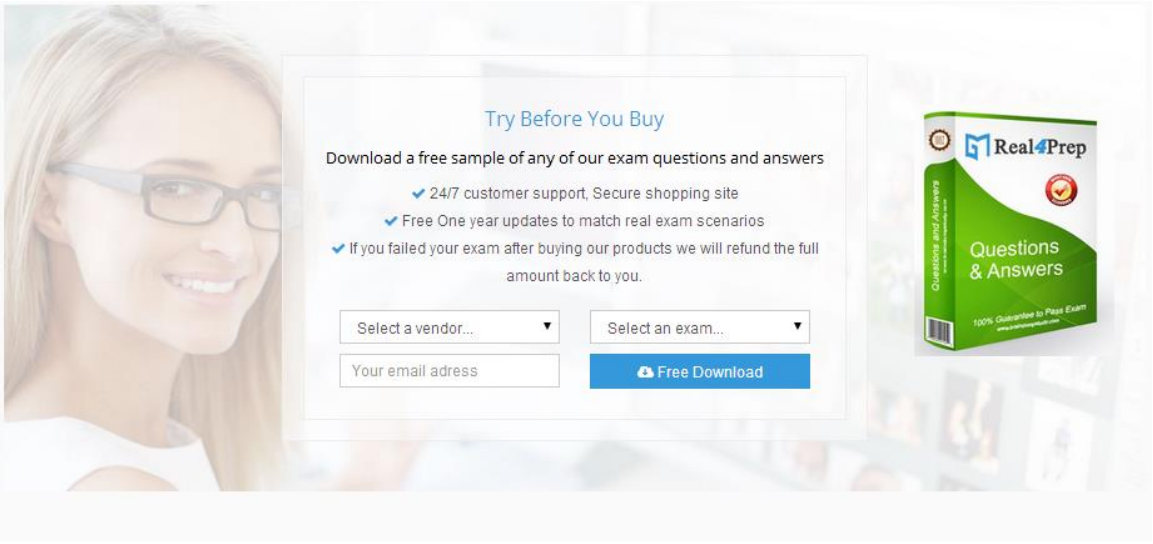
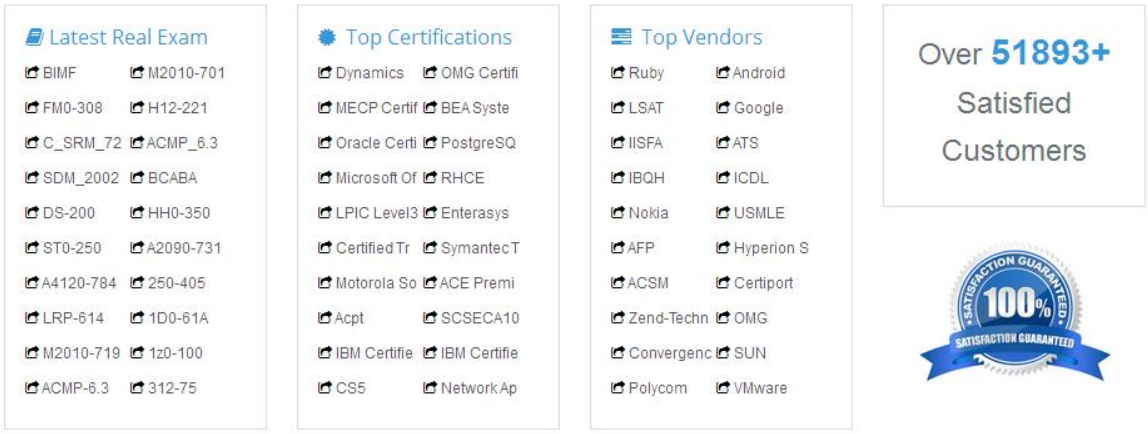
Real4Prep





http://www.real4prep.com

Latest Real Exam Prep Dumps for IT Exam Preparation

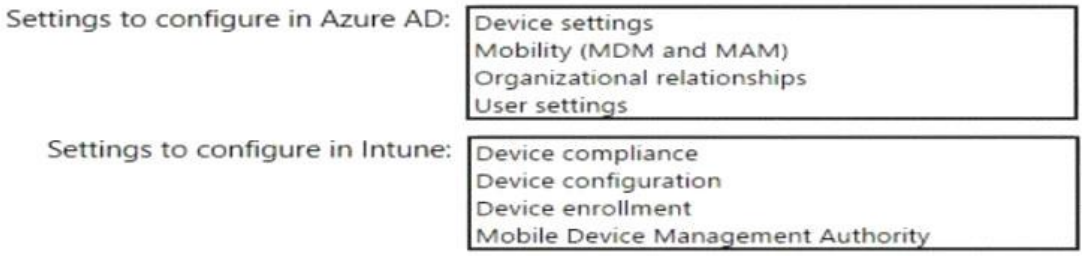
Exam : **MS-102J**

Title : Microsoft 365 Administrator (MS-102日本語版)

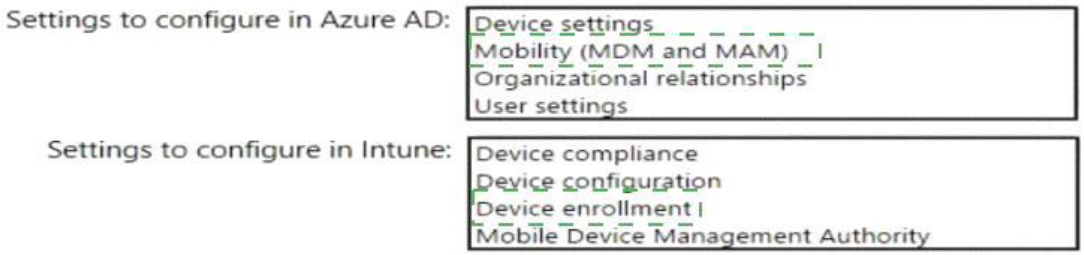
Vendor : Microsoft

Version : DEMO

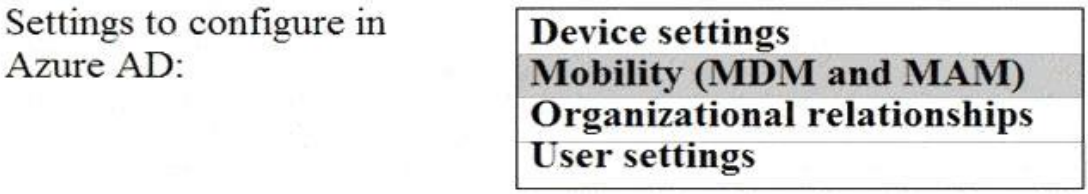
QUESTION NO: 1
Intune の技術要件と計画された変更を満たす必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。
Answer Area

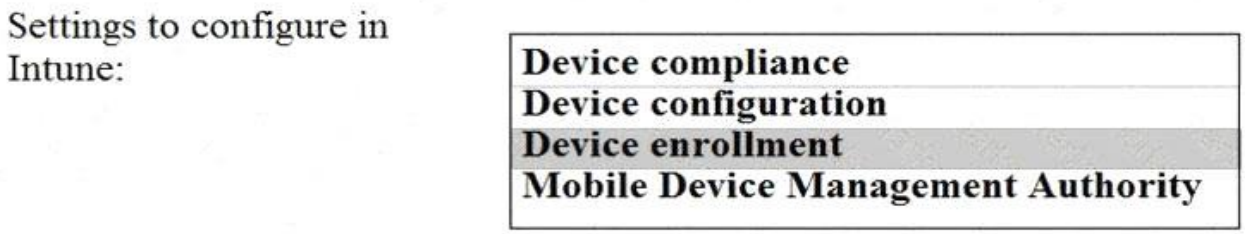


Answer:
Answer Area



Explanation:





Reference:
https://docs.microsoft.com/en-us/intune/windows-enroll
Topic 1, Contoso, LtdOverview
Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.
The company has the employees and devices shown in the following table.

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

Contoso recently purchased a Microsoft 365 ES subscription.
Existing Environment
Requirement
The network contains an on-premises Active Directory forest named contoso.com. The forest contains the servers shown in the following table.

Name	Configuration
Server1	Domain controller
Server2	Member server
Server3	Network Policy Server (NPS) server
Server4	Remote access server
Server5	Microsoft Azure AD Connect server

All servers run Windows Server 2016. All desktops and laptops are Windows 10 Enterprise and are joined to the domain.
The mobile devices of the users in the Montreal and Seattle offices run Android. The mobile devices of the users in the New York office run iOS.
The domain is synced to Microsoft Entra ID (Microsoft Entra ID) and includes the users shown in the following table.

Name	Azure AD role
User1	*None*
User2	Application administrator
User3	Cloud application administrator
User4	Global administrator
User5	Intune administrator

The domain also includes a group named Group1.
Planned Changes
Contoso plans to implement the following changes:
*Implement Microsoft 365.
*Manage devices by using Microsoft Intune.
*Implement Microsoft Entra IDvanced Threat Protection (ATP).
*Every September, apply the latest feature updates to all Windows computers. Every March, apply the latest feature updates to the computers in the New York office only.
Technical Requirements
Contoso identifies the following technical requirements:
*When a Windows 10 device is joined to Microsoft Entra ID, the device must enroll in Intune

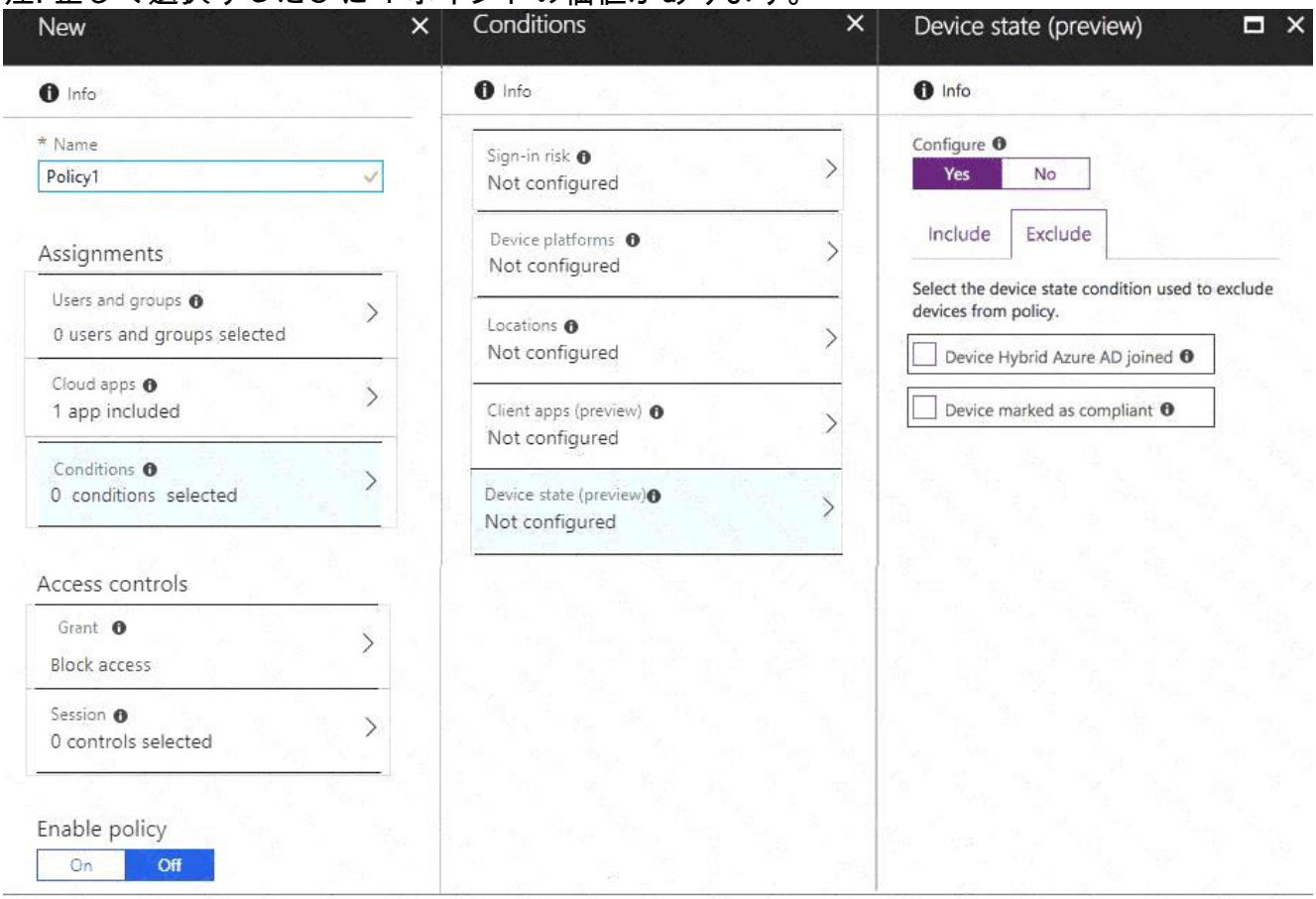
automaticity.
*Dedicated support technicians must enroll all the Montreal office mobile devices in Intune.
*User1 must be able to enroll all the New York office mobile devices in Intune.
*Azure ATP sensors must be installed and must NOT use port mirroring.
*Whenever possible, the principle of least privilege must be used.
*A Microsoft Store for Business must be created.
Compliance Requirements
Contoso identifies the following compliance requirements:
*Ensure that the users in Group1 can only access Microsoft Exchange Online from devices that are enrolled in Intune and configured in accordance with the corporate policy.
*Configure Windows Information Protection (W1P) for the Windows 10 devices.

QUESTION NO: 2
Azure ATP センサーはどのサーバーにインストールする必要がありますか?
A. サーバー 1
B. サーバー 2
C. サーバー 3
D. サーバー 4
E. サーバー 5
Answer: A
References:
https://docs.microsoft.com/en-us/azure-advanced-threat-protection/atp-capacity-planning
However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

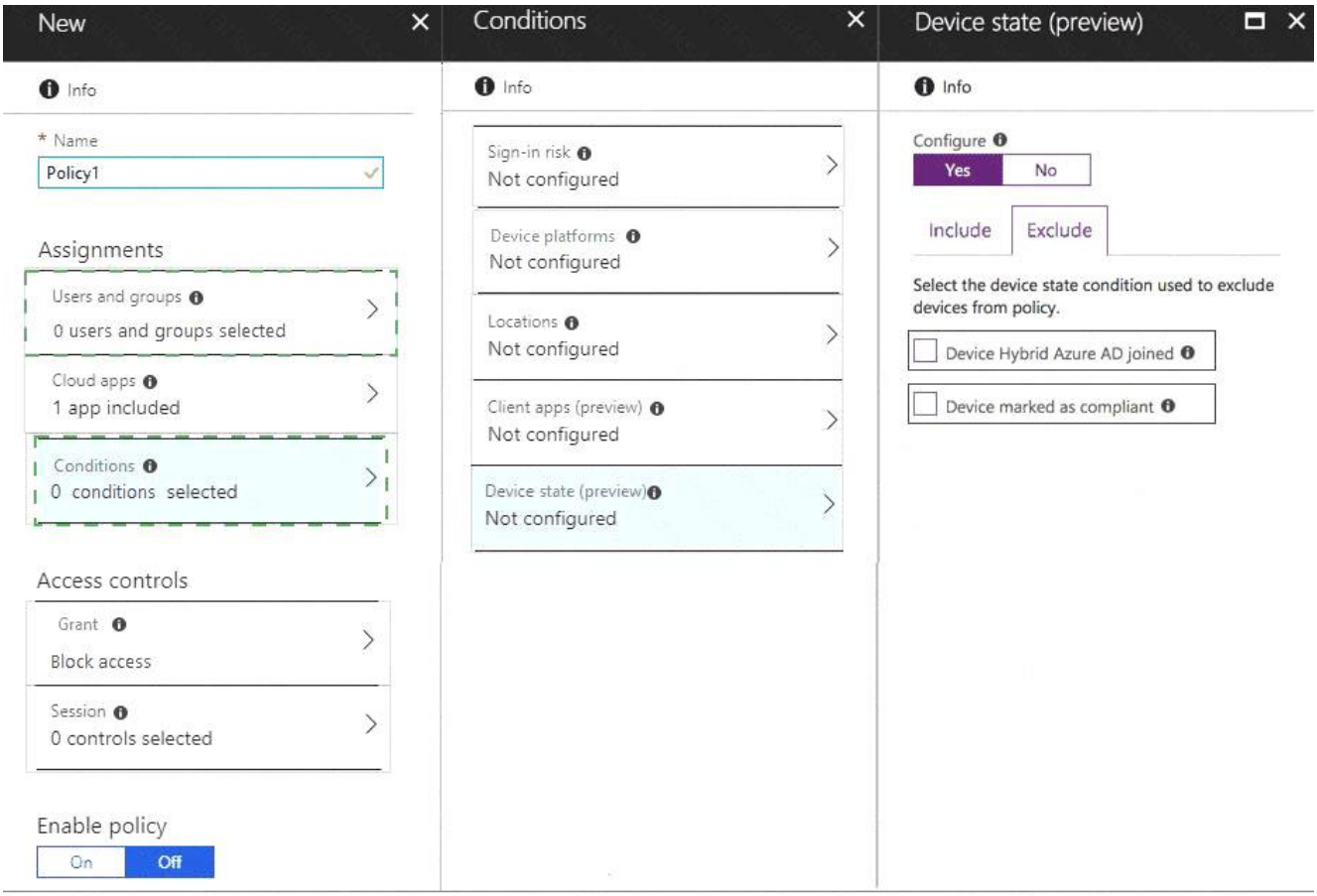
QUESTION NO: 3
注：この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。
このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。
お客様のネットワークには、Microsoft Entra ID (Microsoft Entra ID)
と同期された、contoso.com という名前の Active Directory ドメインが含まれています。
Microsoft System Center Configuration Manager (Current Branch) を使用して、Windows 10 デバイスを管理します。
共同管理のためのパイロット版を設定します。
ドメインにDevice1という名前の新しいデバイスを追加します。Device1にConfiguration Managerクライアントをインストールします。
Microsoft IntuneとConfiguration
Managerを使用してDevice1を管理できることを確認する必要があります。
解決策：Configuration
Managerのデバイスコレクションをパイロットコレクションとして定義します。Device1をコレクションに追加します。
これは目標を達成していると言えるでしょうか？

A. はい
B. いいえ
Answer: A
Explanation:
Device1 has the Configuration Manager client installed so you can manage Device1 by using Configuration Manager. To manage Device1 by using Microsoft Intune, the device has to be enrolled in Microsoft Intune. In the Co-management Pilot configuration, you configure a Configuration Manager Device Collection that determines which devices are auto-enrolled in Microsoft Intune. You need to add Device1 to the Device Collection so that it auto-enrols in Microsoft Intune. You will then be able to manage Device1 using Microsoft Intune. Reference: https://docs.microsoft.com/en-us/configmgr/comanage/how-to-enable

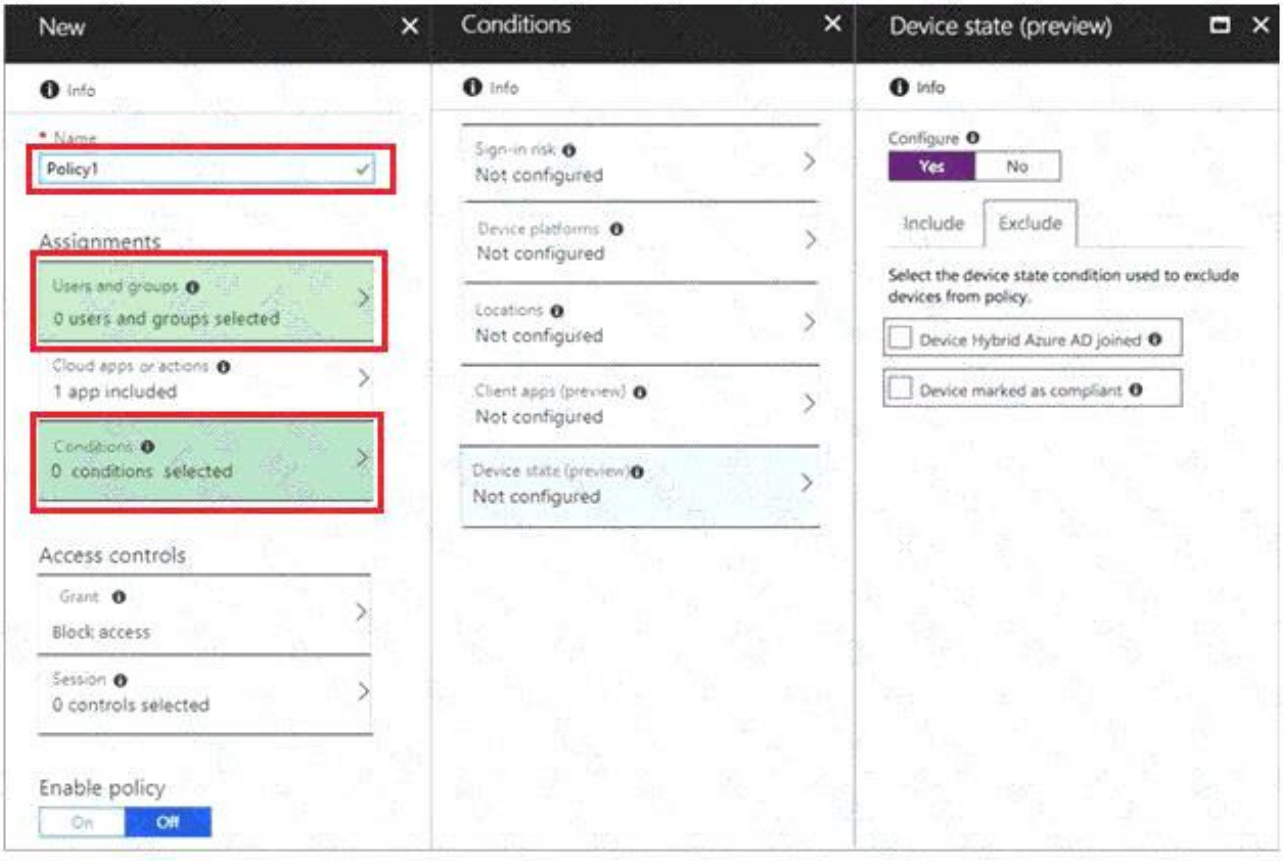
QUESTION NO: 4
コンプライアンス要件を満たすには、条件付きアクセス
ポリシーを構成する必要があります。
Exchange Online をクラウド アプリとして追加します。
Policy1 で構成する必要がある 2
つの追加設定はどれですか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



Explanation:
Suggested answer:



References:https://docs.microsoft.com/en-us/intune/create-conditional-access-intune

QUESTION NO: 5
ユーザー1が技術要件を満たすデバイスを登録できるようにする必要があります。どうすればよいですか？
A. Microsoft Entra ID 管理センターから、User1 にクラウド
デバイス管理者の役割を割り当てます。
B. Microsoft Entra ID
管理センターから、ユーザーごとの最大デバイス数の設定を構成します。
C. Intune 管理センターから、User1 をデバイス登録マネージャーとして追加します。
D. Intune 管理センターから、登録制限を構成します。
Answer: C
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 6
どのサーバーで Defender for ID センサーを使用する必要がありますか?
A. サーバー1
B. サーバー2
C. サーバー3
D. サーバー4
E. サーバー5
Answer: A
Explanation:
However, if the case study had required that the DCs can ' t have any s/w installed, then the answer would have been a standalone sensor on Server2. In this scenario, the given answer is correct. BTW, ATP now known as Defender for Identity.

QUESTION NO: 7
注：この問題は、同じシナリオを提示する一連の問題の一部です。このシリーズの各問題には、提示された目標を満たす可能性のある独自の解答が含まれています。問題セットによっては、複数の正解がある場合もあれば、正解がない場合もあります。
このセクションの質問に回答すると、後から戻って回答することはできません。そのため、これらの質問は復習画面には表示されません。
お客様のネットワークには、Microsoft Entra ID (Microsoft Entra ID)
と同期された、contoso.com という名前の Active Directory ドメインが含まれています。
Microsoft System Center Configuration Manager (Current Branch) を使用して、Windows 10 デバイスを管理します。
共同管理のためのパイロット版を設定します。
ドメインにDevice1という名前の新しいデバイスを追加します。Device1にConfiguration Managerクライアントをインストールします。
Microsoft IntuneとConfiguration
Managerを使用してDevice1を管理できることを確認する必要があります。
解決策：デバイス管理管理センターからデバイス構成プロファイルを作成します。

これは目標を達成していると言えるでしょうか？
A. はい
B. いいえ
Answer: B
Explanation:
It looks like the given answer is correct. There is an on-premises Active Directory synced to Microsoft Entra ID (Microsoft Entra ID) So the co-management path1 - Auto-enroll existing clients 1. Hybrid Microsoft Entra ID 2. Client agent setting for hybrid Microsoft Entra ID-join 3. Configure auto-enrollment of devices to Intune 4. Enable co-management in Configuration Manager https://docs.microsoft.com/en-us/mem/configmgr /comanage/tutorial-co-manage-client

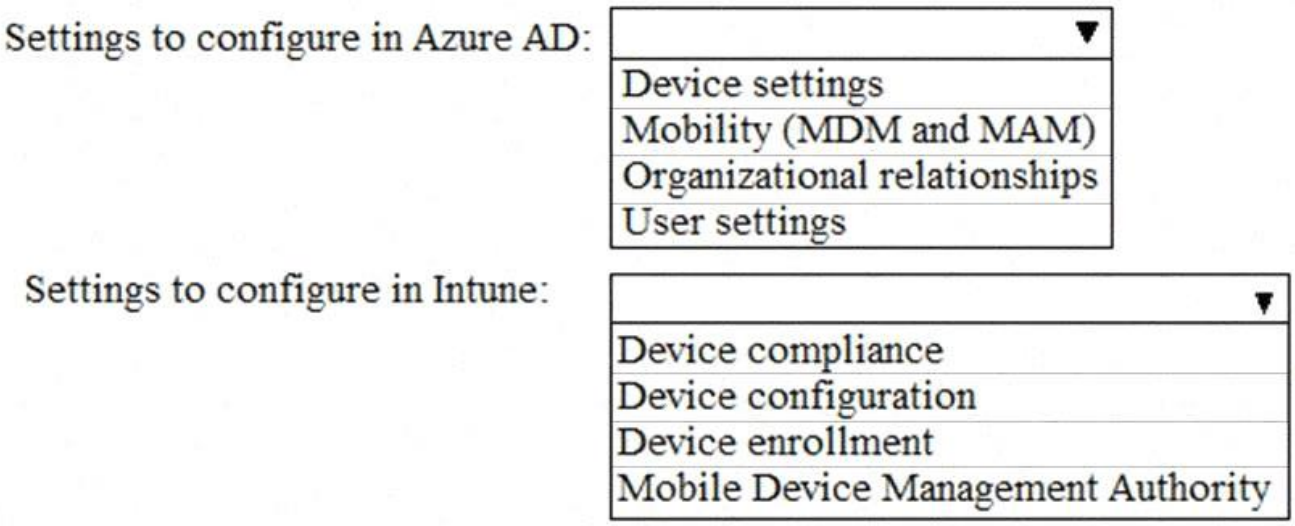
QUESTION NO: 8
3 月の時点で、各オフィスのコンピューターはいつまで Microsoft によってサポートされますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer:

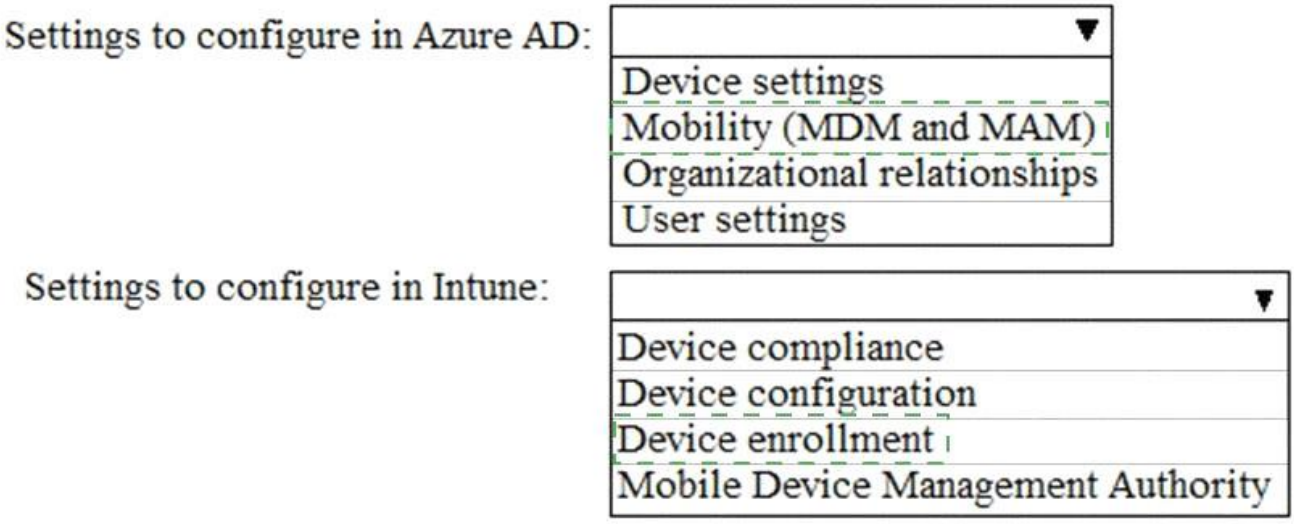
Explanation:

https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet March Feature Updates:
Serviced for 18 months from release date September Feature Updates: Serviced for 30 months from release date References:
https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10

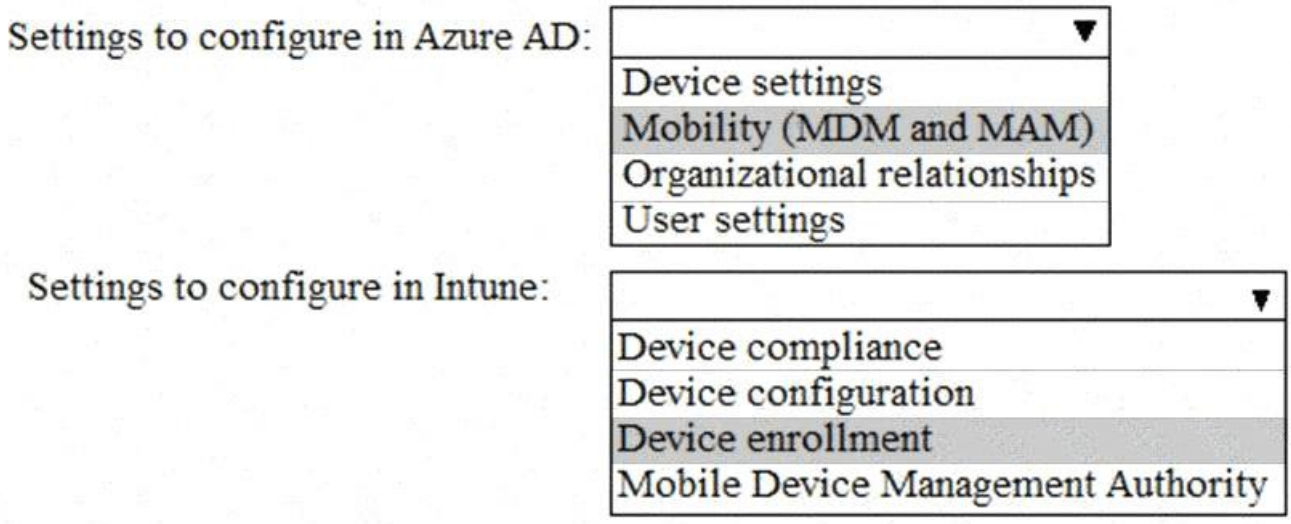
QUESTION NO: 9
Windows 10 デバイスの Intune 要件を満たす必要があります。
あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



Explanation:



References:
https://docs.microsoft.com/en-us/intune/windows-enroll

QUESTION NO: 10

ビジネス向け Microsoft
ストアを作成する必要があります。どのユーザーがストアを作成できますか?
A. ユーザー2
B. ユーザー 3
C. ユーザー 4
D. ユーザー5
Answer: C
References:
https://docs.microsoft.com/en-us/microsoft-store/roles-and-permissions-microsoft-store-for-business

QUESTION NO: 11
サポート技術者がモントリオール オフィスのモバイル
デバイスの技術要件を満たしていることを確認する必要があります。
専任のサポート技術者は最低どれくらい必要ですか?
A. 1
B. 4
C. 7
D. 31
Answer: B
References:
https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/enroll-devices-with-device-enrollment-manager

QUESTION NO: 12
Windows 10 デバイスのコンプライアンス要件を満たす必要があります。
Intune 管理センターから何を作成する必要がありますか?
A. デバイスのコンプライアンス ポリシー
B. デバイス構成プロファイル
C. アプリケーションポリシー
D. アプリ構成ポリシー
Answer: C
Topic 2, A. DatumCase Study:
Overview
Existing Environment
This is a case study Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review

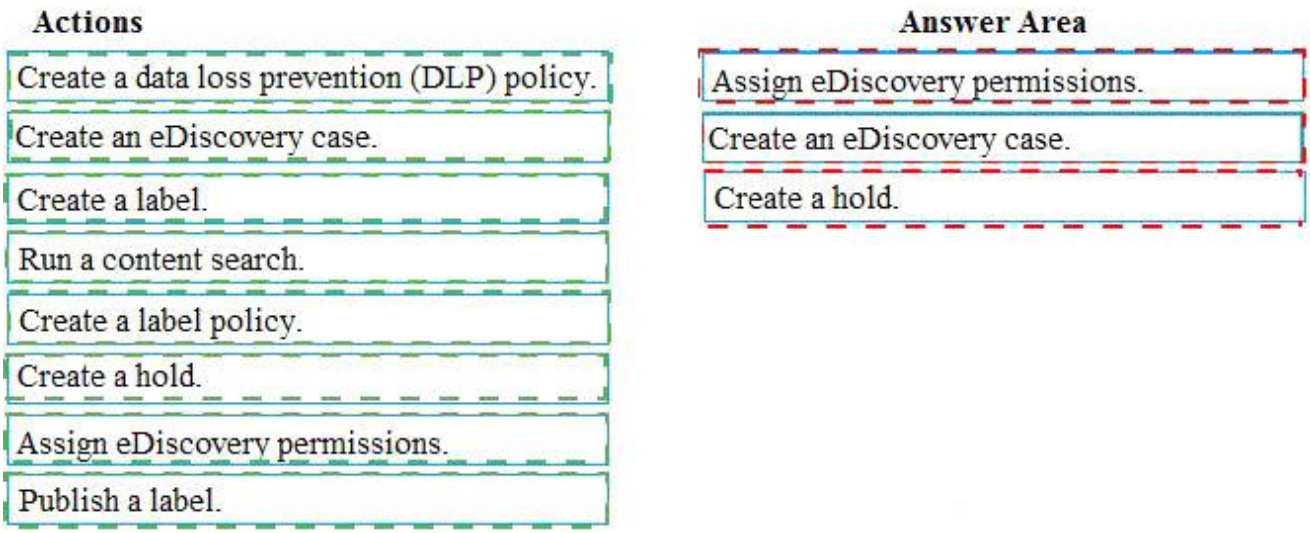
your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study
To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. When you are ready to answer a question, click the Question button to return to the question.
Current Infrastructure
A). Datum recently purchased a Microsoft 365 subscription.
All user files are migrated to Microsoft 365.
All mailboxes are hosted in Microsoft 365. The users in each office have email suffixes that include the country of the user, for example, user1@us.adatum.com or user2#uk.ad3tum.com.
Each office has a security information and event management (SIEM) appliance. The appliances come from three different vendors.
A). Datum uses and processes Personally Identifiable Information (PII).
Problem Statements
Requirements
A). Datum entered into litigation. The legal department must place a hold on all the documents of a user named User1 that are in Microsoft 365.
Business Goals
A). Datum warns to be fully compliant with all the relevant data privacy laws in the regions where it operates.
A). Datum wants to minimize the cost of hardware and software whenever possible.
Technical Requirements
A). Datum identifies the following technical requirements:
Centrally perform log analysis for all offices.
Aggregate all data from the SIEM appliances to a central cloud repository for later analysis.
Ensure that a SharePoint administrator can identify who accessed a specific file stored in a document library.
Provide the users in the finance department with access to Service assurance information in Microsoft Office
365.
Ensure that documents and email messages containing the PII data of European Union (EU) citizens are preserved for 10 years.
If a user attempts to download 1,000 or more files from Microsoft SharePoint Online within 30 minutes, notify a security administrator and suspend the user ' s user account.
A security administrator requires a report that shows which Microsoft 36S users signed in Based on the report, the security administrator will create a policy to require multi-factor authentication when a sign in is high risk.
Ensure that the users in the New York office can only send email messages that contain sensitive US. PII data to other New York office users. Email messages must be monitored to ensure compliance. Auditors in the New York office must have access to reports that show the sent and received email messages containing sensitive U.S. PII data.

QUESTION NO: 13
EU PII データの技術要件を満たす必要があります。
何を作成する必要がありますか?
A. Security & からの保持ポリシー。コンプライアンス管理センター。
B. Exchange 管理センターからの保持ポリシー
C. Exchange 管理センターからのデータ損失防止 (DLP) ポリシー
D. セキュリティとセキュリティのデータ損失防止 (DLP)
ポリシー。コンプライアンス管理センター
Answer: A
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/retention-policies EU PII wants both documents and email message to be preserved so S & C Admin Center for Retention. If this was for Email only, this probably could have been done in EAC.

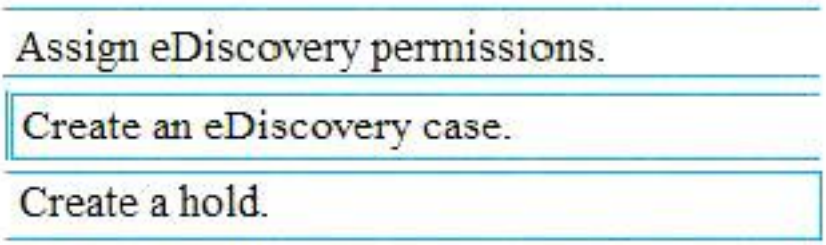
QUESTION NO: 14
法務部門の要件を満たす必要があります。
「セキュリティとセキュリティ」から順番に実行すべき 3
つのアクションはどれですか。コンプライアンス管理センター?回答するには、アクションのリストから適切なアクションを回答領域に移動し、正しい順序で並べます。

Actions	Answer Area
Create a data loss prevention (DLP) policy.	
Create an eDiscovery case.	
Create a label.	
Run a content search.	
Create a label policy.	
Create a hold.	
Assign eDiscovery permissions.	
Publish a label.	

Answer:



Explanation:



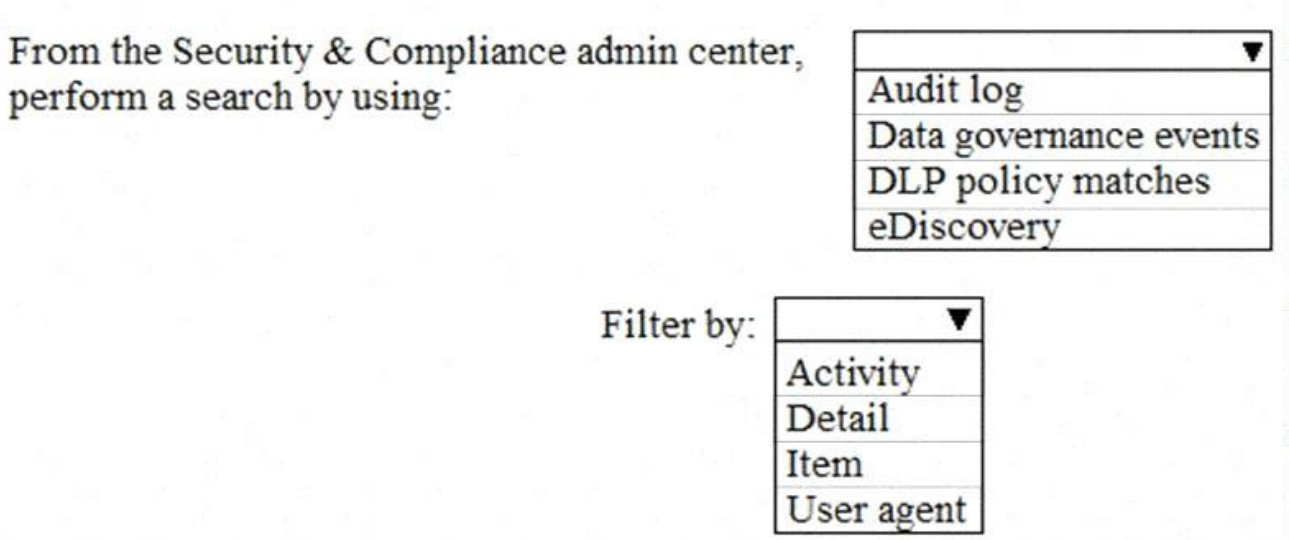
References:
https://www.sherweb.com/blog/ediscovery-office-365/

QUESTION NO: 15
技術要件を満たすには、米国の PII データを保護する必要があります。
何を作成する必要がありますか?
A. ドメイン例外を含むデータ損失防止 (DLP) ポリシー
B.
セキュリティとセキュリティ機密データを含むコンテンツを検出するコンプライアンス保持ポリシー
C. セキュリティとセキュリティアクティビティを含むコンプライアンス アラート ポリシー
D. ユーザー オーバーライドを含むデータ損失防止 (DLP) ポリシー
Answer: A

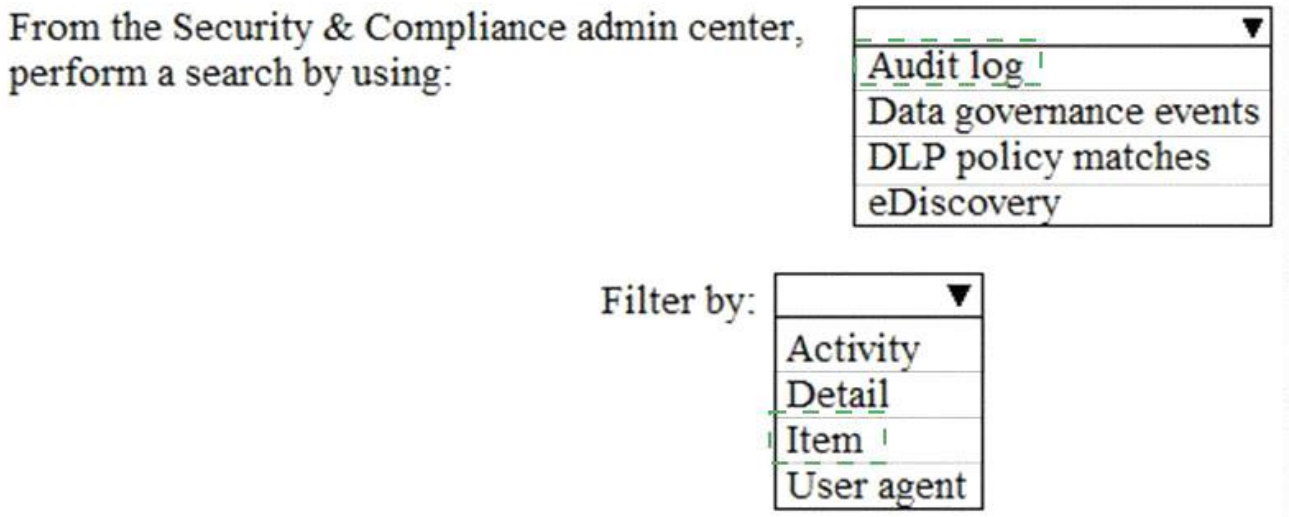
QUESTION NO: 16
セキュリティ管理者向けに解決策を提案する必要があります。その解決策は技術要件を満たしていなければなりません。
推薦状には何を含めるべきでしょうか？
A. Microsoft Microsoft Entra ID (Microsoft Entra ID) 特権ID管理
B. マイクロソフト エントラ ID (Microsoft Entra ID) ID 保護
C. Microsoft Entra ID (Microsoft Entra ID) 条件付きアクセス ポリシー
D. Microsoft Entra ID (Microsoft Entra ID) 認証方法
Answer: B

References:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access- conditions#sign-in-risk states clearly that Sign-in risk

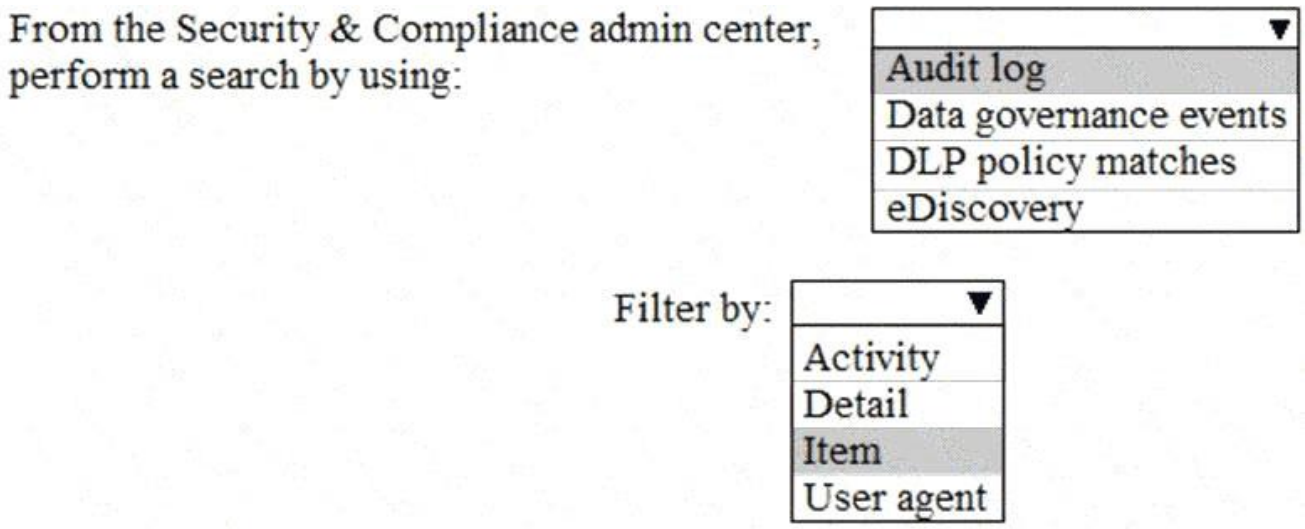
QUESTION NO: 17
SharePoint
管理者の技術要件を満たす必要があります。あなたは何をするべきか？回答するには、回答領域で適切なオプションを選択してください。注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



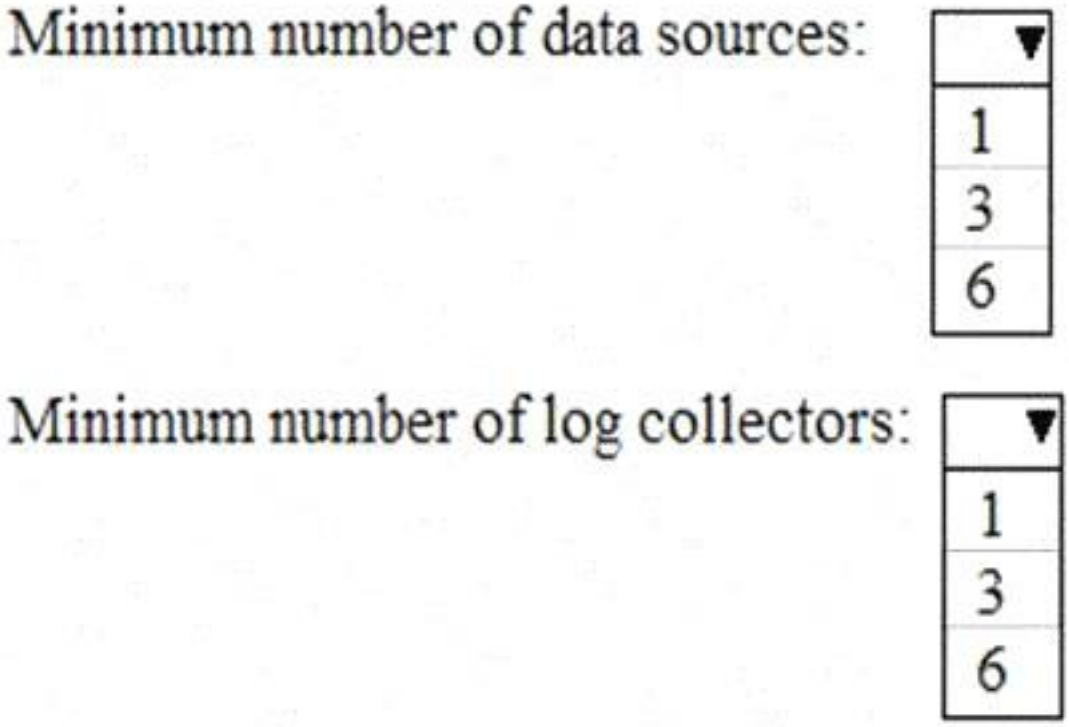
Explanation:



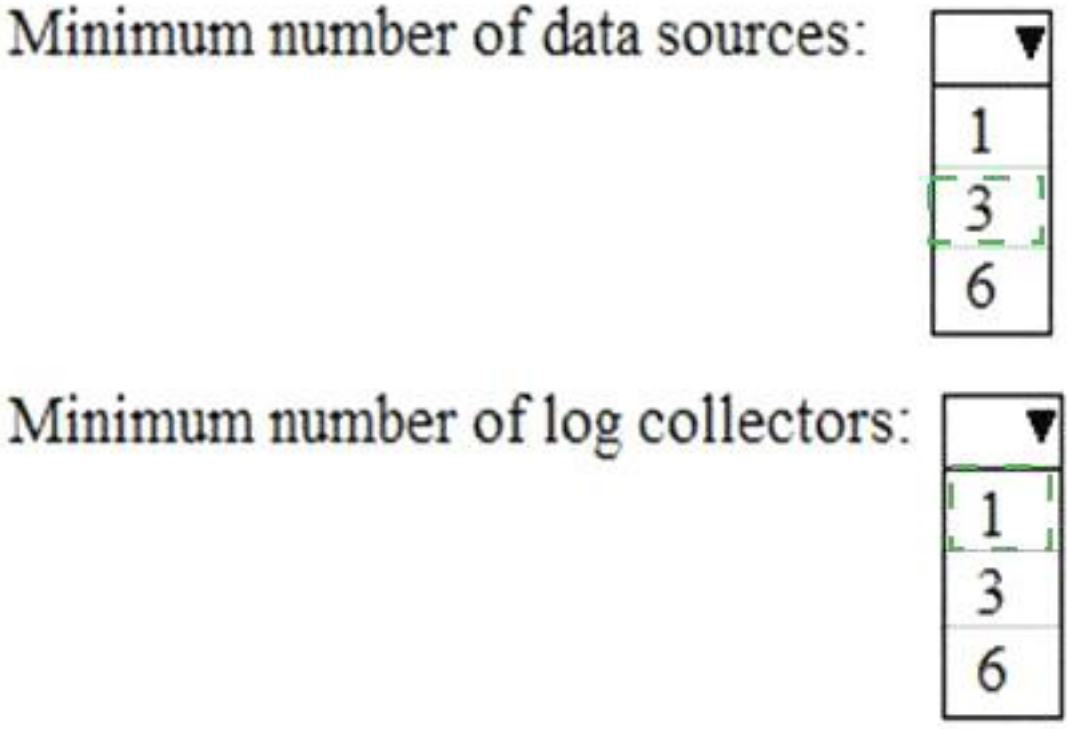
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/search-the-audit-log-in-security-and- compliance#step-3-filter-the-search-results

QUESTION NO: 18
ニューヨーク事務所の監査人はどの報告書を参照すべきでしょうか?
A. DLP ポリシーの一致
B. DLP の誤検知とオーバーライド
C. DLP インシデント
D. 上位の送信者と受信者
Answer: C
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/data-loss-prevention-policies
This report also shows policy matches over time, like the policy matches report. However, the policy matches report shows matches at a rule level; for example, if an email matched three different rules, the policy matches report shows three different line items. By contrast, the incidents report shows matches at an item level; for example, if an email matched three different rules, the incidents report shows a single line item for that piece of content. Because the report counts are aggregated differently, the policy matches report is better for identifying matches with specific rules and fine tuning DLP policies. The incidents report is better for identifying specific pieces of content that are problematic for your DLP policies.

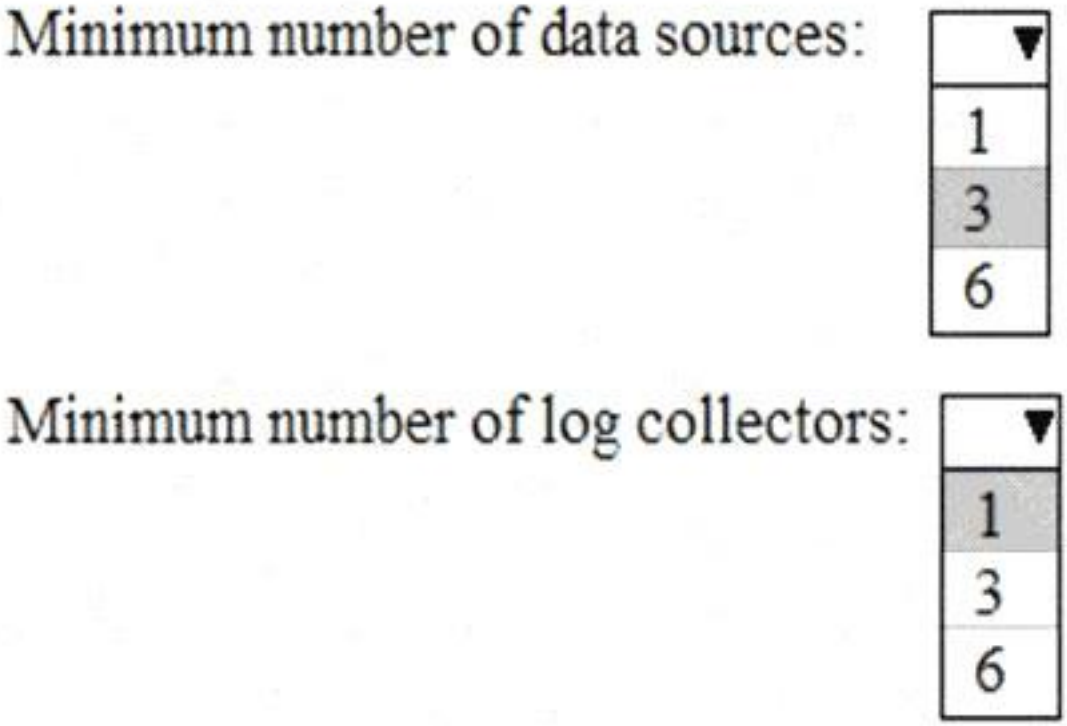
QUESTION NO: 19
ログ分析の技術要件を満たす必要があります。
Microsoft Cloud App Security から作成する必要があるデータ ソースとログ コレクターの最小数はいくつですか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



Explanation:



References:
https://docs.microsoft.com/en-us/cloud-app-security/discovery-docker

QUESTION NO: 20
大量のドキュメントを検索するための技術要件を満たす必要があります。何を作成する必要がありますか?
A. セキュリティとセキュリティのデータ損失防止 (DLP)
ポリシー。コンプライアンス管理センター
B. セキュリティとセキュリティからのアラート ポリシーコンプライアンス管理センター
C. Microsoft Cloud App Security のファイル ポリシー
D. Microsoft Cloud App Security のアクティビティ ポリシー
Answer: D
References:
https://docs.microsoft.com/en-us/office365/securitycompliance/activity-policies-and-alerts
Topic 3, Litware Inc.Case Study
This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.
To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.
At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.
To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

General Overviews

Litware, Inc. is a technology research company. The company has a main office in Montreal and a branch office in Seattle.

Environment

Existing Environment

The network contains an on-premises Active Directory domain named litware.com. The domain contains the users shown in the following table.

Name	Office
User1	Montreal
User2	Montreal
User3	Seattle
User4	Seattle

Microsoft Cloud Environment

Litware has a Microsoft 365 subscription that contains a verified domain named litware.com. The subscription syncs to the on-premises domain.

Litware uses Microsoft Intune for device management and has the enrolled devices shown in the following table.

Name	Platform
Device1	Windows 10
Device2	Windows 8.1
Device3	MacOS
Device4	iOS
Device5	Android

Litware.com contains the security groups shown in the following table.

Name	Members
UserGroup1	All the users in the Montreal office
UserGroup2	All the users in the Seattle office
DeviceGroup1	All the devices in the Montreal office
DeviceGroup2	All the devices in the Seattle office

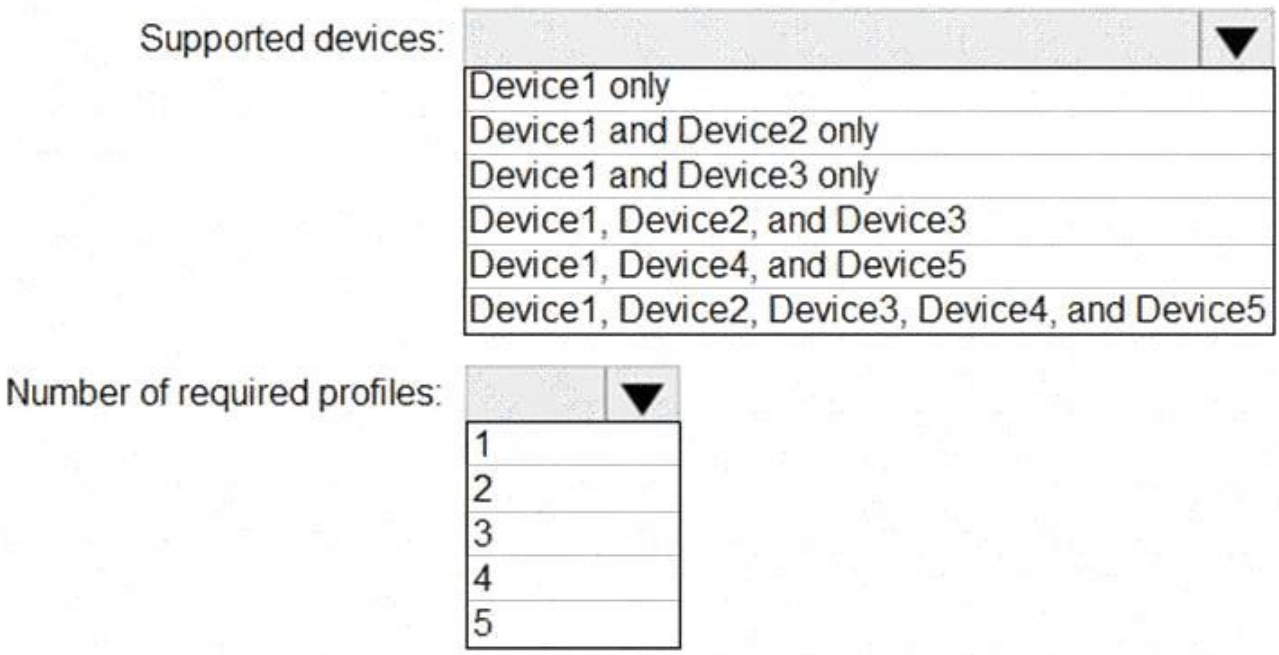
Litware uses Microsoft SharePoint Online and Microsoft Teams for collaboration.
The verified domain is linked to an Microsoft Entra ID (Microsoft Entra ID) tenant named litware.com. Audit log search is turned on for the litware.com tenant.
Problem Statements
Litware identifies the following issues:
Users open email attachments that contain malicious content.
Devices without an assigned compliance policy show a status of Compliant.
User1 reports that the Sensitivity option in Microsoft Office for the web fails to appear.
Internal product codes and confidential supplier ID numbers are often shared during Microsoft Teams meetings and chat sessions that include guest users and external users.
Requirements
Planned Changes
Litware plans to implement the following changes:
Implement device configuration profiles that will configure the endpoint protection template settings for supported devices.
Configure information governance for Microsoft OneDrive, SharePoint Online, and Microsoft Teams.
Implement data loss prevention (DLP) policies to protect confidential information.
Grant User2 permissions to review the audit logs of he litware.com tenant.
Deploy new devices to the Seattle office as shown in the following table.

Name	Platform
Device6	Windows 10
Device7	Windows 10
Device8	iOS
Device9	Android
Device10	Android

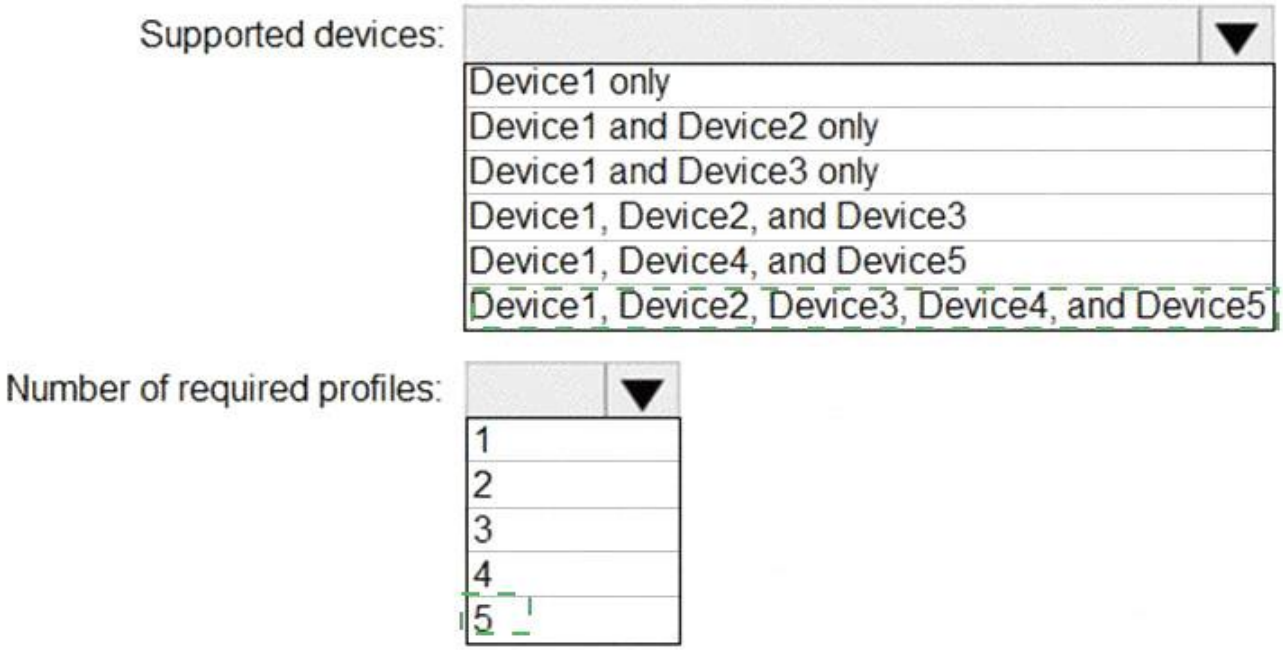
Implement a notification system for when DLP policies are triggered.
Configure a Safe Attachments policy for the litware.com tenant.
Technical Requirements
Litware identifies the following technical requirements:
Retention settings must be applied automatically to all the data stored in SharePoint Online sites, OneDrive accounts, and Microsoft Teams channel messages, and the data must be

retained for five years.
Emails messages that contain attachments must be delivered immediately, and placeholder must be provided for the attachments until scanning is complete.
All the Windows 10 devices in the Seattle office must be enrolled in Intune automatically when the devices are joined to or registered with Microsoft Entra ID.
Devices without an assigned compliance policy must show a status of Not Compliant in the Microsoft Endpoint Manager admin center.
A notification must appear in the Microsoft 365 compliance center when a DLP policy is triggered.
User2 must be granted the permissions to review audit logs for the following activities:
- Admin activities in Microsoft Exchange Online
- Admin activities in SharePoint Online
- Admin activities in Microsoft Entra ID
Users must be able to apply sensitivity labels to documents by using Office for the web.
Windows Autopilot must be used for device provisioning, whenever possible.
A DLP policy must be created to meet the following requirements:
- Confidential information must not be shared in Microsoft Teams chat sessions, meetings, or channel messages.
- Messages that contain internal product codes or supplier ID numbers must be blocked and deleted.
The principle of least privilege must be used.

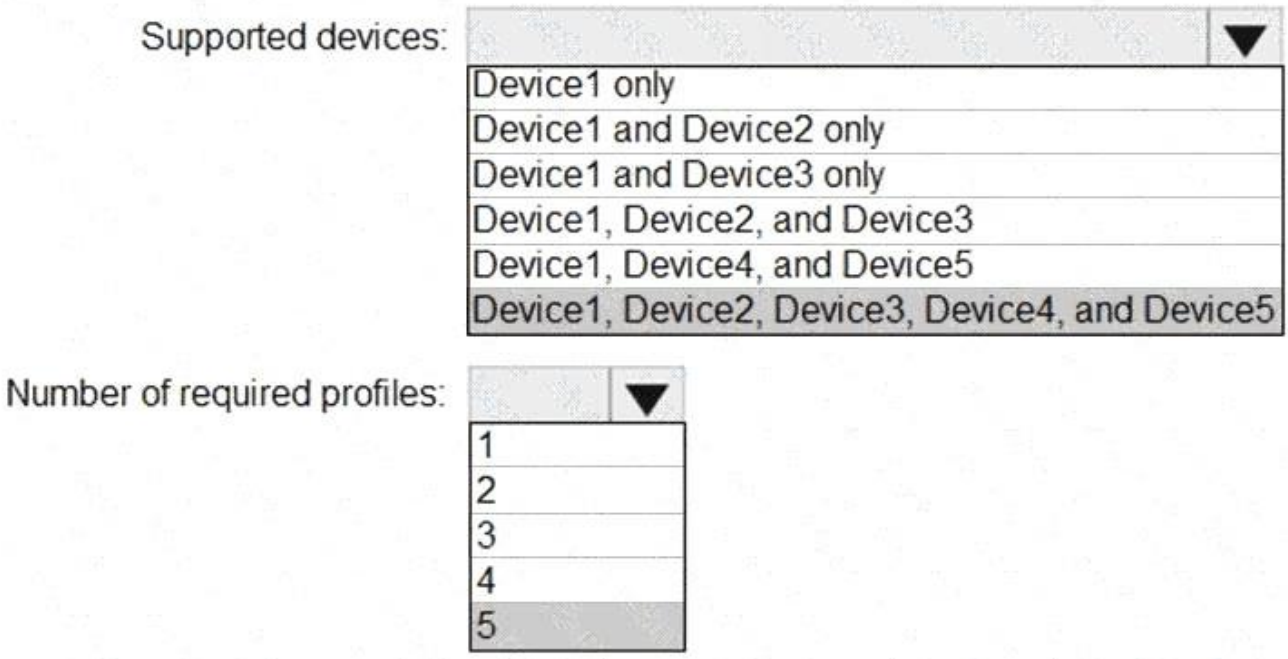
QUESTION NO: 21
計画された変更をサポートするために、エンドポイント保護デバイス構成プロファイルを実装する予定です。
どのデバイスがサポートされるか、および実装する必要があるプロファイルの数を特定する必要があります。
何を識別する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



Explanation:



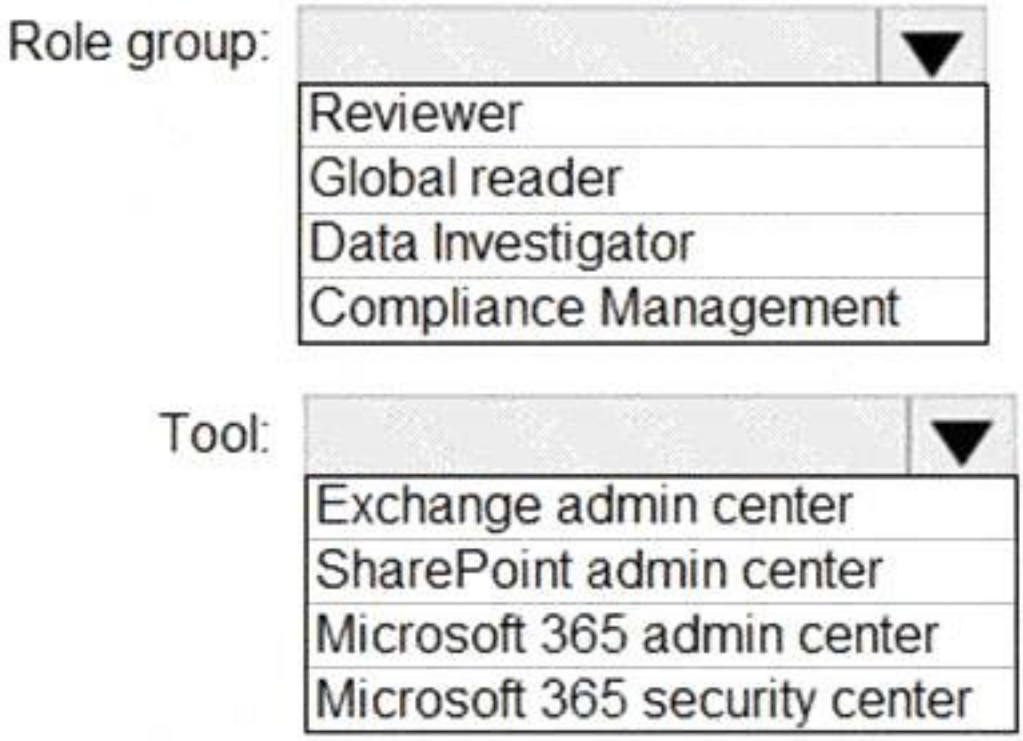
Reference:
https://docs.microsoft.com/en-us/mem/intune/configuration/device-profile-create

QUESTION NO: 22
技術要件を満たすために DLP ポリシーを作成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. 機密情報の種類
B. インサイダー リスク管理設定
C. イベントの種類
D. 機密ラベル
Answer: A
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide

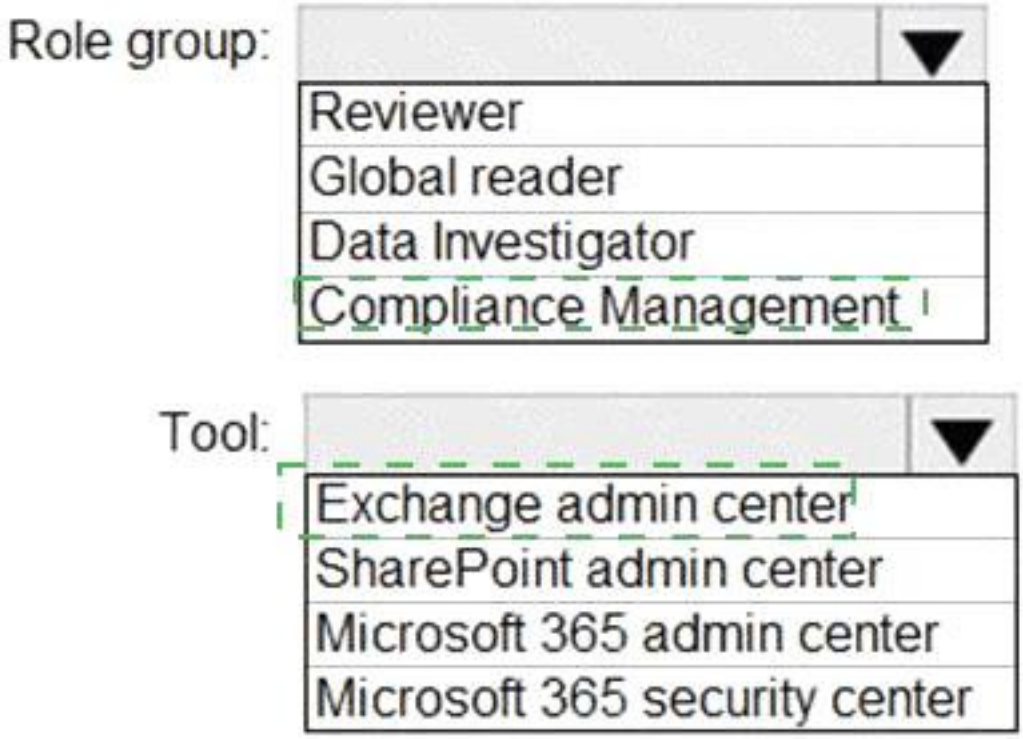
QUESTION NO: 23
計画された DLP ポリシーを作成します。
技術要件を満たすように通知を構成する必要があります。
あなたは何をするべきか ?
A. Microsoft 365 セキュリティ センターから、アラート ポリシーを構成します。
B. Microsoft エンドポイント マネージャー管理センターから、カスタム通知を構成します。
C. Microsoft 365 管理センターから、ブリーフィング電子メールを構成します。
D. Microsoft 365 コンプライアンス センターから、エンドポイント DLP 設定を構成します。
Answer: D
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-configure-view-alerts-policies?view=o365- worldwide

QUESTION NO: 24
技術要件を満たすには、安全な添付ファイル ポリシーを作成する必要があります。
どのオプションを選択する必要がありますか?
A. 置き換えます
B. リダイレクトを有効にする
C. ブロック
D. 動的配信
Answer: D
Reference:
https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security
/safe-attachments.md

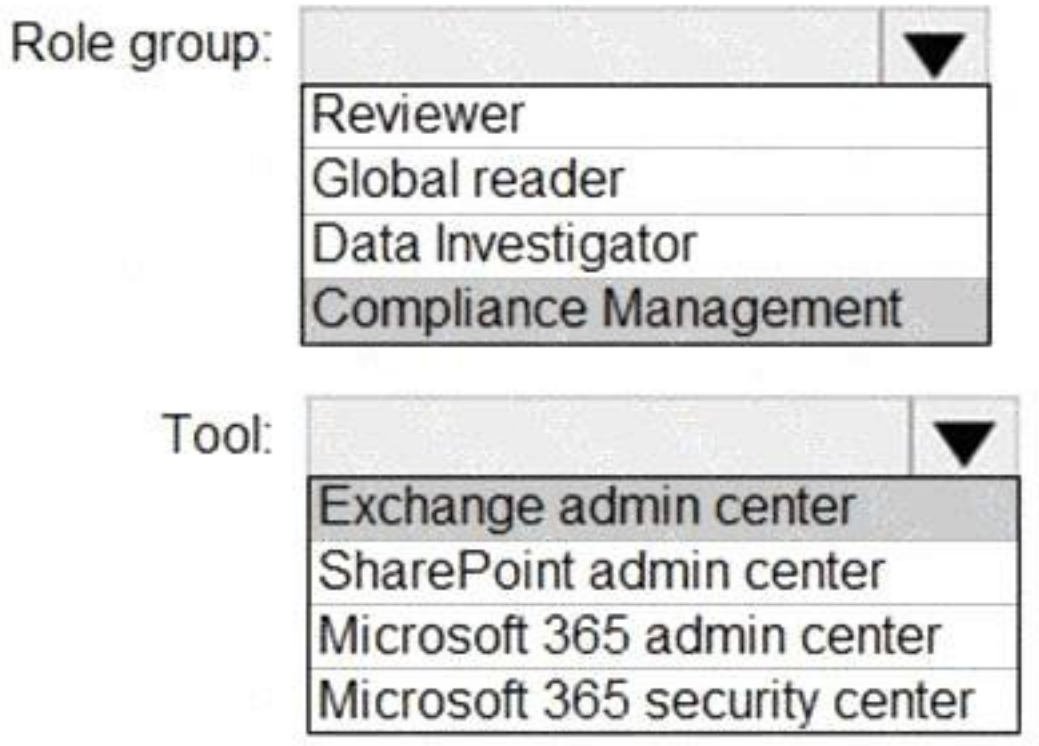
QUESTION NO: 25
User2
が監査ログを確認できることを確認する必要があります。ソリューションは技術要件を満たしている必要があります。
User2
をどの役割グループに追加し、何を使用する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



Explanation:



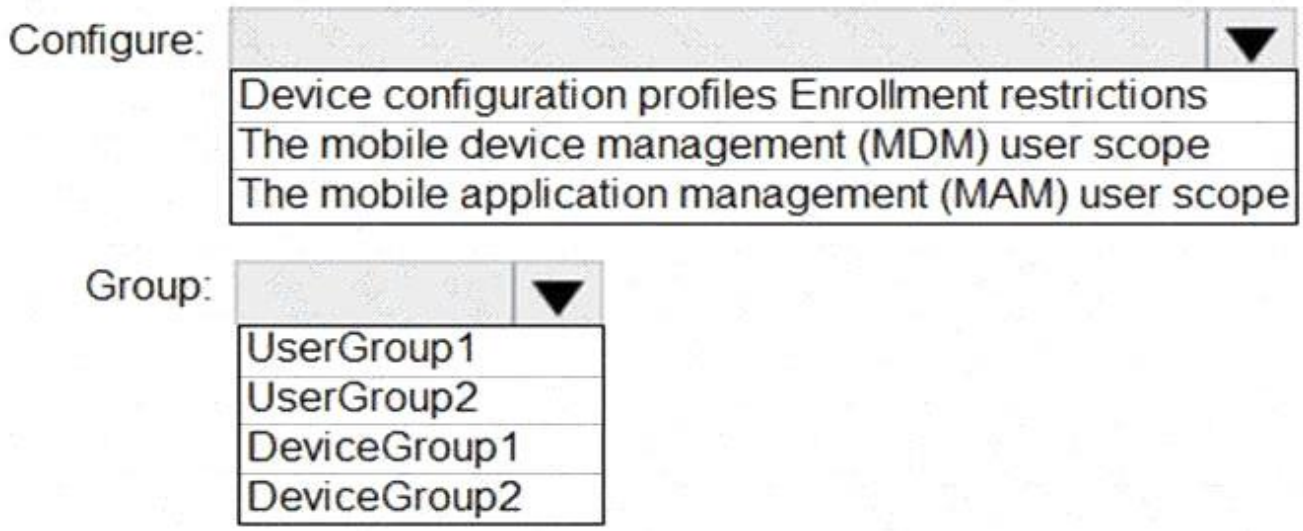
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/search-the-audit-log-in-security-and-compliance?
view=o365-worldwide

QUESTION NO: 26

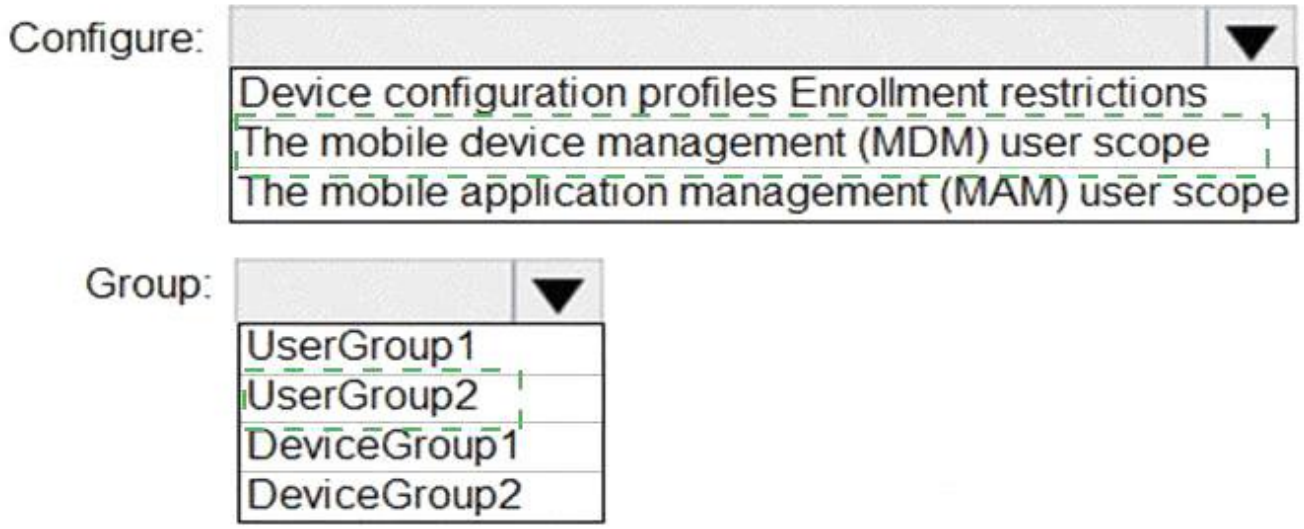
技術要件を満たすようにコンプライアンス設定を構成する必要があります。
Microsoft エンドポイント マネージャー管理センターでは何をする必要がありますか?
A. コンプライアンス ポリシーから、通知設定を変更します。
B. [場所] から、非準拠デバイス用の新しい場所を作成します。
C. [非準拠デバイスの廃棄] から、[すべてのデバイスの廃棄状態をクリア] を選択します。
D. コンプライアンス ポリシー設定を変更します。
Answer: D
Reference:
https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

QUESTION NO: 27
技術要件を満たすように Office on the Web を構成する必要があります。
あなたは何をするべきか？
A. グローバル リーダー ロールを User1 に割り当てます。
B. SharePoint Online および OneDrive で Office ファイルの秘密度ラベルを有効にします。
C. 機密ラベルを適用する自動ラベル付けポリシーを構成します。
D. Office アプリ管理者の役割を User1 に割り当てます。
Answer: B
Reference:
https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels-sharepoint-onedrive-files?
view=o365-worldwide

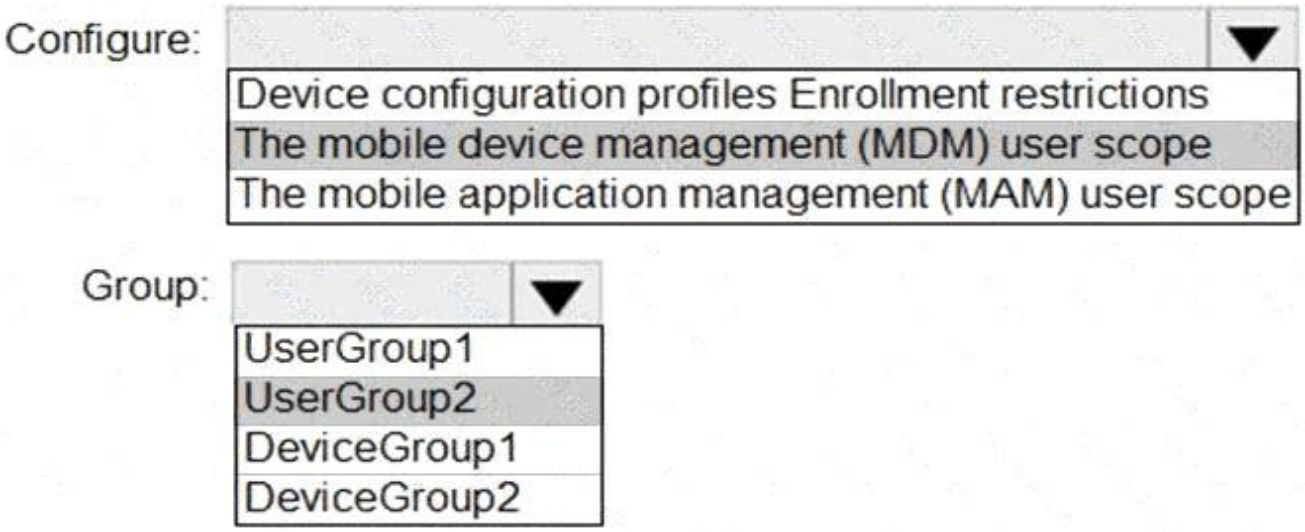
QUESTION NO: 28
Intune
で自動登録を構成する必要があります。ソリューションは技術要件を満たしている必要があります。
何を設定する必要がありますか?また、その設定をどのグループに割り当てる必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。



Answer:



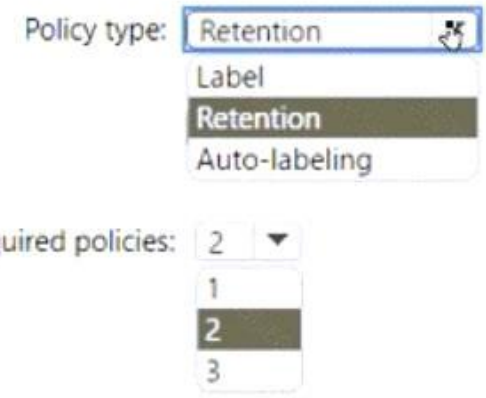
Explanation:



Reference:
https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll

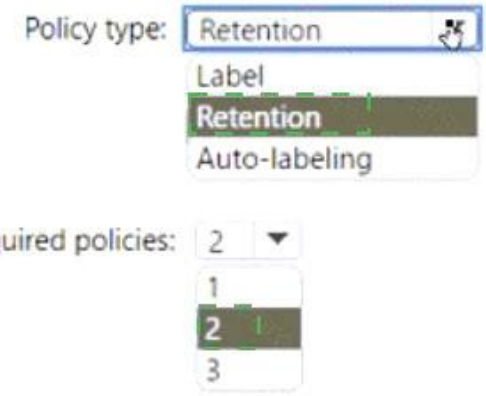
QUESTION NO: 29
技術要件を満たすように情報ガバナンス設定を構成する必要があります。
どのタイプのポリシーを構成する必要がありますか?また、いくつのポリシーを構成する必要がありますか?回答するには、回答領域で適切なオプションを選択してください。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area



Answer:

Answer Area



Explanation:

Answer Area

Topic 4, FabrikamOverview

Fabrikam, Inc. is an electronics company that produces consumer products. Fabrikam has 10,000 employees worldwide.

Fabrikam has a main office in London and branch offices in major cities in Europe, Asia, and the United States.

Existing Environment

Active Directory Environment

The network contains an Active Directory forest named fabrikam.com. The forest contains all the identities used for user and computer authentication. Each department is represented by a top-level organizational unit (OU) that contains several child OUs for user accounts and computer accounts.

All users authenticate to on-premises applications by signing in to their device by using a UPN format of username@fabrikam.com.

Fabrikam does NOT plan to implement identity federation.

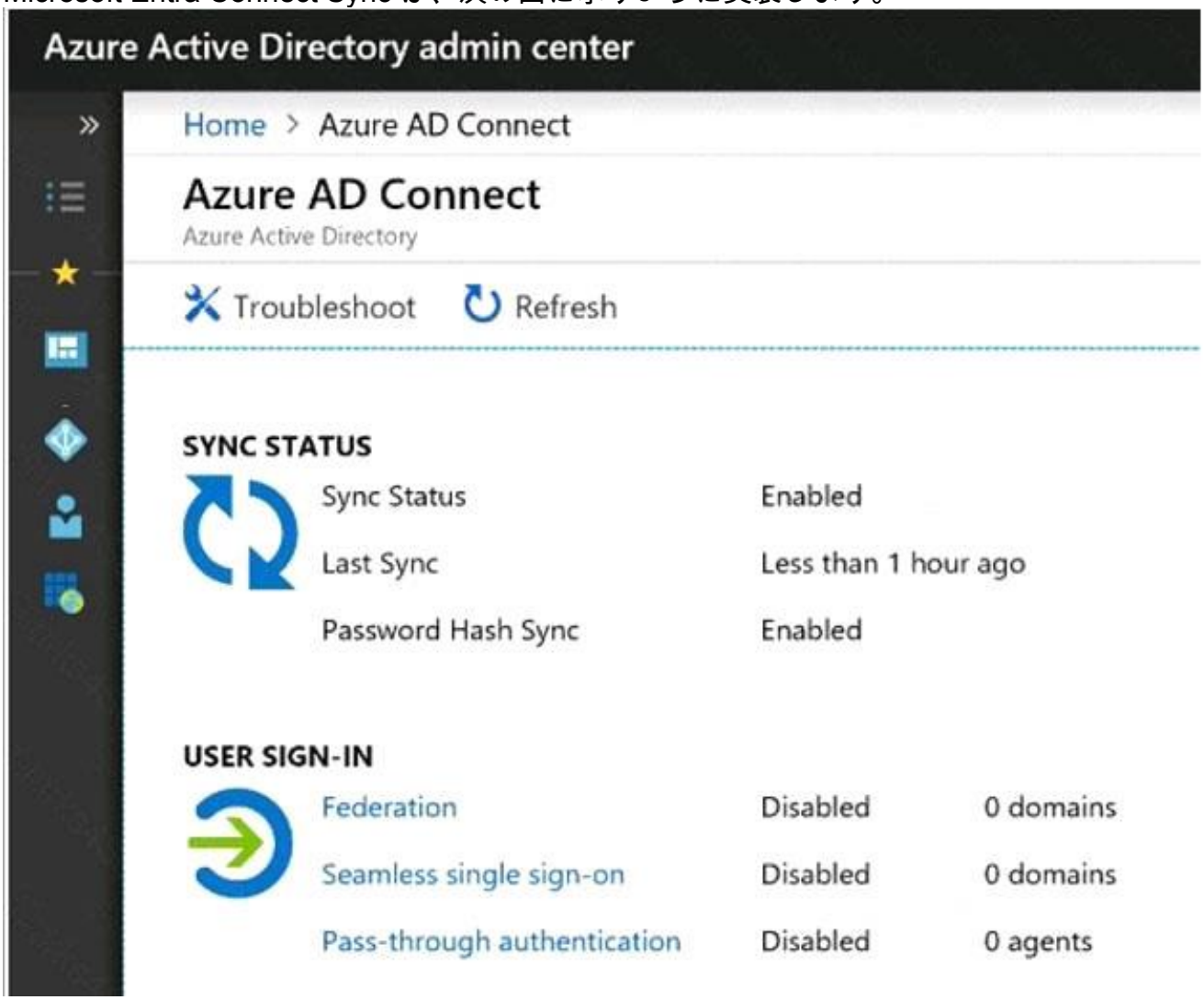
Network Infrastructure
Each office has a high-speed connection to the Internet.
Each office contains two domain controllers. All domain controllers are configured as DNS servers.
The public zone for fabrikam.com is managed by an external DNS server.
All users connect to an on-premises Microsoft Exchange Server 2016 organization. The users access their email by using Outlook Anywhere, Outlook on the web, or the Microsoft Outlook app for iOS. All the Exchange servers have the latest cumulative updates installed.
All shared company documents are stored on a Microsoft SharePoint Server farm.
Requirements
Planned Changes
Fabrikam plans to implement a Microsoft 365 Enterprise subscription and move all email and shared documents to the subscription.
Fabrikam plans to implement two pilot projects:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams will be enabled in Microsoft 365 for the sales department users.
Fabrikam plans to create a group named UserLicenses that will manage the allocation of all Microsoft 365 bulk licenses.
Technical Requirements
Fabrikam identifies the following technical requirements:
All users must be able to exchange email messages successfully during Project1 by using their current email address.
Users must be able to authenticate to cloud services if Active Directory becomes unavailable.
A user named User1 must be able to view all DLP reports from the Microsoft Purview compliance portal.
Microsoft 365 Apps for enterprise applications must be installed from a network share only.
Disruptions to email access must be minimized.
Application Requirements
Fabrikam identifies the following application requirements:
An on-premises web application named App1 must allow users to complete their expense reports online.
App1 must be available to users from the My Apps portal.
The installation of feature updates for Microsoft 365 Apps for enterprise must be minimized.
Security Requirements
Fabrikam identifies the following security requirements:
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
The membership of the UserLicenses group must be validated monthly. Unused user accounts must be removed from the group automatically.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
The principle of least privilege must be used.

QUESTION NO: 30

営業部門のすべてのユーザーが Project1 と Project2
中に正常に認証できることを確認する必要があります。
パイロット プロジェクトにはどの認証戦略を実装する必要がありますか?
A. パススルー認証
B. パススルー認証とシームレスな SSO
C. パスワード ハッシュ同期とシームレスな SSO
D. パスワードハッシュ同期
Answer: C
Explanation:
Project1: During Project1, the mailboxes of 100 users in the sales department will be moved to Microsoft 365.
Project2: After the successful completion of Project1, Microsoft Teams & Skype for Business will be enabled in Microsoft 365 for the sales department users.
After the planned migration to Microsoft 365, all users must be signed in to on-premises and cloud-based applications automatically.
Fabrikam does NOT plan to implement identity federation.
After the planned migration to Microsoft 365, all users must continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable password hash synchronization to enable the users to continue to authenticate to their mailbox and to SharePoint sites by using their UPN.
You need to enable SSO to enable all users to be signed in to on-premises and cloud-based applications automatically.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn

QUESTION NO: 31
User1 にどの役割を割り当てるべきですか?
利用可能な選択肢 (正しい選択肢をすべて選択してください)
A. 衛生管理
B. セキュリティリーダー
C. セキュリティ管理者
D. 記録管理
Answer: C
Explanation:
A user named User1 must be able to view all DLP reports from the Microsoft 365 admin center.
Users with the Security Reader role have global read-only access on security-related features, including all information in Microsoft 365 security center, Microsoft Entra ID, Identity Protection, Privileged Identity Management, as well as the ability to read Microsoft Entra ID sign-in reports and audit logs, and in Office
365 Security & Compliance Center.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles

QUESTION NO: 32
ホットスポット
Microsoft 365 テナントを作成します。
Microsoft Entra Connect Sync は、次の図に示すように実装します。



図に示された情報に基づいて、各記述を完成させる選択肢をドロップダウンメニューを使用して選択してください。
注：正解ごとに1ポイントが加算されます。

Answer Area

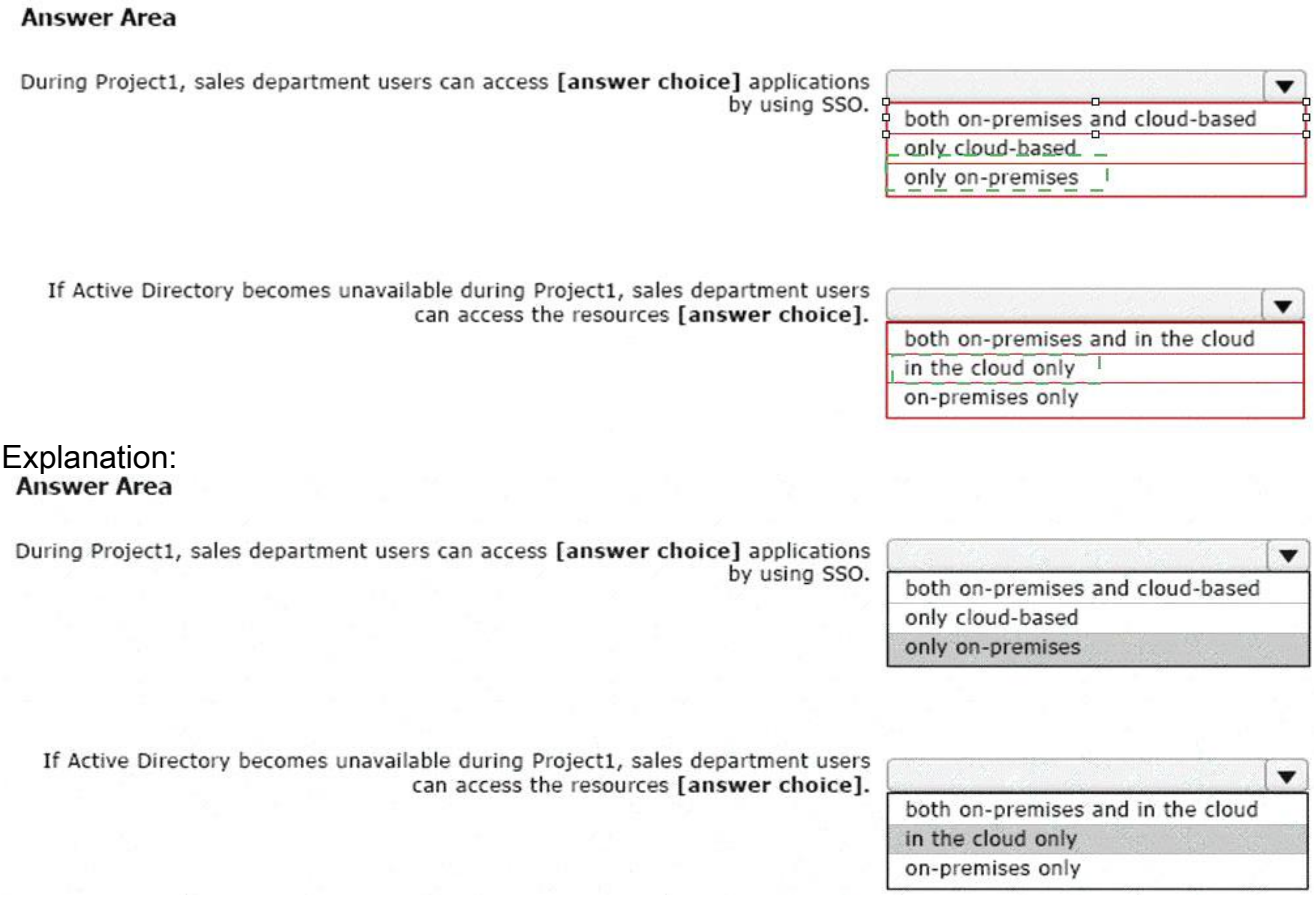
During Project1, sales department users can access **[answer choice]** applications by using SSO.

- both on-premises and cloud-based
- only cloud-based
- only on-premises

If Active Directory becomes unavailable during Project1, sales department users can access the resources **[answer choice]**.

- both on-premises and in the cloud
- in the cloud only
- on-premises only

Answer:



Explanation:

Box 1: only on-premises
In the exhibit, seamless single sign-on (SSO) is disabled. Therefore, as SSO is disabled in the cloud, the Sales department users can access only on-premises applications by using SSO.
In the exhibit, directory synchronization is enabled and active. This means that the on-premises Active Directory user accounts are synchronized to Microsoft Entra ID user accounts. If the on-premises Active Directory becomes unavailable, the users can access resources in the cloud by authenticating to Microsoft Entra ID. They will not be able to access resources on-premises if the on-premises Active Directory becomes unavailable as they will not be able to authenticate to the on-premises Active Directory.
Box 2: in the cloud only

QUESTION NO: 33
Project1 に必要なプロセスを評価しています。
プロジェクトのドメイン名を追加する際に、どの DNS レコードを作成する必要があるかを推奨する必要があります。
どの DNS レコードを推奨する必要がありますか?
A. ホスト (A)
B. ホスト情報
C. テキスト (TXT)
D. エイリアス (CNAME)
Answer: C
Explanation:

When you add a custom domain to Office 365, you need to verify that you own the domain. You can do this by adding either an MX record or a TXT record to the DNS for that domain.
Note:
There are several versions of this question in the exam. The question has two possible correct answers:
Text (TXT)
Mail exchanger (MX)
incorrect answer options you may see on the exam include the following:
alias (CNAME)
Host (A)
host (AAA)
Pointer (PTR)
Name Server (NS)
host information (HINFO)
pointer (PTR)
Reference:
https://docs.microsoft.com/en-us/office365/admin/get-help-with-domains/create-dns-records-at-any-dns- hosting-provider
Topic 5, Litware, IrkLitware, Irk. is a consulting company that has a
main office in Montreal and a branch office in Seattle?
Ltware collaborates with a third-party company named A. Datum Corporation.
The network of Litware contains an Active Directory domain named litware.com. The domain contains three organizational units (OUs) named LitwareAdmins, Montreal Users, and Seattle Users and the users shown in the following table.

Name	OU
Admin1	LitwareAdmins
Admin2	LitwareAdmins
Admin3	LitwareAdmins
Admin4	LitwareAdmins

The domain contains 2,000 Windows 10 Pro devices and 100 servers that run Windows Server 2019.
Litware has a pilot Microsoft 365 subscription that includes Microsoft Office 365 Enterprise E3 licenses and Microsoft Entra ID Premium P2 licenses.
The subscription contains a verified DNS domain named litware.com.
Microsoft Entra Connect Sync is installed and has the following configurations:
* Password hash synchronization is enabled.
* Synchronization is enabled for the UtwareAdmins OU only.
Users are assigned the roles shown in the following table.

Name	Role
Admin1	Global Administrator
Admin2	Helpdesk Administrator
Admin3	Security Administrator
Admin4	User Administrator

Self-service password reset (SSPR) is enabled.
The Microsoft Entra tenant has Security defaults enabled.
Litware identifies the following issues:
* Admin1 cannot create conditional access policies.
* Admin4 receives an error when attempting to use SSPR.
* Users access new Office 365 service and feature updates before the updates are reviewed by Admin2.
Litware plans to implement the following changes:
* Implement Microsoft Intune.
* Implement Microsoft Teams.
* Implement Microsoft Defender for Office 365.
* Ensure that users can install Office 365 apps on their device.
* Convert all the Windows 10 Pro devices to Windows 10 Enterprise E5.
* Configure Microsoft Entra Connect Sync to sync the Montreal Users OU and the Seattle Users OU.
Litware identifies the following technical requirements:
* Administrators must be able to specify which version of an Office 365 desktop app will be available to users and to roll back to previous versions.
* Only Admin2 must have access to new Office 365 service and feature updates before they are released to the company.
* Litware users must be able to invite A. Datum users to participate in the following activities:
o Join Microsoft Teams channels,
o Join Microsoft Teams chats,
o Access shared files.
* Just in time access to critical administrative roles must be required.
* Microsoft 365 incidents and advisories must be reviewed monthly.
* Office 365 service status notifications must be sent to Admin2.
* The principle of least privilege must be used.

QUESTION NO: 34
モントリオールユーザーおよびシアトルユーザーの組織単位(OU)に対する計画変更をサポートするには、Microsoft Entra Connect Sync を構成する必要があります。
あなたはどうすべきでしょうか？
A. Microsoft Entra Connect Sync ウィザードから、[同期オプションのカスタマイズ]を選択します。

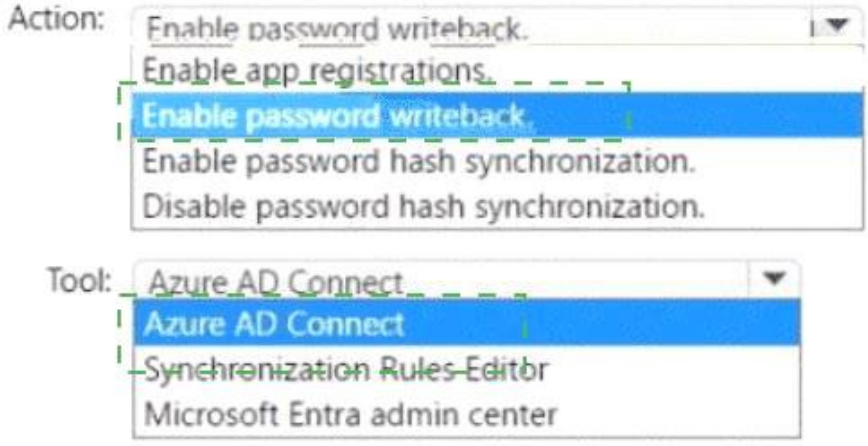
B.PowerShell から Add-ADSyncConnectorAttnbuteinclusion コマンドレットを実行します。
C. PowerShell から、start-ADSyncSyncCycle コマンドレットを実行します。
D. Microsoft Entra Connect Sync ウィザードから、[フェデレーションの管理]
を選択します。
Answer: A

QUESTION NO: 35
Admin4 が SSPR を使用できることを確認する必要があります。
どのツールを使用する必要がありますか。そしてどのアクションを実行する必要がありますか?回答するには、回答領域で適切なオプションを選択します。
注: 正しく選択するたびに 1 ポイントの価値があります。

Answer Area

Answer:

Answer Area



Explanation:

Answer Area