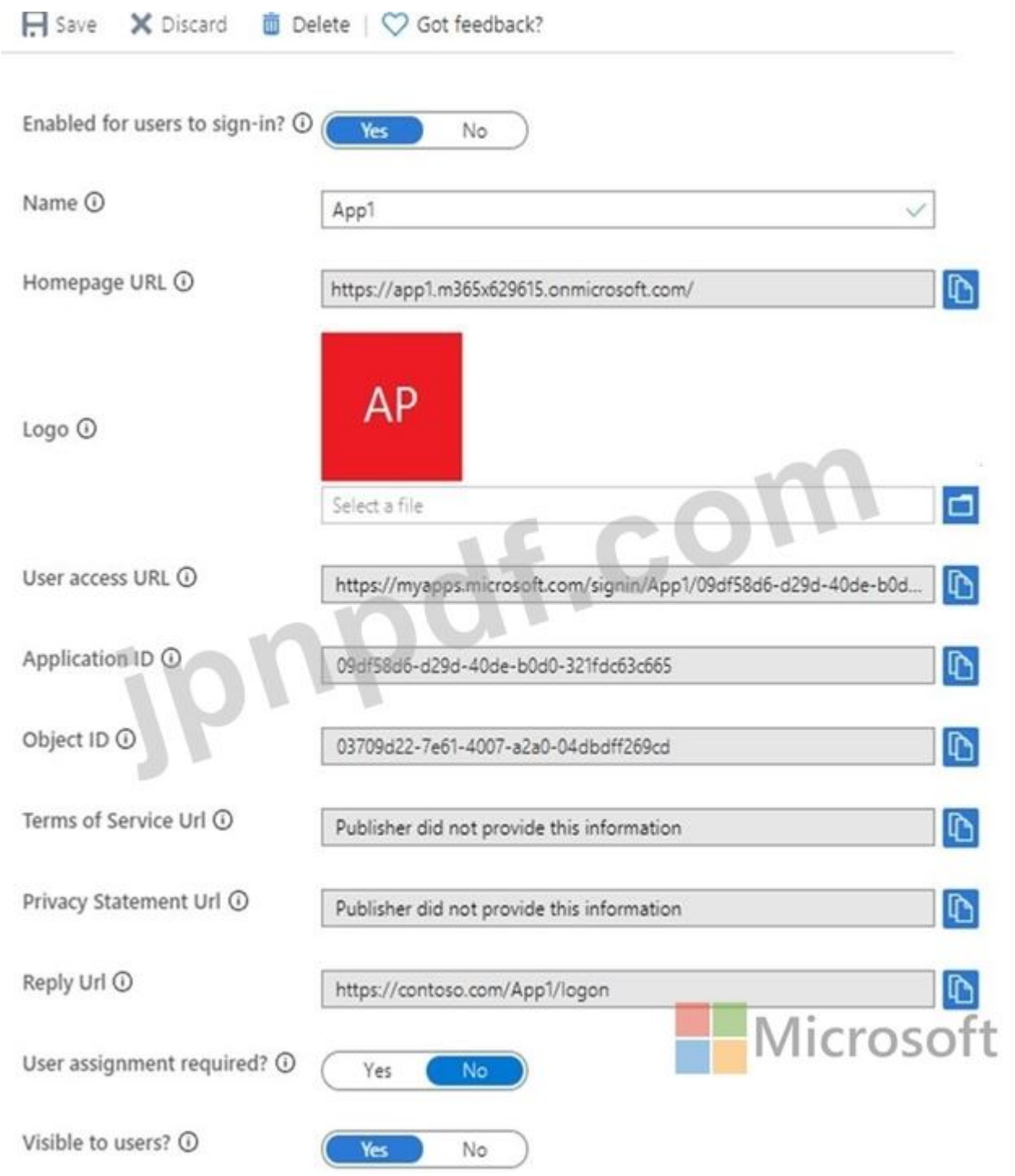
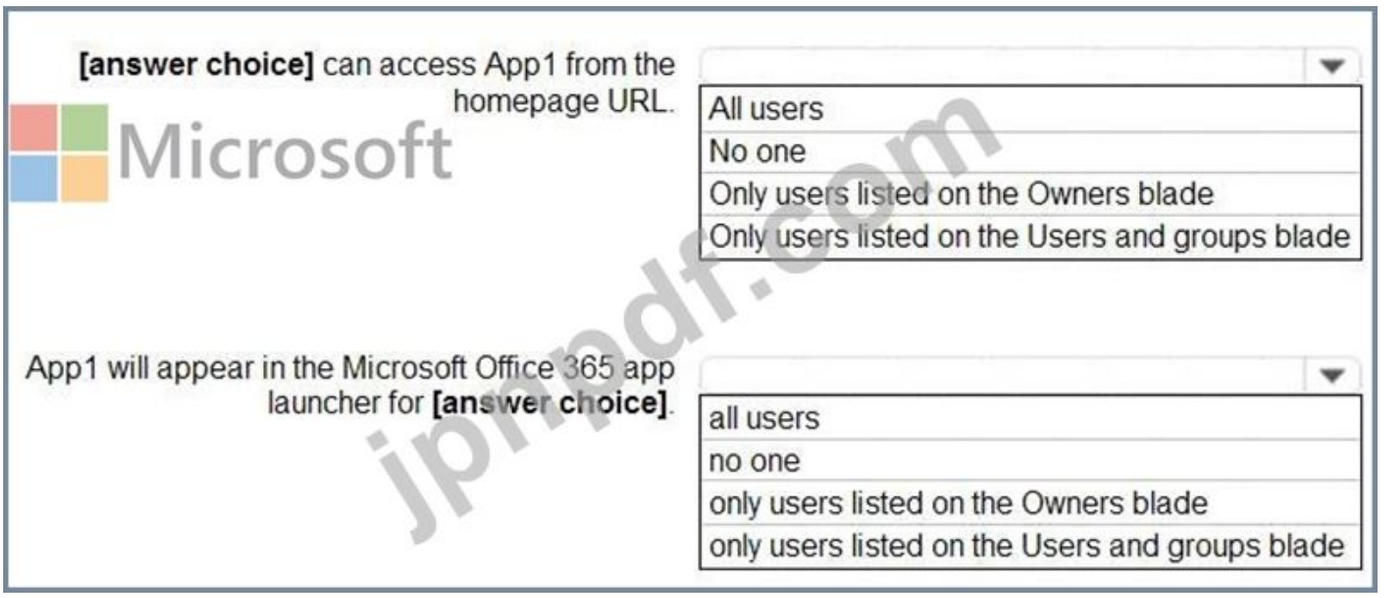
Microsoft.SC-300.v2025-01-27.q108

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:	108
バージョン:	v2025-01-27
アクセス数:	2724
ページビュー数:	1080
https://www.jpnpdf.com/Microsoft.SC-300.v2025-01-27.q108-mondaishu.html	

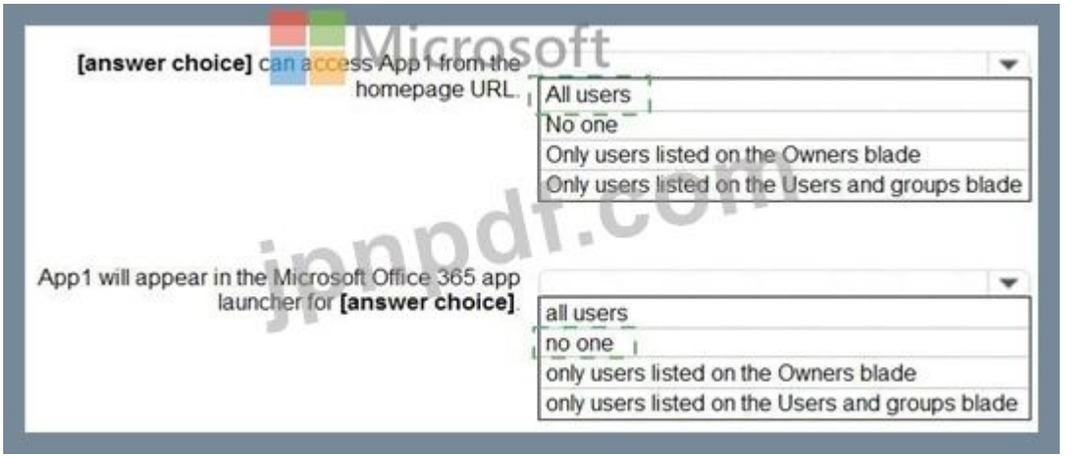
最新問題: **1**
Azure Active Directory (Azure AD) に登録されている App1 という名前のカスタム クラウド アプリがあります。
App1 は次の図に示すように構成されています。



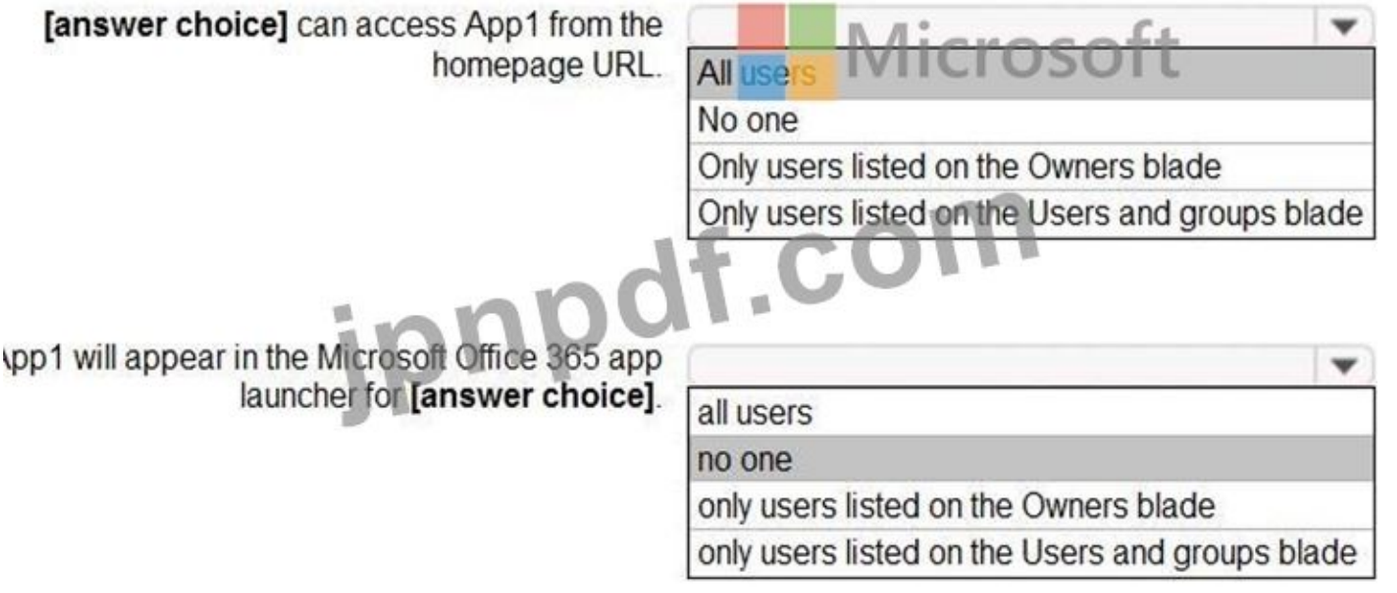
ドロップダウン メニューを使用して、グラフィックに表示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



説明



参照：

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

最新問題**: 2**

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

Name	Type
User1	Member
User2	Member
User3	Guest

Contoso.com には、次の表に示すグループが含まれています。

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

contoso.com から fabrikam.com へのテナント間同期を構成し、User3 と Group2 のテナント間同期を有効にします。

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:

最新問題: **3**
Azure Active Directory (Azure AD) テナントがあります。
リスク検出レポートを開きます。
どのリスク検出タイプがユーザーリスクとして分類されますか?
A. 不可能な旅行
B. 匿名IPアドレス
C. 非典型的な旅行
D. 漏洩した資格情報
Answer: D (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

最新問題: **4**
User1 という名前のユーザーと、次の表に示す条件付きアクセス ポリシーを含む Azure AD テナントがあります。

Name	Status	Conditional Access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

User1 がさまざまな IP アドレスからサインインしようとしたときに、User1 に適用されるポリシーを評価する必要があります。
どの機能を使用すべきでしょうか?
A. Microsoft 365 ネットワーク接続テスト ツール
B. What If ツール
C. アイデンティティセキュリティスコア
D. アクセスレビュー
Answer: B (メーッセージを残す**)**

最新問題: **5**
A Datum ユーザーにライセンスを提供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. OU
C. 配布グループ
D. 行政単位
Answer: (解答を表示する**)**
トピック 1、Contoso, Ltd

概要
Contoso, Ltd 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。Fabcricam には、fabrikam.com という Azure Active Diretory (Azure AD) テナントがあります。
既存の環境
Contoso のオンプレミス ネットワークには、contos.com という名前の Active Directory ドメインが含まれています。このドメインには、Contoso_Resources という名前の組織単位 (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

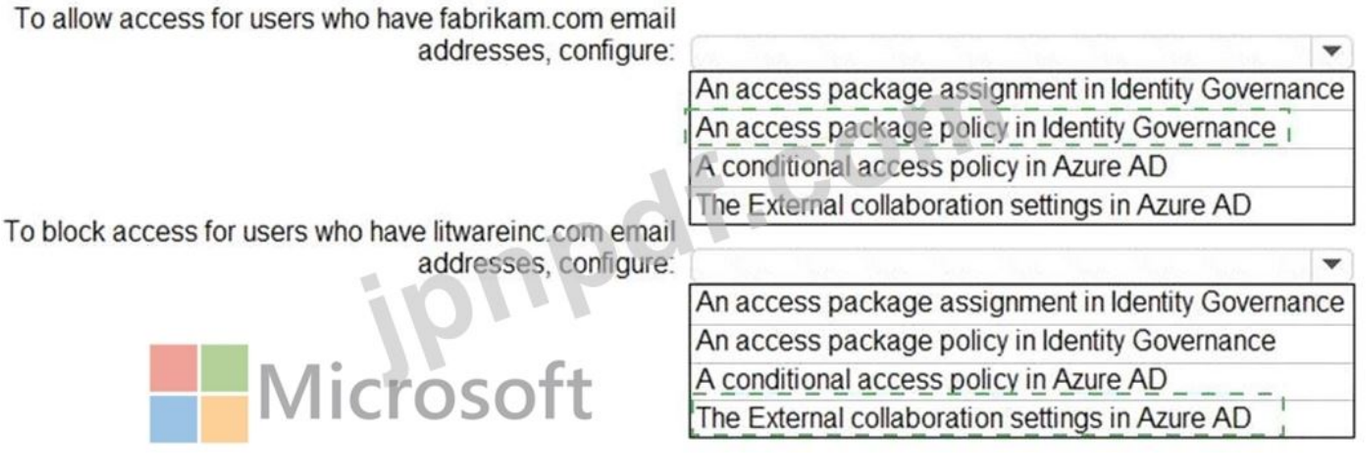
Microsoft 365/Azure 環境
Contoso には、次のライセンスが関連付けられている Contoso.com という名前の Azure AD テナントがあります。
* マイクロソフト Office 365 エンタープライズ E5
* エンタープライズモビリティ + セキュリティ
* Windows 10 エンタープライズ E5
* プロジェクト計画3
Azure AD Connect は、Azure AD と Active Directory Domain Serverless (AD DS) の間で構成されます。Contoso Resources OU のみが同期されます。
ヘルプデスク管理者は、ユーザー設定を管理するために Microsoft 365 管理センターを定期的に使用します。
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。すべてのユーザーには、次の例外を除き、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 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。次の例外を除き、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、プロジェクト管理者ロールに Azure AD Privileged Identity Management (PIM) を使用します。
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であると報告しています。
* 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しいユーザーのライセンス割り当てを簡素化します。Fabrikam のユーザーと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に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 は Corporation という会社を買収する予定です。Adatum という Active Directory OU に 100 人の新しい A Datum 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います。
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。

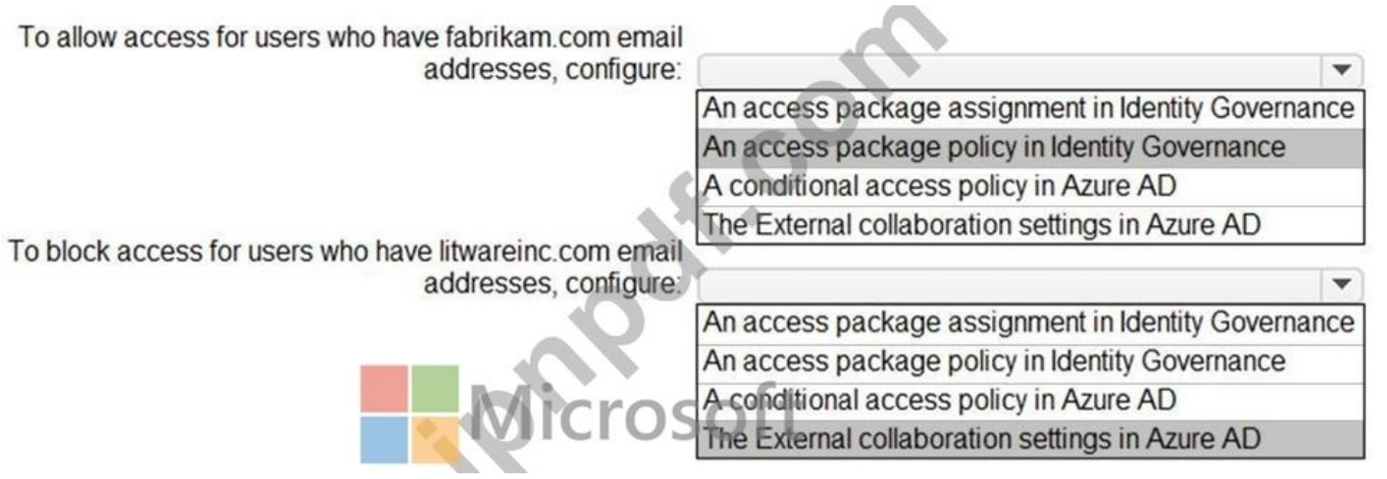
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* ヘルプデスク管理者は、それぞれのオフィス内のユーザーのライセンスのみを管理できる必要があります。
* ユーザーの個人情報が漏洩した可能性がある場合、ユーザーにパスワードの変更を強制する必要があります。

最新問題: **6**
あなたの会社には、contoso.com という名前の Azure Active Directory (Azure AD) テナントがあります。この会社には、Fabrikam, Inc. という名前のビジネス 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 の 2 つの検証済みドメイン名を持っています。両方のドメイン名が Fabrikam の電子メール アドレスに使用されます。
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 にアクセスできるのは、fabrikam.com の電子メール アドレスを持つユーザーのみであることを確認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 ポイントが付与されます。

Answer:

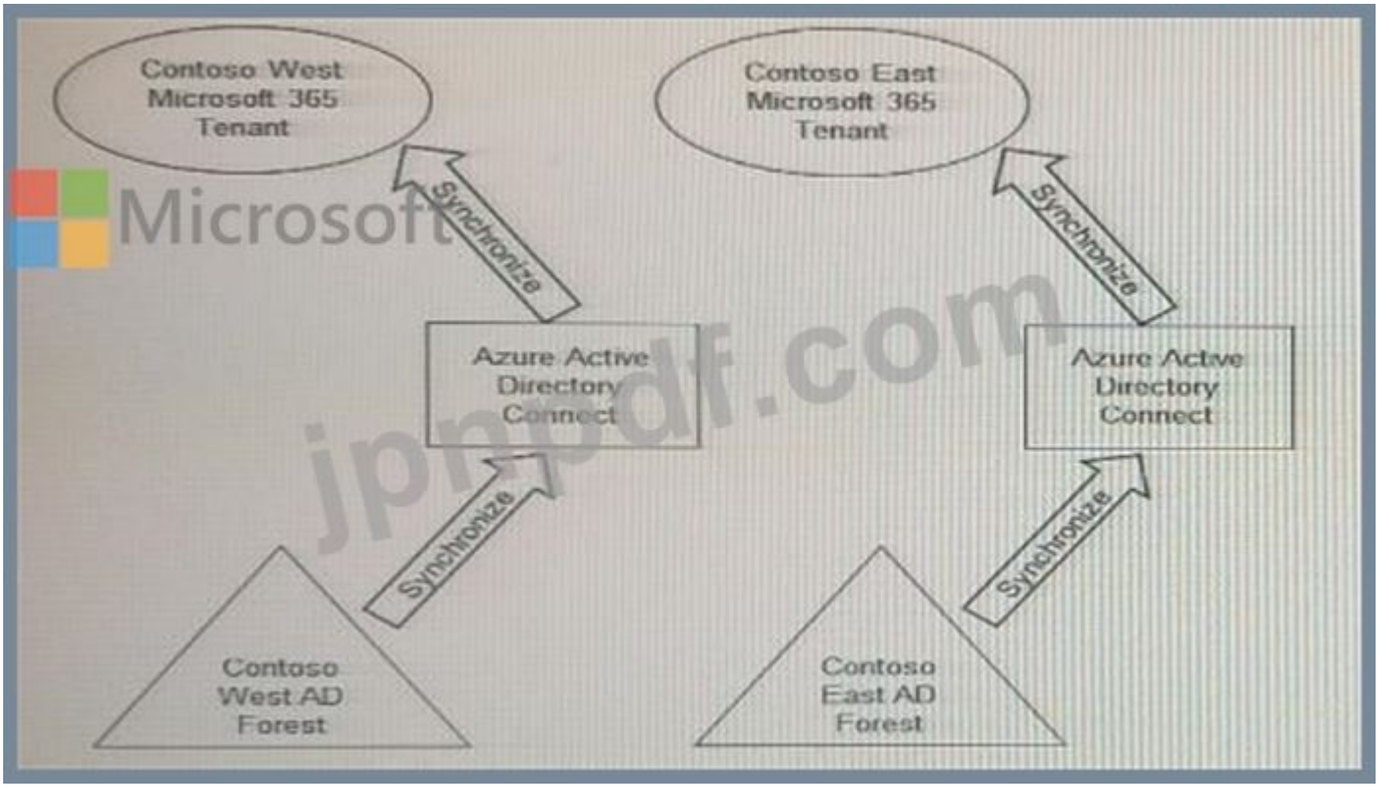


説明
テキストの説明は自動的に生成されます



参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-req
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-cre

最新問題**: 7**
会社には、Contoso East と Contoso West という 2 つの部門があります。両方の部門の Microsoft 365 ID アーキテクチャを次の図に示します。



Contoso East 部門のユーザーに、Contoso West テナントの Microsoft SharePoint Online サイトへのアクセスを割り当てる必要があります。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. 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。

B. 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。

C. 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。

D. Contoso East ユーザーを Contoso West テナントのゲストとして招待します。

Answer: D (メーッセージを残す)

最新問題**: 8**

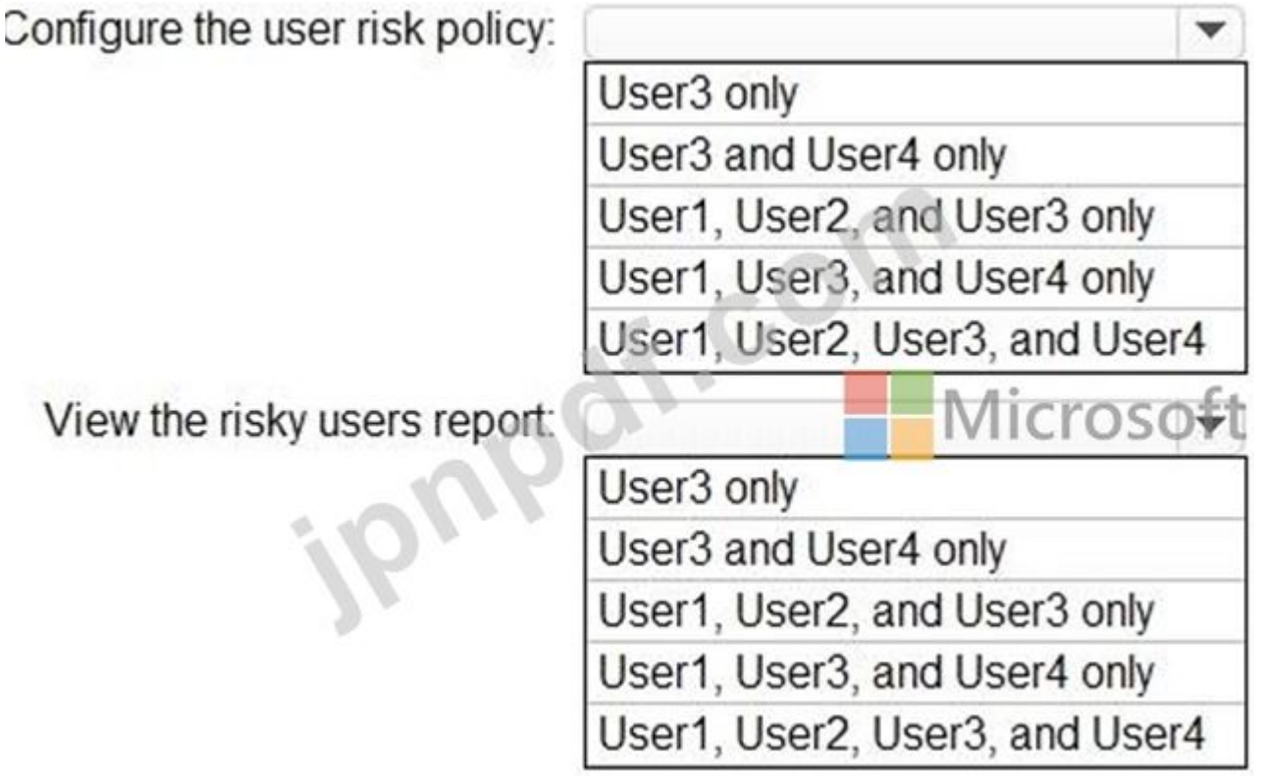
次の表に示すユーザーを含む Azure Active Directory (Azure AD) テナントがあります。

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ます。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

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

最新問題**: 9**
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。
次の各文について、正しい場合は 「はい」を選択してください。そうでない場合は 「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

説明

最新問題: **10**

あなたの会社には Microsoft 365 テナントがあります。

この会社には 300 人のユーザーがいるコール センターがあります。コール センターでは、ユーザーはデスクトップ コンピューターを共有しており、毎日異なるコンピューターを使用する場合があります。コール センターのコンピューターは生体認証用に構成されていません。

ユーザーはコールセンター内に携帯電話を持ち込むことが禁止されています。

コールセンターのユーザーがMicrosoftにアクセスするときに多要素認証 (MFA) を要求する必要があります。

365

サービス。

ソリューションには何を含めるべきですか?

A. 名前付きネットワークロケーション

B. Microsoft Authenticator アプリ

C. Windows Hello for Business 認証

D. FIDO2 トークン

Answer: D (メーッセージを残す)

説明

https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-passwordless

最新問題**: 11**

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。

パ55w0rd12

パ55w0rd12

パ55w0rd12

パ55w.rd12

Pa55w.rd123

Pa55w.rd123

Pa55w.rd123

パ55ワード12

パ55ワード12

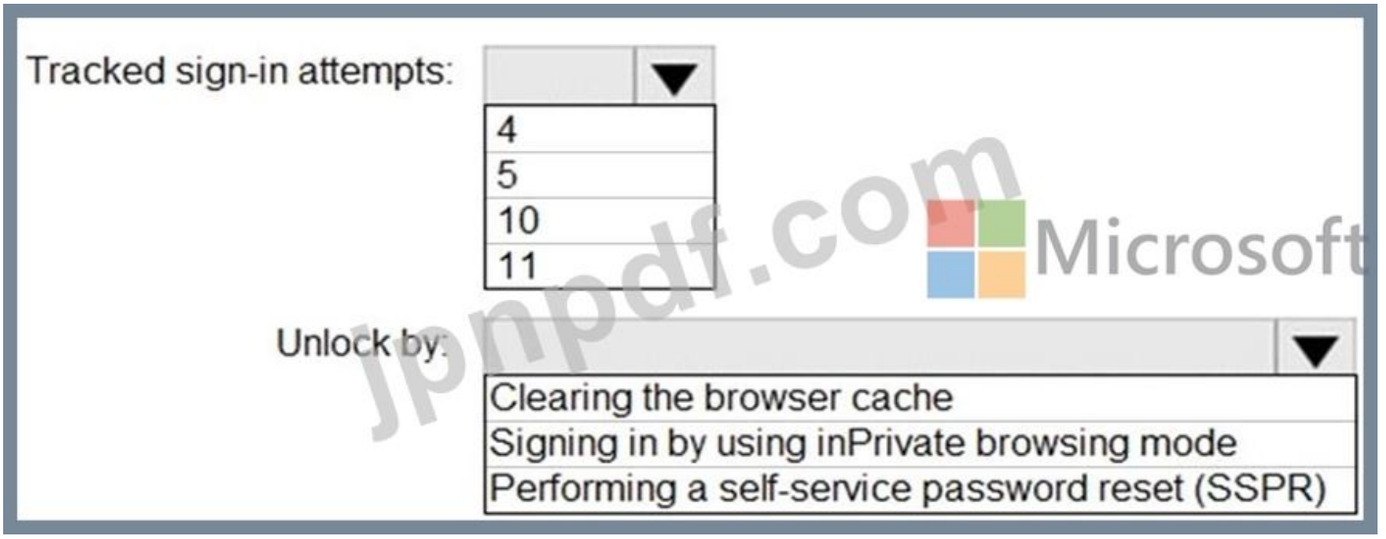
パ55ワード12

パ55w.rd12

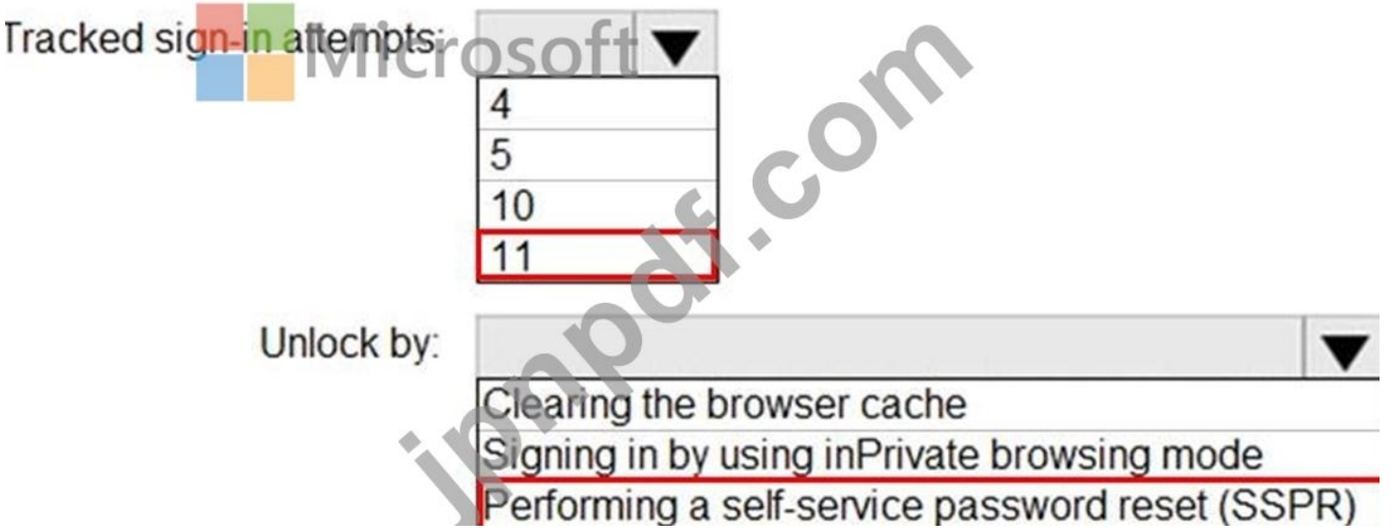
User1 に対して追跡されたサインイン試行の回数と、300 秒のロックアウト期間が終了する前に User1 がアカウントのロックを解除する方法を特定する必要があります。

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 ポイントが付与されます。



Answer:

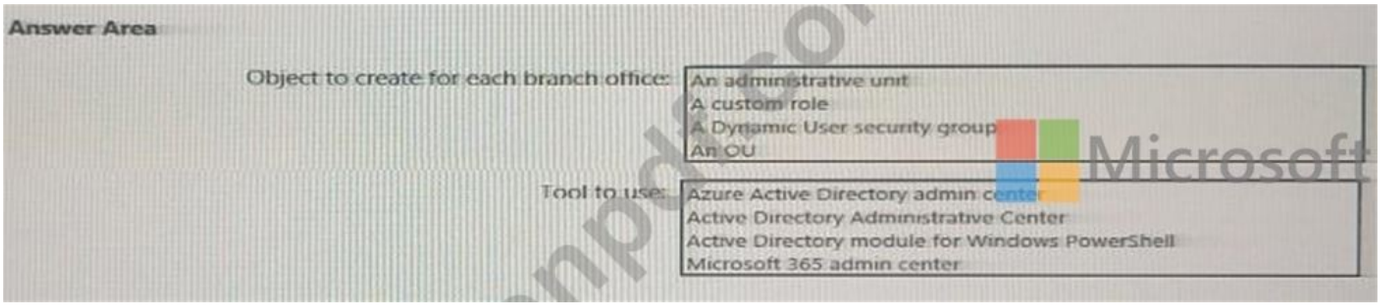


参照：
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment

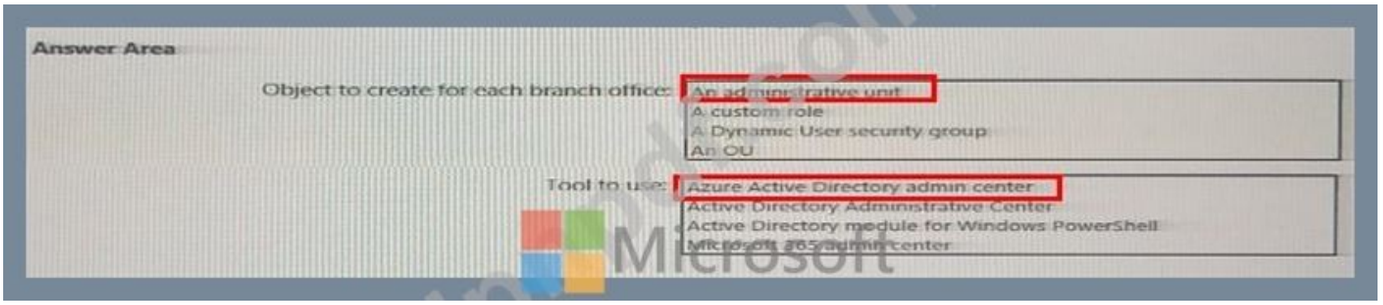
最新問題**: 12**
SSPR の計画された変更を実装します。
User3 が SSPR を使用しようとすると何が起こりますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:
下記の説明の回答を参照してください。
Explanation:
答えは

最新問題**: 13**
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 ポイントが付与されます。



Answer:



トピック3、

概要

データ環境

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は、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、デバイス制限に達したため、サポート部門に連絡してデバイスを Azure AD テナントに参加させる必要がある場合があると報告されています。
* 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を含め、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ています。

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。

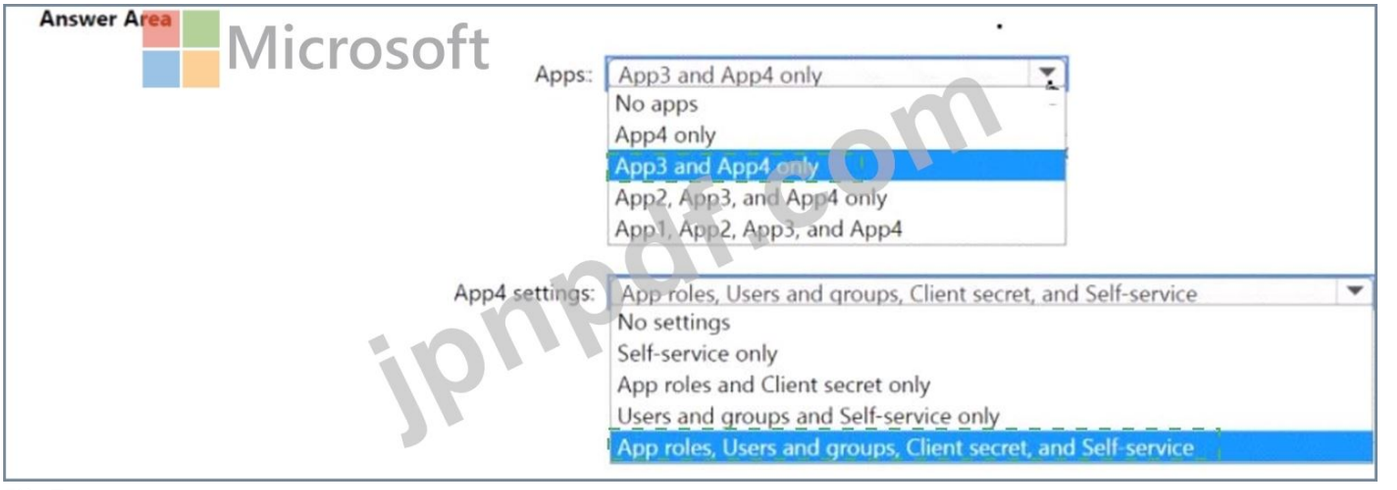
* 特定の管理者ロールが割り当てられているユーザーのみがゲスト ユーザーを招待できるようにします。
* Azure AD に参加または登録できるデバイスの最大数を 10 に増やします。
技術要件
* ユーザー管理者ロールを割り当てられたユーザーは、最大 1 年間、必要に応じてロールを使用する権限を要求できる必要があります。
* ユーザーに対して MFA の登録を促すプロンプトを表示し、猶予期間中に登録をバイパスするオプションを提供する必要があります。
* ユーザーは、SSPR を使用してパスワードをリセットするために、1 つの認証方法を提供する必要があります。使用可能な方法には次のものが含まれます。
* 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**: 14**
Azure AD テナントがあります。
次の表に示すタスクを実行します。

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service.

4 月 5 日に、管理者は App1、App2、App3、および App4 を削除します。
アプリと設定を復元する必要があります。
4 月 16 日に復元できるアプリはどれですか。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 ポイントが付与されます。

Answer:



説明

携帯電話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**: 15**

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 ポイントが付与されます。

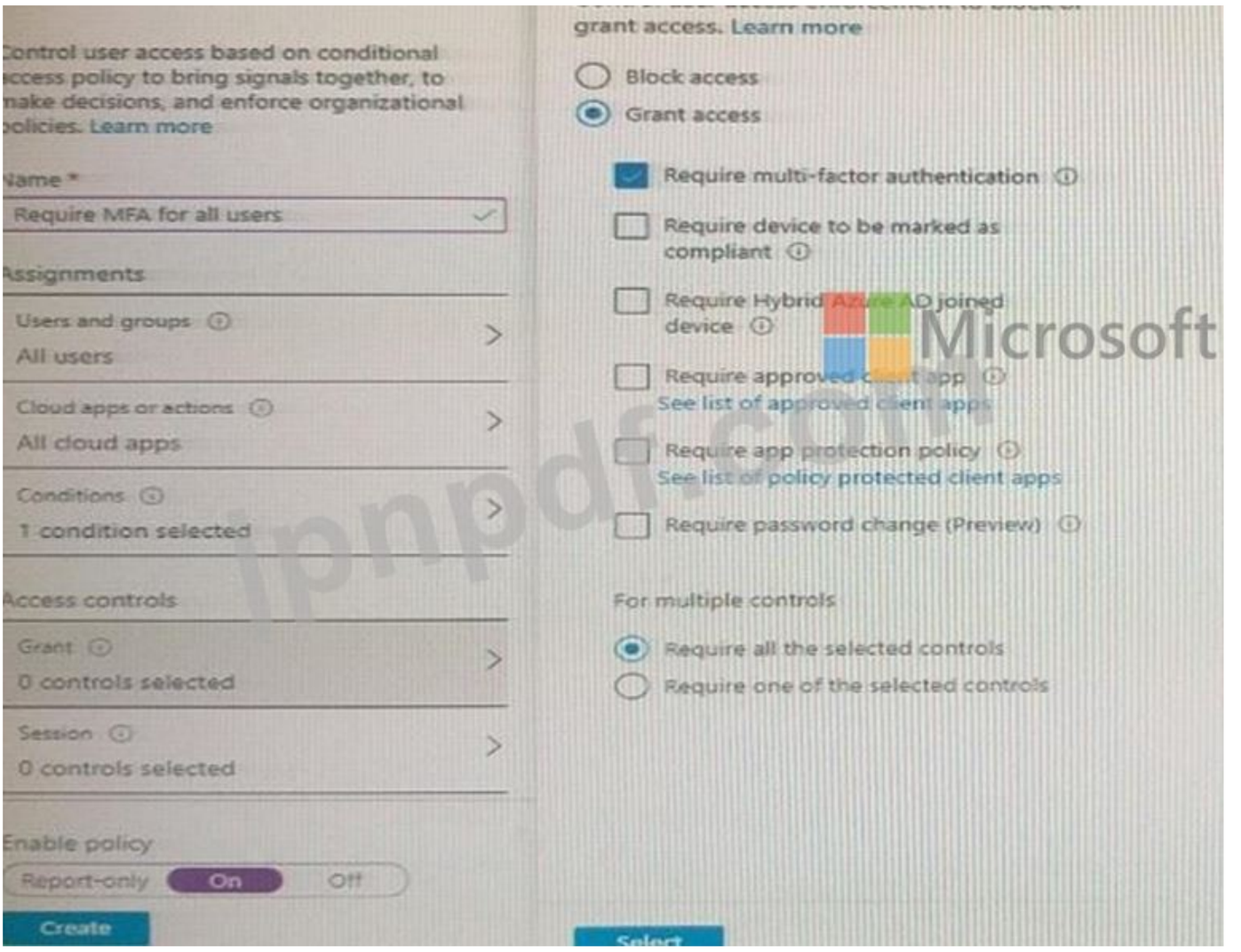
Answer:

最新問題: **16**
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。

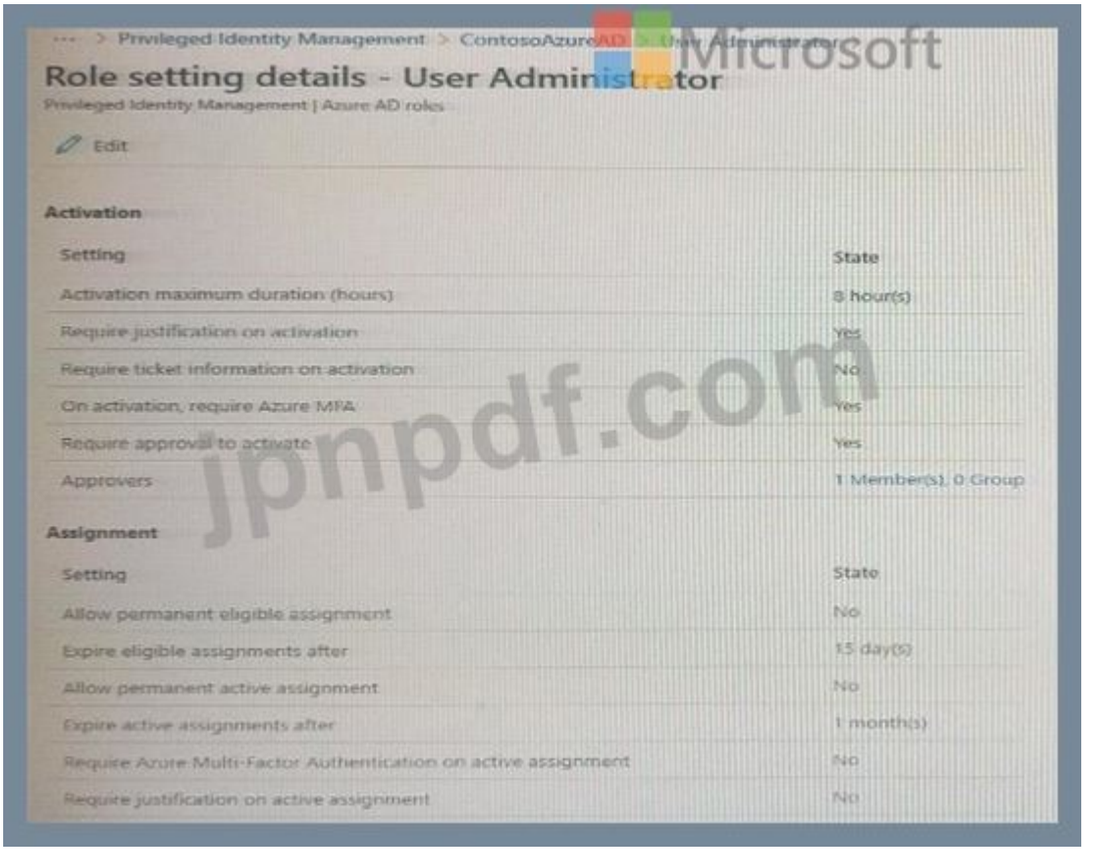
Name	Role
Admin1	Account Administrator
Admin2	Service Administrator
Admin3	SharePoint Administrator

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. 管理者のみ
B. 管理者1、管理者2、管理者3
C. Admin3のみ
D. 管理者2のみ
E. Admin2 と Admin3 のみ
F. Admin1 と Admin2 のみ
Answer: F (メーッセージを残す**)**

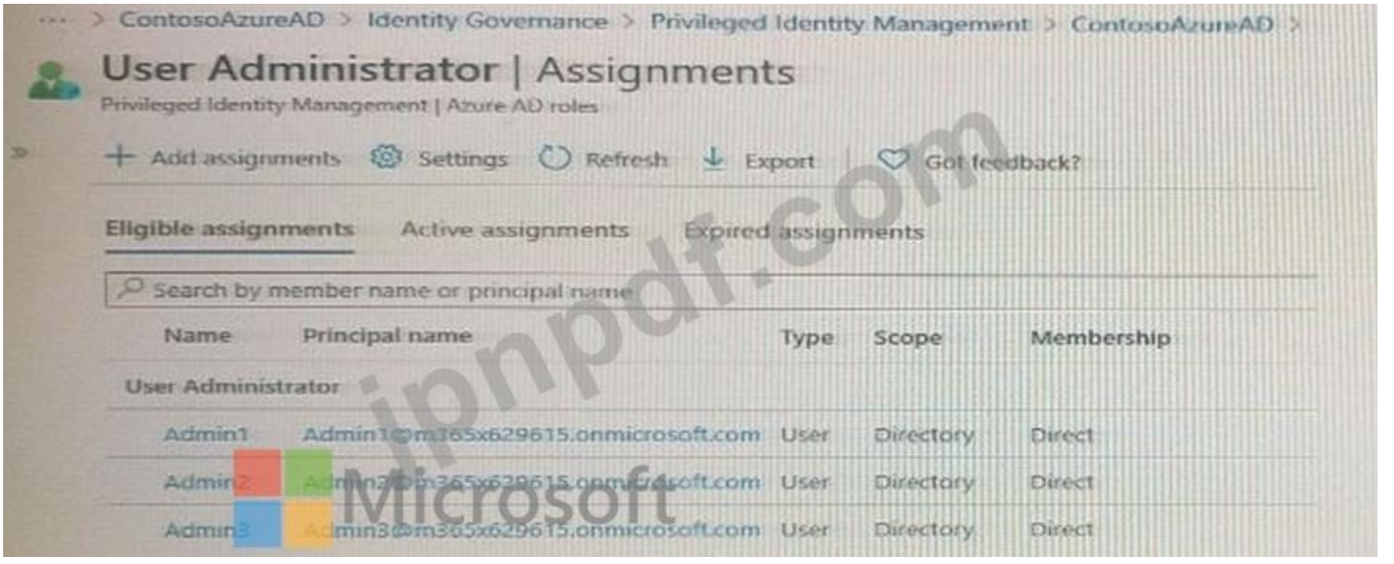
最新問題: **17**
Microsoft 365 テナントがあります。
条件付きアクセス ポリシーは、条件付きアクセス ポリシーの図に示すように構成します。([条件付きアクセス ポリシー] タブをクリックします。)



ユーザー管理者ロール設定は、ロール設定の詳細図に示す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。)



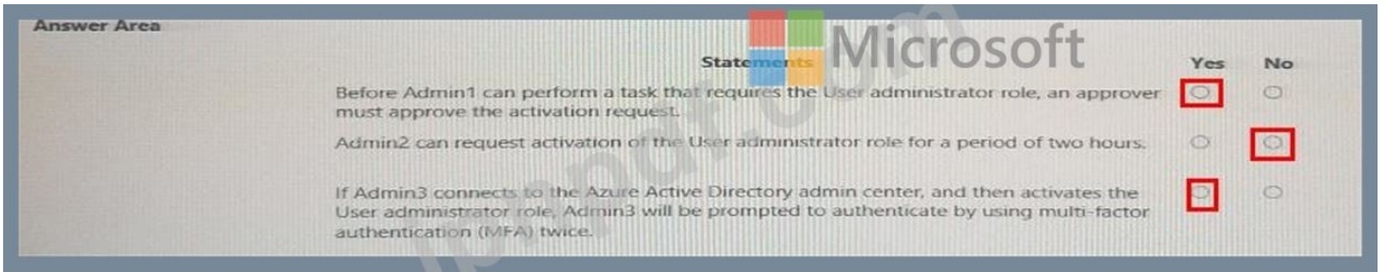
ユーザー管理者ロールの割り当ては、暗記割り当ての展示に示されているように表示されます。
(ロール割り当てラボをクリックします。)



次の各文について、その文が正しい場合は「はい」を選択します。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 ポイントが付与されます。

Answer:



最新問題**: 18**
漏洩した資格情報の認証要件を満たす必要があります。
何をすべきでしょうか?
A. Azure AD Connect で PingFederate とのフェデレーションを有効にします。
B. Azure AD パスワード保護を構成します。
C. Azure AD Connect でパスワード ハッシュ同期を有効にします。
D. Azure AD で認証方法ポリシーを構成します。
Answer: C (メーッセージを残す**)**
トピック 1、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、従業員は米国全土にいます。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。
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 Azure Active Directory (Azure AD) テナントにリンクされた litware.com という名前の Active Directory フォレストが含まれています。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 という名前の 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 のすべてのユーザーは、Microsoft 365 Enterprise E5 ライセンスを所有しています。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。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。
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

両方の Litware オフィスはインターネットに直接接続しています。両方のオフィスは、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。すべてのオンプレミス ドメイン コントローラーはインターネットにアクセスできません。

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。

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 属性の値を変更して、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。
* 外部に漏洩した認証情報を自動的に検出し、修復します

アクセス要件

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。

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を検出したいと考えています。

最新問題: **19**
User1 という名前のユーザーを含む Microsoft 365 サブスクリプションがあります。
User1 が Azure AD ロールのアクセス レビューを作成できることを確認する必要があります。ソリューションでは、最小権限のプリンシパルを使用する必要があります。
User1 に割り当てるべきロールはどれですか?
A. ガバナンス管理者を特定する
B. 特権ロール管理者
C. ユーザー管理者
D. ユーザーアクセス管理
Answer: A (メーッセージを残す**)**

最新問題: **20**
Azure サブスクリプション、Google Cloud Platform (GCP) アカウント、Amazon Web Services (AWS) アカウントをお持ちです。
すべてのプラットフォームにわたる権限の割り当てに関連するリスクを評価するためのソリューションを推奨する必要があります。ソリューションは管理の労力を最小限に抑える必要があります。推奨事項には何を含める必要がありますか?
A. Microsoft Entra ID 保護
B. クラウド アプリ向け Microsoft Defender
C. マイクロソフト センチネル
D. Microsoft Entra 権限管理
Answer: (解答を表示する**)**

最新問題: **21**
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。Fabcricam には、fabrikam.com という Azure Active Diretory (Azure AD) テナントがあります。
トピック 1、Litware, Inc
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 Azure Active Directory (Azure AD) テナントにリンクされた litware.com という名前の Active Directory フォレストが含まれています。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 という名前の 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 のすべてのユーザーは、Microsoft 365 Enterprise E5 ライセンスを所有しています。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。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。
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

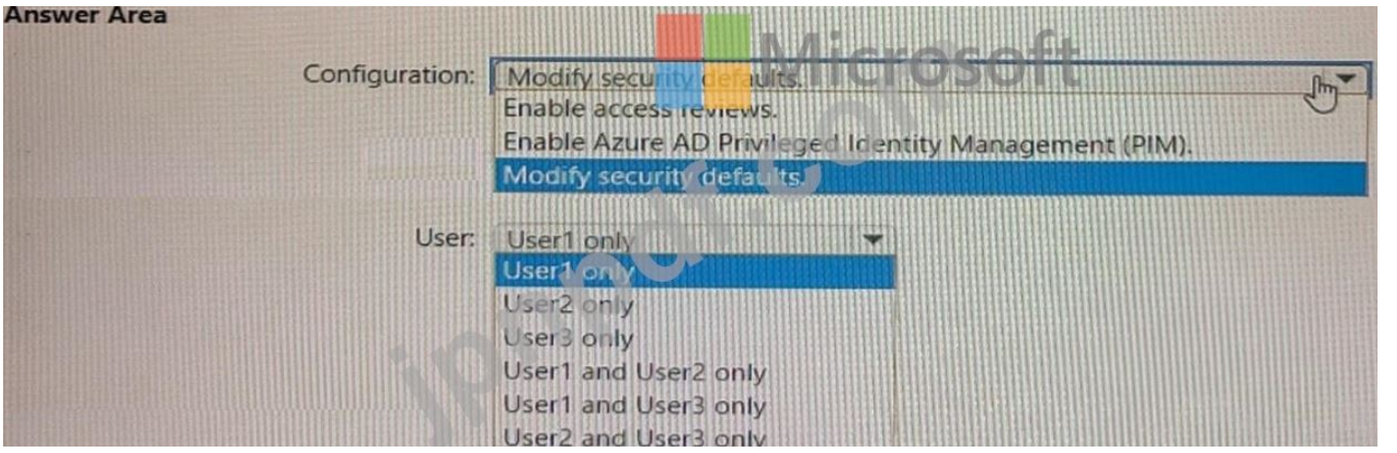
両方の Litware オフィスはインターネットに直接接続しています。両方のオフィスは、サイト間 VPN 接続を使用して Azure サブスクリプション内の仮想ネットワークに接続しています。すべてのオンプレミス ドメイン コントローラーはインターネットにアクセスできません。
委任要件
Litware では、次の委任要件が特定されています。
* Azure AD Privileged Identity Management (PIM) を使用して、特権ロールの管理を委任します。
* 権限のないユーザーがlitware.com Azure ADテナントにアプリケーションを登録できないようにします。
* 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。
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 属性の値を変更して、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。
* 外部に漏洩した認証情報を自動的に検出し、修復します
アクセス要件
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。
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を検出したいと考えています。

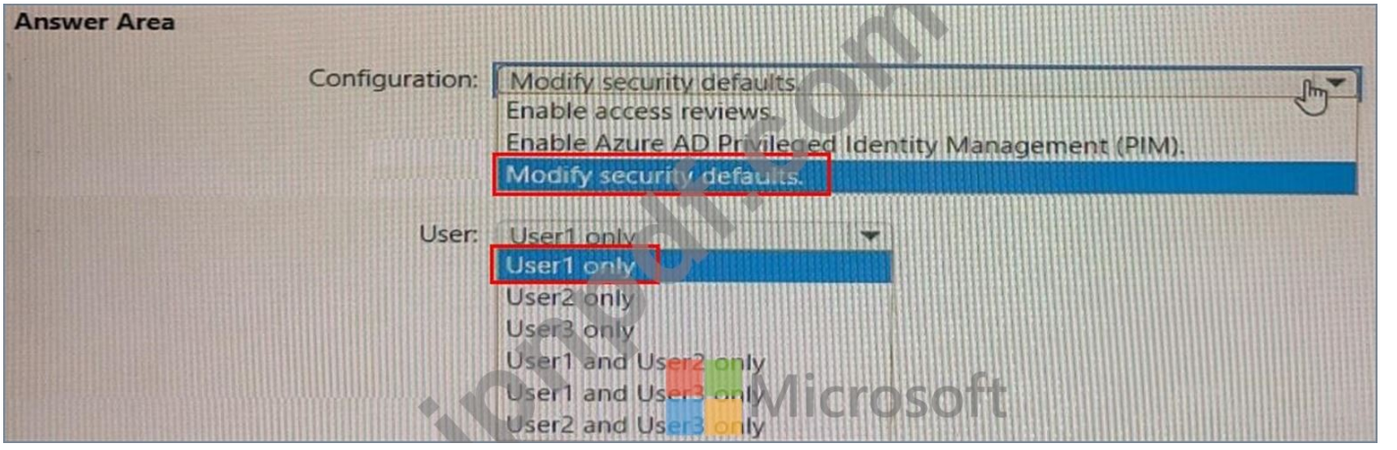
最新問題: **22**
次の表に示すユーザーを含む Azure AD テナントがあります。

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

ユーザー 2 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**: 23**

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。

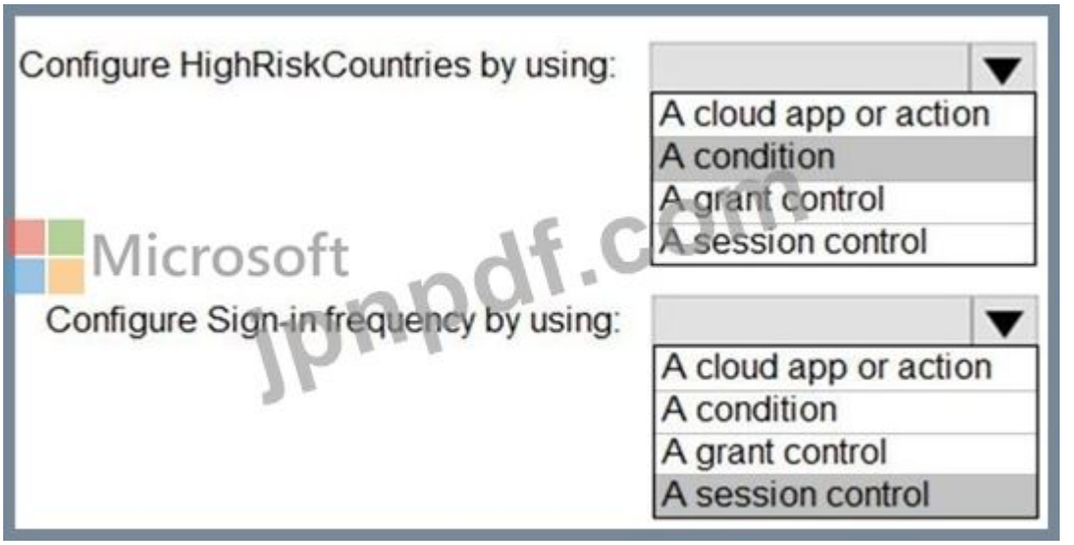
高リスクの国から接続する場合、ユーザーが認証されたままでいられる時間を制限する必要があります。

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ます。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:



参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

最新問題**: 24**
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

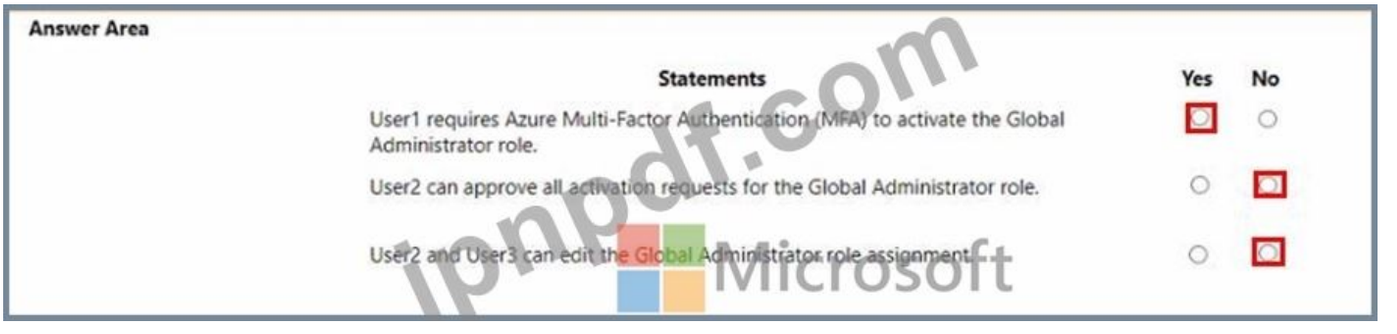
Setting	State
Activation maximum duration (hours)	1 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

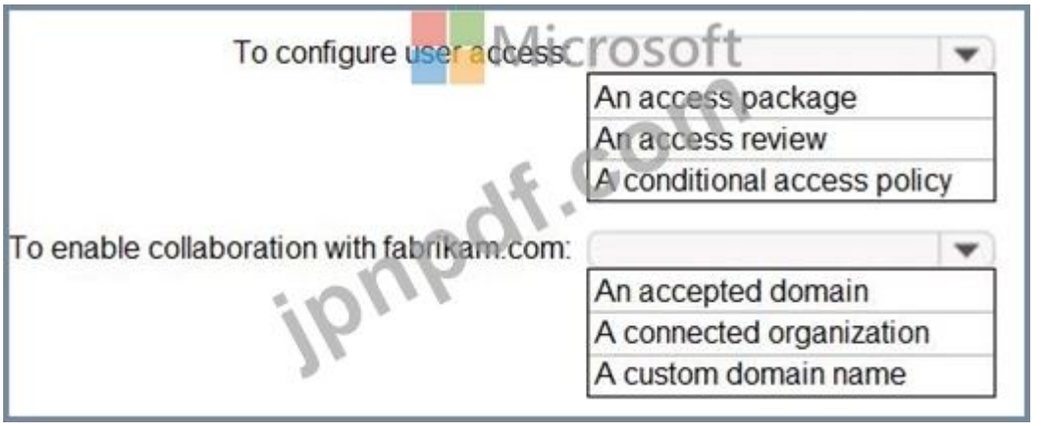
Setting	State
Allow permanent eligible assignment	Yes
Expire eligible assignments after	-
Allow permanent active assignment	Yes
Expire active assignments after	-
Require Azure Multi-Factor Authentication on active assignment	No
Require justification on active assignment	Yes

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

Answer:



最新問題: **25**
マーケティング部門の計画された変更と技術要件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。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization

最新問題: **26**
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)

参照：

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

最新問題**: 27**

既定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。テナントには、次の表に示すユーザーが含まれています。

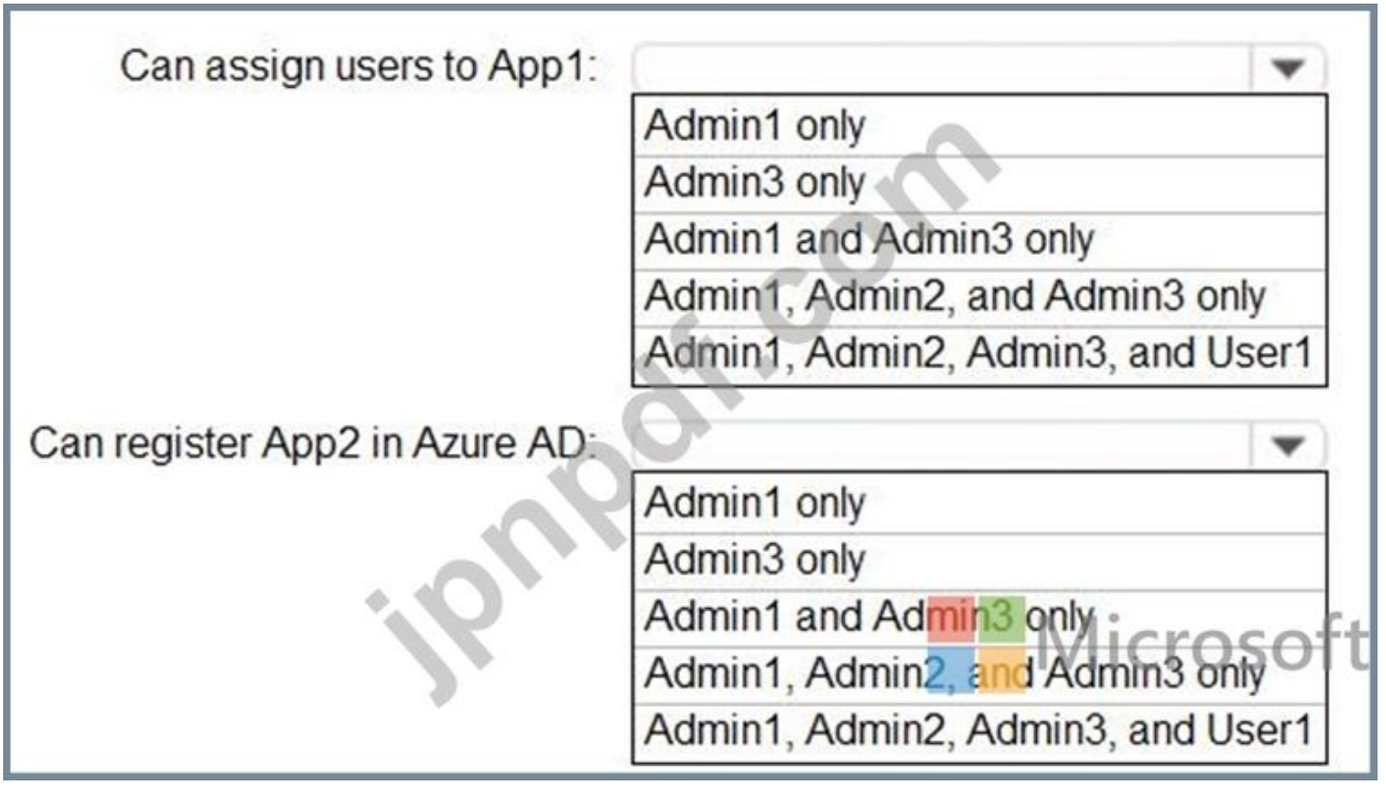
Name	Role
Admin1	Application administrator
Admin2	Application developer
Admin3	Cloud application administrator
User1	User

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

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、回答領域で適切なオプションを選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

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**: 28**
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 ポイントが付与されます。

Answer:

説明

Azure AD Connect settings to modify:

Directory Extensions
Domain Filtering
Optional Features

Assign Azure AD licenses to:

An Azure Active Directory group that has only nested groups
An Azure Active Directory group that has the Assigned membership type
An Azure Active Directory group that has the Dynamic User membership type

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、Microsoftに自動的に追加される必要があります。
適切なライセンスが割り当てられている 365 グループ。

最新問題: **29**
User1 という名前のユーザーと、次の表に示す条件付きアクセス ポリシーを含む Azure AD テナントがあります。

Name	Status	Conditional access requirement
CAPolicy1	On	Users connect from a trusted IP address.
CAPolicy2	On	Users' devices are marked as compliant.
CAPolicy3	Report-only	The sign-in risk of users is low.

User1 がさまざまな IP アドレスからサインインしようとしたときに、User1 に適用されるポリシーを評価する必要があります。
どの機能を使用すべきでしょうか?
A. What If ツール
B. Microsoft 365 ネットワーク接続テスト ツール
C. アイデンティティセキュリティスコア
D. アクセスレビュー
Answer: A (メーッセージを残す**)**

最新問題: **30**
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 ドメインが含まれています。
ユーザーは、Windows 10 を実行し、ドメインに参加しているコンピューターにサインインします。
Azure AD シームレス シングル サインオン (Azure AD シームレス SSO) を実装する予定です。
Azure AD シームレス SSO をサポートするように Windows 10 コンピューターを構成する必要があります。
何をすべきでしょうか?

A. エンタープライズ状態ローミングを有効にします。
B. 設定アプリからサインイン オプションを構成します。
C. ローカルイントラネットゾーンの設定を変更する
D. Azure AD Connect 認証エージェントをインストールします。
Answer: B (メーッセージを残す**)**

最新問題**: 31**
Microsoft Entra Permissions Management を使用する Sub1 という名前の Azure サブスクリプションがあります。Sub1 には User1 という名前のユーザーが含まれています。User1 には Sub1 全体で複数のアクセス許可が付与されています。
User1 に付与されたすべての権限を読み取り専用権限に置き換える必要があります。ソリューションでは、管理作業を最小限に抑える必要があります。
権限管理の修復タブでは何をすべきでしょうか?
A. [権限] サブタブからクイックアクションを使用します。
B. [ロール/ポリシー] サブタブからロールを作成します。
C. 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。
D. [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: B (メーッセージを残す**)**
トピック 3、A Datum Corp概要
Datum Corporation はモントリオールのコンサルティング会社です。
A Datum は最近、バンクーバーに拠点を置く Litware, Inc. という会社を買収しました。
データ環境
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。
Datum には、Microsoft 365 E5 サブスクリプションがあります。サブスクリプションには、Azure AD Connect を使用して adatum.com AD DS ドメインと同期する検証済みドメインが含まれています。Datum には、adatum.com という名前の Azure Active Directory (Azure AD) テナントがあります。テナントでは、セキュリティの既定値が無効になっています。
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
データムは次の問題を識別します。
* 営業部門の複数のユーザーは、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、デバイス制限に達したため、サポート部門に連絡してデバイスを Azure AD テナントに参加させる必要がある場合があると報告されています。
* 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を含め、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ています。
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
Datum は次の技術要件を識別します。
* 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要求できる必要があります。
* ユーザーに対して MFA の登録を促すプロンプトを表示し、猶予期間中に登録をバイパスするオプションを提供する必要があります。
* ユーザーは、SSPR を使用してパスワードをリセットするために、1 つの認証方法を提供する必要があります。使用可能な方法には次のものが含まれます。
* 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: **32**
ADatum ユーザーを同期する必要があります。ソリューションは技術要件を満たしている必要があります。
何をすべきでしょうか?

A. Microsoft Azure Active Directory Connect ウィザードから、同期オプションのカスタマイズを選択します。
B. PowerShell から、Set-ADSyncScheduler を実行します。
C. PowerShell から Start-ADSyncSyncCycle を実行します。
D. Microsoft Azure Active Directory Connect ウィザードから、ユーザー サインインの変更を選択します。
Answer: (解答を表示する**)**
Adatum 組織単位 (OU) を同期するように Azure AD Connect を構成するには、同期オプションのカスタマイズを選択する必要があります。
トピック 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、従業員は米国全土にいます。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。
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 Azure Active Directory (Azure AD) テナントにリンクされた litware.com という名前の Active Directory フォレストが含まれています。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 という名前の 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 のすべてのユーザーは、Microsoft 365 Enterprise E5 ライセンスを所有しています。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。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。
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

両方の Litware オフィスはインターネットに直接接続しています。両方のオフィスは、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。すべてのオンプレミス ドメイン コントローラーはインターネットにアクセスできません。
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。
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 属性の値を変更して、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。
* 外部に漏洩した認証情報を自動的に検出し、修復します
アクセス要件
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。
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を検出したいと考えています。

最新問題**: 33**
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:

o 含める: Group1

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

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

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

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.	○	●

Explanation:

コンピュータ画面のスクリーンショット 説明は自動的に生成されました

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: **34**

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。

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

最新問題: **35**

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 ドレス範囲があります。
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 付き
* 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 個です
* ポリシーを有効にする: オン
次の各文が正しい場合は 「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 ポイントが与えられます。

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.	○	○

Answer:

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: **36**
会社では、2 つの新しい Microsoft 365 ES サブスクリプションと、App という名前のアプリを購入します。
App1 に対して Microsoft Defender for Cloud Apps アクセス 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? (microsoft.com の Microsoft Identity and Access Administrator に基づいて正しい回答を選択してください)
A. App1 のトークン構成を構成します。
B. App1 の API 権限を追加します。
C. アプリによって適用される制限を使用するように条件付きアクセス ポリシーを構成します。
D. 条件付きアクセス アプリ制御を使用するように条件付きアクセス ポリシーを構成します。
Answer: D (メーッセージを残す)
https://learn.microsoft.com/en-us/defender-cloud-apps/access-policy-aad App1 の Microsoft Defender for Cloud Apps アクセス ポリシーを作成するには、アプリで適用される制限を使用するように条件付きアクセス ポリシーを構成する必要があります。これにより、ユーザー、デバイス、場所、アプリの状態などの条件に基づいて、クラウド アプリへのアクセスを制御できます。また、アプリで適用される制限を使用して、管理対象デバイスで実行されているか管理対象外デバイスで実行されているかなど、アプリの状態に基づいてクラウド アプリへのアクセスを制御することもできます。

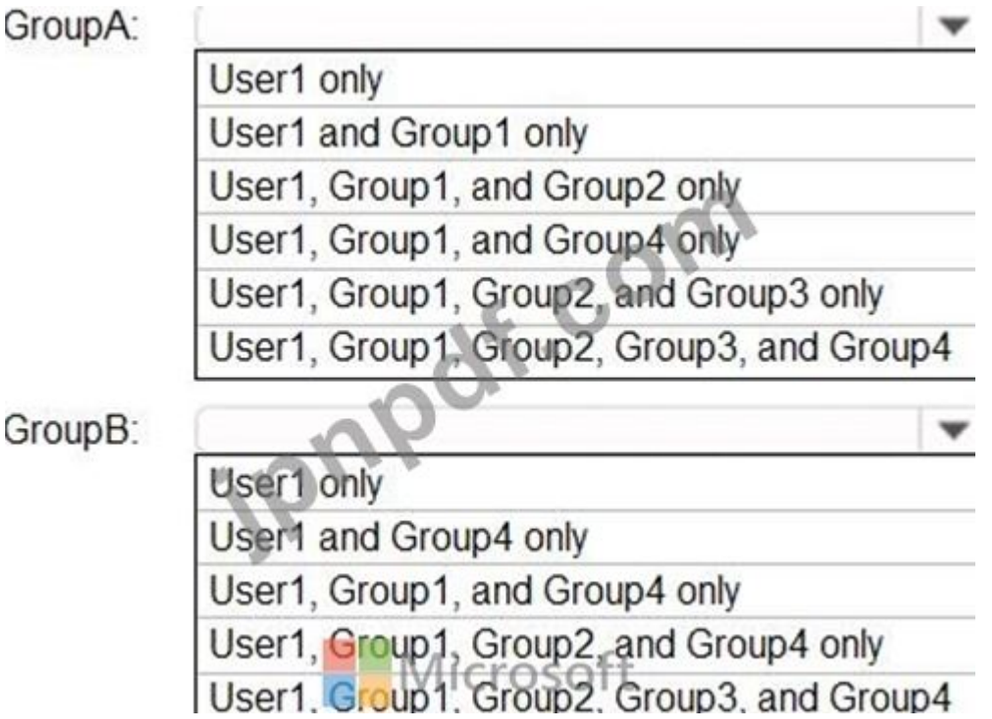
最新問題: **37**
User1 という名前のユーザーと、次の表に示すグループを含む Azure Active Directory (Azure AD) テナントがあります。

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

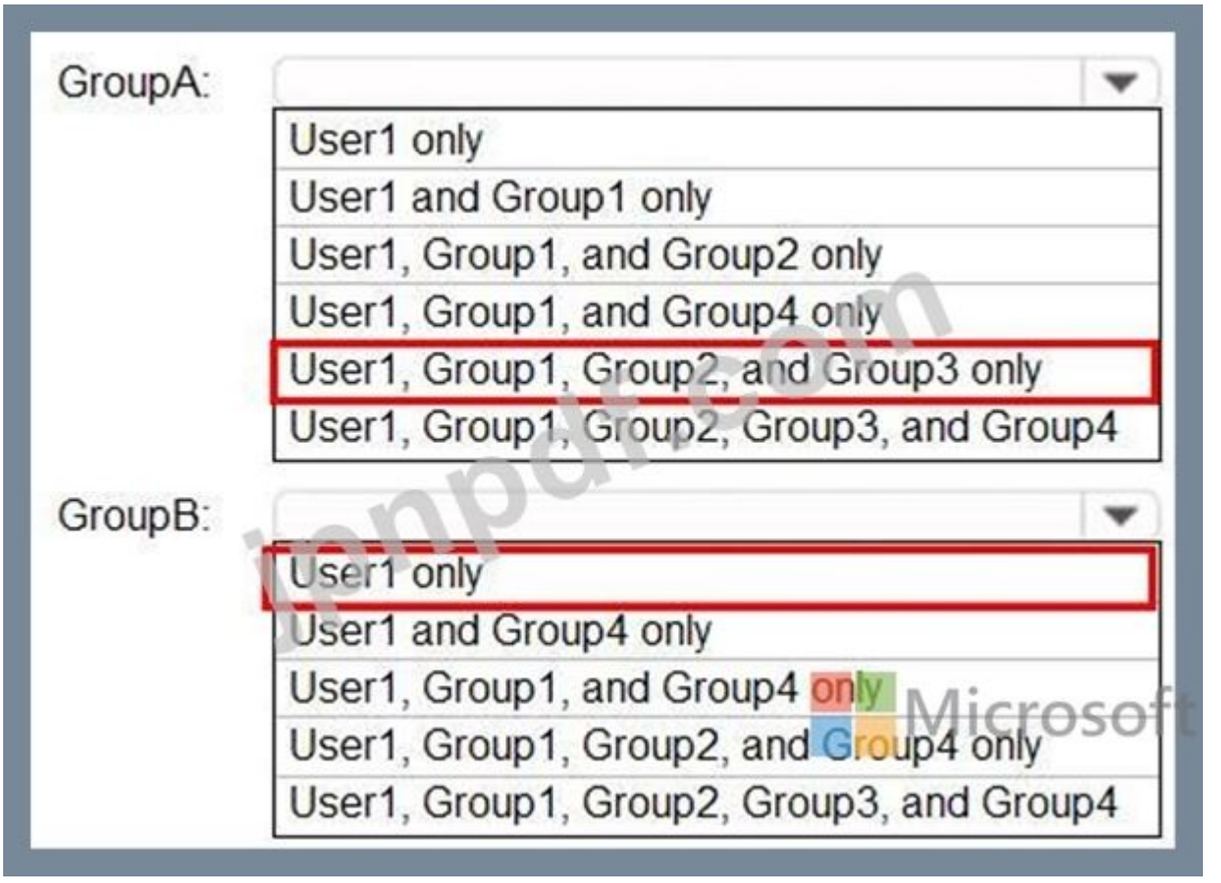
テナントでは、次の表に示すグループを作成します。

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: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



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

最新問題**: 38**
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

各ユーザーの役割権限を比較する必要があります。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。
何を使うべきでしょうか?
A. Microsoft Purview コンプライアンス ポータル
B. Microsoft 365 管理センター
C. Microsoft Entra 管理センター
D. Microsoft 365 Defender ポータル
Answer: C (メーッセージを残す**)**

最新問題**: 39**
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。

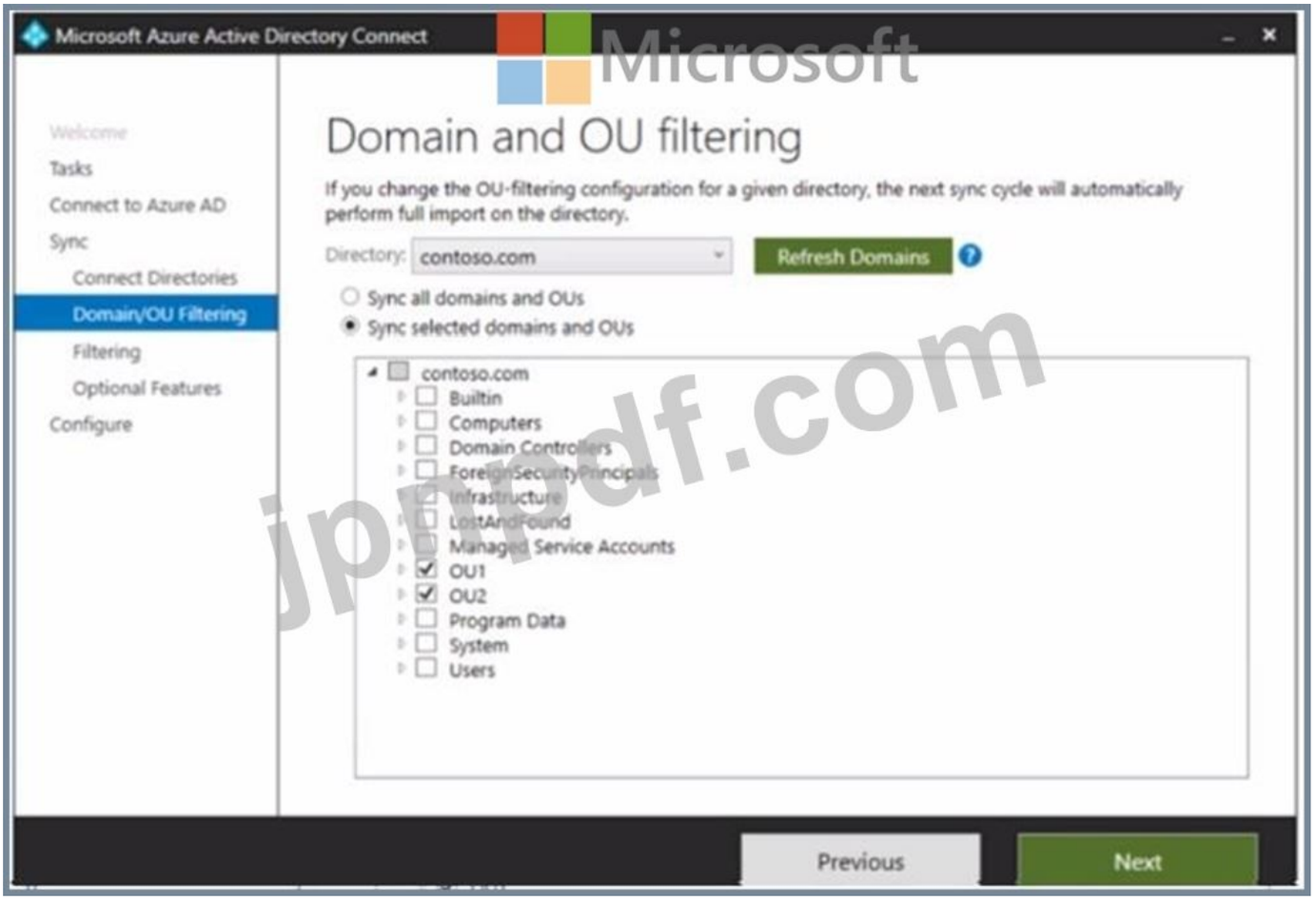
App name	Used by	Microsoft Graph permission
App1	User1	Calendars.Read of type Delegated
App2	User2	Calendars.Read of type Delegated Calendars.ReadWrite of type Application
App3	User3, User4	Calendars.Read of type Application

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

最新問題**: 40**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。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.

Microsoft Entra Connect をインストールします。ドメインと OU のフィルタリング設定を、「ドメインと OU のフィルタリング」の図に示すように構成します (「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。) 次の各ステートメントについて、ステートメントが正しい場合は 「はい」を選択します。それ以外の場合は 「いいえ」を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

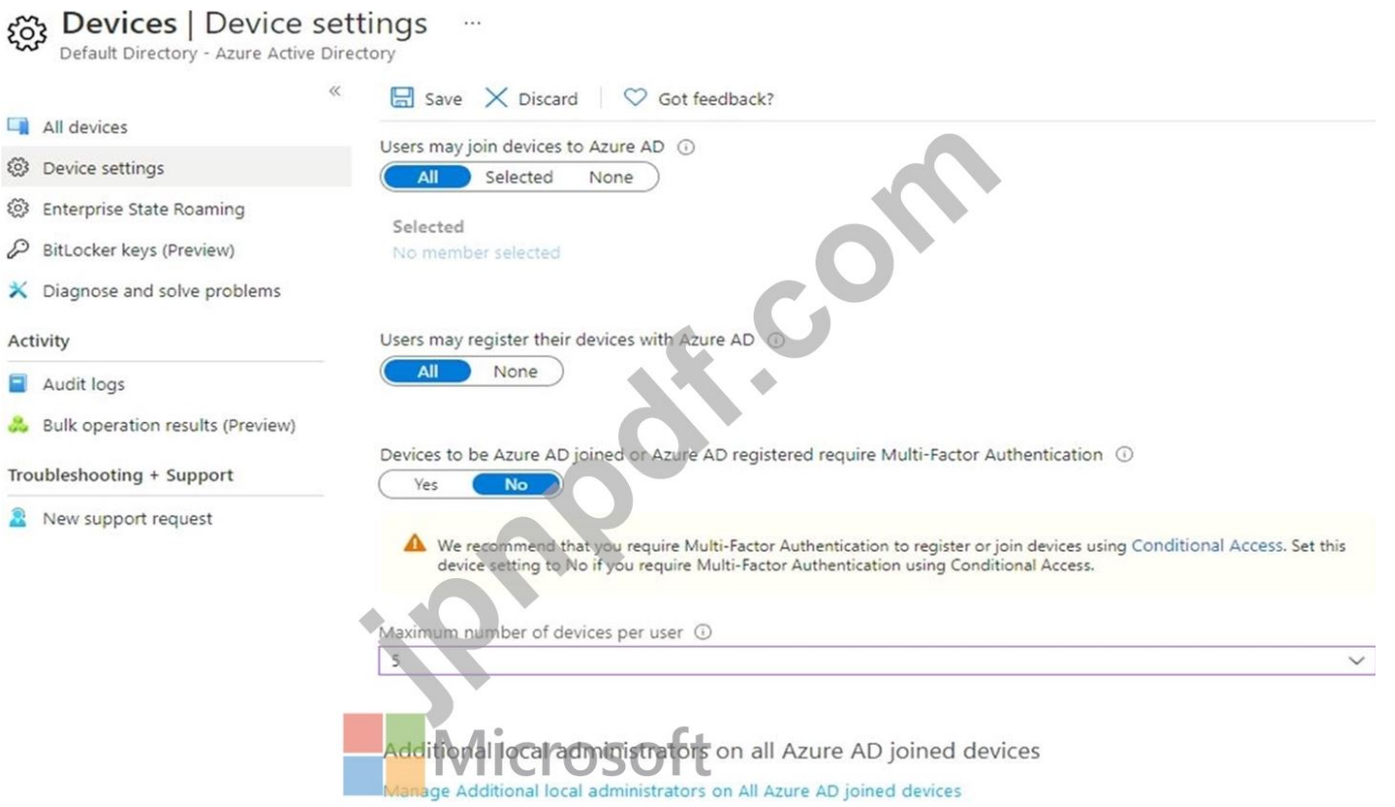
Explanation:

最新問題**: 41**

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

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	**None**

次の図に示すデバイス設定があります。



User1 には次の表に示すデバイスがあります。

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

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

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

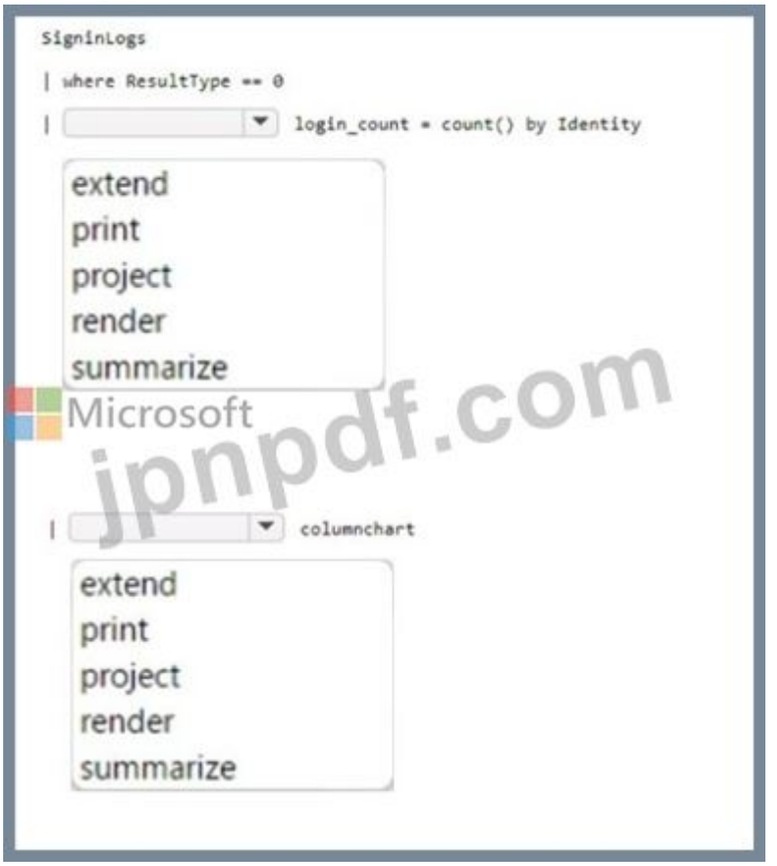
Answer:

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

参照：

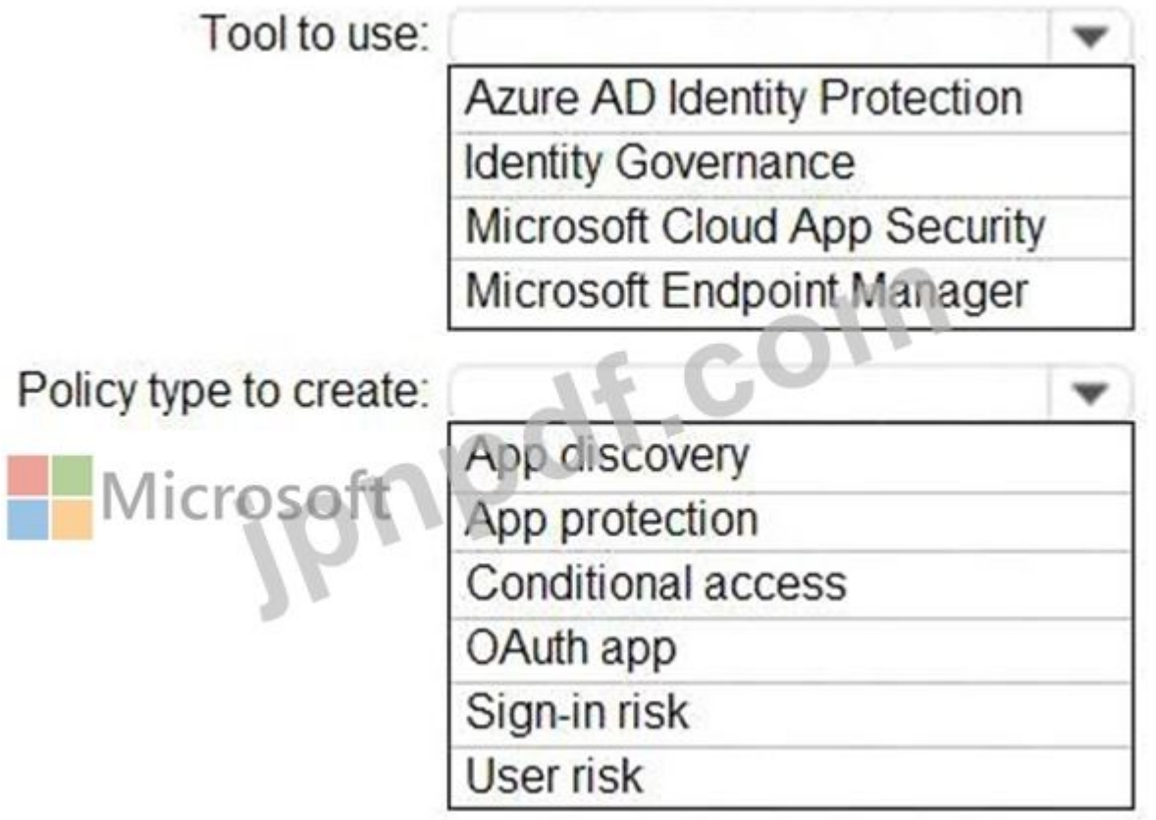
https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

最新問題: **42**
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ます。

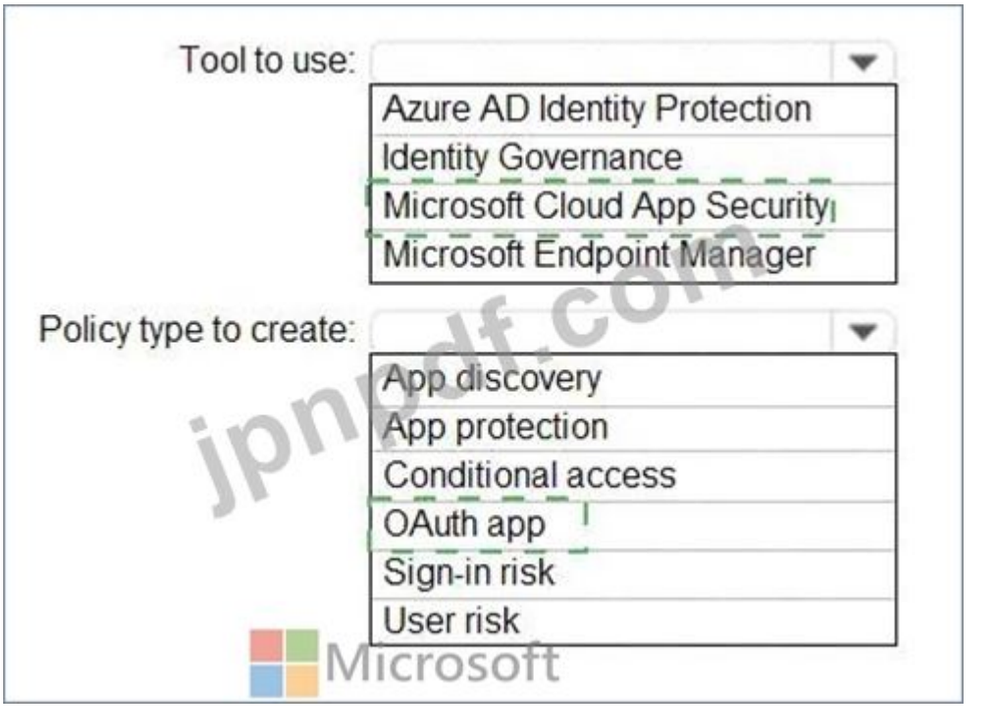


Answer:

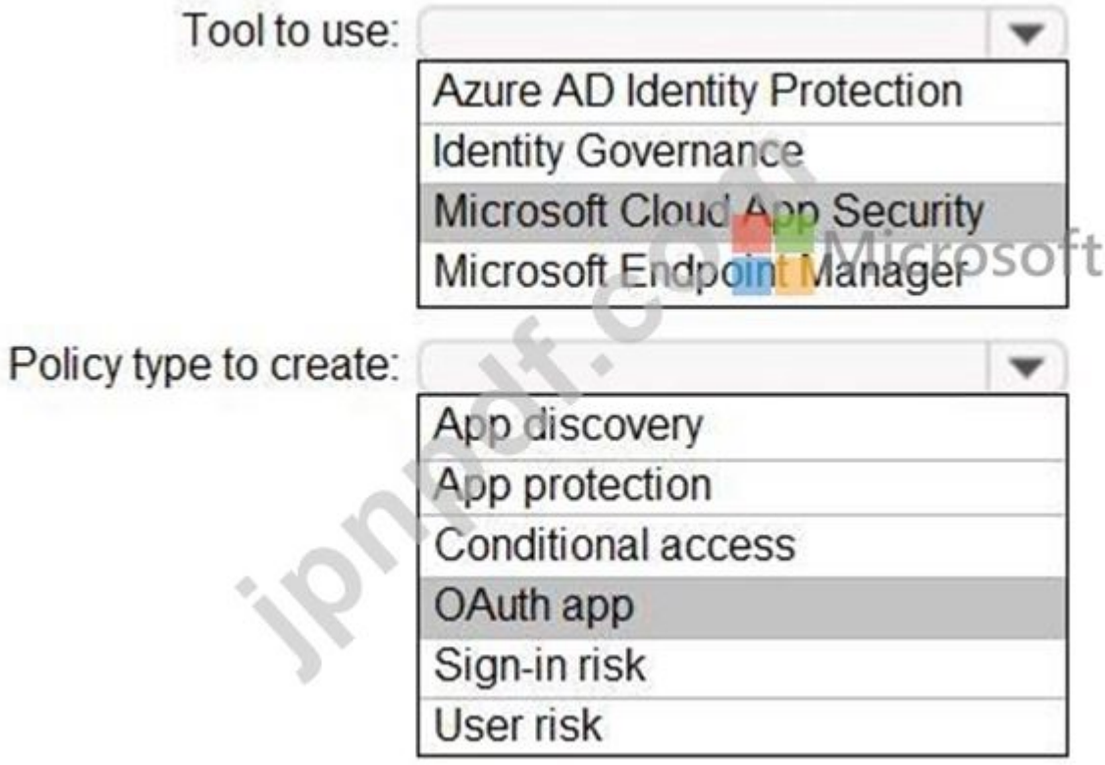
最新問題: **43**
Microsoft 365 テナントがあります。
場合によっては、ユーザーは、それぞれのユーザーの Microsoft 365 データへの制限付きアクセスを必要とする外部のサードパーティ アプリケーションを使用します。ユーザーは、Azure Active Directory (Azure AD) にアプリケーションを登録します。
登録されたアプリケーションがユーザーの電子メールへの読み取りおよび書き込みアクセス権を取得した場合にアラートを受信する必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。


Tool to use:
Azure AD Identity Protection
Identity Governance
Microsoft Cloud App Security
Microsoft Endpoint Manager
Policy type to create:
App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk
Microsoft

Answer:


Tool to use:
Azure AD Identity Protection
Identity Governance
Microsoft Cloud App Security
Microsoft Endpoint Manager
Policy type to create:
App discovery
App protection
Conditional access
OAuth app
Sign-in risk
User risk
Microsoft

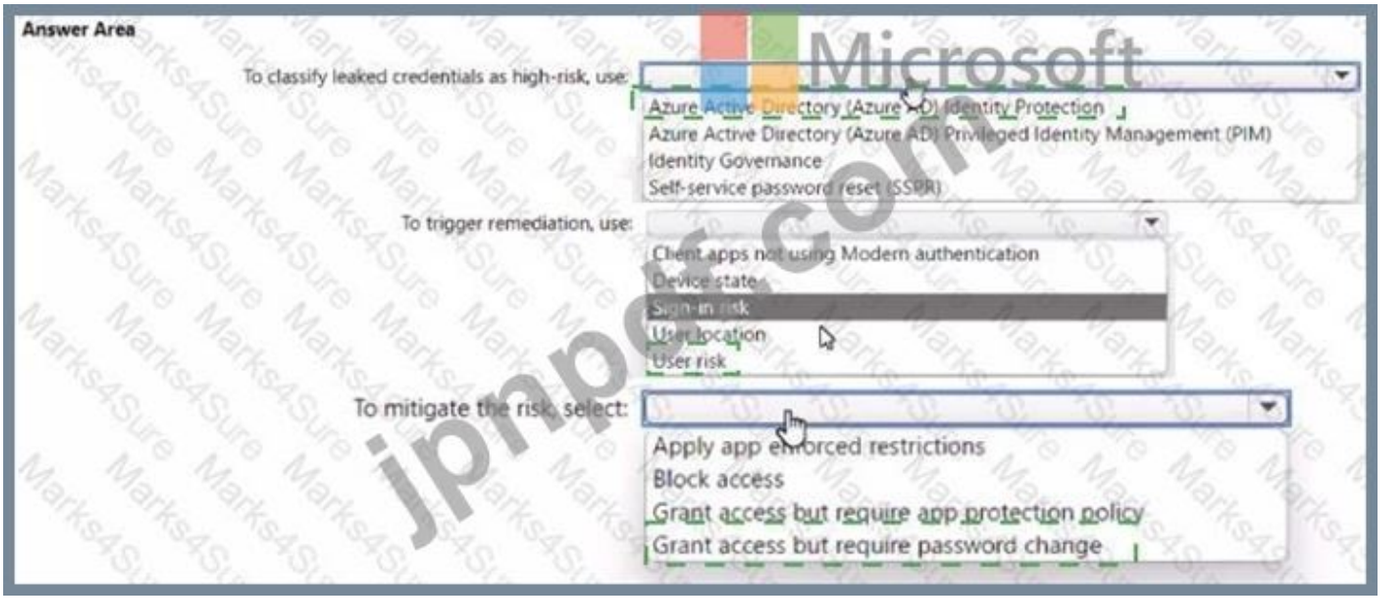
説明



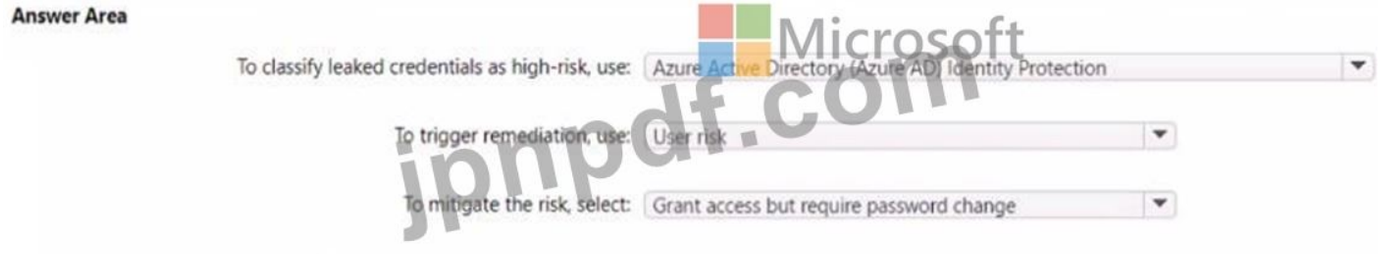
参照：
https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy

最新問題**: 44**
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。ソリューションは次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**: 45**

Azure サブスクリプションをお持ちです。

エンタイトルメント管理から、カスタム拡張機能を含む Catalog1 という名前のカタログを作成する予定です。

最初に何を作成し、Catalog1 を配布するために何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ます。

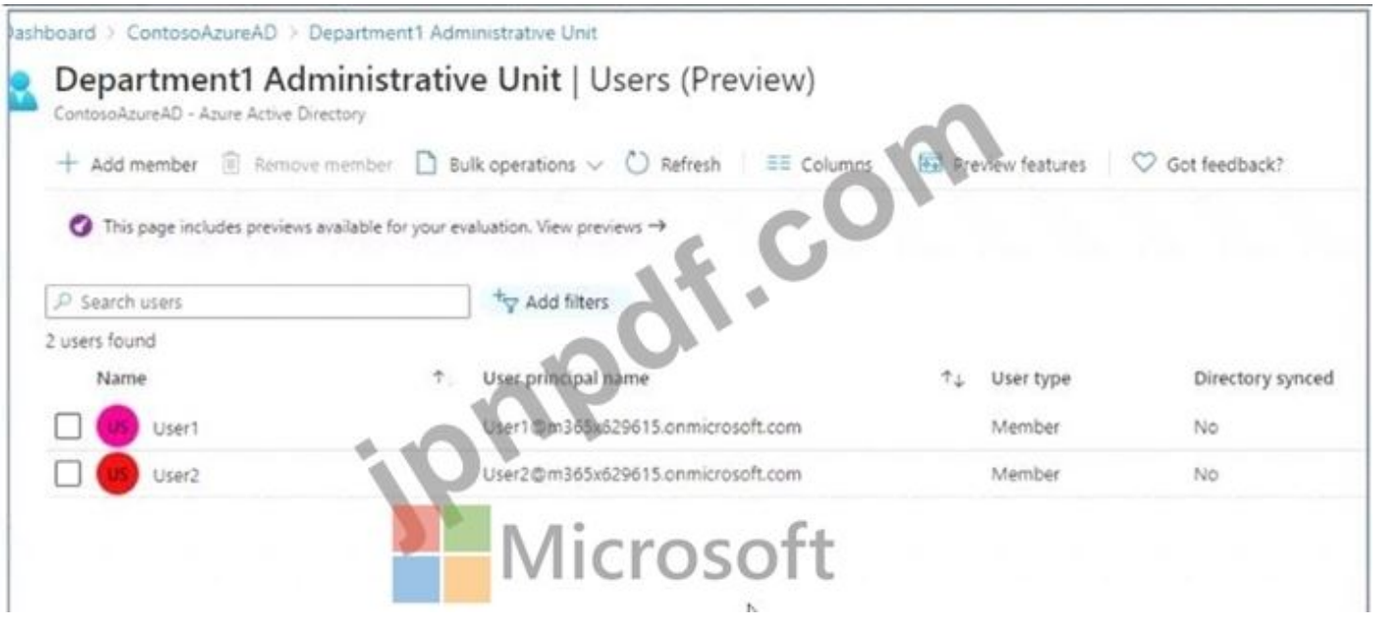
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:

最新問題**: 46**
漏洩した資格情報の認証要件を満たす必要があります。
何をすべきでしょうか?
A. Azure AD Connect で PingFederate とのフェデレーションを有効にします。
B. Azure AD パスワード保護を構成します。
C. Azure AD Connect でパスワード ハッシュ同期を有効にします。
D. Azure AD で認証方法ポリシーを構成します。
Answer: C (メーッセージを残す**)**
参照：
https://docs.microsoft.com/en-us/azure/security/fundamentals/steps-secure-identity

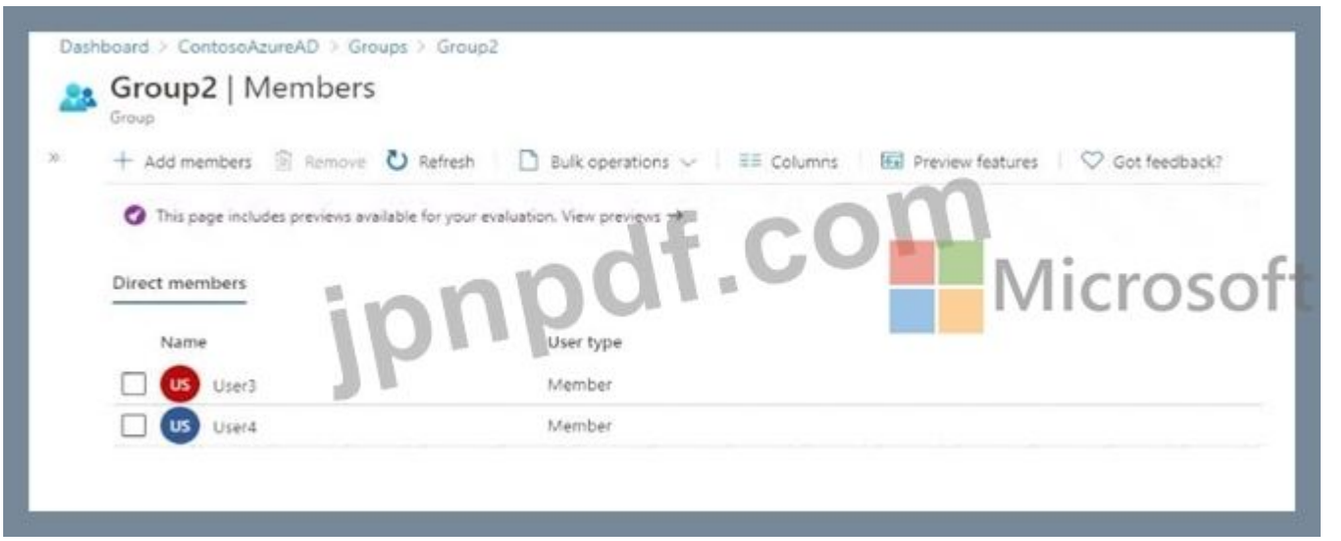
最新問題**: 47**
Group3 というグループと Department1 という管理単位を含む Microsoft Entra テナントがあります。
部門には、[ユーザー] 展示に表示されるユーザーがいます。([ユーザー] タブをクリックします。)



Department1 には、[グループ] 展示に表示されるグループがあります ([グループ] 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、[割り当て] 展示に表示されます。([割り当て] タブをクリックします。)

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。)



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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:

コンピュータ画面のスクリーンショット 説明は自動的に生成されました

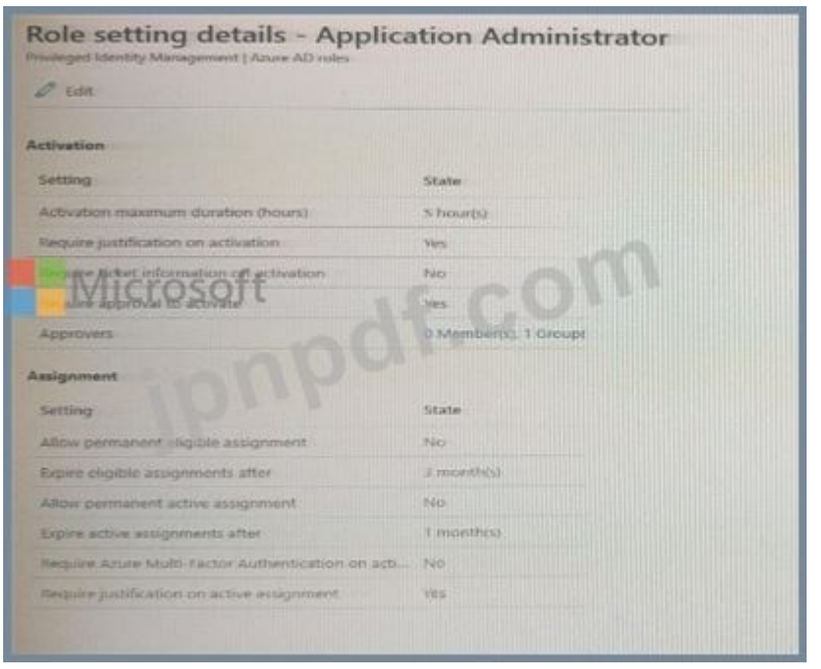
Answer Area

Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	◉	○
Admin1 can add User1 to Group3.	○	◉
Admin3 can reset the password of User1.	◉	○

最新問題: **48**
Log Analytics ワークスペースを作成します。
監査の技術要件を実装する必要があります。
Azure AD で何を構成する必要がありますか?
A. 会社のブランディング
B. 診断設定
C. 外部アイデンティティ
D. アプリ登録
Answer: (解答を表示する**)**
説明/参照:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring ID ガバナンス戦略を計画および実装する質問セット 2

最新問題: **49**
Microsoft Entra ID Premium ライセンスを使用する Microsoft Entra テナントがあります。
テナントの利用規約 (ToU) を構成する予定です。
ToU文書をアップロードする必要があります。
ドキュメントにはどの形式を使用すればよいですか?
A. RTF
B. HTML
C. DOCX
D. PDF
Answer: D (メーッセージを残す**)**

最新問題: **50**
Azure Active Directory (Azure AD) テナントに、User1、User1、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すように、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。)



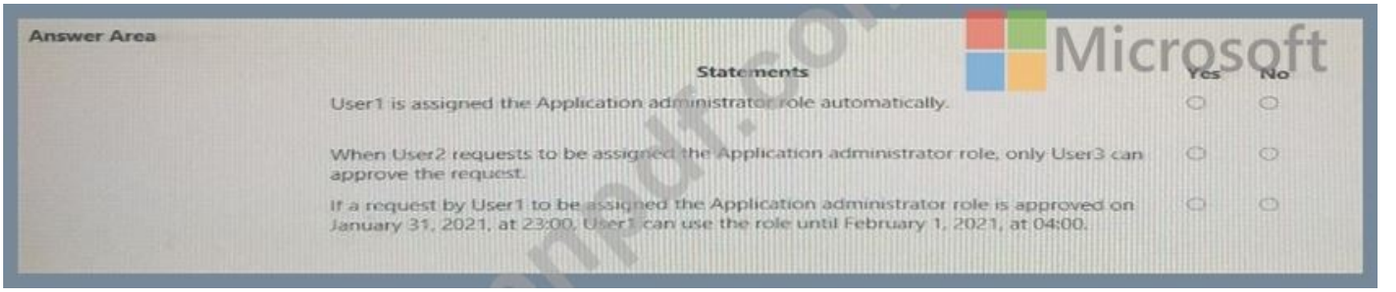
Group1 は、アプリケーション管理者ロールの承認者として構成されています。

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 の場合、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、その文が正しい場合は 「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 ポイントが付与されます。



Answer:

最新問題: **51**

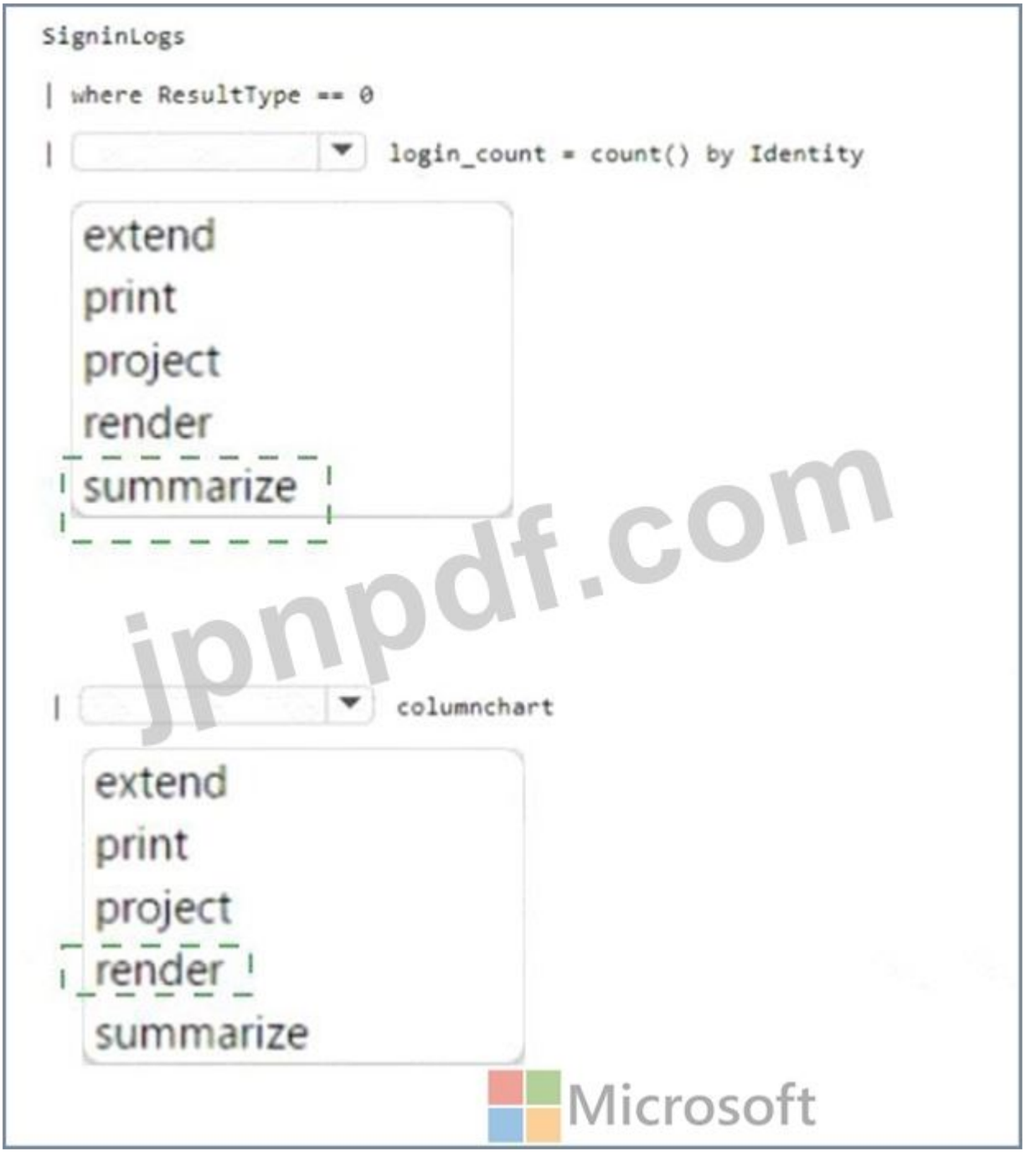
Azure サブスクリプションをお持ちです。

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ます。

Answer:



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
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処理し、ユーザーごとのサインイン数を集計して、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

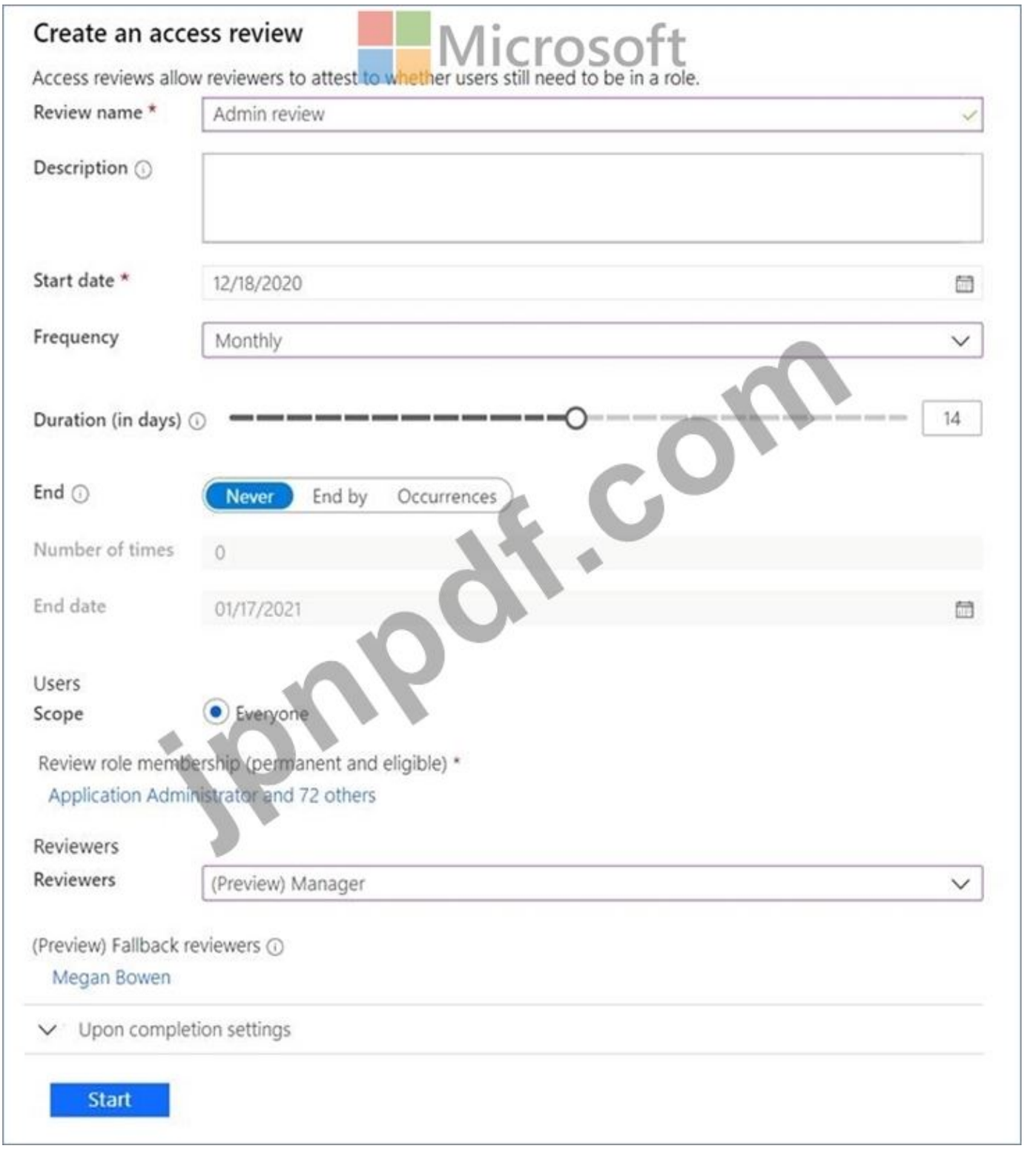
最新問題: **52**

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。
どの機能を使用すべきですか? 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 ポイントが付与されます。

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**: 53**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。
このセクション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 の部門に分かれて組織されています。
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: ロールごとに個別のアクセス レビューを作成します。

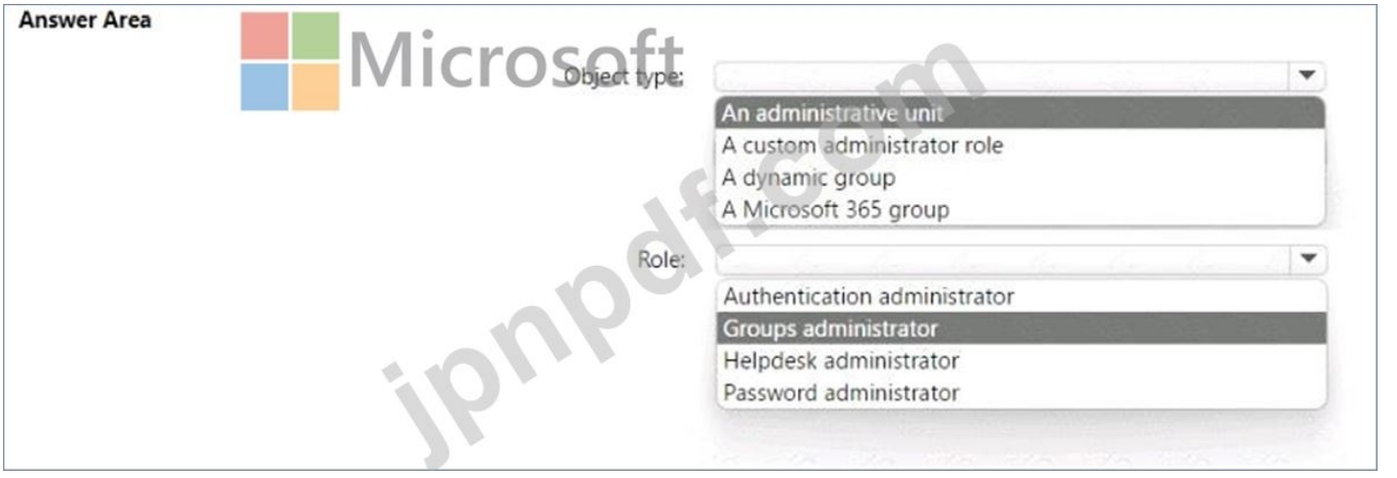
これは目標を満たしていますか?

A. はい

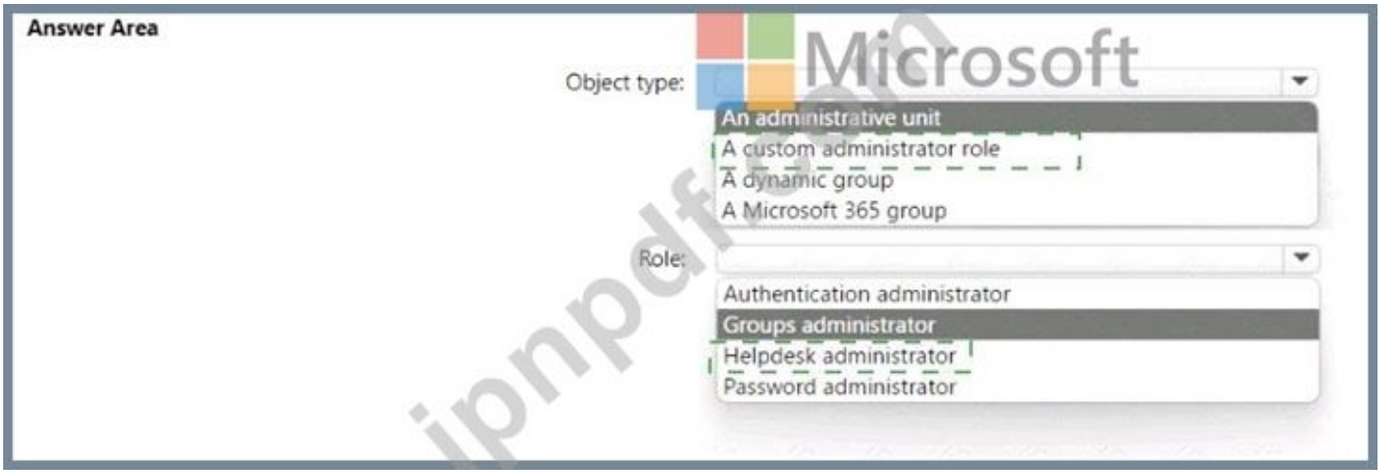
B. いいえ

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**: 54**
5,000 人のユーザーがいる Microsoft 365 テナントがあります。ユーザーのうち 100 人は経営幹部です。経営幹部には専用のサポート チームがあります。
サポート チームがパスワードをリセットし、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。ソリューションでは、最小権限の原則を使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 ポイントが付与されます。

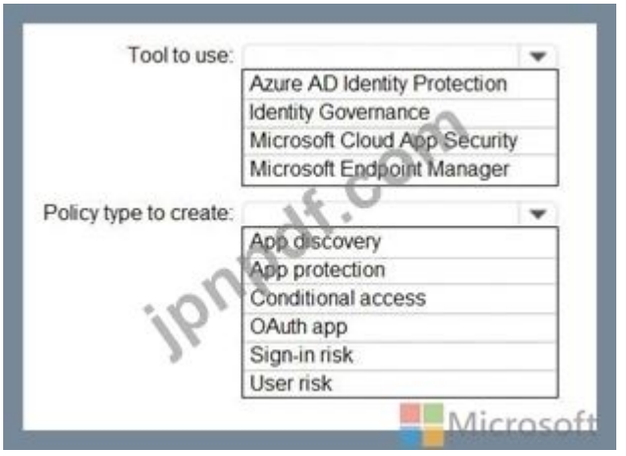


Answer:

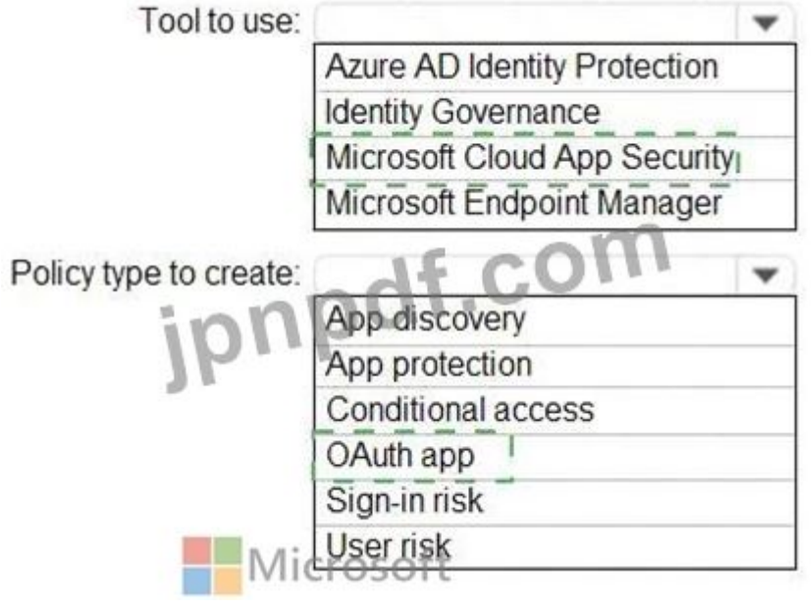


Explanation:

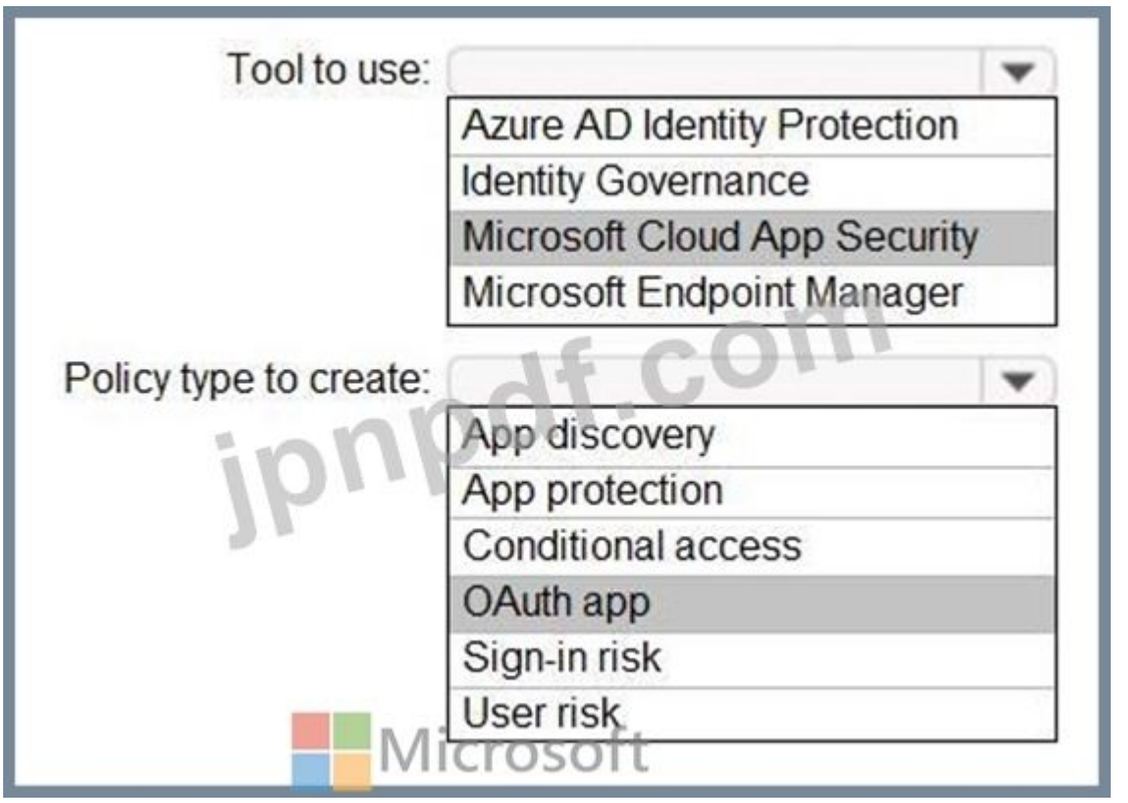
最新問題: **55**
Microsoft 365 テナントがあります。
場合によっては、ユーザーは、それぞれのユーザーの Microsoft 365 データへの制限付きアクセスを必要とする外部のサードパーティ アプリケーションを使用します。ユーザーは、Azure Active Directory (Azure AD) にアプリケーションを登録します。
登録されたアプリケーションがユーザーの電子メールへの読み取りおよび書き込みアクセス権を取得した場合にアラートを受信する必要があります。
どうすればいいでしょうか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



説明



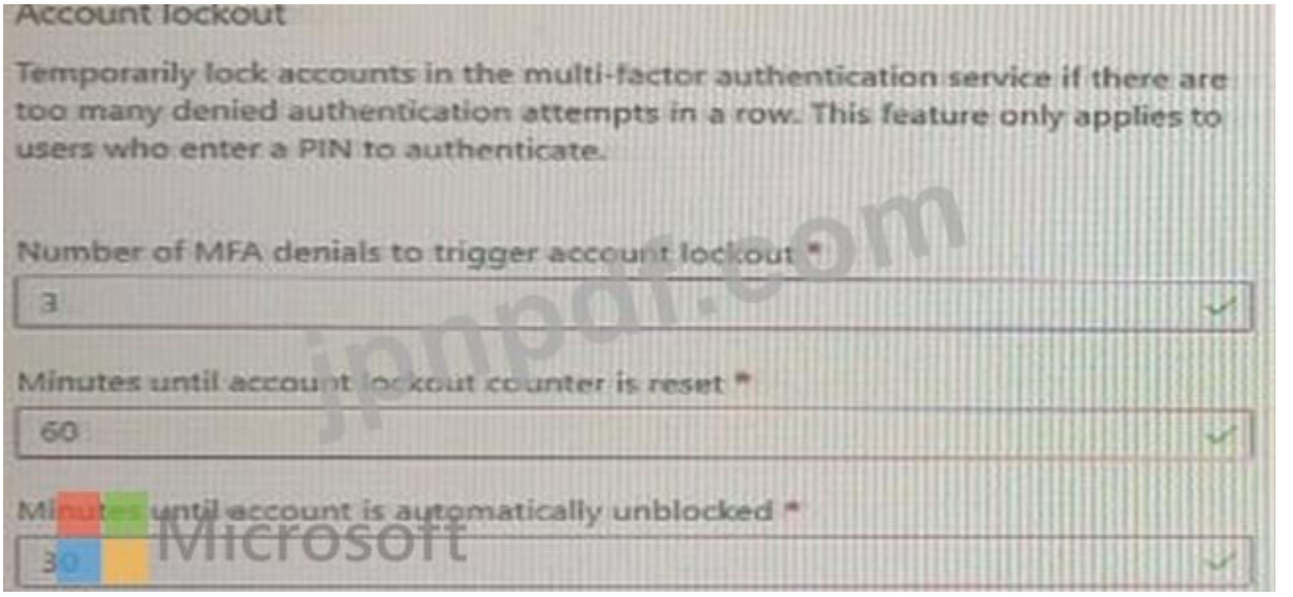
参照：
https://docs.microsoft.com/en-us/cloud-app-security/app-permission-policy

最新問題: **56**
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 ポイントが付与されます。

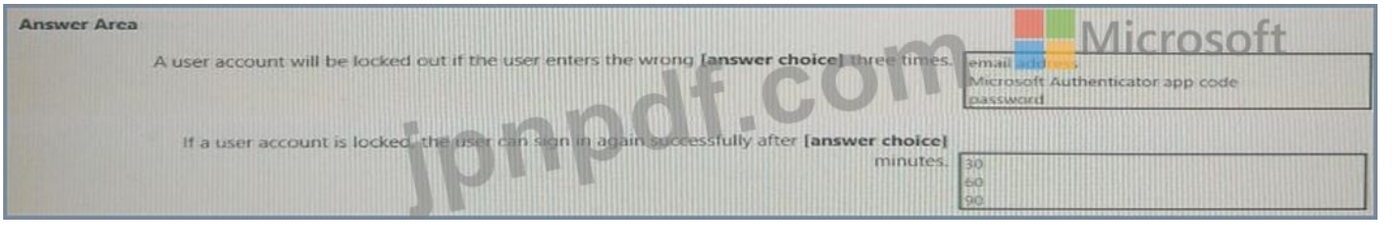
Answer:
答えは

最新問題: **57**

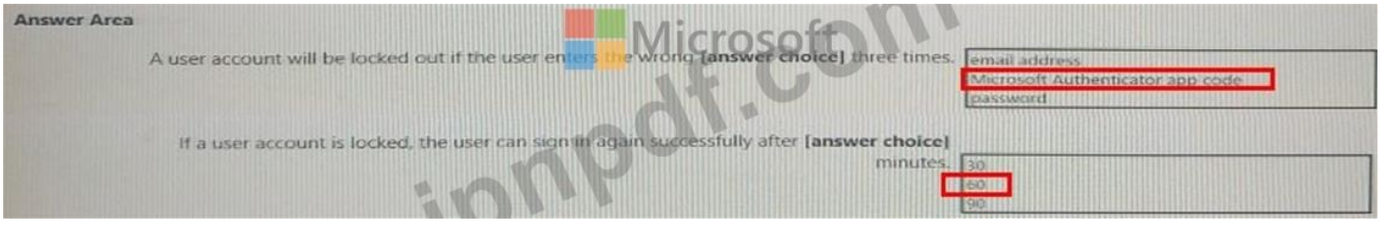
多要素認証 (MFA) が有効になっている Azure Active Directory (Azure AD) テナントがあります。
アカウント ロックアウト設定は、次の図に示すように構成されます。



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ている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 ポイントが付与されます。



Answer:



最新問題**: 58**
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

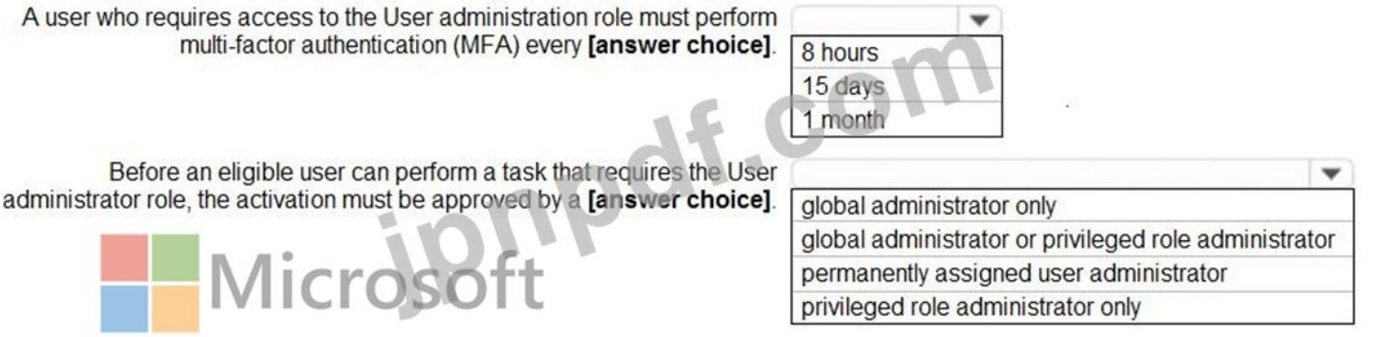
Azure AD で、Appl という名前の新しいエンタープライズ アプリケーションを追加します。App1 に割り当てることができるグループは何ですか?

A. グループ2のみ
B. グループ3のみ
C. グループ1のみ

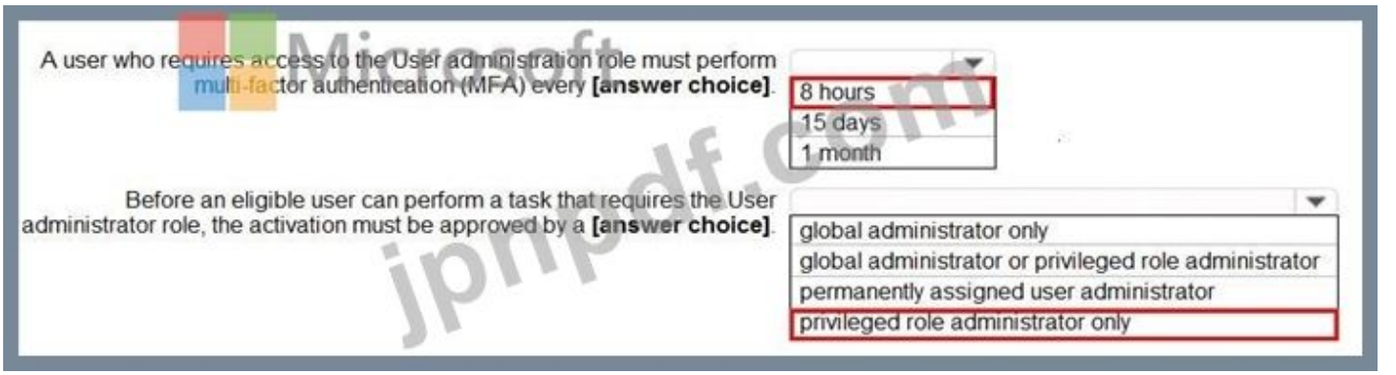
D. グループ1とグループ4
E. グループ1とグループ2のみ
Answer: (解答を表示する**)**

最新問題: **59**
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ている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 ポイントが付与されます。



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: **60**
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. 30日間
B. 90日間
C. 365日
D. 14日間
Answer: A (メーッセージを残す**)**

最新問題: **61**
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。

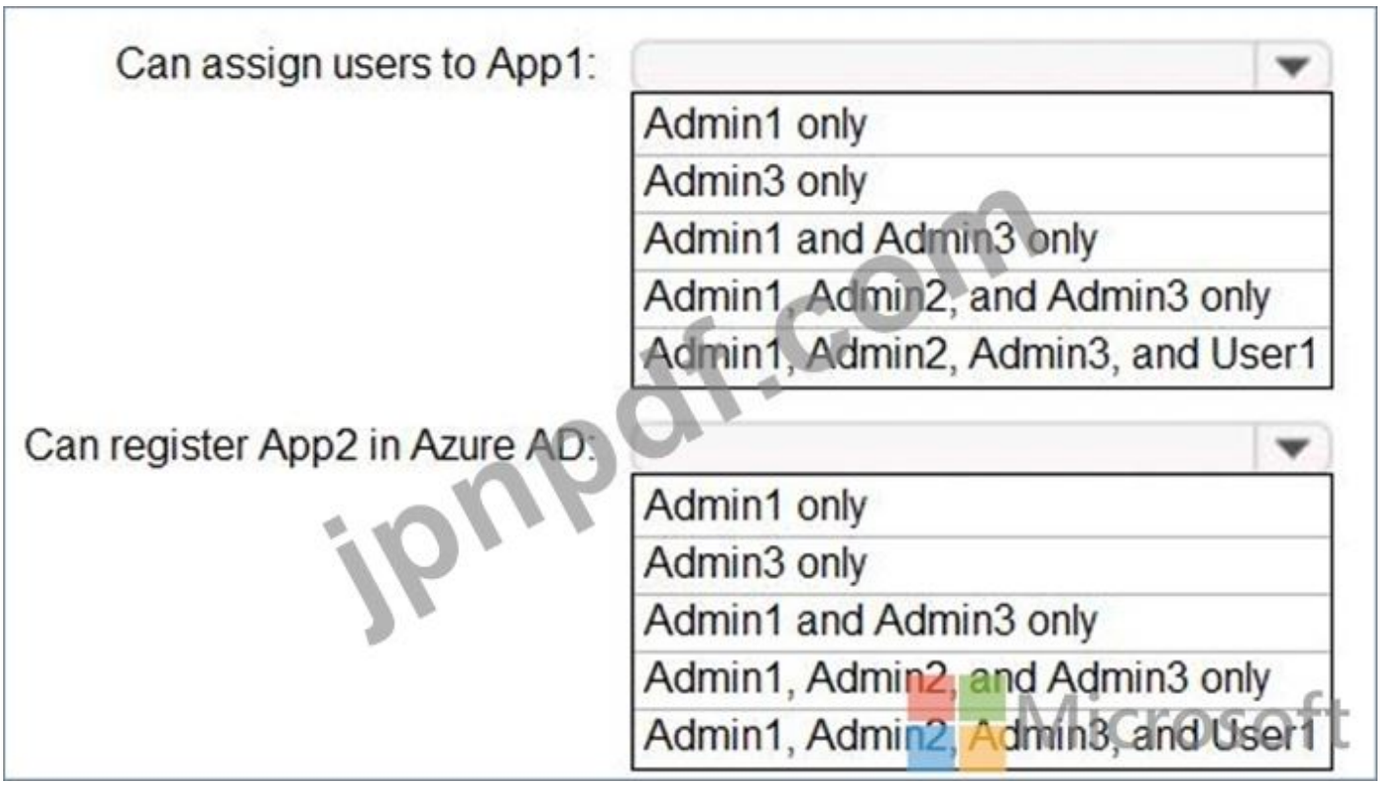
Name	Type	Member of
User1	Member	Group1
User2	Member	Group1
User3	Guest	Group1

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
* 査読者: メンバー(本人)
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とユーザー2のみ
B. ユーザー3のみ
C. ユーザー1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**)**

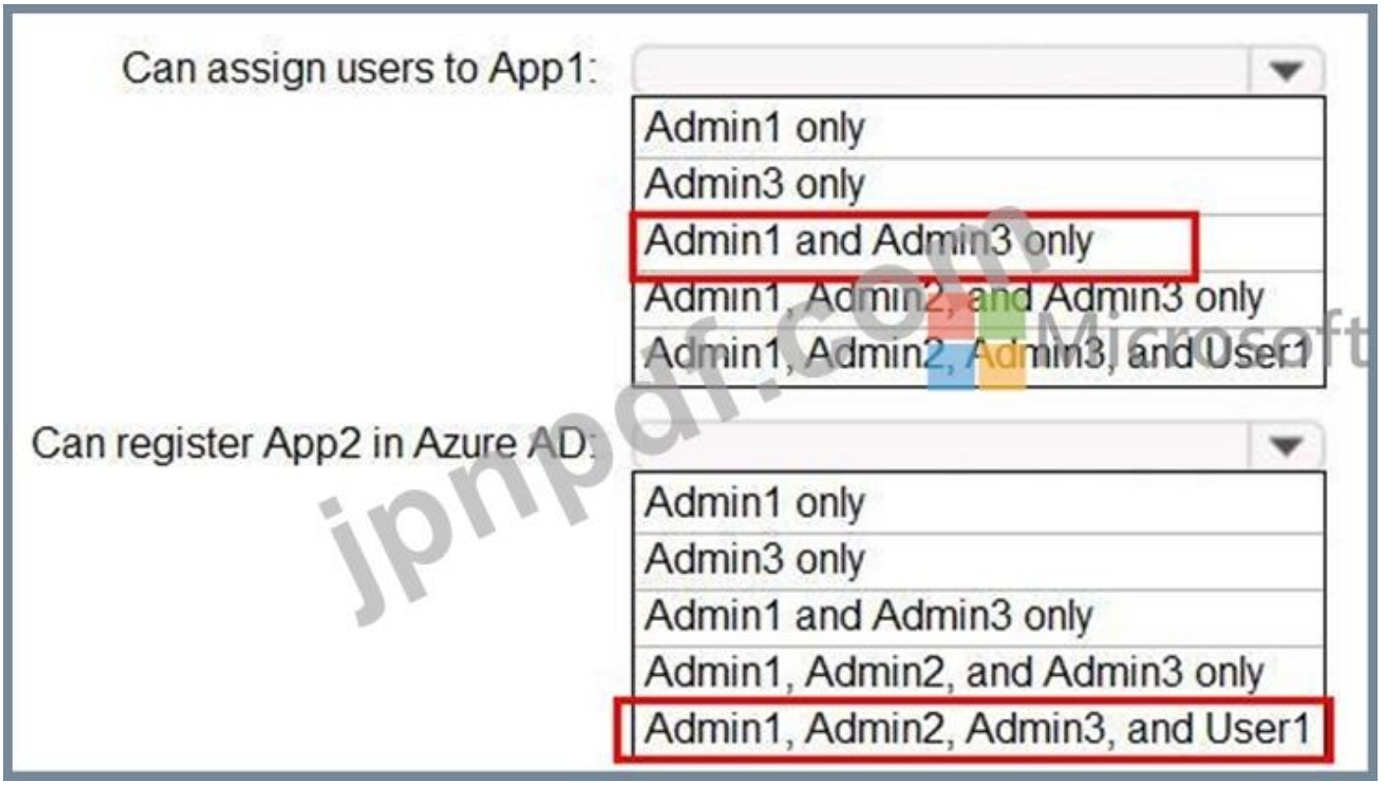
最新問題: **62**
既定のアプリ登録設定を持つ Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれています。

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

App1 と App2 という名前の 2 つのクラウド アプリを購入します。グローバル管理者は、Azure AD に App1 を登録します。
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、回答領域で適切なオプションを選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



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: 63

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なければならない 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: 正解の選択はそれぞれ 1 ポイントの価値があります。
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**)**
参照：
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/tutorial-bulk-invite

最新問題**: 64**
注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。
このセクション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) テナントと同期する 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**)**
トピック 1、Contoso, Ltd
既存の環境
Contoso のオンプレミス ネットワークには、contos.com という名前の Active Directory ドメインが含まれています。このドメインには、Contoso_Resources という名前の組織単位 (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、次のライセンスが関連付けられている 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) の間で構成されます。Contoso Resources OU のみが同期されます。
ヘルプデスク管理者は、ユーザー設定を管理するために Microsoft 365 管理センターを定期的に使用します。
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。すべてのユーザーには、次の例外を除き、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 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。次の例外を除き、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、プロジェクト管理者ロールに Azure AD Privileged Identity Management (PIM) を使用します。
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であると報告しています。

* 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しいユーザーのライセンス割り当てを簡素化します。Fabrikam のユーザーと共同マーケティング キャンペーンで協力します。アクティブ化するには正当性と承認が必要に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 は Corporation という会社を買収する予定です。Adatum という Active Directory OU に 100 人の新しい A Datum 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います。

技術要件

Contoso では、次の技術要件を特定しています。

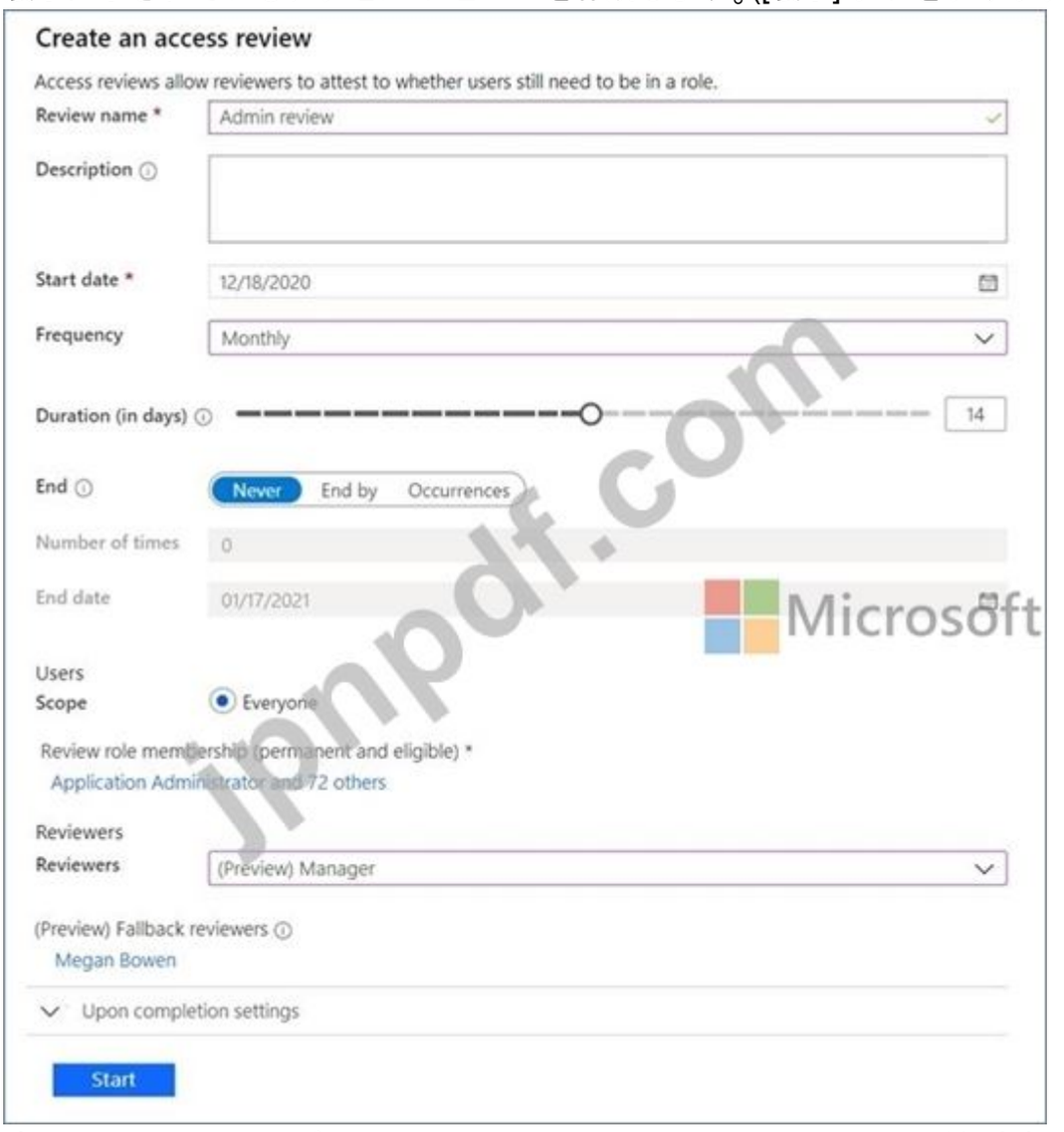
* AH ユーザーは、AD DS から contoso.com Azure AD テナントに同期する必要があります。
* App1 には https://contoso.com/auth-response を指すリダイレクト URI が必要です。
* 新規ユーザーのライセンス割り当ては、ユーザーの所在地に基づいて自動的に割り当てられる必要があります。
* Fabrikam ユーザーは、マーケティング部門の SharePoint サイトに最大 90 日間アクセスできる必要があります。
* Azure AD で実行される管理アクションは監査される必要があります。監査ログは 1 年間保持する必要があります。
* 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ライセンスのみ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**: 65**

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。

このセクション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 の部門に分かれて組織されています。
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。)



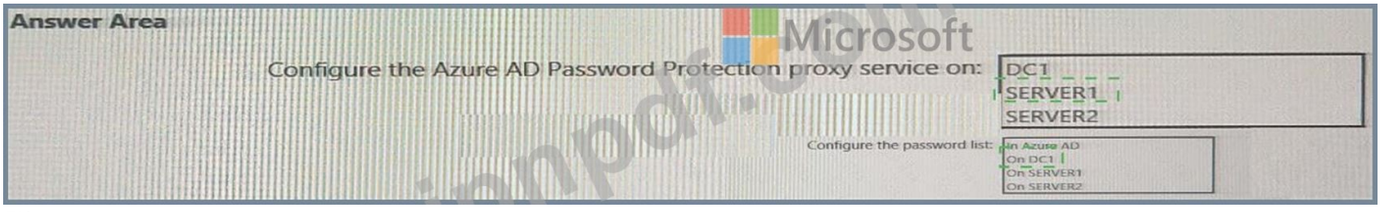
すべてのアクセス レビュー リクエストは Megan Bowen によって受信されていることがわかります。
各部門のマネージャーがそれぞれの部門のアクセスレビューを確実に受け取れるようにする必要があります。
解決策: IT 管理者ユーザー アカウントのプロパティを変更します。
これは目標を満たしていますか?
A. はい
B. いいえ
Answer: A (メーッセージを残す**)**
参照：
D18912E1457D5D1DDCBD40AB3BF70D5D
https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review

最新問題**: 66**

注: この質問は、同じシナリオを提示する一連の質問の一部です。一連の質問にはそれぞれ、定められた目標を満たす独自の解決策が含まれています。質問セットによっては、正しい解決策が複数ある場合もあれば、正しい解決策がない場合もあります。
このセクション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: 条件付きアクセス ポリシーを構成します。
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/参照:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn 認証およびアクセス管理ソリューションを実装する 質問セット 1

最新問題**: 67**
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 ポイントが付与されます。

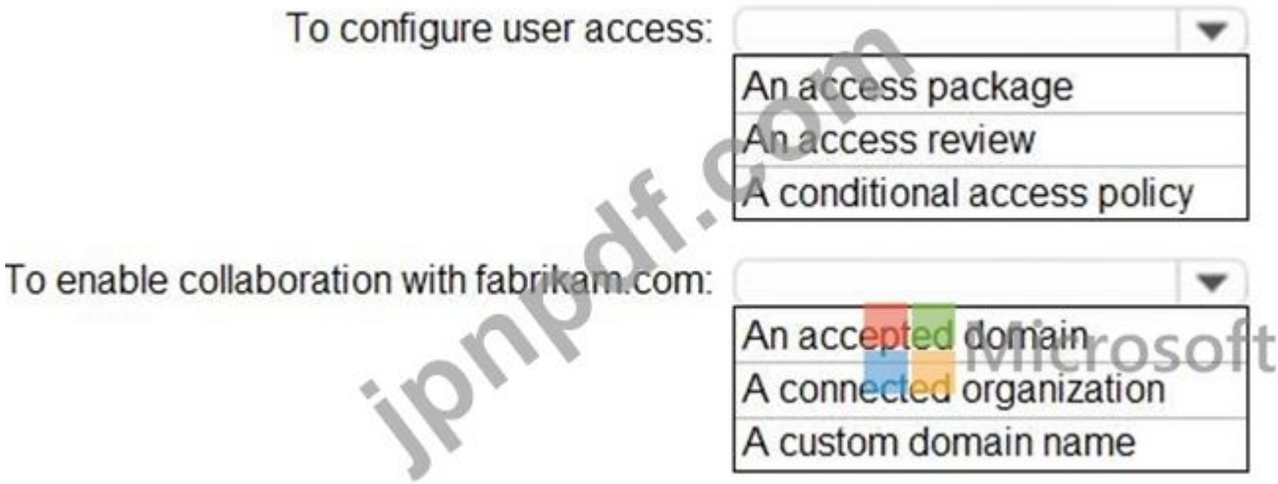
Answer:



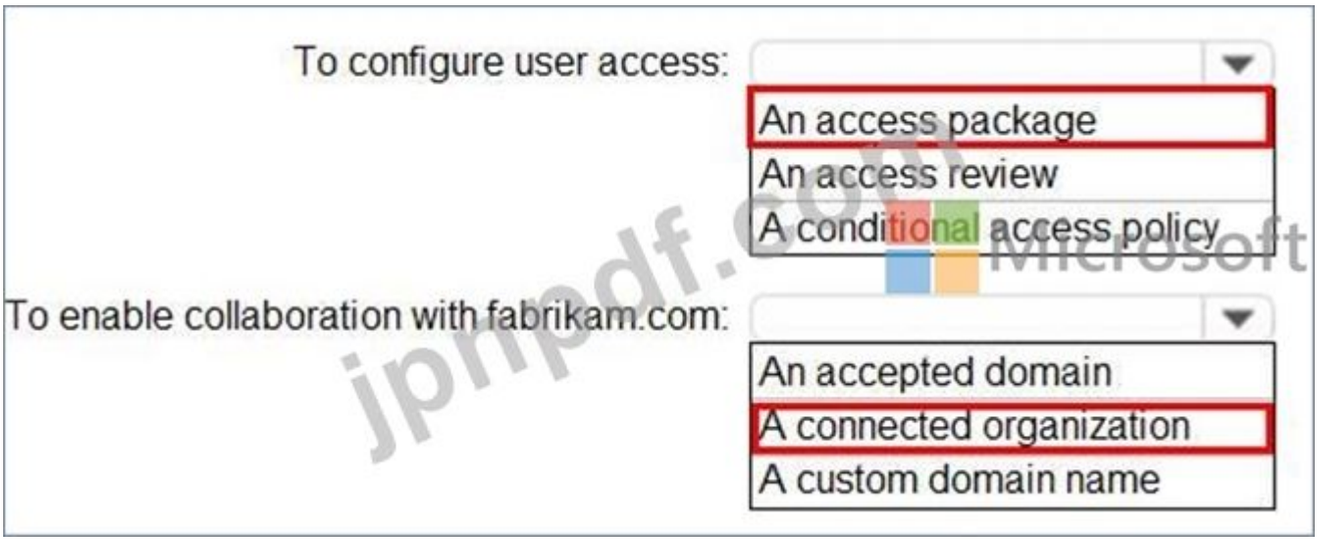
説明
サーバー1
DC1で

最新問題**: 68**
マーケティング部門の計画された変更と技術要件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。
注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:

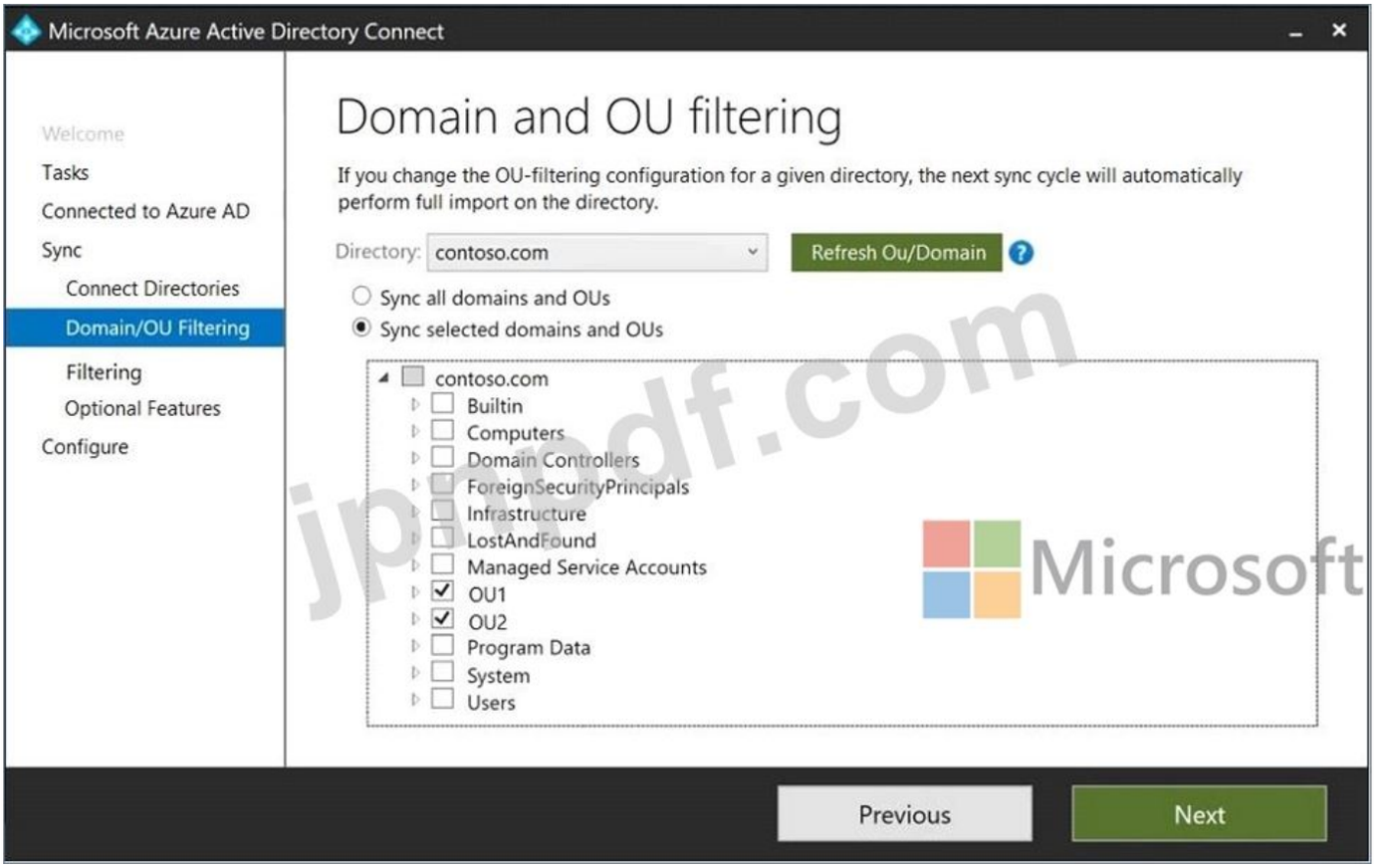


参照：
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization

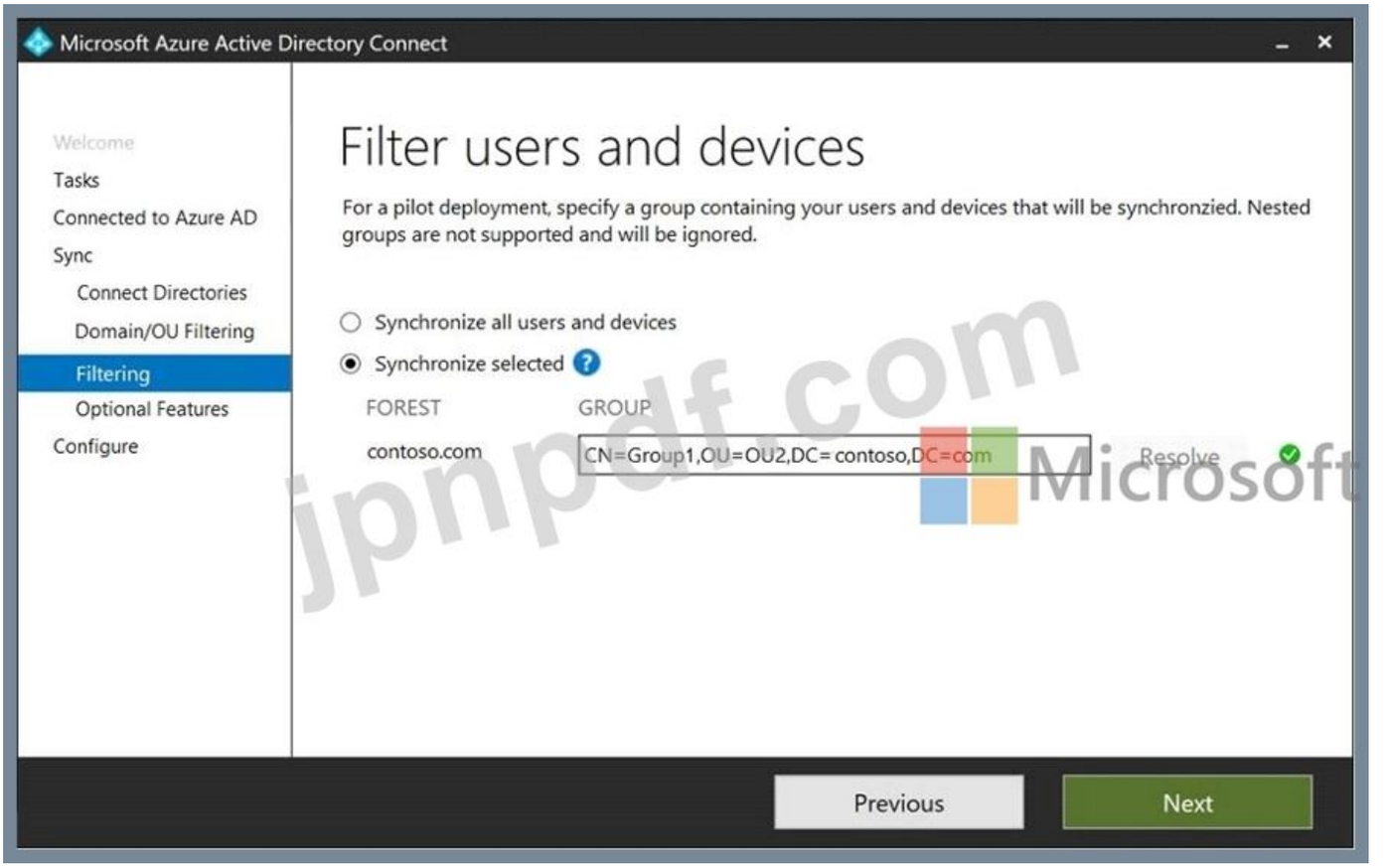
最新問題**: 69**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。このドメインには、次の表に示すオブジェクトが含まれています。

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 のフィルタリング設定を、「ドメインと OU のフィルタリング」の図に示すように構成します (「ドメインと OU のフィルタリング」タブをクリックします)。



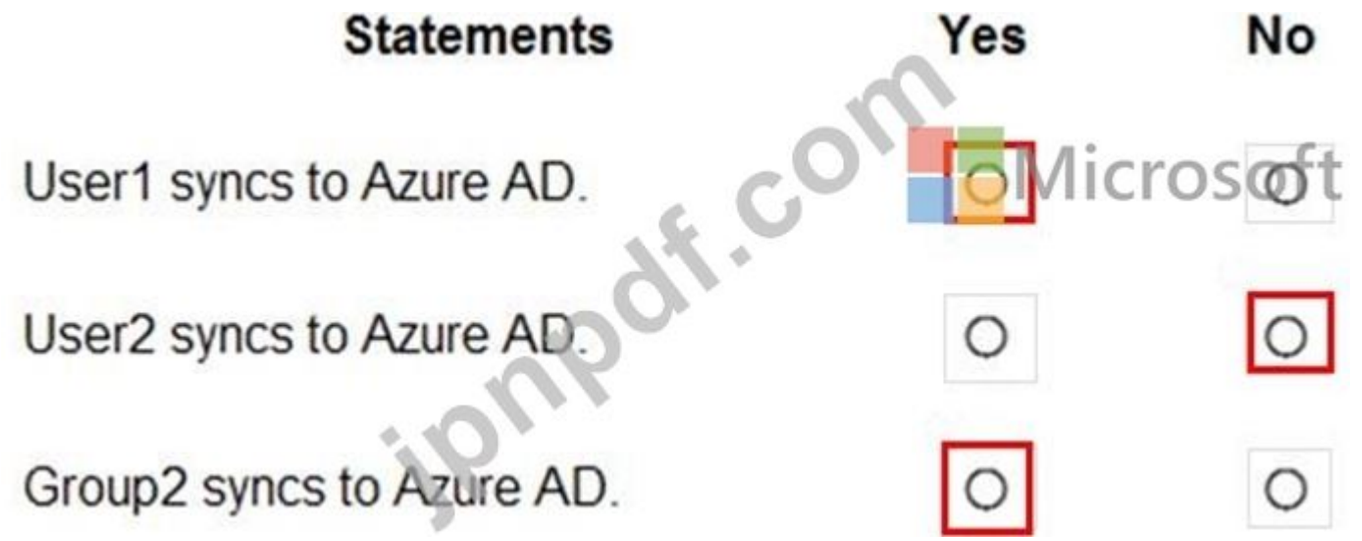
「ユーザーとデバイスのフィルター」設定は、「ユーザーとデバイスのフィルター」の図に示すように構成します。(「ユーザーとデバイスのフィルター」タブをクリックします。)



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

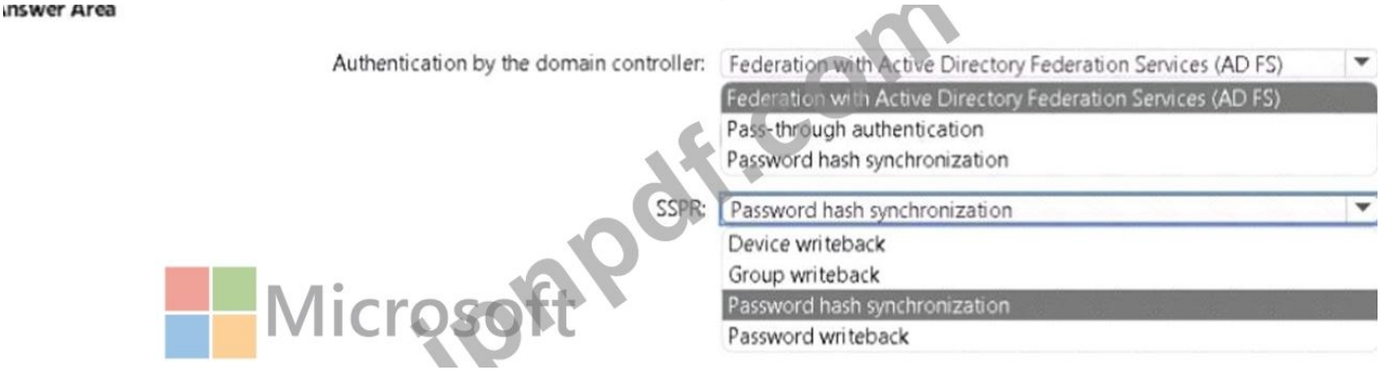
Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:

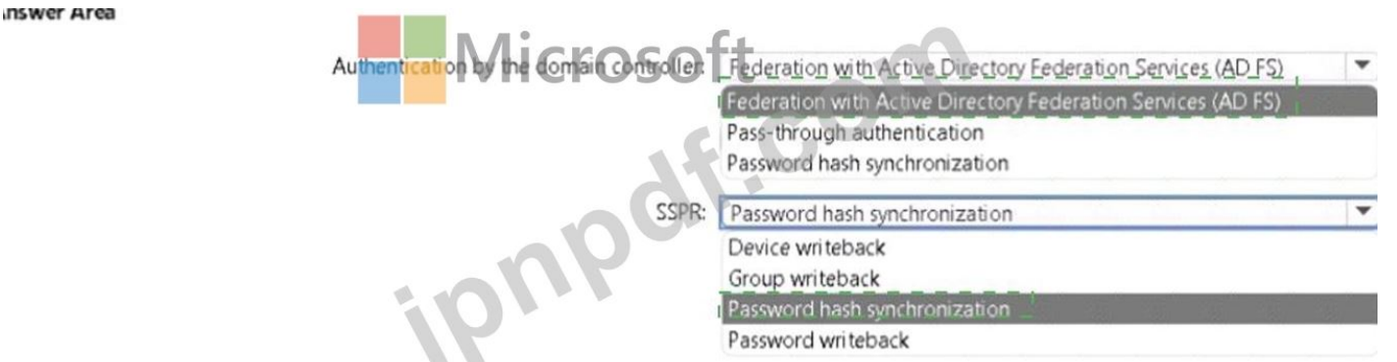


参照：
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-custom

最新問題: **70**
オンプレミス ネットワークには、Azure AD Connect を使用して Azure AD テナントと同期する Active Directory ドメインが含まれています。次の要件を満たすように Azure AD Connect を構成する必要があります。
* Azure AD へのユーザー サインインは、Active Directory ドメイン コントローラーによって認証される必要があります。
* Active Directory ドメイン ユーザーは、Azure AD セルフサービス パスワード リセット (SSPR) を使用できる必要があります。
各要件には何を使用すればよいですか? 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 ポイントが付与されます。



Answer:



説明

最新問題**: 71**

User1 という名前のユーザーを含む Microsoft Entra テナントがあります。

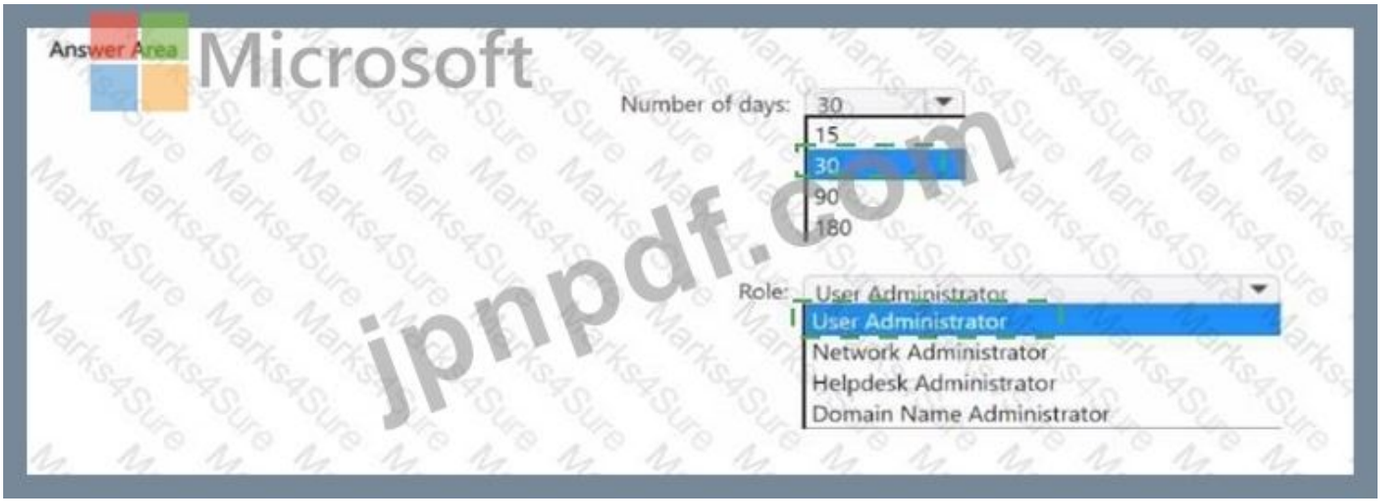
管理者が User1 を削除します。次の点を特定する必要があります。

* User1 アカウントを復元できるオプションの最大日数は何ですか?

* User1 を復元するために使用できる最も権限の少ないロールはどれですか?

回答するには、回答エリアで適切なオプションを選択します。注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer:



Explanation:

最新問題**: 72**

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?

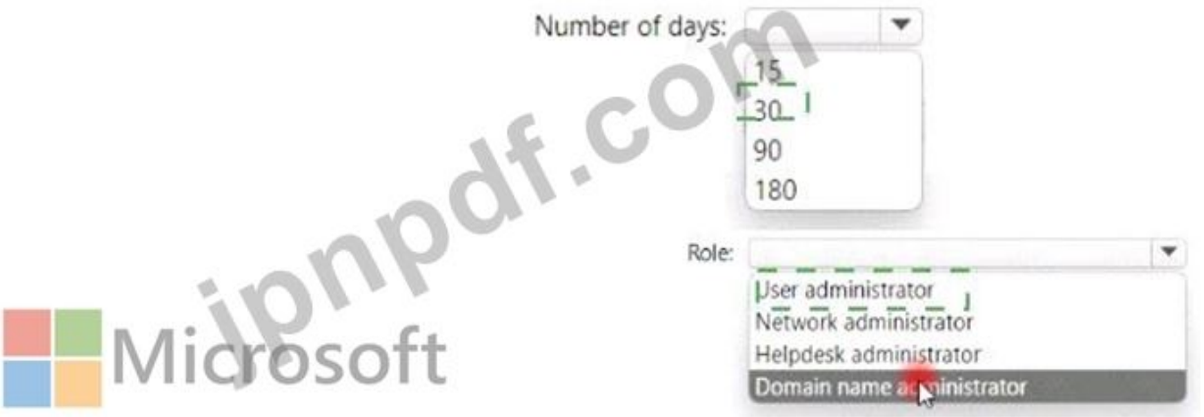
* User1 を復元するために使用できる最も権限の少ないロールはどれですか?

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Answer Area



説明

最新問題**: 73**

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。

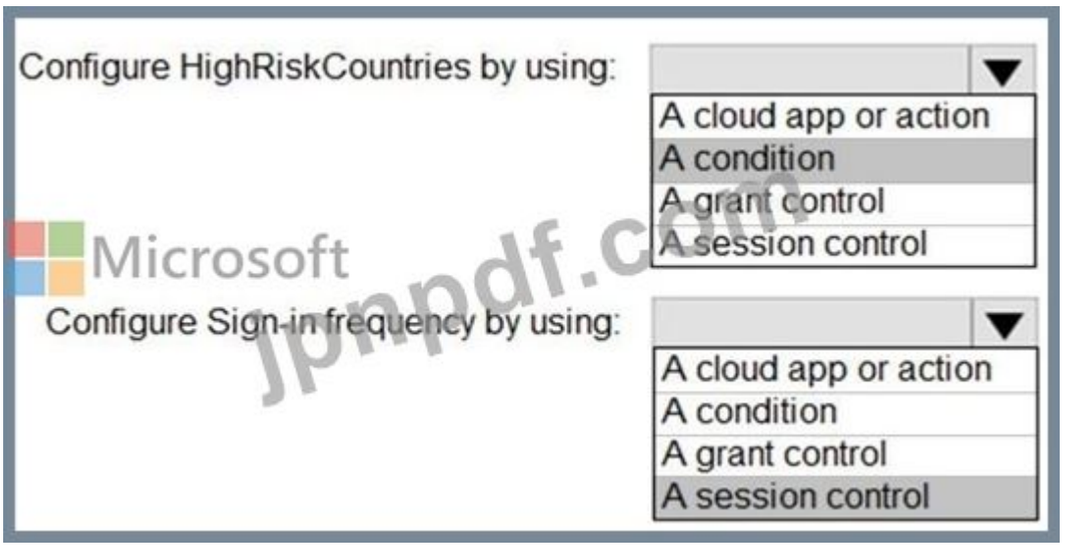
高リスクの国から接続する場合、ユーザーが認証されたままでいられる時間を制限する必要があります。

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ます。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:



参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

最新問題**: 74**
fabrikam.com というドメインを使用する Microsoft 365 テナントがあります。Azure Active Directory (Azure AD) のゲスト招待設定は、図に示すように構成されています。([図] タブをクリックします。)

bsmith@fabrikam.com というユーザーは、次の表に示すユーザーと Microsoft SharePoint Online ドキュメント ライブラリを共有します。

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

どのユーザーにパスコードがメールで送信されますか?

A. ユーザー2のみ

B. ユーザー1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: A (メーッセージを残す)
参照：
https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

最新問題: **75**
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。
次の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

最新問題**: 76**

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。

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

最新問題: **77**

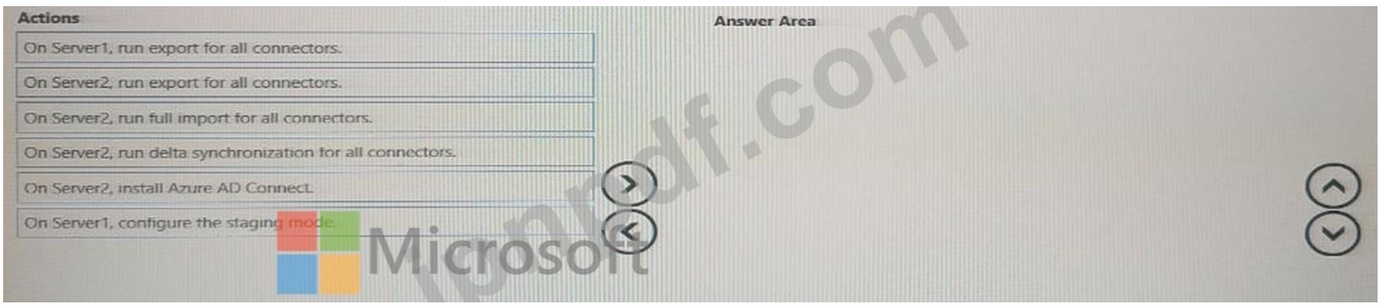
ネットワークには、Azure AD Connect を使用して contoso.com という名前の Azure Active Directory (Azure AD) テナントにリンクされている contoso.com という名前の Active Directory フォレストが含まれています。

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 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。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。

どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクション リストから適切なアクションを回答領域に移動し、正しい順序で並べます。



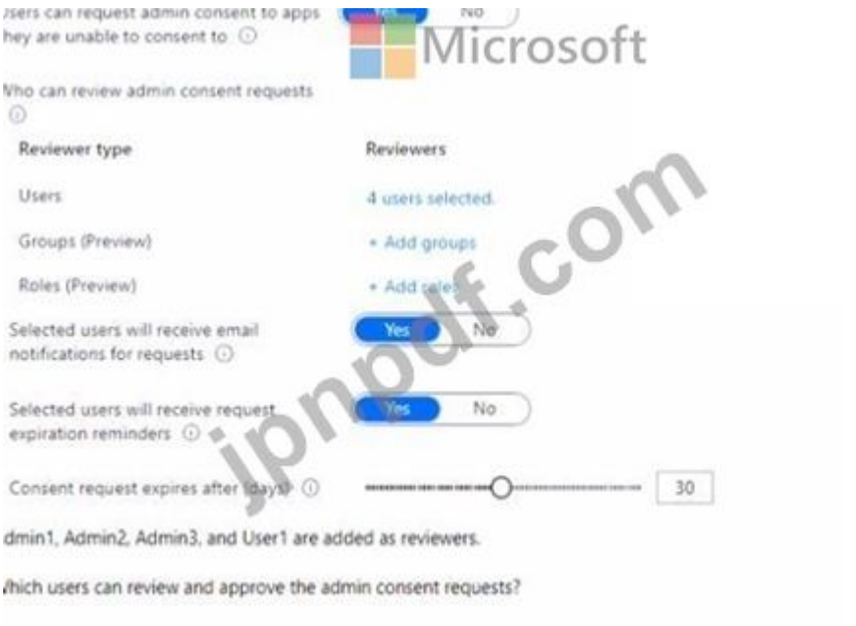
Answer:

1 - サーバー2でフル実行します。
2 - server2 で delta を実行します...
3 - サーバー 1 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**: 78**
次の表に示すユーザーを含む Azure AD テナントがあります。

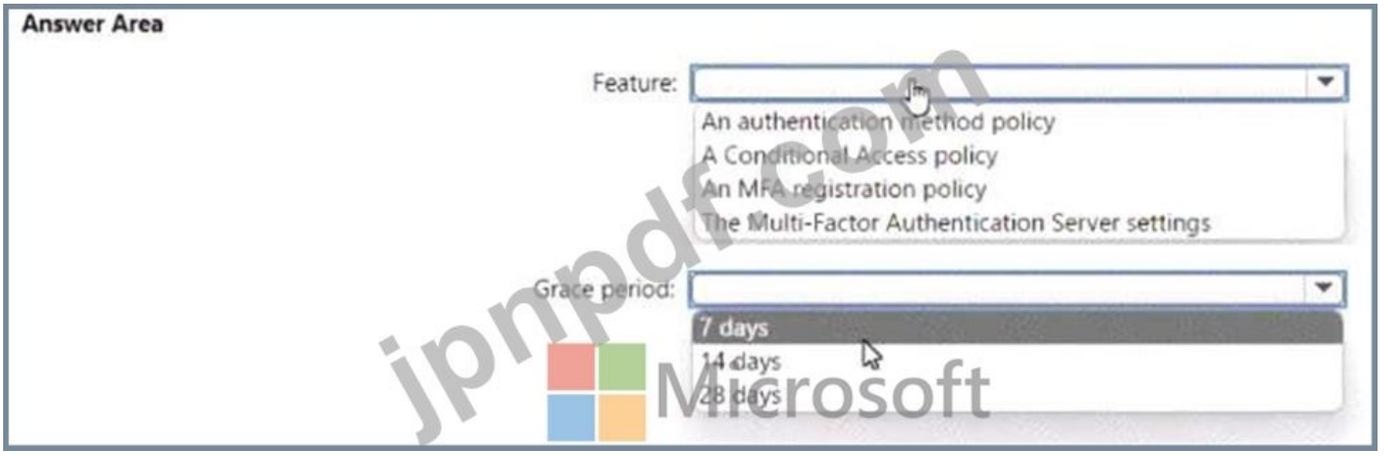
Name	Role
Admin1	Cloud application administrator
Admin2	Application administrator
Admin3	Security administrator
User1	*None*

App1 という名前のエンタープライズ アプリケーションを Azure AD に追加し、User1 を App1 の所有者として設定して、アプリを使用する前に Azure AD にアクセスするための管理者の同意が必要になります。
次の図に示すように、管理者の同意リクエストを強力に構成します。
管理者の同意リクエスト。



A. Admm1、Admm2、Admin3のみ
B. Admm1 と Admin2 のみ
C. Admln1、Admin2、User1のみ
D. Admm1のみ
E. Admm1、Admm2、Admm3、およびUser1
Answer: C (メーッセージを残す)

最新問題: **79**
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。
どの機能を使用すべきですか? 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 ポイントが付与されます。



Answer:

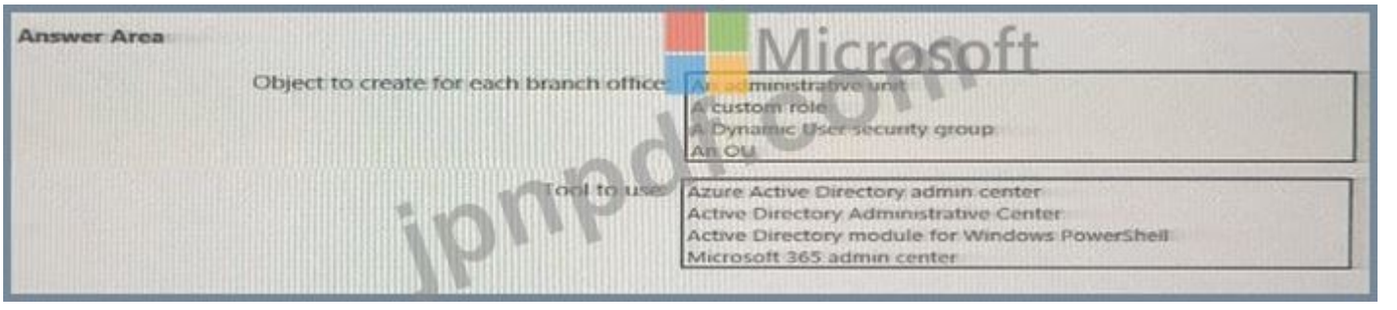
Explanation:

最新問題**: 80**

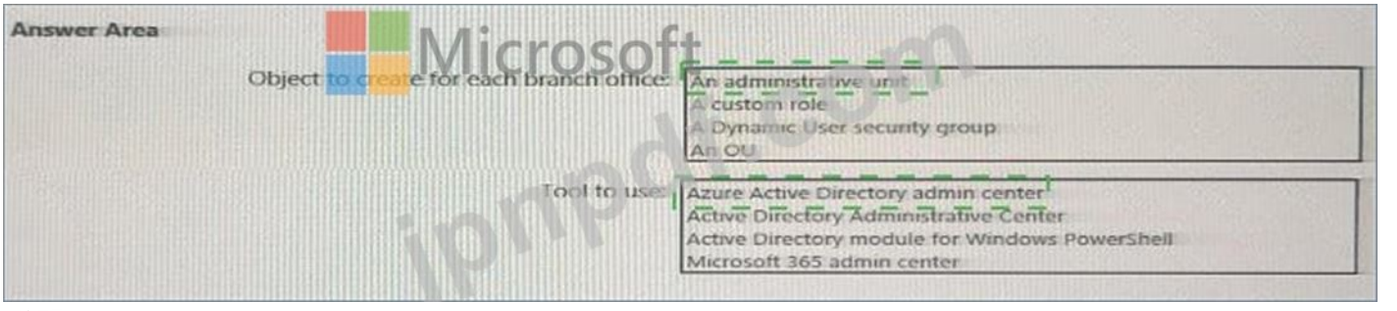
ヘルプデスク管理者によるライセンス管理の技術要件を満たす必要があります。

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 ポイントが付与されます。



Answer:



説明

テキストの説明は自動的に生成されます

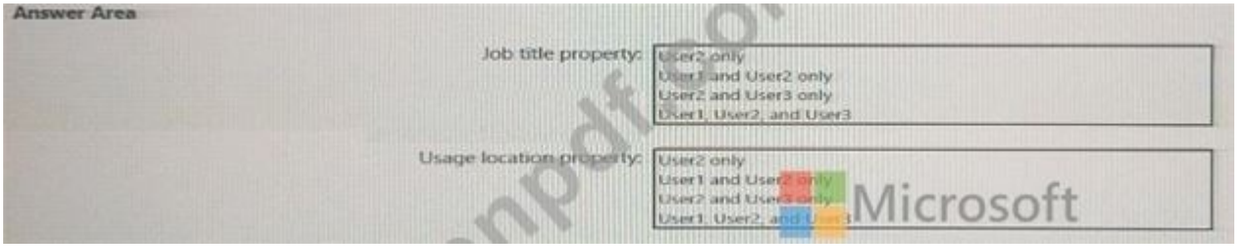
最新問題: **81**

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。

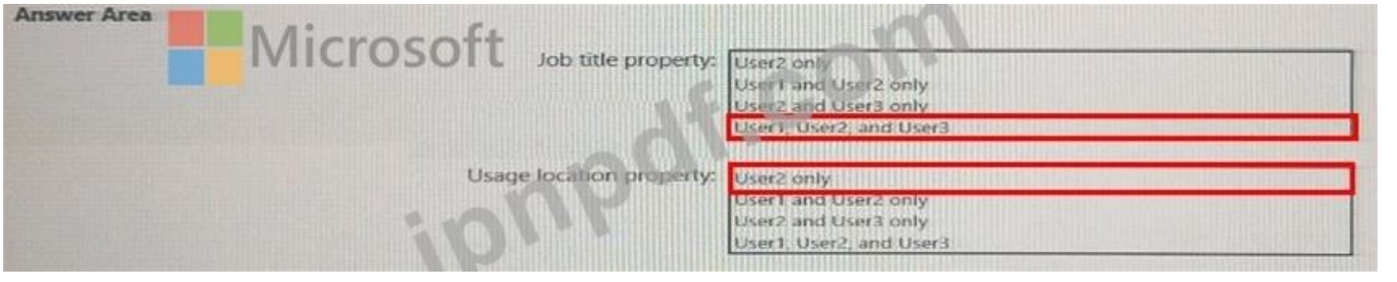
Name	Type	Directory synced
User1	Member	Yes
User2	Member	No
User3	Guest	No

Azure AD で役職プロパティと使用場所プロパティを構成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ます。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



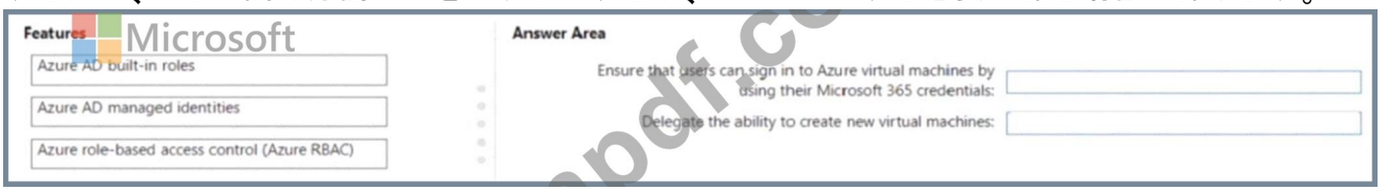
最新問題: **82**

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、次の要件を満たす必要があります。

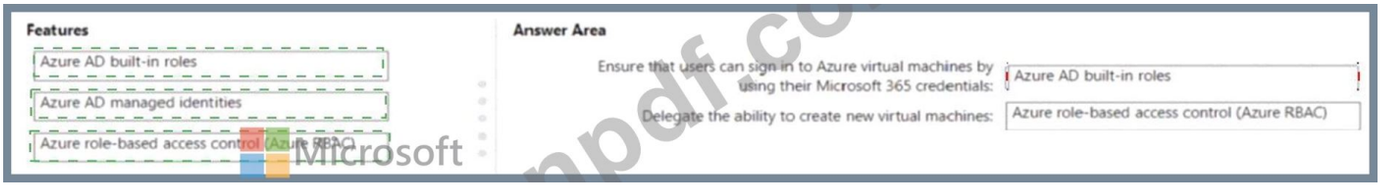
* ユーザーが Microsoft 365 資格情報を使用して Azure 仮想マシンにサインインできることを確認します。

* 新しい仮想マシンを作成する権限を委任します。

各要件には何を使用する必要がありますか? 回答するには、適切な機能を正しい要件にドラッグします。各機能は 1 回、複数回、またはまった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:



説明

最新問題**: 83**

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 ドレス範囲があります。

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

ガント

* 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 個です
* ポリシーを有効にする: オン
次の各文が正しい場合は「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 ポイントが与えられます。

Answer:

最新問題: **84**
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. 更新-MsolfederatedDomain
D. Set-MsolDomain
Answer: A (メーッセージを残す**)**
説明/参照:
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

最新問題: **85**
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。
遠隔地から作業する場合、ユーザーは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: C (メーッセージを残す**)**
Windows 10 では、Windows Hello for Business により、PC およびモバイル デバイスでのパスワードが強力な 2 要素認証に置き換えられます。この認証は、デバイスに関連付けられ、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 段階認証を行うと、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を実行して自分の身元を確認します。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: **86**
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

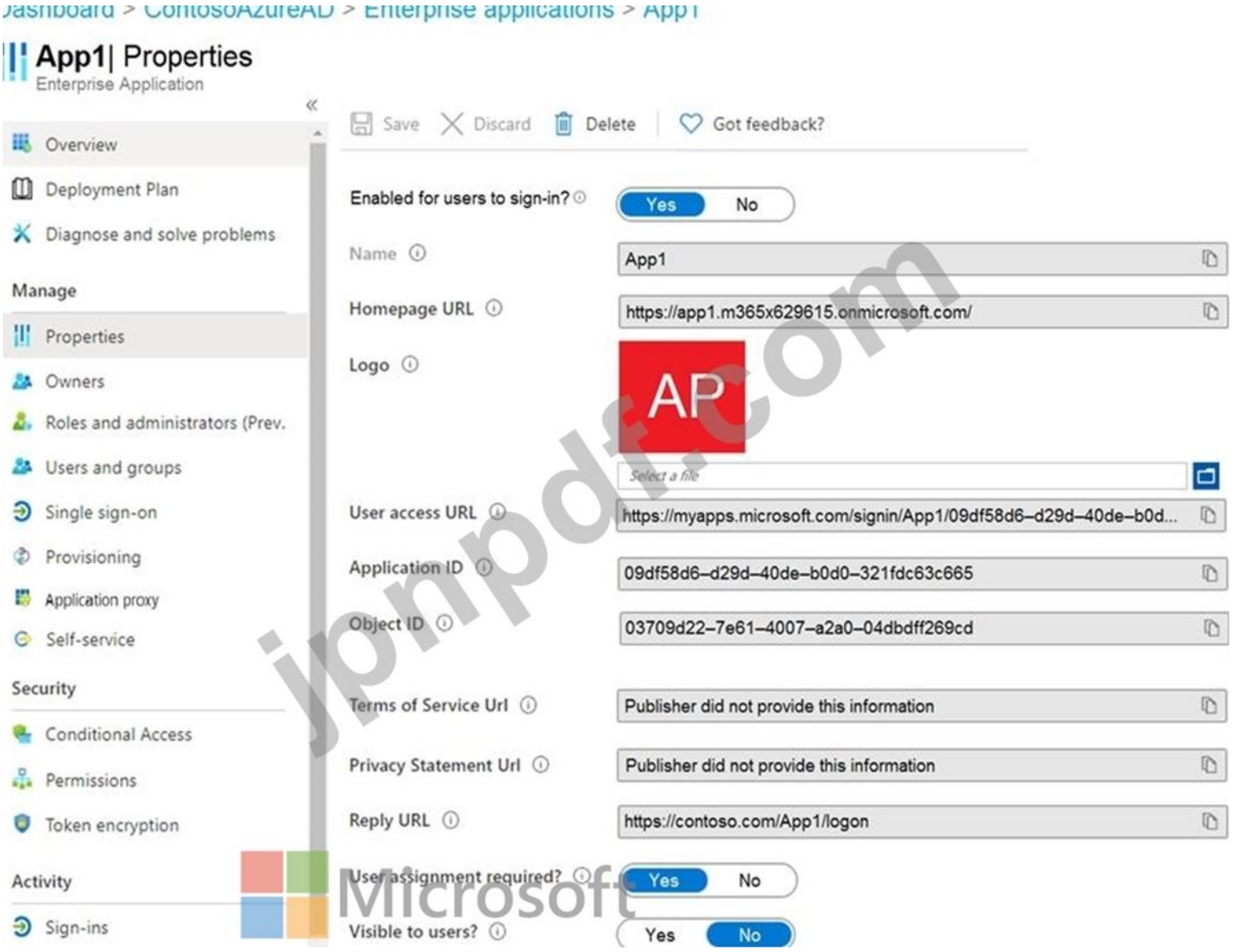
次の表に示すアプリ登録があります。

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

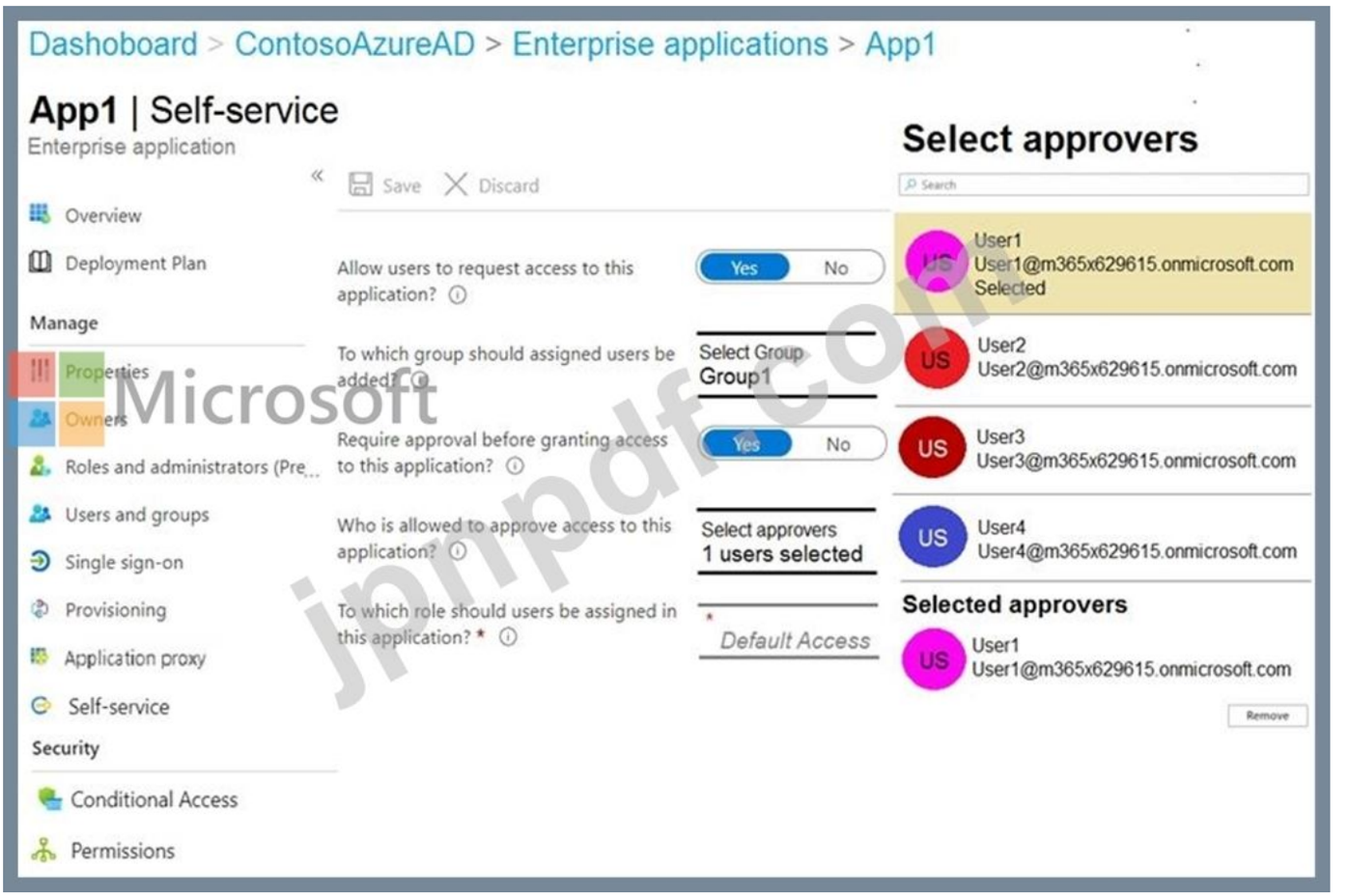
会社のポリシーにより、ユーザー権限の変更は禁止されています。
社内の各ユーザーのカレンダーに予定を作成できるのはどのユーザーですか?
A. ユーザー3
B. ユーザー1
C. ユーザー4
D. ユーザー2
Answer: A (メーッセージを残す**)**

最新問題**: 87**
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。)



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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

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.	○	○

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: **88**
contoso.com の SMTP アドレス空間を使用する 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. 更新-MsolfederatedDomain
D. Set-MsolDomain
Answer: A (メーッセージを残す**)**
説明
https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-self-service-signup

最新問題: **89**
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: (解答を表示する**)**
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: **90**
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 アクセス許可を使用します。どのロールを複製して Role3 を作成できますか?

A. ロール2のみ
B. 組み込みの Azure サブスクリプション ロールと組み込みの Azure AD 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. Role1、Role2 組み込み Azure サブスクリプション ロール、および組み込み Azure AD ロール
E. 組み込みの Azure サブスクリプション ロールのみ
Answer: A (メーッセージを残す**)**

最新問題**: 91**
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、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、正しい順序で並べます。

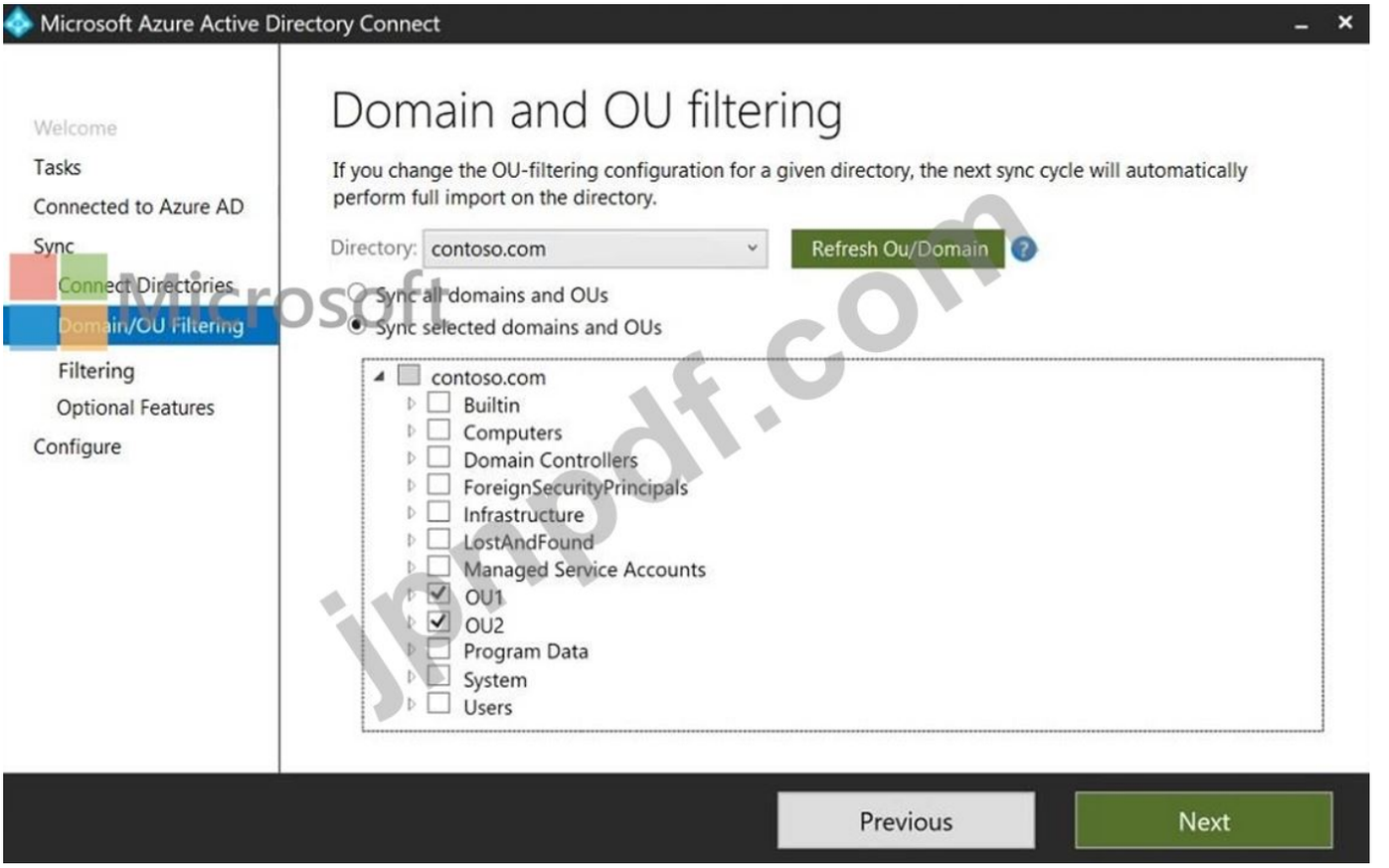
Answer:

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/en-us/cloud-app-security/session-policy-aad

最新問題: **92**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。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 のフィルタリング設定を、「ドメインと OU のフィルタリング」の図に示すように構成します (「ドメインと OU のフィルタリング」タブをクリックします)。



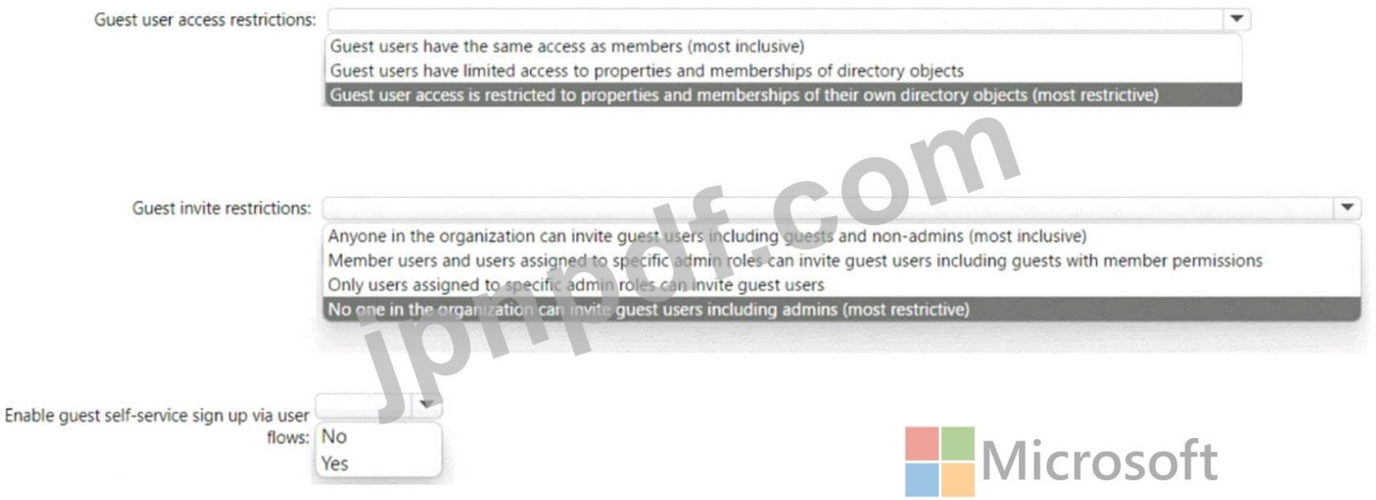
「ユーザーとデバイスのフィルター」設定は、「ユーザーとデバイスのフィルター」の図に示すように構成します。(「ユーザーとデバイスのフィルター」タブをクリックします。)

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

Answer:

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: **93**
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ます。



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電子メール アドレスを照会できなくなり、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ようになります。

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 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: **94**

新しい Microsoft 365 E5 テナントを作成します。

ユーザーが匿名 IP アドレスから Microsoft 365 ポータルに接続するときに、多要素認証 (MFA) を使用するように求めるメッセージが表示されるようにする必要があります。

何を設定すればよいでしょうか?

A. ユーザーリスクポリシー

B. MFA登録ポリシー

C. サインインリスクポリシー

Answer: C (メーッセージを残す**)**

最新問題: **95**

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。ドメインには、次の表に示すサーバーが含まれます。

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

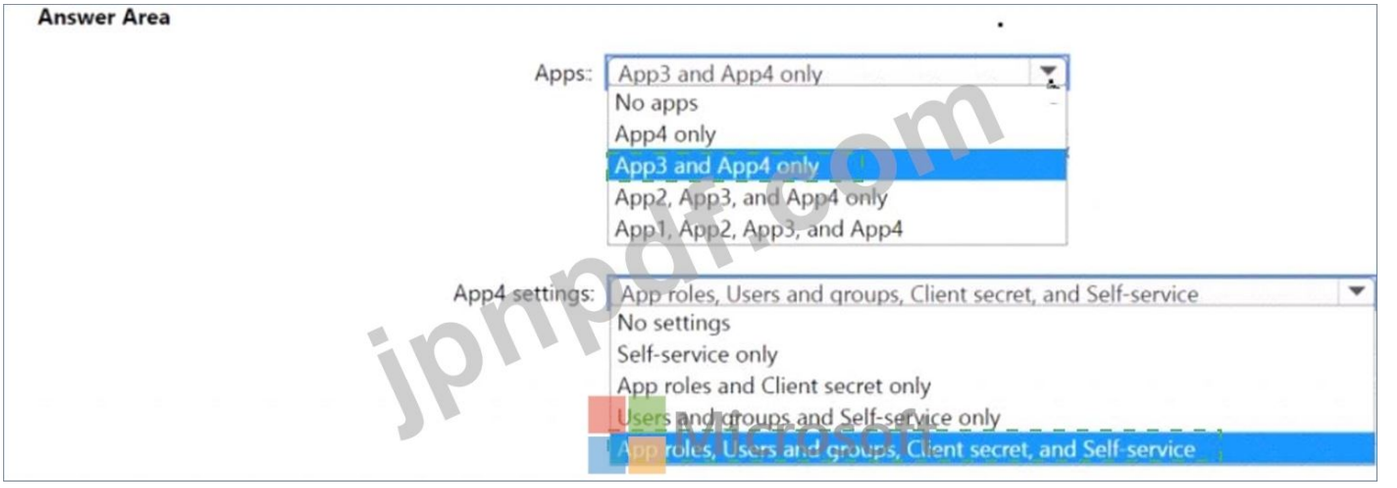
ドメイン コントローラーはインターネットとの通信ができなくなります。
Server1 と Server2 に Azure AD パスワード保護を実装します。
Windows Server 2019 を実行する Server4 という名前の新しいサーバーを展開します。
1 台のサーバーに障害が発生した場合でも、Azure AD パスワード保護が引き続き機能することを確認する必要があります。
Server4 に何を実装する必要がありますか?
A. Azure AD コネクト
B. Azure AD アプリケーション プロキシ
C. パスワード変更通知サービス (PCNS)
D. Azure AD 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-premisesdep

最新問題**: 96**
Azure AD テナントがあります。
次の表に示すタスクを実行します。

Date	Task
March 1	Register four enterprise applications named App1, App2, App3, and App4.
March 15	From the tenant, update the following settings for App1: App roles, Users and groups, Client secret, and Self-service.
March 20	From the tenant, update the following settings for App2: App roles, Users and groups, Client secret, and Self-service.
March 25	From the tenant, update the following settings for App3: App roles, Users and groups, Client secret, and Self-service.
March 30	From the tenant, update the following settings for App4: App roles, Users and groups, Client secret, and Self-service.

4 月 5 日に、管理者は App1、App2、App3、および App4 を削除します。
アプリと設定を復元する必要があります。
4 月 16 日に復元できるアプリはどれですか。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 ポイントが付与されます。

Answer:



Explanation:

携帯電話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**: 97**

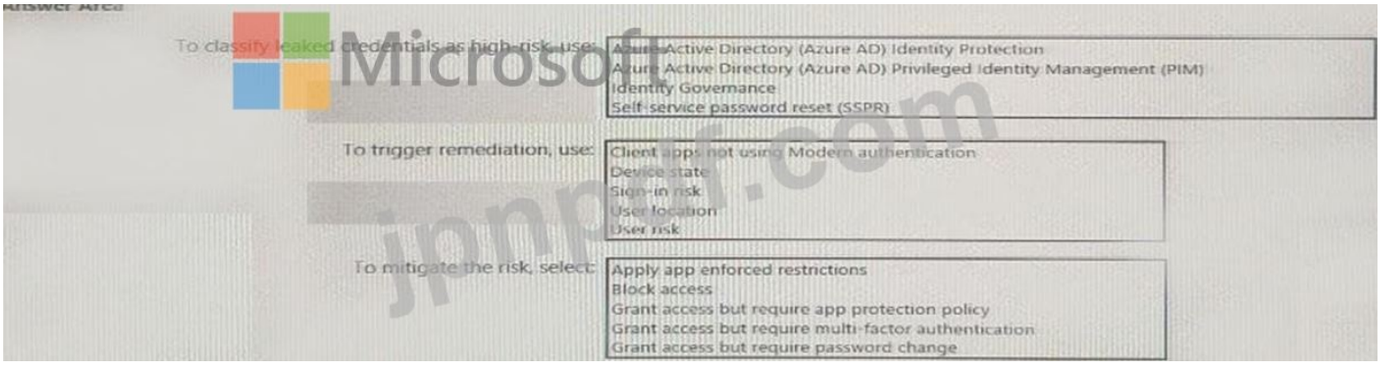
Microsoft 365 テナントがあります。

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。ソリューションは次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扱います。
* 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 ポイントが付与されます。



Answer:

トピック 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、従業員は米国全土にいます。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。

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 Azure Active Directory (Azure AD) テナントにリンクされた litware.com という名前の Active Directory フォレストが含まれています。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 という名前の 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 のすべてのユーザーは、Microsoft 365 Enterprise E5 ライセンスを所有しています。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。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

両方の Litware オフィスはインターネットに直接接続しています。両方のオフィスは、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。すべてのオンプレミス ドメイン コントローラーはインターネットにアクセスできません。

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。

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 属性の値を変更して、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。
* 外部に漏洩した認証情報を自動的に検出し、修復します

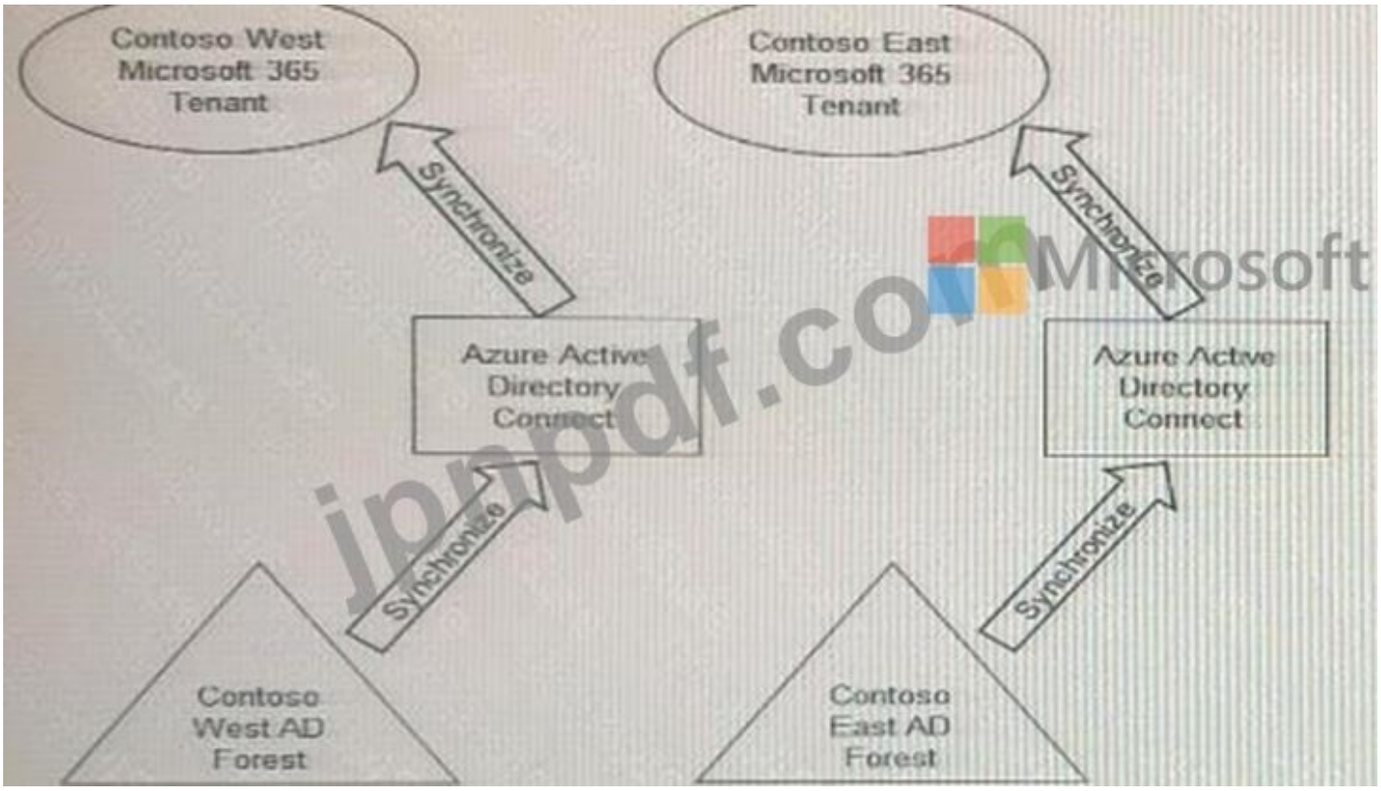
アクセス要件

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。

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を検出したいと考えています。

最新問題: **98**
会社には、Contoso East と Contoso West という 2 つの部門があります。両方の部門の Microsoft 365 ID アーキテクチャを次の図に示します。

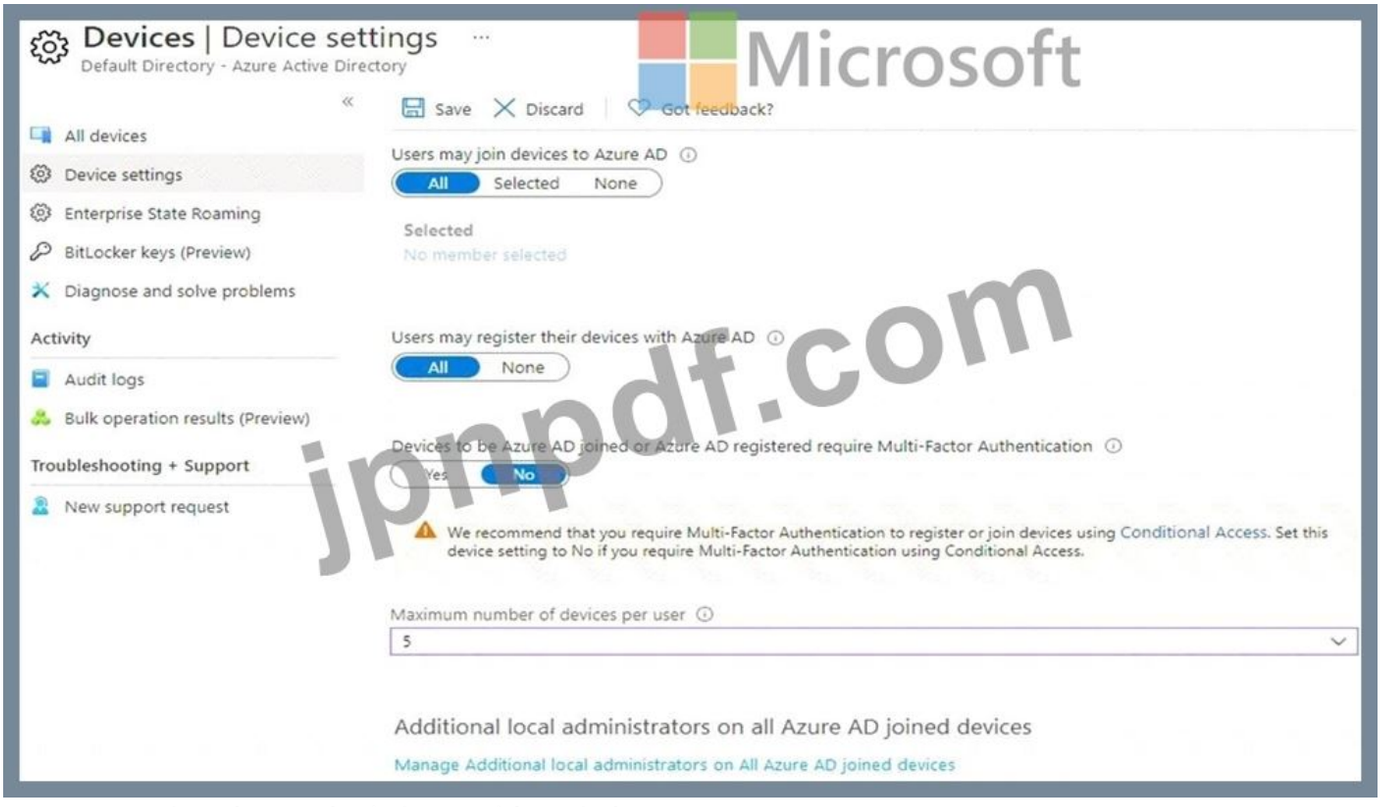


Contoso East 部門のユーザーに、Contoso West テナントの Microsoft SharePoint Online サイトへのアクセスを割り当てる必要があります。ソリューションでは、追加の Microsoft 3G5 ライセンスは必要ありません。
何をすべきでしょうか?
A. Contoso Cast の既存の Azure AD Connect サーバーを構成して、Contoso East Active Directory フォレストを Contoso West テナントに同期します。
B. 2 番目の Azure AD Connect サーバーを Contoso East 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。
C. 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。
D. Contoso East ユーザーを Contoso West テナントのゲストとして招待します。
Answer: A (メーッセージを残す**)**

最新問題: **99**
Azure Active Directory Premium Plan 2 ライセンスを持つ Azure Active Directory (Azure AD) テナントがあります。テナントには、次の表に示すユーザーが含まれています。

Name	Role
Admin1	Cloud device administrator
Admin2	Device administrator
User1	None

次の図に示すデバイス設定があります。



User1 には次の表に示すデバイスがあります。

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

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

注意: 正しい選択ごとに 1 ポイントが付与されます。

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

Answer:

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

Explanation:
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**: 100**
fabrikam.com というドメインを使用する Microsoft 365 テナントがあります。Azure Active Directory (Azure AD) のゲスト招待設定は、図に示すように構成されています。([図] タブをクリックします。)

bsmith@fabrikam.com というユーザーは、次の表に示すユーザーと Microsoft SharePoint Online ドキュメント ライブラリを共有します。

Name	Email	Description
User1	User1@contoso.com	A guest user in fabrikam.com
User2	User2@outlook.com	A user who has never accessed resources in fabrikam.com
User3	User3@fabrkam.com	A user in fabrikam.com

どのユーザーにパスコードがメールで送信されますか?

A. ユーザー2のみ

B. ユーザー1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: A (メーッセージを残す**)**

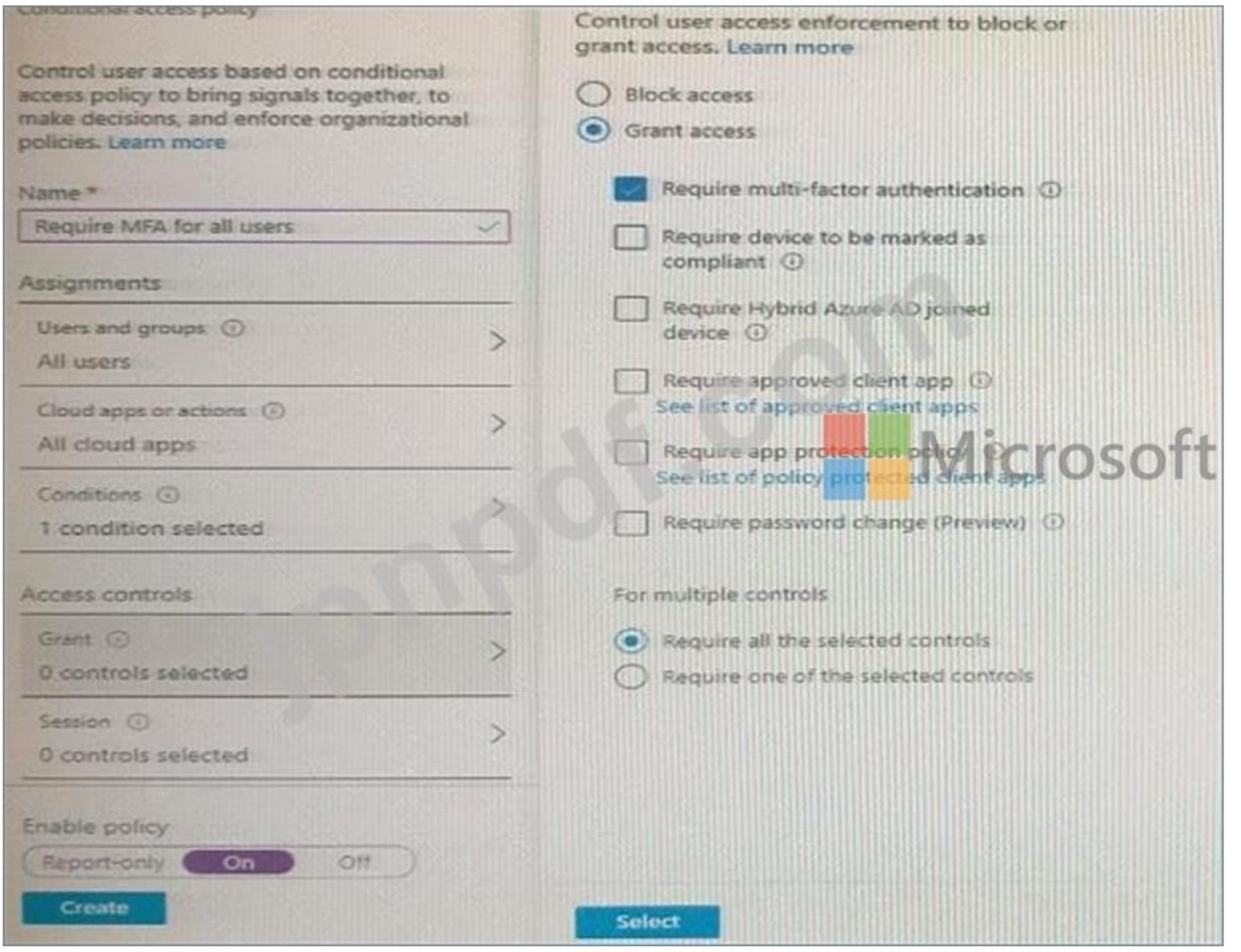
参照：

https://docs.microsoft.com/en-us/azure/active-directory/external-identities/one-time-passcode

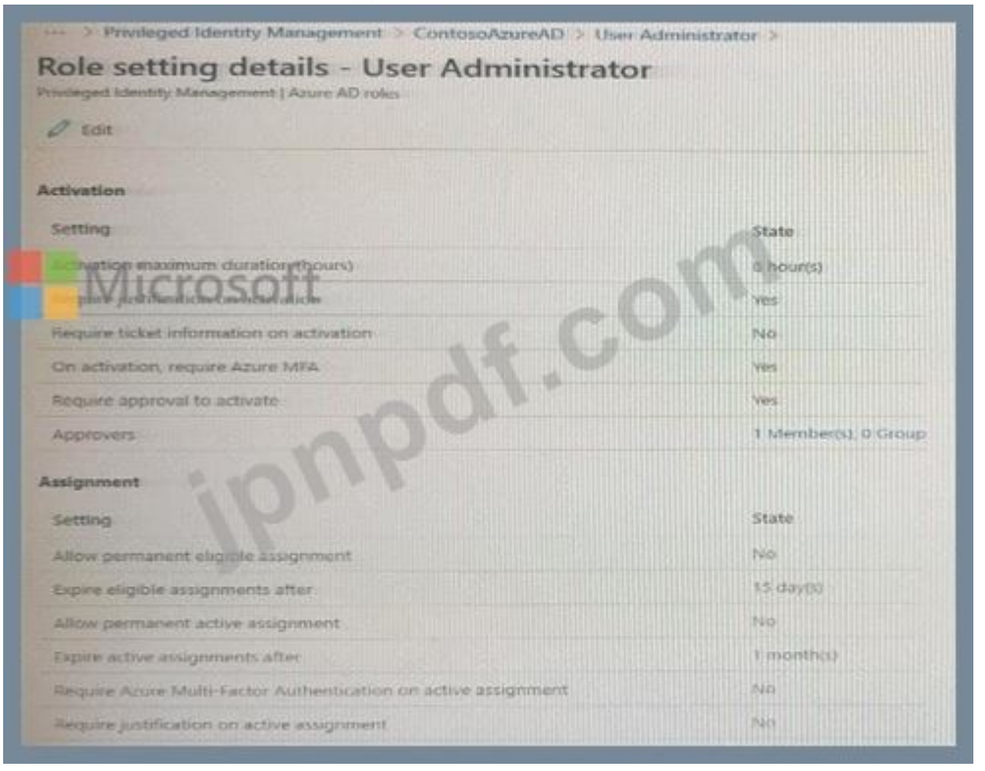
最新問題**: 101**

Microsoft 365 テナントがあります。

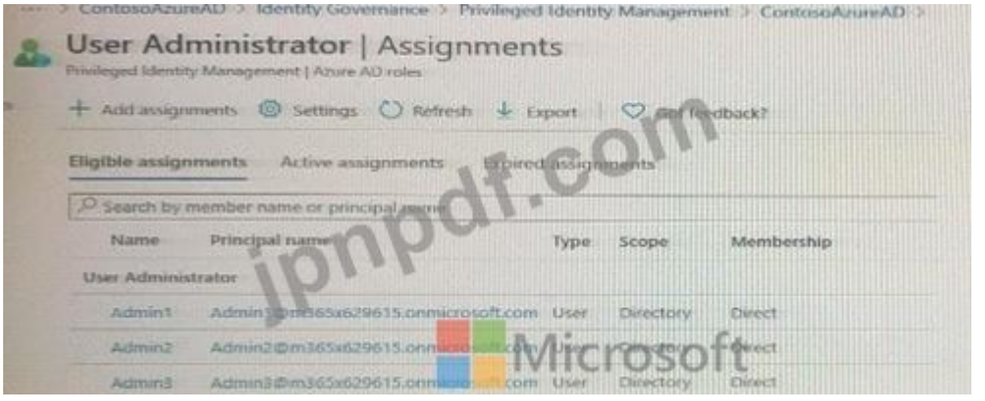
条件付きアクセス ポリシーは、条件付きアクセス ポリシーの図に示すように構成します。([条件付きアクセス ポリシー] タブをクリックします。)



ユーザー管理者ロール設定は、ロール設定の詳細図に示す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。)

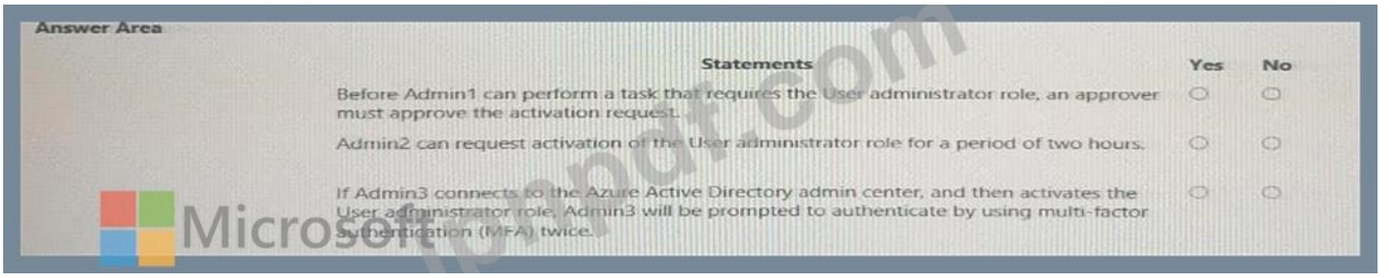


ユーザー管理者ロールの割り当ては、「ロールの割り当て」展示に示されているように表示されます。(「ロールの割り当て」ラボをクリックします。)

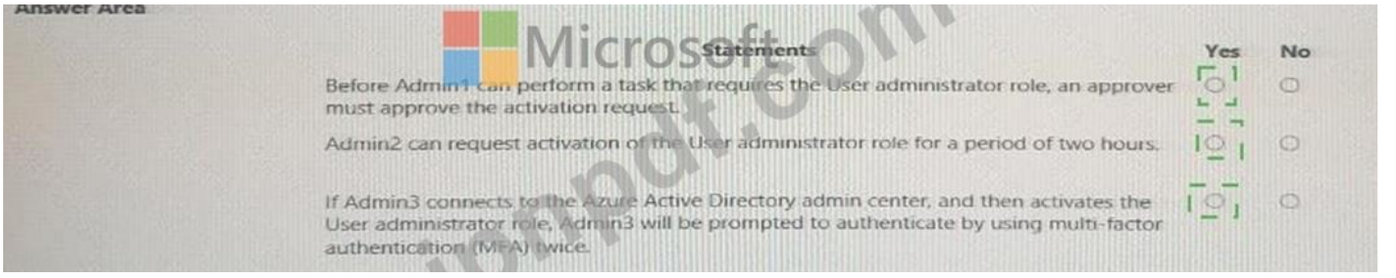


次の各文について、その文が正しい場合は 「はい」を選択します。そうでない場合は 「いいえ」を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。



Answer:



説明

はい

はい

はい

最新問題**: 102**

User1 という名前のユーザーを含む Sub1 という名前の Azure サブスクリプションがあります。

User1 が Sub1 の Microsoft Entra Permissions Management ライセンスを購入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。

User1 に割り当てるべきロールはどれですか?

A. グローバル管理者

B. 権限管理管理者

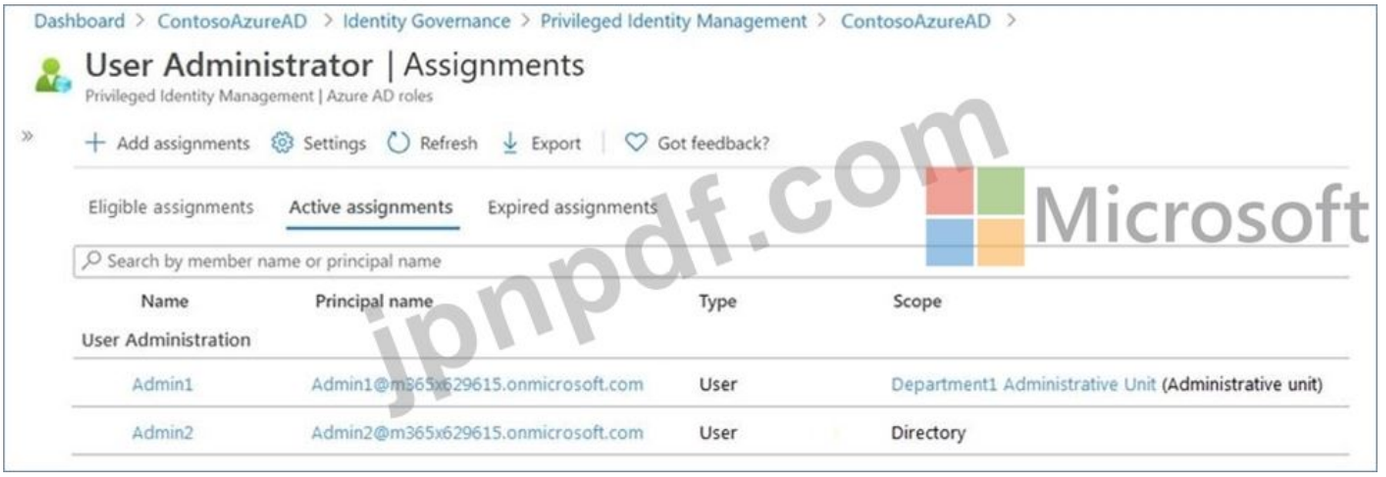
C. ユーザー アクセス管理者

D. 課金管理者

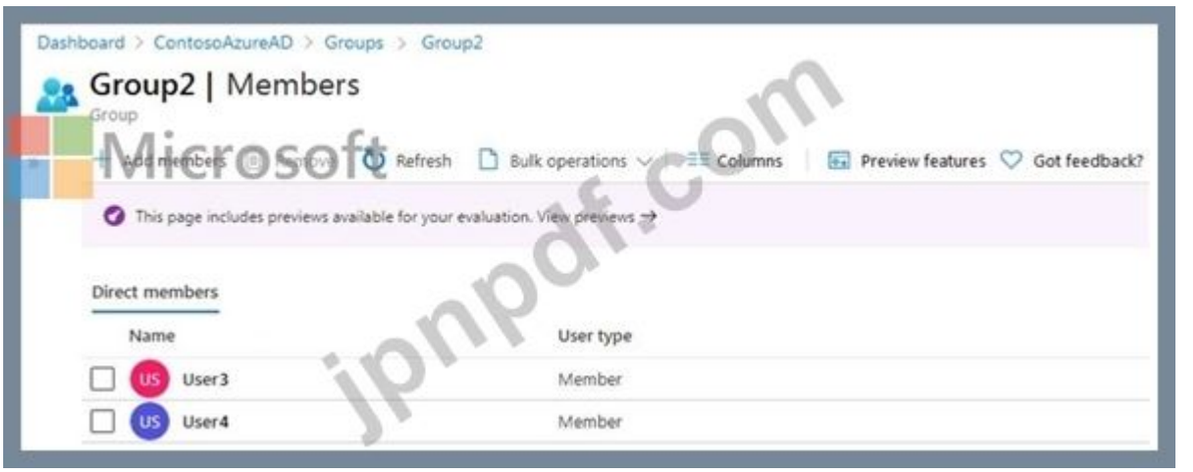
Answer: D (メーッセージを残す)

最新問題**: 103**
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] 展示に表示されているユーザーがいます。([ユーザー] タブをクリックします。)
Department1 には、[グループ] 展示に示されているグループがあります。([グループ] タブをクリックします。)

Department1 には、[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。)



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。)



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

注意: 正しい選択ごとに 1 ポイントが付与されます。

Statements	Yes	No
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.	○	○

説明

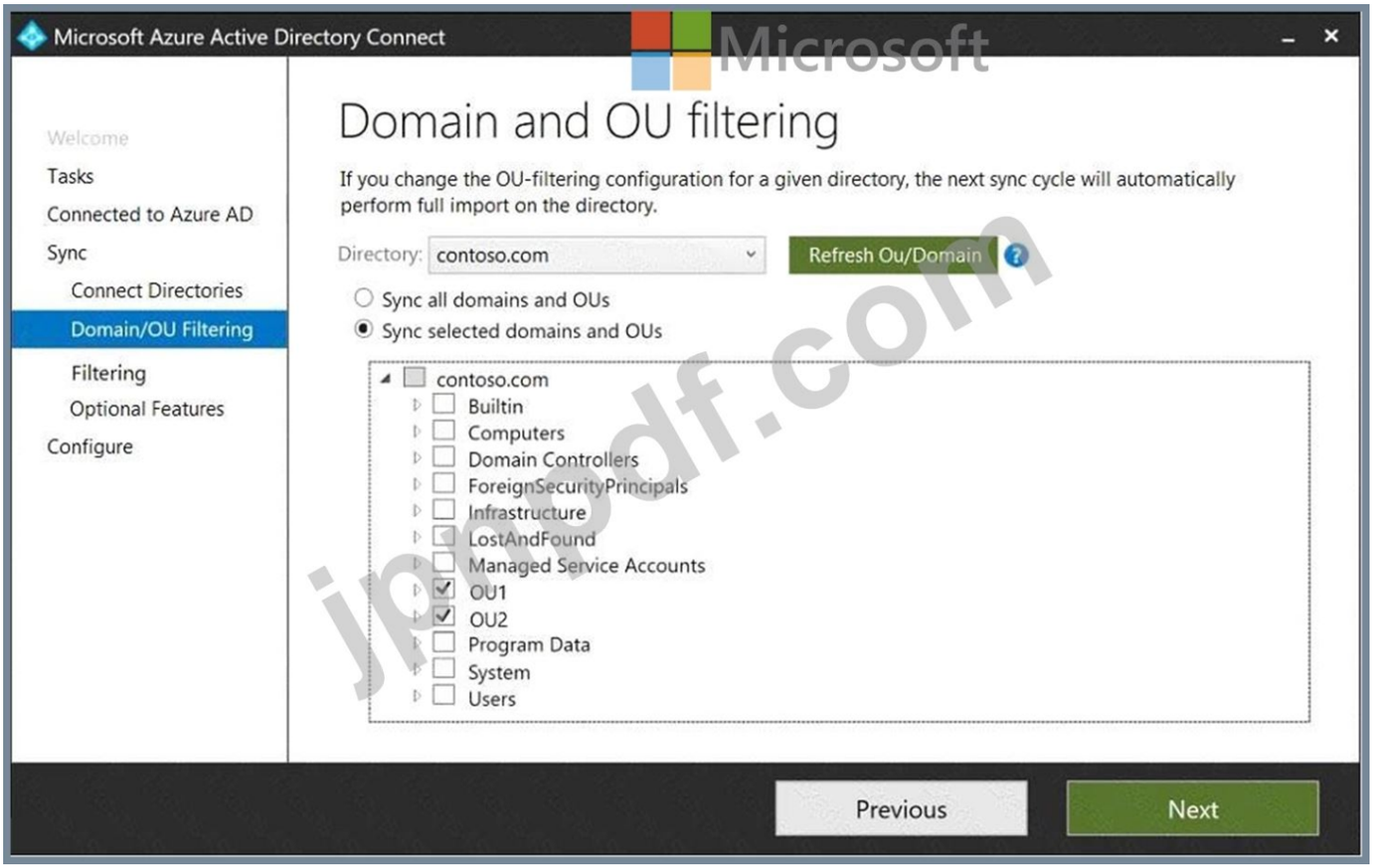
Statements	Yes	No
Admin1 can reset the passwords of User3 and User4.	○	○
Admin1 can add User1 to Group 2	○	○
Admin 2 can reset the password of User1.	○	○

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

最新問題**: 104**
ネットワークには、contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。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 のフィルタリング設定を、「ドメインと OU のフィルタリング」の図に示すように構成します (「ドメインと OU のフィルタリング」タブをクリックします)。

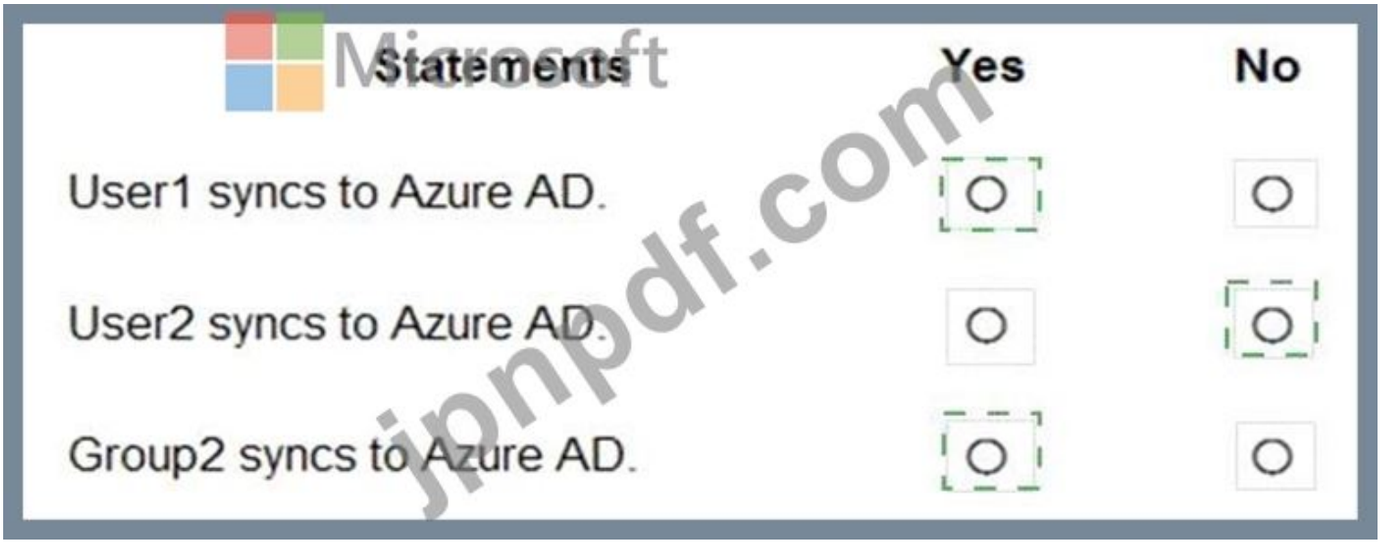


「ユーザーとデバイスのフィルター」設定は、「ユーザーとデバイスのフィルター」の図に示すように構成します。(「ユーザーとデバイスのフィルター」タブをクリックします。)

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

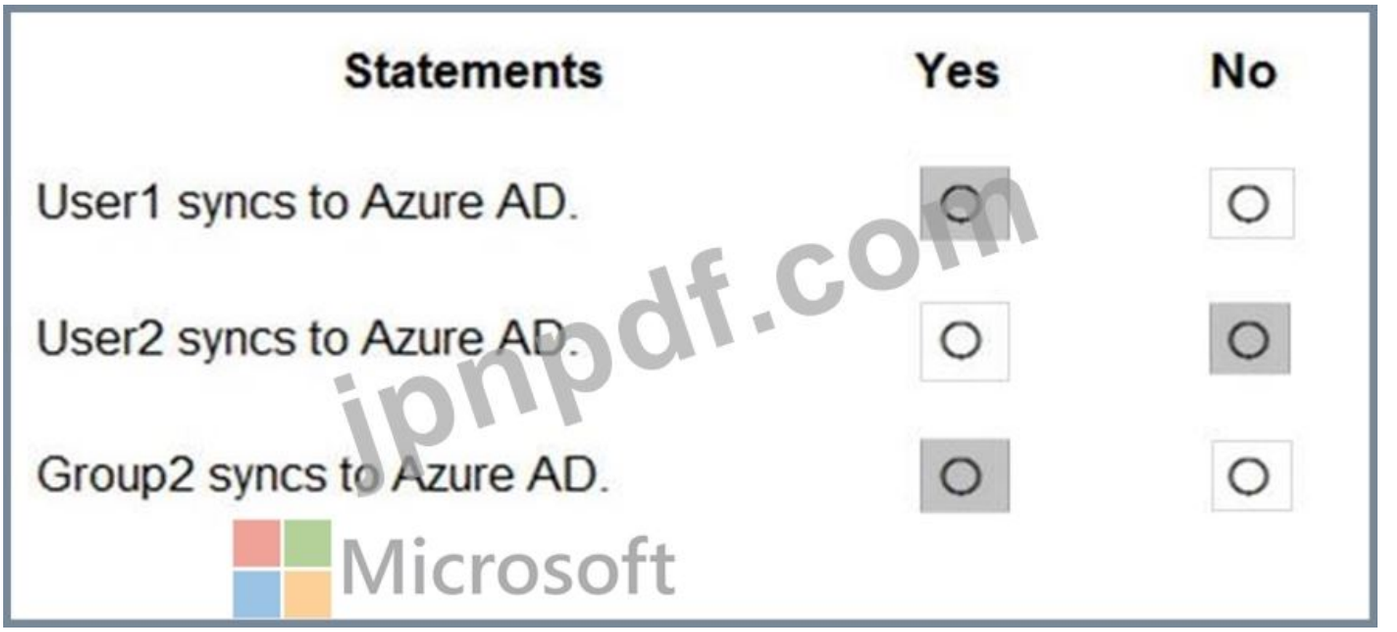
Statements	Yes	No
User1 syncs to Azure AD.	○	○
User2 syncs to Azure AD.	○	○
Group2 syncs to Azure AD.	○	○

Answer:



説明

グラフィカルユーザーインターフェイス、アプリケーションの説明は自動的に生成されます



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: **105**
Azure サブスクリプションをお持ちです。
エンタイトルメント管理から、カスタム拡張機能を含む Catalog1 という名前のカタログを作成する予定です。
最初に何を作成し、Catalog1 を配布するために何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ます。
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer:

Explanation:
ロゴのクローズアップ説明は自動的に生成されました

最新問題: **106**
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。

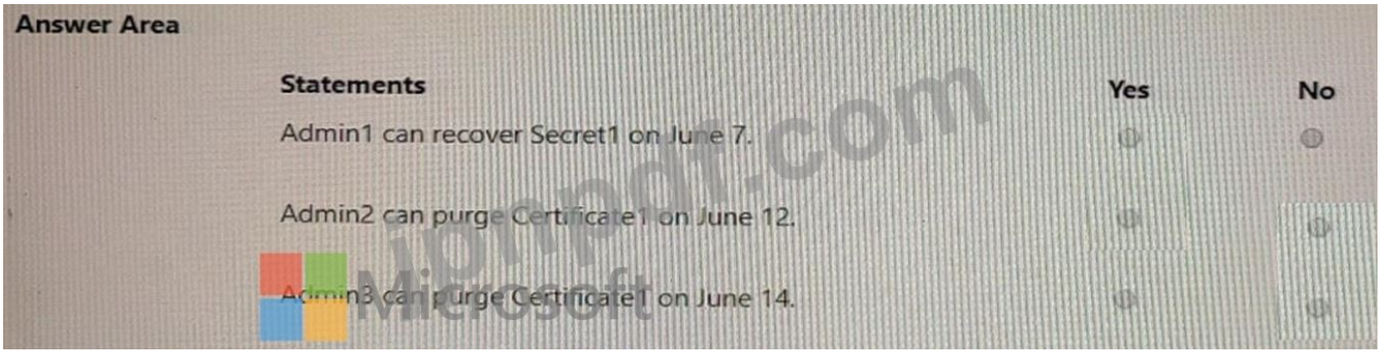
Name	Role
Admin1	Key Vault Administrator
Admin2	Key Vault Contributor
Admin3	Key Vault Certificates Officer
Admin4	Owner

6月1日に、Admin4は次のアクションを実行します。

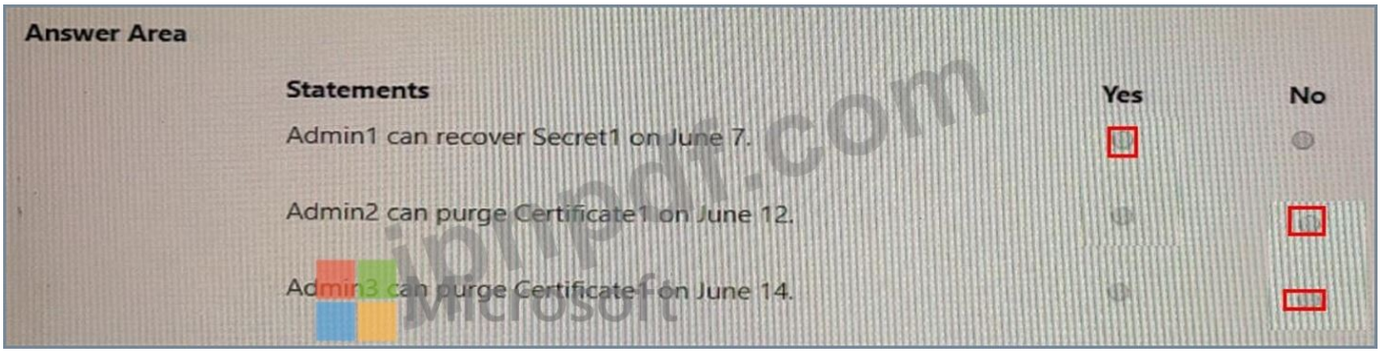
* Key Vault1からCertificate!という名前の証明書を削除します
* KeyVault2からSecret1という名前のシークレットを削除します

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

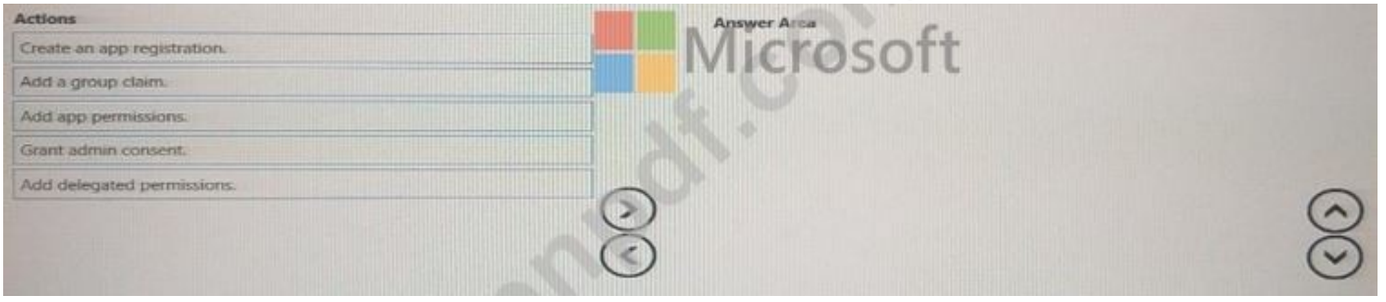
注意: 正しい選択ごとに 1 ポイントが付与されます。



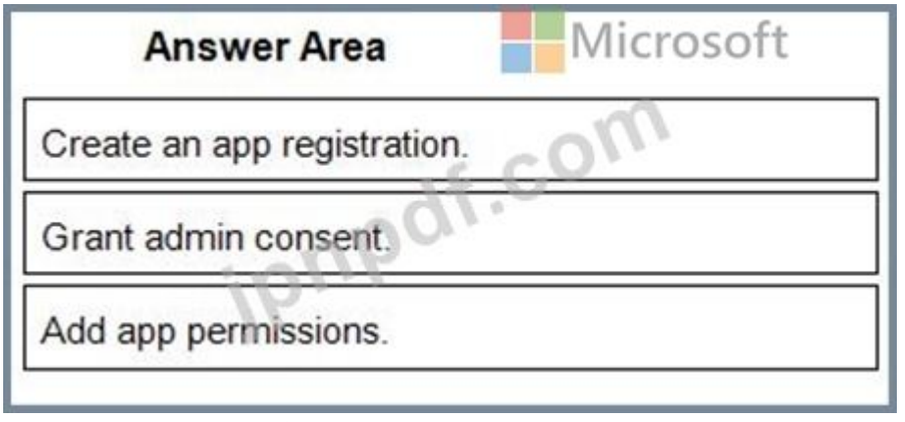
Answer:



最新問題: **107**
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、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、正しい順序で並べます。



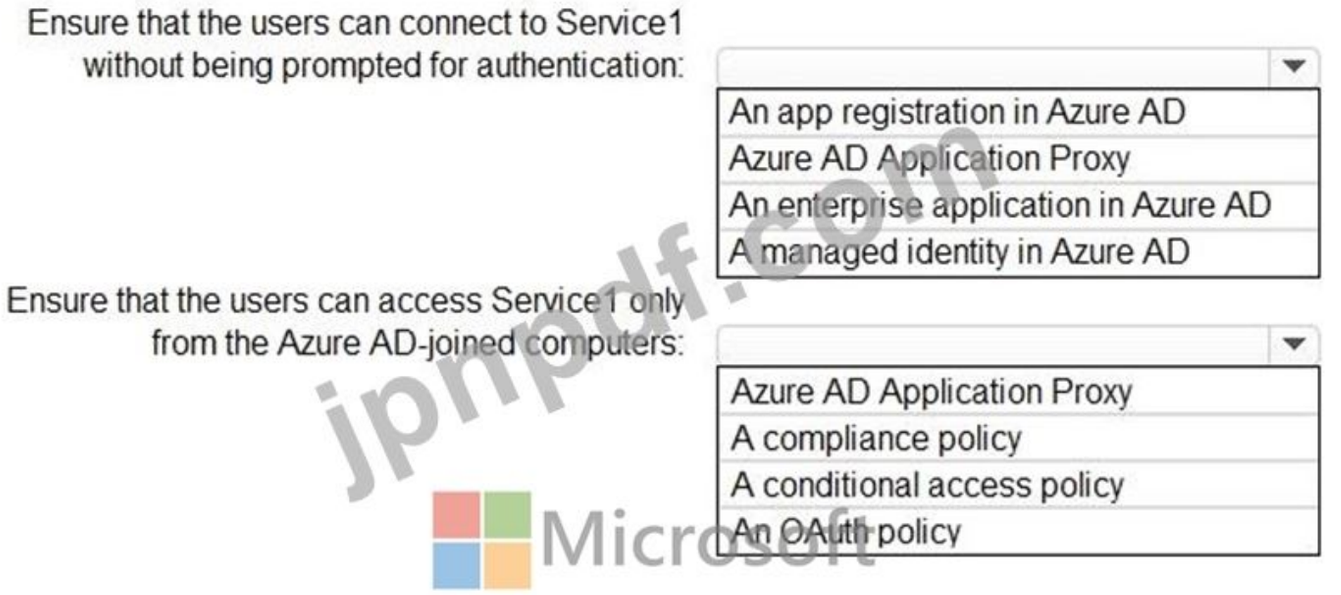
Answer:



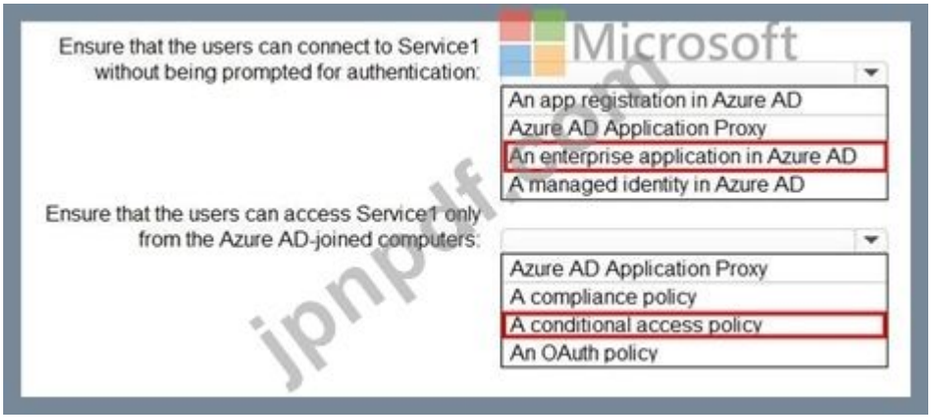
1 - アプリ登録を作成します。
2 - 管理者の同意を与えます。
3 - アプリの権限を追加します。
参照：
https://docs.microsoft.com/en-us/graph/auth/auth-concepts

最新問題: **108**
あなたの会社には 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 という名前のサードパーティ 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。ソリューションでは、ユーザーが Azure AD に参加しているコンピューターからのみ Service1 にアクセスできるようにする必要があります。ソリューションでは、管理の労力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 ポイントが付与されます。



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