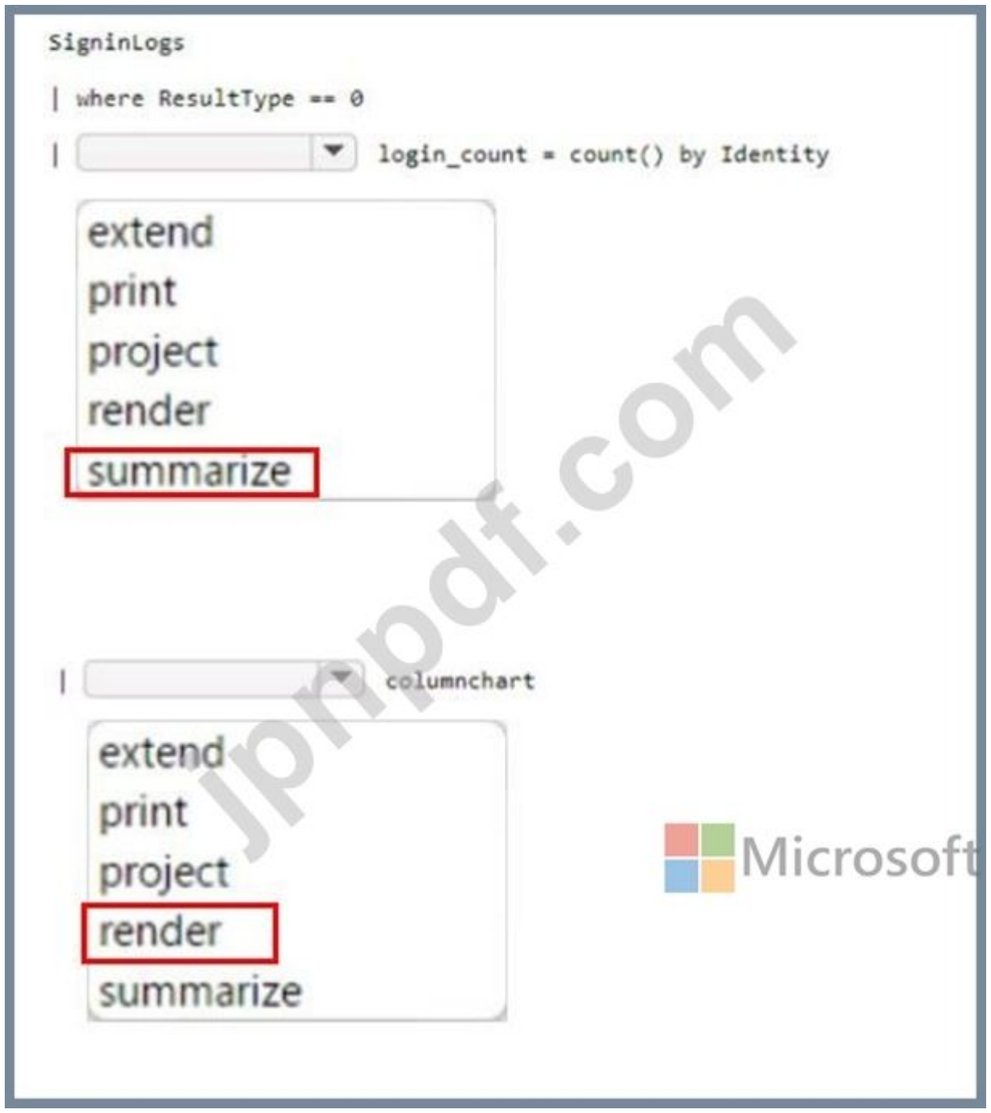
- extend
- print
- project
- render
- summarize

```
|  columnchart
```

- extend
- print
- project
- render
- summarize

jpnpdf.com

Answer:



有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

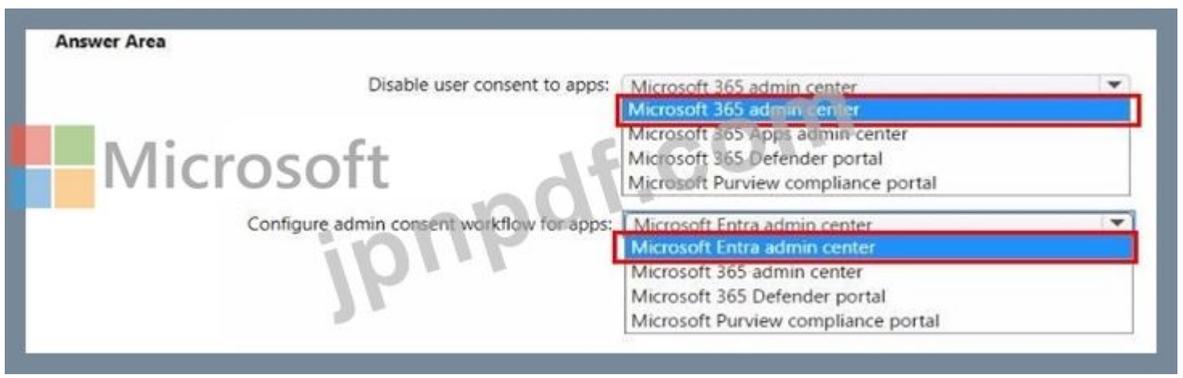
最新問題: **317**
ユーザー管理者ロールの計画された変更を満たす必要があります。
何をすべきでしょうか?
A. アクセスレビューを作成します。
B. ロール設定を変更する

C. 管理者ユニットを作成します。
D. アクティブな割り当てを変更します。
Answer: D (メーッセージを残す)
ロール設定の詳細は次のとおりです: ロール設定の詳細 - ユーザー管理者 Privileged Identity Management | Azure AD ロール 既定の設定 状態 アクティベーション時に理由を要求する はい アクティベーション時にチケット情報を要求する いいえ アクティベーション時に Azure MFA を要求する はい アクティベーションに承認を要求する いいえ 承認者 なし

最新問題: **318**
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のアプリ同意を設定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している必要があります。
* 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べきですか？回答するには、回答で適切なオプションを選択してください。注：正しい選択ごとに1ポイントが加算されます。



Answer:



最新問題: **319**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

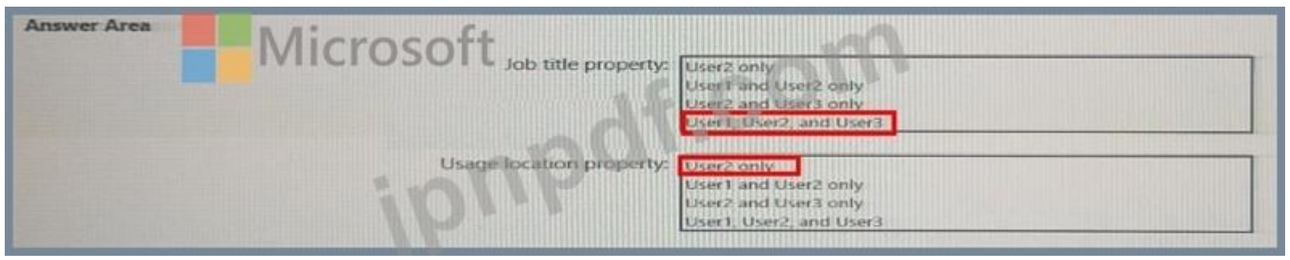
Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

Azure AD で、どのユーザーに対して役職プロパティと使用場所プロパティを構成できますか? 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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



最新問題**: 320**

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。

高度な権限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。ソリューションは管理作業を最小限に抑える必要があります。

何を使うべきでしょうか?

A. Microsoft Entra 権限管理

B. 特権 ID 管理 (PIM)

C. グローバルセキュアアクセス

D. Microsoft Entra 認証済み ID

Answer: A (メーッセージを残す**)**

最新問題**: 321**

Microsoft 365 テナントがあります。

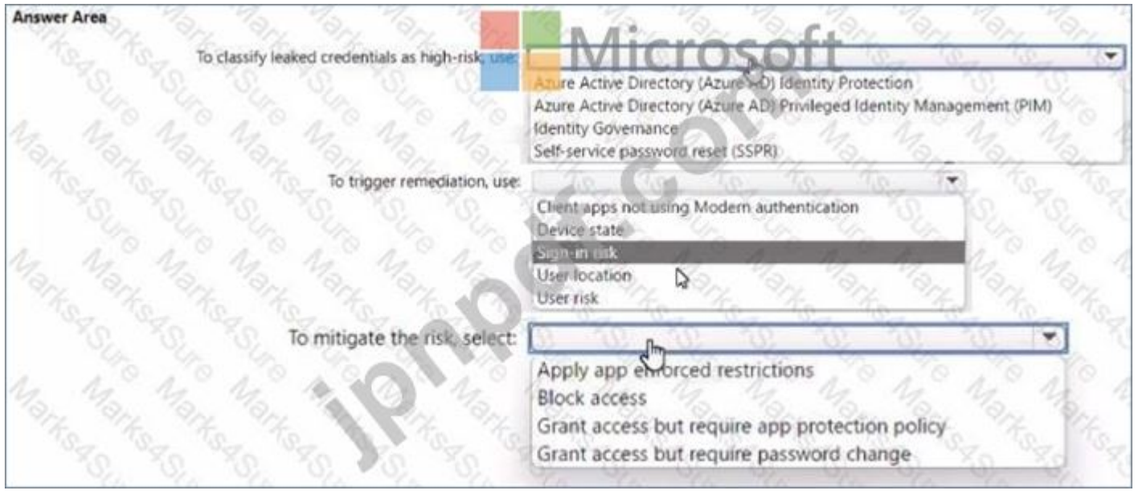
認証情報が漏洩したユーザーを特定する必要があります。ソリューションは以下の要件を満たす必要があります。

* 資格情報が漏洩した疑いのあるユーザーによる ID サイン。

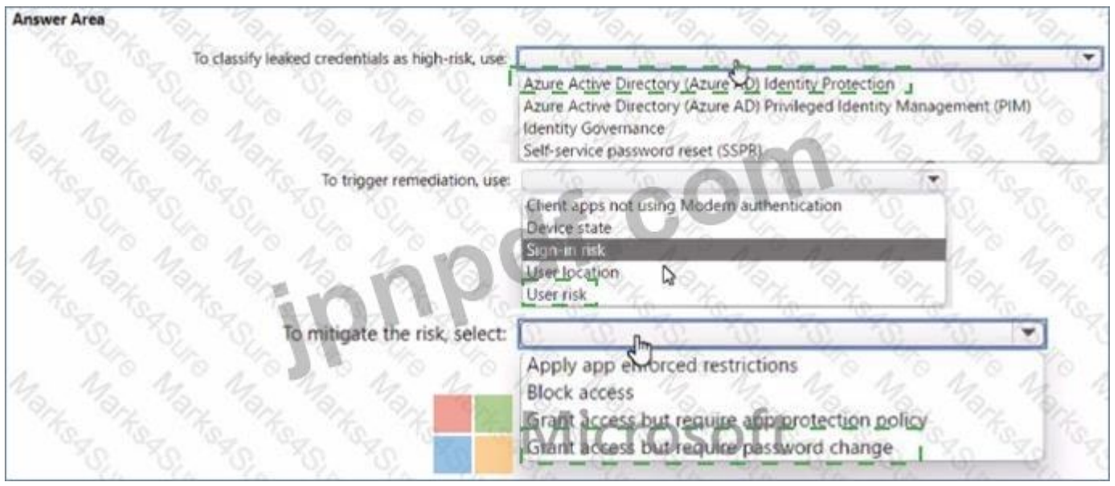
* サインインを高リスクイベントとしてフラグ付けします。

* 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。

何を使うべきでしょうか? 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。



Answer:



Explanation:



最新問題**: 322**

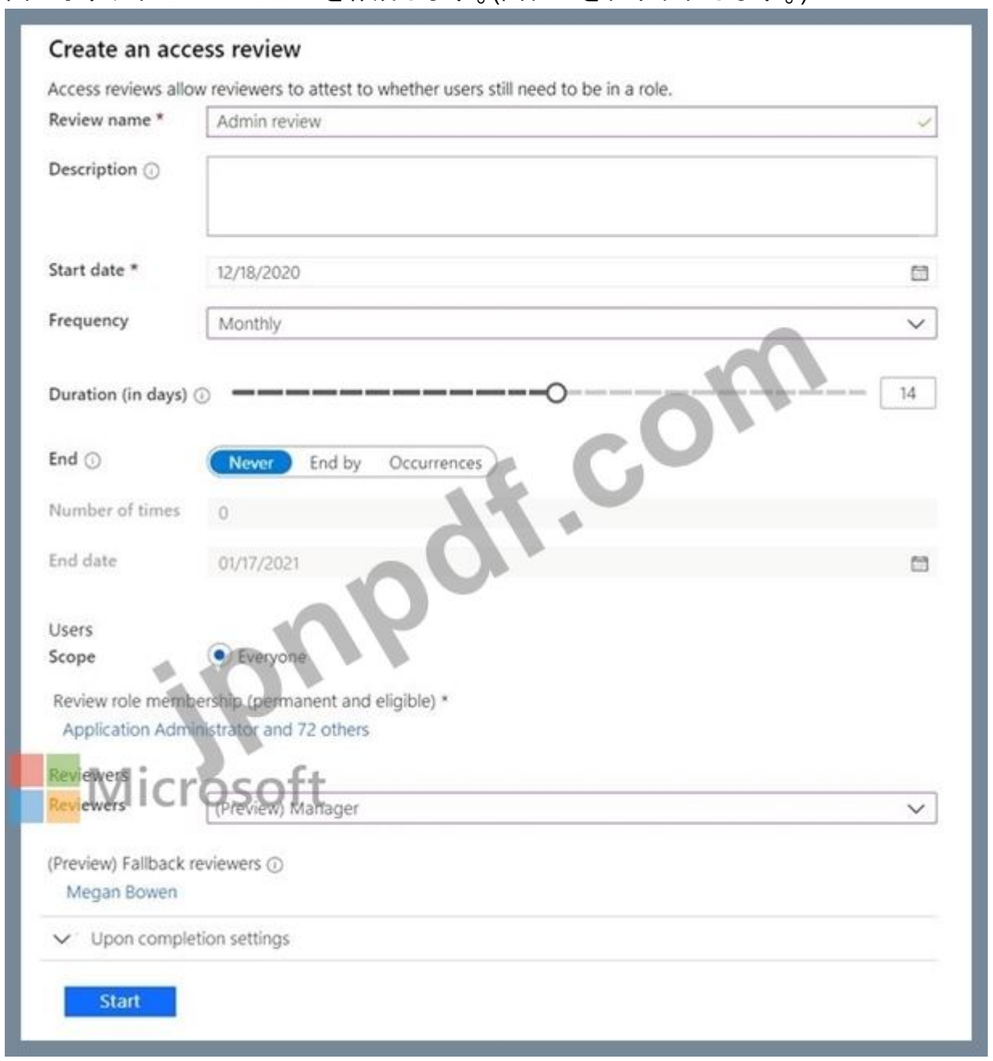
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。質問セットによっては、複数の正解が存在する場合もあれば、正解がない場合もあります。

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。そのため、これらの質問はレビュー画面に表示されません。

Microsoft 365 テナントがあります。

100 人の IT 管理者が 10 の部門に分かれて所属しています。

図に示すアクセス レビューを作成します。(図タブをクリックします。)



すべてのアクセス レビュー リクエストは Megan Bowen 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れるようにする必要があります。
解決策: IT 管理者ユーザー アカウントのプロパティを変更します。
これは目標を満たしていますか?

A. はい

B. いいえ

Answer: A (メーッセージを残す**)**

参照 :

D18912E1457D5D1DDCBD40AB3BF70D5D

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

最新問題**: 323**

注: この問題は、同じシナリオを提示する一連の問題の一部です。一連の問題にはそれぞれ、定められた目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解が存在す

る場合もあれば、正解がない場合もあります。
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。そのため、これらの質問はレビュー画面に表示されません。
Group1 という名前のグループを含む Azure Active Directory (Azure AD) テナントがあります。
Group1 のユーザーに対してのみ多要素認証 (MFA) を有効にする必要があります。
解決策: 多要素認証から一括更新を選択し、Group1 のメンバーを含む CSV ファイルを提供します。
これは目標を満たしていますか?
A. いいえ
B. はい
Answer: (解答を表示する**)**

最新問題**: 324**
ホットスポットに関する質問
Microsoft 36S テナントがあります。
高リスク国のリストを含む、HighRiskCountries という名前の名前付き場所を作成します。
高リスクの国から接続する場合、ユーザーが認証されたままでいられる時間を制限する必要があります。
条件付きアクセス ポリシーでは何を構成す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。
注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area



jpnpdf.com

Answer:

Answer Area

Configure HighRiskCountries by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Configure Sign-in frequency by using:

- A cloud app or action
- A condition
- A grant control
- A session control

Jpnpdf.com

Explanation:

参照：

https://docs.microsoft.com/en-us/azure/active-directory/条件付きアクセス/場所条件

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

最新問題: **325**

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。
次のことを特定する必要があります。
* User1 のアカウントが削除されてから何日後にアカウントを復元できますか?
* 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?
何を特定すべきでしょうか？ 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：正解ごとに1ポイント獲得できます。



Answer:



Explanation:
コンピュータのスクリーンショット 説明は自動的に生成されました



最新問題: **326**
Azure サブスクリプションをお持ちです。

Role1とRole2という2つのカスタムロールを作成する必要があります。ソリューションは以下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。
各ロールにはどのリソース プロバイダーのアクセス許可が必要ですか? 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。
注意: 正しい選択ごとに 1 ポイントが加算されます。
Answer Area



Answer:



最新問題: **327**
litware.com に計画されている変更を適用する必要があります。何を設定すればよいですか？
A. Azure AD テナントと litware.com 間の Azure AD Connect クラウド同期
B. litware.com ドメインを含めるための Azure AD Connect
C. litware.com ドメインの Azure AD Connect のステージング モード
Answer: (解答を表示する**)**
Microsoft SC-300: Identity and Access Administrator 学習ガイドおよび Microsoft Learn モジュール 「Azure AD の同期の実装と管理」によれば、フォレストの信頼を確立せずに複数の Active Directory (AD DS) フォレストからオブジェクトを同期する必要がある場合は、Azure AD Connect Cloud Sync が推奨されるソリューションです。
シナリオでは、adatum.com と litware の間に信頼関係を確立してはならないことが指定されています。
com ですが、A. Datum は litware.com の AD DS ユーザーとグループを既存の Azure AD テナント (adatum.com) に同期する必要があります。
SC-300 トレーニング マテリアルでは次の点が明確にされています。

Azure AD Connect クラウド同期を使用すると、フォレストの信頼や各フォレストへの完全な Azure AD Connect のインストールを必要とせずに、複数の AD フォレストから単一の Azure AD テナントへの同期が可能になります。」ステージング モード (フェールオーバー用のスタンバイ同期サーバーを提供) や同じ Azure AD Connect インスタンスを別のドメインに拡張する (フォレスト間の信頼関係とネットワーク接続が必要) とは異なり、Azure AD Connect クラウド同期では軽量エージェントが使用され、フォレストの信頼に依存しません。
したがって、信頼を作成せずに Litware の AD DS を A. Datum の Azure AD テナントに同期するという要件を満たすには、Azure AD テナントと litware.com ドメインの間に Azure AD Connect Cloud Sync を構成するのが正しい選択です。

最新問題: **328**
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

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 ポイントが加算されます。



Answer:



Explanation:



最新問題: **329**

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はどのように完成させるべきでしょうか？答えは、適切な値を正しいターゲットにドラッグすることです。各値は1回、複数回、または全く使用されない場合があります。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。

注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明

ヌル

"メンバー"

最新問題: **330**

Microsoft 365 テナントがあります。

Azure Monitor を使用して、Azure Active Directory (Azure AD) 監査ログ情報を表示できるようにする必要があります。

まず何をすべきでしょうか?

A. Get-AzureADAuditDirectoryLogs コマンドレットを実行します。

B. Azure AD ブックを作成します。

C. Set-AzureADTenantDetail コマンドレットを実行します。

D. Azure A の診断設定を変更します

Answer: (解答を表示する**)**

最新問題**: 331**

User1 という名前のユーザーを含む contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。

User1 には次の表に示すデバイスがあります。

Name	Platform	Registered in contoso.com
Device1	Windows 10	Yes
Device2	Windows 10	No
Device3	iOS	Yes

2020 年 11 月 5 日に、contoso.com で次の設定の利用規約を作成して適用します。

名前: 用語1

表示名: Contoso 利用規約

ユーザーに利用規約の拡張を要求する: オン

すべてのデバイスでユーザーの同意を求める: オン

同意の有効期限: オン

有効期限: 2020年12月10日

頻度: 毎月

2020年11月15日に、ユーザー1はデバイス3で利用規約1に同意します。

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 ポイントが加算されます。



Answer:



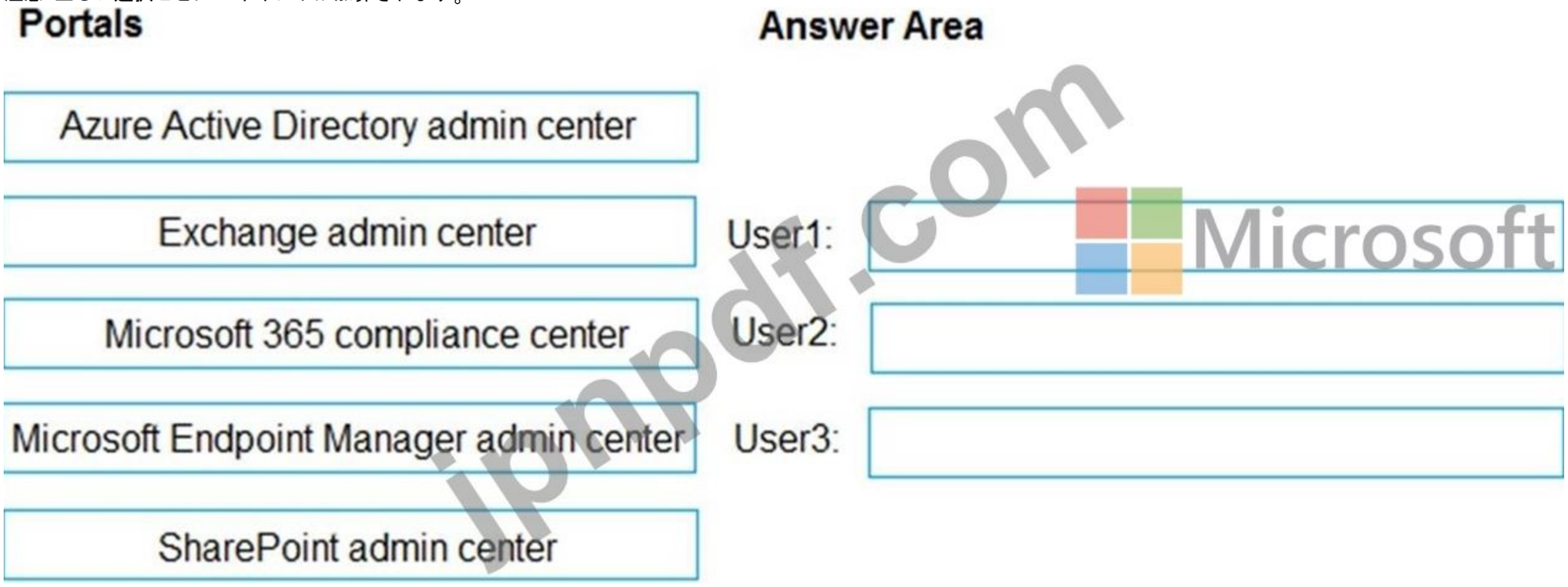
有効な **SC-300** 問題集は GoShiken.com が提供された合格しやすい SC-300 試験問題集！ GoShiken.com が最新の **SC-300** 試験問題集を提供しています。GoShiken.com SC-300 試験問題は最新で、解答が正確でございます。最新の GoShiken.com SC-300 問題集をゲットする人はこちら: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370****30%OFF**問題集溶と正解付きで **30%**ｗ特別割引コード: **Freepdfdumps**)

最新問題**: 332**

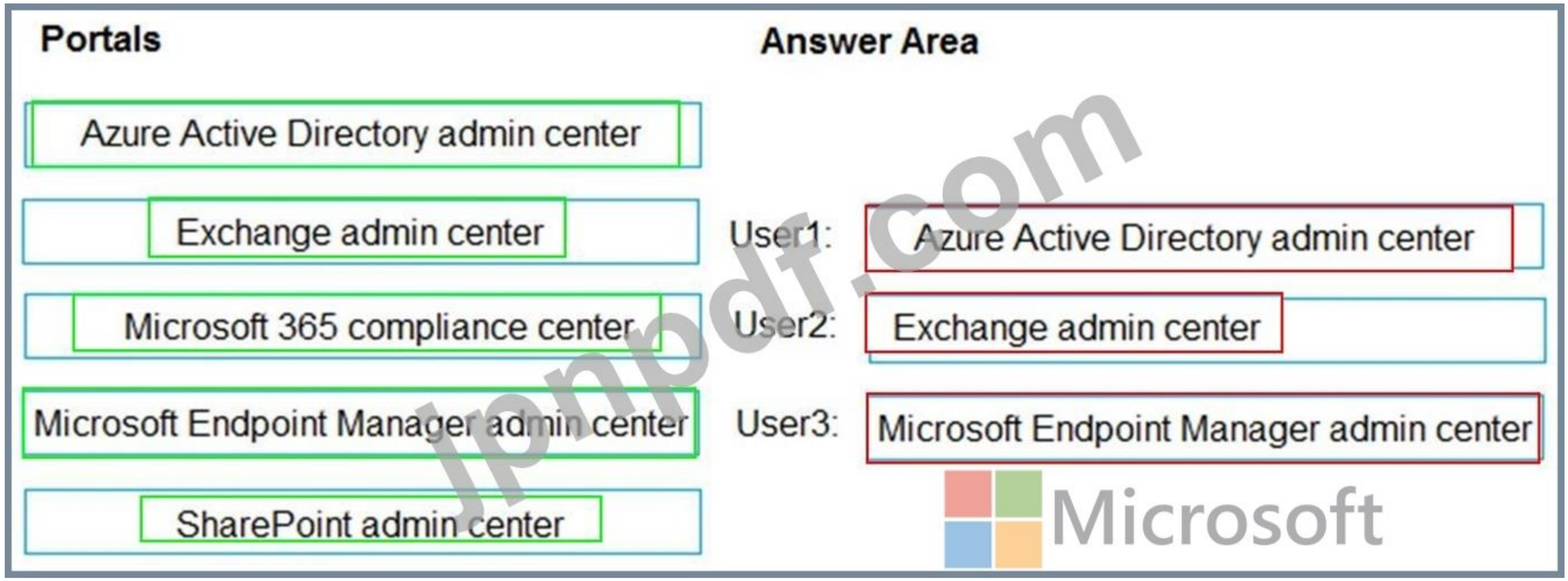
Microsoft 365 E5 サブスクリプションがあり、そこには User1、User2、User3 という名前の 3 人のユーザーが含まれています。
次の表に示すようにユーザーを構成する必要があります。

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

各ユーザーを設定するにはどのポータルを使用すればよいでしょうか？適切なポータルを適切なユーザーにドラッグしてください。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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



Jpnpdf.com

最新問題: **333**
contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。
Azure AD に登録された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. ユーザーリスク条件
C. クライアントアプリの条件
D. サインインリスク条件
Answer: (解答を表示する**)**
説明/参照:
https://docs.microsoft.com/en-us/azure/active-directory/条件付きアクセス/ブロックレガシー認証

最新問題: **334**
Microsoft 365 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

Azure AD で、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何ですか?
A. グループ1とグループ4
B. グループ2のみ
C. グループ3のみ
D. グループ1とグループ2のみ
E. グループ1のみ
Answer: (解答を表示する**)**

最新問題**: 335**
ユーザー管理者ロールの計画された変更を満たす必要があります。
何をすべきでしょうか?
A. アクセスレビューを作成します。
B. ロール設定を変更する
C. 管理者ユニットを作成します。
D. アクティブな割り当てを変更します。
Answer: B (メーッセージを残す**)**
Azure AD ロール向けの Azure AD Privileged Identity Management (PIM) では、試験資料で、ロール設定を編集することで、ロール（ユーザー管理者など）の使用方法をカスタマイズすることが説明されています。これらの設定は、多要素認証の要求、正当化、承認、割り当てなど、アクティベーションの動作を制御します。
アクティベーション期間、通知など、様々な設定が可能です。ガイドでは、管理者は「ロールごとにアクティベーション要件と期限付き資格を設定」し、「アクティベーション時に承認ワークフローとMFAを適用」できるとされています。アクセスレビューは、誰がまだロールを必要としているかを定期的に確認するために使用されますが、ロールのアクティベーション方法に関する運用上の変更は実施しません。「アクティブな割り当て」は、現在アクティブ/資格のある割り当てを保持しているユーザーを表示および変更するだけであり、ロールのアクティベーション動作に関するポリシーを設定するものではありません。
管理単位は特定のディレクトリタスクの範囲を定めますが、PIMのアクティベーション/承認を変更する方法ではありません。
/MFA 要件。したがって、ユーザー管理者ロールの計画的な変更（承認、正当性、MFA による最小権限のアクティブ化など）に対応するには、PIM # Azure AD ロール # ユーザー管理者 # ロール設定を更新します。これは、SC-300 の目標「Azure AD ロールの PIM 設定とポリシーを構成する」と一致しており、アドホックな割り当てではなくポリシーによるガバナンスを確保します。

最新問題**: 336**
Microsoft 365 E5 サブスクリプションをお持ちです。
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 User1 というユーザーが含まれています。
Microsoft Entra Permissions Management を展開する予定です。
User1 が Azure サブスクリプションを Permissions Management にオンボード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 Microsoft Entra ロールはどれですか?
A. アプリケーション管理者
B. グローバル管理者
C. セキュリティ管理者
D. 権限管理管理者

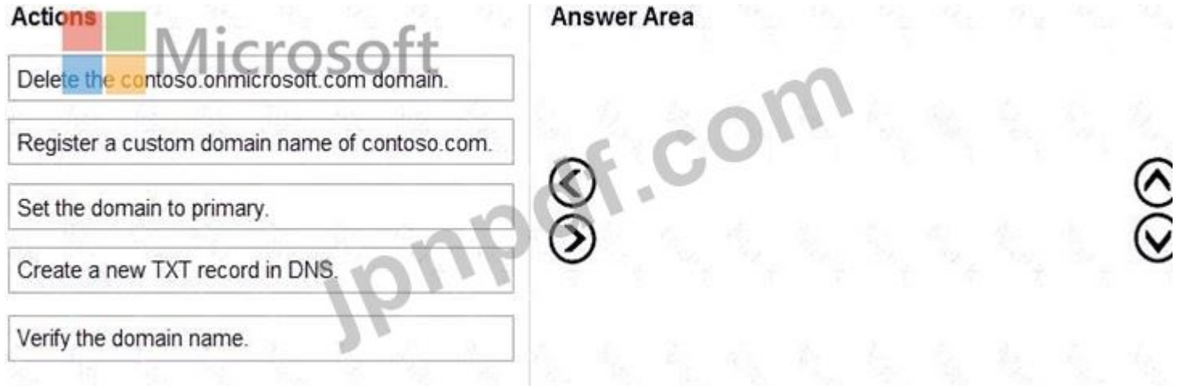
Answer: D (メーッセージを残す)

最新問題: **337**
次の表に示すユーザーを含む Azure AD テナントがあります。

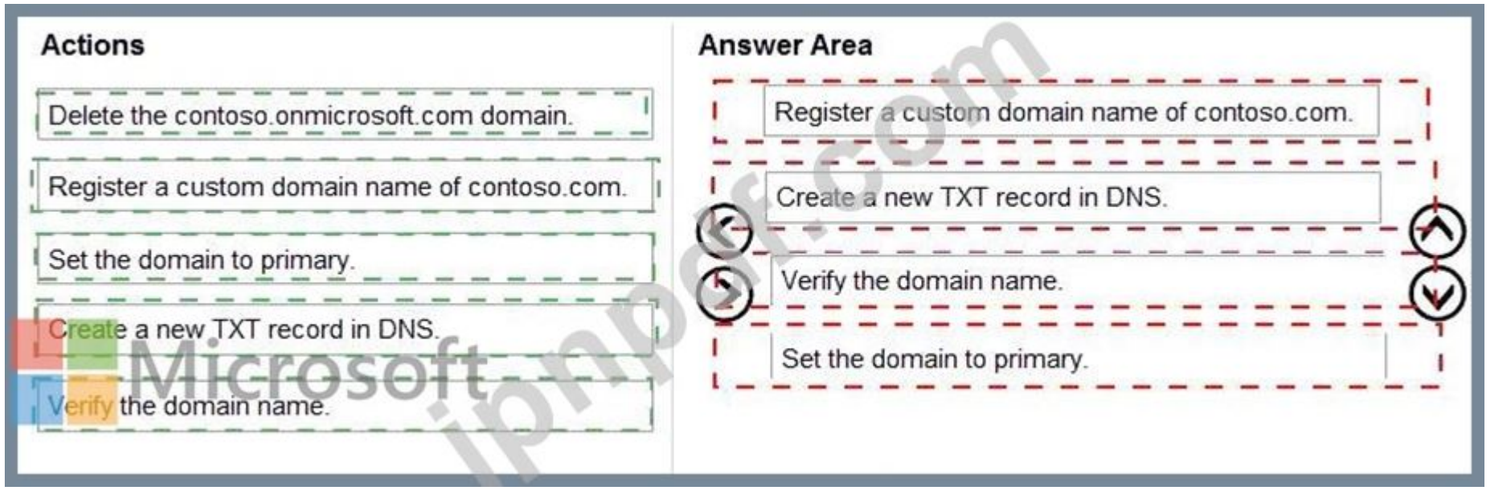
Name	Role
Admin1	User Administrator
Admin2	Password Administrator
Admin3	Application Administrator

各ユーザーのロール権限を比較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。
何を使うべきでしょうか?
A. Microsoft 365 管理センター
B. Microsoft 365 Defender ポータル
C. Microsoft Entra 管理センター
D. Microsoft Purview コンプライアンス ポータル
Answer: (解答を表示する)

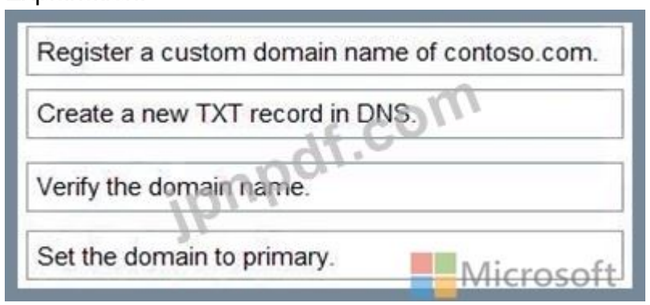
最新問題: **338**
contoso.onmicrosoft.com というドメイン名を使用する新しい Microsoft 365 テナントがあります。
ドメイン レジストラに contoso.com という名前を登録します。
新しい Microsoft 365 ユーザーの既定のドメイン名として contoso.com を使用する必要があります。
どの 4 つのアクションを順番に実行する必要がありますか? 回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



Answer:



Explanation:



参照：
https://practical365.com/office-365 でカスタムドメインを構成する/

最新問題**: 339**
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
User1	Group1
User2	Group2
User3	Group3

テナントには次の表に示す認証方法があります。

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

アプリに表示される番号と携帯電話に表示される番号を照合してクラウド アプリにサインインするユーザーは誰でしょうか?
A. ユーザー2のみ
B. ユーザー2とユーザー3のみ
C. ユーザー3のみ
D. ユーザー1のみ

E. ユーザー1とユーザー2のみ
Answer: (解答を表示する**)**

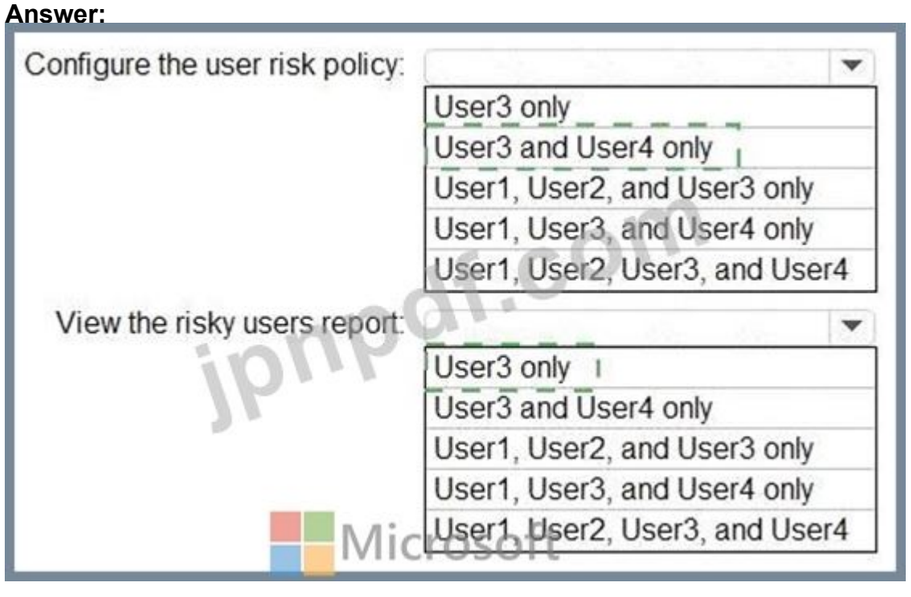
最新問題**: 340**
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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

Azure AD Identity Protection を実装する予定です。
ユーザー リスク ポリシーを構成できるのはどのユーザーですか。また、リスクのあるユーザー レポートを表示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。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



説明
グラフィカルユーザーインターフェース、テキストの説明は自動的に生成されます



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

最新問題: 341
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 Area

Statements	Yes	No
User1 can perform an access review for User1.	○	○
User1 can perform an access review for Managed2.	○	○
User1 can perform an access review for User3.	○	○

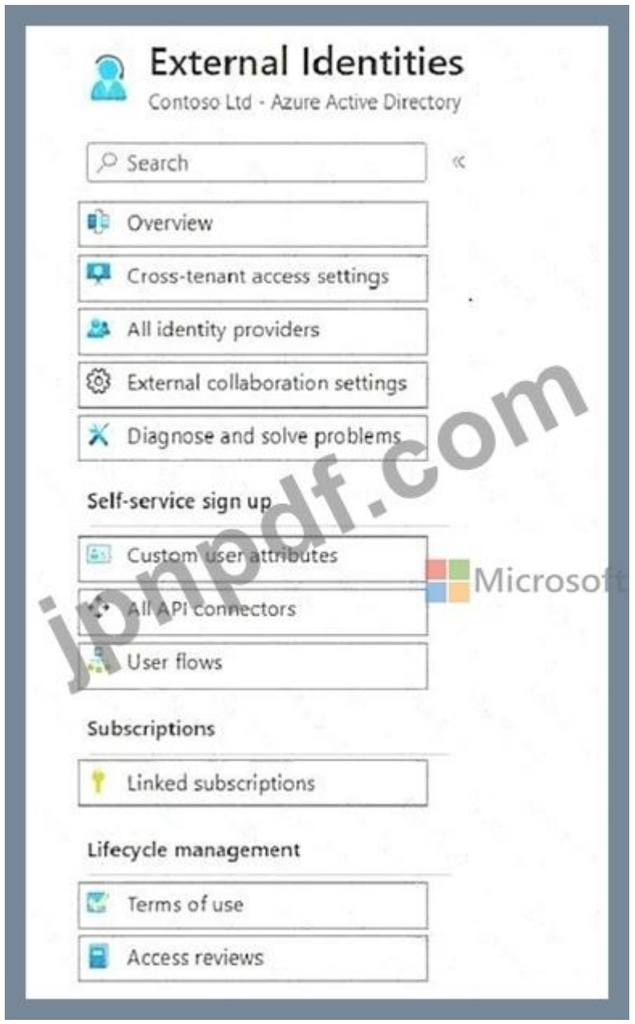
Answer:



Microsoft jpnpdf.com

Explanation:
ユーザー1はユーザー1のアクセスレビューを実行できます: いいえ
User1 は Managed2 のアクセスレビューを実行できます: はい
ユーザー1はユーザー3のアクセスレビューを実行できます: はい
このシナリオでは、次の条件で、Group1 に対して Review1 という名前のアクセス レビューが構成されています。
* レビュー範囲: チーム + グループ
* 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: グループ所有者
* 代替レビュアー: なし
設定により、アクセスレビューのレビュアーはGroup1のオーナーであるUser1とUser4になります。したがって、これら2人のユーザーにはGroup1のメンバー全員をレビューする権限が付与されます。
グループ1には次のメンバーが含まれます。
* User1 (ユーザー、所有者でもある)
* Managed2 (マネージドID)
* グループ2 (ユーザー3を含む)
スコープが 「すべてのユーザー」に設定されているため、社内メンバーと社外メンバーの両方が含まれます。ただし、SC-300資料では、レビュー担当者は自身のアクセスをレビューできないことが強調されています。Microsoft Learnでは次のように記載されています。
「レビュー担当者は、レビュー対象グループのメンバーであっても、アクセスレビューで自身のアクセスを承認または拒否することはできません。」したがって、
* ユーザー1は自分自身をレビューできません # いいえ
* User1 は Managed2 をレビューできます # はい、Managed2 は Group1 のメンバーであるため
* ユーザー1はユーザー3をレビューできます。# はい。ユーザー3はグループ2のメンバーであり、グループ2自体がグループ1のメンバーであるため、ユーザー3のメンバーシップは間接的にレビュー範囲の一部となります。この動作は、レビュー範囲がネストされたグループメンバーも含まれるというSC-300ガイダンスと一致しています。
「すべてのユーザー」およびレビュー担当者 (所有者) は、自分を除くすべてのメンバーを評価できます。

最新問題: **342**
Microsoft Entra テナントがあります。
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
* 月間アクティブユーザー数 (MAU)に基づく価格設定
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 ポイントが加算されます。



jpndf.com
Microsoft

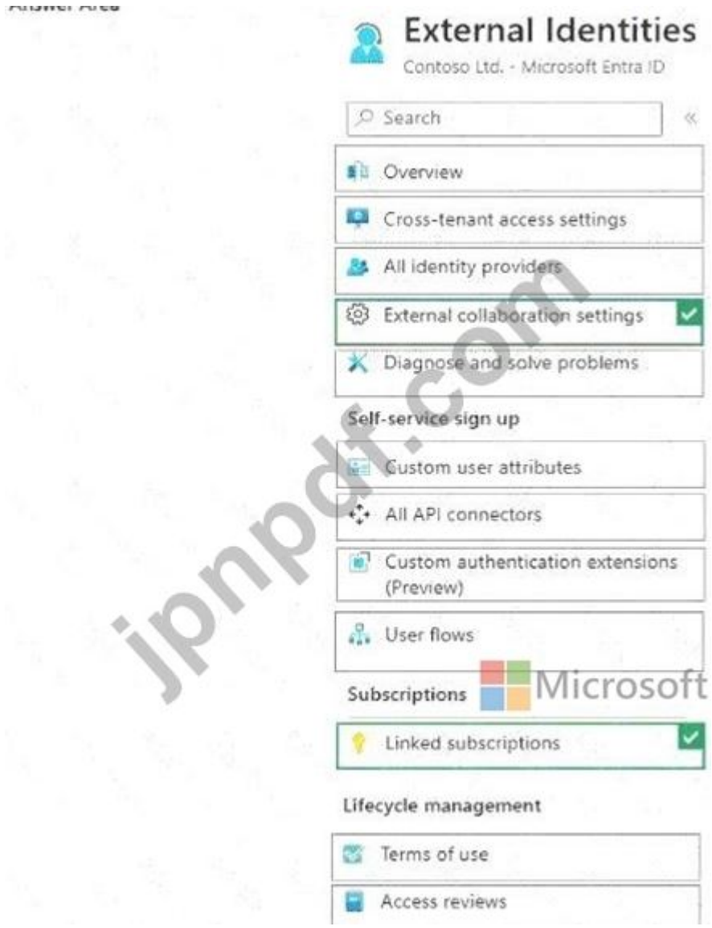
Answer:



jpnpdf.com

Explanation:

Answer Area

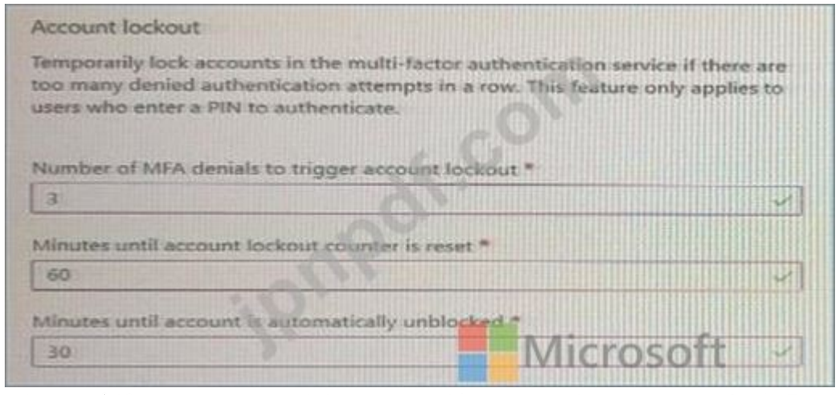


jpnpdf.com
Microsoft

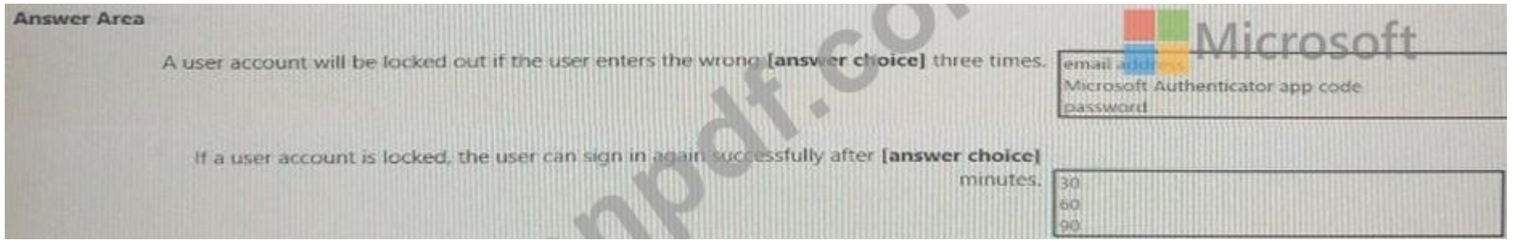
公式の Microsoft Identity and Access Administrator (SC-300) 学習ガイドと Microsoft Learn ドキュメント（『Microsoft Entra ID で外部 ID を管理する」) によると、Microsoft Entra ID の外部 ID により、組織は B2B コラボレーションや B2C セルフサービス サインアップなどの機能を使用して、組織外のユーザーと安全にコラボレーションできるようになります。
必要な 2 つの構成を分析してみましょう。
* B2Bコラボレーション：外部コラボレーション設定ページでは、管理者が外部ユーザー（ゲスト）が社内リソースとどのようにやり取りするかを設定できます。これには、ゲストユーザーの招待、コラボレーションの制限、引き換えポリシー、B2Bユーザーのアクセス権限の設定が含まれます。Microsoftのドキュメントには次のように明記されています。
『外部コラボレーション設定を使用して、ディレクトリ内の B2B コラボレーション ユーザーの動作と制限を管理します。」したがって、B2B コラボレーションを有効化または調整するには、外部コラボレーション設定を構成する必要があります。
* 月間アクティブユーザー数（MAU）ベースの価格設定：Microsoft Entra External Identities の価格は月間アクティブユーザー数（MAU）に基づいており、課金のためにはAzureサブスクリプションにリンクされている必要があります。この設定は『リンクされたサブスクリプション」で確認できます。Microsoft のドキュメントでは以下のように説明されています。
『外部 ID の MAU ベースの課金を有効にするには、[リンクされたサブスクリプション] オプションで Microsoft Entra テナントを Azure サブスクリプションにリンクする必要があります。」サブスクリプションをリンクすると、Microsoft は MAU 料金モデルに合わせて、毎月のアクティブな外部ユーザー数に基づいて課金できるようになります。
したがって：
* B2Bコラボレーション # 外部コラボレーション設定
* MAUベースの価格設定 # リンクされたサブスクリプション

最新問題: **343**

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 ロックアウト設定は、次の図に示すように構成されます。



ドロップダウン メニューを使用して、グラフィックに表示された情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが加算されます。



Answer:



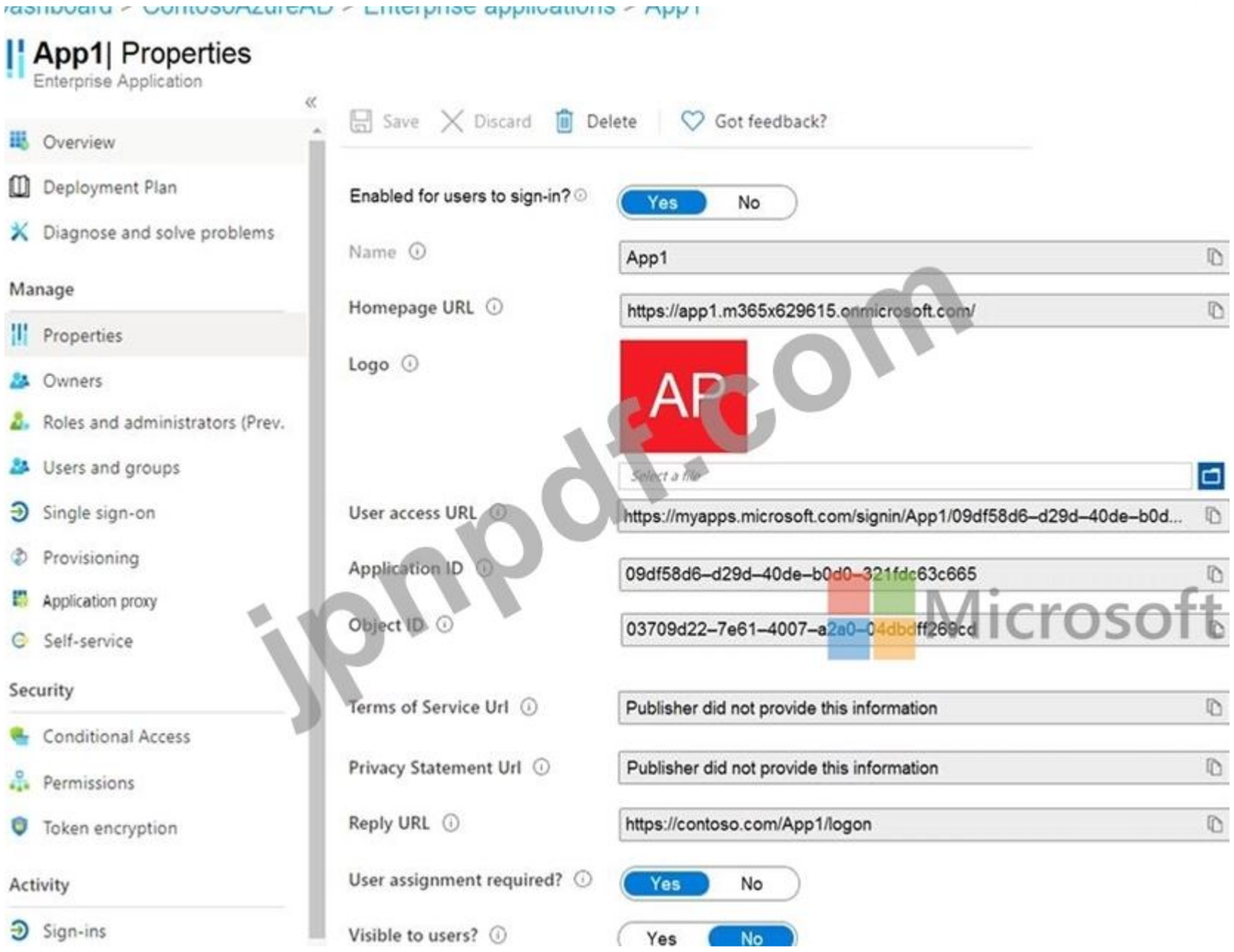
最新問題: **344**
ユーザー管理者ロールの計画された変更を満たす必要があります。
何をすべきでしょうか?
A. アクセスレビューを作成します。
B. ロール設定を変更する
C. 管理者ユニットを作成します。
D. アクティブな割り当てを変更します。
Answer: (解答を表示する**)**
ロール設定の詳細は次のとおりです: ロール設定の詳細 - ユーザー管理者 Privileged Identity Management | Azure AD ロール 既定の設定 状態 アクティベーション時に理由を要求する はい アクティベーション時にチケット情報を要求する いいえ アクティベーション時に Azure MFA を要求する はい アクティベーションに承認を要求する いいえ 承認者 なし
トピック3、概要
データム環境
A. Datum のオンプレミス ネットワークには、adatum.com という名前の Active Directory ドメイン サービス (AD DS) フォレストが含まれています。

テナントには次の表に示すユーザーが含まれます。
問題ステートメント
* 営業部門の複数のユーザーが最大5台のデバイスを所有しています。営業部門のユーザーからは、デバイス数の上限に達したため、Azure ADテナントにデバイスを追加するためにサポート部門に連絡しなければならないことがあるという報告があります。
* 最近のセキュリティインシデントでは、複数のユーザーが認証情報を漏洩し、サインインに疑わしいブラウザが使用され、匿名のIPアドレスからリソースにアクセスされたことが明らかになりました。
* デバイス管理者ロールを IT_Group1 に割り当てようとすると、選択リストにグループが表示されません。
* 組織内の誰でも、他のゲストや管理者以外のユーザーも含め、ゲスト ユーザーを招待できます。
* ヘルプデスクはユーザーのパスワードのリセットに時間がかかりすぎます。
* 現在、ユーザーは認証にパスワードのみを使用します。
要件
A、Datum は以下の変更を実施する予定です。
* セルフサービス パスワード リセット {SSPR} を構成します。
* すべてのユーザーに対して多要素認証 (MFA) を構成します。
* Package1 という名前のアクセス パッケージのアクセス レビューを構成します。
* 組織データへのアプリケーション アクセスには管理者の承認が必要です。
* AD DS ユーザーと groupsoflitware.com を Azure AD テナントと同期します。
* 特定の管理者ロールが割り当てられているユーザーのみがゲスト ユーザーを招待できるようにします。
* Azure AD に参加または登録できるデバイスの最大数を 10 に増やします。
技術要件
* ユーザー管理者ロールを割り当てられたユーザーは、最大 1 年間、必要に応じてロールを使用する権限をリクエストできる必要があります。
* ユーザーには MFA への登録を促すプロンプトが表示され、猶予期間中に登録をバイパスするオプションが提供される必要がある。
* SSPRを使用してパスワードをリセットするには、ユーザーは1つの認証方法を提供する必要があります。利用可能な方法には以下が含まれます。
* メールアドレス
* 電話
* セキュリティに関する質問
* Microsoft Authenticator アプリ
* adatum.com と litware.com AD DS ドメイン間に信頼関係を確立してはなりません。
* 最小権限の原則を使用する必要があります。

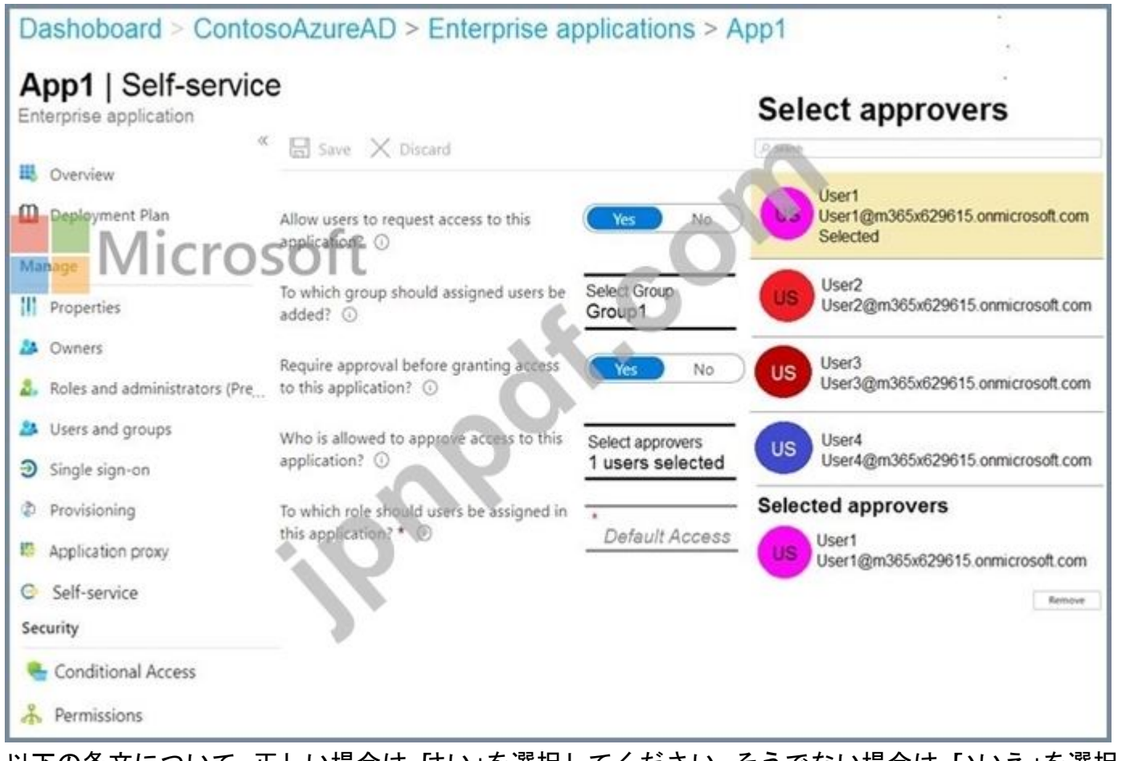
最新問題: **345**
Group1 の図に示すように、Group1 という名前のグループを含む Microsoft 365 テナントがあります。([Group1] タブをクリックします。)



App1 のプロパティ」の図に示すように、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 のセルフサービスは、App1 セルフサービス」の図に示すように構成します。(App1 セルフサービス」タブをクリックします。)



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 ポイントが加算されます。

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Answer:

Answer Area

Statements	Yes	No
The members of Group3 can access App1 without first being approved by User1.	○	○
After you configure self-service for App1, the owner of Group1 is User1.	○	○
App1 appears in the Microsoft Office 365 app launcher of User4.	○	○

Valid SC-300 Dumps shared by GoShiken.com for Helping Passing SC-300 Exam! GoShiken.com now offer the **newest SC-300 exam dumps**, the GoShiken.com SC-300 exam **questions have been updated** and **answers have been corrected** get the **newest** GoShiken.com SC-300 dumps with Test Engine here: https://www.goshiken.com/Microsoft/SC-300-mondaishu.html (**370** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)