Microsoft.MD-102-JPN.v2026-02-17.q158

試験コード：	MD-102-JPN
試験名称：	Endpoint Administrator (MD-102日本語版)
認証ベンダー：	Microsoft
無料問題の数：	158
バージョン：	v2026-02-17
ページの閲覧量：	117
問題集の閲覧量：	2783

https://www.jpnshiken.com/shiken/Microsoft.MD-102-JPN.v2026-02-17.q158.html

質問: **1**

Microsoft 365 サブスクリプションがあり、User1 と User2 という 2 人のユーザーがいます。ユーザーが次のタスクを実行できることを確認する必要があります。

* ユーザー1 はグループを作成し、ユーザーを管理できる必要があります。
* ユーザー2 は、管理ユーザーのパスワードをリセットできる必要があります。

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。

各ユーザーにどのロールを割り当てる必要がありますか? 答えるには、適切なロールを正しいユーザーにドラッグします。各ロールは、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。

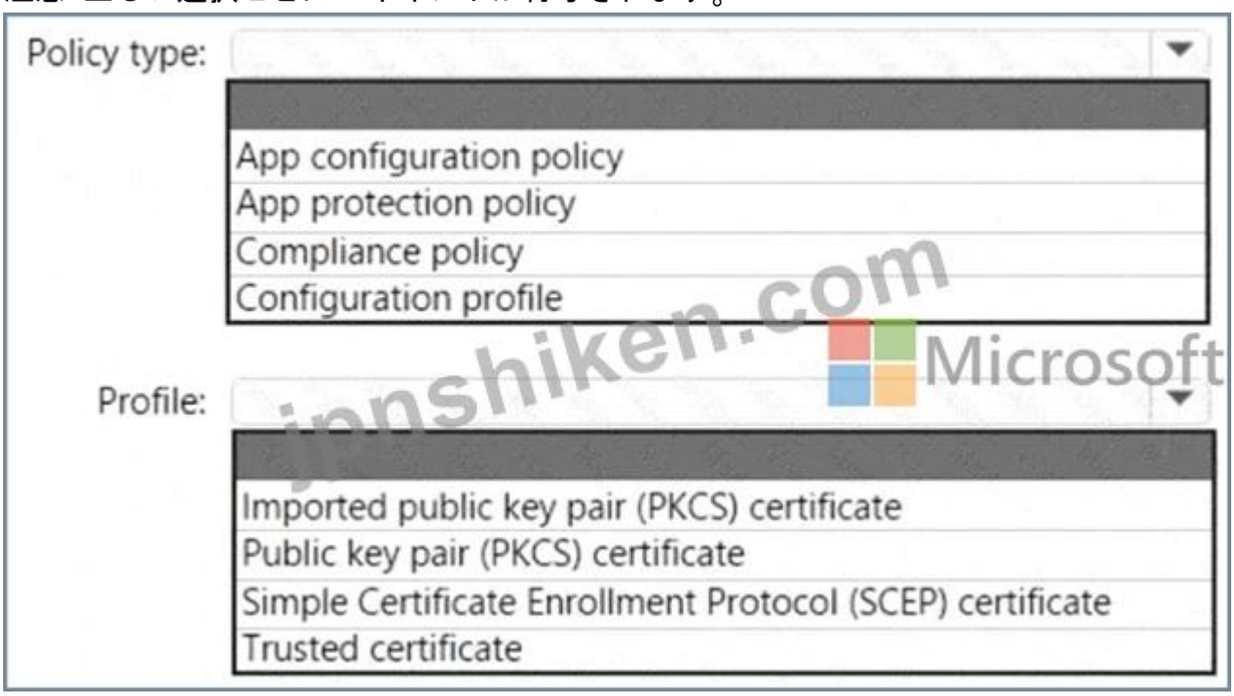
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

Microsoft 365 or Office 365 subscription comes with a set of admin roles that you can assign to users in your organization using the Microsoft 365 admin center. Each admin role maps to common business functions and gives people in your organization permissions to do specific tasks in the admin centers1.
To ensure that User1 can create groups and manage users, you should assign the User Administrator role to User1. This role allows User1 to create and manage all aspects of users and groups, including resetting passwords for non-administrative users1.
To ensure that User2 can reset passwords for non-administrative users, you should assign the Helpdesk Administrator role to User2. This role allows User2 to reset passwords, manage service requests, and monitor service health for non-administrative users1.

質問**: 2**
Microsoft 365 テナントと内部証明機関 (CA) があります。
管理対象デバイスにルート CA 証明書を展開するには、Microsoft Intune を使用する必要があります。
どのタイプの Intune ポリシーとプロファイ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ます。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解**:**

Explanation:
Box 1: Configuration profile
Create a trusted certificate profile.
Box 2: Trusted certificate
When using Intune to provision devices with certificates to access your corporate resources and network, use a trusted certificate profile to deploy the trusted root certificate to those devices.
Trusted root certificates establish a trust from the device to your root or intermediate (issuing) CA from which the other certificates are issued.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root

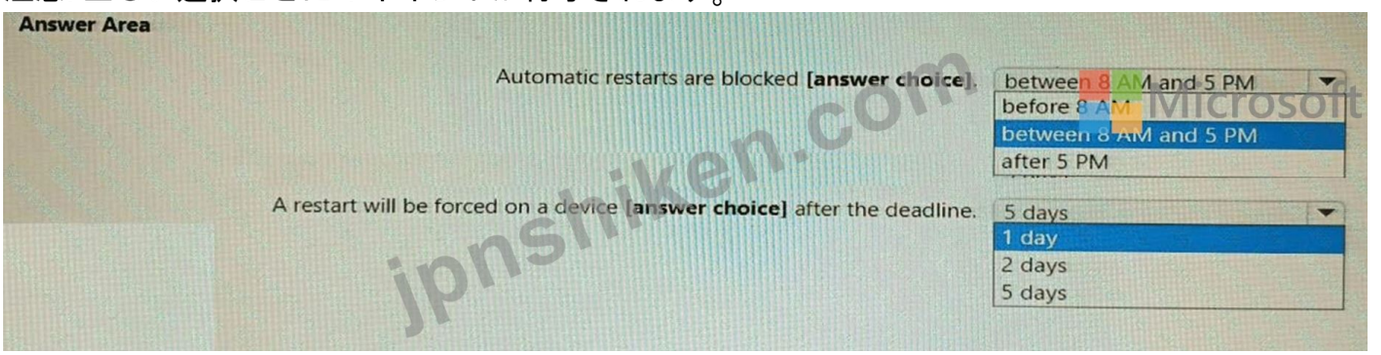
質問: **3**
Microsoft 365 E5 サブスクリプションをお持ちです。すべての Windows デバイスは Microsoft Intune に登録されています。
Policy1 という名前のアプリ保護ポリシーを作成し、Policy1 をデバイスに適用する必要があります。Policy1 を使用して何を保護できますか?
A. Microsoft Outlook
B. Microsoft Teams
C. Microsoft OneDrive
D. Microsoft Edge
正解: **(**正解を表示します**)**

質問: **4**
Microsoft Intune を使用する Microsoft 365 サブスクリプションがあります。
Intune を使用して Windows 更新プログラムを管理する予定です。

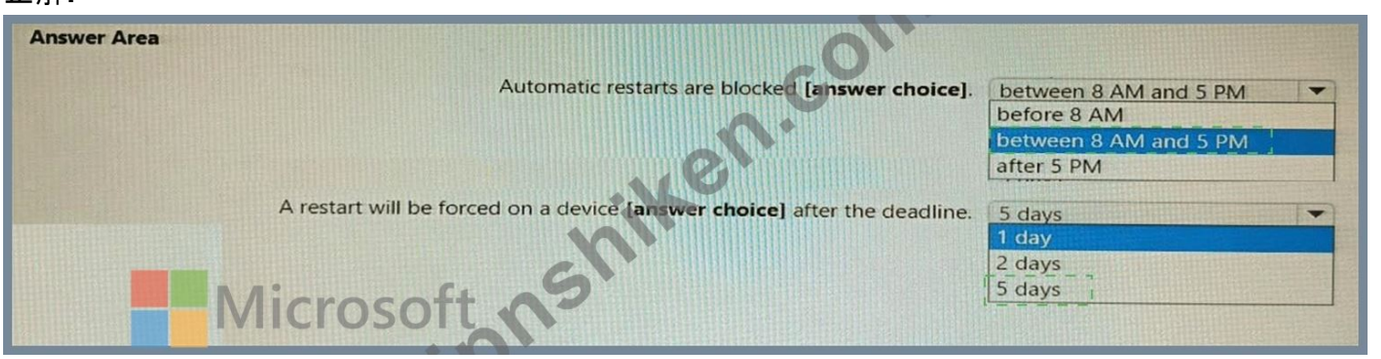
Windows 10 以降の更新リングを作成し、次の図に示すようにリングのユーザー エクスペリエンス設定を構成します。

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。

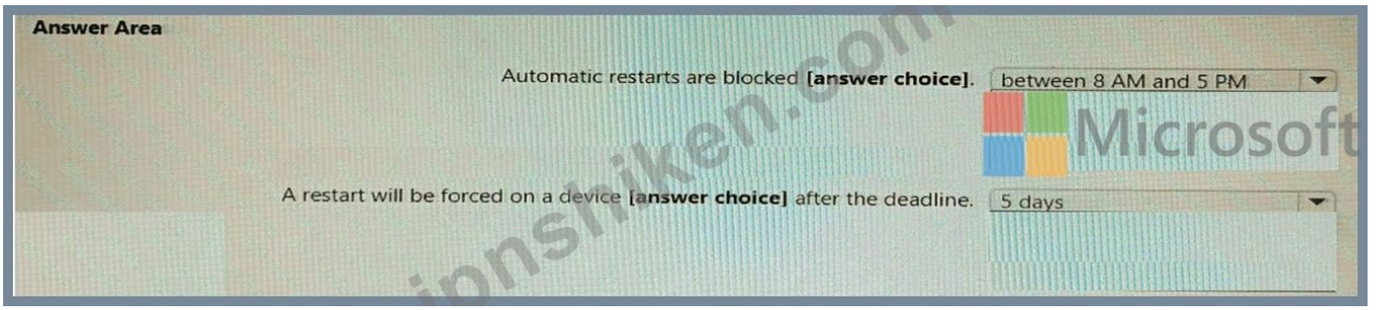
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



質問: **5**

ネットワークには Active Directory ドメインが含まれています。

ドメインには、Windows 10 を実行する Computer 1、Compute2、Compute3、Compute4 という 4 台のコンピューターが含まれています。次のアクションを実行します。

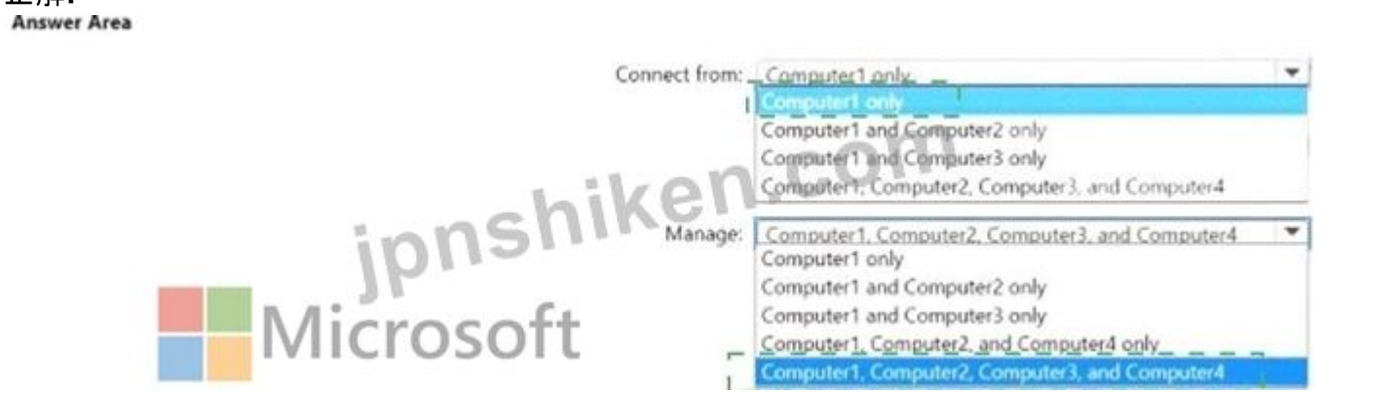
* Computer1 に Windows Admin Center をインストールし、TCP ポート 80.443. および 6516 経由の受信通信を許可するように Windows Defender ファイアウォールを構成します。
* Computed では、Enable-PS Remoting コマンドレットを実行します。
* コンピュータ3では、Windows Defenderファイアウォールを構成して、Windowsリモート管理（WinRM）トラフィックを許可します。
* Computer4 で、winrm quickconfig コマンドを実行します。

Windows Admin Center を使用してコンピューターをリモートで管理する必要があります。

どのコンピューターから Windows Admin Center に接続できますか。また、どのコンピューターを Windows Admin Center を使用して管理できますか。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。

正解:



Explanation:

質問: 6

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。

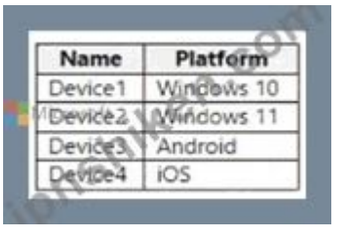
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

質問: 7

次の表に示すように、Microsoft Intune に登録されているデバイスがあります。



Name	Platform
Device1	Windows 10
Device2	Windows 11
Device3	Android
Device4	iOS

アプリ構成ポリシーを適用できるデバイスはどれですか?

A. デバイス2のみ

B. デバイス1とデバイス2のみ

C. デバイス3とデバイス4のみ

D. デバイス2、デバイス3、デバイス4のみ

E. デバイス1、デバイス2、デバイスB、デバイス4

正解: **(**正解を表示します**)**

The correct answer is D because app configuration policies can be applied to managed devices and managed apps1. Managed devices are enrolled and managed by Intune, while managed apps are integrated with Intune App SDK or wrapped using the Intune Wrapping Tool1. Device2, Device3, and Device4 are either enrolled in Intune or have managed apps installed, so they can receive app configuration policies2. Device1 is not enrolled in any MDM solution and does not have any managed apps installed, so it cannot receive app configuration policies2. References: 1: App configuration policies for Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/apps/app-configuration-policies-overview 2: Policy sets - Microsoft Intune | Microsoft Learn https://learn.microsoft.com/en-us/mem/intune/fundamentals/policy-sets

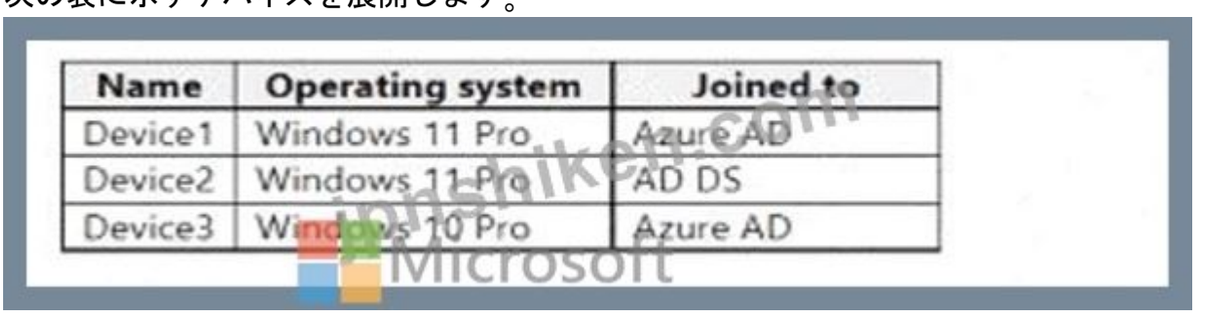
質問: **8**

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 Domain Services (AD DS) ドメインが含まれています。テナントには、次の表に示すユーザーが含まれています。

Name	Member of	On-premises sync
User1	Group1	Disabled
User2	Group2	Enabled

Windows 10/11 Enterprise E5 ライセンスを Gtoup1 と Uset2 に割り当てます。

次の表に示すデバイスを展開します。



Name	Operating system	Joined to
Device1	Windows 11 Pro	Azure AD
Device2	Windows 11 Pro	AD DS
Device3	Windows 10 Pro	Azure AD

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。

正解:

Explanation:

質問: **9**

Microsoft Intune を含む Microsoft 365 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、Intune に登録されている Windows 11 デバイスが含まれています。サブスクリプションには、Department Department2 および Department3 という名前の 3 つのグループが含まれています。

Microsoft 365 アプリを Windows 11 デバイスに展開する必要があります。ソリューションは次の要件を満たしている必要があります。

* Department1 と Department2 のユーザーには、Microsoft Project と Visio を含む完全な Microsoft 365 アプリ スイートが提供される必要があります。
* Department3 のユーザーには、Microsoft Project を含む完全な Microsoft 365 アプリ スイートが提供される必要がありますが、Visio は提供されません。
* その他のすべてのユーザーは、Microsoft Project または Visio を含まない完全な Microsoft 365 アプリ スイートを受け取る必要があります。

作成する必要があるデプロイメントの最小数はいくつですか?

A. 4
B. 1
C. 2
D. 3

正解: **(**正解を表示します**)**

質問: **10**
次のデバイス コンプライアンス ポリシー設定を持つ Microsoft Intune サブスクリプションがあります。
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 「準拠」としてマークする
コンプライアンスステータスの有効期間（日数）14
1 月 1 日に、次の表に示すように、Windows 10 デバイスを Intune に登録します。

Name	BitLocker Drive Encryption (BitLocker)	Firewall	Scope (Tags)	Member of
Device1	Enabled	Off	Tag1	Group1
Device2	Disabled	On	Tag2	Group2

1 月 4 日に、次の 2 つのデバイス コンプライアンス ポリシーを作成します。
名前: ポリシー1
プラットフォーム: Windows 10 以降
BitLockerが必要: 必要
デバイスを非準拠としてマーク: 非準拠から 5 日後
スコープ (タグ): タグ1
名前: ポリシー2
プラットフォーム: Windows 10 以降
ファイアウォール: 必須
デバイスを非準拠としてマーク: 直ちに
スコープ (タグ): タグ2
1 月 5 日に、Policy1 と Policy2 を Group1 に割り当てます。
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
On January 7, Device1 is marked as compliant.	○	○
On January 8, Device1 is marked as compliant.	○	○
On January 8, Device2 is marked as compliant.	○	○

正解:

Explanation:

Box 1: No.

Policy1 and Policy2 apply to Group1 which Device1 is a member of. Device1 does not meet the firewall requirement in Policy2 so the device will immediately be marked as non-compliant.

Box 2: No

For the same reason as Box1.

Box 3: Yes

Policy1 and Policy2 apply to Group1. Device2 is not a member of Group1 so the policies don't apply. The Scope (tags) have nothing to do with whether the policy is applied or not. The tags are used in RBAC.

質問: **11**

Microsoft Intune を使用する Microsoft 365 E5 サブスクリプションがあります。ログ データを Log Analytics に送信するように Intune を構成します。Intune への登録に失敗したデバイスに関連するイベントを確認する必要があります。何を監視する必要がありますか?

A. Intune デバイス ログ

B. デバイスコンプライアンス組織ログ

C. 操作ログ

D. 監査ログ

正解: **(**正解を表示します**)**

質問: **12**

Contoso Help Desk というグループを含む contoso.com という Microsoft Entra テナントがあります。
Windows デバイスが contoso.com に参加するたびに、Contoso Help Desk がローカルの Administrators グループに追加されていることを確認する必要があります。
何をすべきでしょうか?
A. contoso.com に対して Microsoft Entra ローカル管理者パスワード ソリューション (LAPS) を有効にします。
B. Contoso Help Desk にクラウド デバイス管理者のロールを割り当てます。
C. Microsoft Entra 参加デバイスのローカル管理者の役割を Contoso Help Desk に割り当てます。
D. Enterprise State Roaming 設定を構成します。
正解: **C** (コメントを発表する)

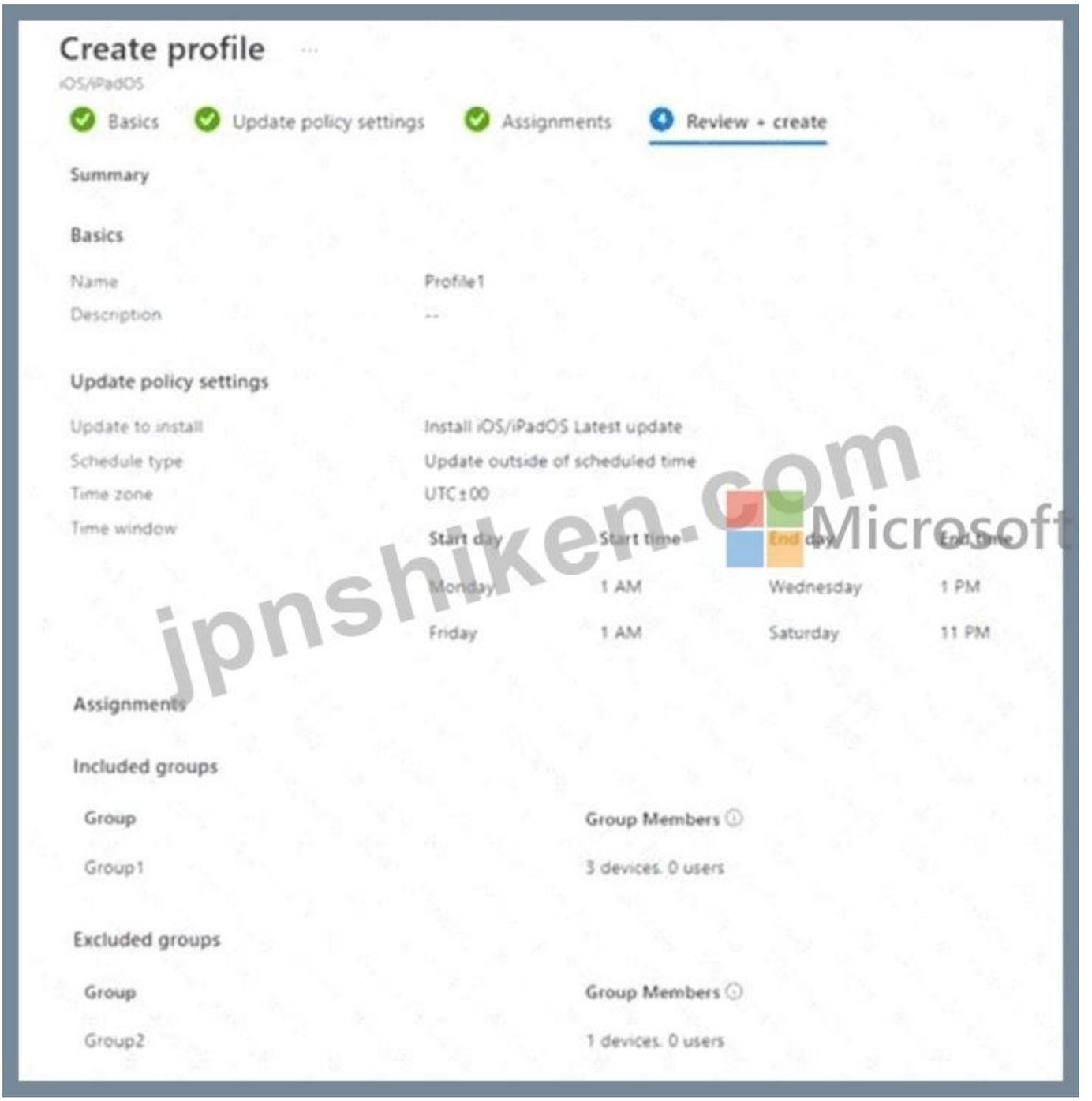
質問: **13**
Microsoft Intune を使用する Microsoft 365 ES サブスクリプションがあります。
デバイスは、次の表に示すように Intune に登録されます。

Name	Platform	Enrolled by using
Device1	iOS	Apple Automated Device Enrollment (ADE)
Device2	iPadOS	Apple Automated Device Enrollment (ADE)
Device3	iPadOS	The Company Portal app

デバイスは、次の表に示すグループのメンバーです。

Name	Members
Group1	Device1, Device2, Device3
Group2	Device2

次の図に示すように、JOS/iPadOS 更新プロファイルを作成します。



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 Area

Statements	Yes	No
If an iOS update becomes available on Tuesday at 5 AM, the update is installed on Device1 automatically on Wednesday.	○	○
If an iPadOS update becomes available on Thursday at 2 AM, the update is installed on Device2 automatically on Thursday.	○	○
If an iPadOS update becomes available on Friday at 4 PM, the update is installed on Device3 automatically on Sunday.	○	○

正解:

Explanation:

質問: **14**

Microsoft 365 E5 サブスクリプションをお持ちです。

ゼロタッチ登録を使用して、Android Enterprise デバイスを Microsoft Intune に登録する必要があります。

まず何をすべきでしょうか?

A. ゼロタッチ登録ポータルから、ゼロタッチ構成を作成します。

B. Microsoft Intune 管理センターから、Managed Google Play アカウントをリンクします。

C. Microsoft Intune 管理センターから、ゼロタッチ構成を作成します。

D. Microsoft Intune 管理センターから、登録制限を構成します。

正解: **(正解を表示します)**

質問: **15**

Microsoft 365 サブスクリプションをお持ちです。

Microsoft Intune にデバイスを登録する予定です。以下の要件を満たす必要があります。

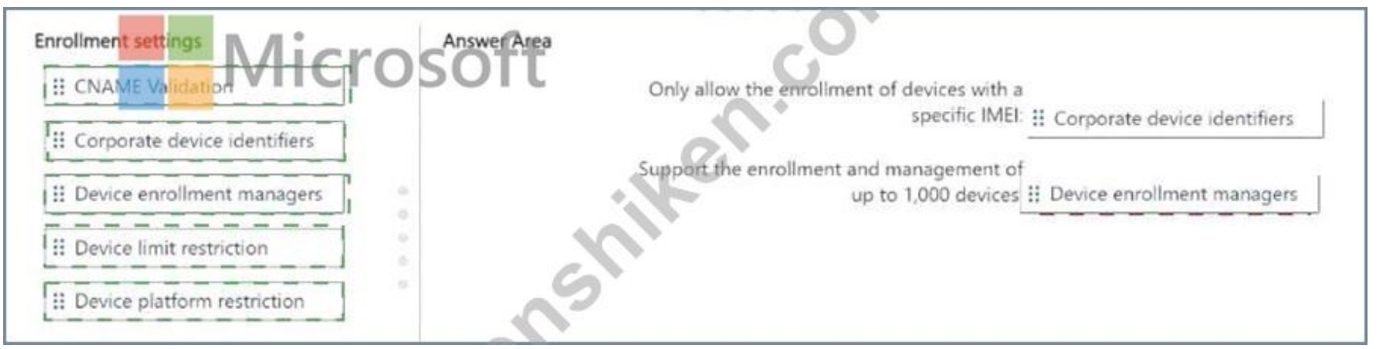
* 特定の国際モバイル機器識別子 (IMEI) を持つデバイスの登録のみを許可します。
* 最大1,000台のデバイスの登録と管理をサポート

各要件に対してどの登録設定を行うべきでしょうか? 適切な設定を適切な要件にドラッグしてください。各設定は、1回使用することも、複数回使用することも、まったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。

デバイス

正解:



Explanation:

質問: **16**

Windows 11 を実行する 500 台のコンピューターを含む Microsoft 365 サブスクリプションがあります。コンピューターは Azure AD に参加しており、Microsoft Intune に登録されています。

コンピューター上で Microsoft Defender ウイルス対策を管理する予定です。

ユーザーがMicrosoft Defenderウイルス対策を無効にでき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. Microsoft Intune 管理センターから、セキュリティ ベースラインを作成します。

B. Microsoft 365 Defender ポータルから、改ざん防止を有効にします。

C. Microsoft Intune 管理センターから、アカウント保護ポリシーを作成します。

D. Microsoft Intune 管理センターから、エンドポイント検出および応答 (EDR) ポリシーを作成します。

正解: **(**正解を表示します**)**

Tamper protection is a feature of Microsoft Defender Antivirus that prevents users or malicious software from disabling or modifying the antivirus settings. Tamper protection can be enabled from the Microsoft 365 Defender portal for devices that are Azure AD joined and enrolled in Microsoft Intune. This will prevent users from turning off Microsoft Defender Antivirus or changing its

configuration through Windows Security, PowerShell, Registry, or Group Policy. References: [Enable tamper protection]

質問: **17**

Microsoft Intune を含む Microsoft 365 サブスクリプションをお持ちです。

次の表に示すように、Windows 11 を実行するコンピューターがあります。

Name	Azure AD status	Intune	BitLocker Drive Encryption (BitLocker)	Firewall
Computer1	Joined	Enrolled	Disabled	Enabled
Computer2	Registered	Enrolled	Enabled	Enabled
Computer3	Registered	Not enrolled	Enabled	Disabled

次の表に示すグループがあります。

Name	Members
Group1	Computer1, Computer2
Group2	Computer3

次の表に示すコンプライアンス ポリシーを作成して割り当てます。

Name	Configuration	Action for noncompliance	Assignment
Policy1	Require BitLocker to be enabled on the device.	Mark device as noncompliant after 10 days.	Group1
Policy2	Require firewall to be on and monitoring.	Mark device as noncompliant immediately.	Group2

翌日、コンピューターのコンプライアンス ステータスを確認します。

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。

正解:

Explanation:

質問: **18**

Microsoft 365 Business Standard サブスクリプションと 100 台の Windows 10 Pro デバイスを所有しています。

Microsoft 365 E5 サブスクリプションを購入します。

Windows 10 Pro デバイスを Windows 10 Enterprise にアップグレード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。

どのアップグレード方法を使用すればよいですか?

A. Windows オートパイロット

B. Microsoft Deployment Toolkit (MDT) のライトタッチ展開

C. サブスクリプションの有効化

D. Windows インストール メディアを使用したインプレース アップグレード

正解: **(**正解を表示します**)**

Subscription Activation is a feature that allows you to upgrade from Windows 10 Pro or Windows 11 Pro to Windows 10 Enterprise or Windows 11 Enterprise without needing a product key or reinstallation. You just need to assign a subscription license (such as Microsoft 365 E5) to the user in Azure AD, and then sign in to the device with that user account. The device will automatically activate Windows Enterprise edition using the firmware-embedded activation key for Windows Pro edition. This method minimizes administrative effort and simplifies the upgrade process. References: Windows subscription activation, Deploy Windows Enterprise licenses

質問: **19**

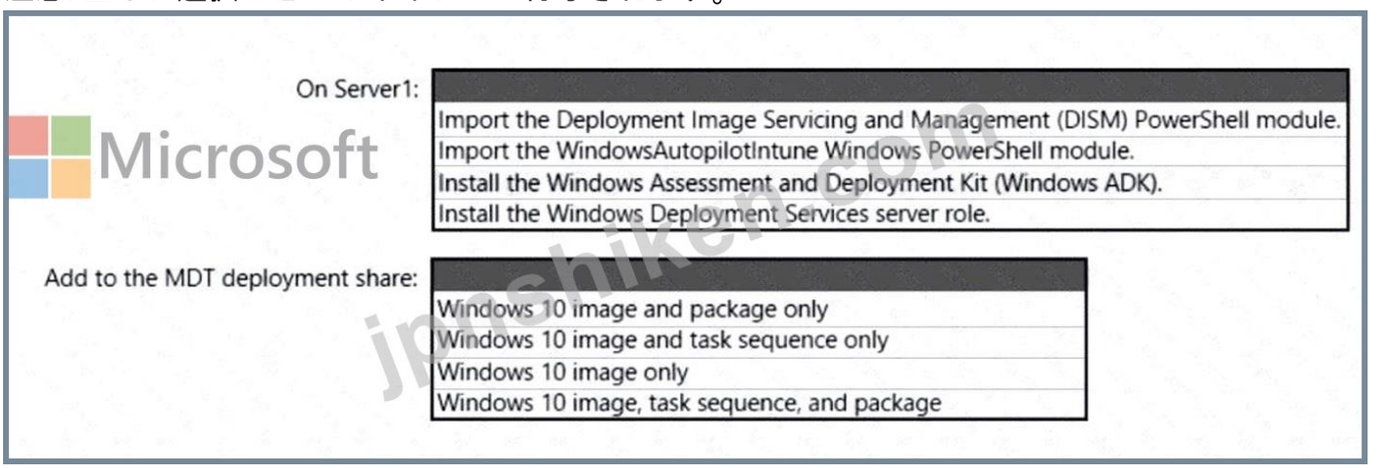
Server1 という名前のサーバーと、Windows 8.1 を実行するコンピューターがあります。Server1 には、Microsoft Deployment Toolkit (MDT) がインストールされています。

MDT 展開ウィザードを使用して、Windows 8.1 コンピューターを Windows 10 にアップグレードする予定です。

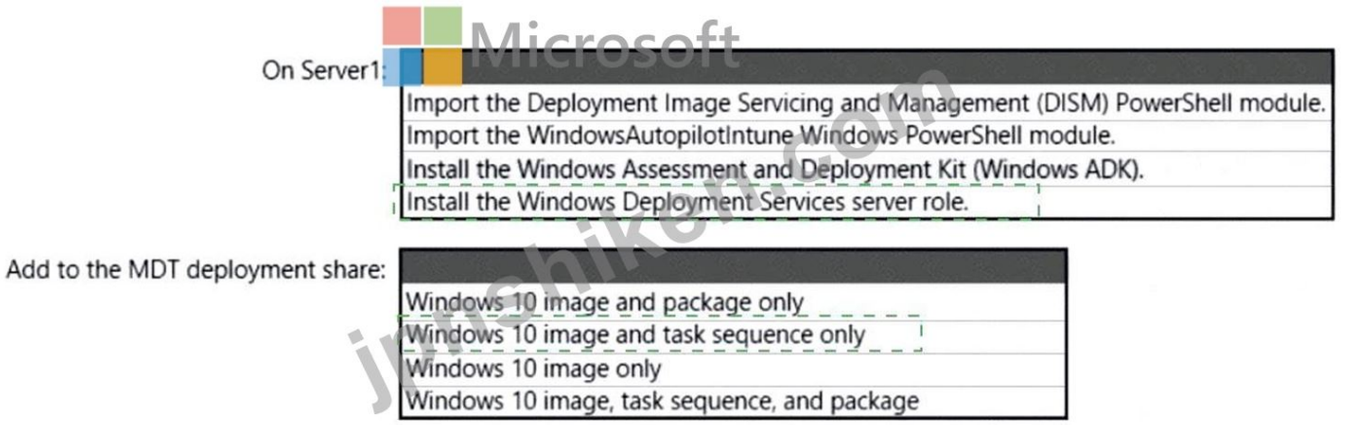
Server1 に展開共有を作成する必要があります。

Server1 で何を行う必要がありますか? また、MDT 展開共有に追加する必要がある最小限のコンポーネントは何ですか? 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。



正解:



Explanation:

Box 1: Install the Windows Deployment Services role.

Install and initialize Windows Deployment Services (WDS)

On the server:

Open an elevated Windows PowerShell prompt and enter the following command:

Install-WindowsFeature -Name WDS -IncludeManagementTools

WDSUTIL /Verbose /Progress /Initialize-Server /Server:MDT01 /RemInst:"D:\RemoteInstall"

WDSUTIL /Set-Server /AnswerClients:All Box 2: Windows 10 image and task sequence only Create the reference image task sequence In order to build and capture your Windows 10 reference image for deployment using MDT, you will create a task sequence.

Reference: https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/prepare-for-windows- deployment-with-mdt
https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/create-a-windows-10-reference- image

質問: **20**
Microsoft 365 サブスクリプションがあり、その中に User1 というユーザーと、Microsoft Intune に登録されている 500 台の Windows デバイスが含まれています。
攻撃面の縮小 (ASR) ルールを構成し、そのルールを警告モードで有効にします。
ユーザー1はfile1.exeというファイルをダウンロードします。ユーザー1がfile1.exeを実行しようとすると、コンテンツがブロックされているというメッセージが表示されます。ユーザーはコンテンツのブロックを解除します。
次にユーザーにコンテンツのブロック解除を促すメッセージが表示されるまで、どのくらいの時間がかかりますか?
A. 24時間
B. 1週間
C. 1時間
D. 10分
正解: **A (**コメントを発表する**)**

質問: **21**
会社には、複数の Windows 10 デバイスを含む contoso.com という名前の Azure AD テナントがあります。
新しい Windows 10 デバイスを contoso.com に参加させると、ユーザーは 4 桁の PIN を設定するように求められます。
ユーザーが Windows 10 デバイスを contoso.com に参加させるときに、6 桁の PIN を設定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。
解決策: Microsoft Entra 管理センターから、自動モバイル デバイス管理 (MDM) 登録を構成します。Microsoft Intune 管理センターから、Windows Hello for Business 登録オプションを構成します。
これは目標を満たしていますか?
A. いいえ
B. はい
正解: **(**正解を表示します**)**

質問: **22**
Microsoft 365 E5 サブスクリプションをお持ちです。
Android Enterprise デバイス用の Microsoft Intune 登録プロファイルがあり、次の設定があります。
* 名前: プロフィール1
* トークンの種類: 企業所有、完全管理

プロファイル1を使用して、新しいAndroidデバイスをIntuneに登録する必要があります。デバイスを登録するには何を使用すればよいですか？
A. QRコード
B. Microsoft Authenticate アプリ
C. ポータルサイトアプリ
D. Intune アプリ
正解: **B** (コメントを発表する)

質問: **23**
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
Microsoft Intune を使用して、Windows デバイスを展開および管理します。
会社を辞めたユーザーのデバイスが 100 台あります。
以前のユーザーがインストールしたデータとアプリケーションをすべて削除して、デバイスを新しいユーザー向けに再利用する必要があります。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。
あなたは何をするべきか？
A. 新しい構成プロファイルをデバイスに展開します。
B. デバイスに Windows 11 のクリーン インストールを実行します。
C. デバイスで Windows Autopilot のリセットを実行します。
D. デバイスでインプレース アップグレードを実行します。
正解: (正解を表示します)

質問: **24**
Microsoft 365 E5 サブスクリプションをお持ちです。すべてのデバイスは Microsoft Intune に登録されています。
多要素認証 (MFA) を必要とする Policy! という名前の条件付きアクセス ポリシーを作成します。
ポリシー 1 が非準拠としてマークされたデバイスにのみ適用されるようにする必要があります。ポリシー 1 のどの設定を構成する必要がありますか?
A. 条件に基づいてデバイスをフィルターする
B. セッション
C. 対象リソース
D. グラント
E. 条件下のデバイス プラットフォーム
正解: (正解を表示します)

質問: **25**
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
デバイスを管理するには、Microsoft Intune を使用します。
次の表に示すデバイスがあります。

Name	Operating system	Activation type
Device1	Windows 10 Pro for Workstation	Key
Device2	Windows 11 Pro	Key
Device3	Windows 11 Pro	Subscription

サブスクリプションのアクティベーションを使用して Windows 11 Enterprise に変更できるデバイスはどれですか?

A. デバイス3のみ

B. デバイス2とデバイス3のみ

C. デバイス1とデバイス2のみ

D. デバイス1、デバイス2、デバイス3

正解**: B (**コメントを発表する**)**

https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#subscription- activation-for-enterprise:~:text=For%20versions%20of%20Windows%20newer%20than%20Windows%2010%2C%20an%20upgrade%20to%20Windows%2010%20would%20first%20be%20required%2C%20followed%20by%20upgrading%20to%20the%20version%20of%20Windows%20Enterprise%20newer%20than%20Windows%2010

質問**: 26**

Windows 11 展開タスクの管理に使用される Microsoft Deployment Toolkit (MDT) ソリューションがあります。

MDT には、次の表に示すオペレーティング システム イメージが含まれています。

Name	Description
Image1.wim	Custom-built Windows 11 image that has preinstalled custom apps
Image2.wim	Custom-built Windows 11 image without apps
Install.wim	Default Windows 11 image

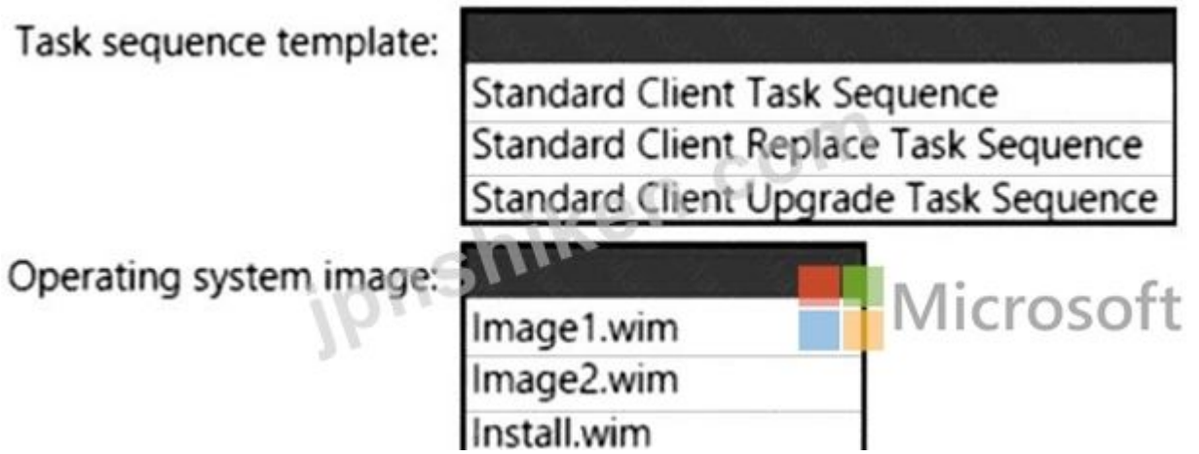
Windows 10 を実行している複数のコンピューターで Windows 11 のインプレース アップグレードを実行する必要があります。

展開ワークベンチから、新しいタスク シーケンス ウィザードを開きます。

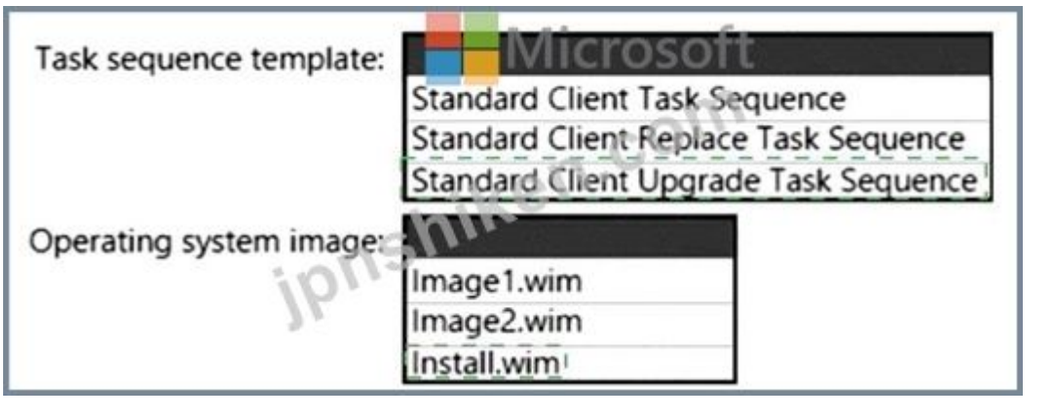
タスク シーケンスに使用するタスク シーケンス テンプレートとオペレーティング システム イメージを特定する必要があります。ソリューションでは、管理作業を最小限に抑える必要があります。

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。



正解:



Explanation:

Box 1: Standard Client Upgrade Task Sequence

Use Template: Standard Client Upgrade Task Sequence

In-place upgrade is the preferred method to use when migrating from Windows 10 to a later release of Windows 10, and is also a preferred method for upgrading from Windows 7 or 8.1 if you do not plan to significantly change the device's configuration or applications. MDT includes an in-place upgrade task sequence template that makes the process really simple.

Box 2: Install.wim

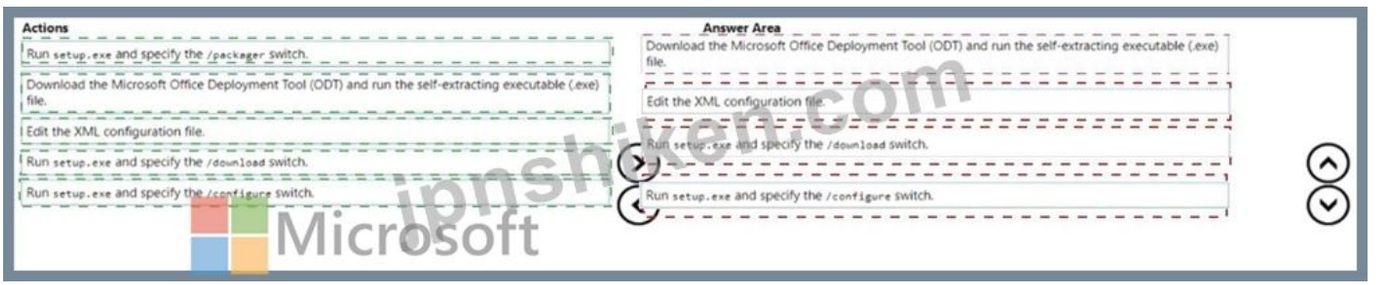
In-place upgrade differs from computer refresh in that you cannot use a custom image to perform the in-place upgrade. I Reference: https://docs.microsoft.com/en-us/windows/deployment/deploy-windows-mdt/upgrade-to-windows-
10-with-the-microsoft-deployment-toolkit

質問: **27**

Microsoft 365 E5 サブスクリプションと、Windows 11 を実行するコンピューターを所有しています。

Microsoft 365 Apps for enterprise のカスタマイズされたインストールを作成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、コマンドレットのリストから適切なコマンドレットを回答領域に移動し、正しい順序で並べます。

正解**:**



Explanation:

1. Download ODT application
2. Create a configuration file (XML)
3. setup.exe /download to download the installation files
4. setup.exe /configure to deploy the application

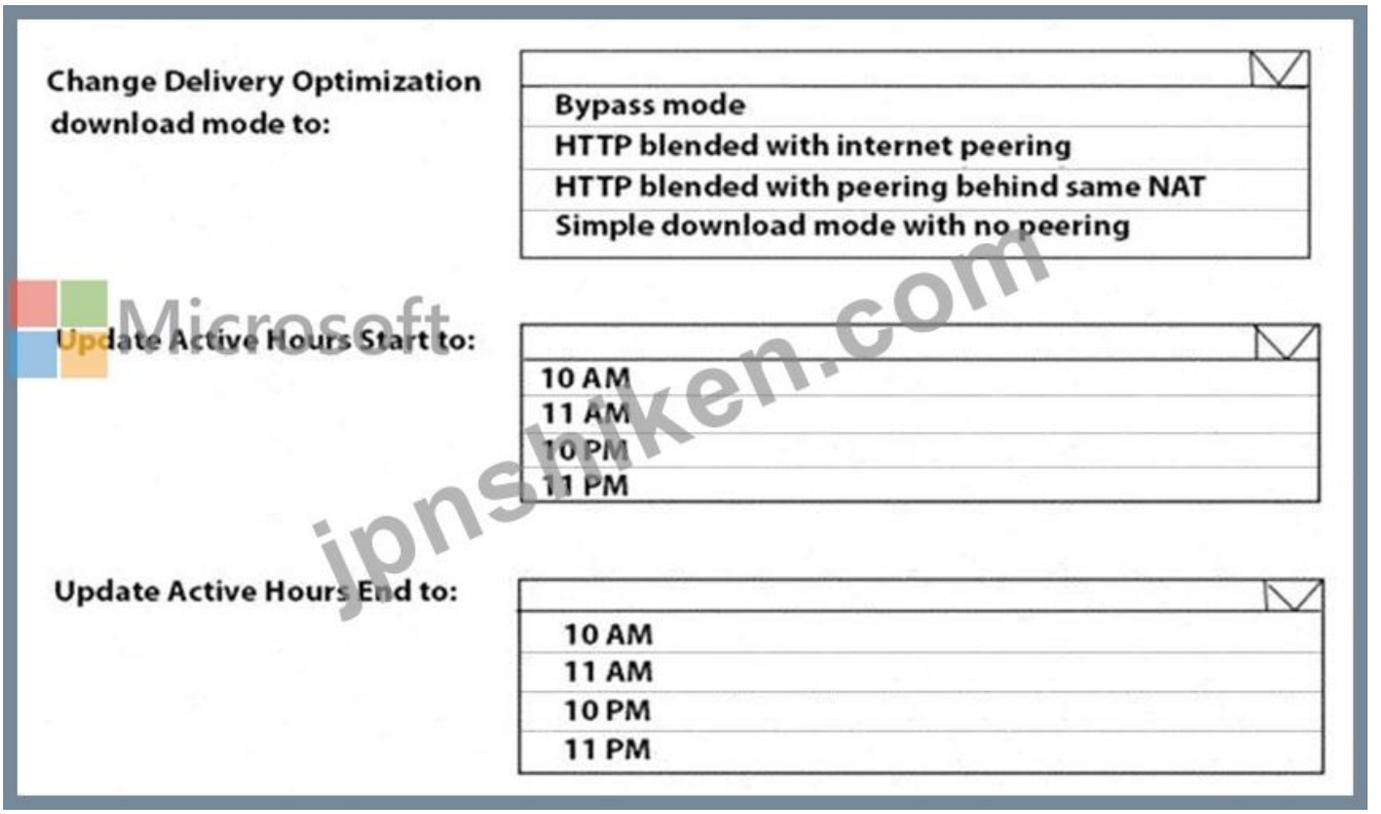
https://learn.microsoft.com/en-us/deployoffice/deploy-microsoft-365-apps-local-source

質問**: 28**

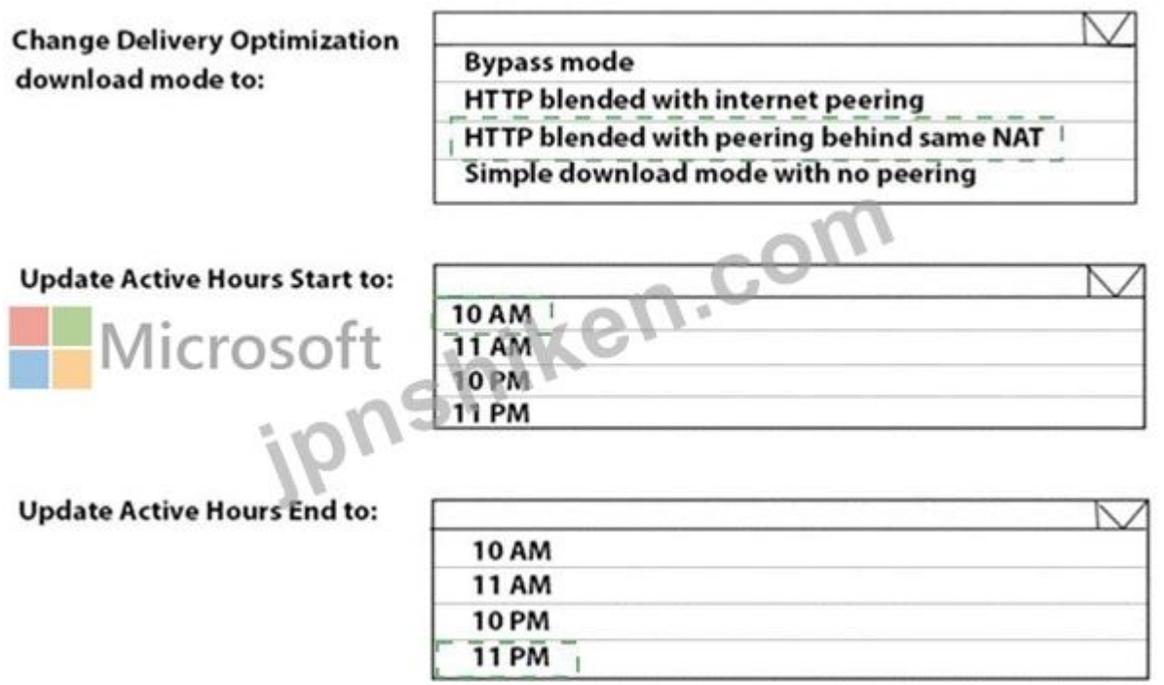
ロサンゼルス オフィスのパフォーマンス問題を解決する必要があります。

更新設定をどのように構成すればよいですか? 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。

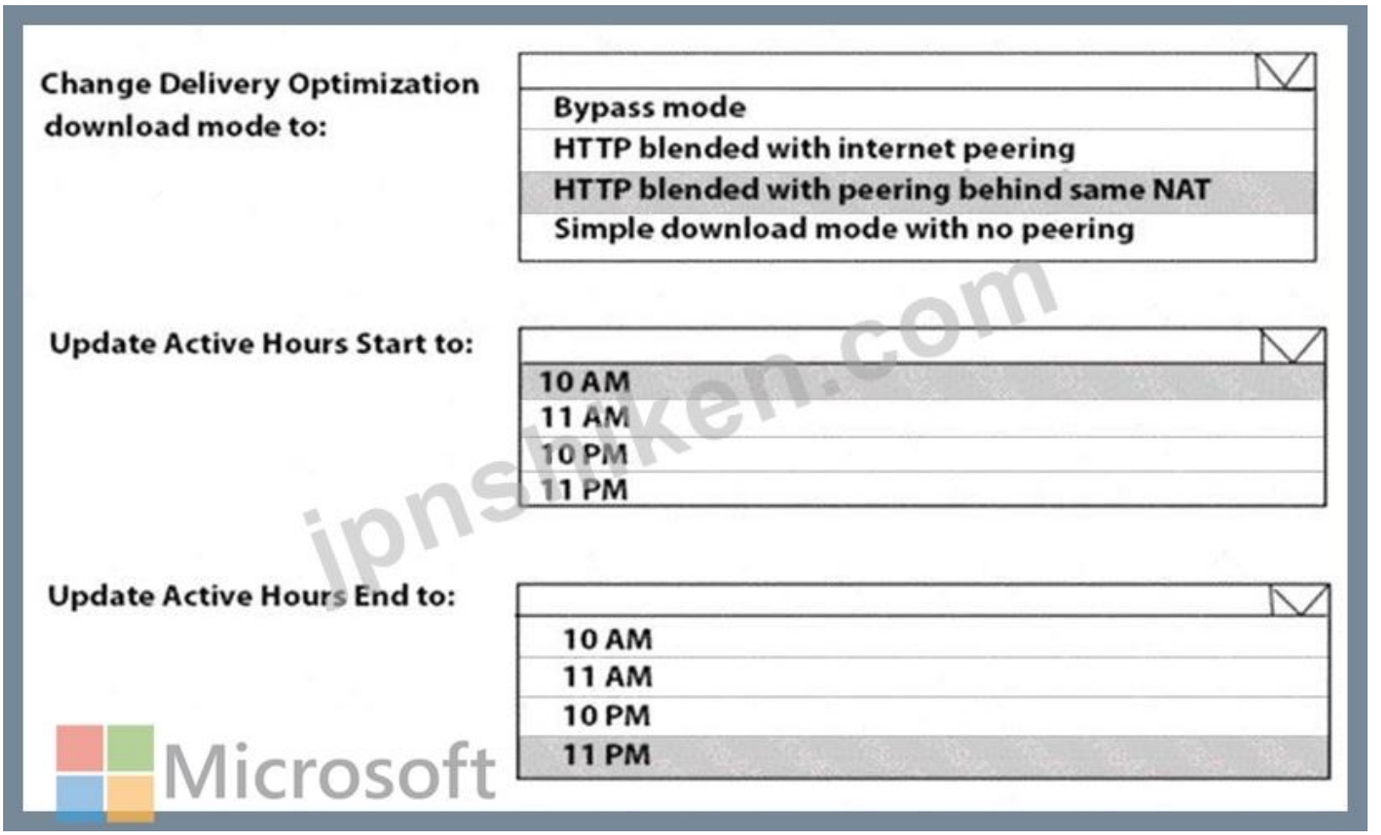
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:

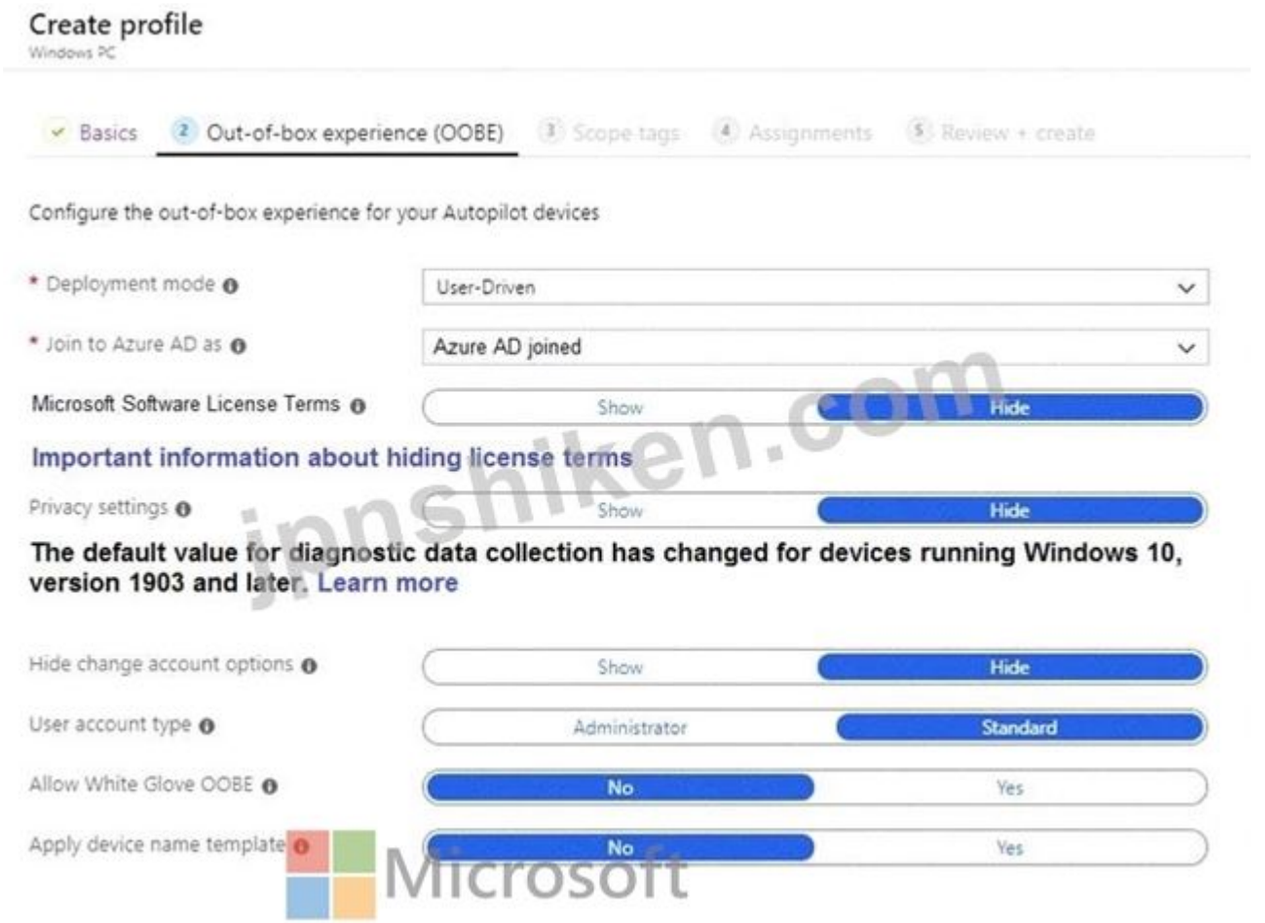


Reference:
https://docs.microsoft.com/en-us/windows/deployment/update/waas-delivery-optimization
https://2pintsoftware.com/delivery-optimization-dl-mode/

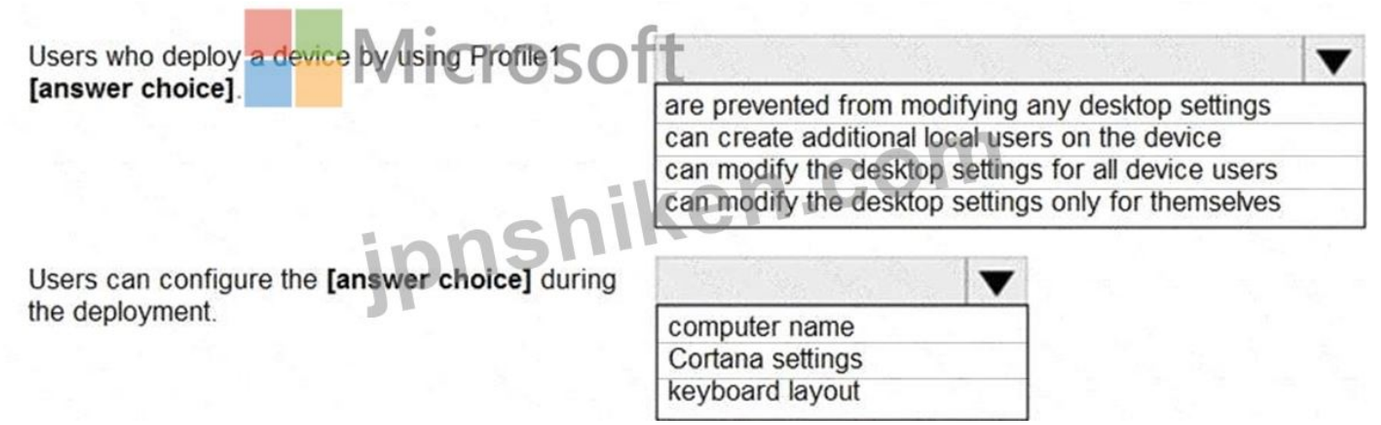
質問: **29**
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
デバイスを管理するには、Microsoft Intune を使用します。
Intune に登録されている Device1 という名前の Windows 11 デバイスがあります。Device1 は 30 日間オフラインになっています。
Device1 を Intune から直ちに削除する必要があります。ソリューションでは、デバイスが再度チェックインしたときに、Intune によってプロビジョニングされたアプリとデータがすべて削除されるようにする必要があります。ユーザーがインストールしたアプリ、個人データ、および OEM がインストールしたアプリは保持する必要があります。
何を使うべきでしょうか?
A. 削除アクション
B. 退却アクション
C. フレッシュスタートアクション
D. オートパイロットリセットアクション
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe#delete-devices-from-the-intune- admin-center

質問: **30**

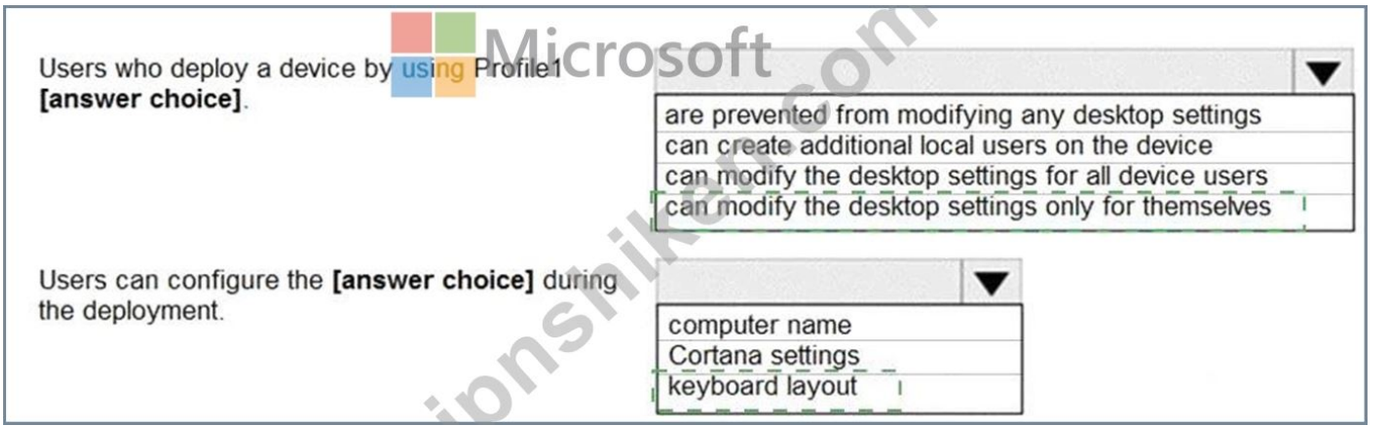
Microsoft Intune サブスクリプションをお持ちです。
次の図に示すように、Profile1 という名前の Windows Autopilot 展開プロファイルを作成しています。



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。



正解:



Explanation:

Can modify the desktop settings only for themselves

Keyboard Layout

質問: **31**

次の表に示すデバイスを含む Microsoft Entra テナントがあります。

Name	Platform	Join type	Microsoft Intune
Device1	Windows 11	Microsoft Entra joined	Enrolled
Device2	Windows 11	Microsoft Entra joined	Not enrolled
Device3	Windows 11	Microsoft Entra registered	Enrolled
Device4	Android	Microsoft Entra registered	Enrolled

エンドポイント権限管理 (EPM) を実装できるデバイスはどれですか?

A. デバイス1とデバイス3のみ

B. デバイス1、デバイス2、デバイス3、デバイス4

C. デバイス1のみ

D. デバイス1とデバイス2のみ

E. デバイス1、デバイス3、デバイス4のみ

正解: **C** (コメントを発表する)

質問: **32**

次の表に示すオブジェクトを含む Microsoft 365 テナントがあります。

Name	Type
Admin1	User
Group1	Microsoft 365 group
Group2	Distribution group
Group3	Mail-enabled security group
Group4	Security group

Microsoft Intune 管理センターで、App1 という名前の Microsoft 365 アプリ アプリを作成しています。App1 をどのオブジェクトに割り当てることができますか?

A. グループ3とグループ4のみ

B. Admin1、Group3、Group4のみ

C. グループ1、グループ3、グループ4のみ

D. グループ1、グループ2、グループ3、グループ4のみ

E. Admin1、Group1、Group2、Group3、Group4

正解: **(**正解を表示します**)**

In the Microsoft Intune admin center, you can assign apps to users or devices. Users can be assigned to apps by using user groups or individual user accounts. Devices can be assigned to apps by using device groups. In this scenario, the objects shown in the table are as follows:

Admin1 is an individual user account that belongs to the Global administrators role group.

Group1 is a user group that contains 100 users.

Group2 is a device group that contains 50 devices.

Group3 is a user group that contains 200 users.

Group4 is a device group that contains 150 devices.

Since App1 is a Microsoft 365 Apps app, it can only be assigned to users, not devices. Therefore, Group2 and Group4 are not valid objects for app assignment. Admin1 is also not a valid object for app assignment, because individual user accounts can only be used for testing purposes, not for production deployment.

Therefore, the only valid objects for app assignment are Group1 and Group3, which are user groups.

質問: **33**

Windows 10 を実行する Computer1 と Computed という 2 台のコンピューターがあります。

Computed ではリモート デスクトップが有効になっています。

コンピュータ 1 から、リモート デスクトップ接続を使用してコンピュータ 2 に接続します。

リモート デスクトップ セッション内から Computer1 のローカル ドライブにアクセスできることを確認する必要があります。

何をすべきでしょうか?

A. コンピュータ 2 の Windows Defender ファイアウォールから、ファイルとプリンターの共有を許可します。

B. コンピュータ 2 から、リモート デスクトップ設定を構成します。

C. コンピューター 1 の Windows Defender ファイアウォールから、リモート デスクトップを許可します。
D. Computer1 から、リモート デスクトップ接続の設定を構成します。
正解: **(**正解を表示します**)**

質問: **34**
contoso.com という名前の Azure AD テナントがあります。
Windows Autopilot を使用して、次の表に示す Windows 10 デバイスを構成する予定です。

Name	Memory	TPM
Device1	16 GB	None
Device2	8 GB	Version 1.2
Device3	4 GB	Version 2.0

Windows Autopilot 自己展開モードを使用して構成できるデバイスはどれですか?
A. デバイス2のみ
B. デバイス3のみ
C. デバイス2とデバイス3のみ
D. デバイス 1、デバイス 2、デバイス 3
正解: **(**正解を表示します**)**
Windows Autopilot self-deploying mode requires devices that have a firmware-embedded activation key for Windows 10 Pro or Windows 11 Pro. This feature allows devices to automatically activate Windows Enterprise edition using the subscription license assigned to the user. Device1 does not have a firmware- embedded activation key, so it cannot use self-deploying mode. Device2 and Device3 have firmware- embedded activation keys for Windows 10 Pro, so they can use self-deploying mode. References: Windows Autopilot self-deploying mode (Public Preview), Deploy Windows Enterprise licenses

質問: **35**
Microsoft Intune に登録されている Computer1 という名前の Windows 10 デバイスがあります。
Computer1 を、顧客向けのフルスクリーン アプリケーションを 1 つ実行するパブリック ワークステーションとして構成する必要があります。
Microsoft Intune 管理センターではどの構成プロファイル タイプのテンプレートを使用する必要がありますか?
A. キオスク
B. マルチユーザー共有デバイス
C. デバイスの制限
D. エンドポイント保護
正解: **(**正解を表示します**)**

質問: **36**
Microsoft 365 サブスクリプションをお持ちです。

次の種類のデバイスに対して Microsoft Intune 登録を有効にする予定です。
* 構成マネージャーを使用して管理されている既存の Windows 11 デバイス
* 個人のiOSデバイス
ソリューションでは、ユーザーの混乱を最小限に抑える必要があります。
各デバイス タイプにはどの登録方法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。

正解:

Explanation:
https://learn.microsoft.com/en-us/mem/configmgr/comanage/overview
for co-management
https://learn.microsoft.com/en-us/mem/intune/enrollment/ios-user-enrollment-supported-actions iOS user enrollment for BYOD

質問: **37**
注: このセクションには、同じシナリオと問題を扱う1つ以上の質問セットが含まれています。各質問は、問題に対する独自の解決策を提示します。その解決策が、定められた目標を満たしているかどうかを判断してください。
セット内の複数の解決策が問題を解決できる可能性があります。また、セット内のどの解決策も問題を解決できない可能性もあります。
このセクションの質問に回答した後は、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。
contoso.com という名前の Microsoft Entra テナントがあります。

Devtce1 という名前の Android デバイスを購入します。
Devtce1 を contoso.com に登録する必要があります。
解決策: Google Chrome アプリを使用します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解**: (**正解を表示します**)**

質問**: 38**
Microsoft Intune が含まれる Microsoft 365 サブスクリプションをお持ちです。
次の設定を含む UpdateRing1 という名前の更新リングがあります。
* 自動更新動作: スケジュールされた時間に自動的にインストールして再起動します
* 自動行動頻度: 月の最初の週
* 設置予定日：火曜日
* 予定インストール時間: 午前3時
Microsoft Intone管理センターで、UpdateRing1の機能更新プログラムの「アンインストール」を選択します。デバイスからの機能更新プログラムの削除はいつ開始されますか？
A. 翌月の第1火曜日
B. ポリシーを受け取ったらすぐに
C. 来週の火曜日
D. ユーザーがアンインストールを承認したとき
正解**: (**正解を表示します**)**

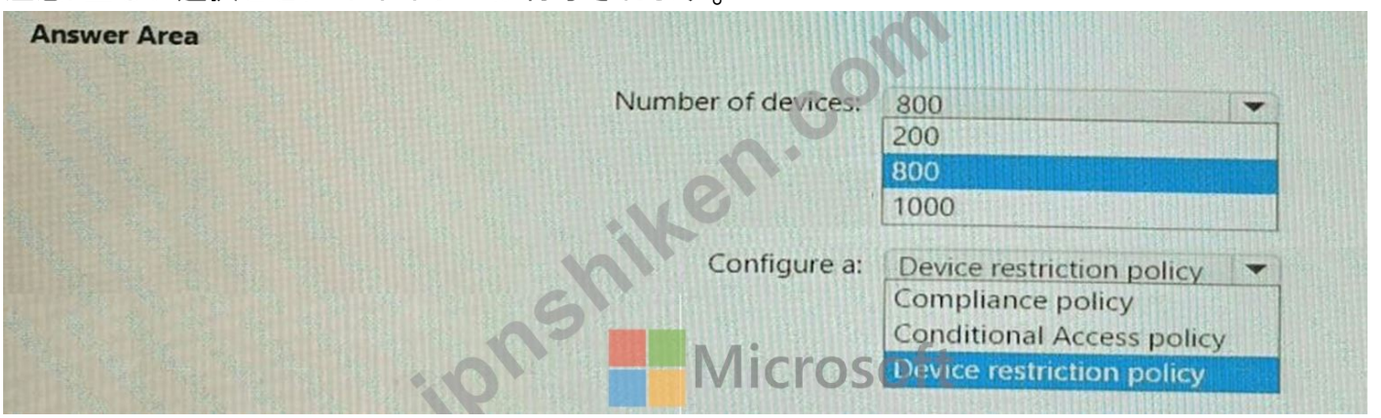
質問**: 39**
Windows 365 Enterprise ライセンスを持つ Microsoft 365 サブスクリプションをお持ちです。
クラウド PC のテンプレートとしてカスタム Windows 11 イメージを使用する予定です。
Windows 11 を実行し、次の構成を持つ Hyper-V 仮想マシンがあります。
* 名前: VM1
* ディスクサイズ: 64 GB
* ディスクフォーマット: VHDX
* ディスクタイプ: 固定サイズ
* 世代: 第2世代
VM1 をカスタム イメージのソースとして使用できることを確認する必要があります。まず VM1 で何を行う必要がありますか?
A. ディスクフォーマットをVHDに変更する
B. ディスクタイプを動的拡張に変更します
C. 世代を第 1 世代に変更します。
D. ディスクサイズを増やします。
正解**: (**正解を表示します**)**

質問: **40**
contoso.com という名前の Azure AD テナントがあります。
Windows 11 を実行するコンピューターを 25 台購入する予定です。コンピューターをユーザーに直接配送する予定です。
すぐに使用できる環境 (OBE) 中に、ユーザーにサインインを求めるメッセージが表示され、コンピューターが Microsoft Intune を使用するように構成されていることを確認する必要があります。
どの 2 つのコンポーネントを構成する必要がありますか? それぞれの正解はソリューションの一部を示します。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. プロビジョニング パッケージ
B. 自動登録
C. unattend.xml 応答ファイル
D. 自己展開モード用の Windows Autopilot 展開プロファイル
E. ユーザー主導モード用の Windows Autopilot 展開プロファイル
正解: **(**正解を表示します**)**
Self-deploying mode doesn't presently associate a user with the device (since no user ID or password is specified as part of the process).
Ref: https://learn.microsoft.com/en-us/autopilot/self-deploying#:~:text=Self%2Ddeploying%20mode%
20doesn%27t%20presently%20associate%20a%20user%20with%20the%20device%20(since%20no%
20user%20ID%20or%20password%20is%20specified%20as%20part%20of%20the%20process).
Windows Autopilot user-driven mode
Ref: https://learn.microsoft.com/en-us/autopilot/user-driven#:~:text=Specify%20your%20e%2Dmail%20address%20and%20password%20for%20your%20organization%20account.

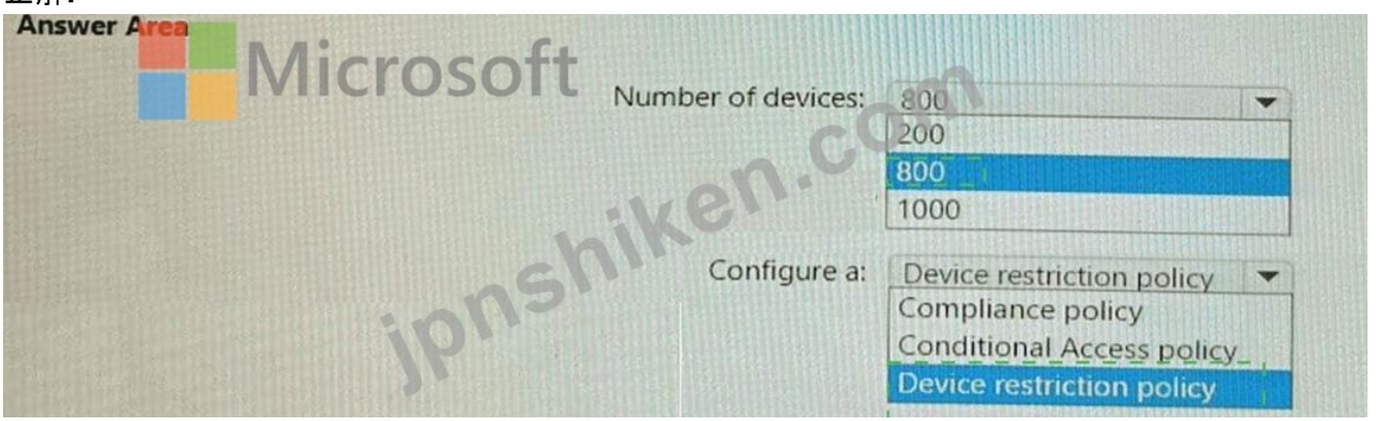
質問: **41**
会社では、すべてのユーザーに対して Windows 10 Enterprise を標準化しています。
ユーザーの中には、小売店から自分のコンピューターを購入している人もいます。コンピューターでは Windows 10 Pro が稼働しています。
コンピューターを Windows 10 Enterprise にアップグレードし、コンピューターを Azure AD に参加させ、いくつかの Microsoft Store アプリをインストールするためのソリューションを推奨する必要があります。ソリューションは、次の要件を満たす必要があります。
* ユーザーがインストールしたアプリケーションが保持されていることを確認します。
* ユーザーの介入を最小限に抑えます。
目標を達成するための最善の推奨事項は何ですか?
複数の回答を選択することで目標を達成できる場合があります。
最も適切な回答を選択してください。
A. Windows オートパイロット
B. Windows 展開サービス (WDS)

C. Windows 構成デザイナーのプロビジョニング パッケージ
D. Microsoft 展開ツールキット (MDT)
正解: **(**正解を表示します**)**

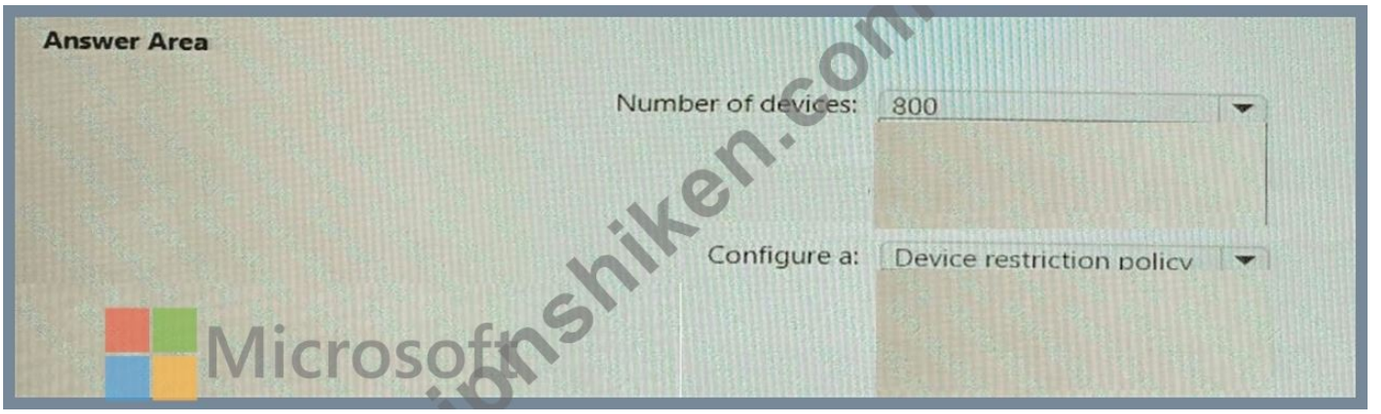
質問: **42**
1,000 台の iOS デバイスを含む Microsoft 365 サブスクリプションがあります。デバイスは次のように Microsoft Intune に登録されています。
* Intune ポータル サイトを使用して 200 台のデバイスが登録されています。
* Apple Automated Device Enrollment (ADE) を使用して 800 台のデバイスが登録されています。
iOS/iPadOS 15.5 をインストールするように構成された、ポリシー 1 という名前の iOS/iPadOS ソフトウェア更新ポリシーを作成します。
Policy1 では何台の iOS デバイスが更新されますか? また、iOS/iPadOS 15.5 のみが確実にインストールされるようにするには、何を構成する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



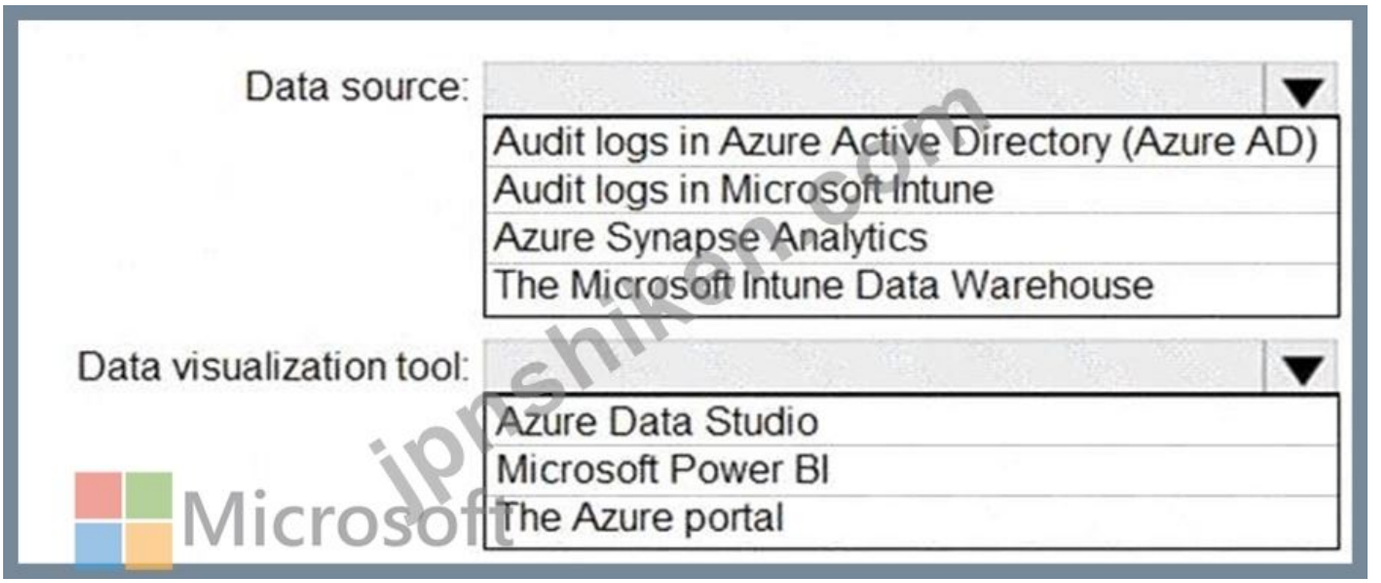
Explanation:



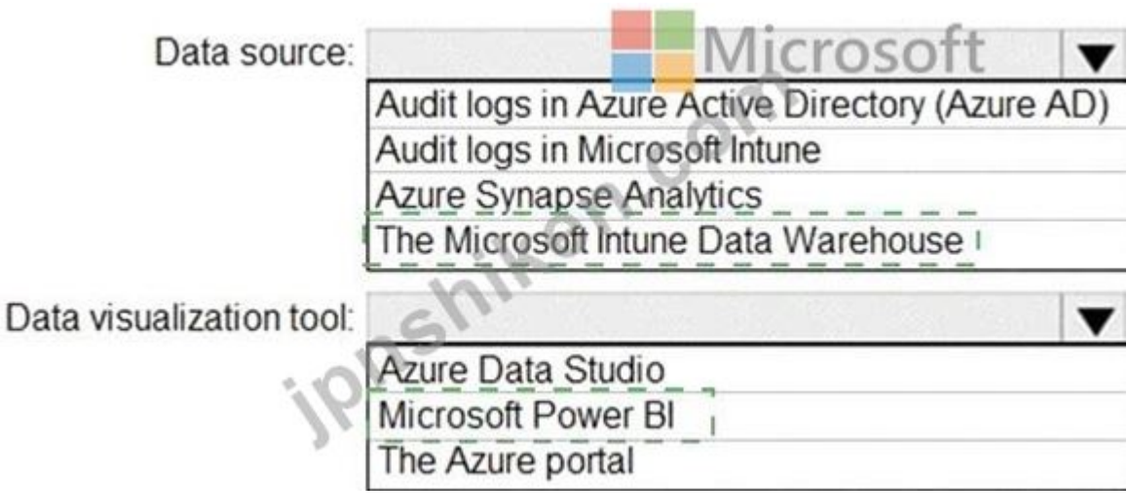
Policy 1 will update 800 iOS devices that are enrolled by using Apple Automated Device Enrollment (ADE). This is because ADE devices are supervised devices that support software update policies in Intune1. Devices that are enrolled by using the Intune Company Portal are not supervised devices and do not support software update policies2.
To ensure that only iOS/iPadOS 15.5 is installed, you should configure a device restriction policy that restricts visibility of software updates. This will prevent users from manually updating the OS to a newer version than the one you specified in Policy 11. You can use the Deployment Workbench to create and assign a device restriction profile to your ADE devices3.

質問: **43**
Microsoft Intune に登録されているデバイスを含む Microsoft 365 E5 サブスクリプションがあります。
デバイス クエリを使用して、デバイスの状態に関するオンデマンド情報を提供する予定です。ソリューションではコストを最小限に抑える必要があります。まず何をすべきでしょうか。
A. 診断情報の収集リモート アクションを使用します。
B. Intune Suite アドオンを購入します。
C. デバイスをエンドポイント分析にオンボードします。
D. Intune Advanced Analytics アドオンを購入します。
正解: **(**正解を表示します**)**

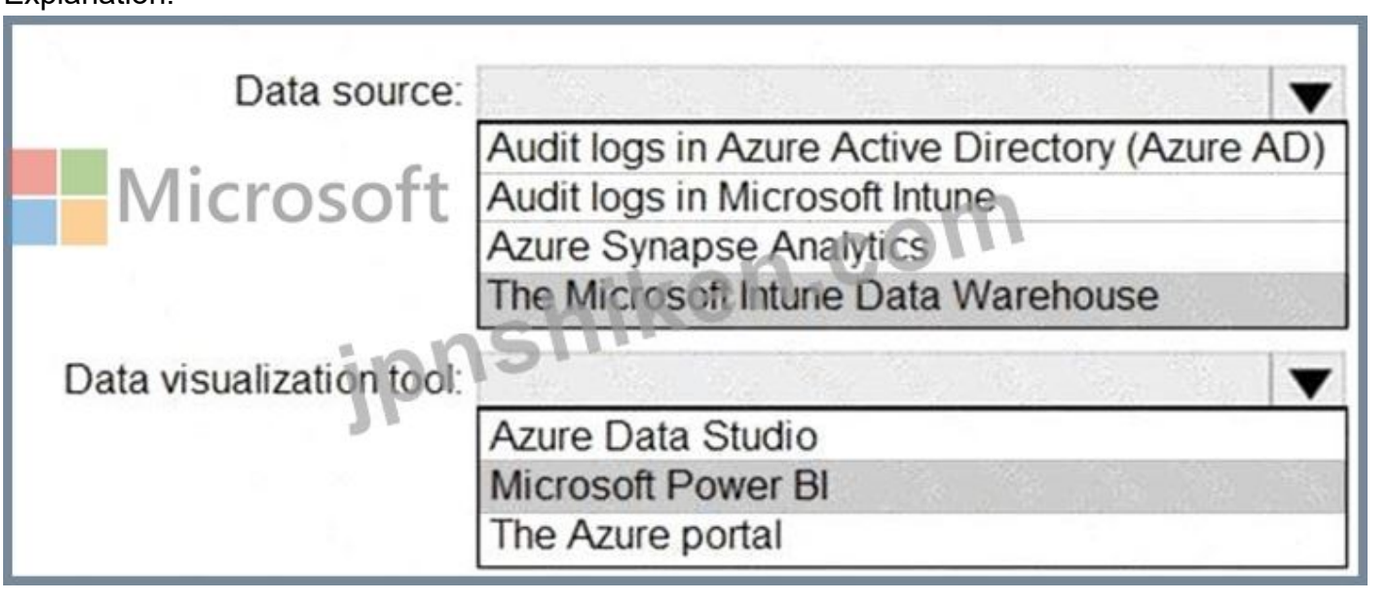
質問: **44**
Windows 10 デバイスを管理するには、Microsoft Endpoint Manager を使用します。
次のレポートを提供するレポート ソリューションを設計しています。
コンプライアンスポリシーの動向
デバイスとユーザー登録の傾向
モバイルデバイスのアプリとオペレーティングシステムのバージョンの内訳
設計にはデータ ソースとデータ視覚化ツールを推奨する必要があります。
何を推奨しますか? 回答するには、回答エリアで適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference:

https://docs.microsoft.com/en-us/mem/intune/developer/reports-nav-create-intune-reports

https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

質問: **45**

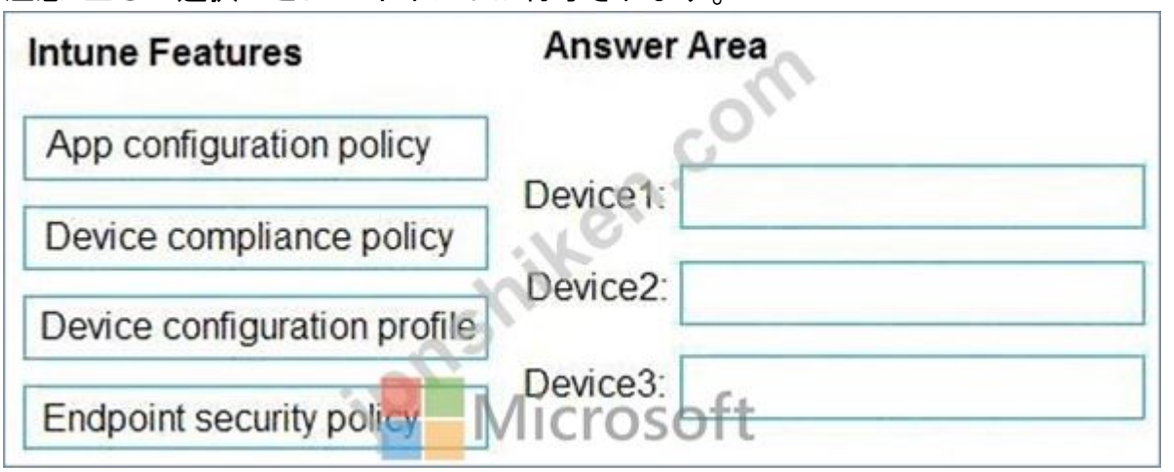
-

次の表に示すデバイスを含む Microsoft 365 サブスクリプションがあります。

各デバイスごとに Microsoft Edge 設定を構成する必要があります。

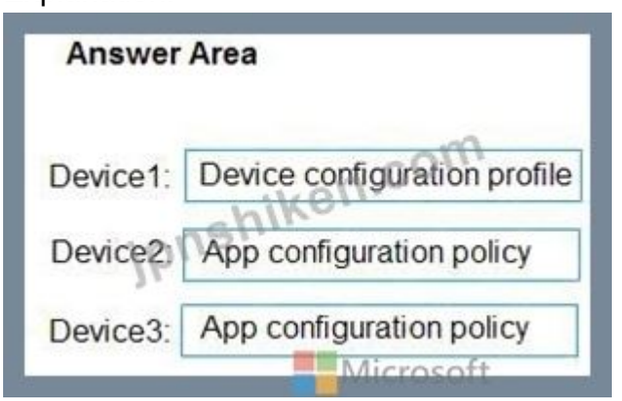
何を使用すればよいでしょうか。答えるには、適切な Intune 機能を正しいデバイスにドラッグします。各機能は、1 回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:



Windows: https://learn.microsoft.com/en-us/deployedge/configure-edge-with-intune#:~:text=You%20can%

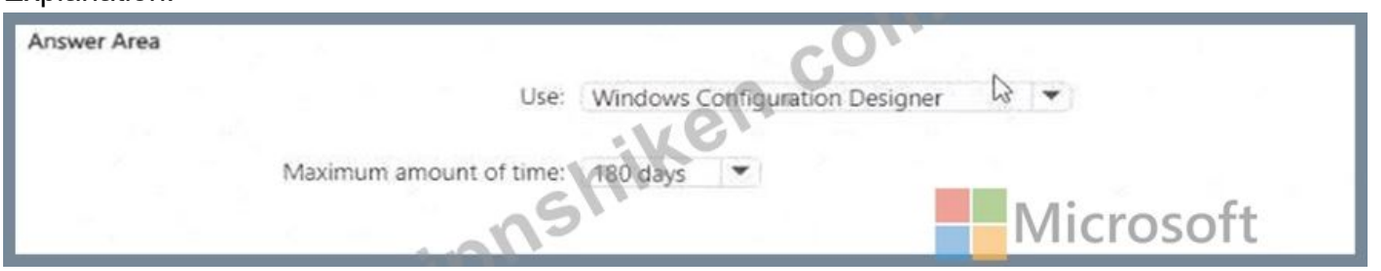
20configure%20Microsoft%20Edge%20policies%20and%20settings%20by%20adding%20a%20device%
20configuration%20profile%20to%20Microsoft%20Intune.
Android: https://developer.android.com/work/managed-configurations
Apple: https://developer.apple.com/library/archive/samplecode/sc2279/Introduction/Intro.html

質問: **46**
Microsoft 365 E5 サブスクリプションをお持ちです。
名前に 「Marketing」という単語が含まれるすべてのデバイスを含む動的デバイス グループを作成する必要があります。どのデバイス メンバーシップ ルールを使用すればよいですか?
A. (device.displayName -in "'Marketing'")
B. (device.displayName -contains "Marketing")
C. (device.displayName -contains "'Marketing'")
D. (device.displayName -in "Marketing")
正解: **(**正解を表示します**)**

質問: **47**
Microsoft 365 E5 サブスクリプションがあり、Microsoft Intune を使用しています。
Windows デバイスを 50 台購入します。
Microsoft Entra に参加しているデバイスの Intune への自動登録を構成します。
デバイスを Microsoft Entra に参加させるには、プロビジョニング パッケージを使用する必要があります。
プロビジョニング パッケージを作成するには何を使用すればよいですか。また、一括登録にパッケージを使用できる最大時間はどれくらいですか。回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:



質問: **48**

Microsoft 365 サブスクリプションをお持ちです。すべてのデバイスで Windows 10 が実行されます。

ユーザーが Windows Insider プログラムにデバイスを登録できないようにする必要があります。

Microsoft Intune 管理センターから実行する必要がある 2 つの構成は何ですか? それぞれの正解は完全なソリューションです。

注意: 正しい選択ごとに 1 ポイントが付与されます。

A. Windows 10 以降のセキュリティ ベースライン

B. アプリ構成ポリシー

C. Windows 10 以降の更新リング

D. デバイス制限デバイス構成プロファイル

E. カスタムデバイス構成プロファイル
正解**: (**正解を表示します**)**

質問**: 49**
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。
会社には、複数の Windows 10 デバイスを含む contoso.com という名前の Azure AD テナントがあります。
新しい Windows 10 デバイスを contoso.com に参加させると、ユーザーは 4 桁の PIN を設定するように求められます。
ユーザーが Windows 10 デバイスを contoso.com に参加させるときに、6 桁の PIN を設定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。
解決策: Microsoft Entra 管理センターから、認証方法を構成します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解**: B (**コメントを発表する**)**

質問**: 50**
MKG 部門ユーザーの要件を満たす必要があります。
何をすべきでしょうか?
A. MKG 部門のユーザーに Microsoft Store for Business の購入者ロールを割り当てます。
B. Microsoft Store for Business から App1 の APPX ファイルをダウンロードします。
C. App1をプライベートストアに追加する
D. MKG 部門ユーザーに Microsoft Store for Business の基本購入者ロールを割り当てます。
E. Microsoft Store for Business から App1 を取得します
正解**: (**正解を表示します**)**
References:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store Enable the users in the MKG department to use App1.
The private store is a feature in Microsoft Store for Business and Education that organizations receive during the signup process. When admins add apps to the private store, all employees in the organization can view and download the apps. Your private store is available as a tab in Microsoft Store app, and is usually named for your company or organization. Only apps with online licenses can be added to the private store.
Reference:
https://docs.microsoft.com/en-us/microsoft-store/distribute-apps-from-your-private-store

質問: **51**
共同管理をサポートするように環境を構成する前に、何をアップグレードする必要がありますか?
A. ドメインの機能レベル
B. 構成マネージャー
C. ドメイン コントローラ
D. Windows Server 更新サービス (WSUS)
正解: **B (**コメントを発表する**)**
References:
https://docs.microsoft.com/en-us/sccm/comanage/tutorial-co-manage-clients
Topic 3, Contoso Ltd, Case 2
Overview
Contoso, Ltd, is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
Contoso has the users and computers shown in the following table.

Location	Users	Laptops	Desktop 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

The company has IT, human resources (HR), legal (LEG), marketing (MKG) and finance (FIN) departments.
Contoso uses Microsoft Store for Business and recently purchased a Microsoft 365 subscription.
The company is opening a new branch office in Phoenix. Most of the users in the Phoenix office will work from home.
Existing Environment
The network contains an Active Directory domain named contoso.com that is synced to Microsoft Azure Active Directory (Azure AD).
All member servers run Windows Server 2016. All laptops and desktop computers run Windows 10 Enterprise.
The computers are managed by using Microsoft System Center Configuration Manager. The mobile devices are managed by using Microsoft Intune.
The naming convention for the computers is the department acronym, followed by a hyphen, and then four numbers, for example, FIN-6785. All the computers are joined to the on-premises Active Directory domain.
Each department has an organization unit (OU) that contains a child OU named Computers. Each computer account is in the Computers OU of its respective department.
Intune Configuration

The domain has the users shown in the following table.

Name	Role	Member of
User1	Intune administrator	GroupA
User2	*None*	GroupB

User2 is a device enrollment manager (DEM) in Intune.
The devices enrolled in Intune are shown in the following table.

Name	Platform	Encryption	Member of
Device1	Android	Disabled	Group1
Device2	iOS	Not applicable	Group2, Group3
Device3	Android	Disabled	Group2, Group3
Device4	iOS	Not applicable	Group2

The device compliance policies in Intune are configured as shown in the following table.

Name	Platform	Require encryption	Assigned
Policy1	Android	Not configured	Yes
Policy2	iOS	Not applicable	Yes
Policy3	Android	Require	Yes

The device compliance policies have the assignments shown in the following table:

Name	Include	Exclude
Policy1	Group3	*None*
Policy2	Group2	Group3
Policy3	Group1	*None*

The device limit restrictions in Intune are configured as shown in the following table.

Priority	Name	Device limit	Assigned to
1	Restriction1	15	GroupB
2	Restriction2	10	GroupA
Default	All users	5	All users

Requirements

Planned Changes

Contoso plans to implement the following changes:

Provide new computers to the Phoenix office users. The new computers have Windows 10 Pro preinstalled and were purchased already.

Start using a free Microsoft Store for Business app named App1.

Implement co-management for the computers.

Technical Requirements:

Contoso must meet the following technical requirements:

Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Deploy Windows 10 Enterprise to the computers of the Phoenix office users by using Windows Autopilot.
Monitor the computers in the LEG department by using Windows Analytics.
Create a provisioning package for new computers in the HR department.
Block iOS devices from sending diagnostic and usage telemetry data.
Use the principle of least privilege whenever possible.
Enable the users in the MKG department to use App1.
Pilot co-management for the IT department.

質問: **52**
Phoenix オフィス コンピューターの展開を準備する必要があります。
まず何をすべきでしょうか?
A. 各コンピューターのハードウェア ID 情報を CSV ファイルに抽出し、ビジネス向け Microsoft Store のデバイス設定からファイルをアップロードします。
B. コンピューターを一般化し、Azure ポータルの Azure Active Directory ブレードからモビリティ (MDM および MAM) 設定を構成します。
C. コンピューターを一般化し、Azure ポータルの Azure Active Directory ブレードからデバイス設定を構成します。
D. 各コンピューターのハードウェア ID 情報を XLSX ファイルに抽出し、Microsoft Store for Business のデバイス設定からファイルをアップロードします。
正解: **(**正解を表示します**)**
References:
https://docs.microsoft.com/en-us/microsoft-store/add-profile-to-devices#manage-autopilot-deployment- profiles

質問: **53**
会社所有の Windows デバイス 100 台を交換します。
デバイスを安全に消去して廃止するには、Microsoft Deployment Toolkit (MDT) を使用する必要があります。ソリューションは、次の要件を満たしている必要があります。
* ユーザー状態をバックアップします。
* 管理作業を最小限に抑えます。
どのタスク シーケンス テンプレートを使用する必要がありますか?
A. Litetouch OEM タスク シーケンス
B. 標準クライアント置換タスクシーケンス
C. 標準クライアントタスクシーケンス
D. Sysprep とキャプチャ
正解: **B (**コメントを発表する**)**

質問: **54**

Microsoft Intune を使用し、100 台の Windows 10 デバイスを含む Microsoft 365 サブスクリプションがあります。デバイスで次のアクションを実行するには、Intune 構成プロファイルを作成する必要があります。

* カスタムスタートレイアウトを展開します。
* ローカル管理者アカウントの名前を変更します。

各アクションにはどのプロファイル タイプ テンプレートを使用する必要がありますか? 回答するには、回答で適切なオプションを選択します。注: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

Device Restrictions

Ref: https://www.anoopcnair.com/start-menu-taskbar-custom-layout-intune-cloudpc/#:~:text=%E2%80%9D%20and%20select-,Device%20Restrictions,-.

Endpoint protection -> Local device security options -> Accounts -> Rename Admin Account Ref: https://www.tenable.com/audits/items/CIS_MS_InTune_for_Windows_10_2004_Level_1_v1.0.1.audit:de2d07c913ec5c2b64b23e97adf74c64#:~:text=Note%20This%20recommendation%20can%20also%20be%20set%20using%20the%20Endpoint%20protection%20profile%20using%20Local%20device%20security%20options/Accounts%20settings.

質問: **55**
Phoenix オフィス コンピューターの展開を準備する必要があります。
まず何をすべきでしょうか?
A. コンピューターを一般化し、Azure Active Directory 管理センターからモビリティ (MDM および MAM) 設定を構成します。
B. 各コンピューターのハードウェア ID 情報を CSV ファイルに抽出し、Azure ポータルの Microsoft Intune ブレードからファイルをアップロードします。
C. 各コンピューターのハードウェア ID 情報を XML ファイルに抽出し、ビジネス向け Microsoft Store のデバイス設定からファイルをアップロードします。
D. 各コンピューターのシリアル番号情報を CSV ファイルに抽出し、Azure ポータルの Microsoft Intune ブレードからファイルをアップロードします。
正解: **(**正解を表示します**)**
Reference:
https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/existing-devices

質問: **56**
Microsoft 365 E5 サブスクリプションと、Windows 10 を実行するコンピューターが 100 台あります。
Microsoft Office 展開ツール (ODT) を使用して、Microsoft Office Professional Plus 2019 をコンピューターに展開する必要があります。
ODT のカスタマイズ ファイルを作成するには何を使用すればよいですか?
A. Microsoft Purview コンプライアンス ポータル
B. Microsoft Intune 管理センター
C. Microsoft 365 管理センター
D. Microsoft 365 アプリ管理センター
正解: **(**正解を表示します**)**

質問: **57**
Microsoft Intune に登録されている 100 台の Windows 10 デバイスを含む Microsoft 365 E5 サブスクリプションがあります。
エンドポイント分析を使用する予定です。
ベースライン メトリックを作成する必要があります。
まず何をすべきでしょうか?
A. Azure Monitor ブックを作成します。
B. エンドポイント分析に 10 台のデバイスをオンボードします。
C. Log Analytics ワークスペースを作成します。
D. ベースライン回帰しきい値を変更します。
正解: **(**正解を表示します**)**
Onboarding from the Endpoint analytics portal is required for Intune managed devices.
Reference: https://docs.microsoft.com/en-us/mem/analytics/enroll-intune

質問: **58**
Microsoft 365 E5 サブスクリプションをお持ちです。
Microsoft Intune を使用してすべての Windows 11 デバイスを管理します。
Attack Surface Reduction Rules プロファイルに基づいて Profile1 という名前の攻撃対象領域削減 (ASR) ポリシーを作成し、すべてのデバイスに Profile! を割り当てます。
ユーザーから、Adobe Reader プラグインがブロックされているという報告がありました。
プラグインがブロックされていないことを確認する必要があります。
何をすべきでしょうか?
A. デバイス コンプライアンス ポリシーを作成し、そのポリシーをすべてのデバイスに割り当てます。
B. Profile1 にスコープ タグを追加します。
C. Profile1 でルール除外ごとに ASR のみを設定します。
D. エンドポイント権限管理ポリシーを作成し、そのポリシーをすべてのデバイスに割り当てます。
正解: **C** (コメントを発表する)

質問: **59**
Microsoft 365 サブスクリプションをお持ちです。
アプリ保護ポリシーを使用して、Android デバイス上の企業データを保護します。
Android デバイスから接続するすべてのユーザーが、モバイル アプリケーション管理 (MAM) をサポートするアプリから接続する場合にのみ企業データにアクセスでき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. アプリ構成ポリシー
B. 条件付きアクセスポリシー
C. デバイス構成プロファイル
D. デバイスコンプライアンスポリシー
正解: **B** (コメントを発表する)
https://learn.microsoft.com/en-us/mem/intune/protect/app-based-conditional-access-intune#:~:text=Microsoft%20Intune%20app%20protection%20policies%20work%20with%20Microsoft%20Entra%20Conditional%20Access%20to%20help%20protect%20your%20organizational%20data%20on%20devices%20your%20employees%20use.

質問: **60**
Microsoft 365 E5 サブスクリプションがあり、Microsoft Intune Suite を使用しています。
Intune を使用して修復スクリプト パッケージを実行する予定です。
Microsoft Intune 管理センターで最初に行うべきことは何ですか?
A. Windows エンタープライズ証明書をアップロードします。

B. 派生資格情報の設定を構成します。
C. Windows ライセンス検証を有効にします。
D. プロセッサ構成で Windows 診断データを有効にします。
正解: **(**正解を表示します**)**

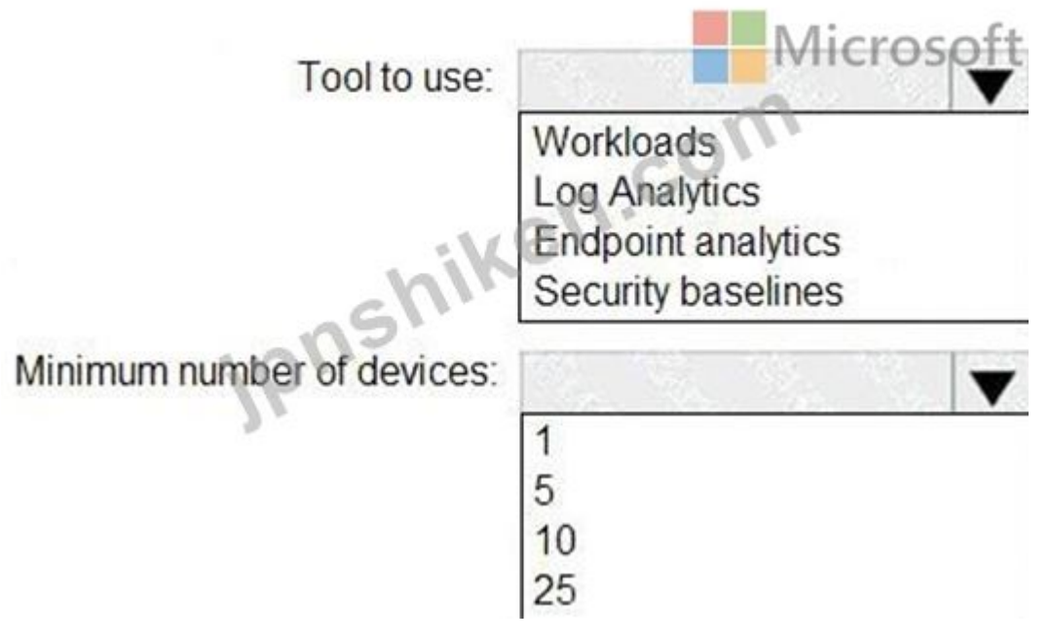
質問: **61**
次の表に示すリソースを含む Microsoft Intune 展開があります。

Name	Type	Platform
Comply1	Device compliance policy	Windows 10 and later
Comply2	Device compliance policy	iOS/iPadOS
CA1	Conditional Access policy	*Not applicable*
Conf1	Device configuration profile	Windows 10 and later
Office1	Office app policy	*Not applicable*

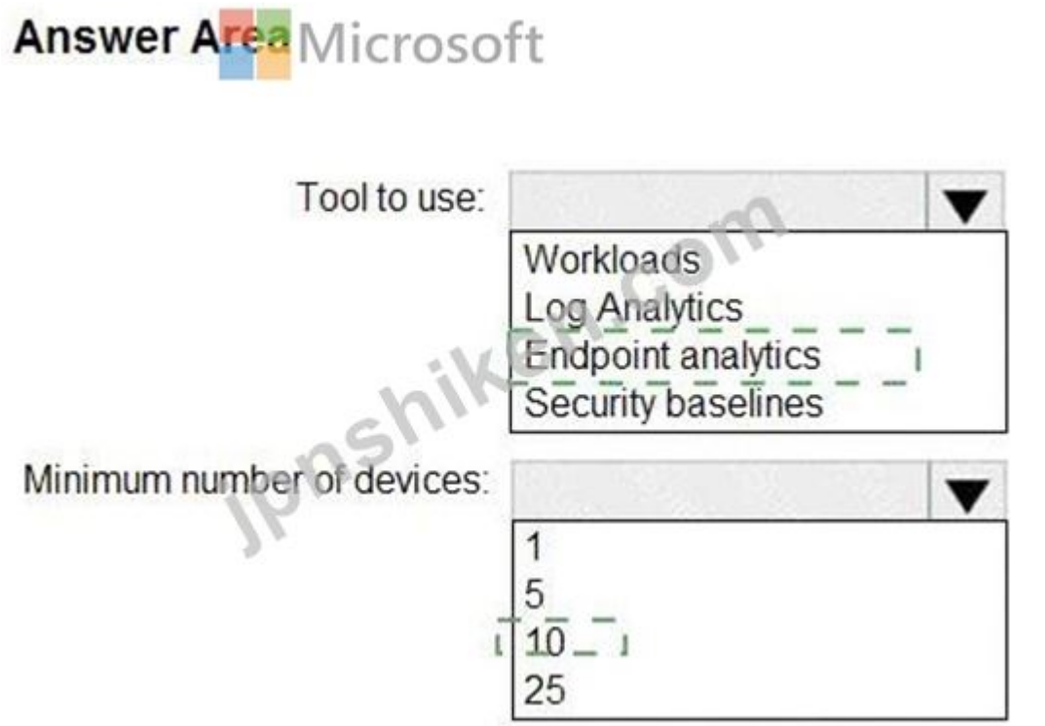
Set1 という名前のポリシー セットを作成し、Comply1 を Set1 に追加します。
Set1 に追加できるリソースは何ですか?
A. CA1. Conf1. および Office 1 のみ
B. 準拠2. CA1、Conf1. および Office1
C. Conf1のみ
D. Comply2のみ
E. Comply2 と Conf1 のみ
正解: **(**正解を表示します**)**

質問: **62**
Microsoft Intune を使用する Microsoft 365 テナントがあります。
Microsoft Intune 管理センターから、登録済みの Windows 10 デバイスのスタートアップ スコアとアプリの信頼性スコアを監視するためのベースラインを作成することを計画します。
ベースラインを作成するために使用するツールと、ベースラインの作成に必要なデバイスの最小数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 Area



正解:



Explanation:
Endpoint Analytics
Minimum 10 devices
(Ref: https://learn.microsoft.com/en-us/mem/analytics/startup-performance#bkmk_report:~:text=The%
20table%20only%20lists%20processes%20that%20affect%20a%20minimum%20of
%2010%20devices%
20in%20your%20tenant.)

質問: **63**

次の表に示すユーザーを含む Azure Active Directory Premium プラン 2 サブスクリプションがあります。

Name	Member of	Assigned license
User1	Group1	Enterprise Mobility + Security E5
User2	Group2	Enterprise Mobility + Security E5

次の表に示すデバイスを購入します。

Name	Type
Device1	Windows 10
Device2	Android

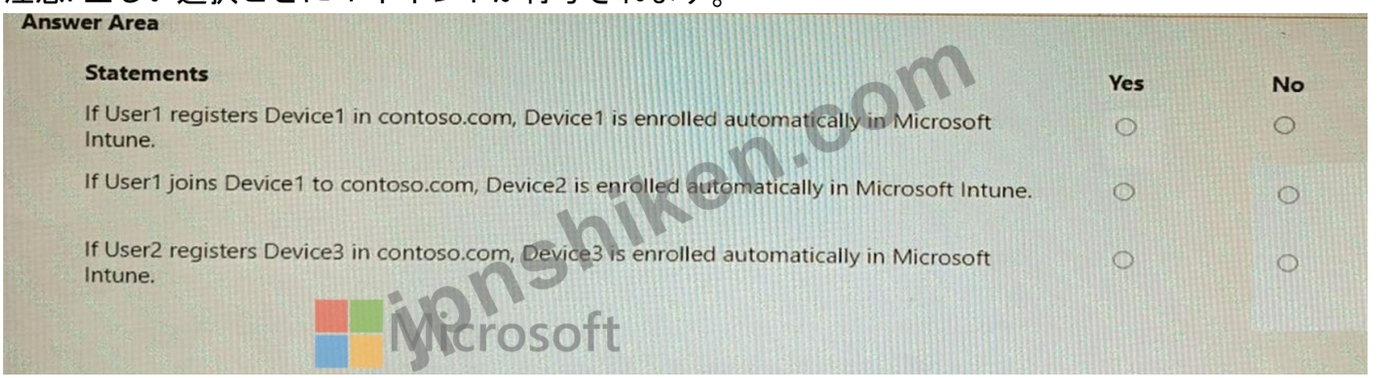
次の設定を使用して、自動モバイル デバイス管理 (MDM) とモバイル アプリケーション管理 (MAM) の登録を構成します。

MDM ユーザー スコープ: グループ 1

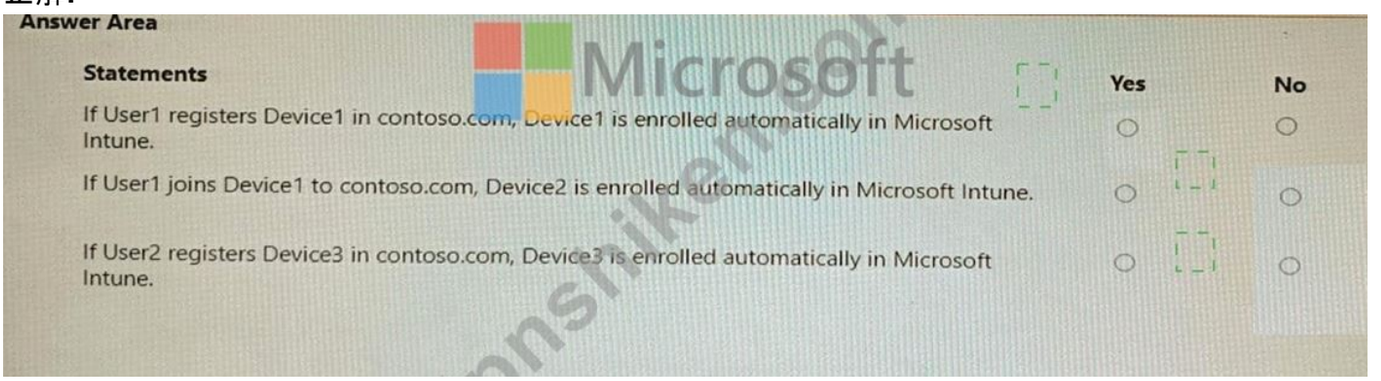
MAM ユーザー スコープ: グループ 2

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。

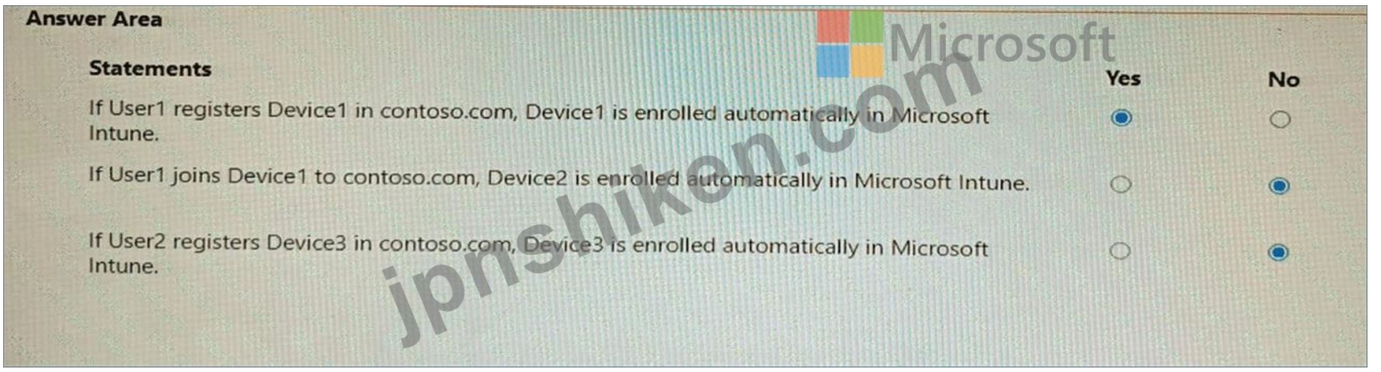
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll
https://powerautomate.microsoft.com/fr-fr/blog/mam-flow-mobile/

質問: **64**
次の表に示すデバイスを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Platform	Join type
Device1	Windows 11	Microsoft Entra registered
Device2	Windows 11	Microsoft Entra joined
Device3	Android	Microsoft Entra registered
Device4	iOS	Microsoft Entra registered

すべてのデバイスが Microsoft Intune に登録され、Microsoft 365 Apps for enterprise がインストールされています。Microsoft 365 のクラウド ポリシー サービスを使用して Microsoft 365 Apps for enterprise を管理できるデバイスはどれですか?
A. デバイス1とデバイス2のみ
B. デバイス1、デバイス2、デバイス3のみ
C. デバイス1、デバイス2、デバイス4のみ
D. デバイス1、デバイス2、デバイス3、およびデバイス4
E. デバイス1のみ
正解: **(正解を表示します)**

質問: **65**
Microsoft Entra テナントがあります。
Group1 という名前の動的デバイス グループを作成しています。
Group1 には、Microsoft Entra に登録されている Windows デバイスのみが含まれます。
Group1 の動的メンバーシップ ルールをどのように構成すればよいですか? 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。

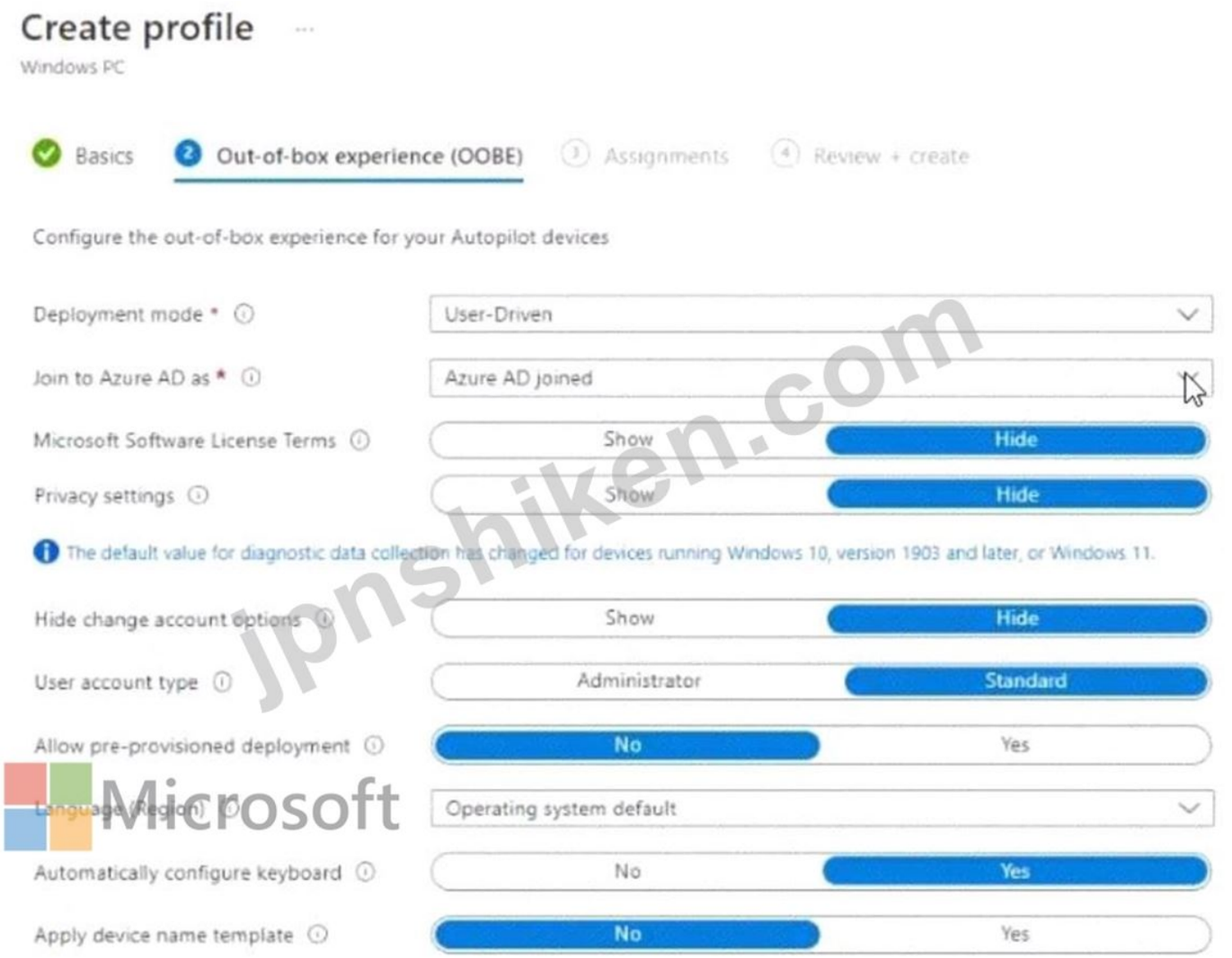
正解:

Explanation:

質問: **66**

ハイブリッド Azure AD テナントがあります。

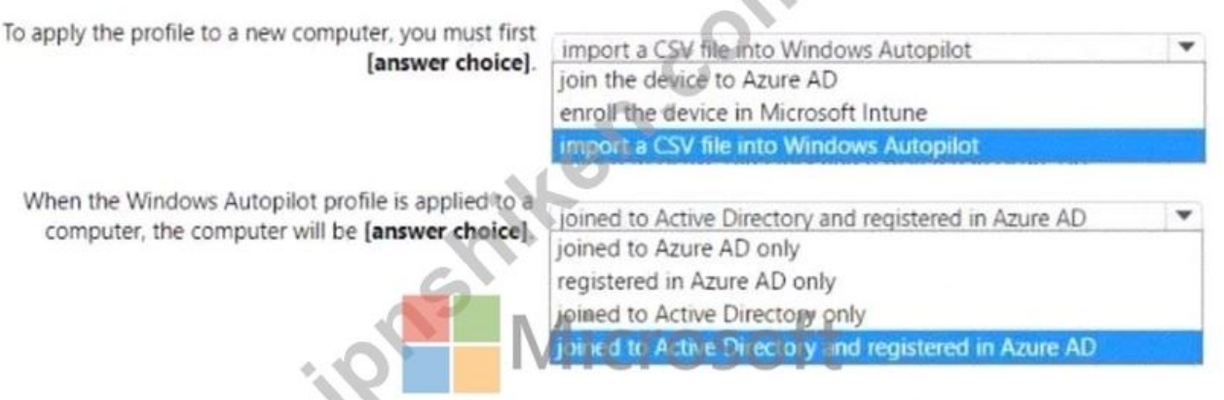
次の図に示すように、Windows Autopilot 展開プロファイルを構成します。



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。

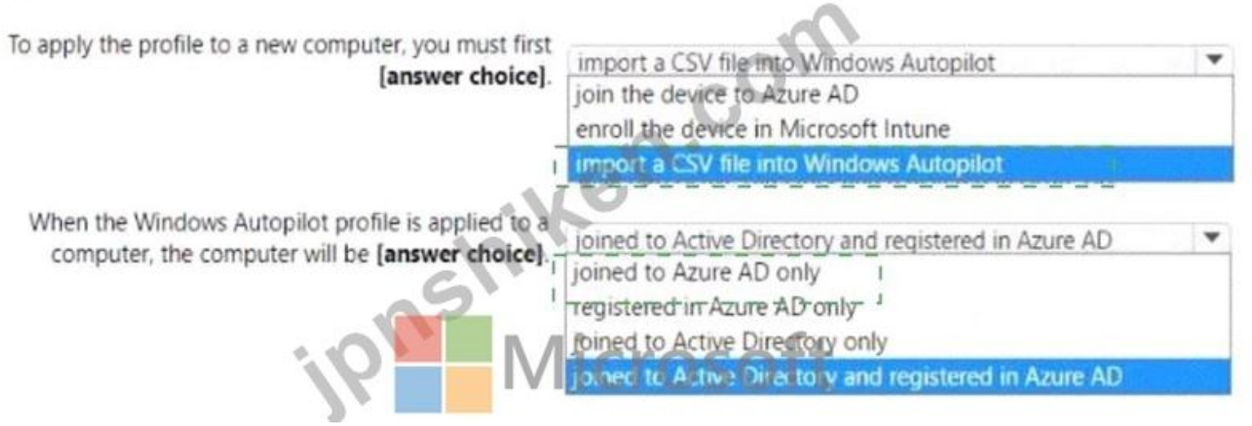
注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

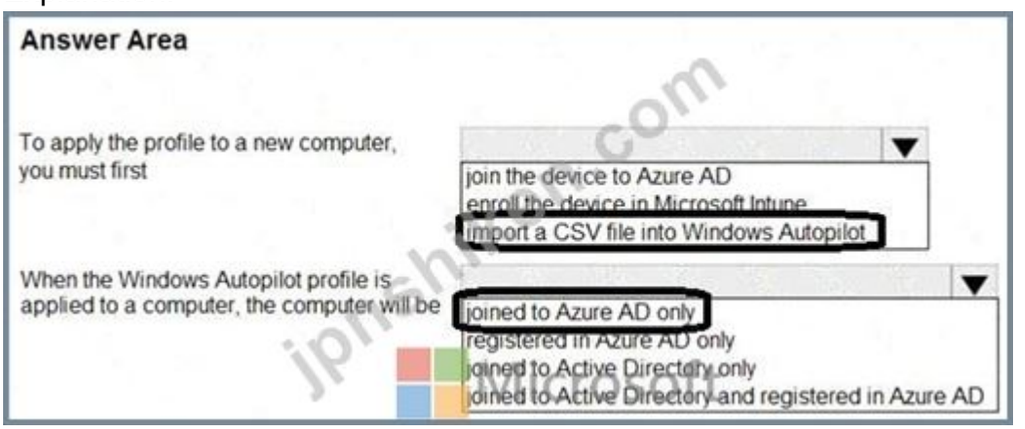


正解:

Answer Area



Explanation:



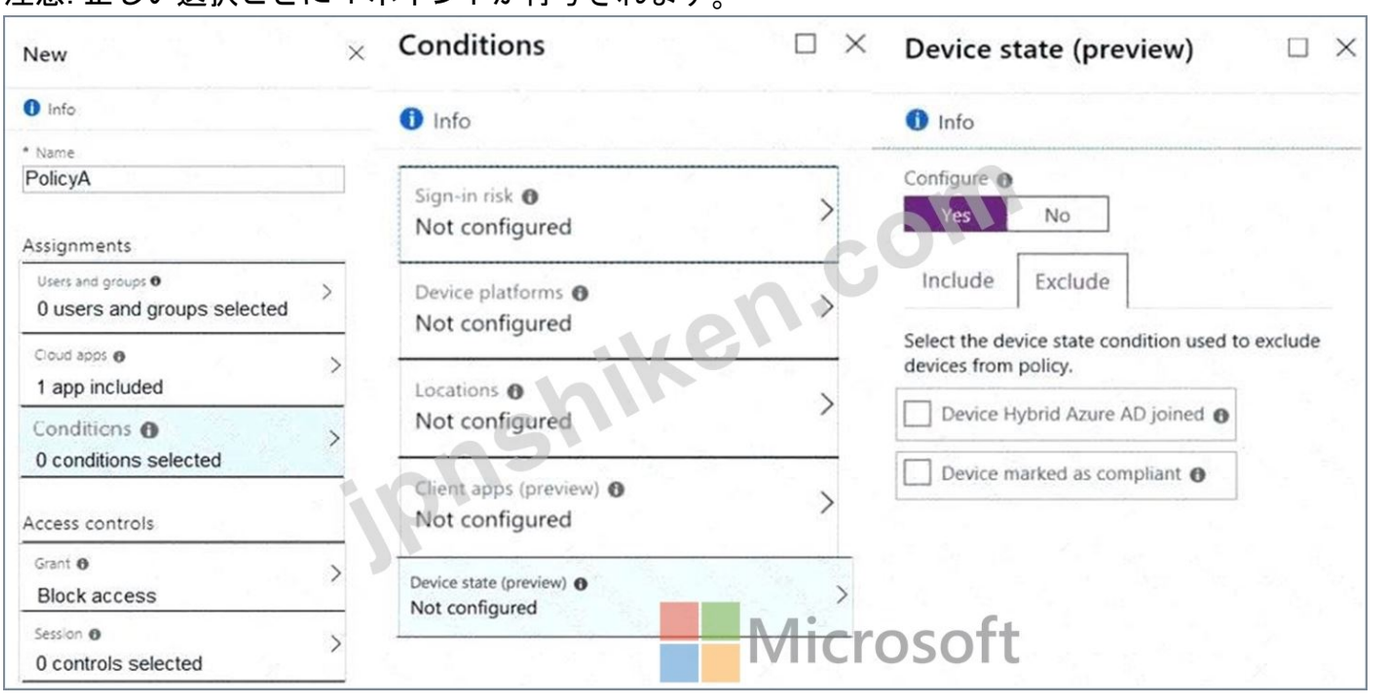
質問**: 67**

Office 365 Exchange Online に割り当てられた新しい条件付きアクセス ポリシーが必要です。

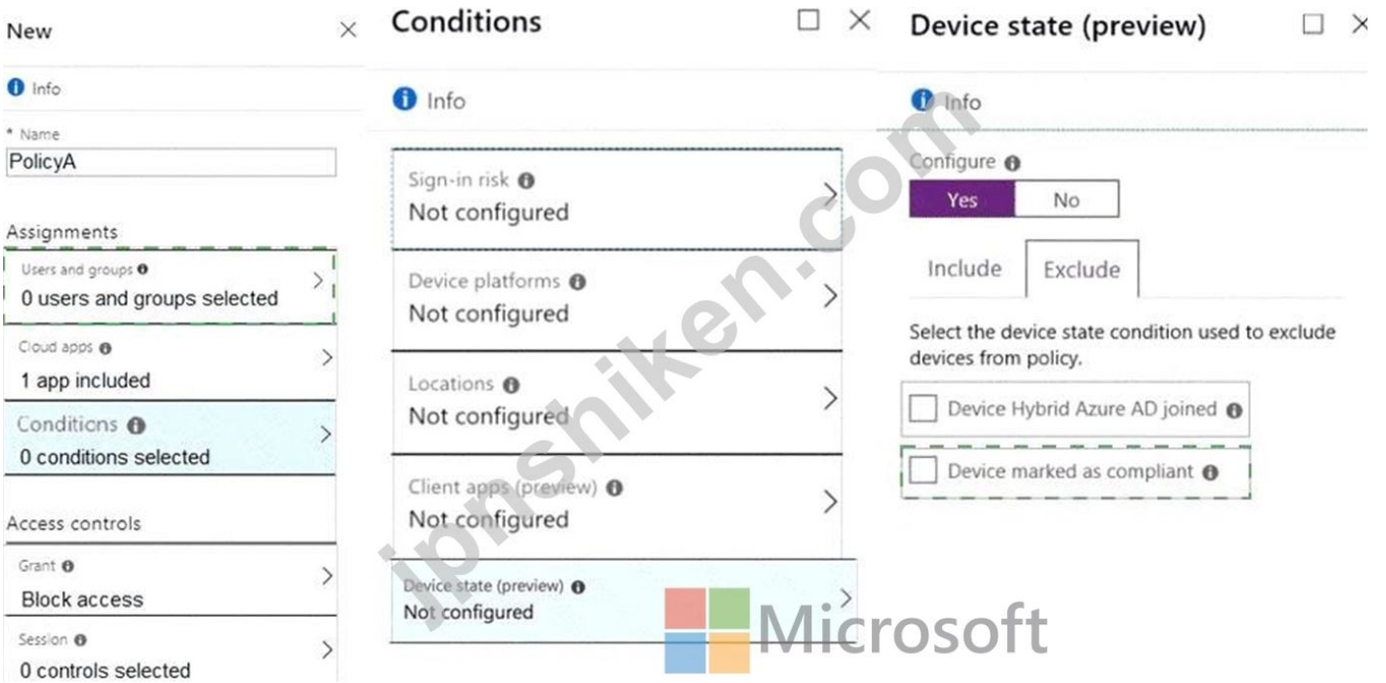
Group4 の技術要件を満たすようにポリシーを構成する必要があります。

ポリシーで構成する必要がある 2 つの設定はどれですか? 回答するには、回答領域で適切な設定を選択します。

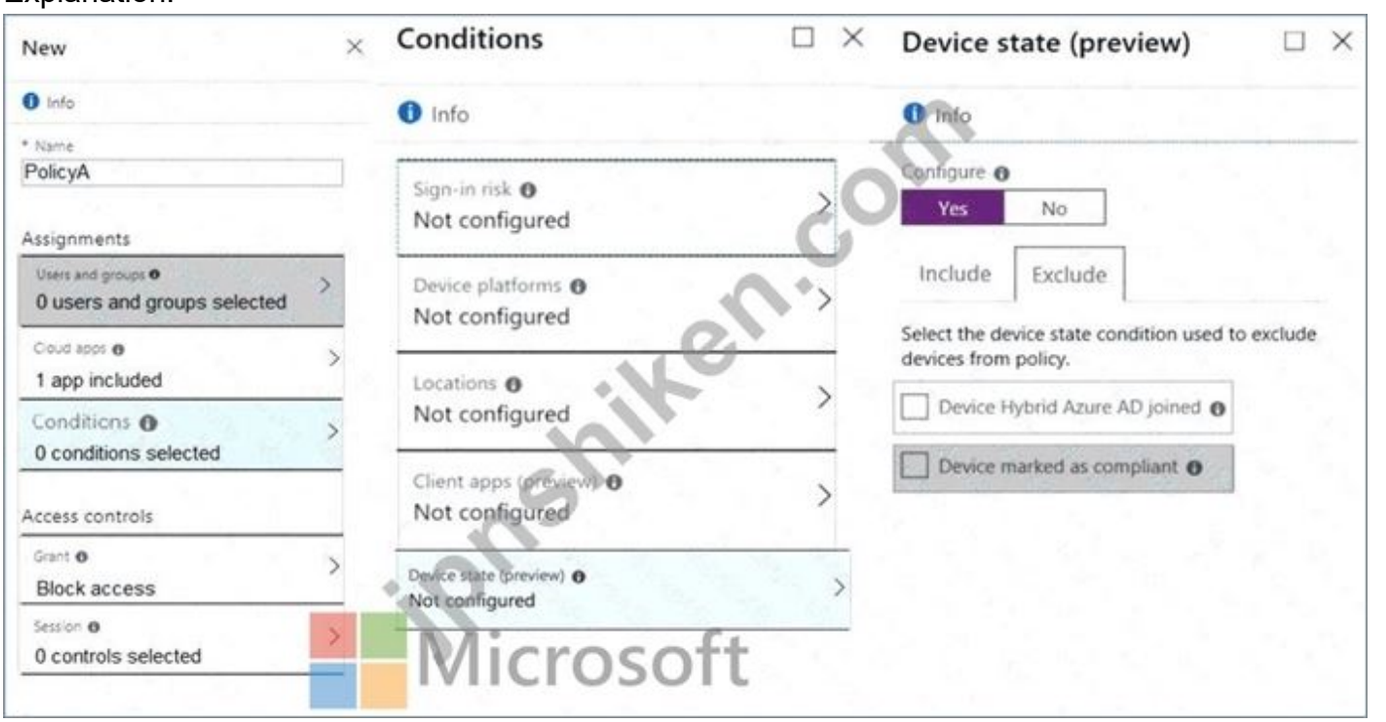
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



The policy needs to be applied to Group4 so we need to configure Users and Groups.

The Access controls are set to Block access

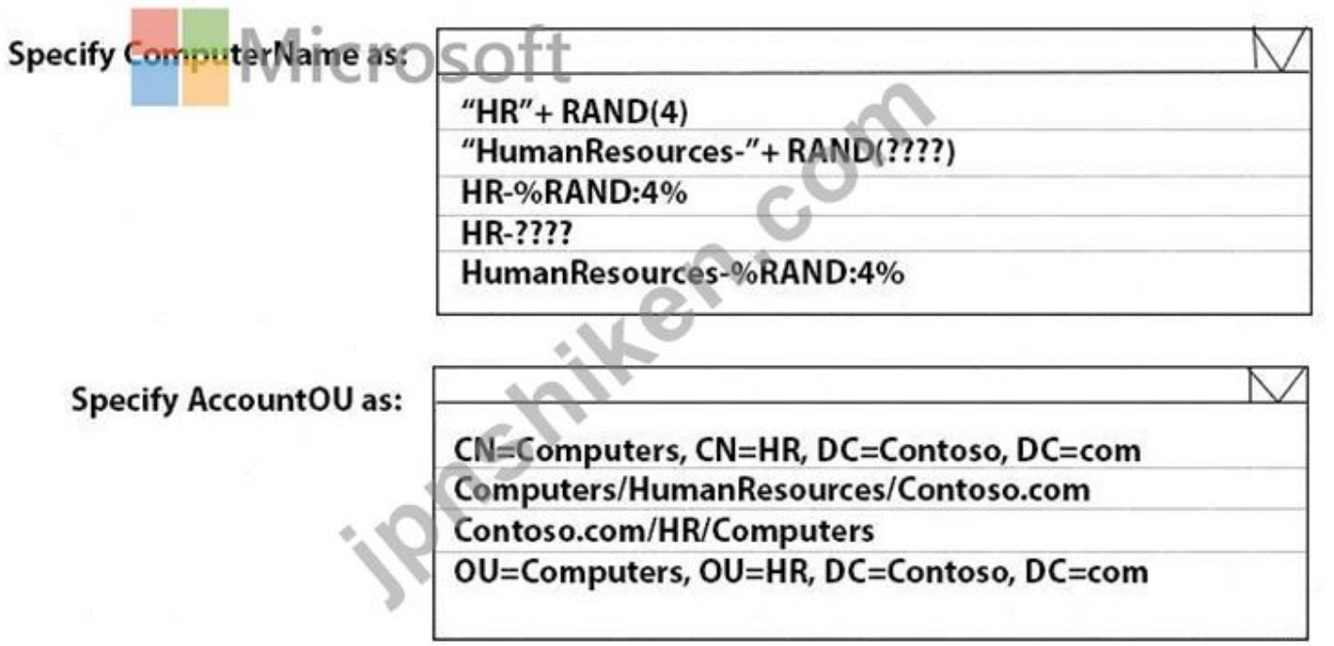
We therefore need to exclude compliant devices.

From the scenario:

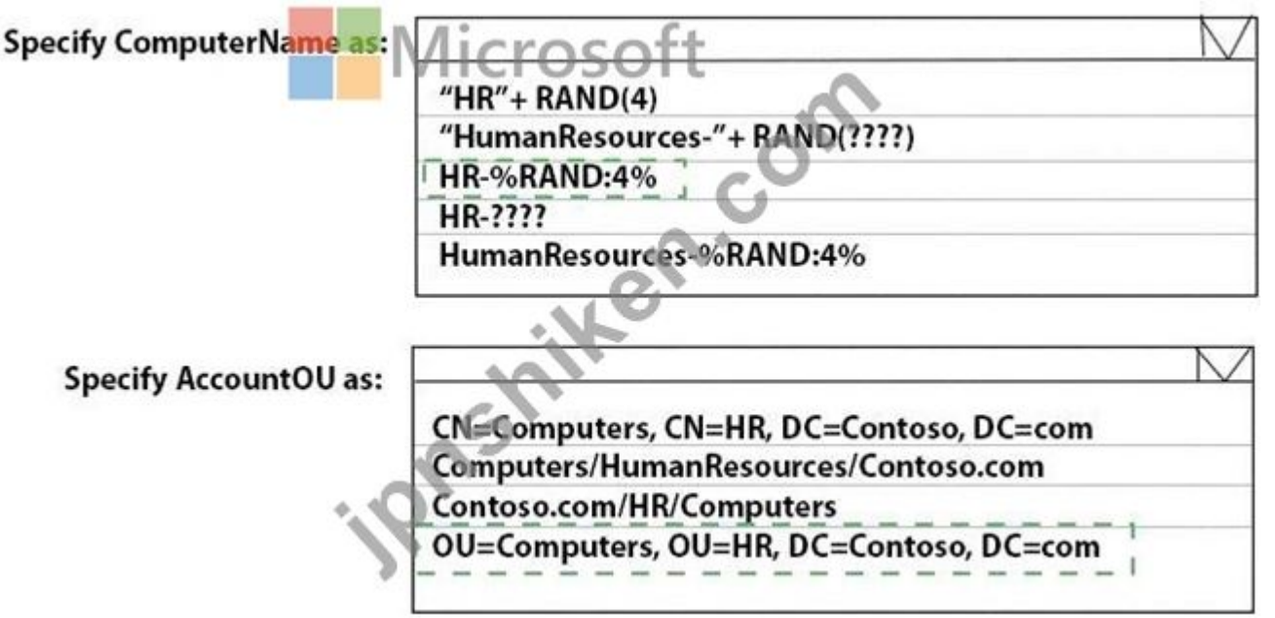
Ensure that the users in a group named Group4 can only access Microsoft Exchange Online from devices that are enrolled in Intune.

Note: When a device enrolls in Intune, the device information is updated in Azure AD to include the device compliance status. This compliance status is used by conditional access policies to block or allow access to e- mail and other organization resources.
References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/overview
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/conditions
https://docs.microsoft.com/en-us/intune/device-compliance-get-started

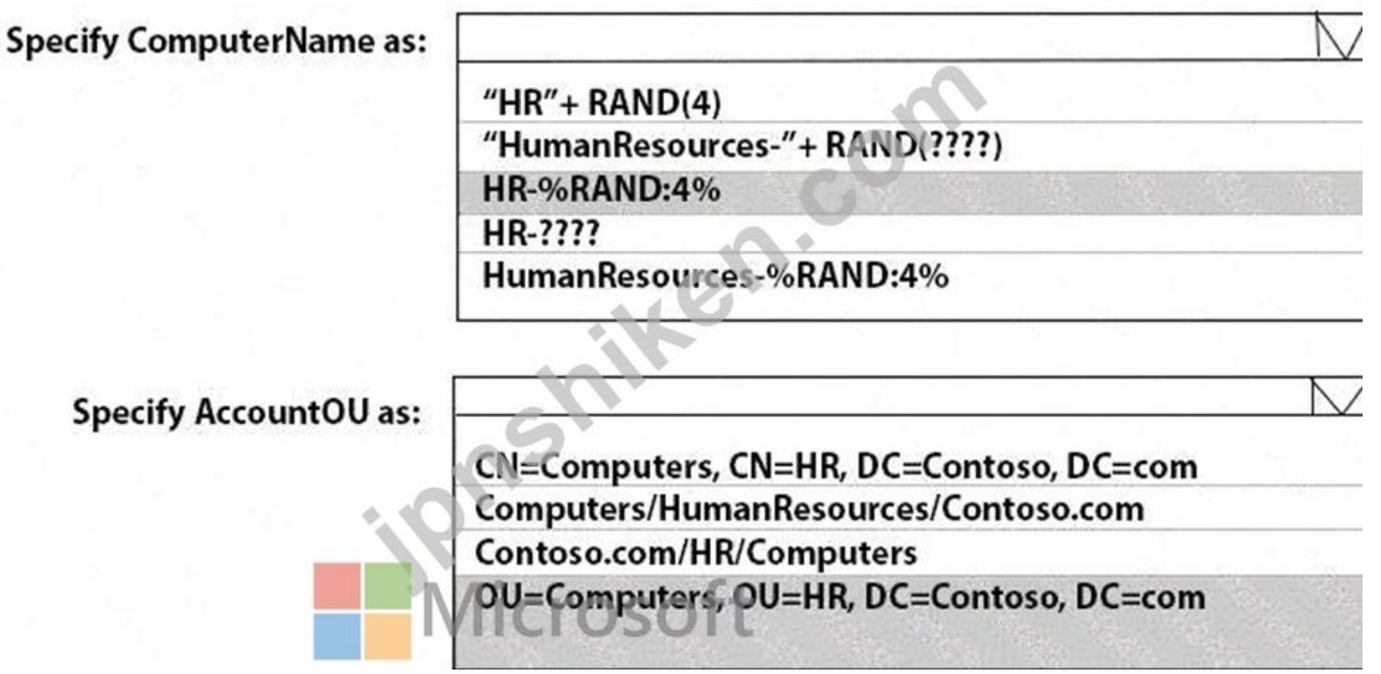
質問**: 68**
新しい人事部門のコンピューターの技術要件を満たす必要があります。
プロビジョニング パッケージをどのように構成すればよいですか? 回答するには、回答領域で適切なオプションを選択してください。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解**:**



Explanation:



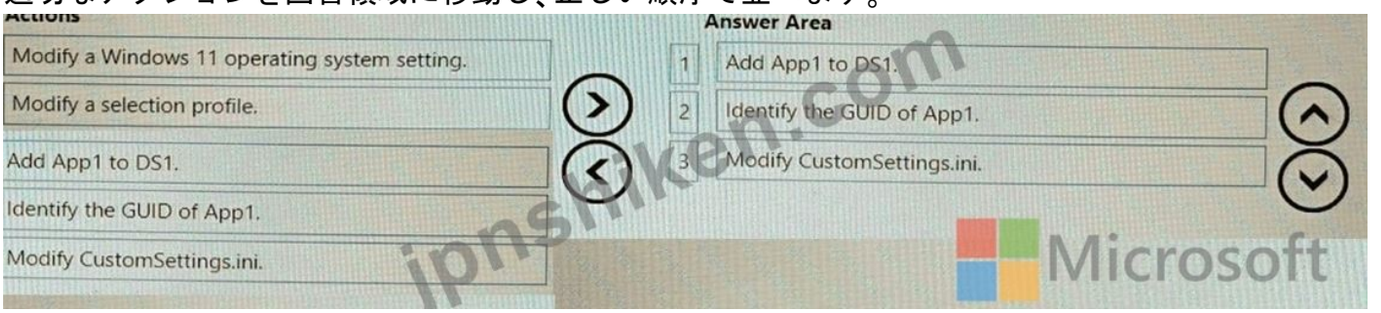
Reference:
https://docs.microsoft.com/en-us/windows/configuration/wcd/wcd-accounts

質問**: 69**
Windows 10 Pro を実行するコンピューターが 25 台あります。
Microsoft Intune を使用する Microsoft 365 E5 サブスクリプションがあります。
インプレース アップグレードを使用して、コンピューターを Windows 11 Enterprise にアップグレードする必要があります。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。
何を使うべきでしょうか?
A. サブスクリプションの有効化
B. Microsoft Deployment Toolkit (MDT) と Windows 11 Enterprise のデフォルト イメージ

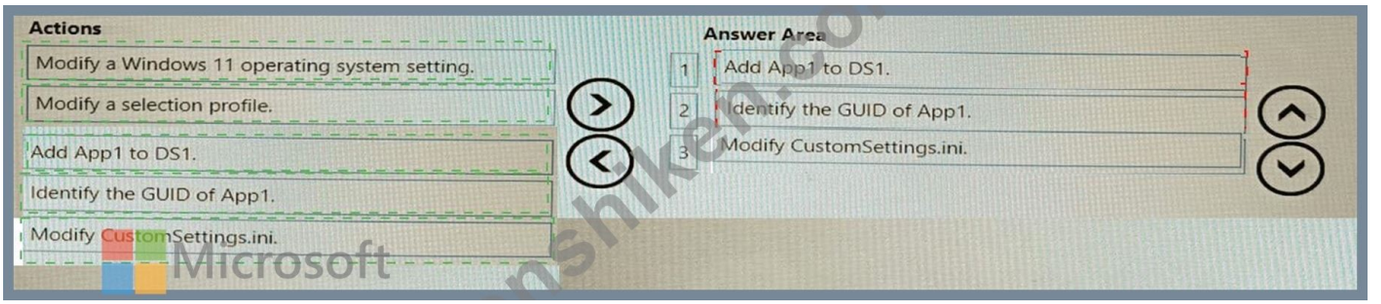
C. Windows オートパイロット
D. Microsoft Configuration Manager と Windows 11 Enterprise のカスタム イメージ
正解: **C** (コメントを発表する)

質問: **70**
Azure Log Analytics ワークスペースを含む Microsoft Azure サブスクリプションがあります。
Windows 10 を実行する Computer1 という名前の新しいコンピューターを展開します。Computer1 はワークグループ内にあります。
Log Analytics を使用して Computer1 からのイベントをクエリできることを確認する必要があります。
Computer1 では何をすればよいでしょうか?
A. Azure AD に参加します。
B. Windows Defender ファイアウォールを構成する
C. イベントサブスクリプションを作成します。
D. Azure Monitor エージェントをインストールします。
正解: (正解を表示します)
https://learn.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-windows-client#prerequisites

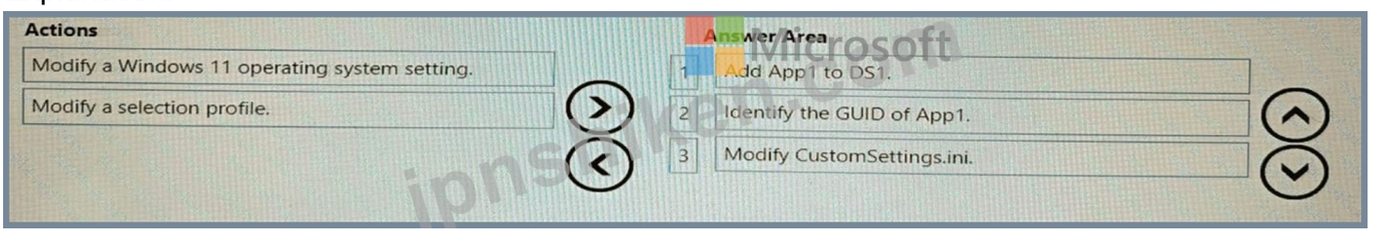
質問: **71**
DS1 という名前の Microsoft Deployment Toolkit (MDT) 展開共有があります。
Windows 11 イメージを DS1 にインポートします。
App1 という名前のアプリケーションの実行可能インストーラーがあります。
イメージを展開するすべてのタスク シーケンスに対して App1 がインストールされていることを確認する必要があります。
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクション リストから適切なアクションを回答領域に移動し、正しい順序で並べます。



正解:



Explanation:



MDT is a tool that allows you to automate the deployment of Windows operating systems and applications.

To install an application for all the task sequences that deploy a Windows 11 image, you need to perform the following three actions in sequence:

Add App1 to DS1. You can use the Deployment Workbench to import the executable installer of App1 to a folder in your deployment share. This will create an application entry with a unique GUID that identifies App11.

Identify the GUID of App1. You can find the GUID of App1 by opening the application properties in the Deployment Workbench and looking at the Application GUID field1. You can copy the GUID to use it later.

Modify CustomSettings.ini. You can edit the CustomSettings.ini file in your deployment share to specify which applications to install for each task sequence. You can use the Applications property to list the GUIDs of the applications you want to install, separated by commas1. For example, if you want to install App1 and another application with GUID {1234-5678-90AB-CDEF}, you can use this line:

Applications={GUID of App1},{1234-5678-90AB-CDEF}

These are the three actions you need to perform to ensure that App1 will be installed for all the task sequences that deploy the Windows 11 image from DS1. I hope this helps you. # If you want to learn more about MDT and how to deploy applications with it, you can check out these resources:

Get started with the Microsoft Deployment Toolkit (MDT) (Windows 10)

How to deploy applications with the Microsoft Deployment Toolkit

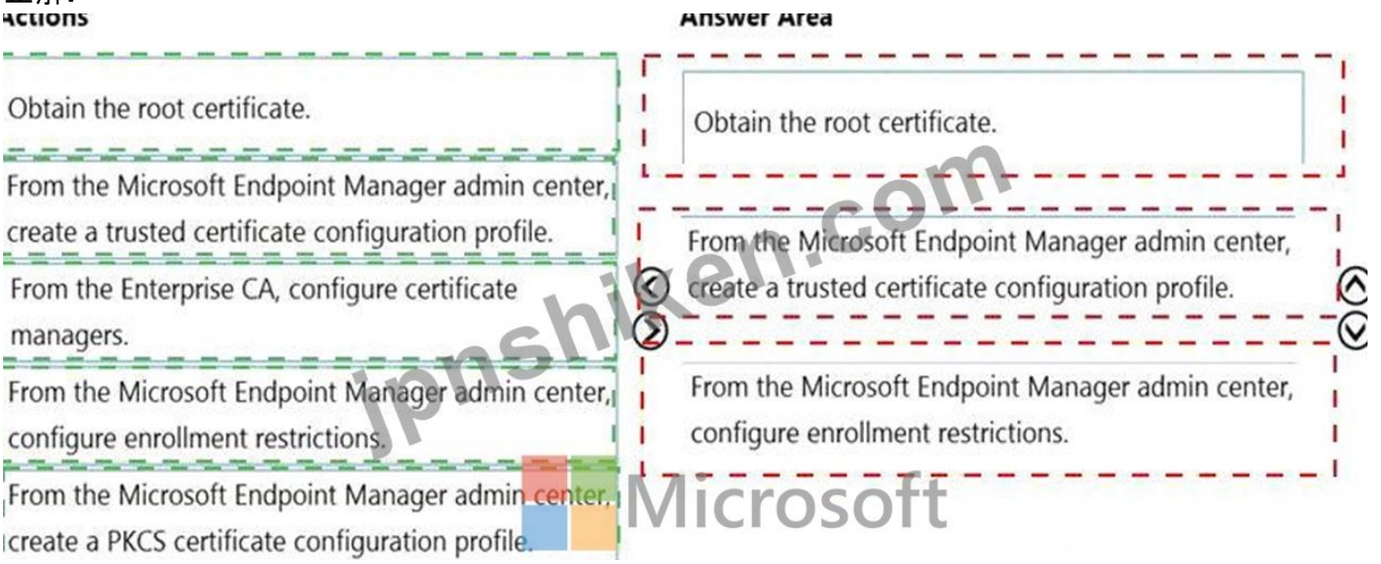
質問**: 72**

オンプレミスのエンタープライズ証明機関 (CA) への PFX 証明書コネクタを使用するように構成された Microsoft Intune サブスクリプションがあります。

公開キー ペア (PKCS) 証明書を使用して Android デバイスの自動登録を構成するには、Intune を使用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。

正解:

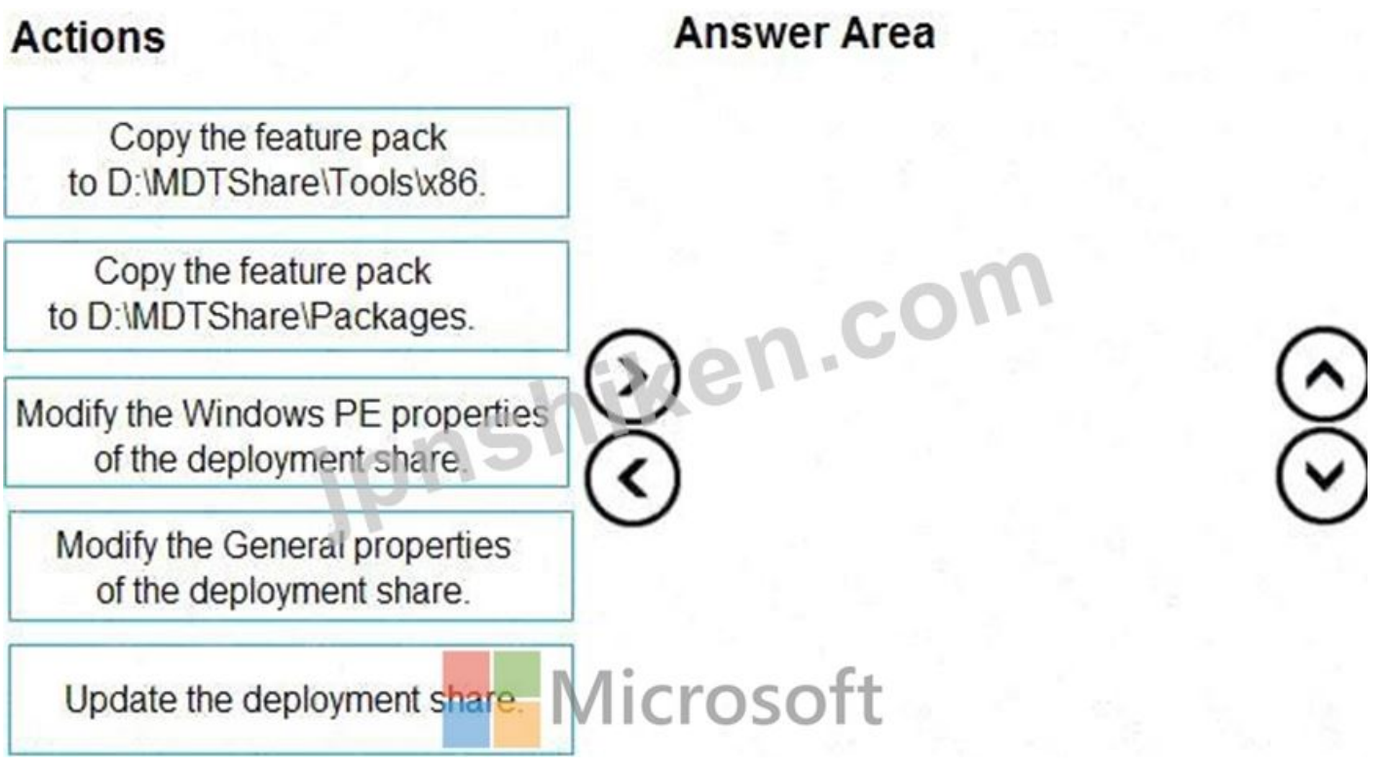


Explanation:

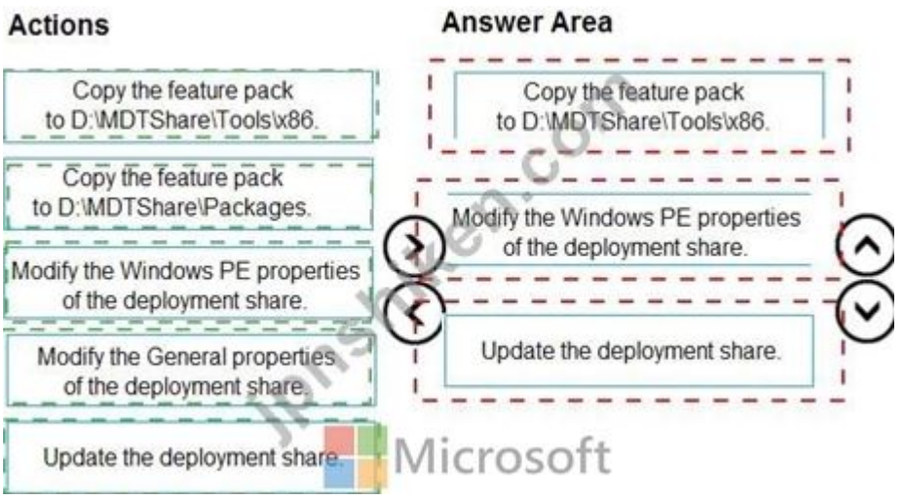
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/certificates-pfx-configure

質問: **73**

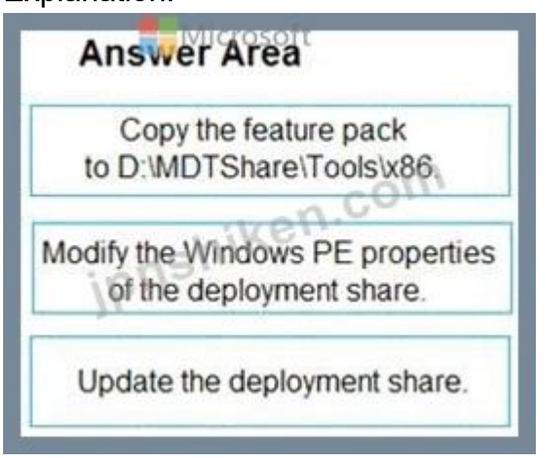
D:\MDTShare というパスを持つ Microsoft Deployment Toolkit (MDT) 展開共有があります。
ブート イメージに機能パックを追加する必要があります。
どの 3 つのアクションを順番に実行する必要がありますか? 回答するには、アクション リストから適切なアクションを回答領域に移動し、正しい順序で並べます。



正解:



Explanation:



Step 1: Copy the feature pack to D:\MDTShare\Tools\x86

Add a feature pack, DaRT 10 (part of MDOP 2015), to the boot images.

1. Copy the CAB files to the deployment share: MDTShare\Tools\x86

2. In the Deployment Workbench, right-click the MDTShare deployment share and select Properties.
Step 2: Modify the Windows PE properties of the deployment share
3. On the Windows PE tab, in the Platform drop-down list, make sure x86 is selected.
4. On the Features sub tab, select the Microsoft Diagnostics and Recovery Toolkit (DaRT) checkbox.
Step 3: Update the deployment share
Like the MDT Build Lab deployment share, the MDT Production deployment share needs to be updated after it has been configured. This is the process during which the Windows PE boot images are created.

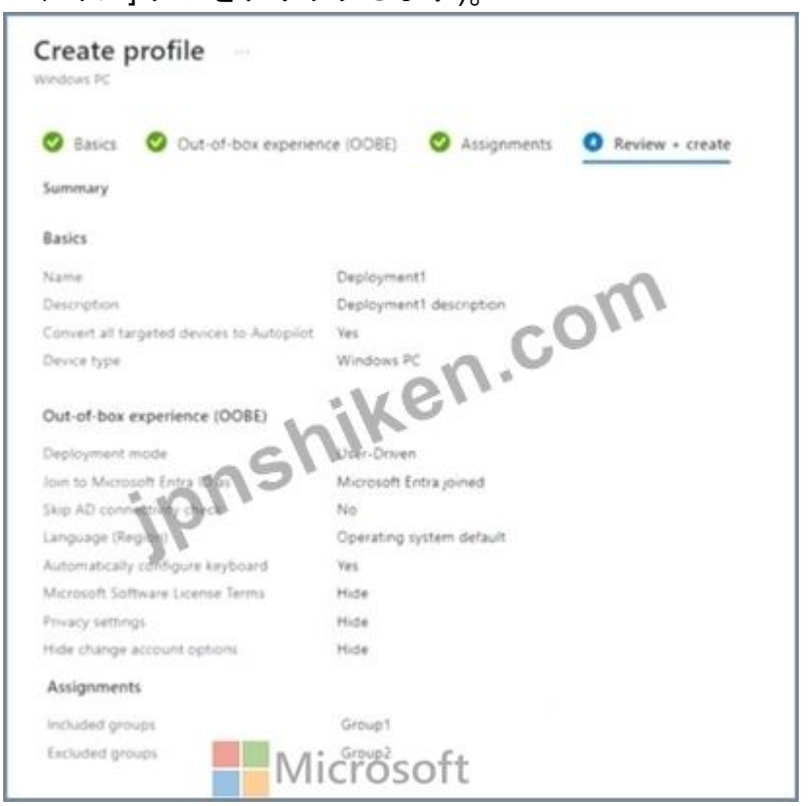
質問: **74**
次の表に示すデバイスを含む Microsoft Entra テナントがあります。

Name	Platform	Join type	Ownership
Device1	Windows 11	Microsoft Entra registered	Personal
Device2	Windows 10	Microsoft Entra joined	Corporate
Device3	Windows 11	Microsoft Entra joined	Corporate

テナントには、次の表に示すグループが含まれます。

Name	Members
Group1	Device1, Device2, Device3
Group2	Device3

展開プロファイルの図に示すように、Windows Autopilot 展開プロファイルを作成します ([展開プロファイル] 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 Area

正解:

Answer Area

Explanation:

質問: **75**

次の表に示すデバイスがあります。

Name	Operating system	Domain member
Device1	Windows 11 Enterprise	No
Device2	Windows 10 Pro	Yes
Device3	Android	No
Device4	Mac OS X	No

Microsoft Defender for Endpoint を実装する予定です。

Microsoft Defender for Endpoint にオンボードできるデバイス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?

A. デバイス1のみ

B. デバイス2のみ

C. デバイス1、デバイス2のみ

D. デバイス1、デバイス2、デバイス3のみ

E. デバイス1、デバイス2、デバイス3、デバイス4
正解**: D (**コメントを発表する**)**
Here is the list of Windows versions. Win10 and Win11 supported. The sentence "(standalone or as part of other Microsoft 365 plans)" excludes the domain needs.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/minimum-requirements?view=o365-worldwide
Here is the link for Android. No information about the specific version therefore it is supported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint- android?view=o365-worldwide Here is the link for MacOS System requirements: 14 (Sonoma), 13 (Ventura), 12 (Monterey). MAC OS X is older therefore unsupported.
https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint- mac?view=o365-worldwide

質問**: 76**
Windows 11 を実行する個人用デバイスにモバイル デバイス管理 (MDM) を実装する必要があります。ソリューションは次の要件を満たしている必要があります。
* Microsoft Intune を使用して個人用デバイスを管理できることを確認します。
* ユーザーが個人のデバイスから会社のデータにシームレスにアクセスできるようにします。
* ユーザーが個人アカウントを使用してのみ個人デバイスにサインインできるようにします。デバイスを Azure AD に追加するには何を使用すればよいですか?
A. ハイブリッド Microsoft Entra 結合
B. Microsoft Entra が参加しました
C. Microsoft Entra 登録済み
正解**: (**正解を表示します**)**
To implement MDM for personal devices that run Windows 11, you should use Azure AD registered. Azure AD registered devices are devices that are connected to your organization's resources using a personal device and a personal account. You can manage these devices by using Microsoft Intune and enable seamless access to company data. Users can only sign in to their personal devices by using their personal account, not their organizational account. Azure AD registered devices support Windows 10 or newer, iOS, Android, macOS, and Ubuntu 20.04/22.04 LTS1.
The other options are not suitable for this scenario because:
Hybrid Azure AD join is for corporate-owned and managed devices that are joined to both on-premises Active Directory and Azure AD. Users can sign in to these devices by using their organizational account that exists in both directories2.
AD joined is for devices that are joined only to on-premises Active Directory. These devices are not managed by Microsoft Intune and do not have access to cloud resources3.
References: What are Azure AD registered devices?, What are hybrid Azure AD joined devices?, What is an Active Directory domain join?

質問: **77**
Microsoft Intune を含む Microsoft 365 サブスクリプションをお持ちです。
企業所有の Android デバイス 500 台が完全に管理対象デバイスとして登録されています。
デバイスに展開するには、App1 という名前のアプリを準備する必要があります。
実行すべき 2 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。
注意: 正解は1点です。
A. Intune ポータル サイトから Appl をダウンロードします。
B. OEMConfig プロファイルを作成します。
C. Managed Google Play ストアから、App1 を承認します。
D. App1 を Intune と同期します。
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/mem/intune/apps/apps-add-android-for-work

質問: **78**
あなたの会社では Microsoft Intune を使用しています。
500 台を超える Android および iOS デバイスが Intune テナントに登録されています。
新しい Intune ポリシーを展開する予定です。デバイスにインストールされている Android または iOS のバージョンに応じて、異なるポリシーが適用されます。
Android または iOS のバージョンに基づいて、ポリシーがデバイスをターゲットにできることを確認する必要があります。
最初に何を設定する必要がありますか?
A. Azure AD で動的なメンバーシップ ルールを持つグループ
B. Intune のデバイス カテゴリ
C. Azure AD のデバイス設定
D. Intune の企業デバイス識別子
正解: **A (**コメントを発表する**)**

質問: **79**
Microsoft Intune を含む Microsoft 365 E5 サブスクリプションをお持ちです。このサブスクリプションには「Group!」というグループが含まれています。Group1 には Intune に登録されているデバイスが含まれています。
Intune でリモート ヘルプを展開します。

サポート管理者のみが Group1 内のデバイスからリモート ヘルプ セッションに参加できるように、リモート ヘルプを構成する必要があります。
どのような種類の Microsoft Entra オブジェクトを作成し、どのような種類のポリシーを構成する必要がありますか。7 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。
デバイス

正解:

Explanation:

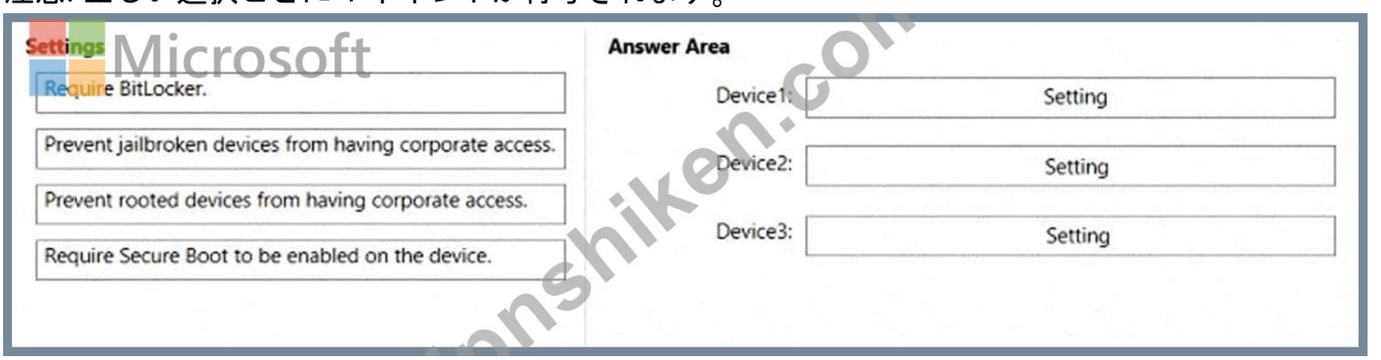
質問: **80**
ネットワークには Active Directory ドメイン サービス (AD DS) ドメインが含まれています。ドメインには、Windows 10 を実行するクライアント コンピューターが 100 台含まれています。
現在、貴社には展開インフラストラクチャがありません。
同社はボリューム ライセンス契約を通じて Windows 11 ライセンスを購入します。
コンピューターを Windows 11 にアップグレードする方法を推奨する必要があります。ソリューションではライセンス コストを最小限に抑える必要があります。
推薦書には何を含めるべきでしょうか?
A. Microsoft 展開ツールキット (MDT)

B. 構成マネージャー
C. サブスクリプションの有効化
D. Windows オートパイロット
正解: **(**正解を表示します**)**

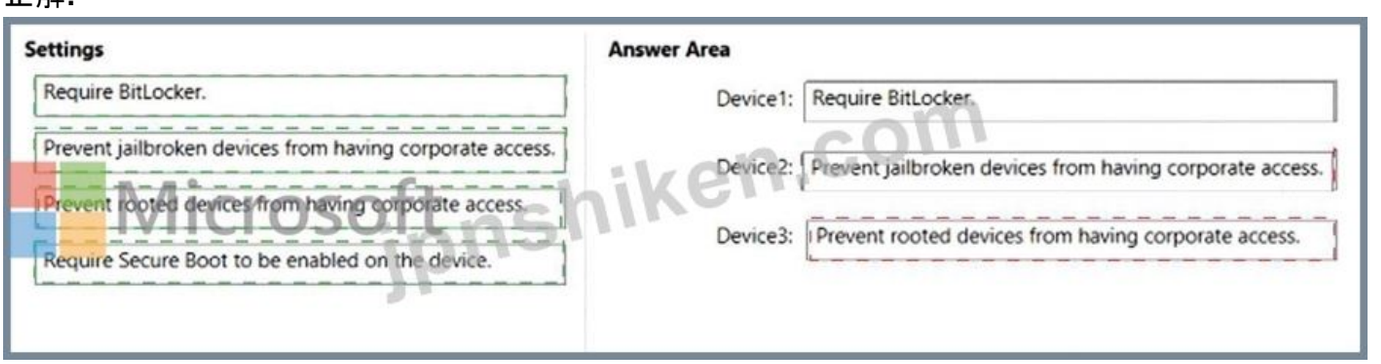
質問: **81**
次の表に示すデバイスを含む Microsoft 365 サブスクリプションがあります。

Name	Type
Device1	Windows 10
Device2	iOS
Device3	Android Enterprise

信頼できるファームウェアまたはオペレーティング システム ビルドを実行しているデバイスのみがネットワーク リソースにアクセスできるようにする必要があります。
各デバイスにどのコンプライアンス ポリシー設定を構成する必要がありますか? 答えるには、適切な設定を正しいデバイスにドラッグします。各設定は、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。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:
Box 1:
Device Compliance settings for Windows 10/11 in Intune

There are the different compliance settings you can configure on Windows devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require BitLocker, set a minimum and maximum operating system, set a risk level using Microsoft Defender for Endpoint, and more.
Note: Windows Health Attestation Service evaluation rules
Require BitLocker:
Windows BitLocker Drive Encryption encrypts all data stored on the Windows operating system volume.
BitLocker uses the Trusted Platform Module (TPM) to help protect the Windows operating system and user data. It also helps confirm that a computer isn't tampered with, even if its left unattended, lost, or stolen. If the computer is equipped with a compatible TPM, BitLocker uses the TPM to lock the encryption keys that protect the data. As a result, the keys can't be accessed until the TPM verifies the state of the computer.
Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
Require - The device can protect data that's stored on the drive from unauthorized access when the system is off, or hibernates.
Box 2: Prevent jailbroken devices from having corporate access
Device Compliance settings for iOS/iPadOS in Intune
There are different compliance settings you can configure on iOS/iPadOS devices in Intune. As part of your mobile device management (MDM) solution, use these settings to require an email, mark rooted (jailbroken) devices as not compliant, set an allowed threat level, set passwords to expire, and more.
Device Health
Jailbroken devices
Supported for iOS 8.0 and later
Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
Block - Mark rooted (jailbroken) devices as not compliant.
Box 3: Prevent rooted devices from having corporate access.
Device compliance settings for Android Enterprise in Intune
There are different compliance settings you can configure on Android Enterprise devices in Intune. As part of your mobile device management (MDM) solution, use these settings to mark rooted devices as not compliant, set an allowed threat level, enable Google Play Protect, and more.
Device Health - for Personally-Owned Work Profile
Rooted devices
Not configured (default) - This setting isn't evaluated for compliance or non-compliance.
Block - Mark rooted devices as not compliant.
Reference: https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-windows
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-android-for-work
https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-create-ios

質問: 82

Microsoft 365 E5 サブスクリプションと 100 台の管理されていない iPad デバイスがあります。
特定の iOS アップデートをデバイスに展開する必要があります。ユーザーが iOS の最新バージョンを手動でインストールできないようにする必要があります。
実行すべき 2 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. Intune ポータル サイトを使用して、デバイスを Microsoft Intune に登録します。
B. コンプライアンス ポリシーを作成します。
C. Apple Business Manager を使用して、デバイスを Microsoft Intune に登録します。
D. iOS アプリのプロビジョニング プロファイルを作成します。
E. デバイス構成プロファイルを作成します。
正解**: C,E (**コメントを発表する**)**
To deploy a specific iOS update to the unmanaged iPad devices, you need to perform the following actions:
Enroll the devices in Microsoft Intune by using Apple Business Manager. Apple Business Manager is a service that allows you to enroll and manage iOS/iPadOS devices in bulk. You can use Apple Business Manager to assign devices to Microsoft Intune and enroll them as supervised devices. Supervised devices are devices that have more management features and restrictions than unsupervised devices. You can also use Apple Business Manager to create device groups and assign roles and permissions12.
Create a device configuration profile. A device configuration profile is a policy that you can create and assign in Microsoft Intune to configure settings on your devices. You can use a device configuration profile to manage software updates for iOS/iPadOS supervised devices. You can choose to deploy the latest update or an older update, specify a schedule for the update installation, and delay the visibility of software updates on the devices34.
The other options are not correct for this scenario because:
Enrolling the devices in Microsoft Intune by using the Intune Company Portal is not suitable for unmanaged devices. The Intune Company Portal is an app that users can download and install on their personal or corporate-owned devices to enroll them in Microsoft Intune. However, this method requires user interaction and consent, and does not enroll the devices as supervised devices5.
Creating a compliance policy is not necessary for this scenario. A compliance policy is a policy that you can create and assign in Microsoft Intune to evaluate and enforce compliance settings on your devices. You can use a compliance policy to check if the devices meet certain requirements, such as minimum OS version, encryption, or password settings. However, a compliance policy does not deploy or manage software updates on the devices6.
Creating an iOS app provisioning profile is not relevant for this scenario. An iOS app provisioning profile is a file that contains information about the app and its distribution method. You can use an iOS app provisioning profile to deploy custom or line-of-business apps to your iOS/iPadOS devices by using Microsoft Intune. However, an iOS app provisioning profile does not affect the software updates on the devices7.

References: What is Apple Business Manager?, Enroll iOS/iPadOS devices in Intune, Manage iOS/iPadOS software update policies in Intune, Software updates planning guide and scenarios for supervised iOS/iPadOS devices in Microsoft Intune, Enroll your personal device in Intune, Device compliance policies in Microsoft Intune, Add an iOS app provisioning profile with Microsoft Intune

質問: **83**
Windows Autopilot 展開の一部としてコンピューター オブジェクトを作成できることを確認する必要があります。ソリューションは技術要件を満たしている必要があります。
コンピュータ オブジェクトを作成する権限を何に付与する必要がありますか?
A. サーバー2
B. サーバー1
C. グループA
D. DC1
正解: **(**正解を表示します**)**
Reference:
https://blog.matrixpost.net/set-up-windows-autopilot-production-environment-part-2/

質問: **84**
DS1 という名前の Microsoft Deployment Toolkit (MDT) 展開共有があります。
Out-of-Box Drivers ノードでは、さまざまなハードウェア モデル用のドライバーを含むフォルダーを作成します。
PnP 検出を使用してハードウェア モデルの 1 つ用のドライバーをインストールするには、Inject Drivers MDT タスクを構成する必要があります。
まず何をすべきでしょうか?
A. 選択プロファイルを作成します。
B. OS パッケージをインポートします。
C. タスク シーケンスに Gather タスクを追加します。
D. タスク シーケンスに検証タスクを追加します。
正解: **A (**コメントを発表する**)**

質問: **85**
Azure AD に参加しているコンピューターの技術要件を満たすには、何を構成する必要がありますか?
A. Azure ポータルの Microsoft Intune ブレードからの Windows Hello for Business。
B. エンドポイント保護プロファイルのアカウント オプション。
C. グループ ポリシー オブジェクト (GPO) 内のパスワード ポリシー設定。
D. Microsoft Office 365 ポータルからのパスワード ポリシー。
正解: **(**正解を表示します**)**
References:

https://docs.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-manage- inorganization

質問: **86**
あなたの会社には Microsoft 365 サブスクリプションがあります。
財務部門のすべてのユーザーは、iOS または Android を実行する個人用デバイスを所有しています。
すべてのデバイスは Microsoft Intune に登録されています。
財務部門では毎月新しいユーザーが追加されます。
同社は、財務部門のユーザー向けに App1 というモバイル アプリケーションを開発しています。
財務部門のユーザーのみが Appl をダウンロードできるようにする必要があります。
まず何をすべきでしょうか?
A. Microsoft Entra に App1 を登録します。
B. iOS および Android アプリケーションのベンダー ストアに App1 を追加します。
C. App1 を Microsoft Deployment Toolkit (MDT) 展開共有に追加します。
D. App1 を Intune に追加します。
正解: **(**正解を表示します**)**

質問: **87**
Microsoft Intune を使用し、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	Member of
User1	Group1
User2	None
User3	None

図に示すように、Set1 という名前のポリシー セットを作成します。([図] タブをクリックします。)

Device management Edit

Device configuration profiles (1)

Name	Platform	Profile Type
ConfigurationProfile1	Windows 10 and later	Device restrictions

Device compliance policies (1)

Name	Platform	Profile Type
CompliancePolicy1	Windows 10 and later	Windows 10 and later co...

Device enrollment Edit

Windows autopilot deployment profiles

No results

Enrollment status pages

No results.

Assignments Edit

Included groups	All Users
Excluded groups	Group1

次の表に示すように、Intune にデバイスを登録します。

Name	Operating system	User
Device1	Windows 10	User1
Device2	Windows 11	User2
Device3	Android	User3

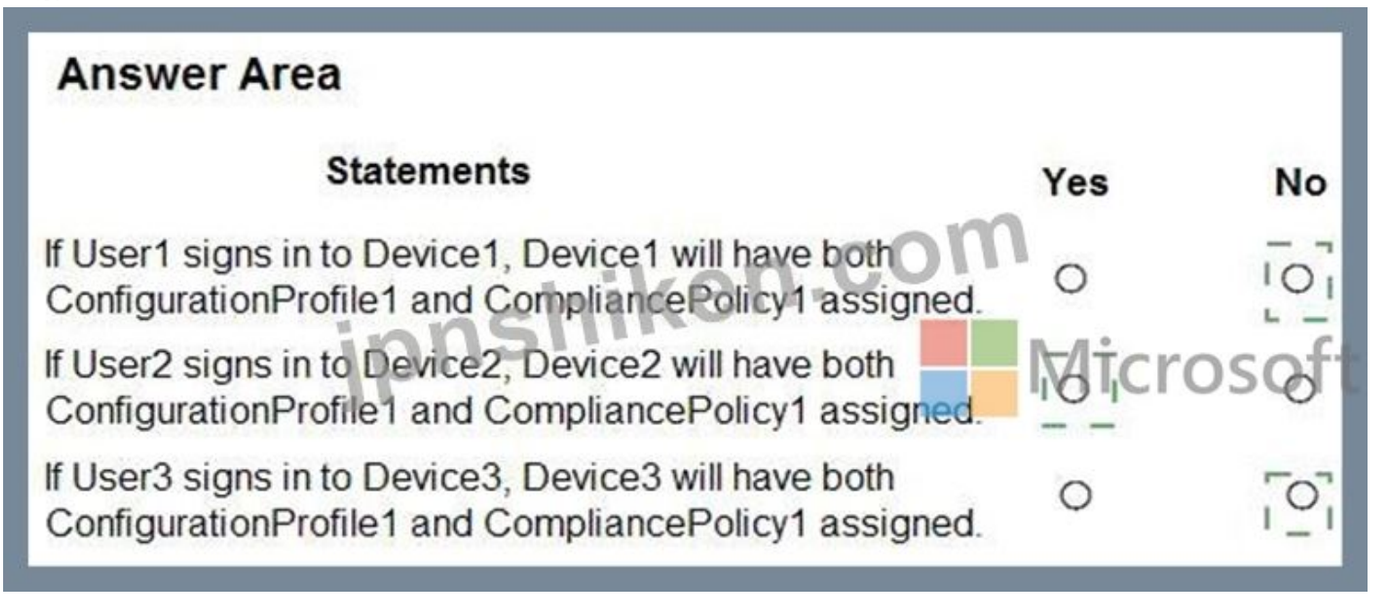
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

Statements	Yes	No
If User1 signs in to Device1, Device1 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User2 signs in to Device2, Device2 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○
If User3 signs in to Device3, Device3 will have both ConfigurationProfile1 and CompliancePolicy1 assigned.	○	○

正解:



Explanation:

質問: **88**

Microsoft Intune と Intune データ ウェアハウスを使用します。

データ ウェアハウスに保存されているデータを含むデバイス インベントリ レポートを作成する必要があります。

レポートを作成するには何を使用すればよいですか?

A. Azure ポータル アプリ
B. エンドポイント分析
C. 企業ポータル アプリ
D. Microsoft Power BI
正解**: D (**コメントを発表する**)**
You can use the Power BI Compliance app to load interactive, dynamically generated reports for your Intune tenant. Additionally, you can load your tenant data in Power BI using the OData link. Intune provides connection settings to your tenant so that you can view the following sample reports and charts related to:
Devices
Enrollment
App protection policy
Compliance policy
Device configuration profiles
Software updates
Device inventory logs
Note: Load the data in Power BI using the OData link
With a client authenticated to Azure AD, the OData URL connects to the RESTful endpoint in the Data Warehouse API that exposes the data model to your reporting client. Follow these instructions to use Power BI Desktop to connect and create your own reports.
Sign in to the Microsoft Endpoint Manager admin center.
Select Reports > Intune Data warehouse > Data warehouse.
Retrieve the custom feed URL from the reporting blade, for example:
https://fef.{yourtenant}.manage.microsoft.com/ReportingService/DataWarehouseFEService/dates?api- version=v1.0 Open Power BI Desktop.
Choose File > Get Data. Select OData feed.
Choose Basic.
Type or paste the OData URL into the URL box.
Select OK.
If you have not authenticated to Azure AD for your tenant from the Power BI desktop client, type your credentials. To gain access to your data, you must authorize with Azure Active Directory (Azure AD) using OAuth 2.0.
Select Organizational account.
Type your username and password.
Select Sign In.
Select Connect.
Select Load.
Reference: https://docs.microsoft.com/en-us/mem/intune/developer/reports-proc-get-a-link-powerbi

質問**: 89**
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。

Windows 11 を実行するデバイスを管理するには、Microsoft in tune を使用します。
登録されているすべてのデバイスのローカル管理者グループから User1 を削除する必要があります。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。
何を設定すればよいでしょうか?
A. アプリ構成ポリシー
B. デバイスコンプライアンスポリシー
C. アカウント保護ポリシー
正解**: (**正解を表示します**)**

質問**: 90**
150 台のハイブリッド Azure AD 参加済み Windows デバイスを含む Microsoft 365 E5 サブスクリプションがあります。すべてのデバイスは Microsoft Intune に登録されています。次の要件を満たすように、デバイスで配信の最適化を構成する必要があります。
* インターネットおよびローカル ネットワーク上の他のコンピューターからのダウンロードを許可します。
* 使用帯域幅の割合を 50 に制限します。
何を使うべきでしょうか?
A. 構成プロファイル
B. Windows Update for Business グループ ポリシー設定
C. Microsoft ピアツーピア ネットワーク サービス グループ ポリシー設定
D. Windows 10 以降のプロファイル用の更新リング
正解**: C (**コメントを発表する**)**
A configuration profile is the correct answer because it allows you to configure Delivery Optimization settings for Windows devices in Intune. You can specify the download mode, bandwidth limit, caching options, and more. A configuration profile is a template that contains one or more settings that you can apply to groups of devices. References:
Windows 10 Delivery Optimization settings for Intune - Microsoft Intune | Microsoft Learn Delivery Optimization settings in Microsoft Intune

質問**: 91**
User! という名前のユーザーと Appl という名前の Web アプリを含む Microsoft 365 E5 サブスクリプションがあります。
App1 は最新の認証要求のみを受け入れる必要があります。
次の設定を持つ CAPolicy1 という名前の条件付きアクセス ポリシーを作成する予定です。
* 課題
° ユーザーまたはワークロード ID: User1
° クラウドアプリまたはアクション: App1
* アクセス制御
° 許可: アクセスをブロック

アプリケーションへのレガシー認証リクエストのみをブロックする必要があります。CAPolicy1 に追加する条件はどれですか。
A. デバイスのフィルター
B. デバイスプラットフォーム
C. ユーザーリスク
D. サインインリスク
E. クライアントアプリ
正解**: (**正解を表示します**)**
you can use the client apps condition to block legacy authentication requests to App11. Legacy authentication is a term that refers to authentication protocols that do not support modern authentication features such as multi-factor authentication or conditional access2. Examples of legacy authentication protocols include Basic Authentication, Digest Authentication, NTLM, and Kerberos2. To block legacy authentication requests, you need to configure the client apps condition to include Other clients, which covers any client that uses legacy authentication protocols13. References: 1: Conditional Access: Block legacy authentication | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/block-legacy-authentication 2:
What is legacy authentication? | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection
/conditional-access/legacy-authentication 3: Client apps condition in Azure Active Directory Conditional Access | Microsoft Learn https://learn.microsoft.com/en-us/mem/identity-protection/conditional-access/client- apps-condition

質問**: 92**
Azure AD テナントと、Azure AD に参加し、Microsoft Intune を使用して管理されている 100 台の Windows 10 デバイスがあります。
デバイス上で Microsoft Defender ファイアウォールと Microsoft Defender ウイルス対策を構成する必要があります。ソリューションは管理作業を最小限に抑える必要があります。
実行すべき 2 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。
注意: 正しい選択ごとに 1 ポイントが付与されます。
A. Microsoft Defender ウイルス対策を構成するには、グループ ポリシー オブジェクト (GPO) を作成し、Windows Defender ウイルス対策設定を構成します。

B. Microsoft Defender ファイアウォールを構成するには、デバイス構成プロファイルを作成し、デバイスの制限設定を構成します。
C. Microsoft Defender ウイルス対策を構成するには、デバイス構成プロファイルを作成し、エンドポイント保護設定を構成します。
D. Microsoft Defender ウイルス対策を構成するには、デバイス構成プロファイルを作成し、デバイスの制限設定を構成します。
E. Microsoft Defender ファイアウォールを構成するには、デバイス構成プロファイルを作成し、エンドポイント保護設定を構成します。
F. Microsoft Defender ファイアウォールを構成するには、グループ ポリシー オブジェクト (GPO) を作成し、セキュリティが強化された Windows Defender ファイアウォールを構成します。
正解**: (**正解を表示します**)**
To configure Microsoft Defender Firewall and Microsoft Defender Antivirus on Azure AD joined devices that are managed by Intune, you need to create a device configuration profile and configure the Endpoint protection settings. You can use this profile to configure various settings for firewall and antivirus protection on the devices. References: https://docs.microsoft.com/en-us/mem/intune/protect/endpoint-protection- windows-10

質問**: 93**
次の表に示すユーザーを含む Azure AD テナントがあります。

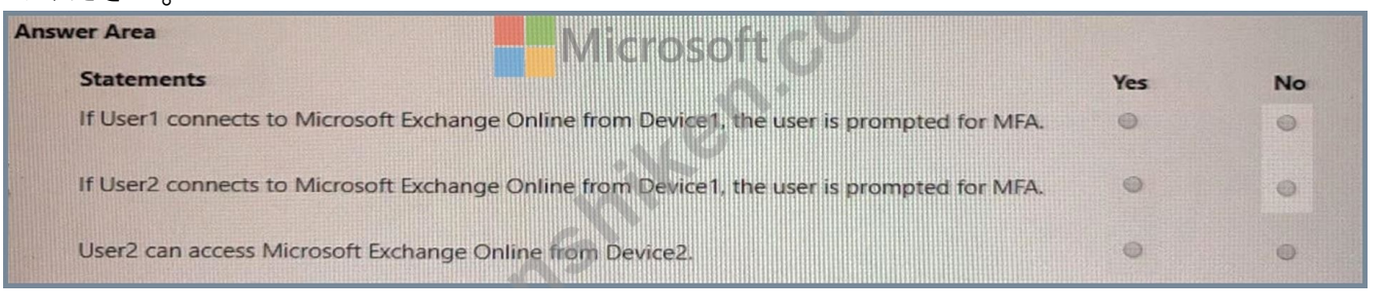
Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Enabled

次の表に示すデバイスがあります。

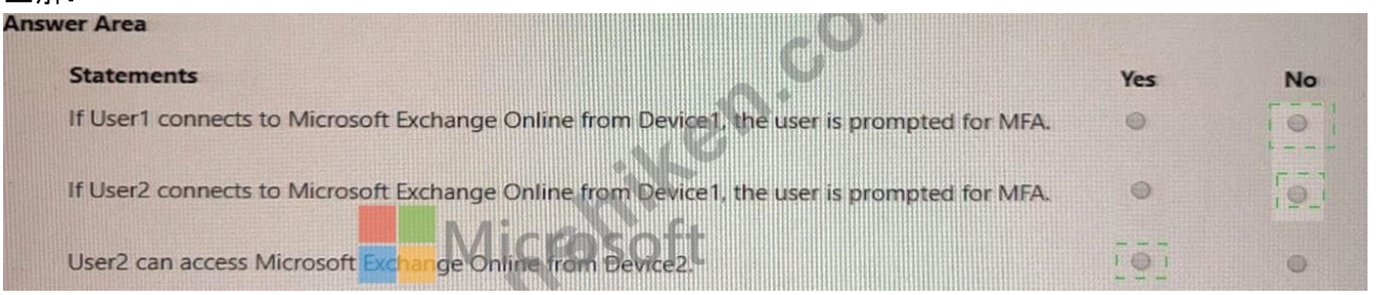
Name	Platform
Device1	Android
Device2	iOS

次の設定を持つ CAPolicy1 という名前の条件付きアクセス ポリシーがあります。
* 課題
o ユーザーまたはワークロード ID: ユーザー 1。User1
o クラウドアプリまたはアクション: Office 365 Exchange Online
o 条件: デバイスプラットフォーム: Windows、iOS
* アクセス制御
o 多要素認証を要求する
次の設定を持つ CAPolicy2 という名前の条件付きアクセス ポリシーがあります。
課題
o ユーザーまたはワークロード ID: 使用済み、User2
o クラウドアプリまたはアクション: Office 365 Exch

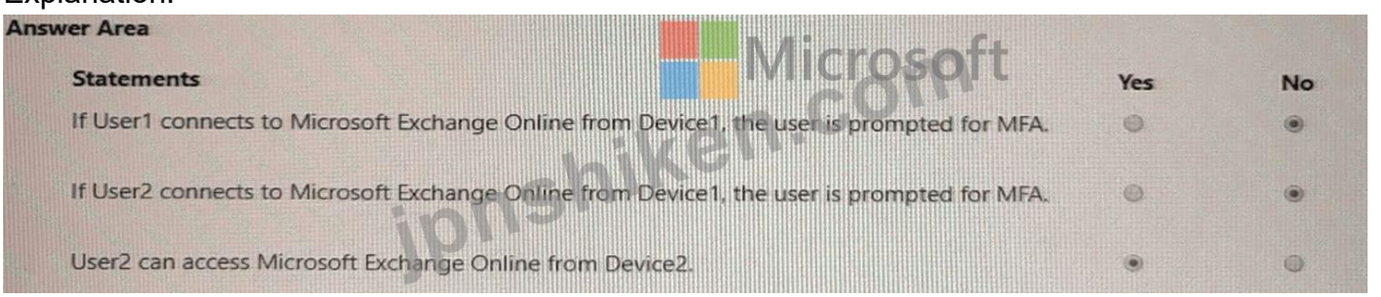
o 条件
デバイスプラットフォーム: Android、iOS
デバイスのフィルター
ルールに一致するデバイス: フィルタリングされたデバイスをポリシーから除外する
ルール構文: device.displayName- "1" を含む
アクセス制御
ブロックアクセスを許可する
以下の各文について、正しい場合は「はい」を選択してください。そうでない場合は「いいえ」を選択してください。



正解:



Explanation:



質問: **94**
iOS デバイスの技術要件を満たす必要があります。
Intune で作成する必要があるオブジェクトはどれですか?
A. コンプライアンスポリシー
B. アプリ保護ポリシー
C. デプロイメントプロファイル
D. デバイス構成プロファイル
正解: **D** (コメントを発表する)
References:
https://docs.microsoft.com/en-us/intune/device-restrictions-configure
https://docs.microsoft.com/en-us/intune/device-restrictions-ios

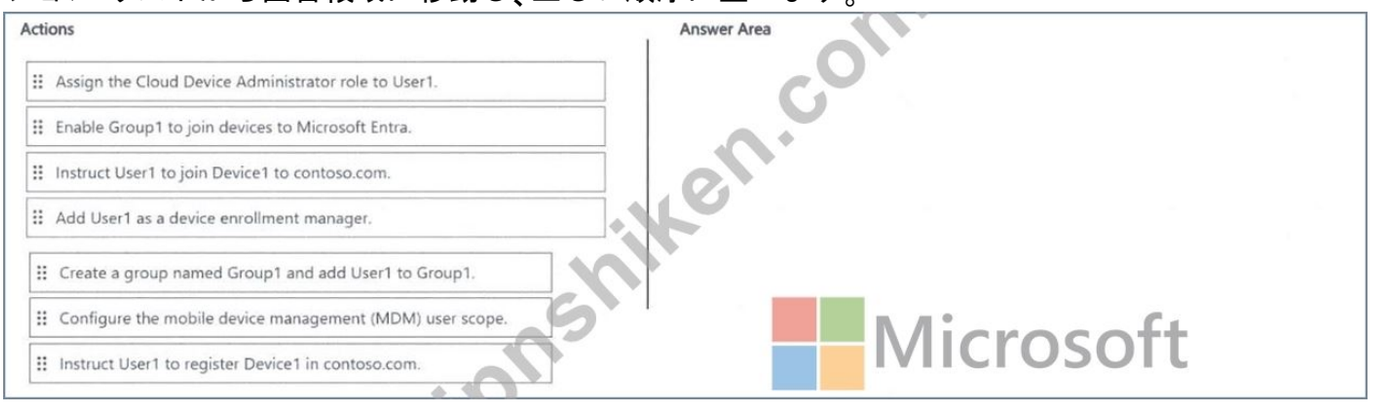
質問: **95**

contoso.com という Microsoft Entra テナントにリンクされた Microsoft 365 E5 サブスクリプションがあります。このサブスクリプションには、User1 というユーザーと、Device1 という新しい Windows 11 デバイスが含まれています。

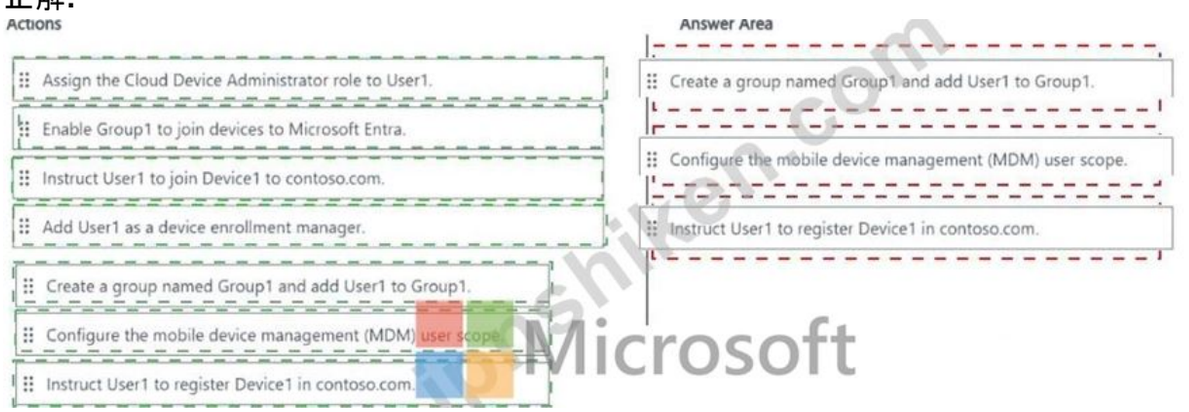
User1 は Device1 を Microsoft Intune に自動的に登録する必要があります。

他のすべてのユーザーが自動登録を使用できないようにする必要があります。

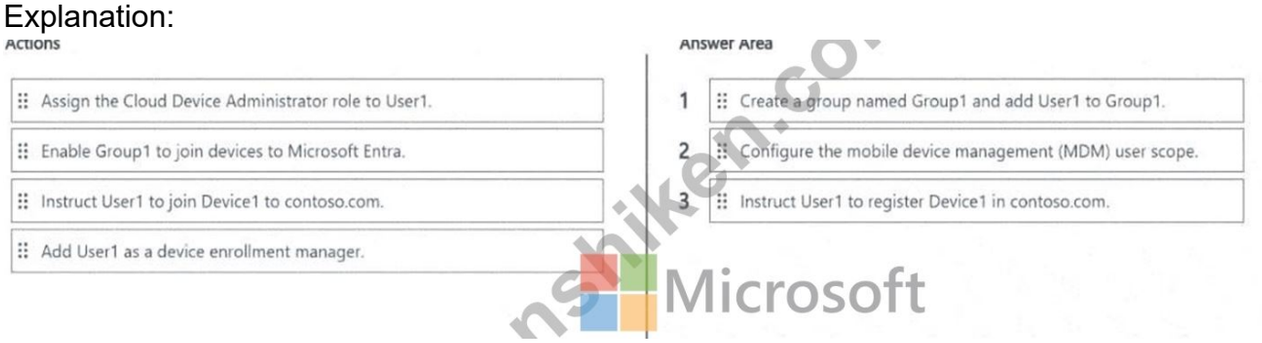
順番に実行する必要がある 3 つのアクションはどれですか。回答するには、適切なアクションをアクション リストから回答領域に移動し、正しい順序に並べます。



正解:



Explanation:



質問: **96**

次の表に示すグループを含む Microsoft Entra テナントがあります。

Name	Members
Group1	User1
Group2	User2

Microsoft Intune は、次の表に示す登録制限で構成されます。

Name	MDM	Personally owned devices	Minimum version	Included groups	Priority
Restriction1	Allow	Block	*None*	Group1	1
Restriction2	Allow	Allow	10.0.22000	Group1 Group2	2

次の表に示すデバイスを購入します。

Name	Operating system
Device1	Windows 11
Device2	Windows 10
Device3	Windows 11

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

注意: 正しい選択ごとに 1 ポイントが加算されます。

Answer Area

Statements	Yes	No
User2 can enroll Device1 by using the Company Portal app.	○	○
User1 can enroll Device2 by using automatic enrollment.	○	○
User1 can enroll Device3 by using the Company Portal app.	○	○

正解:

Answer Area

Statements	Yes	No
User2 can enroll Device1 by using the Company Portal app.	○	○
User1 can enroll Device2 by using automatic enrollment.	○	○
User1 can enroll Device3 by using the Company Portal app.	○	○

Explanation:

Answer Area

Statements	Yes	No
User2 can enroll Device1 by using the Company Portal app.	○	●
User1 can enroll Device2 by using automatic enrollment.	●	○
User1 can enroll Device3 by using the Company Portal app.	○	●

質問: **97**
オンプレミス ネットワークには、Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
VNet1 という名前の仮想ネットワークを含む Azure サブスクリプションがあります。VNet1 には 5 つの仮想マシンが含まれており、オンプレミス ネットワークには接続されていません。
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
Windows 365 Enterprise ライセンスを購入します。
Cloud PC を展開する必要があります。ソリューションは次の要件を満たしている必要があります。
* すべてのユーザーは、制限なくいつでもクラウド PC にアクセスできる必要があります。
* ユーザーは VNet1 上の仮想マシンに接続できる必要があります。
Windows 365 のプロビジョニング ポリシーをどのように構成すればよいでしょうか。答えるには、適切なオプションを正しい設定にドラッグします。各オプションは、1 回、複数回、またはまったく使用しないこともできます。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。
注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

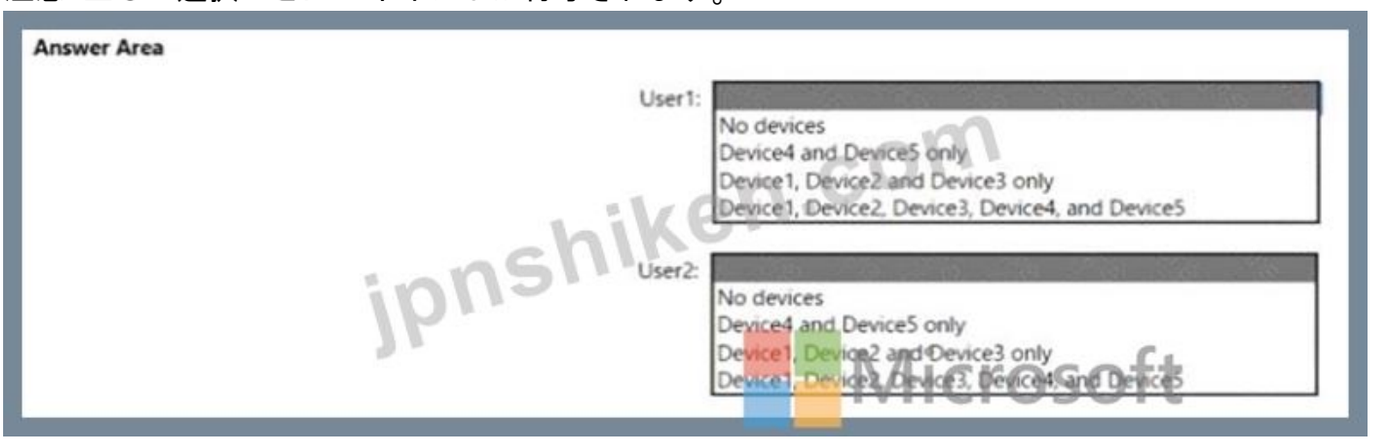
Explanation:

質問: **98**

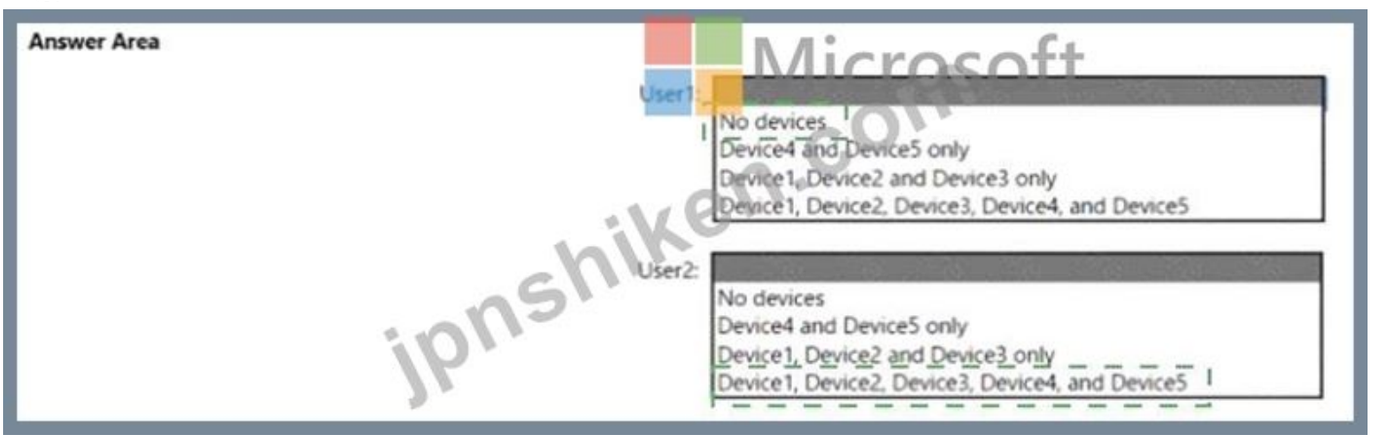
ユーザー1とユーザー2は設定の同期を使用する予定です。

ユーザーはどのデバイスで設定の同期を使用できますか? 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。

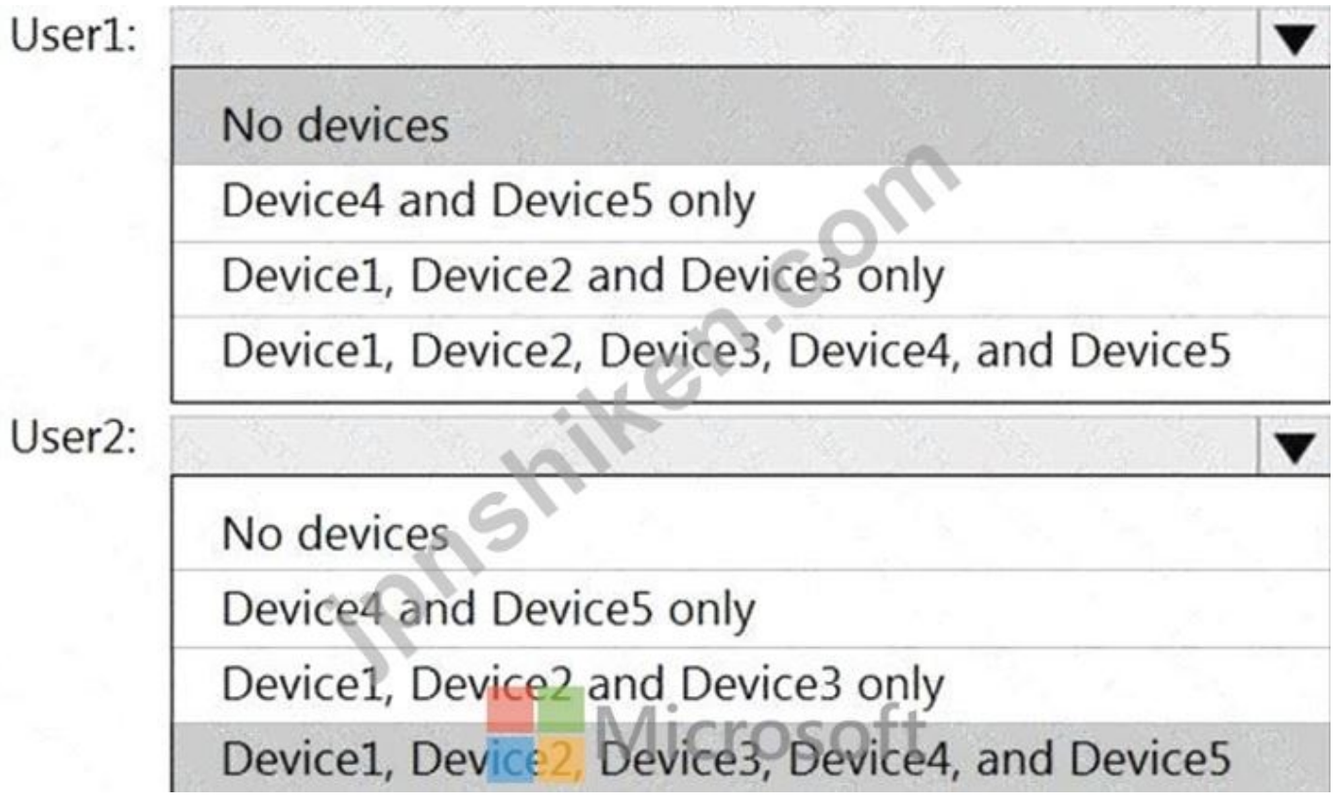
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



Reference:
https://www.jeffgilb.com/managing-local-administrators-with-azure-ad-and-intune/

質問: **99**
Microsoft 365 サブスクリプションをお持ちです。
Windows Autopilot を使用して 25 台の Windows 11 デバイスをプロビジョニングする予定です。
OOBE (Out-of-Box Experience) 設定を構成する必要があります。
Microsoft Intune 管理センターで何を作成する必要がありますか?
A. 登録ステータス ページ (ESP)
B. デプロイメントプロファイル
C. コンプライアンスポリシー
D. PowerShell スクリプト
E. 構成プロファイル
正解: **B (**コメントを発表する**)**
https://learn.microsoft.com/en-us/autopilot/profiles#:~:text=On%20the%20Out%2Dof%2Dbox%20experience%20(OOBE)%20page%2C%20for%20Deployment%20mode%2C%20choose%20one%20of%
20these%20two%20options%3A

質問: **100**
Windows 10 を実行し、Active Directory ドメインに参加しているコンピューターが 200 台あります。
グループ ポリシーを使用して、すべてのコンピューターで Windows リモート管理 (WinRM) を有効にする必要があります。
実行すべき 3 つのアクションはどれですか? それぞれの正解は解決策の一部を示しています。

注意: 正しい選択ごとに 1 ポイントが付与されます。
A. リモート シェル アクセスを許可する設定を有効にします。
B. WinRM によるリモート サーバー管理を許可する設定を有効にします。
C. Windows リモート管理 (WS-Management) サービスのスタートアップの種類を自動に設定します。
D. Windows Defender ファイアウォールの 受信リモート デスクトップ例外を許可する」設定を有効にします。
E. リモートレジストリサービスのスタートアップの種類を自動に設定する
F. Windows Defender ファイアウォールを有効にします: 受信リモート管理例外設定を許可します。
正解**: (**正解を表示します**)**
To enable WinRM on domain computers using Group Policy, you need to perform the following actions:
Enable the Allow remote server management through WinRM setting under Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service. This setting allows you to specify the IP address ranges that can connect to the WinRM service.
Set the Startup Type of the Windows Remote Management (WS-Management) service to Automatic under Computer Configuration > Preferences > Control Panel Settings > Services. This setting ensures that the WinRM service starts automatically on the computers.
Enable the Windows Defender Firewall: Allow inbound remote administration exception setting under Computer Configuration > Policies > Security Settings > Windows Firewall and Advanced Security > Windows Firewall and Advanced Security > Inbound Rules. This setting creates a firewall rule that allows incoming TCP connections on port 5985 for WinRM. References: How to Enable WinRM via Group Policy, Installation and configuration for Windows Remote Management

質問**: 101**
10 台の Android Enterprise デバイスを含む Microsoft 365 E5 サブスクリプションがあります。各デバイスには企業所有の仕事用プロファイルがあり、Microsoft Intune に登録されています。
キオスク モードで単一のアプリを実行するようにデバイスを構成する必要があります。
デバイス制限プロファイルでどの構成設定を変更する必要がありますか?
A. 一般
B. ユーザーとアカウント
C. システムセキュリティ
D. デバイスエクスペリエンス
正解**: (**正解を表示します**)**
To configure the devices to run a single app in kiosk mode, you need to modify the Device experience settings in the device restrictions profile. You can specify the app package name and activity name for the app that you want to run in kiosk mode. References:
https://docs.microsoft.com/en-us/mem/intune/configuration
/device-restrictions-android-for-work#device-experience

質問: **102**
Microsoft Intune に登録された Windows 11 デバイスを含む Microsoft 365 サブスクリプションがあります。
重要なセキュリティ パッチがデバイスにインストールされているかどうかを識別するには、デバイス クエリを使用する必要があります。
どのテーブルをターゲットにすべきでしょうか?
A. システム情報
B. ファイル情報
C. OSバージョン
D. Windowsレジストリ
E. WindowsQfe
正解: **E (**コメントを発表する**)**

質問: **103**
Active Directory に参加し、Microsoft Intune に登録されている Device! という名前の Windows 10 デバイスがあります。
Device1 はグループ ポリシーと Intune を使用して管理されます。
Intune 設定がグループ ポリシー設定を上書きす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. デバイス構成プロファイル
B. デバイスコンプライアンスポリシー
C. MDM セキュリティ ベースライン プロファイル
D. グループ ポリシー オブジェクト (GPO)
正解: **A (**コメントを発表する**)**
A device configuration profile is a collection of settings that can be applied to devices enrolled in Microsoft Intune. You can use device configuration profiles to manage Windows 10 devices that are joined to Active Directory and enrolled in Intune. To ensure that the Intune settings override the Group Policy settings, you need to enable the policy CSP setting called MDMWinsOverGP in the device configuration profile. This setting will give precedence to the MDM policy over any conflicting Group Policy settings. References: [Use policy CSP settings to create custom device configuration profiles]

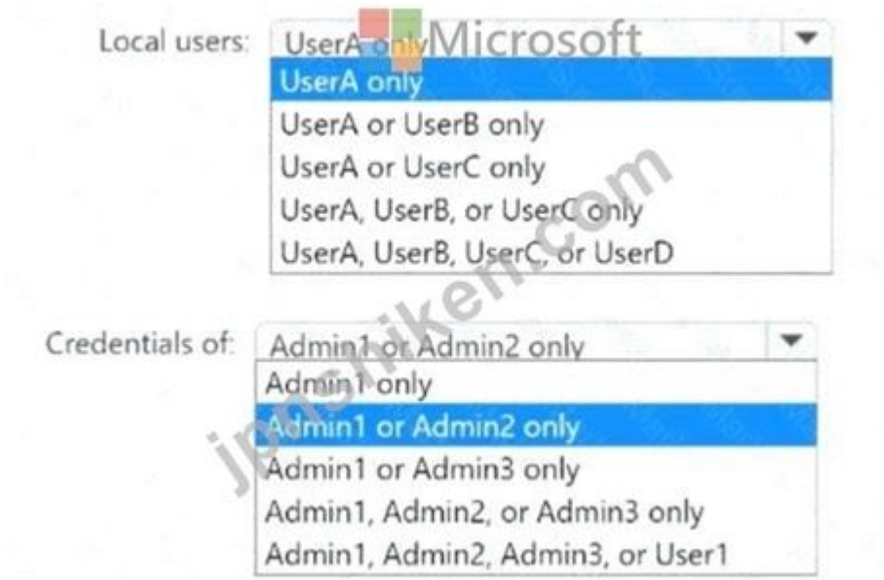
質問: **104**
次の表に示すユーザーを含む contoso.com という名前の Microsoft Entra テナントがあります。

Name	Role
Admin1	Global Administrator
Admin2	Cloud Device Administrator
Admin3	Directory Writer
User1	None

テナントには、Windows 11 を実行する Computer1 という名前のスタンドアロン ワークグループ コンピューターが含まれています。Computer1 には、次の表に示すローカル ユーザーが含まれています。

Name	Member of
UserA	Administrators
UserB	Power Users
UserC	Device Owners
UserD	Users

Computer1 を contoso.com に参加させる必要があります。
どのローカル ユーザーが Computer1 を contoso.com に参加させられるでしょうか。また、どのユーザーの Microsoft Entra 資格情報を使用できますか。回答するには、回答領域で適切なオプションを選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:

質問: **105**
Microsoft Intune に登録されている 500 台の macOS デバイスを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Defender for Endpoint ウイルス対策ポリシーを macOS デバイスに適用できることを確認する必要があります。ソリューションでは、管理作業を最小限に抑える必要があります。
何をすべきでしょうか?
A. macOS デバイスを Microsoft Purview コンプライアンス ポータルにオンボードします。
B. Microsoft Intune 管理センターから、セキュリティ ベースラインを作成します。
C. macOS デバイスに Defender for Endpoint をインストールします。
D. Microsoft Intune 管理センターから構成プロファイルを作成します。
正解: **(**正解を表示します**)**
To apply Microsoft Defender for Endpoint antivirus policies to the macOS devices, you need to install Defender for Endpoint on the devices. You can use Intune to deploy a script that installs Defender for Endpoint on macOS devices. After installation, you can use Intune to create and assign antivirus policies to the devices. References: https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft- defender-atp/mac-install-with-intune

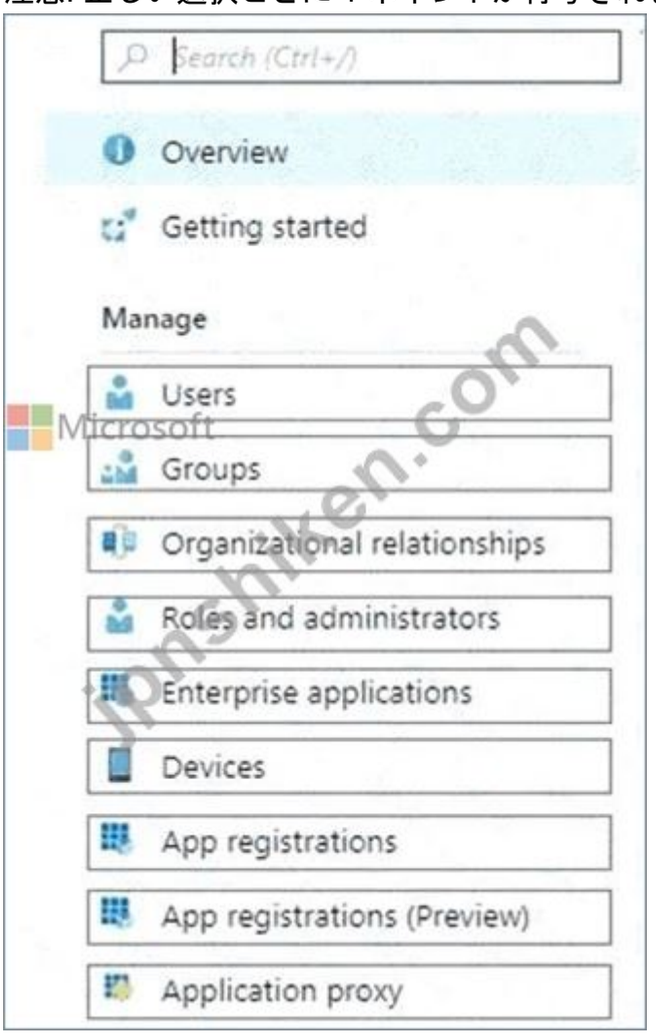
質問: **106**
Azure サブスクリプションをお持ちです。
デバイス 1 という名前のオンプレミスの Windows 11 デバイスがあります。
Azure Monitor を使用して Device1 を監視する予定です。
サブスクリプションに DCR1 という名前のデータ収集ルール (DCR) を作成します。
DCR1 を何に関連付けるべきでしょうか?
A. Azure ネットワーク ウォッチャー
B. デバイス1
C. Log Analytics ワークスペース
D. 監視対象オブジェクト
正解: **(**正解を表示します**)**
To monitor Device1 by using Azure Monitor, you should associate DCR1 with Device1. A data collection rule (DCR) defines the data collection process in Azure Monitor, such as what data to collect, how to transform it, and where to send it. A DCR can be associated with multiple virtual

machines and specify different data sources, such as Azure Monitor Agent, custom logs, or Azure Event Hubs1. To associate a DCR with a virtual machine, you need to install the Azure Monitor Agent on the machine and then select the DCR from the list of available rules2. You can also use Azure Policy to automatically install the agent and associate a DCR with any virtual machines or virtual machine scale sets as they are created in your subscription3.
The other options are not correct for this scenario because:
Azure Network Watcher is a service that provides network performance monitoring and diagnostics for Azure resources. It is not related to data collection rules or Azure Monitor4.
A Log Analytics workspace is a destination where you can send the data collected by a data collection rule. It is not an entity that you can associate a DCR with5.
A Monitored Object is not a valid term in the context of Azure Monitor or data collection rules.
References: Data collection rules in Azure Monitor, Configure data collection for Azure Monitor Agent, Use Azure Policy to install Azure Monitor Agent and associate with a DCR, What is Azure Network Watcher?, Log Analytics workspaces in Azure Monitor

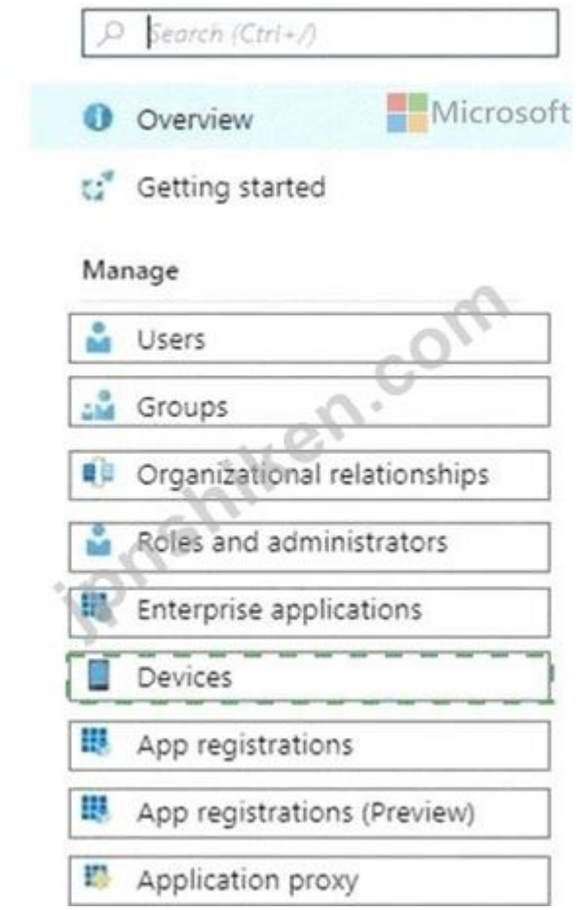
質問: **107**
会社では、Azure AD、Microsoft 365、Microsoft Intune、Azure Information Protection を実装しています。会社のセキュリティ ポリシーには、次のように記載されています。
* 個人用デバイスを Intune に登録する必要はありません。
* ユーザーは、企業の電子メール データにアクセスする前に PIN を使用して認証する必要があります。
* ユーザーは個人の iOS および Android デバイスを使用して企業のクラウド サービスにアクセスできます。
* ユーザーが企業の電子メールデータを Microsoft OneDrive for Business 以外のクラウド ストレージ サービスにコピーできないようにする必要があります。
セキュリティ ポリシーを適用するにはソリューションを構成する必要があります。
何を作ればよいでしょうか?
A. Microsoft Purview コンプライアンス ポータルからのデータ損失防止 (DIP) ポリシー
B. Microsoft Intune 管理センターからのデバイス構成プロファイル
C. Microsoft Intune 管理センターからのアプリ保護ポリシー
D. Microsoft Purview コンプライアンス ポータルからの内部リスク管理ポリシー
正解: **C** (コメントを発表する)

質問: **108**
Microsoft Intune を含む Microsoft 365 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、企業所有の完全に管理された Android Enterprise デバイスが含まれています。
Profile1 という名前のデバイス制限プロファイル タイプを持つ構成プロファイルを展開する予定です。Profile1 は、システム更新のメンテナンス ウィンドウを割り当てます。
Profile1 の構成設定から何を構成する必要がありますか?
A. 接続性
B. 一般
C. デバイスエクスペリエンス
D. 電源設定
正解: **(正解を表示します)**

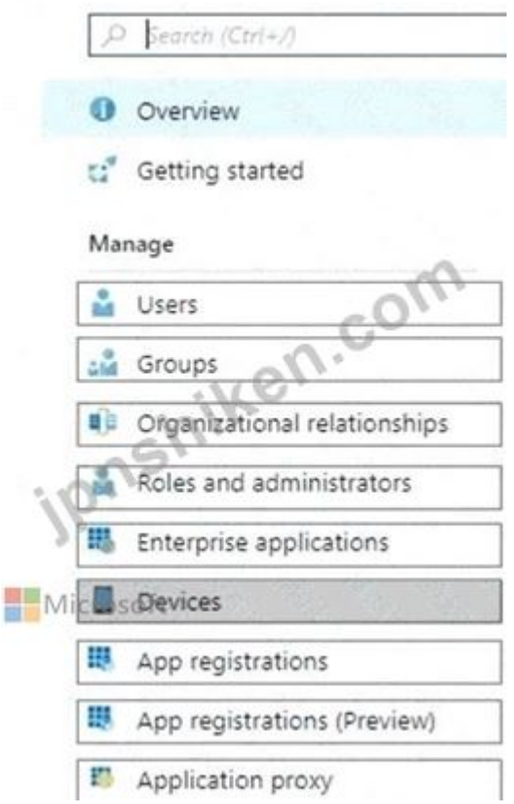
質問: **109**
Windows AutoPilot の技術要件を満たす必要があります。
Azure Active Directory ブレードから構成する必要がある 2 つの設定はどれですか? 回答するには、回答領域で適切な設定を選択します。
注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:



Explanation:



References:

https://docs.microsoft.com/en-us/windows/deployment/windows-autopilot/windows-autopilot-reset

質問: **110**
会社には、複数の Windows 10 デバイスを含む contoso.com という名前の Azure AD テナントがあります。
新しい Windows 10 デバイスを contoso.com に参加させると、ユーザーは 4 桁の PIN を設定するように求められます。
ユーザーが Windows 10 デバイスを contoso.com に参加させるときに、6 桁の PIN を設定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。
解決策: Microsoft Entra 管理センターから、自動モバイル デバイス管理 (MDM) 登録を構成します。Microsoft Intune 管理センターから、デバイス制限プロファイルを作成して割り当てます。
これは目標を満たしていますか?
A. いいえ
B. はい
正解: **(**正解を表示します**)**

質問: **111**
Windows 11 Pro を実行するコンピューターがあります。コンピューターは Azure AD に参加し、Microsoft Intune に登録されています。コンピューターを Windows 11 Enterprise にアップグレードする必要があります。Intune で何を構成する必要がありますか?
A. デバイス登録ポリシー
B. デバイス構成プロファイル
C. デバイスのクリーンアップルール
D. デバイスコンプライアンスポリシー
正解: **(**正解を表示します**)**

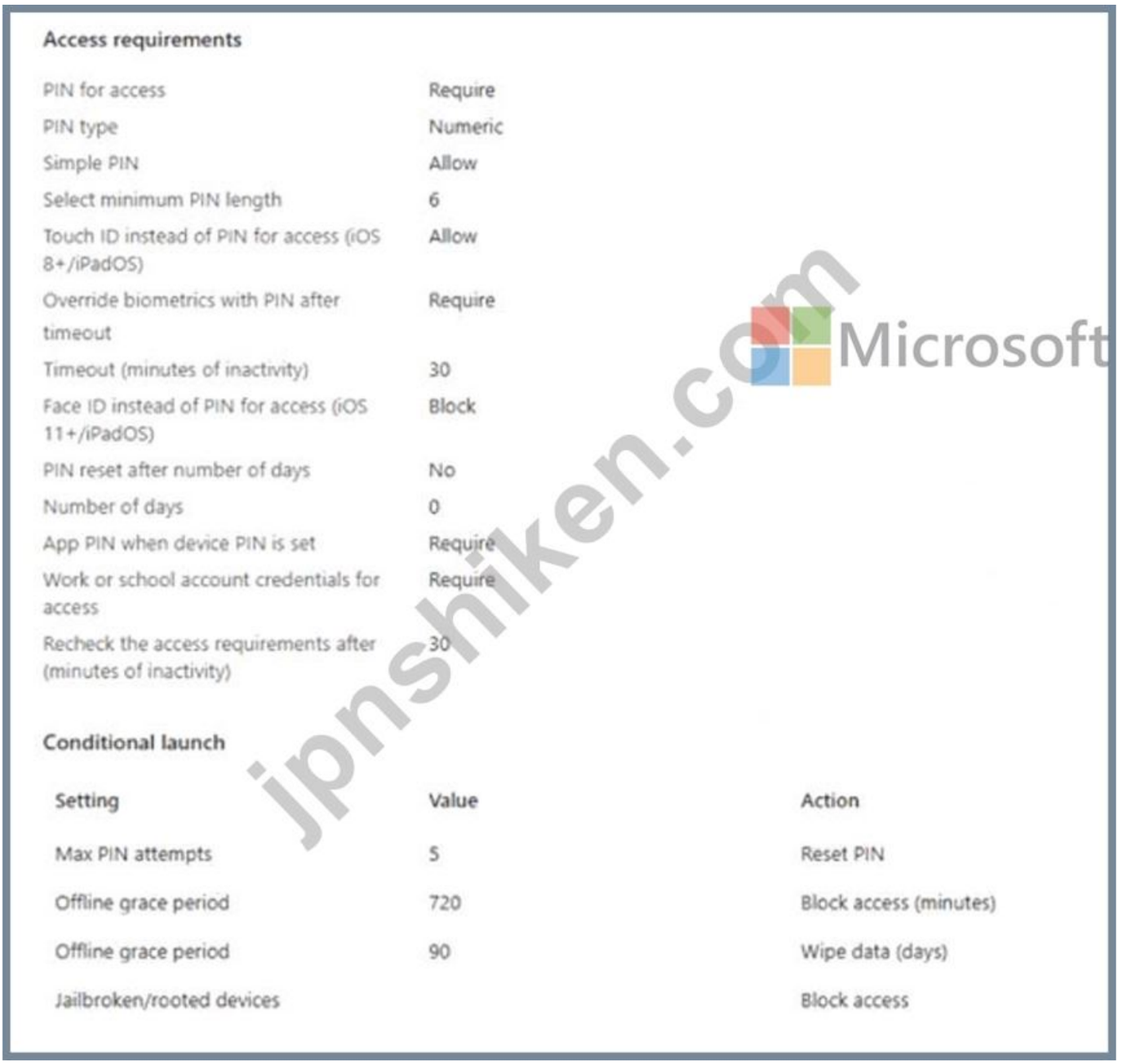
質問: **112**
Microsoft Deployment Toolkit (MDT) がインストールされています。
参照コンピューターにWindows 11をインストールしてカスタマイズします
参照コンピューターのイメージをキャプチャし、そのイメージを複数のコンピューターに展開できることを確認する必要があります。
イメージをキャプチャする前に実行するコマンドはどれですか?
A. 嫌悪感
B. wpeinit
C. システム準備
D. bcdedit
正解: **(**正解を表示します**)**
To capture an image of a reference computer and make it ready for deployment to multiple computers, you need to run the sysprep command with the /generalize option. This option removes all unique system information from the Windows installation, such as the computer name, security identifier (SID), and driver cache. The other commands are not used for this purpose. References: Sysprep (Generalize) a Windows installation

質問: **113**

Microsoft 365 サブスクリプションをお持ちです。

デバイスを管理するには、Microsoft Intune Suite を使用します。

次の図に示すような iOS アプリ保護ポリシーがあります。



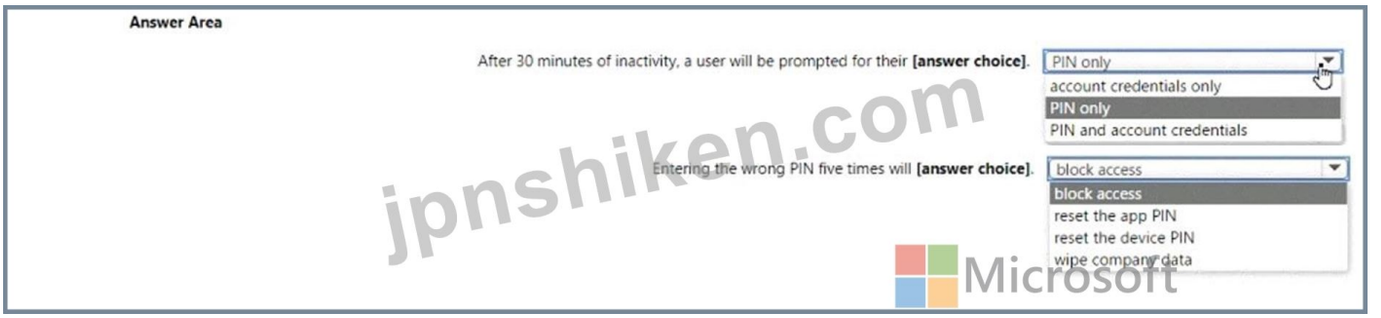
Access requirements

PIN for access	Require
PIN type	Numeric
Simple PIN	Allow
Select minimum PIN length	6
Touch ID instead of PIN for access (iOS 8+/iPadOS)	Allow
Override biometrics with PIN after timeout	Require
Timeout (minutes of inactivity)	30
Face ID instead of PIN for access (iOS 11+/iPadOS)	Block
PIN reset after number of days	No
Number of days	0
App PIN when device PIN is set	Require
Work or school account credentials for access	Require
Recheck the access requirements after (minutes of inactivity)	30

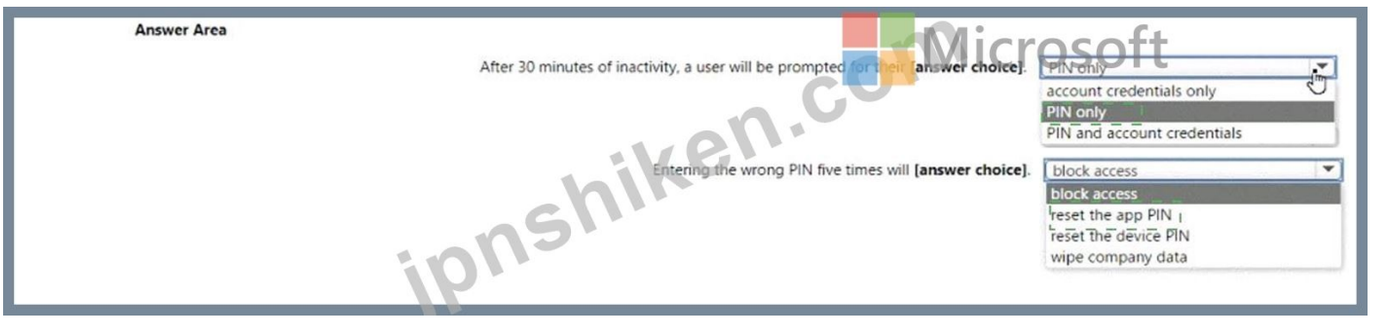
Conditional launch

Setting	Value	Action
Max PIN attempts	5	Reset PIN
Offline grace period	720	Block access (minutes)
Offline grace period	90	Wipe data (days)
Jailbroken/rooted devices		Block access

ドロップダウンメニューを使用して、図に示された情報に基づいて各文を完成させる回答の選択肢を選択します。注: 正しい選択はそれぞれ1ポイントです。



正解:



Explanation:

Box 1 = PIN only

Box 2 = reset the PIN app

iOS/iPadOS app protection policy settings - Microsoft Intune | Microsoft Learn

https://learn.microsoft.com/en- us/mem/intune/apps/app-protection-policy-settings-ios

質問: **114**

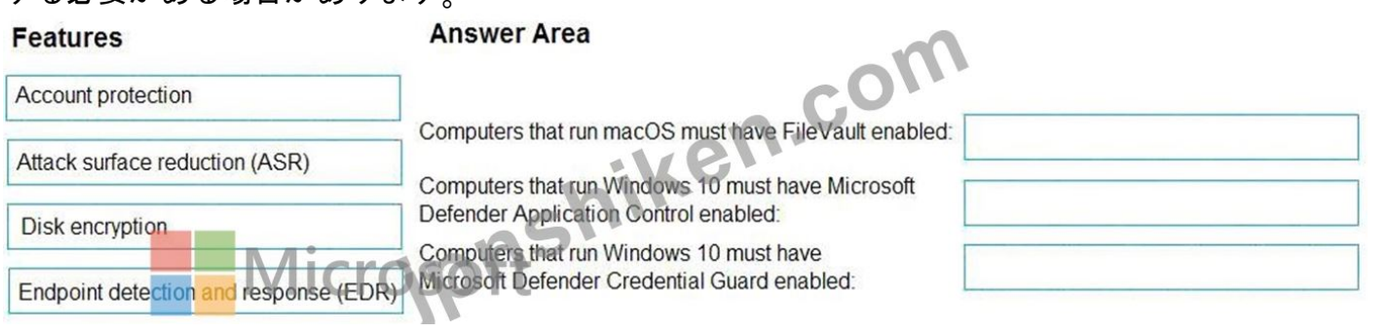
-

Microsoft Intune に登録されているデバイスを含む Microsoft 365 サブスクリプションがあります。

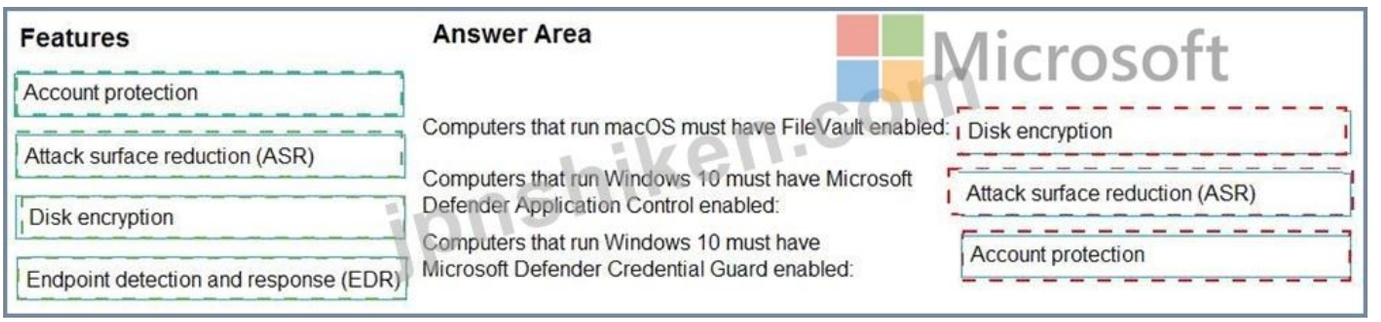
次の要件を適用するには、エンドポイント セキュリティ ポリシーを作成する必要があります。

* macOS を実行するコンピュータでは、FileVault が有効になっている必要があります。
* Windows 10 を実行するコンピューターでは、Microsoft Defender Credential Guard が有効になっている必要があります。
* Windows 10 を実行するコンピューターでは、Microsoft Defender アプリケーション制御が有効になっている必要があります。

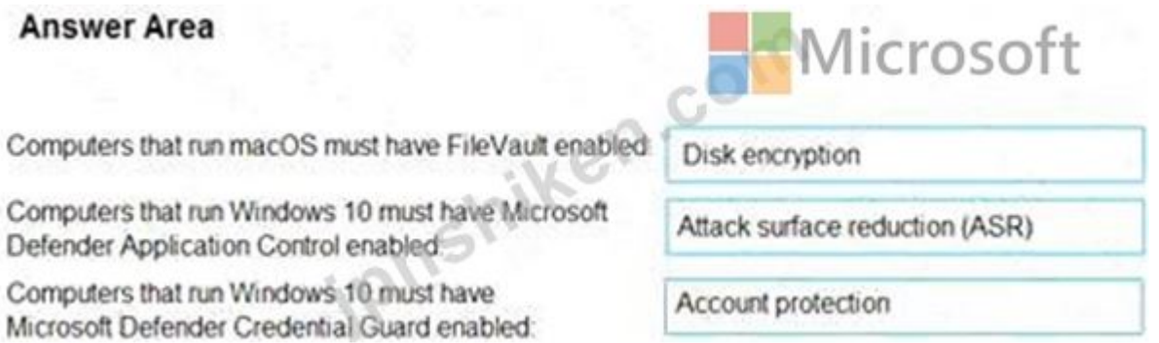
各要件に対してどのエンドポイント セキュリティ機能を使用する必要がありますか? 回答するには、適切な機能を正しい要件にドラッグします。各機能は、1 回、複数回、またはまったく使用されない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。



正解:



Explanation:



Disk Encryption

ASR - Ref https://learn.microsoft.com/en-us/mem/intune/protect/endpoint-security-asr-policy#:~:text=Application%20control%20%2D%20Application,Constrained%20Language%20Mode.

Account Protection - Ref https://learn.microsoft.com/en-us/windows/security/identity-protection/credential- guard/configure?tabs=intune#:~:text=You%20can%20also%20configure%20Credential%20Guard%20by%20using%20an%20account%20protection%20profile%20in%20endpoint%20security.

質問: **115**

Server! というオンプレミス サーバーがあり、MDT1 という Microsoft Deployment Toolkit (MDT) 展開共有をホストしています。MDT1 がマルチキャスト展開をサポートしていることを確認する必要があります。Server1 に何をインストールすればよいでしょうか。

A. Windows Server 更新サービス (WSUS)

B. Windows 展開サービス (WDS)

C. マルチパスI/O (MPIO)

D. マルチポイントコネクタ

正解: **B (**コメントを発表する**)**

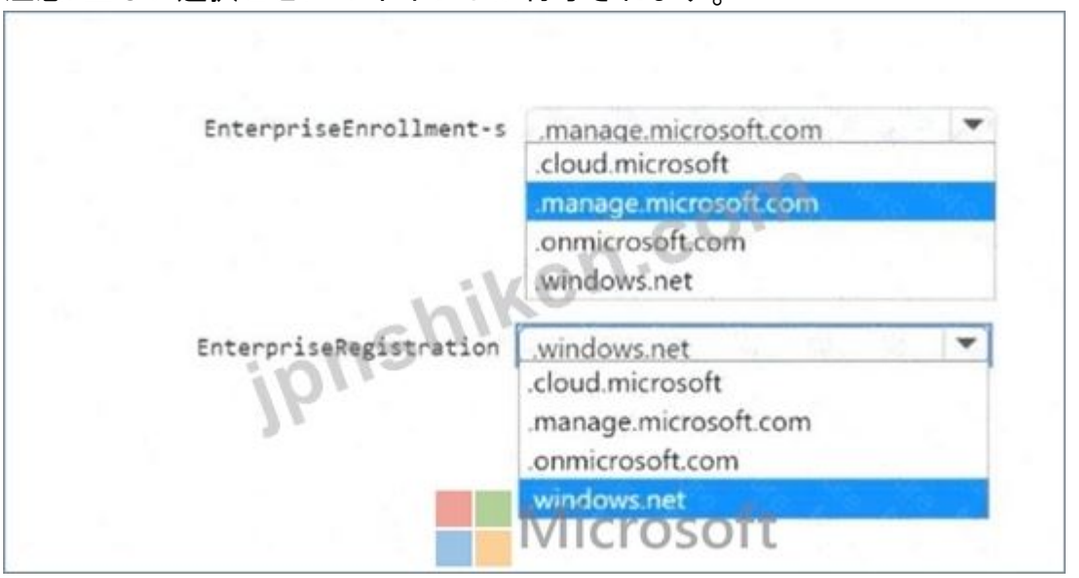
質問: **116**

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

Microsoft Intune を使用してデバイスを管理します。自動 Intune 登録は無効になっています。

ユーザーからは、デバイスの登録時にモバイル デバイス管理 (MDM) サーバーのアドレスを入力する必要があるという報告があります。

デバイスの登録時のユーザーの操作を減らすために、次の CNAME DNS ホスト名レコードを作成する予定です。
EnterpriseEnrollment.contoso.com
EnterpriseRegistration.contoso.com
登録要求を Intune サーバーにリダイレクトするには、各 CNAME レコードの完全修飾ドメイン名 (FQDN) を構成する必要があります。
各 FQDN をどのように構成すればよいですか? 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。



正解:

Explanation:

質問: **117**

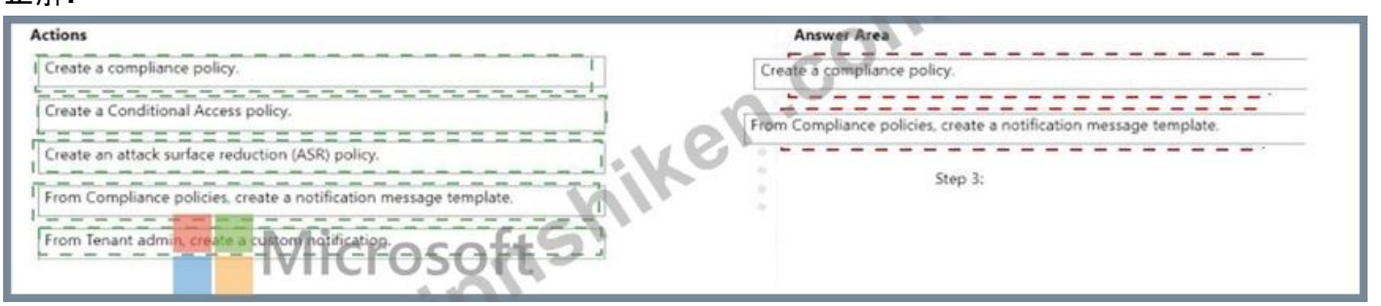
Microsoft Intune が含まれる Microsoft 365 ES サブスクリプションをお持ちです。

サブスクリプションには、Intune に登録され、個人所有の仕事用プロファイルを持つ Android Enterprise デバイスが含まれています。すべての Android デバイスは、Group1 というグループのメンバーです。

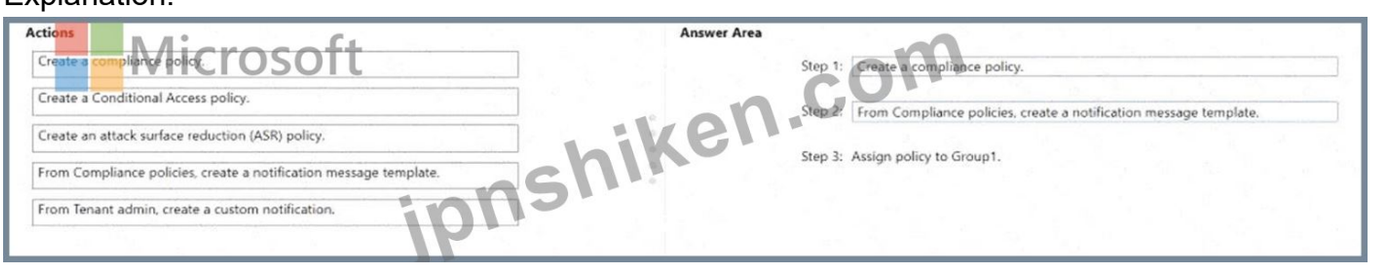
Android デバイスに最新のセキュリティ プロバイダーがない場合、エンド ユーザーと Intune 管理者が電子メール メッセージを受信するようにする必要があります。Microsoft Intune 管理センターからどのアクションを順番に実行する必要がありますか。回答するには、適切なアクションを正しい順序にドラッグします。各アクションは、1 回、複数回、またはまったく使用しない場合があります。コンテンツを表示するには、ペイン間の分割バーをドラッグするか、スクロールする必要がある場合があります。

注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:



Explanation:



質問: **118**

Microsoft Intune を使用する Microsoft 365 サブスクリプションがあります。

Windows Autopilot を使用して 25 台の Windows 11 デバイスをプロビジョニングする予定です。

デバイスのプロビジョニング中に次の要件を満たす必要があります。

* アプリとプロファイルの展開の進行状況を表示します。
* デバイスを Azure AD に参加させます。

各要件を満たすには、何を構成する必要がありますか? 回答するには、適切な設定を正しい要件にドラッグします。各設定は、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。

注意: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-status

質問: **119**

ネットワークにはオンプレミスの Active Directory ドメイン サービス (AD DS) ドメインが含まれています。
Microsoft Intune が含まれ、AD DS ドメインと同期する Microsoft 365 E5 サブスクリプションがあります。
Windows ローカル管理者パスワード ソリューション (Windows LAPS) が Microsoft Entra ID で有効になっています。
サブスクリプションには、次の表に示すカスタム ロールがあります。

Name	Permission
Role1	microsoft.directory/deviceLocalCredentials/password/read
Role2	microsoft.directory/deviceLocalCredentials/standard/read
Role3	microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceLocalCredentials/password/read

Microsoft Entra には、次の表に示すユーザーが含まれます。

Name	Built-in role	Assigned custom roles
User1	Helpdesk Administrator	Role1
User2	Security Reader	Role2
User3	*None*	Role3

次の表に示すデバイスがあります。

Name	Domain Join Type
Device1	Joined to AD DS
Device2	Microsoft Entra hybrid joined
Device3	Microsoft Entra joined

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

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	○	○
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	○
User3 can use Microsoft Entra to read the local administrator password of Device3.	○	○

正解:

Answer Area

Statements	Yes	No
User1 can use Microsoft Entra to read the local administrator password of Device1.	○	○
User2 can use Microsoft Entra to read the local administrator password of Device2.	○	○
User3 can use Microsoft Entra to read the local administrator password of Device3.	○	○

Explanation:

質問**: 120**

Windows 10 を実行する 1,000 台のコンピューターを管理しています。すべてのコンピューターは Microsoft Intune に登録されています。Intune を使用して、コンピューターのサービス チャネル設定を管理します。

コンピュータのサービス状態を確認する必要があります。

何をすべきでしょうか?

A. ソフトウェア更新から、更新リングごとの展開状態を表示します。

B. ソフトウェア更新から監査ログを表示します。

C. デバイス構成 - プロファイルから、デバイスのステータスを表示します。

D. デバイス コンプライアンス」から、デバイス コンプライアンスを表示します。

正解**: A (**コメントを発表する**)**

https://learn.microsoft.com/en-us/mem/intune/protect/windows-update-reports#reports-for-update-rings-for- windows-10-and-later-policy:~:text=IncompatibleServicingChannel

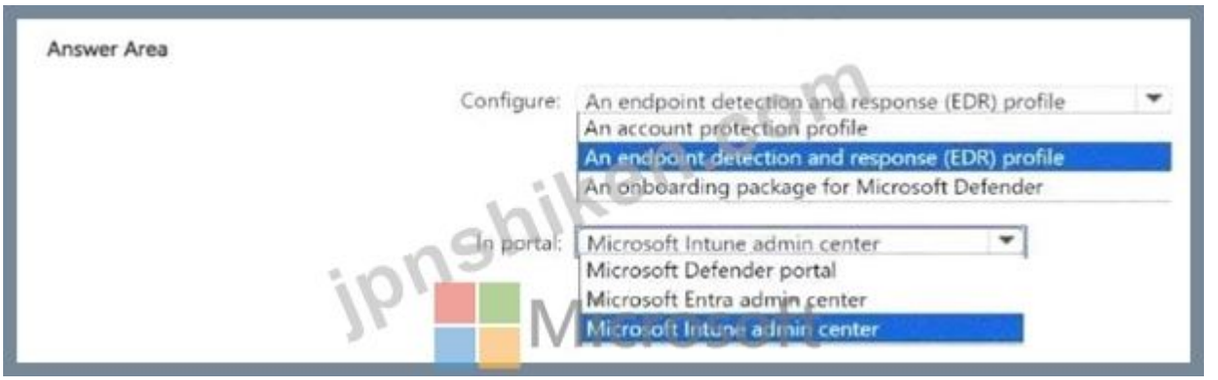
質問**: 121**

Microsoft Intune と Microsoft Defender for Endpoint が含まれる Microsoft 365 サブスクリプションをお持ちです。

ユーザーは Windows 11 を実行するデバイスを所有しています。

Defender for Endpoint から Intune への接続を展開します。

デバイスが Intune に登録されると、そのデバイスが Defender for Endpoint に自動的にオンボードされるようにする必要があります。何を構成して、どのポータルを使用する必要がありますか? 回答するには、回答領域で適切なオプションを選択してください。注: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:

質問: **122**

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

Name	Description
Group1	Azure AD group that contains a user named User1
Group2	Azure AD group that contains iOS devices

iOS デバイスからの Microsoft Exchange Online へのアクセスをブロックする CAPolicy1 という名前の条件付きアクセス ポリシーを作成します。CAPolicy1 を Group1 に割り当てます。

User1 は iOS デバイスから Exchange Online に引き続き接続できることがわかります。
CAPolicy1 が強制されてい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. 新しい利用規約 (TOU) を構成します。
B. CAPolicy1 を Group2 に割り当てます。
C. CAPolicy1 を有効にする
D. CAPolicy1 に条件を追加してデバイスをフィルタリングします。
正解: **(**正解を表示します**)**
Common signals that Conditional Access can take in to account when making a policy decision include the following signals:
* User or group membership
Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
* Device
Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
Use filters for devices to target policies to specific devices like privileged access workstations.
* Etc.
Reference: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

質問: **123**
contoso.com という名前の Azure AD テナントがあります。次の表に示すデバイスがあります。

Name	Platform
Device1	Windows 11
Device2	Windows 10
Device3	iOS
Device4	Ubuntu Linux

Azure AD に参加できるデバイスはどれですか。また、contoso.com に登録できるデバイスはどれですか。回答するには、回答で適切なオプション a を選択します。注: 正しい選択ごとに 1 ポイントが付与されます。

正解:

Explanation:

質問**: 124**

Microsoft Intune を使用する Microsoft 365 E5 サブスクリプションがあります。

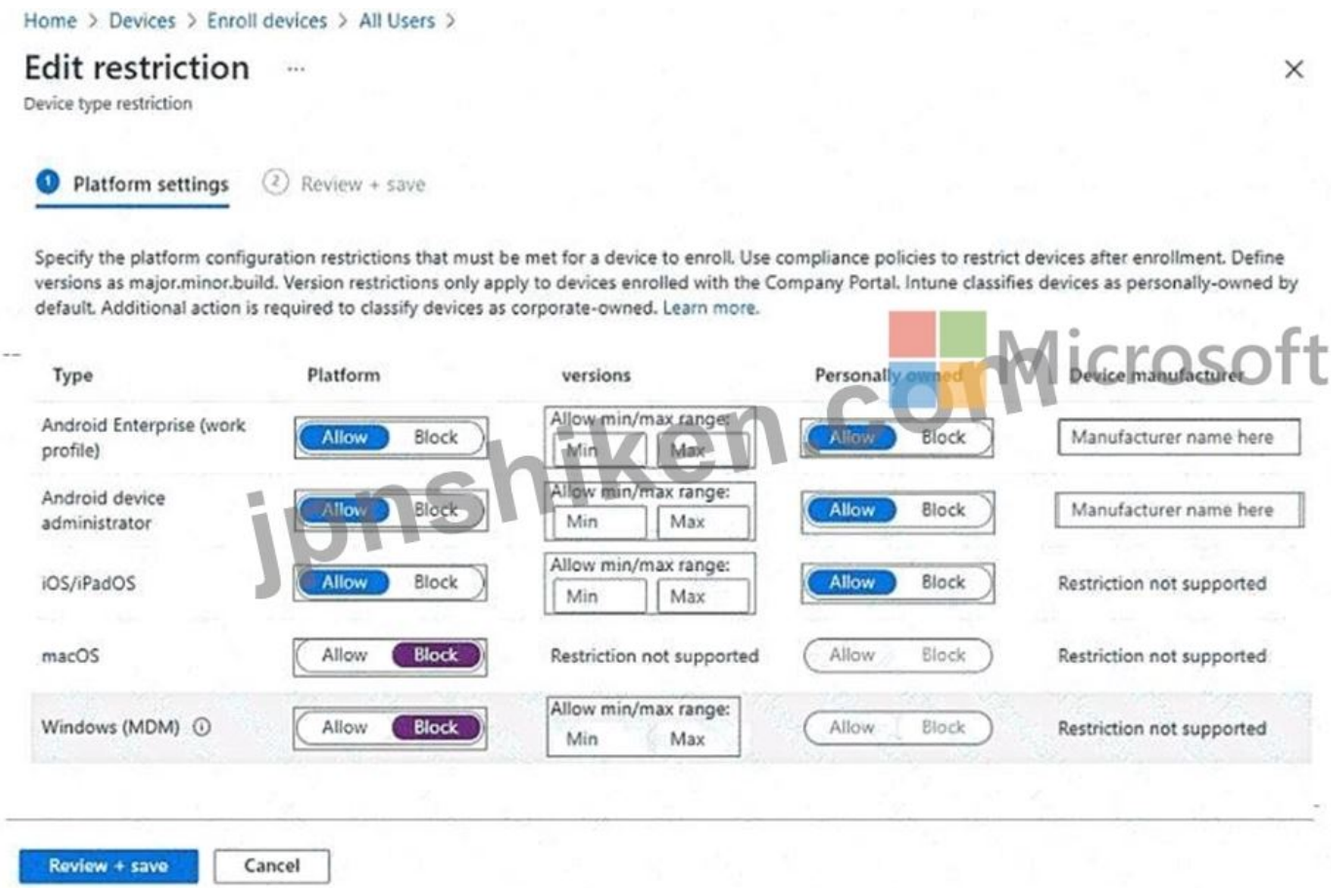
ユーザーが登録できるデバイスを次の要件を満たすものに限る必要があります。

* 仕事用プロファイルの使用をサポートする Android デバイス。

* iOS 16.0 以降を実行する iOS デバイス。

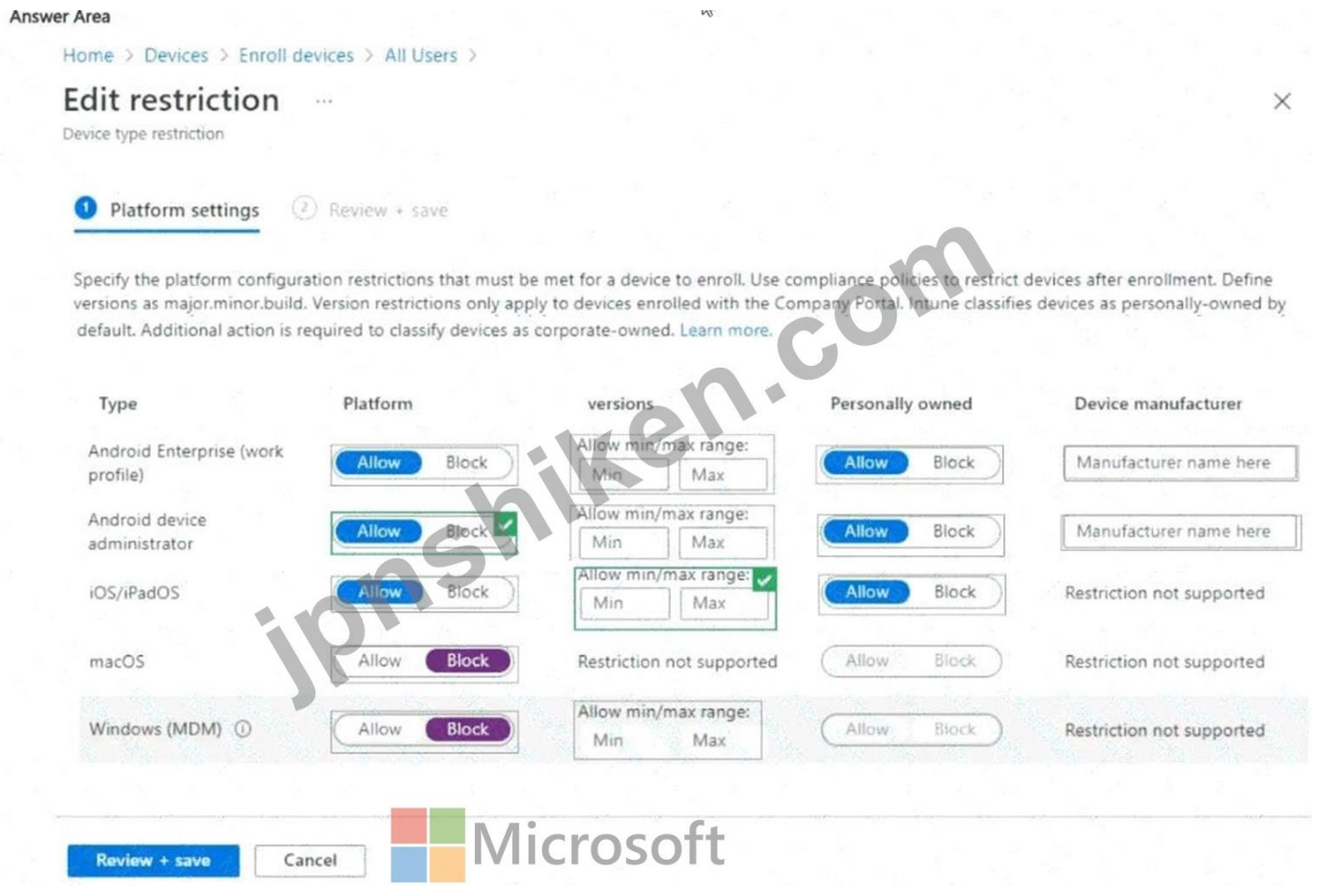
変更する必要がある 2 つの制限はどれですか。回答するには、回答領域で制限を選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:



質問: **125**
Microsoft 365 E5 サブスクリプションをお持ちです。
すべての Windows デバイスは Microsoft Intune に登録されています。
すべてのデバイスにリモート ヘルプ アプリを展開する必要があります。
ソリューションでは管理上の労力を最小限に抑える必要があります。
どのタイプのアプリを展開する必要がありますか?
A. Windows アプリ (Win32)
B. マイクロソフト 365
C. マイクロソフトストア
D. 基幹業務 (LOB)
正解: **(**正解を表示します**)**

質問: **126**
Microsoft 365 サブスクリプションをお持ちです。
次の表に示すように、Microsoft Intune に登録されているデバイスがあります。
Intune を使用してどのデバイスにアプリを展開できますか?
A. デバイス1のみ
B. デバイス1、デバイス2、デバイス3のみ
C. デバイス1とデバイス3のみ
D. デバイス1、デバイス2、デバイス3、デバイス4

E. デバイス1とデバイス2のみ
正解: **(**正解を表示します**)**

質問: **127**
Microsoft 365 サブスクリプションがあります。サブスクリプションには、Windows 11 を実行し、Microsoft Intune に登録されている 500 台のコンピューターが含まれています。毎月のセキュリティ更新プログラムの展開を管理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。
* 品質保証のため、更新プログラムはテスト コンピューターのグループに展開する必要があります。
* 品質保証テストの 15 日後に更新プログラムが自動的に展開される必要があります。
Microsoft Intune 管理センターで何を作成する必要がありますか?
A. 機能更新ポリシー
B. 更新リング
C. セキュリティベースライン
D. デバイス構成プロファイル
正解: **(**正解を表示します**)**

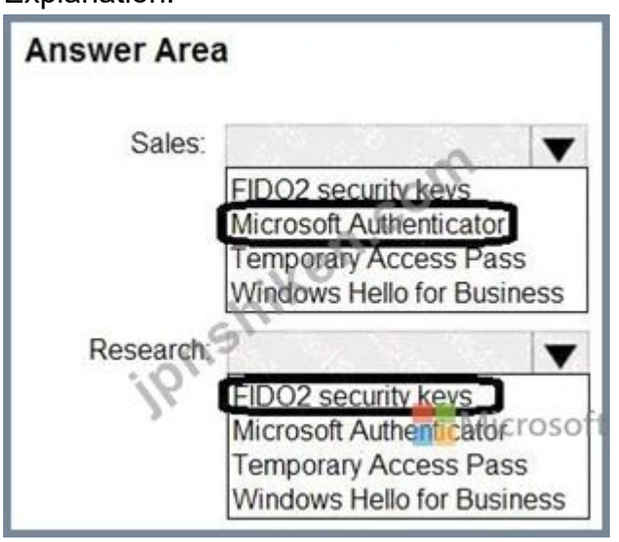
質問: **128**
ネットワークにはcontoso.comというActive Directoryドメインがあります。このドメインには、Windows 10を実行しているComputer1とComputer2という2台のコンピューターが含まれています。Computer1でInvoke-Commandコマンドレットを実行し、Computer1に対していくつかのPowerShellコマンドを実行する必要があります。まず何をすべきでしょうか？
A. Computed で、Computer! をリモート管理ユーザー グループに追加します。
B. Computer1 で、HcK-PSSession コマンドレットを実行します。
C. Active Directory から、計算されたコンピューター アカウントの委任に対して信頼された設定を構成します。
D. 計算時に、Enable-PSRemoting コマンドレットを実行します。
正解: **(**正解を表示します**)**

質問: **129**
Microsoft 365 サブスクリプションをお持ちです。
すべてのユーザーに対してパスワードレス認証を有効にする必要があります。ソリューションは次の要件を満たす必要があります。
* 研究部門のユーザーはモバイル デバイスを使用できないため、別の方法を使用して管理されていない Linux デバイスから認証する必要があります。
* サービスにアクセスするには、営業部門のユーザーが携帯電話を使用して認証する必要があります。
* 管理上の労力を最小限に抑える必要があります。
各部門ではどの認証方法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。

正解:

Explanation:



質問: **130**

Microsoft 365 サブスクリプションがあり、その中に User1 というユーザーが含まれています。User! には、Windows 10/11 Enterprise E3 ライセンスが割り当てられています。デバイスを管理するには、Microsoft Intune Suite を使用します。User1 は次のデバイスをアクティブ化します。

* デバイス1: Windows 11 Enterprise
* デバイス2: Windows 10 Enterprise

* デバイス3: Windows 11 Enterprise
User1 はさらに何台のデバイスをアクティブ化できますか?
A. 2
B. 3
C. 7
D. 8
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/windows/deployment/windows-subscription-activation#licenses

質問: **131**
ネットワークには Active Directory ドメインが含まれています。ドメインには Windows 11 を実行するコンピューターが 1,000 台含まれています。
すべてのコンピューターのリモート デスクトップ設定を構成する必要があります。ソリューションは次の要件を満たしている必要があります。
* クリップボードの内容の共有を防止します。
* ユーザーがネットワーク レベル認証 (NLA) を使用して認証されていることを確認します。
グループ ポリシー管理エディターのどの 2 つのノードを使用する必要がありますか? 回答するには、回答で適切なノード (a) を選択します。注: 正しい選択ごとに 1 ポイントが付与されます。

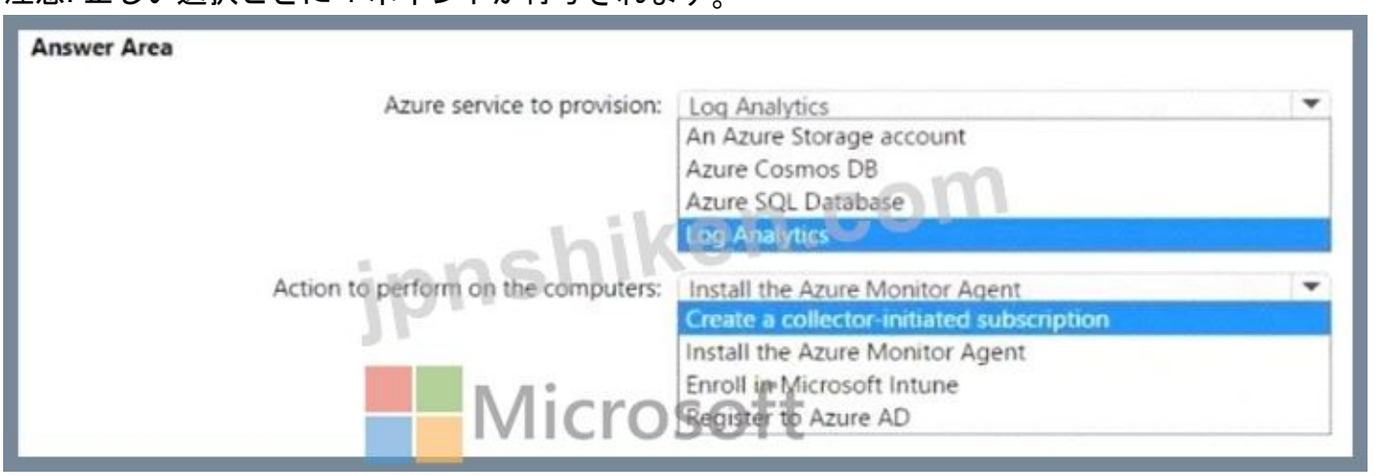
正解:

Explanation:

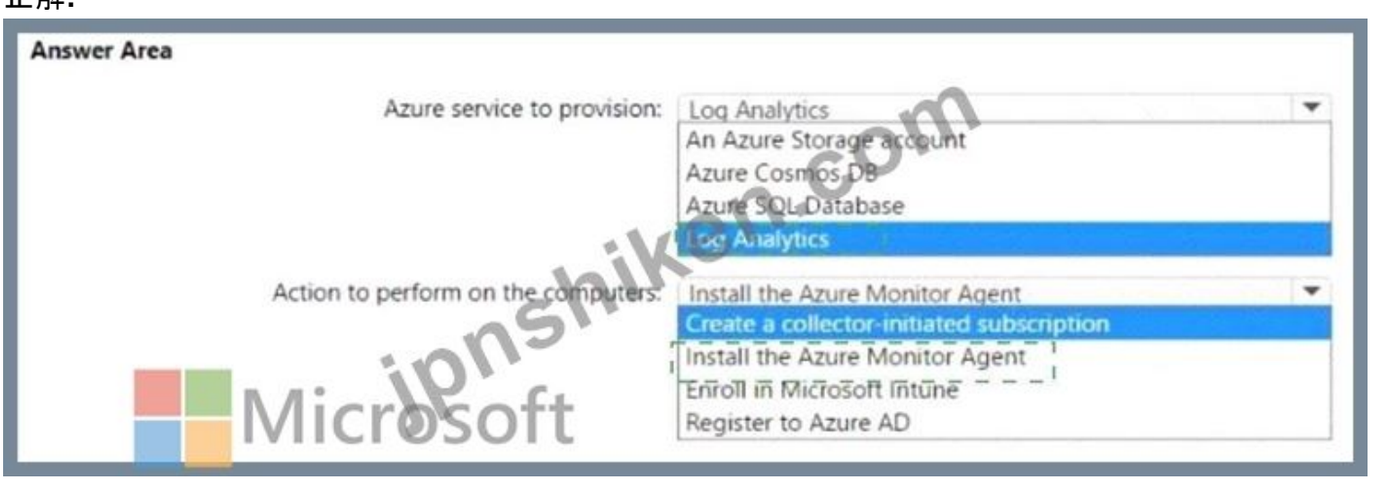
Device and Resource Re-direct
Security

質問: **132**
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
Windows 11 デバイスを管理するには、Microsoft Intune を使用します。
ユーザーに番号の一致を要求するパスワードレス認証を実装する必要があります。どの認証方法を使用すればよいですか?
A. FI002 セキュリティ キー
B. テキストメッセージ
C. 音声通話
D. Microsoft 認証システム
正解: **(**正解を表示します**)**

質問: **133**
Windows 10 を実行し、Active Directory ドメインのメンバーであるコンピューターが 1,000 台あります。
コンピューターから Azure へのイベント トグをキャプチャ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。



正解:



Explanation:

質問: **134**

どのユーザーが Device6 を Intune に登録できますか?

A. ユーザー4とユーザー2のみ

B. ユーザー1、ユーザー2、ユーザー3、ユーザー4

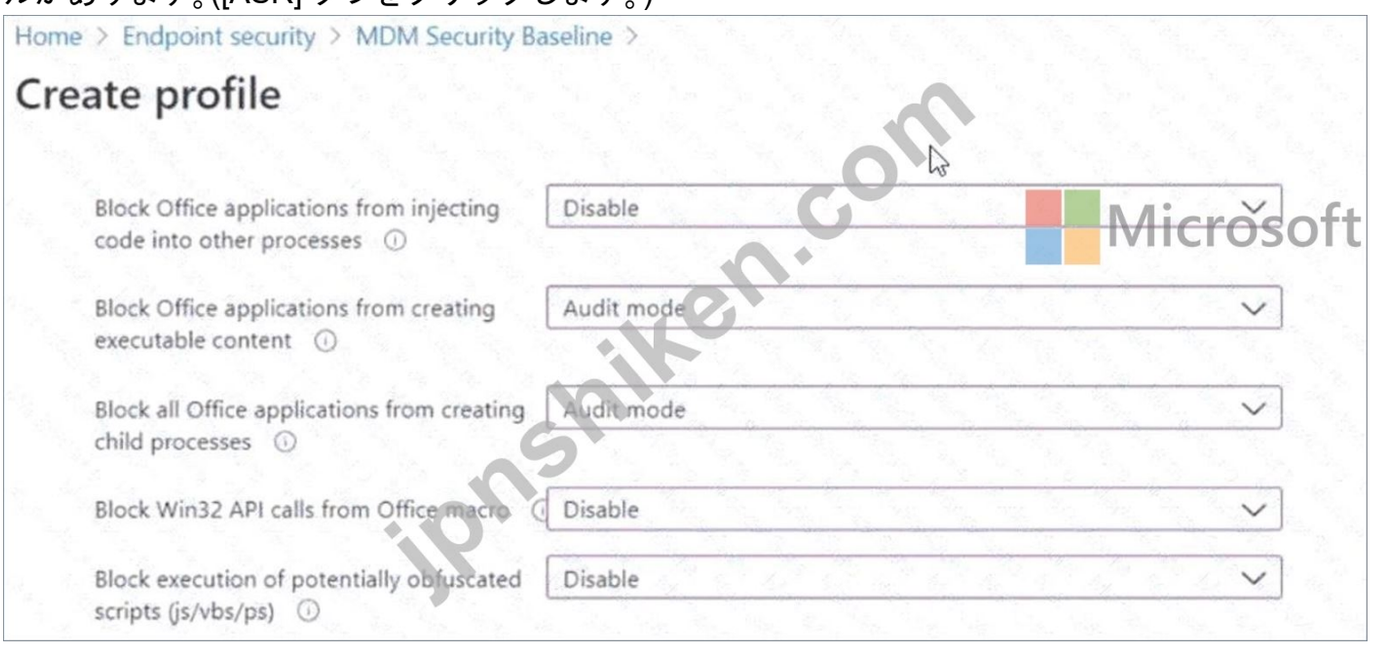
C. ユーザー4とユーザー1のみ

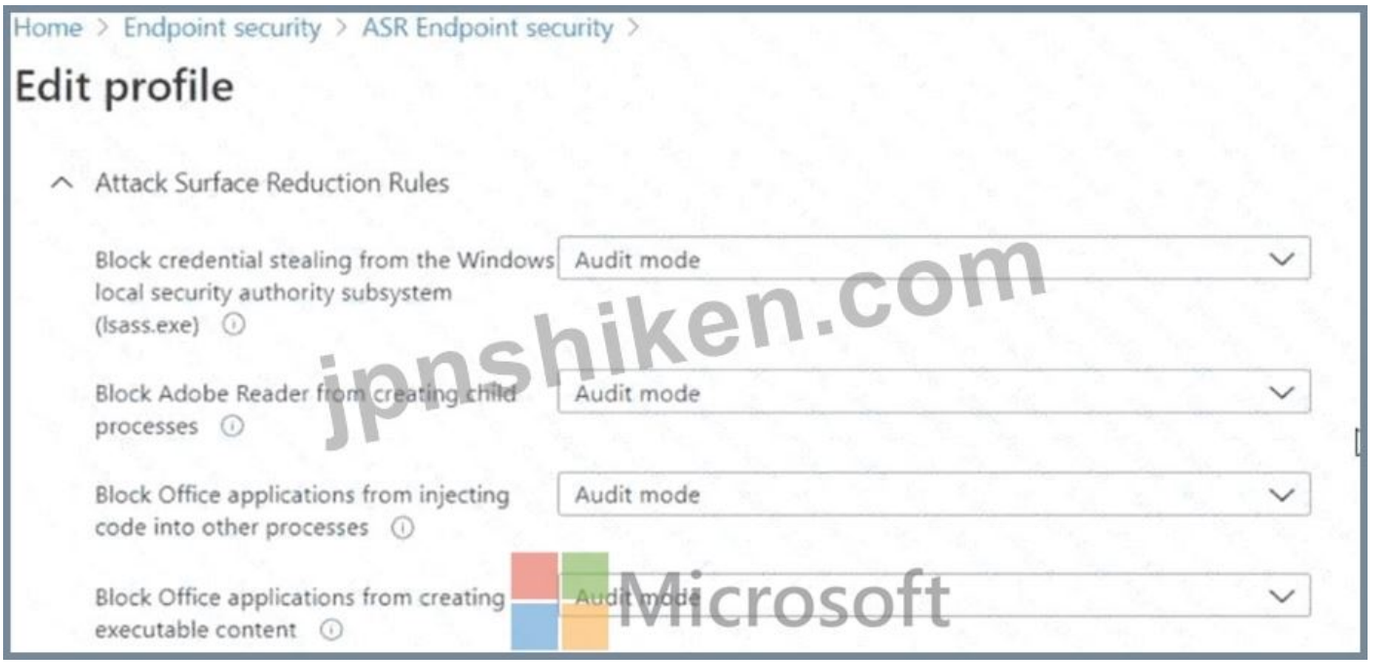
D. ユーザー4。ユーザーランド ユーザー2のみ

正解: **(正解を表示します)**

質問: **135**

MDM 展示に表示されている MDM セキュリティ ベースライン プロファイルがあります。([MDM] タブをクリックします。) ASR 展示に表示されている ASR エンドポイント セキュリティ プロファイルがあります。([ASR] タブをクリックします。)





Microsoft Intune に登録されているデバイスに両方のプロファイルを展開する予定です。デバイス上で以下の設定をどのように構成するかを特定する必要があります。

* Office アプリケーションによる実行可能コンテンツの作成をブロックする
* OfficeマクロからのWin32 API呼び出しをブロックする

現在、設定は各デバイスごとにローカルで無効になっています。

デバイスの効果的な設定は何ですか? 回答するには、回答エリアで適切なオプションを選択してください。

注意: 正しい選択ごとに 1 ポイントが付与されます。

Answer Area

正解:

Explanation:
lock Office App from creating executable content: Audit Mode
Both are set to Audit so that's what it will do.
Block Win32 API calls from the Office Macro: Audit
If you set the Baseline policy as Disable or Not Configured (same thing), and you have any other setting in the ASR, the ASR configuration will take over. That's how enterprise environments enforce granular controls of policies that are enforced for a smaller subset of the employee population. The article below (Jan 27, 2024) outlines the scenario and provides comments about this. In theory this also makes sense. If the baseline policy is configured to do nothing, and the ASR policy is configured to Audit, Block or Warn, I should think the ASR policy setting will take over the configuration.

質問: **136**
次の表に示す仮想マシンを含む Hyper-V ホストがあります。

Name	Generation	Virtual processors	Memory
VM1	1	4	16 GB
VM2	2	1	8 GB
VM3	2	2	4 GB

どの仮想マシンに Windows 11 をインストールできますか?
A. VM1 と VM2 のみ
B. VM1のみ
C. VM3のみ
D. VM2 と VM3 のみ
E. VM1、VM2、VM3
正解: **(**正解を表示します**)**

質問: **137**

Microsoft Intune を使用する 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、次の表に示すユーザーが含まれています。

Name	Member of
User1	Group1, Group2
User2	Group2
User3	Group3

Group2 と Group3 は Group1 のメンバーです。

すべてのユーザーは Microsoft Excel を使用します。

Microsoft Endpoint Manager 管理センターから、次の表に示すポリシーを作成します。

Name	Type	Priority	Assigned to	Default file format for Excel
Policy1	Policies for Office apps	0	Group1	OpenDocument Spreadsheet (*.ods)
Policy2	Policies for Office apps	1	Group2	Excel Binary Workbook (*.xlsb)

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
When User1 saves a new spreadsheet, the .ods format is used.	○	○
When User2 saves a new spreadsheet, the .xlsb format is used.	○	○
When User3 saves a new spreadsheet, the .xlsx format is used.	○	○

正解:

Statements	Yes	No
When User1 saves a new spreadsheet, the .ods format is used.	○	○
When User2 saves a new spreadsheet, the .xlsb format is used.	○	○
When User3 saves a new spreadsheet, the .xlsx format is used.	○	○

Explanation:
Box 1: Yes
User1 is member of Group1 and Group2.
Policy1 with priority 0 is assigned to Group1: default file format for Excel is.ods.
Policy2 with priority 1 is assigned to Group2: default file format for Excel is.xlsb.
Note: Key points to remember about policy order
Policies are assigned an order of priority.
Devices receive the first applied policy only.
You can change the order of priority for policies.
Default policies are given the lowest order of priority.
Box 2: No
User2 is member of Group2.
Group2 and Group3 are members of Group1.
Box 3: No
User3 is member of Group3.
Group2 and Group3 are members of Group1.
Reference: https://learn.microsoft.com/en-us/microsoft-365/security/defender-business/mdb-policy-order

質問: **138**
Windows 11 を実行する Computer! という名前のコンピューターがあります。
User1 というユーザーは、リモート デスクトップを使用して Computer1 に接続する予定です。
リモート デスクトップ接続が確立され、サインイン ページが表示される前に、User1 のデバイスが認証されていることを確認する必要があります。
Computer1 では何をすればよいでしょうか?
A. リモート デスクトップ構成サービスを構成します。
B. ネットワーク レベル認証 (NLA) を有効にします。
C. 評価ベースの保護をオンにします。
D. ネットワーク探索をオンにします。

正解: **B** (コメントを発表する)

質問: **139**
ネットワークには Active Directory ドメインが含まれています。ドメインには Windows 10 を実行する 10 台のコンピューターが含まれています。財務部門のユーザーがこれらのコンピューターを使用します。
Windows 10 を実行する Computer1 という名前のコンピューターがあります。
Computer1 から、財務部門のコンピューターで Windows PowerShell コマンドを実行するスクリプトを実行する予定です。
財務部門のコンピューターでコンピューターから PowerShell コマンドを実行できることを確認する必要があります。
財務部門のコンピューターでは何をすべきでしょうか?
A. Windows PowerShell から、Enable-MMAgent コマンドレットを実行します。
B. ローカル グループ ポリシーから、リモート シェル アクセスを許可する設定を有効にします。
C. Windows PowerShell から、Enable-PSRemoting コマンドレットを実行します。
D. ローカル グループ ポリシーから、スクリプトの実行を有効にする設定を有効にします。
正解: **C** (コメントを発表する)
Enable-PSRemoting is specifically designed to enable remote PowerShell access. This cmdlet configures the necessary settings on the target computers to allow remote PowerShell connections. The other options are not directly related to enabling remote PowerShell: Enable-MMAgent is used for managing mobile devices. The
"Allow Remote Shell Access" group policy setting is primarily for enabling remote access for command prompt (cmd.exe), not PowerShell. The "Turn on Script Execution" group policy setting controls whether scripts can run locally on a computer, but it doesn't enable remote PowerShell access. By running Enable- PSRemoting on the finance department computers, you'll ensure that they are ready to receive and execute PowerShell commands from Computer1.

質問: **140**
ネットワークには Active Directory ドメインが含まれています。ドメインには Admin1 という名前のユーザーが含まれています。すべてのコンピューターは Windows 10 を実行しています。
コンピューター上で Windows PowerShell リモート処理を有効にします。
Admin1 がコンピューターへのリモート PowerShell 接続を確立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、最小権限の原則を使用する必要があります。
Admin1 をどのグループに追加する必要がありますか?
A. パワーユーザー
B. リモートデスクトップユーザー
C. リモート管理ユーザー
D. アクセス制御支援演算子
正解: (正解を表示します)

質問: **141**
Microsoft 365 サブスクリプションをお持ちです。
すべてのデバイスを管理するには、Microsoft Intune を使用します。
ユーザーは Microsoft アプリがインストールされた iOS デバイスを持っています。
ユーザーが Microsoft Excel とデバイスにインストールされている他のアプリ間でデータを切り取り、コピー、貼り付けできないようにする必要があります。
何を設定すればよいですか？
A. iOS アプリのプロビジョニング プロファイル
B. Microsoft Office アプリのポリシー
C. アプリ構成ポリシー
D. アプリ保護ポリシー
正解: **(**正解を表示します**)**

質問: **142**
Microsoft Intune を使用する Microsoft 365 サブスクリプションがあります。
Android Enterprise デバイスにアプリを展開できることを確認する必要があります。
まず何をすべきでしょうか?
A. 構成プロファイルを作成します。
B. パートナー デバイス管理設定を構成します。
C. 証明書コネクタを追加します。
D. 管理対象 Google Play アカウントを Intune にリンクします。
正解: **D (**コメントを発表する**)**

質問: **143**
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。サブスクリプションには、次の表に示すように、Microsoft Intune に登録されているデバイスが含まれています。

Name	Platform	Member of	Description
Device1	Windows 11	Group1	Disk encryption is not configured.
Device2	Windows 10	Group2	Disk encryption is configured.
Device3	Android	Group3	Device local storage is not encrypted.

Microsoft Edge はすべてのデバイスで利用できます。
Intune には、次の表に示すデバイス コンプライアンス ポリシーがあります。

Name	Platform	Setting	Applied to
Compliance1	Windows 10 and later	Require encryption of data storage on device	Group2
Compliance2	Android Enterprise	Require encryption of data storage on device	Group3

コンプライアンス ポリシー設定は、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。)
次の条件付きアクセス ポリシーを作成します。

* 名前: ポリシー1
* 課題
o ユーザーとグループ: ユーザー1
o クラウド アプリまたはアクション: Office 365 SharePoint Online
* アクセス制御
o 承認デバイスが準拠としてマークされることを要求する
* ポリシーを有効にする: オン

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 ポイントが与えられます。

Answer Area

Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	○

正解:

Answer Area

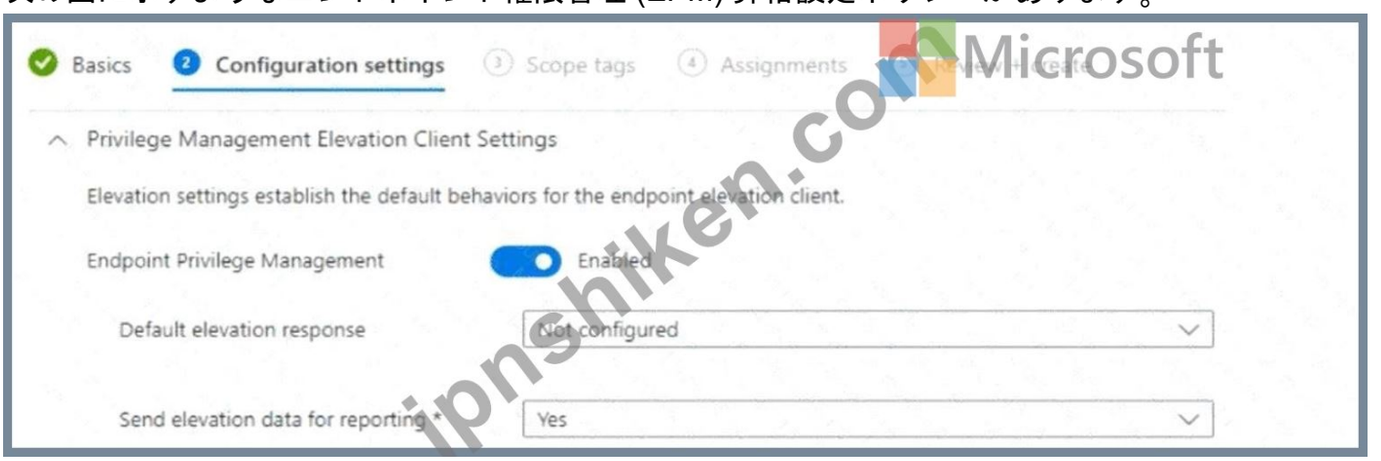
Statements	Yes	No
User1 can access Microsoft SharePoint Online from Device1 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device2 by using Microsoft Edge.	○	○
User1 can access Microsoft SharePoint Online from Device3 by using Microsoft Edge.	○	○

Explanation:

質問: 144

Microsoft 365 サブスクリプションがあり、Microsoft Intune を使用しています。

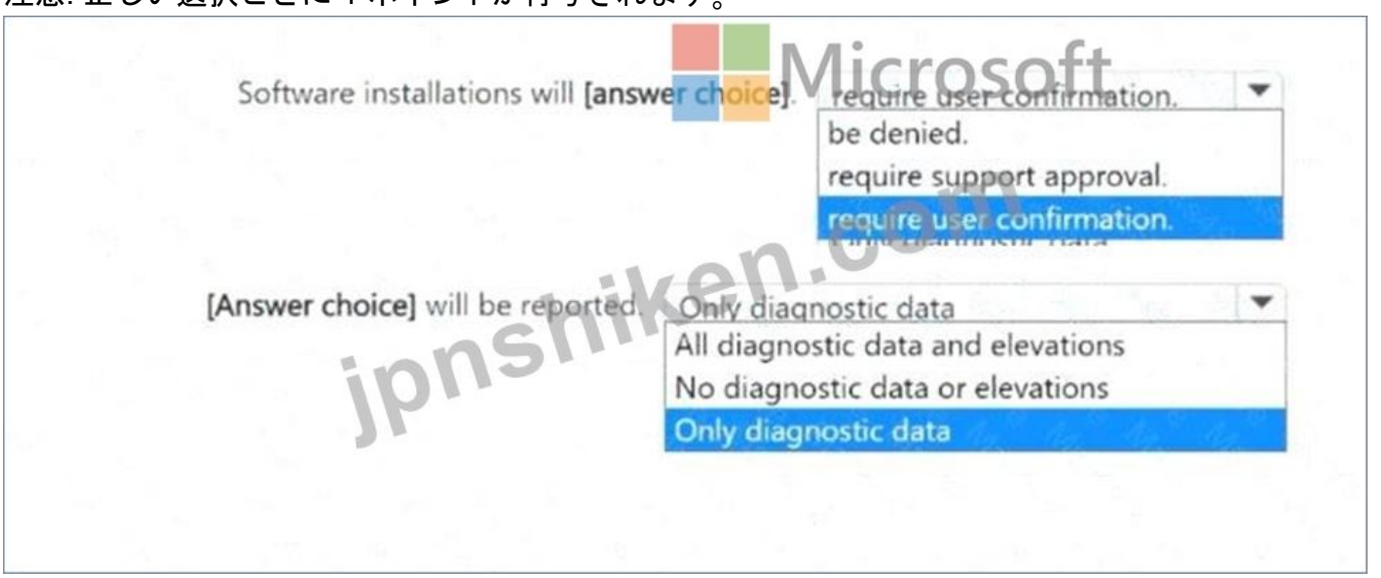
次の図に示すようなエンドポイント権限管理 (EPM) 昇格設定ポリシーがあります。



EPM 昇格ルール ポリシーは構成されていません。

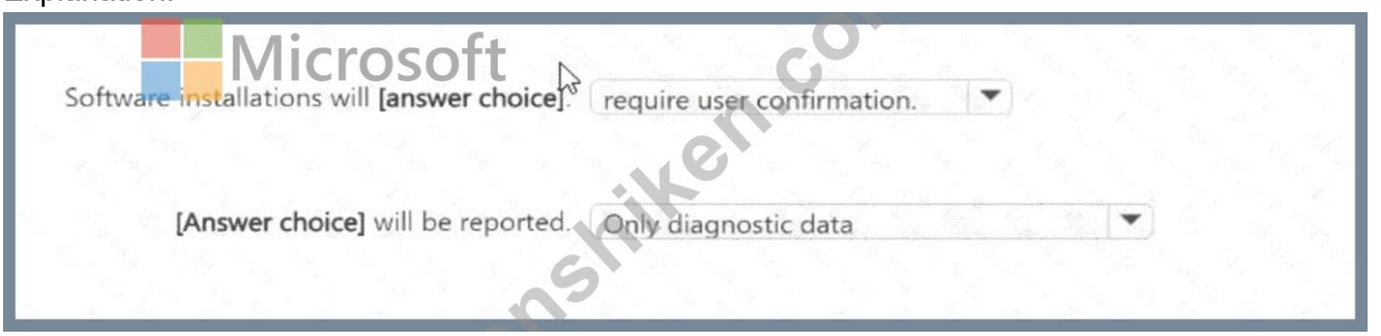
ドロップダウン メニューを使用して、グラフィックに表示されている情報に基づいて各ステートメントを完成させる回答の選択肢を選択します。

注意: 正しい選択ごとに 1 ポイントが付与されます。



正解:

Explanation:



質問: **145**

Group1 という名前のグループを含む Microsoft 365 E5 サブスクリプションがあります。Group1 のメンバーだけがデバイスを Microsoft Entra テナントに参加できるようにする必要があります。Microsoft Entra 管理センターで何を構成する必要がありますか?

A. エンタープライズ ステート ローミング

B. デバイス設定

C. 機動性

D. ユーザー設定

正解: **(**正解を表示します**)**

質問: **146**

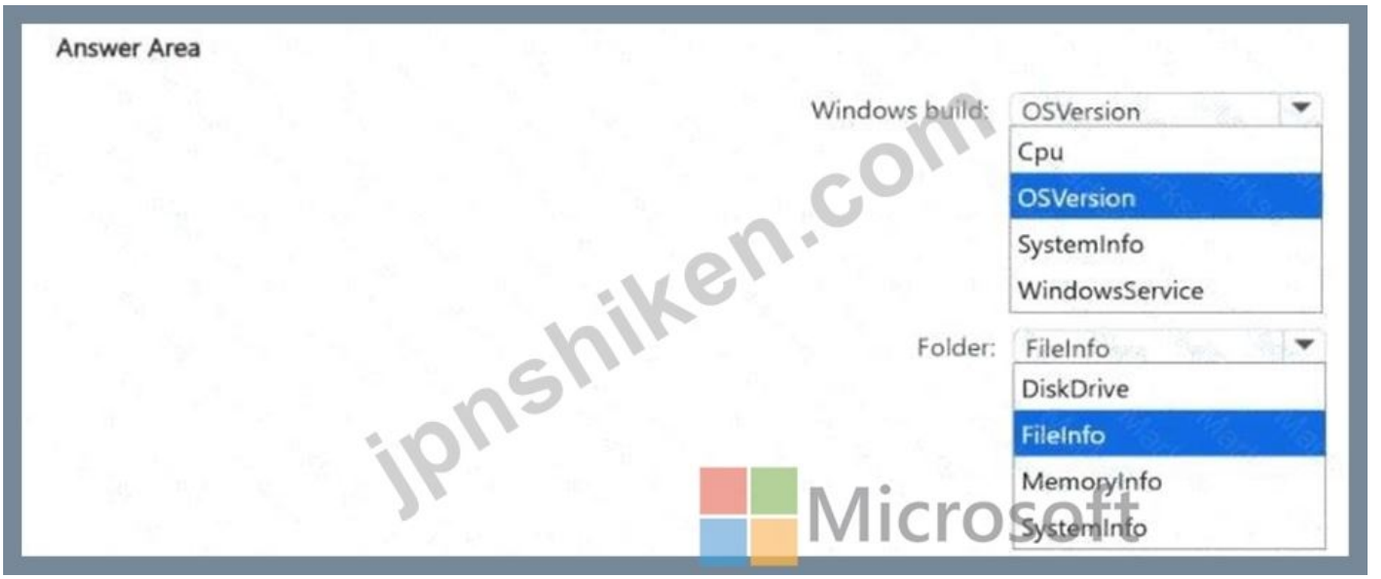
64 ビット版の Windows 10 Enterprise を実行し、Microsoft Office 2019 がインストールされている、Device1 という名前の Windows 11 対応デバイスがあります。次の表に示す Windows 11 Enterprise イメージがあります。

Name	Platform	Description
Image1	x64	Custom Windows 11 image that has Office 2021 installed
Image2	x64	Default Windows 11 image created by Microsoft

Device1 のインプレース アップグレードを実行するために使用できるイメージはどれですか?
A. 画像のみ
B. 画像1のみ
C. 画像1と画像2
正解**: (**正解を表示します**)**

質問**: 147**
Microsoft Intune に登録されているデバイスの種類は次のとおりです。
* ウィンドウズ10
* アンドロイド
* iOS
Microsoft Intune 管理センターで VPN プロファイルを作成できるのはどの種類のデバイスですか?
A. Windows 10 および Android のみ
B. Windows 10 および iOS のみ
C. Windows 10、Android、iOS
D. Android と iOS のみ
E. Windows 10 のみ
正解**: (**正解を表示します**)**

質問**: 148**
Device1 と Device2 という名前の 2 つのデバイスを含む Microsoft 365 E5 サブスクリプションがあります。
Microsoft Intune を使用してデバイスを管理します。
次の要件を満たすには、デバイス クエリを使用する必要があります。
* デバイス上の Windows ビルドを識別します。
* デバイスの C ドライブにフォルダーが存在するかどうかを検証します。
各要件についてどのテーブルをターゲットに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。



正解:

Explanation:

質問: **149**

注: このセクションには、同じシナリオと問題を扱う1つ以上の質問セットが含まれています。各質問は、問題に対する独自の解決策を提示します。その解決策が、定められた目標を満たしているかどうかを判断してください。

セット内の複数の解決策が問題を解決できる可能性があります。また、セット内のどの解決策も問題を解決できない可能性もあります。

このセクションの質問に回答した後は、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。

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

Device1 という名前の Android デバイスを購入します。
Device1 を contoso.com に登録する必要があります。
解決策: Microsoft Intune ポータル サイト アプリを使用します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**

質問: **150**
Microsoft Intuでデバイス構成プロファイルを作成しています
プロファイルで特定の OMA-URI 設定を構成する必要があります。
どのプロファイル タイプのテンプレートを使用する必要がありますか?
A. 個人情報保護
B. カスタム
C. デバイスの制限
D. デバイスの制限 (Windows 10 チーム)
正解: **B (**コメントを発表する**)**

質問: **151**
次の表に示すユーザーを含む Microsoft 365 E5 サブスクリプションがあります。

Name	Role
Admin1	Application admin
Admin2	Cloud application admin
Admin3	Office apps admin
Admin4	Security admin

Microsoft 365 アプリ管理センターで、Microsoft Office のカスタマイズを作成します。
管理センターから Office カスタマイズ ファイルをダウンロードできるのはどのユーザーですか?
A. Admin1、Admin2、Admin3、および Admin4
B. Admin1、Admin2、Admin3のみ
C. Admin3のみ
D. Admin3 と Admin4 のみ
E. Admin1とAdmin3のみ
正解: **(**正解を表示します**)**
* Admin1
An application admin has full access to enterprise applications, applications registrations, and application proxy settings.

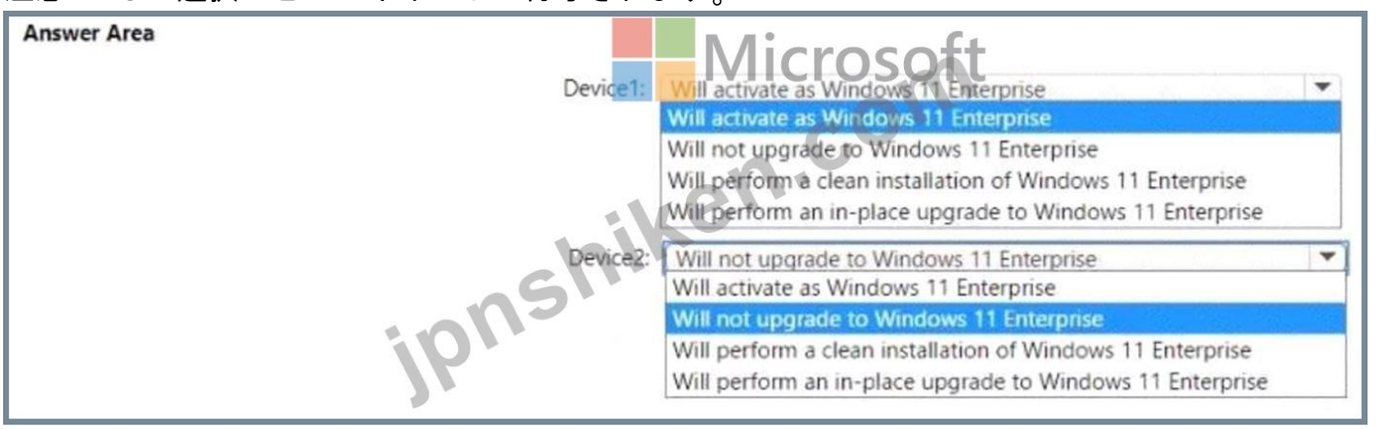
* Admin2
Mark your app as publisher verified.
In Azure AD this user must be a member of one of the following roles: Application Admin, Cloud Application Admin, or Global Admin.
* Admin3
Office Apps admin - Assign the Office Apps admin role to users who need to do the following:
- Use the Office cloud policy service to create and manage cloud-based policies for Office
- Create and manage service requests
- Manage the What's New content that users see in their Office apps
- Monitor service health
Reference:
Office Apps admin - Assign the Office Apps admin role to users who need to do the following
https://docs.microsoft.com/en-us/azure/active-directory/develop/mark-app-as-publisher-verified

質問: **152**
会社には Windows 10 を実行するコンピューターが 200 台あります。コンピューターは Microsoft Intune を使用して管理されています。現在、Windows 更新プログラムは配信の最適化を使用せずにダウンロードされています。配信の最適化を使用するには、コンピューターを構成する必要があります。Intune で何を作成する必要がありますか?
A. デバイスコンプライアンスポリシー
B. Windows 10 アップデート リング
C. デバイス構成プロファイル
D. アプリ保護ポリシー
正解: **(正解を表示します)**

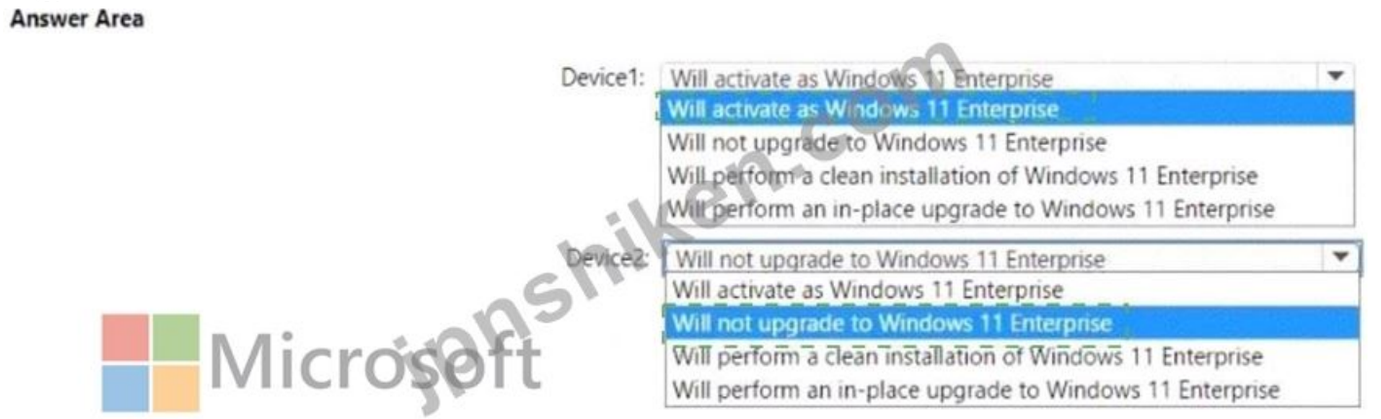
質問: **153**
ネットワークには、Azure AD と同期する contoso.com という名前のオンプレミスの Active Directory ドメインが含まれています。User! という名前のユーザーは、次の表に示すドメインに参加しているデバイスを使用します。

Name	Operating system
Device1	Windows 10 Pro
Device2	Windows 11 Pro

Microsoft Entra 管理センターで、Windows 11 Enterprise E5 ライセンスを User1 に割り当てます。
User1 が次にデバイスにサインインしたときに何が起こるかを特定する必要があります。
各デバイスについて何を識別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。



正解:



Explanation:

Device 1:
Will activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 1 has Windows 11 Pro, so it meets the requirement.
When User1 signs in to Device 1 with their Azure AD account, the device will automatically activate as Windows 11 Enterprise without changing the edition.
Will not activate as Windows 11 Enterprise. According to Deploy Windows Enterprise licenses, Windows 11 Enterprise E5 license is a subscription license that can be assigned to users who have a supported and licensed version of Windows 10 Pro or Windows 11 Pro. Device 2 has Windows 10

Home, so it does not meet the requirement. When User1 signs in to Device 2 with their Azure AD account, the device will not activate as Windows 11 Enterprise by subscription.

質問: **154**
ネットワークには、contoso.com という名前の Active Directory ドメインが含まれています。このドメインには、Windows 10 を実行する Computer1 という名前のコンピューターが含まれています。次の表に示すグループがあります。

Name	Type	Location
Group1	Universal distribution group	Contoso.com
Group2	Global security group	Contoso.com
Group3	Group	Computer1
Group4	Group	Computer1

Group4 に追加できるグループはどれですか?
A. グループ2のみ
B. グループ1、グループ2、グループ3
C. グループ1とグループ2のみ
D. グループ2とグループ3のみ
正解: **(**正解を表示します**)**

質問: **155**
Microsoft Intune Suite を使用する Microsoft 365 サブスクリプションをお持ちです。
デバイスを管理するには、Microsoft Intune を使用します。
Intune での自動登録が構成されています。
ワークグループには 100 台の Windows 11 デバイスがあります。
デバイスを企業のワイヤレス ネットワークに接続し、100 台の新しい Windows デバイスを Intune に登録する必要があります。
何を使うべきでしょうか?
A. プロビジョニング パッケージ
B. グループ ポリシー オブジェクト (GPO)
C. モバイルデバイス管理 (MDM) 自動登録
D. デバイス構成ポリシー
正解: **(**正解を表示します**)**
https://learn.microsoft.com/en-us/mem/intune/enrollment/windows-bulk-enroll
"" Join new Windows devices to Microsoft Entra ID and Intune. To bulk enroll devices for your Microsoft Entra tenant, you create a provisioning package with the Windows Configuration Designer (WCD) app.
Applying the provisioning package to corporate-owned devices joins the devices to your Microsoft Entra tenant and enrolls them for Intune management. Once the package is applied, it's ready for your Microsoft Entra users to sign in. ""

質問: **156**
注: このセクションには、同じシナリオと問題を扱う1つ以上の質問セットが含まれています。各質問は、問題に対する独自の解決策を提示します。その解決策が、定められた目標を満たしているかどうかを判断してください。
セット内の複数の解決策が問題を解決できる可能性があります。また、セット内のどの解決策も問題を解決できない可能性もあります。
このセクションの質問に回答した後は、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。
contoso.com という名前の Microsoft Entra テナントがあります。
Device1 という名前の Android デバイスを購入します。
Device1 を contoso.com に登録する必要があります。
解決策: Microsoft Authenticator アプリを使用します。
これは目標を満たしていますか?
A. はい
B. いいえ
正解: **(**正解を表示します**)**

質問: **157**
Microsoft Intune に登録された 100 台のデバイスを含む Microsoft 365 サブスクリプションがあります。
起動プロセスと各デバイスの再起動頻度を確認する必要があります。
何を使うべきでしょうか?
A. エンドポイント分析
B. Intune データ ウェアハウス
C. Azure モニター
D. デバイス管理
正解: **(**正解を表示します**)**
Endpoint analytics within Microsoft Intune specifically provides insights into device performance and health, including information about startup processes and restart frequency. It offers features like:
Startup performance: Analyzes boot and sign-in times, identifying slow devices and their specific bottlenecks.
Restart frequency: Tracks how often devices restart overall and per model, helping identify unusual occurrences.
Model performance: Compares boot and sign-in performance across different device models.

質問: **158**
Microsoft Intune に登録されている 1,000 台の Android デバイスを含む Microsoft 365 サブスクリプションがあります。次の設定を含むアプリ構成ポリシーを作成します。
* デバイス登録タイプ: 管理対象デバイス

* プロフィールタイプ: すべてのプロフィールタイプ
* プラットフォーム: Android Enterprise
どの 2 種類のアプリをポリシーに関連付けることができますか? 正解ごとに完全なソリューションが提示されます。注: 正解の選択ごとに 1 ポイントが付与されます。
A. Android Enterprise システム アプリ
B. Androidアプリ内蔵
C. Webリンク
D. Android ストア アプリ
E. マネージド Google Play ストア アプリ
正解: **(**正解を表示します**)**