Microsoft.MS-500.v2019-11-17.q43

試験コード：	MS-500
試験名称：	Microsoft 365 Security Administration
認証ベンダー：	Microsoft
無料問題の数：	43
バージョン：	v2019-11-17
ページの閲覧量：	1276
問題集の閲覧量：	13445

https://www.jpnshiken.com/shiken/Microsoft.MS-500.v2019-11-17.q43.html

質問: **1**

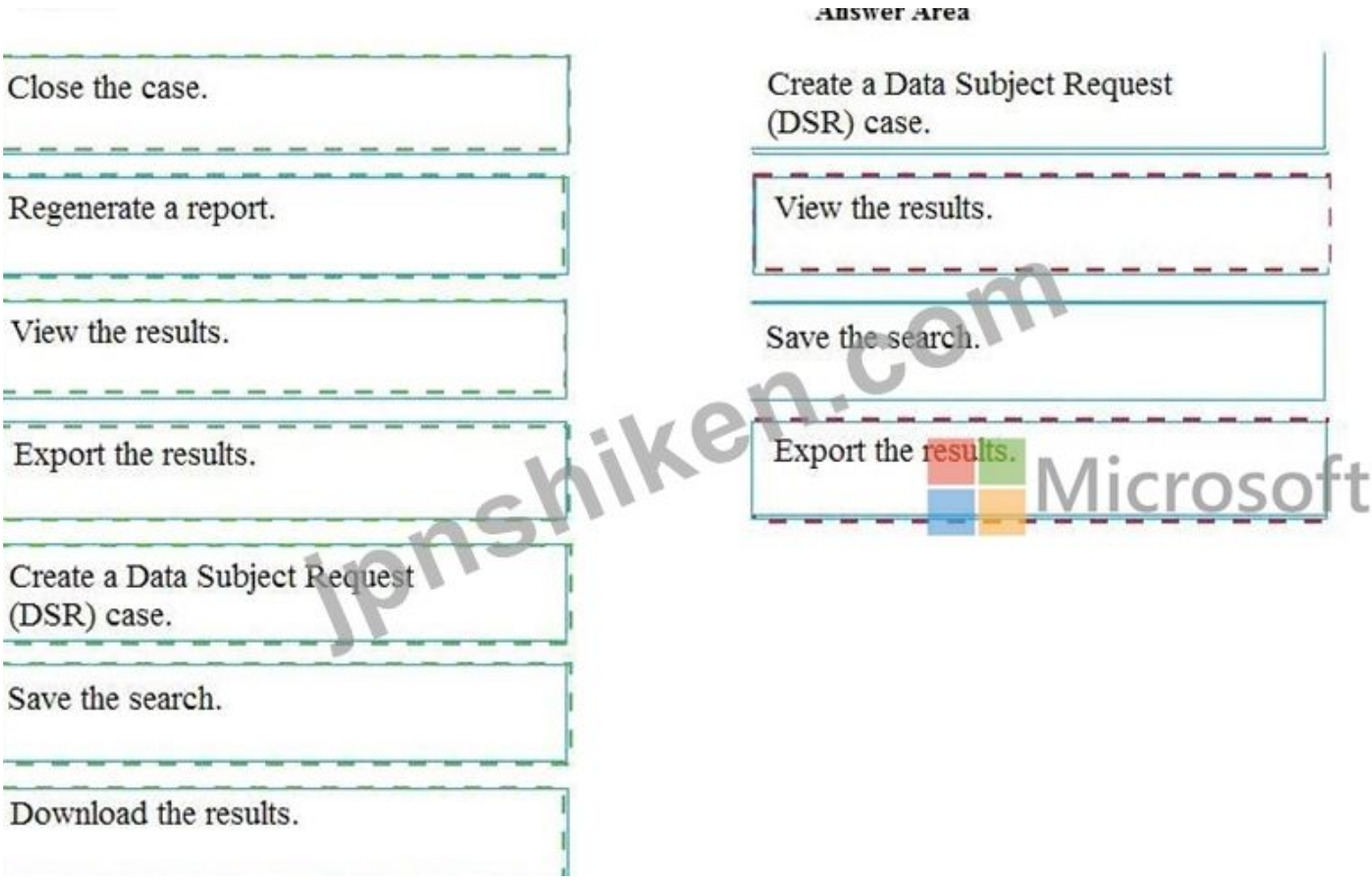
Microsoft 365サブスクリプションがあります。

顧客は、名前で彼女を参照するすべてのドキュメントを提供するように要求します。

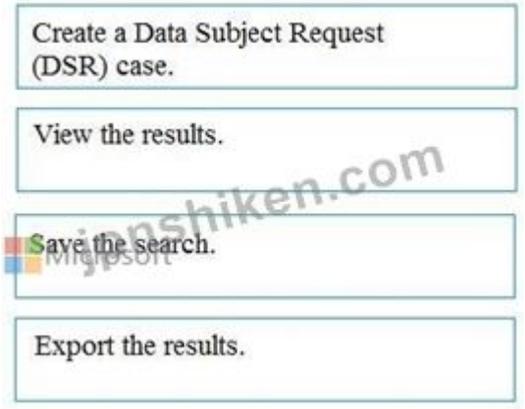
お客様にコンテンツのコピーを提供する必要があります。

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

正解:



説明



参照：

https://docs.microsoft.com/en-us/microsoft-365/compliance/gdpr-dsr-office365

質問: **2**

contoso.comの既定のドメイン名を使用するMicrosoft 365サブスクリプションがあります。

Microsoft Azure Active Directory Azure AD)には、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1
User2	Group1, Group2
User3	Group3

Microsoft Intuneには、次の表に示すように2つのデバイスが登録されています。

Name	Platform
Device1	Android
Device2	Windows 10

両方のデバイスには、App1、App2、およびApp3という名前の3つのアプリがインストールされています。
次の設定を持つProtectionPolicy1という名前のアプリ保護ポリシーを作成します。
*保護されたアプリ :App1
*免除アプリ :App2
* Windows情報保護モード :ブロック
ProtectionPolicy1をGroup1およびGroup3に適用します。Group2をProtectionPolicy1から除外します。
以下の各ステートメントについて、ステートメントが真である場合は 「はい」を選択します。それ以外の場合は、「いいえ」を選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。

正解:

説明

質問: **3**
自動化された電子メールメッセージをITチームに向ける問題を解決する必要があります。
どのツールを最初に実行する必要がありますか？
A. 同期サービスマネージャー
B. Azure AD Connectウィザード

C. 同期ルールエディター
D. IdFix
正解: **(**正解を表示します**)**
説明
参照：
https://docs.microsoft.com/en-us/office365/enterprise/fix-problems-with-directory-synchronization

質問: **4**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
次の表に示すユーザーを含むMicrosoft 365サブスクリプションがあります。

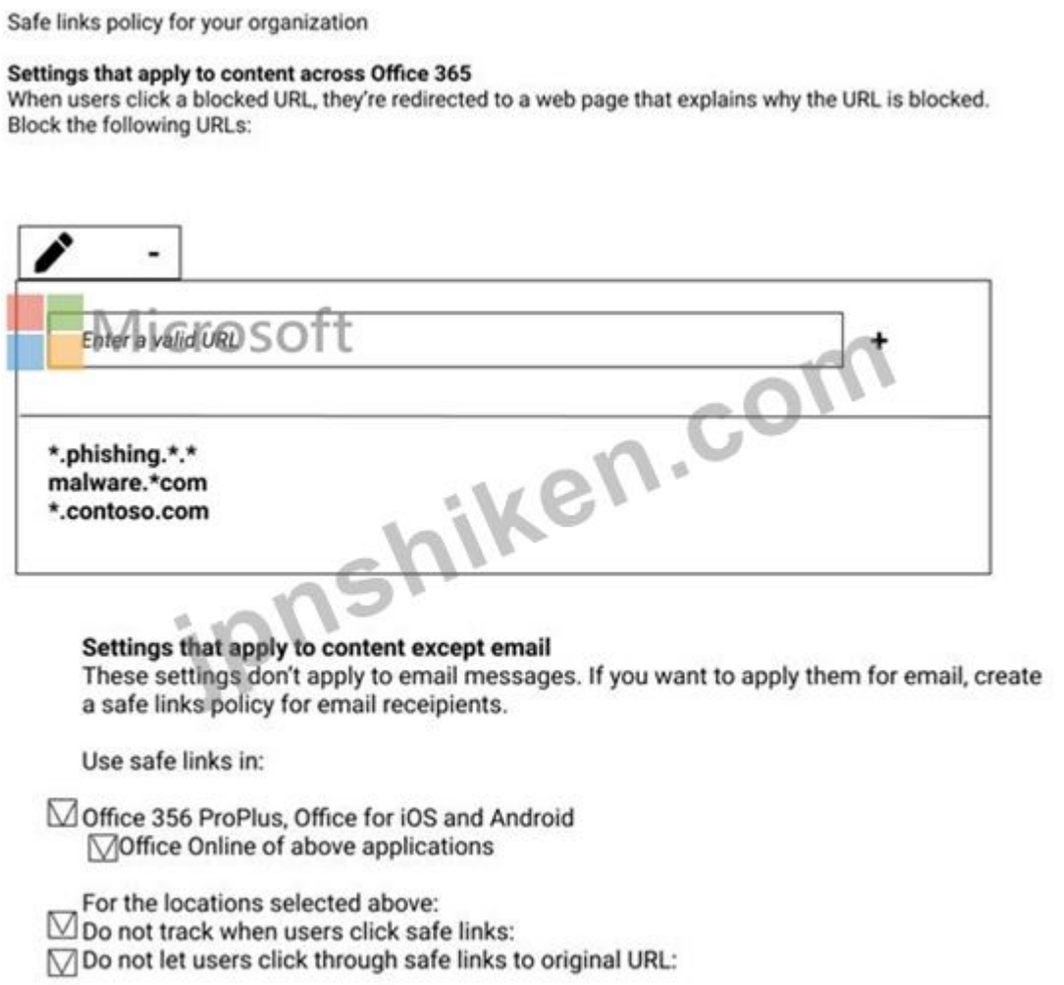
Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

サブスクリプションのすべてのユーザーがCompliance Managerレポートにアクセスできることがわかります。
コンプライアンスマネージャーのリーダーロールは、どのユーザーにも割り当てられていません。
User5という名前のユーザーがCompliance Managerレポートにアクセスできないようにするソリューションを推奨する必要があります。
解決策 :コンプライアンスマネージャーリーダーの役割をUser1に割り当てることをお勧めします。
これは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**

質問: **5**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
contoso.comという名前のMicrosoft Azure Active Directory (Azure AD)テナントに関連付けられているMicrosoft 365 E5サブスクリプションがあります。

Active Directoryフェデレーションサービス（AD FS）を使用して、オンプレミスのActive Directoryとテナントをフェデレーションします。Azure AD Connectには次の設定があります。
*ソースアンカー：objectGUID
*パスワードハッシュ同期：無効
*パスワードの書き戻し：無効
*ディレクトリ拡張属性の同期：無効
* Azure ADアプリと属性フィルター：無効
* Exchangeハイブリッド展開：無効
*ユーザーの書き戻し：無効
Azure AD Identity Protectionで漏えいした資格情報の検出を使用できることを確認する必要があります。
解決策：Azure ADアプリと属性フィルターの設定を変更します。
それは目標を達成していますか？
A. はい
B. いいえ
正解: **B** (コメントを発表する)

質問: **6**
fabrikam.comのデフォルトドメイン名を使用するMicrosoft 365サブスクリプションがあります。
次の展示に示すように、安全なリンクポリシーを作成します。



ユーザーがMicrosoft Word Onlineから安全にアクセスできるURLはどれですか？

A. fabrikam.phishing.fabrikam.com

B. Malware.fabrikam.com

C. fabrikam.contoso.com

D. www.malware.fabrikam.com

正解**: (**正解を表示します**)**

説明

参照：

https://docs.microsoft.com/en-us/office365/securitycompliance/set-up-a-custom-blocked-urls-list-wtih-atp

質問**: 7**

User1にどのロールを割り当てる必要がありますか？

A. グローバル管理者

B. ユーザー管理者

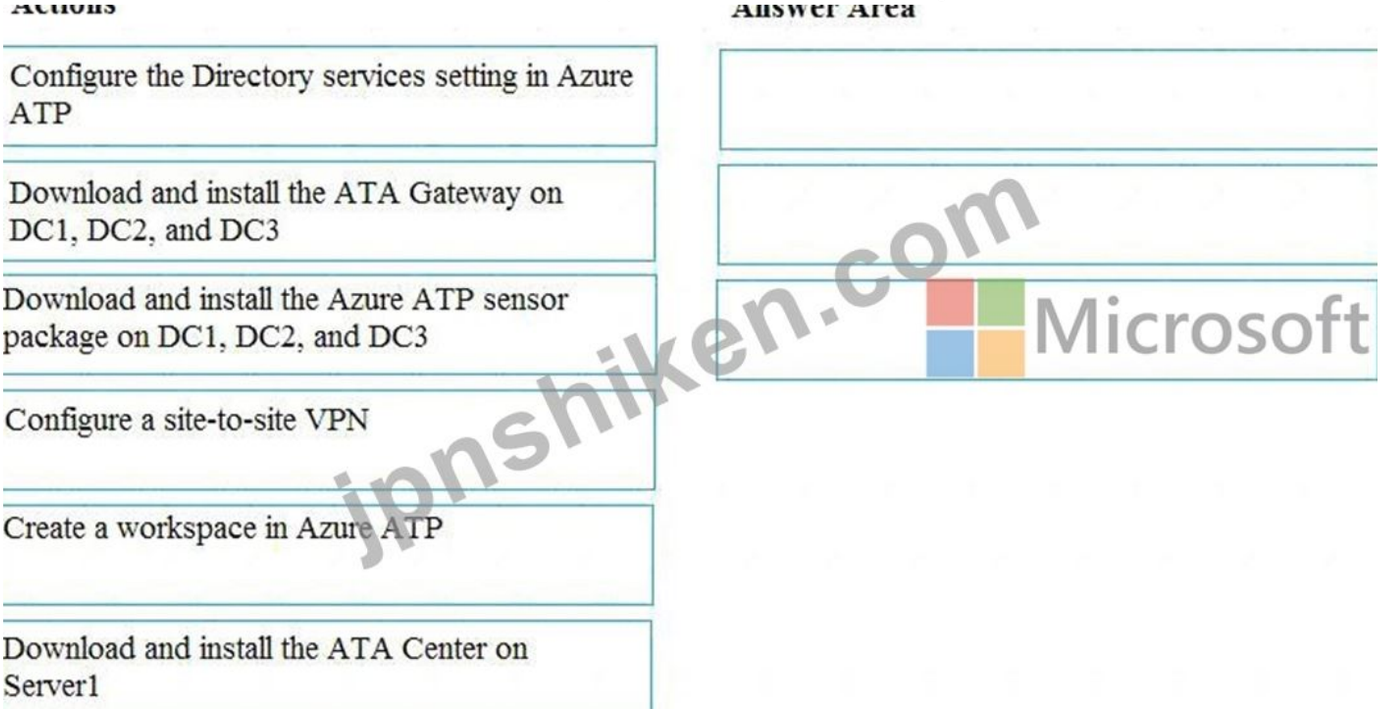
C. 特権ロール管理者

D. セキュリティ管理者

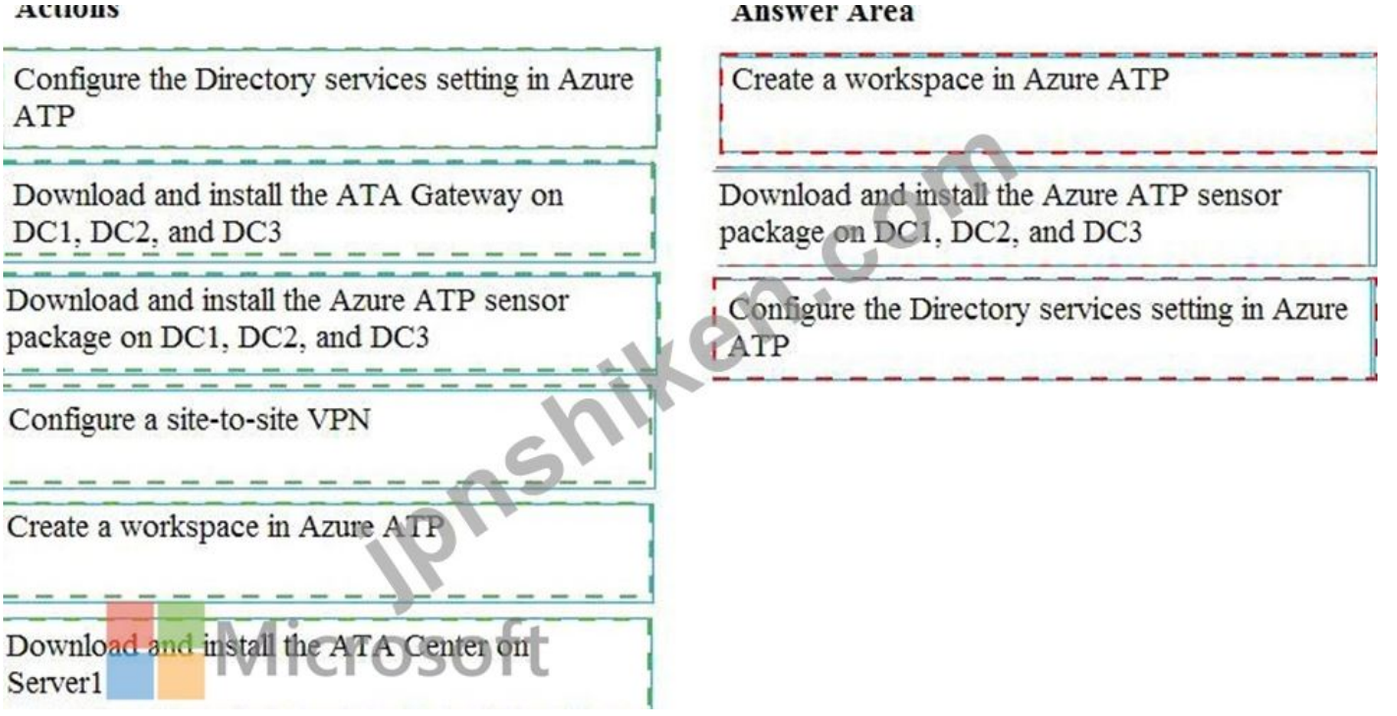
正解**: (**正解を表示します**)**

説明
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access

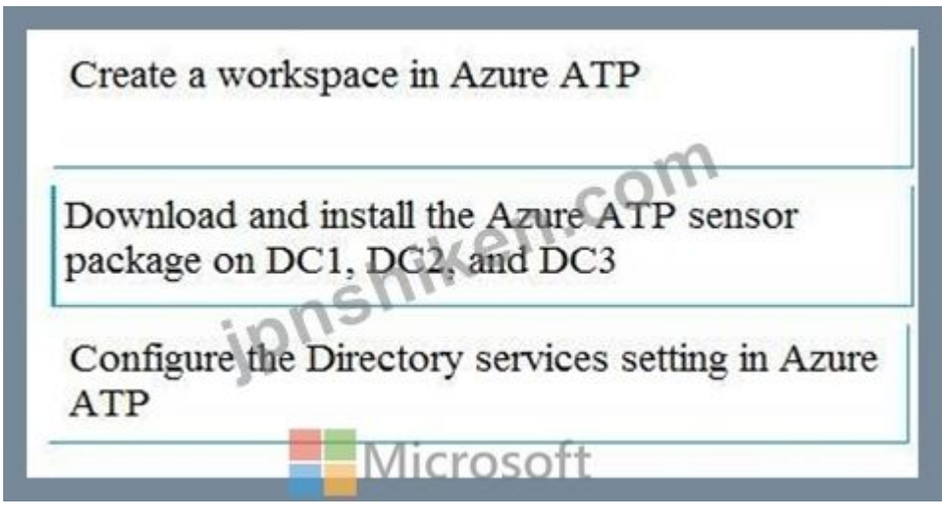
質問: **8**
Active Directoryの脅威検出を設定する必要があります。ソリューションはセキュリティ要件を満たしている必要があります。
順番に実行する必要がある3つのアクションはどれですか？回答するには、適切なアクションをアクションのリストから回答エリアに移動し、正しい順序に並べます。



正解:



説明



質問: **9**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
contoso.comという名前のMicrosoft Azure Active Directory（Azure AD）テナントに関連付けられているMicrosoft 365 E5サブスクリプションがあります。
Active Directoryフェデレーションサービス（AD FS）を使用して、オンプレミスのActive Directoryとテナントをフェデレーションします。Azure AD Connectには次の設定があります。
*ソースアンカー :objectGUID
*パスワードハッシュ同期：無効
*パスワードの書き戻し：無効
*ディレクトリ拡張属性の同期：無効
* Azure ADアプリと属性フィルター：無効
* Exchangeハイブリッド展開：無効
*ユーザーの書き戻し：無効
Azure AD Identity Protectionで漏えいした資格情報の検出を使用できることを確認する必要があります。
解決策 :ソースアンカー設定を変更します。
それは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**

質問: **10**
ネットワークには、オンプレミスのActive Directoryドメインが含まれています。ドメインには、Windows Serverを実行し、高度な監査が有効になっているサーバーが含まれています。

サーバーのセキュリティログは、サードパーティのSIEMソリューションを使用して収集されます。
Microsoft 365サブスクリプションを購入し、スタンドアロンセンサーを使用してAzure Advanced Threat Protection（ATP）の展開を計画します。
機密グループが変更されたとき、および悪意のあるサービスが作成されたときを検出できることを確認する必要があります。
あなたは何をするべきか？
A. Office 365セキュリティ＆コンプライアンスセンターで監査を構成します。
B. Azure ATPセンサーの遅延更新をオフにします。
C. Azure ATPセンサーのドメインシンクロナイザー候補の設定を変更します。
D. SIEMとAzure ATPを統合します。
正解**: C (**コメントを発表する**)**
説明
参照：
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/install-atp-step5

質問**: 11**
Microsoft 365サブスクリプションがあります。
保持ポリシーを作成し、そのポリシーをExchange Onlineメールボックスに適用します。
保持ポリシータグをメールボックスアイテムにできるだけ早く割り当てることができるようにする必要があります。
あなたは何をするべきか？
A. Exchange Online PowerShellから、Start-RetentionAutoTagLearningを実行します
B. Exchange Online PowerShellから、Start-ManagedFolderAssistantを実行します
C. セキュリティとコンプライアンスの管理センターから、データ損失防止（DLP）ポリシーを作成します
D. セキュリティとコンプライアンスの管理センターから、ラベルポリシーを作成します
正解**: (**正解を表示します**)**
説明
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/labels

質問**: 12**
Microsoft 365サブスクリプションがあります。
昨日、保持ラベルを作成し、ラベルをMicrosoft Exchange Onlineメールボックスに公開しました。
できるだけ早くラベルを手動で割り当てられるようにする必要があります。
あなたは何をするべきか？
A. Exchange Online PowerShellから、Start-ManagedFolderAssistantを実行します
B. セキュリティとコンプライアンスの管理センターから、データ損失防止（DLP）ポリシーを作成します

C. Exchange Online PowerShellから、Start-RetentionAutoTagLearningを実行します
D. セキュリティとコンプライアンスの管理センターから、ラベルポリシーを作成します
正解: **A** (コメントを発表する)

質問: **13**
Contoso、Ltdという会社のMicrosoft 365サブスクリプションがあります。すべてのデータはMicrosoft 365にあります。
Contosoは、Litware、Incという名前のパートナー企業と連携しています。LitwareにはMicrosoft 365サブスクリプションがあります。
ContosoのユーザーがMicrosoft OneDriveのファイルをLitwareの特定のユーザーと共有できるようにする必要があります。
OneDrive管理センターから実行する必要がある2つのアクションはどれですか？それぞれの正解はソリューションの一部を示しています。
注 :それぞれの正しい選択には1ポイントの価値があります。
A. OneDrive外部共有のアクセス許可レベルを上げる
B. リンク設定を変更します
C. OneDrive外部共有のアクセス許可を最小許容レベルに変更します
D. OneDrive外部共有のアクセス許可レベルを下げる
E. デバイスアクセス設定を変更します
F. 同期設定を変更します
正解: **B,D** (コメントを発表する)
説明
参照：
https://docs.microsoft.com/en-us/sharepoint/turn-external-sharing-on-or-off

質問: **14**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
次の表に示すユーザーを含むMicrosoft 365サブスクリプションがあります。

Name	Role
User1	Compliance Manager Contributor
User2	Compliance Manager Assessor
User3	Compliance Manager Administrator
User4	Portal Admin

サブスクリプションのすべてのユーザーがCompliance Managerレポートにアクセスできることがわかります。
コンプライアンスマネージャーのリーダーロールは、どのユーザーにも割り当てられていません。
User5という名前のユーザーがCompliance Managerレポートにアクセスできないようにするソリューションを推奨する必要があります。
解決策 :コンプライアンスマネージャーの投稿者ロールからUser1を削除することをお勧めします。
それは目標を達成していますか？
A. はい
B. いいえ
正解: **(**正解を表示します**)**
説明
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/working-with-compliance-manager

質問: **15**
Microsoft 365 Enterprise E5サブスクリプションがあります。
Windows Defender Advanced Threat Protection（Windows Defender ATP）を使用します。
Microsoft Office 365 Threat IntelligenceとWindows Defender ATPを統合する必要があります。
統合をどこで構成する必要がありますか？
A. Microsoft 365管理センターから、[設定]を選択し、[サービスとアドイン]を選択します。
B. セキュリティとコンプライアンスの管理センターで、[脅威管理]を選択し、[エクスプローラー]を選択します。
C. Microsoft 365管理センターから、[セキュリティとコンプライアンス]を選択します。
D. セキュリティとコンプライアンスの管理センターから、[脅威管理]を選択し、[脅威追跡]を選択します。
正解: **(**正解を表示します**)**
説明
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/integrate-office-365-ti-with-wdatp

質問: **16**
Microsoft 365サブスクリプションがあります。
すべてのMicrosoft Exchange Onlineユーザーの監査を有効にする必要があります。
あなたは何をするべきか？
A. Exchange管理センターから、ジャーナルルールを作成します
B. Set-MailboxDatabaseコマンドレットを実行します
C. Set-Mailboxコマンドレットを実行します
D. Exchange管理センターから、メールフローメッセージトレースルールを作成します。

正解: (正解を表示します)
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/enable-mailbox-auditing

質問: 17
Microsoft 365サブスクリプションがあります。
Microsoft 365管理センターから、新しいユーザーを作成します。
ユーザーにレポートリーダーの役割を割り当てる予定です。
レポートリーダーロールの権限を確認する必要があります。
どの管理センターを使用する必要がありますか？
A. クラウドアプリのセキュリティ
B. Microsoft 365
C. Azure Active Directory
D. セキュリティとコンプライアンス
正解: (正解を表示します)

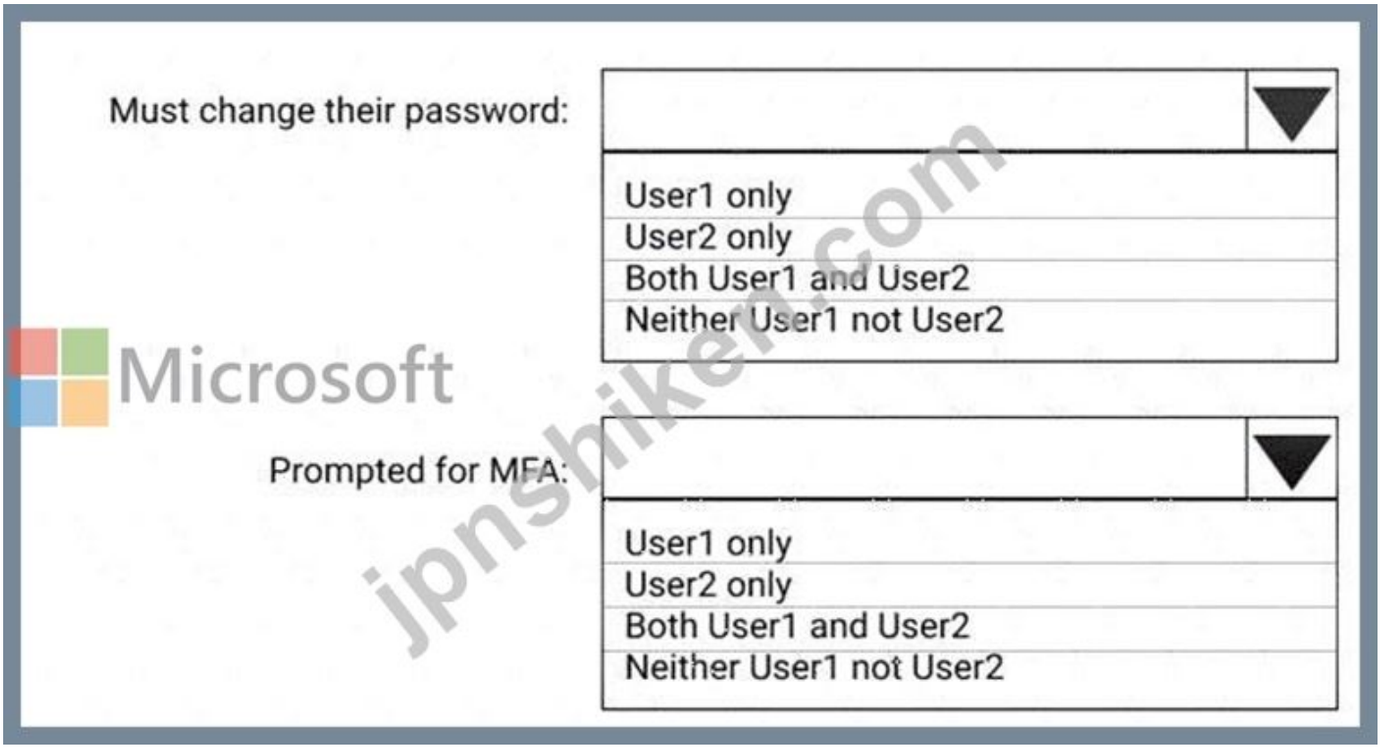
質問: 18
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、正しい解決策がない場合もあります。
このセクションの質問に回答すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
Microsoft 365テナントがあります。Microsoft Azure Information Protectionで CompanyConfidentialという名前のラベルを作成します。
CompanyConfidentialをグローバルポリシーに追加します。
ユーザーはCompanyConfidentialを使用して電子メールメッセージを保護し、ラベルを複数の外部受信者に送信します。外部の受信者は、電子メールメッセージを開くことができないと報告します。
外部受信者が送信された保護された電子メールメッセージを開くことができるようにする必要があります。
解決策 :ラベルの暗号化設定を変更します。
これは目標を達成していますか？

A. いいえ
B. はい
正解: **(**正解を表示します**)**

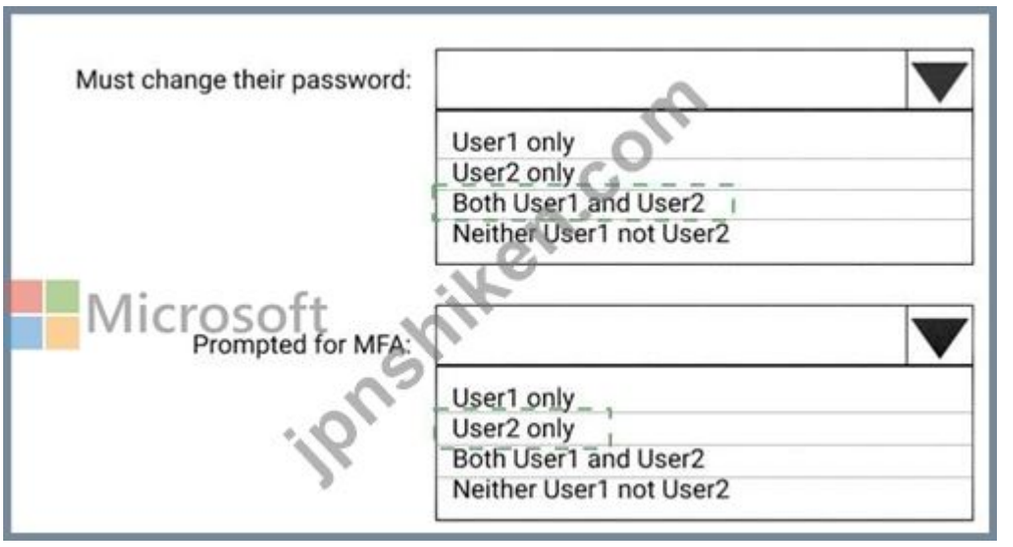
質問: **19**
次の表に示すユーザーを含む、contoso.comという名前のMicrosoft Azure Active Directory（Azure AD）テナントがあります。

Name	Member	Multi-factor authentication (MFA) status
User1	Group1	Disabled
User2	Group1, Group2	Enabled

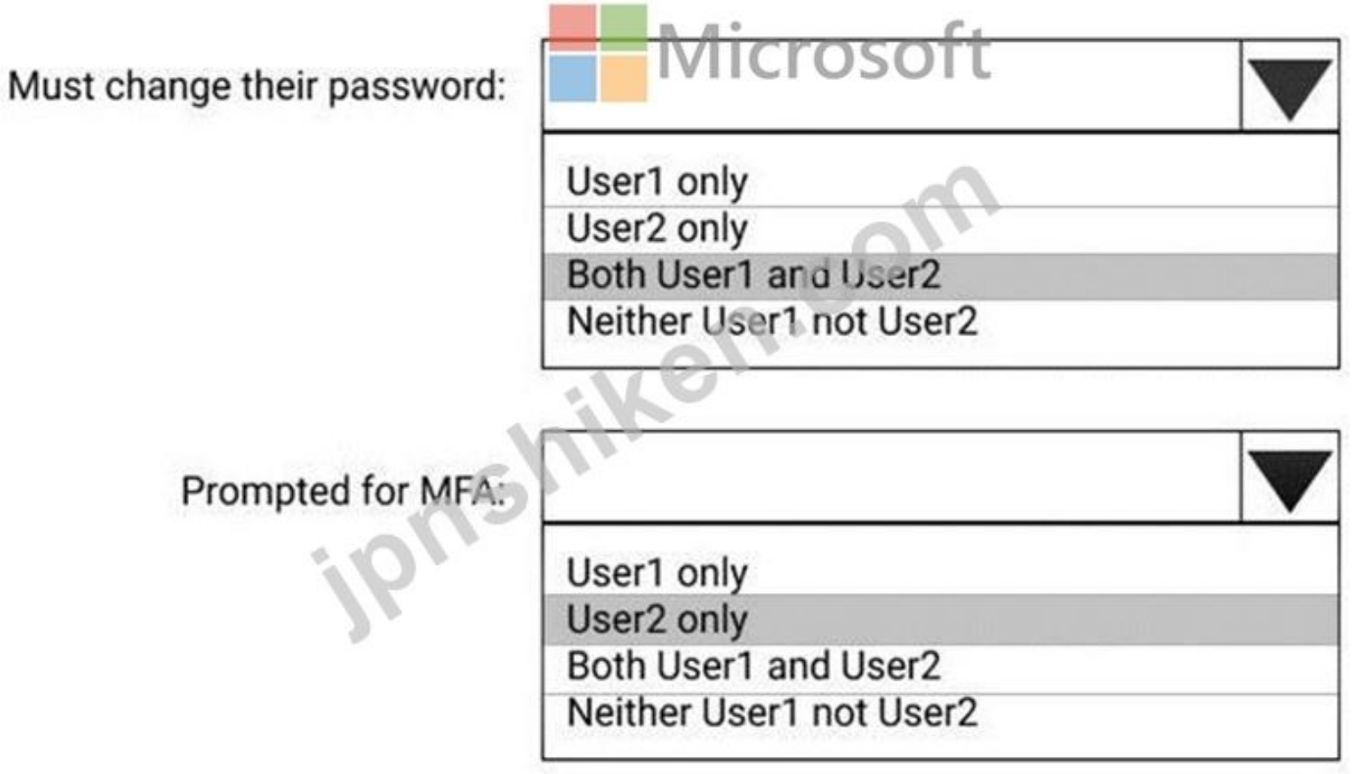
次の設定を持つAzure AD Identity Protectionユーザーリスクポリシーを作成して適用します。
*割り当て :Group1を含め、Group2を除外します
*条件：低以上のサインインのリスク
*アクセス :アクセスを許可し、パスワードの変更が必要
ポリシーがUser1およびUser2にどのように影響するかを識別する必要があります。
User1とUser2がなじみのない場所からサインインするとどうなりますか？回答するには、回答エリアで適切なオプションを選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



説明



質問: **20**

ネットワークには、オンプレミスのActive Directoryドメインが含まれています。ドメインには、Windows Serverを実行し、高度な監査が有効になっているサーバーが含まれています。

サーバーのセキュリティログは、サードパーティのSIEMソリューションを使用して収集されます。

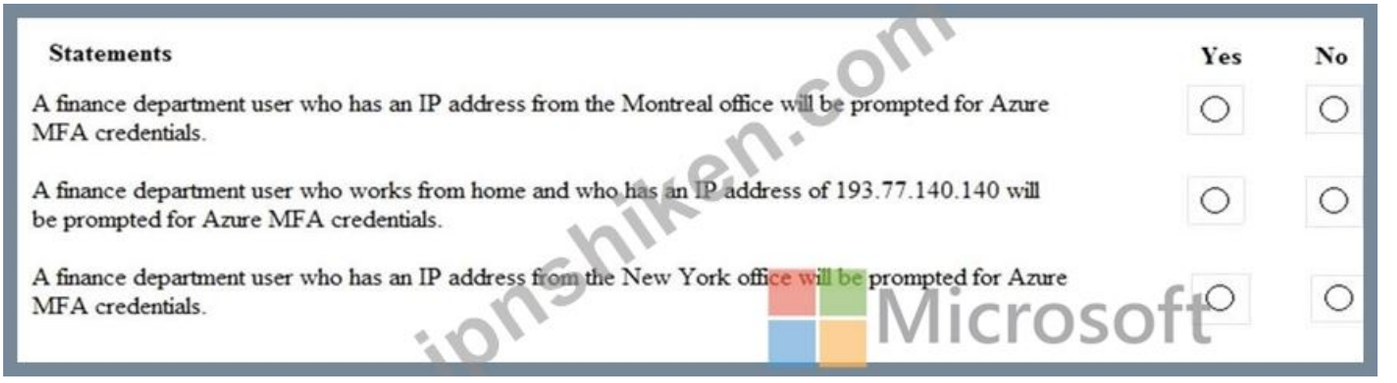
Microsoft 365サブスクリプションを購入し、スタンドアロンセンサーを使用してAzure Advanced Threat Protection（ATP）の展開を計画します。

機密グループが変更されたとき、および悪意のあるサービスが作成されたときを検出できることを確認する必要があります。

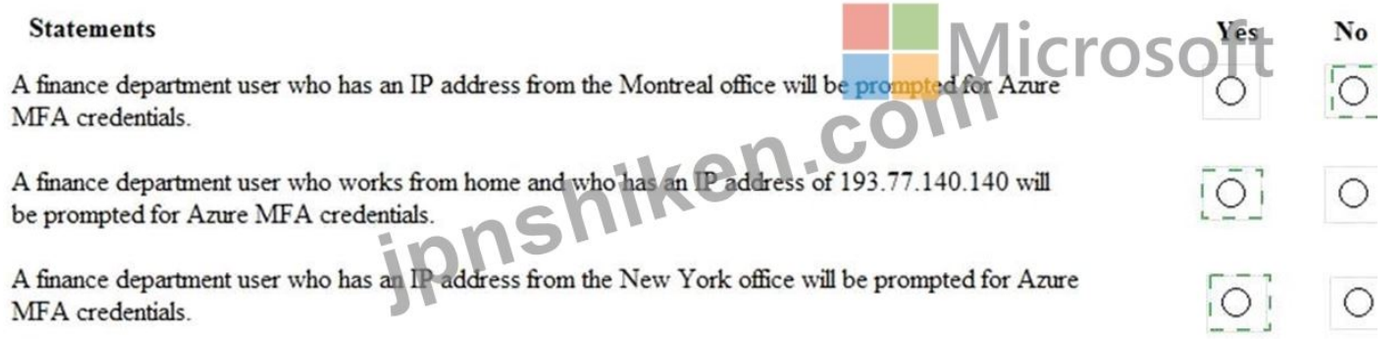
あなたは何をするべきか？

A. ドメインコントローラーでイベント転送を構成する
B. Office 365セキュリティ＆コンプライアンスセンターで監査を構成します。
C. Azure ATPセンサーの遅延更新をオンにします。
D. サーバーのアカウント管理の監査グループポリシー設定を有効にします。
正解: **A** (コメントを発表する)
参照：
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/configure-event-forwarding

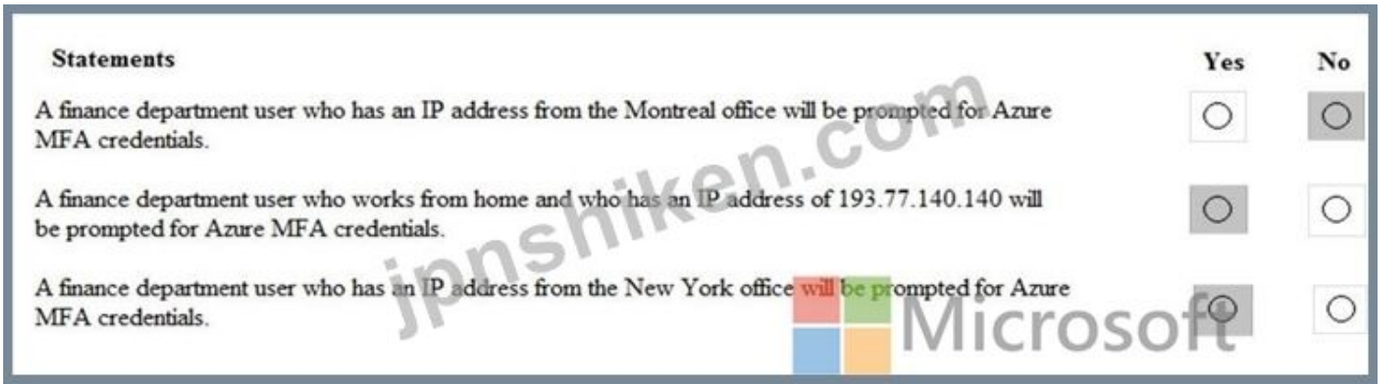
質問: **21**
Azure MFA資格情報の入力を求められる財務部門ユーザーを評価しています。
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。
注 :それぞれの正しい選択には1ポイントの価値があります。



正解:



説明



質問: **22**
ハイブリッドMicrosoft 365環境があります。
すべてのコンピューターはWindows 10 Enterpriseを実行し、Microsoft Office 365 ProPlusがインストールされています。すべてのコンピューターがActive Directoryに参加しています。
Windows Server 2016を実行するServer1という名前のサーバーがあります。Server1はテレメトリデータベースをホストします。テレメトリデータの個人情報がマイクロソフトに送信されないようにする必要があります。
あなたは何をするべきか？
A. コンピューターで、tdadm.exeを実行します
B. Server1で、readinessreportcreator.exeを実行します
C. コンピューターでレジストリを構成します
D. Server1でレジストリを構成します
正解: **C (**コメントを発表する**)**

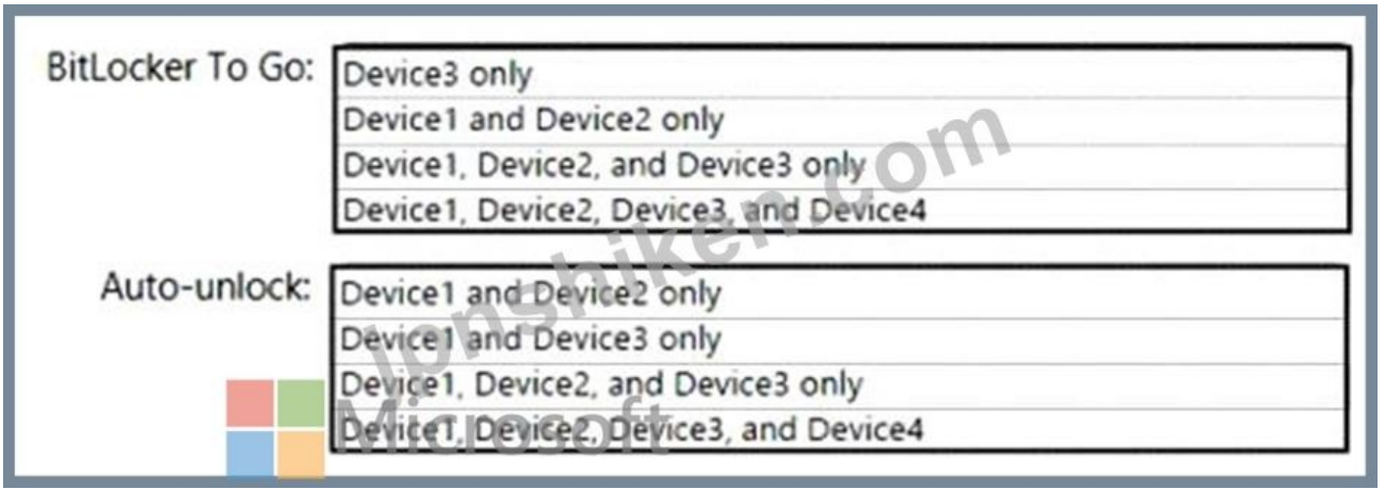
質問: **23**
Microsoft 365 E5サブスクリプションがあります。
すべてのユーザーにAdvanced Threat Protection（ATP）安全な添付ファイルポリシーを実装します。
ユーザーは、添付ファイルを含む電子メールメッセージの受信に予想以上の時間がかかると報告しています。
添付ファイルを含む電子メールメッセージの受信にかかる時間を短縮する必要があります。このソリューションでは、すべての添付ファイルでマルウェアをスキャンする必要があります。マルウェアのある添付ファイルはブロックする必要があります。
ATPから何をすべきですか？
A. アクションをブロックに設定します
B. 例外を追加
C. 条件を追加します
D. アクションを動的配信に設定します
正解: **(**正解を表示します**)**
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/dynamic-delivery-and-previewing

質問: **24**
contoso.comという名前のMicrosoft Azure Active Directory（Azure AD）テナントがあります。
次の表に示すように、4つのWindows 10デバイスがテナントに参加しています。

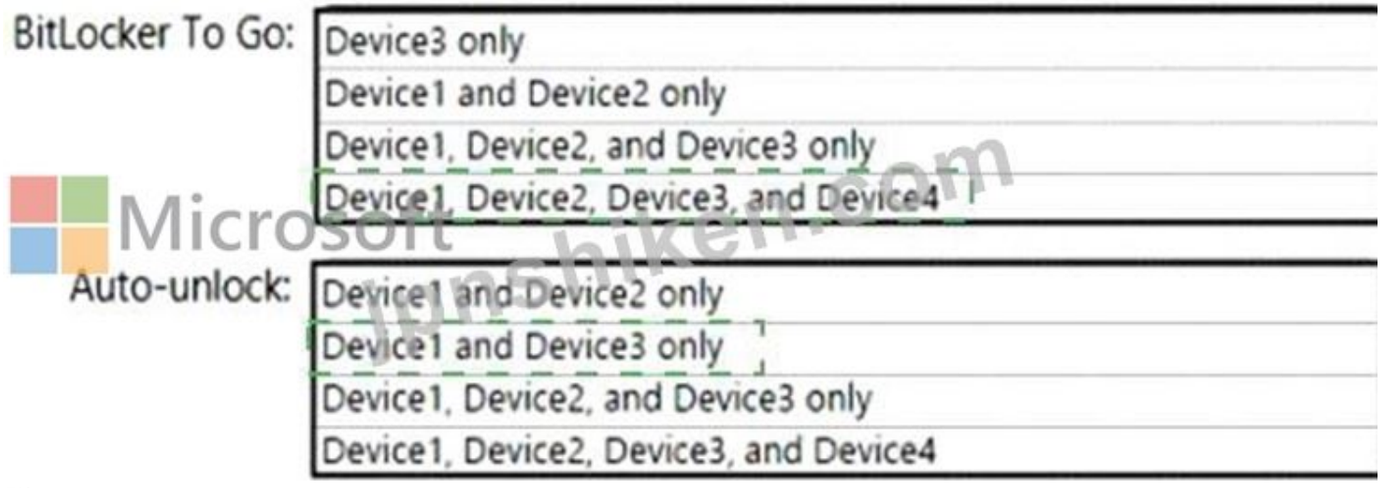
Name	Has TPM	BitLocker Drive Encryption (BitLocker) -protected C drive	BitLocker Drive Encryption (BitLocker) -protected D drive
Device1	Yes	Yes	No
Device2	Yes	No	Yes
Device3	No	Yes	Yes
Device4	No	No	No

BitLocker To Goを使用できるのはどのデバイスで、自動ロック解除を有効にできるのはどのデバイスですか？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 :それぞれの正しい選択には1ポイントの価値があります。



正解:



説明

質問: **25**

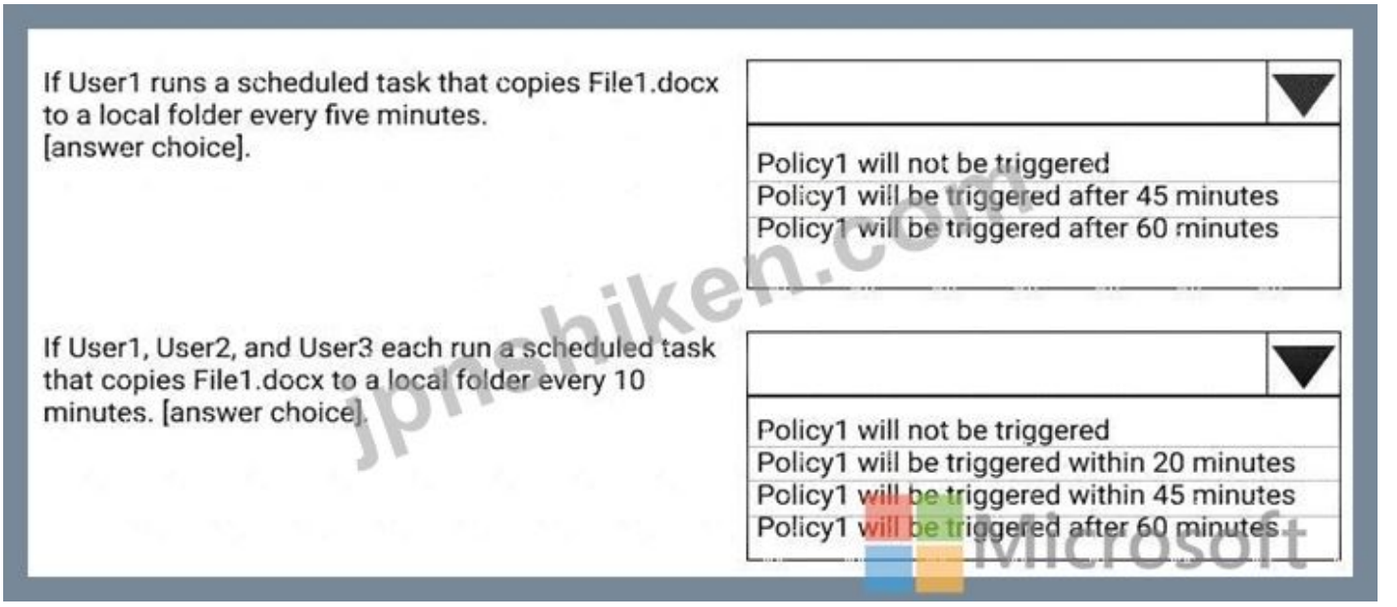
User1、User2、およびUser3という名前の3人のユーザーを含むMicrosoft 365サブスクリプションがあります。

File1.docxという名前のファイルがMicrosoft OneDriveに保存されます。自動化されたプロセスにより、File1.docxが毎分更新されます。

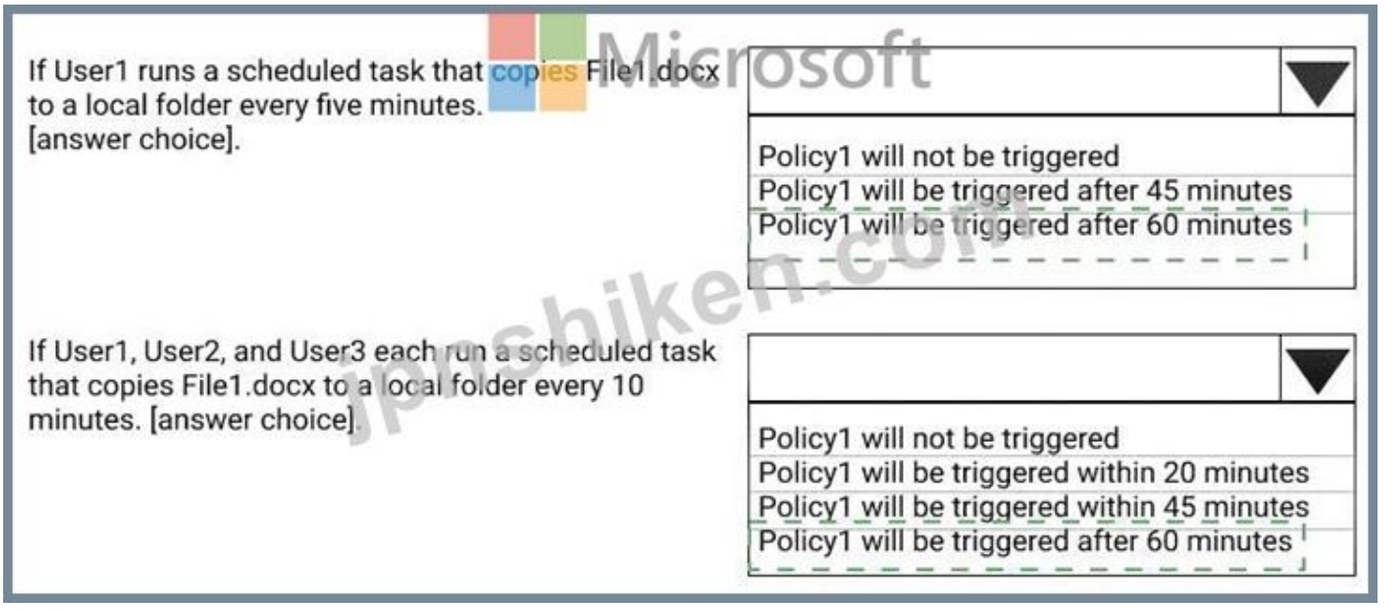
次の図に示すように、Policy1という名前のアラートポリシーを作成します。

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

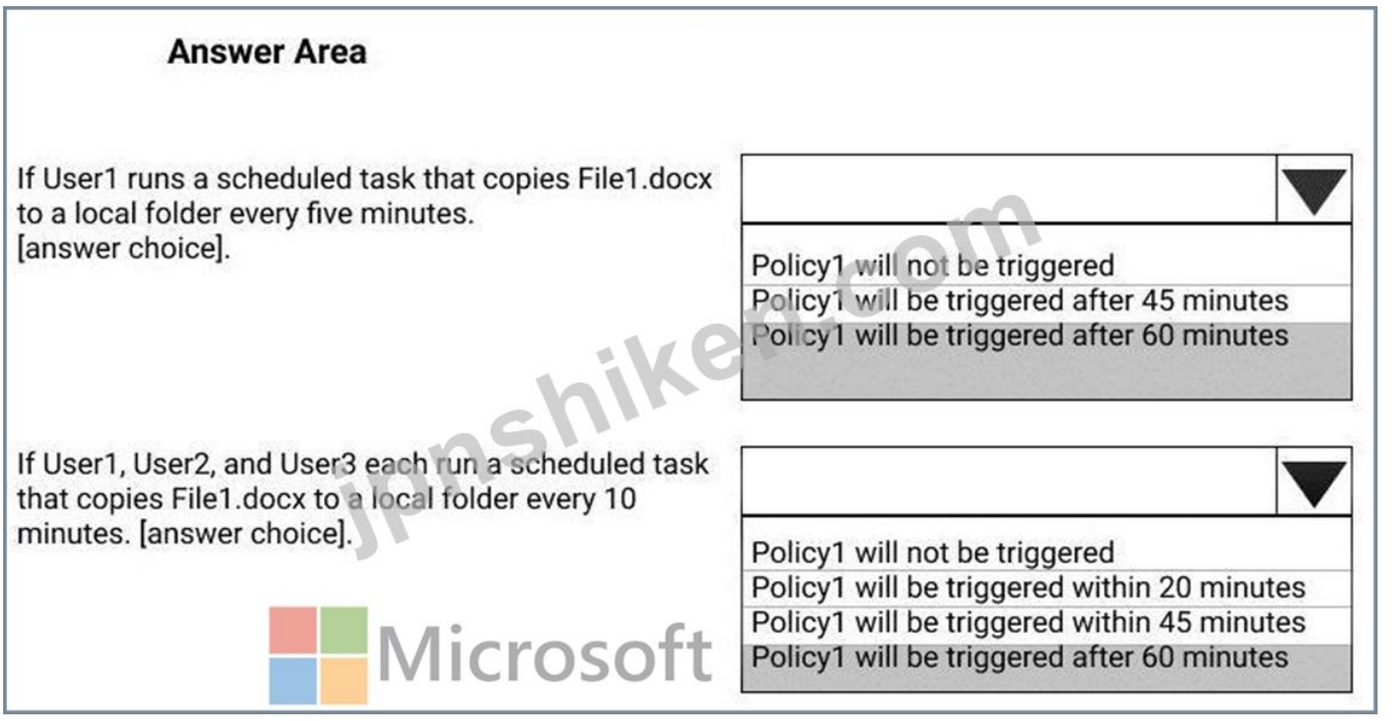
注 :それぞれの正しい選択には1ポイントの価値があります。


If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].
Policy1 will not be triggered
Policy1 will be triggered after 45 minutes
Policy1 will be triggered after 60 minutes
If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].
Policy1 will not be triggered
Policy1 will be triggered within 20 minutes
Policy1 will be triggered within 45 minutes
Policy1 will be triggered after 60 minutes

正解:


If User1 runs a scheduled task that copies File1.docx to a local folder every five minutes. [answer choice].
Policy1 will not be triggered
Policy1 will be triggered after 45 minutes
Policy1 will be triggered after 60 minutes
If User1, User2, and User3 each run a scheduled task that copies File1.docx to a local folder every 10 minutes. [answer choice].
Policy1 will not be triggered
Policy1 will be triggered within 20 minutes
Policy1 will be triggered within 45 minutes
Policy1 will be triggered after 60 minutes

説明



参照：

https://docs.microsoft.com/en-us/office365/securitycompliance/alert-policies

質問: **26**

ワークロード管理者のセキュリティ要件を満たすために、アクセスレビューを構成する予定です。アクセスレビューポリシーを作成し、範囲とグループを指定します。

他にどの設定を構成する必要がありますか？回答するには、回答エリアで適切なオプションを選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。

正解:

説明

質問: **27**

Microsoft 365サブスクリプションがあります。

Exchange管理者の役割を割り当てられているすべてのユーザーが、既定で多要素認証（MFA）を有効にしていることを確認する必要があります。

目標を達成するために何を使うべきですか？

A. セキュリティとコンプライアンスのアクセス許可

B. Microsoft Office 365ユーザー管理

C. Microsoft Azure ADグループ管理

D. Microsoft Azure Active Directory（Azure AD）特権ID管理

正解: **(**正解を表示します**)**

質問: **28**

Microsoft 365サブスクリプションがあります。

Advanced Threat Protection（ATP）安全な添付ファイルポリシーを作成します。

検疫内の添付ファイルの保持期間を構成する必要があります。

どのタイプの脅威管理ポリシーを作成する必要がありますか？
A. スパム対策
B. マルウェア対策
C. DKIM
D. ATPアンチフィッシング
正解: (正解を表示します)

質問: **29**
Microsoft 365サブスクリプションがあります。
ユーザーがどのコンテンツをデータ損失防止（DLP）ポリシーの対象とするかを手動で指定できるようにする必要があります。
最初に何を作成する必要がありますか？
A. Microsoft Office 365の保持ラベル
B. カスタムの機密情報タイプ
C. データ主体要求（DSR）
D. Microsoft Office 365の安全な添付ファイルポリシー
正解: (正解を表示します)
説明
参照：
https://docs.microsoft.com/en-us/office365/securitycompliance/manage-gdpr-data-subject-requests-with-thedsr-c

質問: **30**
Group3を作成する必要があります
グループを作成する2つの可能な方法は何ですか？
A. Microsoft 365管理センターのOffice 365グループ
B. Microsoft 365管理センターのメールが有効なセキュリティグループ
C. Microsoft 365管理センターのセキュリティグループ
D. Microsoft 365管理センターの配布リスト
E. Azure AD管理センターのセキュリティグループ
正解: (正解を表示します)
トピック2、Contoso、Ltd
概要
Contoso、Ltd.は、モントリオールにメインオフィス、シアトルとニューヨークに3つの支社を持つコンサルティング会社です。
会社には、次の表に示すオフィスがあります。

Location	Employees	Laptops	Desktops computers	Mobile devices
Montreal	2, 500	2, 800	300	3, 100
Seattle	1, 000	1, 100	200	1, 500
New York	300	320	30	400

Contosoには、IT、人事（HR）、法務、マーケティング、財務部門があります。ContosoはMicrosoftを使用しています
365。
既存の環境
インフラ
ネットワークには、Microsoft Azure Active Directory（Azure AD）テナントに同期されるcontoso.comという名前のActive Directoryドメインが含まれています。パスワードの書き戻しが有効になっています。
ドメインには、Windows Server 2016を実行するサーバーが含まれます。ドメインには、Windows 10 Enterpriseを実行するラップトップおよびデスクトップコンピューターが含まれます。
各クライアントコンピューターには単一のボリュームがあります。
各オフィスは、NATデバイスを使用してインターネットに接続します。オフィスには、次の表に示すIPアドレスがあります。

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24
New York	192.168.0.0/16	198.35.3.0/24

名前付きの場所は、次の表に示すようにAzure ADで定義されます。

Name	IP address range	Trusted
Montreal	10.10.0.0/16	Yes
New York	192.168.0.0/16	No

[多要素認証]ページから、198.35.3.0 / 24のアドレススペースが信頼済みIPリストに定義されます。
Azure Multi-Factor Authentication（MFA）は、財務部門のユーザーに対して有効になっています。
テナントには、次の表に示すユーザーが含まれます。

Name	User type	City	Role
User1	Member	Seattle	None
User2	Member	Sea	Password administrator
User3	Member	SEATTLE	None
User4	Guest	SEA	None
User5	Member	London	None
User6	Member	London	Customer LockBox Access Approver
User7	Member	Sydney	Reports reader
User8	Member	Sydney	User administrator
User9	Member	Montreal	None

テナントには、次の表に示すグループが含まれます。

Name	Group type	Dynamic membership rule
ADGroup1	Security	User.city-contains “SEA”
ADGroup2	Office 365	User.city-match “Sea”

カスタマーロックボックスは、Microsoft 365で有効になっています。
Microsoft Intuneの構成
Intuneに登録されているデバイスは、次の表に示すように構成されます。

Name	Platform	Encryption	Member of
Device1	Android	Disabled	GroupA, GroupC
Device2	Windows 10	Enabled	GroupB, GroupC
Device3	Android	Disabled	GroupB, GroupC
Device4	Windows 10	Disabled	GroupB
Device5	iOS	Not applicable	GroupA
Device6	Windows 10	Enabled	None

Intuneのデバイスコンプライアンスポリシーは、次の表に示すように構成されます。

Name	Platform	Encryption	Assigned
DevicePolicy1	Android	Not configured	Yes
DevicePolicy2	Windows 10	Required	Yes
DevicePolicy3	Android	Required	Yes

デバイスコンプライアンスポリシーには、次の表に示す割り当てがあります。

Name	Include	Exclude
DevicePolicy1	GroupC	None
DevicePolicy2	GroupB	GroupC
DevicePolicy3	GroupA	None

[コンプライアンスポリシーが割り当てられていないデバイスをマークする]設定が[準拠]に設定されます。
必要条件
技術的要件
Contosoは、次の技術要件を特定します。
*最小特権の原則を使用する
*レポートリーダーの役割をユーザーに割り当てるためにUser1を有効にする
* User6がカスタマーロックボックスリクエストをできるだけ早く承認するようにします
* User9がAzure ADの特権ID管理を実装できることを確認する

質問: **31**
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。
Microsoft Exchange Onlineに適用される条件付きアクセスポリシーがあります。条件付きアクセスポリシーは、条件付きアクセスアプリ制御を使用するように構成されています。
User1がExchange Onlineからの印刷をブロックするMicrosoft Cloud App Securityポリシーを作成する必要があります。
どのタイプのCloud App Securityポリシーを作成する必要がありますか？

A. セッションポリシー
B. Cloud Discoveryの異常検出ポリシー
C. アクティビティポリシー
D. アプリの許可ポリシー
正解: **(**正解を表示します**)**

質問: **32**
次の表に示すマイクロソフトの条件があります。

Name	Pattern	Case sensitivity
Condition1	Product1	Off
Condition2	Product2	On

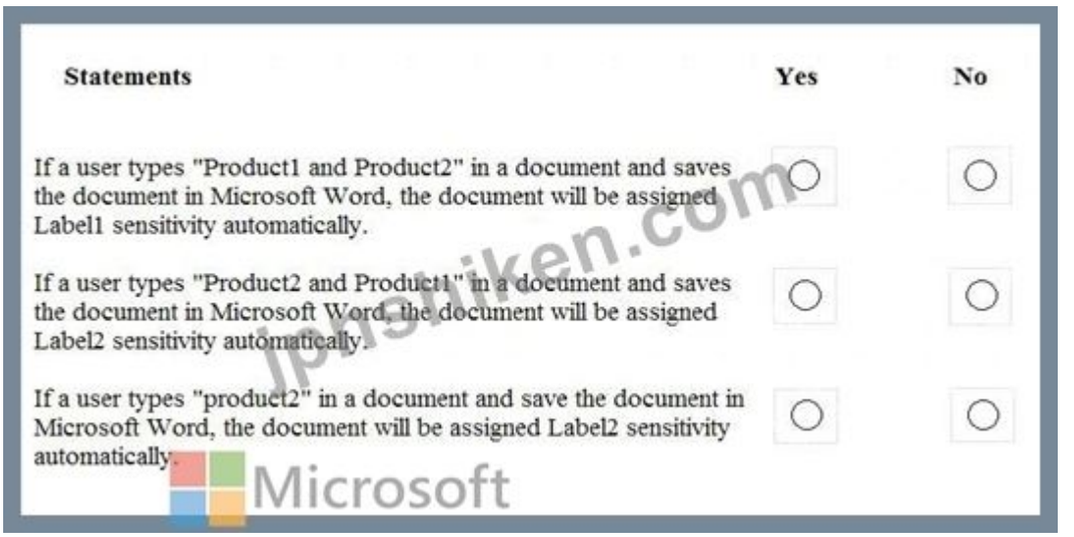
次の表に示すAzure Information Protectionラベルがあります。

Name	Use condition	Label is applied
Label1	Condition1	Automatically
Label2	Condition2	Automatically

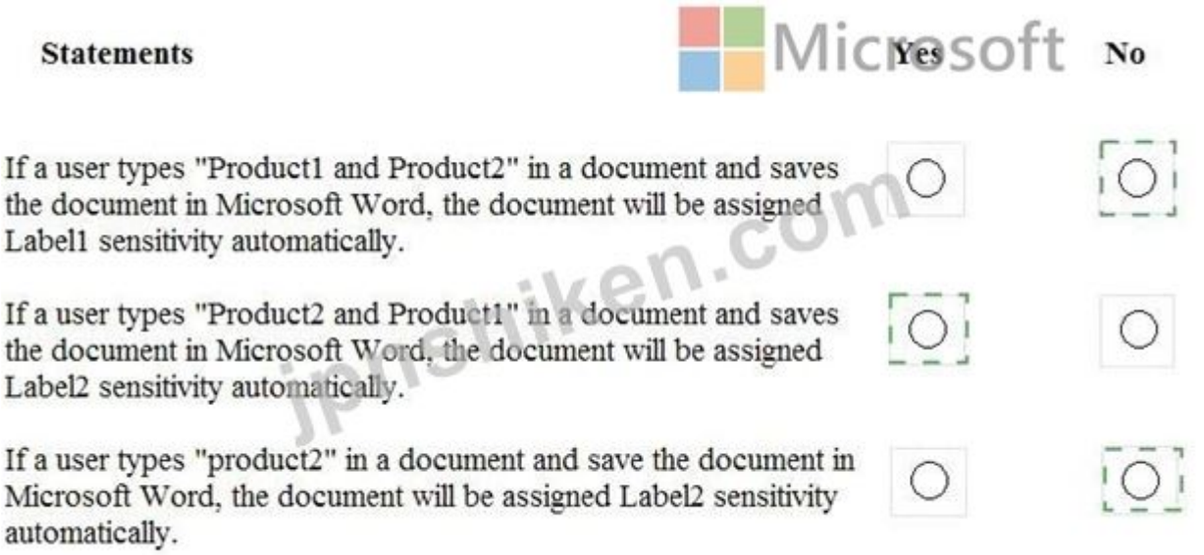
次の表に示すAzure Information Protectionポリシーがあります。

Name	Applies to	Use label	Set the default label
Global	*Not applicable*	*None*	None
Policy1	User1	Label1	None
Policy2	User2	Label2	None

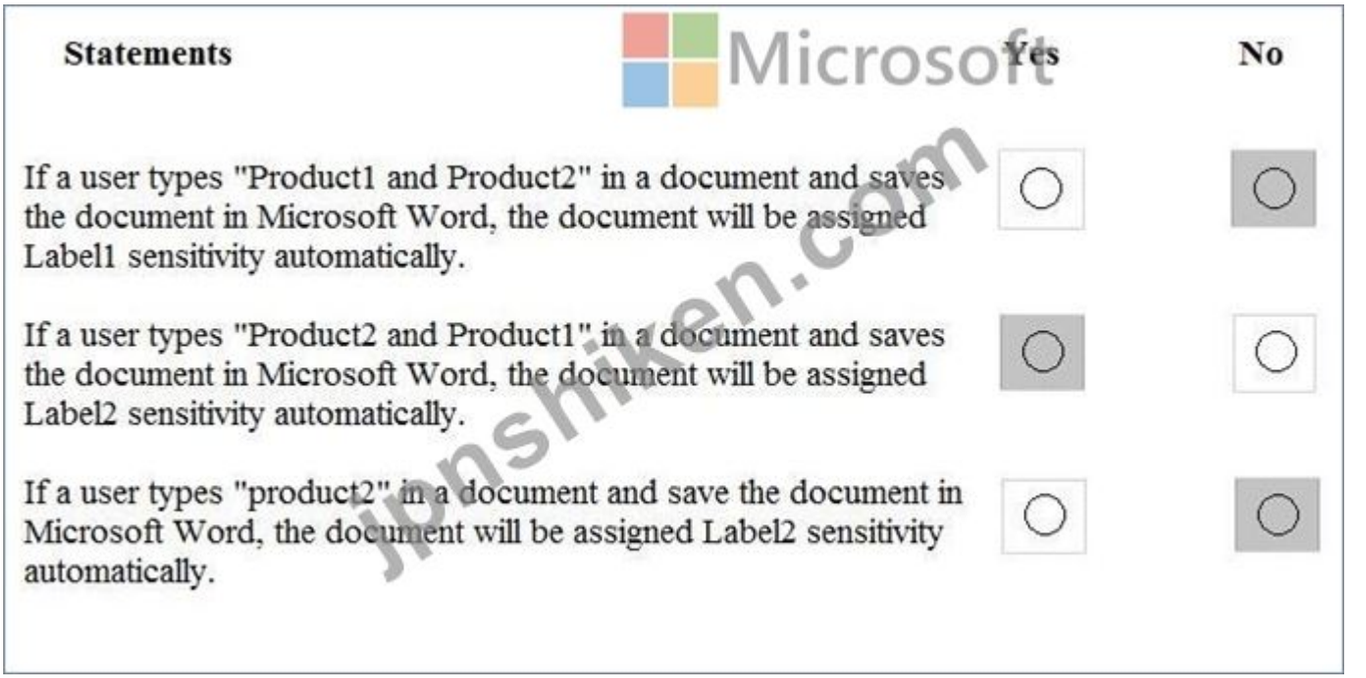
以下の各ステートメントについて、ステートメントが真である場合は「はい」を選択します。それ以外の場合は、「いいえ」を選択します。


Statements
Yes
No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.
Microsoft

正解:


Statements
Yes
No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.

説明


Statements
Yes
No
If a user types "Product1 and Product2" in a document and saves the document in Microsoft Word, the document will be assigned Label1 sensitivity automatically.
If a user types "Product2 and Product1" in a document and saves the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.
If a user types "product2" in a document and save the document in Microsoft Word, the document will be assigned Label2 sensitivity automatically.

質問: **33**
Admin1とAdmin2のサインインを保護するソリューションを推奨する必要があります。
推奨事項に何を含めるべきですか？
A. デバイスコンプライアンスポリシー
B. アクセスレビュー
C. ユーザーリスクポリシー
D. サインインリスクポリシー
正解: **C** (コメントを発表する)
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-user-risk-policy
トピック1、Litware、Inc
概要
Litware、Inc.は、シカゴの本社に1,000人のユーザーが、サンフランシスコの支社に100人のユーザーがある金融会社です。
既存の環境
内部ネットワークインフラストラクチャ
ネットワークには単一のドメインフォレストが含まれます。フォレストの機能レベルはWindows Server 2016です。
ユーザーは、Active Directoryで定義されているサインイン時間制限の対象となります。
ネットワークには、次の表に示すIPアドレス範囲があります。

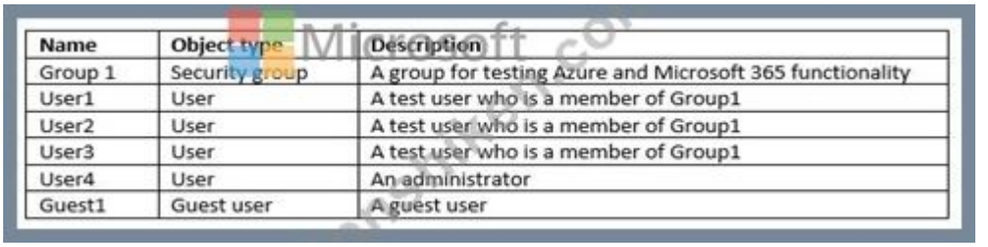
Location	IP address range
Chicago office internal network	192.168.0.0/20
Chicago office perimeter network	172.16.0.0/24
Chicago office external network	131.107.83.0/28
San Francisco office internal network	192.168.16.0/20
San Francisco office perimeter network	172.16.16.0/24
San Francisco office external network	131.107.16.218/32

オフィスは、マルチプロトコルラベルスイッチング（MPLS）を使用して接続します。
ネットワークでは次のオペレーティングシステムが使用されます。
* Windows Server 2016
* Windows 10 Enterprise
* Windows 8.1 Enterprise
内部ネットワークには、次の表に示すシステムが含まれます。

Office	Name	Configuration
Chicago	DC1	Domain controller
Chicago	DC2	Domain controller
San Francisco	DC3	Domain controller
Chicago	Server1	SIEM-server

Litwareはサードパーティの電子メールシステムを使用します。
クラウドインフラ
Litwareは最近、すべてのユーザー用にMicrosoft 365サブスクリプションライセンスを購入しました。

Microsoft Azure Active Directory (Azure AD) Connectがインストールされ、デフォルトの認証設定が使用されます。
ユーザーアカウントはまだAzure ADに同期されていません。
次の表に示すMicrosoft 365ユーザーとグループがあります。



Name	Object type	Description
Group 1	Security group	A group for testing Azure and Microsoft 365 functionality
User1	User	A test user who is a member of Group1
User2	User	A test user who is a member of Group1
User3	User	A test user who is a member of Group1
User4	User	An administrator
Guest1	Guest user	A guest user

計画的な変更
Litwareは、次の変更を実装する予定です。
*メールシステムをMicrosoft Exchange Onlineに移行する
* Azure AD特権ID管理を実装する
セキュリティ要件
Litwareは、次のセキュリティ要件を識別します。
*すべてのAzure ADユーザーアカウントを含むGroup2という名前のグループを作成します。Group2は、Windows Analyticsへの制限されたアクセスを提供するために使用されます
*パイロットユーザーにAzure Information Protectionポリシーを適用するために使用されるGroup3という名前のグループを作成します。Group3にはユーザーアカウントのみを含める必要があります
* Azure Advanced Threat Protection (ATP)を使用して、フォレストをターゲットとするセキュリティの脅威を検出する
* Active Directoryからロックアウトされたユーザーがazure ADおよびActive Directoryにサインインできないようにする
* User1のコンプライアンス管理者ロールの永続的な適格な割り当てを実装する
*ドメインに参加しているサーバーでWindows DefenderとWindows Defender ATPを統合する
*デフォルトでゲストユーザーアカウントのAzureリソースへのアクセスを禁止する
*ドメインに参加しているすべてのコンピューターがAzure ADに登録されていることを確認する
多要素認証 (MFA)の要件
Microsoft Office 365およびAzureのセキュリティ機能は、パイロットAzureユーザーアカウントを使用してテストされます。
MFAをテストするための次の要件を特定します。
*パイロットユーザーは、シカゴオフィスの内部ネットワークからサインインしていない限り、MFAを使用する必要があります。
MFAは、シカゴオフィスの内部ネットワークでは使用しないでください。
*認証の試みが疑わしい場合、ユーザーの場所に関係なく、MFAを使用する必要があります
*正当な認証試行の中断は最小限に抑える必要があります一般要件Litwareは、Active Directoryフォレストでの追加のサーバーおよびサービスの展開を最小限に抑えたいと考えています。

質問: 34

パートナーとデータを共有するための技術的要件およびセキュリティ要件を満たすソリューションを推奨する必要があります。
推奨事項に何を含めるべきですか？それぞれの正解はソリューションの一部を示しています。
注 :それぞれの正しい選択には1ポイントの価値があります。
A. アクセスレビューを作成します。
B. Azure Active Directory管理センターで外部コラボレーション設定を変更します。
C. ゲスト招待者の役割をUser1に割り当てます。
D. グローバル管理者ロールをUser1に割り当てます。
正解: **(**正解を表示します**)**

質問: **35**
User9の技術要件を満たす必要があります。あなたは何をするべきか？
A. 特権管理者の役割をUser9に割り当て、User9の携帯電話番号を構成します
B. コンプライアンス管理者の役割をUser9に割り当て、User9の携帯電話番号を構成します
C. セキュリティ管理者の役割をUser9に割り当てます
D. グローバル管理者ロールをUser9に割り当てます
正解: **(**正解を表示します**)**
説明
https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-give-access

質問: **36**
会社にはメインオフィスとMicrosoft 365サブスクリプションがあります。
物理的にオフィスにいないすべてのユーザーに条件付きアクセスを使用して、Microsoft Azure Multi-Factor Authentication（MFA）を実施する必要があります。
構成には何を含める必要がありますか？
A. ユーザーリスクポリシー
B. サインインリスクポリシー
C. Azure Active Directory（Azure AD）の名前付き場所
D. Azure MFAサーバー
正解: **(**正解を表示します**)**
説明
参照：
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition

質問: **37**
Microsoft 365サブスクリプションがあります。
マルウェアを検疫するために、高度な脅威保護（ATP）安全な添付ファイルポリシーを作成します。
検疫内の添付ファイルの保持期間を構成する必要があります。

Security＆Compliance管理センターからどのタイプの脅威管理ポリシーを作成する必要がありますか？
A. DKIM
B. マルウェア対策
C. ATPアンチフィッシング
D. スパム対策
正解: **(**正解を表示します**)**

質問: **38**
ハイブリッドMicrosoft 365環境があります。すべてのコンピューターはWindows 10を実行し、Microsoft Intuneを使用して管理されます。
準拠としてマークされたWindows 10コンピューターのみがオンプレミスネットワークへのVPN接続を確立できるようにするMicrosoft Azure Active Directory（Azure AD）条件付きアクセスポリシーを作成する必要があります。
最初に何をすべきですか？
A. Azure Active Directory管理センターから、新しい証明書を作成します
B. Azure ADでアプリケーションプロキシを有効にする
C. Active Directory管理センターから、ダイナミックアクセス制御ポリシーを作成します
D. Azure Active Directory管理センターから、認証方法を構成します
正解: **A (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/ad-ca-vpn-connectivitywindows10

質問: **39**
Microsoft 365サブスクリプションがあります。
ユーザーが、Microsoft OneDriveのいくつかのファイルに変更が加えられたことを報告します。
ユーザーのOneDriveで、どのファイルがどのユーザーによって変更されたかを識別する必要があります。
あなたは何をするべきか？
A. Azure Active Directory管理センターから、監査ログを開きます
B. OneDrive管理センターから、選択します
C. セキュリティとコンプライアンスから、電子情報開示検索を実行します
D. Microsoft Cloud App Securityから、アクティビティログを開きます
正解: **D (**コメントを発表する**)**
参照：
https://docs.microsoft.com/en-us/cloud-app-security/activity-filters

質問: **40**
Group2を作成する必要があります。

グループを作成する2つの可能な方法は何ですか？
A. Azure AD管理センターのセキュリティグループ
B. Microsoft 365管理センターのOffice 365グループ
C. Microsoft 365管理センターの配布リスト
D. Microsoft 365管理センターのセキュリティグループ
E. Microsoft 365管理センターのメールが有効なセキュリティグループ
正解: **(**正解を表示します**)**

質問: **41**
注 :この質問は、同じシナリオを提示する一連の質問の一部です。シリーズの各質問には、記載された目標を達成する可能性のある独自のソリューションが含まれています。一部の質問セットには複数の正しい解決策がある場合もあれば、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すると、その質問に戻ることはできません。その結果、これらの質問はレビュー画面に表示されません。
contoso.comという名前のオンプレミスActive Directoryドメインがあります。
Windows Serverを実行するServer1という名前のサーバーにAzure AD Connectをインストールして実行します。
Azure AD Connectイベントを表示する必要があります。
Server1のディレクトリサービスイベントログを使用します。
それは目標を達成していますか？
A. はい
B. いいえ
正解: **B (**コメントを発表する**)**
説明
参照：
https://support.pingidentity.com/s/article/PingOne-How-to-troubleshoot-an-AD-Connect-Instance

質問: **42**
ネットワークには、contoso.comというオンプレミスのActive Directoryドメインが含まれています。ドメインには、次の表に示すグループが含まれます。

Name	Type	Email address
Group1	Security Group – Domain Local	Group1@contoso.com
Group2	Security Group – Universal	None
Group3	Distribution Group – Global	None
Group4	Distribution Group – Universal	Group4@contoso.com

ドメインは、次の表に示すグループを含むMicrosoft Azure Active Directory（Azure AD）テナントに同期されます。

Name	Type	Membership type
Group11	Security group	Assigned
Group12	Security group	Dynamic
Group13	Office	Assigned
Group14	Mail-enabled security group	Assigned

Policy1という名前のAzure Information Protectionポリシーを作成します。

Policy1を適用する必要があります。

Policy1はどのグループに適用できますか？回答するには、回答エリアで適切なオプションを選択します。

注 :それぞれの正しい選択には1ポイントの価値があります。

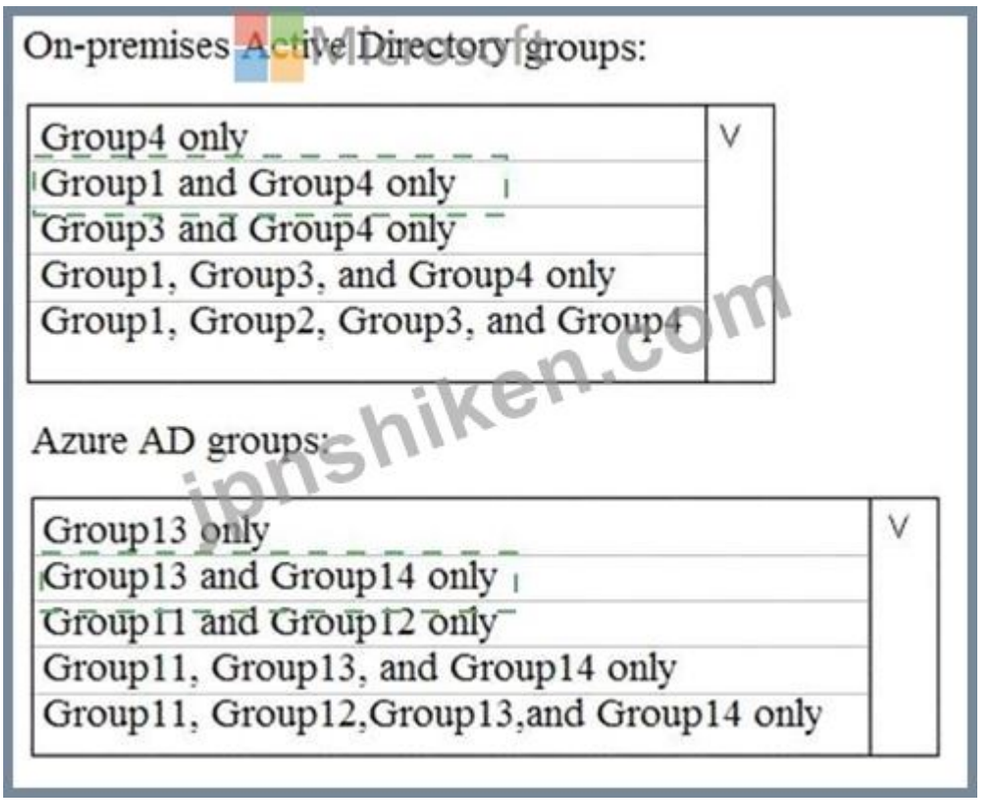
On-premises Active Directory groups:

Group4 only
Group1 and Group4 only
Group3 and Group4 only
Group1, Group3, and Group4 only
Group1, Group2, Group3, and Group4

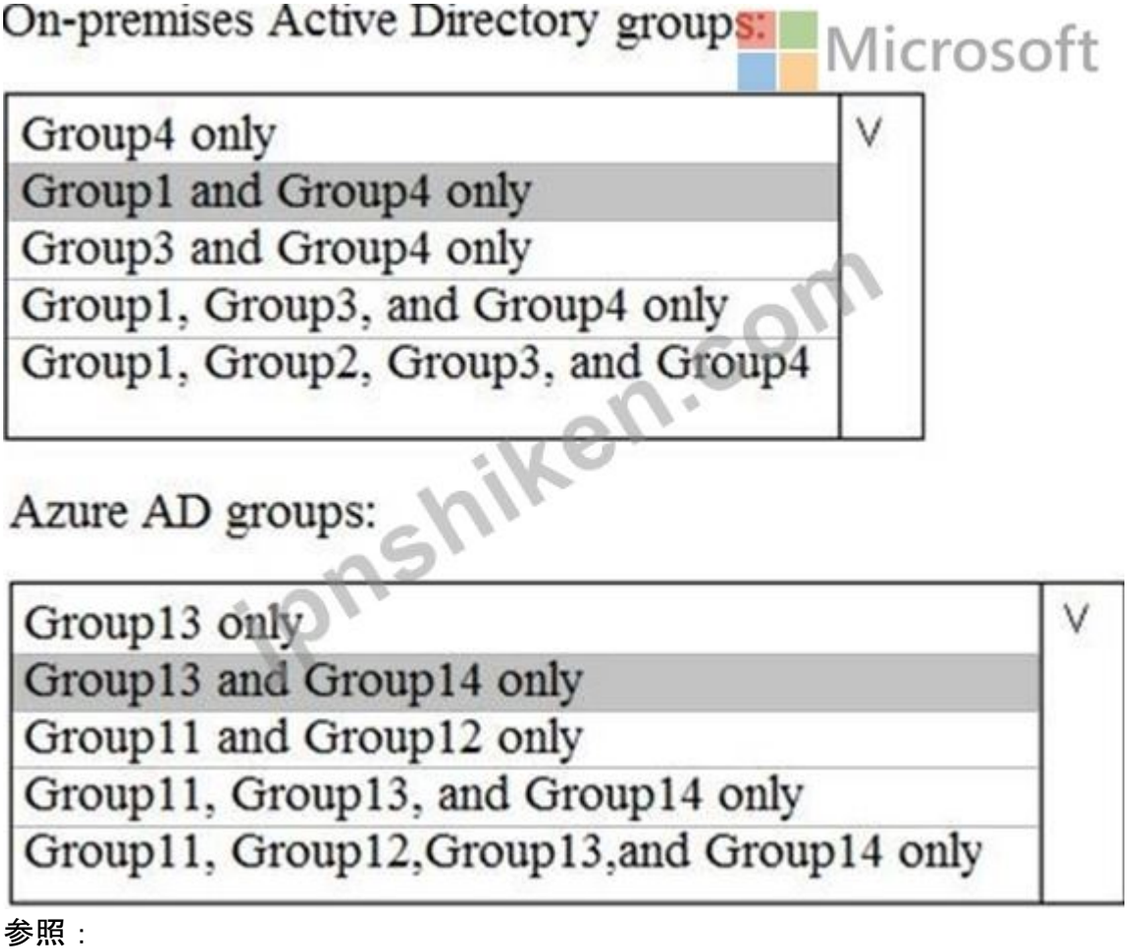
Azure AD groups:

Group13 only
Group13 and Group14 only
Group11 and Group12 only
Group11, Group13, and Group14 only
Group11, Group12,Group13,and Group14 only

正解:



説明



参照：

https://docs.microsoft.com/en-us/azure/information-protection/prepare

質問: 43

最近、Microsoft 365サブスクリプションで複数のラベルポリシーを作成して公開しました。
ユーザーが手動で適用したラベルと、自動的に適用されたラベルを表示する必要があります。
セキュリティとコンプライアンスの管理センターから何をすべきですか？
A. [検索と調査]から[電子情報開示]を選択します
B. データガバナンスから、イベントを選択します
C. [検索と調査]から[コンテンツ検索]を選択します
D. レポートから、ダッシュボードを選択します
正解: **(**正解を表示します**)**